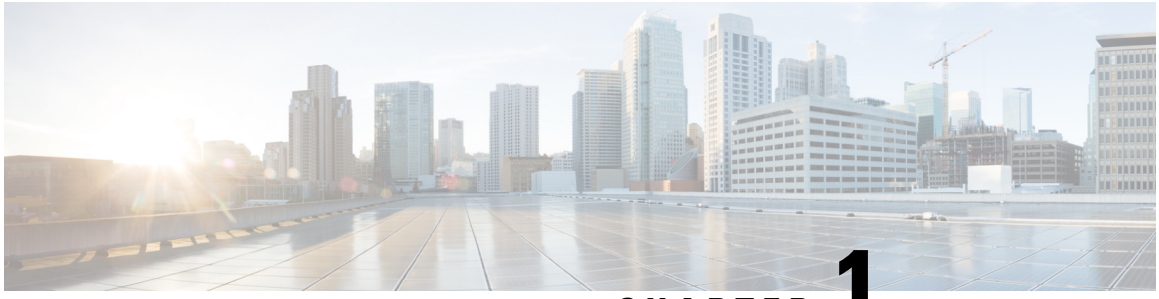
Cisco Crosswork Infrastructure 4.1 and Applications Installation Guide

First Published: 2021-11-12

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco Crosswork Overview

This chapter contains the following topics:

About this guide

This guide explains the requirements and process to install Cisco Crosswork Infrastructure, along with Cisco Crosswork Data Gateway and the Cisco Crosswork applications. It also explains the process to upgrade your Cisco Crosswork to the latest version. This guide is relevant for customers using the Cisco Crosswork Network Controller solution, the Cisco Routed Optical Networking solution, or any of the Crosswork applications.

There are Integrated Components that integrate with Cisco Crosswork, such as Cisco NSO, but they are NOT covered in this document. Please refer to the respective install documentation of those components for more details.

Audience

This guide is for experienced network users and operators who want to use Cisco Crosswork Infrastructure and applications in their network. This guide assumes that you are familiar with the following:

- Using a Docker container
- Running scripts in Python
- Deploying OVF templates using VMware vCenter
- Deploying using OVF tool
- Deploying a virtual machine on Cisco Cloud Services Platform (CSP)

Introduction

Cisco Crosswork Infrastructure is a microservices-based platform and is the foundation required for running Crosswork on-premise applications. It employs a cluster architecture to be extensible, scalable, and highly available. The Crosswork cluster consists of at least three VMs or nodes operating in a hybrid configuration. Additional VMs or nodes in a worker configuration can be added, as needed, to match the requirements of your network. A hybrid node can run infrastructure and application pods, while a worker node can run only application pods.

Note Hereafter in this guide, Cisco Crosswork Infrastructure is referred to as "Cisco Crosswork".

Cisco Crosswork uses **Cisco Crosswork Data Gateway (CDG)**, a software package that is separated out into its own Virtual Machine (VM), to gather information from the managed devices and forward it to Cisco Crosswork as well as external destinations. The information is then analyzed and processed by the Crosswork applications, and used to manage the network or respond to changes in the network. Crosswork Data Gateway can also be configured to collect and forward data from network devices to non-Crosswork users and applications. The number of Crosswork Data Gateways deployed in your network depends on the number of devices, the amount of data being collected, the overall topology, and your redundancy requirements. Please consult with your Cisco account team for guidance on your deployment to best meet your needs.

Integrated Components

Cisco Network Services Orchestrator functions as the provider for Crosswork to configure the devices according to their expected functions, including configuring model-driven telemetry (MDT) sensor paths, if any, for data collection. Cisco NSO is vital in supplying device management and configuration-maintenance services.

Cisco Segment Routing Path Computation Element (SR-PCE) is an IOS-XR multi-domain stateful PCE supporting both Segment Routing Traffic Engineering (ST-TE) and Resource Reservation Protocol Traffic Engineering (RSVP-TE). Cisco Crosswork uses the combination of telemetry and data collected from the Cisco SR-PCE to analyze and compute optimal TE tunnels.

Cisco Crosswork can also integrate with other providers (Cisco WAE, Syslog and Alert) and servers (TACACS+ and LDAP).

Cisco Crosswork Product Portfolio

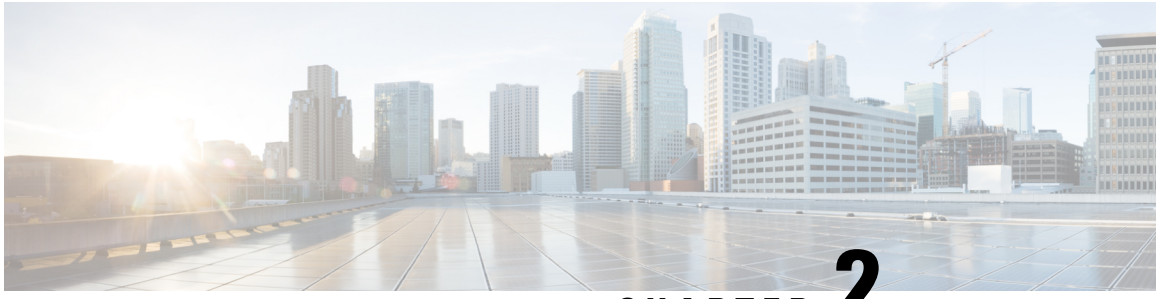
Cisco Crosswork Infrastructure provides a flexible platform to deploy different Crosswork products and each product is downloaded and added to the platform.

The list of Crosswork products are:

- **Cisco Crosswork Optimization Engine** is a Crosswork application that provides real-time network optimization allowing operators to effectively maximize network capacity utilization, as well as increase service velocity. Leveraging real-time protocols, such as BGP-LS and Path Computation Element Communication Protocol (PCEP) and Segment Routing Path Computation Element (SR-PCE) Cisco Crosswork Optimization Engine enables closed-loop tracking of the network state, quickly reacting to changes in network conditions to support a self-healing network.

- **Cisco Crosswork Zero Touch Provisioning** is a Crosswork application that allows users to quickly and easily bring up devices using a Cisco-certified software image and a day-zero software configuration of the customer's choice. After it is provisioned in this way and configured to Cisco NSO, the new device is onboarded to the Crosswork device inventory, where it can be monitored and managed like other devices.
- **Cisco Crosswork Network Controller** is an integrated Crosswork solution that combines essential components, such as Cisco Network Services Orchestrator, Segment Routing Path Computation Element (SR-PCE), Crosswork Active Topology, and Crosswork Optimization Engine. The solution enables you to proactively manage your end-to-end networks, and it provides intent-based and closed-loop automation solutions to ensure faster innovation, optimal user experience, and operational excellence.
  - **Cisco Crosswork Active Topology** application is a part of Cisco Crosswork Network Controller and it enables visualization of topology and services on logical and geographical maps.
  - **Cisco Crosswork Service Health (Automated Assurance)** application is an optional component of Cisco Crosswork Network Controller that overlays a service level view of the environment and makes it easier for operators to monitor if services (for example, L2/L3 VPN) are healthy based on the rules established by the operator.
  - **Cisco Crosswork Health Insights** application is an optional network health component of Cisco Crosswork Network Controller that performs real-time Key Performance Indicator (KPI) monitoring, alerting, and troubleshooting. Cisco Crosswork Health Insights enables programmable monitoring and analytics, and builds dynamic detection and analytics modules that allow operators to monitor and alert on network events based on user-defined logic.
  - **Cisco Crosswork Change Automation** application is an optional component of Cisco Crosswork Network Controller that automates the process of deploying changes to the network. Orchestration is defined via an embedded Ansible Playbook and then configuration changes are pushed to Cisco Network Services Orchestrator (NSO) to be deployed to the network.

For information on the installation and configuration requirements of Cisco Crosswork products, see Installation Dependencies for Cisco Crosswork Products, on page 18.



CHAPTER 2

Cisco Crosswork Installation Requirements

This chapter contains the following topics:

Cisco Crosswork Infrastructure Requirements

This section explains the requirements for installing the Cisco Crosswork.

The Crosswork cluster for 4.1 release consists of at least three VMs or nodes operating in a hybrid configuration. This is the minimum configuration necessary to support the applications in a typical network. Additional VMs or nodes in a worker configuration can be added later to scale your deployment, as needed, to match the requirements of your network or as other applications are introduced.

In addition to the Crosswork cluster VMs, at least one VM is needed to deploy Crosswork Data Gateway. This configuration can be scaled by adding additional resources if it is determined that either your use case requires more resources or to support Crosswork Data Gateway high availability (HA), or both.

The data center resources need to run NSO are addressed in the NSO installation Guide and are not addressed in this document.

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. For more information on manual installation, see Install Cisco Crosswork Manually, on page 38.
- 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, on page 6
- CSP Data Center Requirements, on page 7

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

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 (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
- Allowed hardware list:

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 3 VMs of the following minimum configuration: **VMware vCenter:** • Small (*for lab deployments only*): 8 vCPUs | 48 GB RAM Memory| 1 TB disk space | (Optional) 2 GB RAM disk • Large: 12 vCPUs | 96 GB RAM Memory | 1 TB disk space **Cisco CSP:** • Small (*for lab deployments only*): 8 CPU cores | 48 GB RAM Memory| 1 TB disk space | (Optional) 2 GB RAM disk • Large: 12 CPU cores | 96 GB RAM Memory | 1 TB disk space **Note** For assistance in adjusting VM Memory and CPU configuration post installation, contact your Cisco Customer Experience team. 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. • Upgrade of the cluster temporarily requires double the total disk space used by the cluster.
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.

Requirement	Description
IP Addresses	2 IP subnets, one for the Management network and one for Data network, with each allowing a minimum of 4 assignable IP addresses (IPv4 or IPv6). A Virtual IP (VIP) address is used to access the cluster, and then 3 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.

Port Requirements

As a general policy, ports that are not needed should be disabled. To view a list of all the open listening ports once all the applications are installed and active, log in as a Linux CLI admin user on any Crosswork cluster VM, and run the **netstat -aln** command.

The following ports are needed by Cisco Crosswork to operate correctly.

Table 2: External Ports

Port	Protocol	Usage
22	TCP	Remote SSH traffic
111	TCP/UDP	GlusterFS (port mapper)
179	TCP	Calico BGP (Kubernetes)
500	UDP	IPSec
2379/2380	TCP	Kubernetes etcd
4500	UDP	IPSec
6443	TCP	kube-apiserver (Kubernetes)
9100	TCP	Kubernetes metamonitoring
10250	TCP	kubelet (Kubernetes)
24007	TCP	GlusterFS
30603	TCP	User interface (NGINX server listens for secure connections on port 443)
30604	TCP	Used for Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server.
30606	TCP	Docker Registry
30607	TCP	Crosswork Data Gateway vitals collection
30608	TCP	Data Gateway gRPC channel with Data Gateway VMs
30609	TCP	Used by the Expression Orchestrator (Crosswork Service Health)
30610	TCP	Used by the Metric Scheduler (Crosswork Service Health)
30617	TCP	Used for Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server.
30620	TCP	Used to receive plug and play HTTP traffic on the ZTP server.

Port	Protocol	Usage
30621	TCP	For FTP (available on data interface only). The additional ports used for file transfer are 31121 (TCP), 31122 (TCP), and 31123 (TCP). This port is available only when the supported application is installed on Cisco Crosswork and the FTP settings are enabled.
30622	TCP	For SFTP (available on data interface only) This port is available only when the supported application is installed on Cisco Crosswork and the SFTP settings are enabled.
30649	TCP	To set up and monitor Crosswork Data Gateway collection status.
30650	TCP	astack gRPC channel with astack-client running on Data Gateway VMs
30993, 30994, 30995	TCP	Crosswork Data Gateway sending the collected data to Crosswork Kafka destination.
49152:49170	TCP	GlusterFS

Table 3: Destination Ports

Port	Protocol	Usage
7	TCP/UDP	Discover endpoints using ICMP
22	TCP	Initiate SSH connections with managed devices
53	TCP/UDP	Connect to DNS
123	UDP	Network Time Protocol (NTP)
830	TCP	Initiate NETCONF
2022	TCP	Used for communication between Crosswork and Cisco NSO (for NETCONF).
8080	TCP	REST API to SR-PCE
8888	TCP	Used for communication between Crosswork and Cisco NSO (for HTTPS).
20243	TCP	Used by the DLM Function Pack for communication between DLM and Cisco NSO
20244	TCP	Used to internally manage the DLM Function Pack listener during a Reload Packages scenario on Cisco NSO

Supported Web Browsers

After installing the Cisco Crosswork cluster, you require one of the following web browsers to log into the Cisco Crosswork UI:

Table 4: Supported Web Browsers

Browser	Version
Google Chrome (recommended)	75 or later
Mozilla Firefox	70 or later

The recommended display resolution: 1600 x 900 pixels or higher (minimum: 1366 x 768).

In addition to using a supported browser, all client desktops accessing geographical maps in the Crosswork applications must be able to reach the mapbox.com site. Customers not wishing to have Cisco Crosswork access an external site can choose to install the map files locally. For more information, see the *Set Up Maps* chapter in the *Cisco Crosswork Infrastructure 4.1 and Applications Administration Guide*.

Cisco Crosswork Data Gateway Requirements

You can deploy Crosswork Data Gateway on both VMware and Cisco Cloud Services Platform (Cisco CSP). This section provides information about the general guidelines and minimum requirements for installing Crosswork Data Gateway on both platforms.

- Crosswork Data Gateway VM Requirements
- Crosswork Data Gateway Ports Requirements

Cisco Crosswork Data Gateway VM Requirements

Cisco Crosswork Data Gateway provides two On-Premise deployment options:

1. **Standard**: Choose this option to install Crosswork Data Gateway to be used with all Crosswork applications, except Crosswork Health Insights, and Crosswork Service Health (Automated Assurance).
2. **Extended**: Choose this option to install Crosswork Data Gateway for use with Crosswork applications that need micro services to be deployed on the Crosswork Data Gateway - Crosswork Health Insights and Crosswork Service Health (Automated Assurance).

The table below lists the deployment profiles that must be used for installing Crosswork Data Gateway in each Crosswork product:

Note Extended Crosswork Data Gateways are compatible with applications that can otherwise use Standard Crosswork Data Gateways. If any of the deployed applications require Extended Crosswork Data Gateways, then the Crosswork Data Gateways of other applications should also be configured as Extended Crosswork Data Gateways only.

Table 5: Mandatory deployment type for Crosswork Data Gateway

Cisco Crosswork Product	Crosswork Data Gateway Deployment
Crosswork Network Controller (combination of Crosswork Active Topology & Crosswork Optimization Engine)	Standard
Crosswork Optimization Engine	Standard
Crosswork Change Automation	Extended
Crosswork Health Insights	Extended
Crosswork Zero Touch Provisioning	Standard
Crosswork Service Health (Automated Assurance)	Extended

The VM resource requirements for Crosswork Data Gateway differ between Standard and Extended deployments. As a result, Crosswork Data Gateway must be re-installed when moving from Standard to Extended configuration.

Requirements for both types of deployments are listed below.

Note The requirements are same for both VMware and Cisco CSP, unless stated otherwise.

Table 6: Cisco Crosswork Data Gateway VM Requirements

Requirement	Description
Data Center	VMware • VMware vSphere 6.7 or above. • VMware vCenter Server 7.0, ESXi 7.0 or later installed on hosts. • VMware vCenter Server 6.7 (Update 3g or later), ESXi 6.7 Update 1 installed on hosts. Cisco CSP • Cisco CSP 2.8.0.276 or later Allowed_hardware_list = ['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'] **Note** CSP host or cluster is setup and installed with a minimum of 2 physical ethernet interfaces. If you plan to install Crosswork Data Gateway on Cisco CSP, plan also for a third ethernet interface.

Requirement	Description
Memory	• Standard: 32 GB • Extended: 96 GB
Disk space	• Standard: 55 GB (Minimum) • Extended: 550 GB (Minimum)
vCPU	• Standard: 8 • Extended: 16

<table>
<tr><th>Requirement</th><th>Description</th></tr>
<tr><td>Interfaces</td><td>
Minimum: 1
Maximum: 3
Cisco Crosswork Data Gateway can be deployed with either 1, 2, or 3 interfaces as per the combinations below:
Note If you use one interface on your Crosswork cluster, you must use only one interface on the Crosswork Data Gateway. If you use two interfaces on your Crosswork Cluster, then you can use two or three interfaces on the Crosswork Data Gateway as per your network requirements.
<table>
<tr><th>No. of NICs</th><th>vNIC0</th><th>vNIC1</th><th>vNIC2</th></tr>
<tr><td>1</td><td>• Management Traffic
• Control/Data Traffic
• Device Access Traffic</td><td>—</td><td>—</td></tr>
<tr><td>2</td><td>• Management Traffic</td><td>• Control/Data Traffic
• Device Access Traffic</td><td>—</td></tr>
<tr><td>3</td><td>• Management Traffic</td><td>• Control/Data Traffic</td><td>• Device Access Traffic</td></tr>
</table>
• Management traffic: for accessing the UIs and command line and passing Control/Data information between servers (for example, a Crosswork application to Crosswork Data Gateway or NSO).
• Control/Data traffic: for data and configuration transfer between Cisco Crosswork Data Gateway and Crosswork applications and other external data destinations.
• Device access traffic: for device management (NSO or a Crosswork application to the devices as a result of KPI configuration or playbook execution) and telemetry data being forwarded to the Cisco Crosswork Data Gateway.
Note Due to security policies, traffic from subnets of a vNIC received on other vNICs is dropped. For example, in a 3 vNIC model setup, all device traffic (incoming and outgoing) must be routed through vNIC2. Crosswork Data Gateway drops device traffic received over vNIC0 and vNIC1 will be dropped.
</td></tr>
</table>

Requirement	Description
IP Addresses	1, 2, or 3 IPv4/IPv6 addresses based on the number of interfaces you choose to use. **Note** Crosswork does not support dual stack configurations. Therefore, ALL addresses for the environment must be either IPv4 or IPv6. During installation, you will need to provide IP address for Management Traffic and Control/Data Traffic only. IP address for Device Access Traffic is assigned during Crosswork Data Gateway pool creation as explained in the Section: *Create a Crosswork Data Gateway Pool* in the *Cisco Crosswork Infrastructure 4.1 and Applications Administration Guide*.
NTP Servers	The IPv4/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 devices, clients, and servers across your network. Confirm that the NTP IP address or host name is reachable on the network or installation will fail. Also, the ESXi hosts that will run the Crosswork application and Cisco 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. Confirm 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.

Crosswork Data Gateway Ports Requirements

The following tables show the minimum set of ports required for Crosswork Data Gateway to operate correctly.

Note SCP port can be tuned.

Inbound: Crosswork Data Gateway listens on the specified ports.

Outbound: Crosswork Data Gateway connects to external destination IP on the specified ports.

Table 7: Ports to be Opened for Management Traffic

Port	Protocol	Used for...	Direction
22	TCP	SSH server	Inbound
22	TCP	SCP client	Outbound
123	UDP	NTP Client	Outbound
53	UDP	DNS Client	Outbound

Port	Protocol	Used for...	Direction
30607	TCP	Crosswork Controller	Outbound

Table 8: Ports to be Opened for Device Access Traffic

Port	Protocol	Used for...	Direction
161	UDP	SNMP Collector	Outbound
1062	UDP	SNMP Trap Collector **Note** This is the default port. You customize this from the Interactive Console of the VM.	Inbound
9010	TCP	MDT Collector	Inbound
22	TCP	CLI Collector	Outbound
6514	TLS	Syslog Collector **Note** These are the default ports. You customize these values from the Interactive Console of the VM.	Inbound
9898	TCP		
9514	UDP		
Site Specific Default ports differ from XR, XE to vendor. Check platform-specific documentation.	TCP	gNMI Collector	Outbound

Table 9: Ports to be Opened for Control/Data Traffic

Port	Protocol	Used for...	Direction
30649	TCP	Crosswork Controller	Outbound
30993 30994 30995	TCP	Crosswork Kafka	Outbound

Port	Protocol	Used for...	Direction
Site Specific	Site Specific	Kafka and gRPC Destination	Outbound

Cisco NSO and NED Requirements

The requirements in the following table are applicable if you plan to use Cisco Network Services Orchestrator.

Table 10: Supported Cisco NSO and NED versions

Software/Driver	Version
Cisco Network Services Orchestrator (Cisco NSO)	5.5.2.12 You must install the necessary function packs based on the Crosswork applications that are being deployed. For more information, see Installation Dependencies for Cisco Crosswork Products, on page 18
Cisco Network Element Driver (NED)	**Cisco IOS XR:** • CLI: 7.33.12 • NETCONF: 6.6.3, 7.3, 7.315, 7.4.1 **Cisco IOS:** • CLI: 6.74.8

Installation Dependencies for Cisco Crosswork Products

This sections explains the installation and configuration dependencies for each Crosswork product.

Mandatory Function Packs

Depending on the Cisco Crosswork application or solution that you are using, there are mandatory Function Packs (FP) that must be installed to make the product functional. The table below provides references to each FP installation procedure:

Table 11: List of mandatory Function Packs

Crosswork Product	Required Function Pack
Crosswork Network Controller (combination of Crosswork Active Topology & Crosswork Optimization Engine)	• Cisco NSO Transport-SDN Function Pack Bundle Installation Guide 3.0 • Cisco NSO Transport-SDN Function Pack Bundle User Guide 3.0 • Cisco NSO DLM Service Pack Installation Guide 4.1.0 • Cisco Crosswork Telemetry Traffic Collector Function Pack Installation Guide 4.1.0-209
Crosswork Health Insights	• Cisco NSO DLM Service Pack Installation Guide 4.1.0 • Cisco Crosswork Telemetry Traffic Collector Function Pack Installation Guide 4.1.0-209 • Cisco Crosswork Change Automation NSO Function Pack Installation Guide 4.1.0
Crosswork Change Automation	
Crosswork Optimization Engine	• Cisco NSO DLM Service Pack Installation Guide 4.1.0 • Cisco Crosswork Telemetry Traffic Collector Function Pack Installation Guide 4.1.0-209

Providers Required

Cisco Crosswork applications rely on external services such as Cisco Network Services Orchestrator (NSO) or SR-PCE for various tasks like configuration changes, segment routing path computation, and so on. In order to manage the access and reuse of information between Crosswork applications, providers (such as NSO or SR-PCE) need to be configured for each external service. The provider family determines the type of service that provider supplies to Cisco Crosswork, and the parameters unique to that service, which must be configured.

Depending on what Crosswork application or solution is used, you must configure certain provider families with specific parameters, as explained in the table below:

Table 12: List of Mandatory Provider Configurations

Cisco Crosswork Product	Cisco NSO Provider	Cisco SR-PCE Provider
Crosswork Network Controller (combination of Crosswork Active Topology & Crosswork Optimization Engine)	Mandatory Required protocols are HTTPS and NETCONF. Set **Property Key** as *forward* and **Property Value** as *true*.	Mandatory Required protocol is HTTP.
Crosswork Optimization Engine	Optional	Mandatory Required protocol is HTTP.

Cisco Crosswork Product	Cisco NSO Provider	Cisco SR-PCE Provider
Crosswork Change Automation	Mandatory Required protocol is NETCONF. Set **Property Key** as *forward* and **Property Value** as *true*.	Optional
Crosswork Health Insights		
Crosswork Zero Touch Provisioning	Optional	Optional

Network Topology Models

The following figures show the different topology models, and the corresponding network components and connections needed to install and use Cisco Crosswork.

Figure 1: Cisco Crosswork - 1 NIC Network Topology

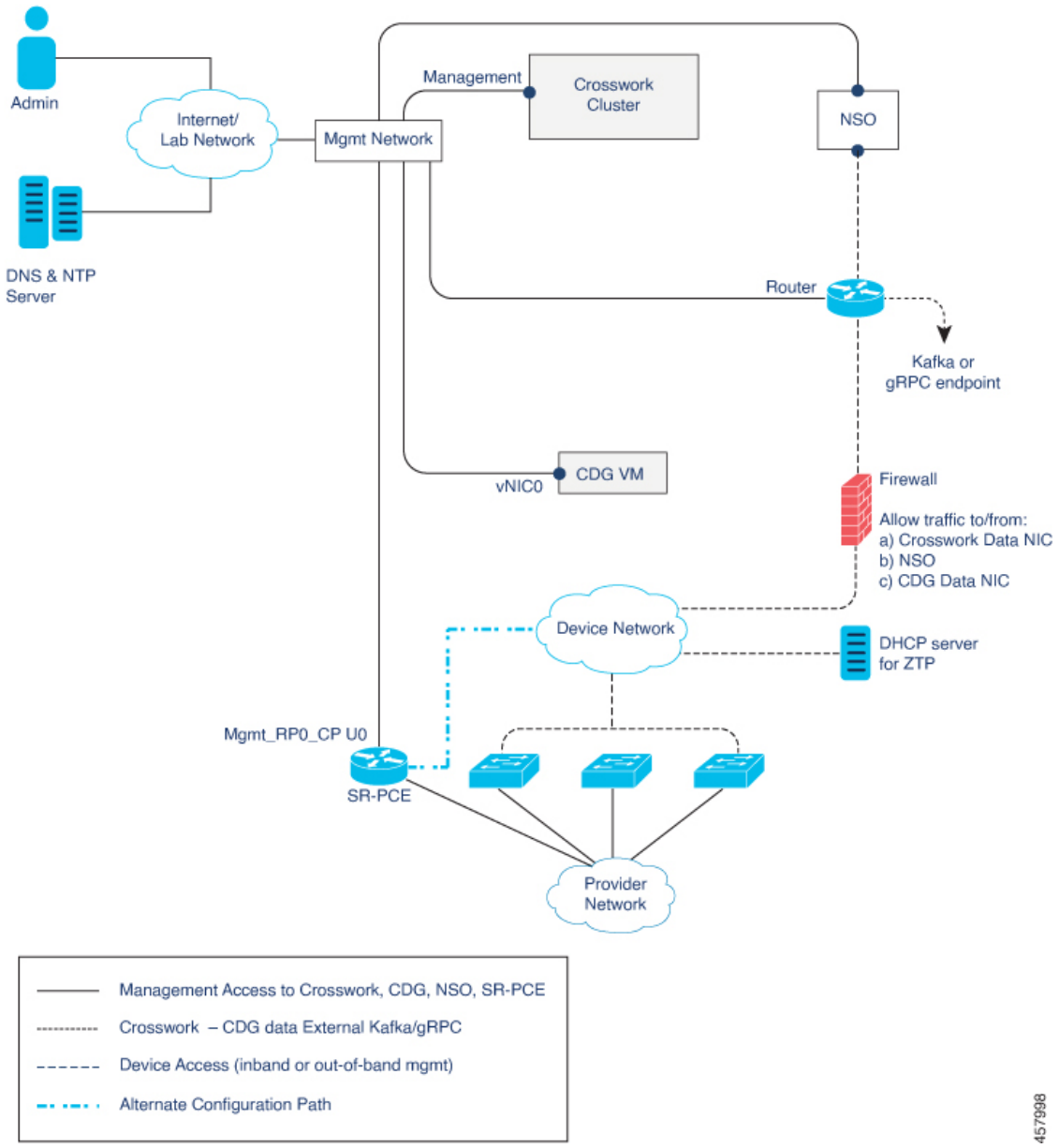


Figure 2: Cisco Crosswork - 2 NIC Network Topology

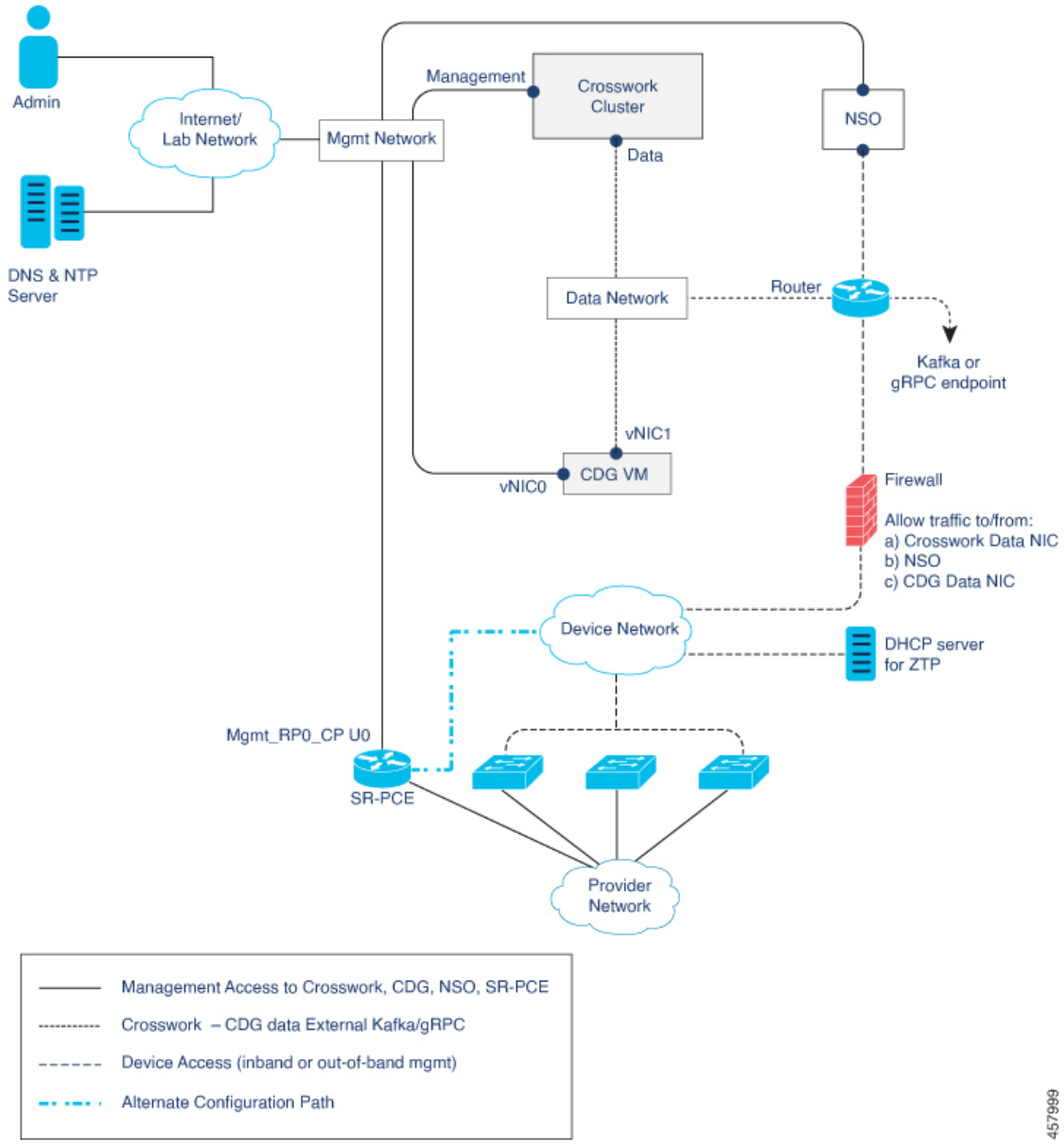
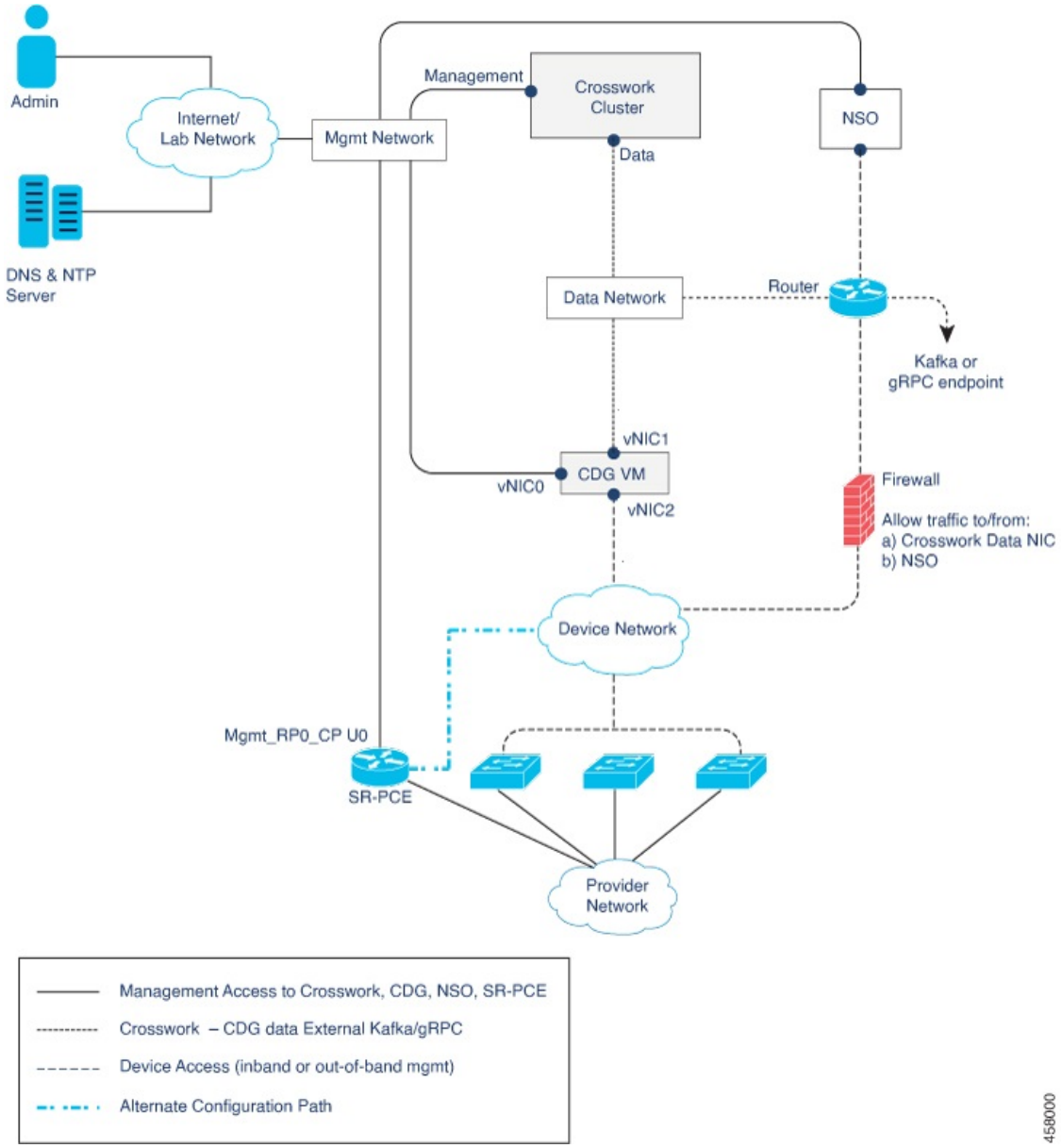


Figure 3: Cisco Crosswork - 3 NIC Network Topology



There are three types of traffic flowing between the network components, as explained below:

Table 13: Types of Network Traffic

Traffic	Description
Management	For accessing the UI and command line, and passing Data information between servers (for example, Cisco Crosswork to Crosswork Data Gateway or NSO)
Data	Data and configuration transfer between Crosswork Data Gateway and Cisco Crosswork, and other data destinations (external Kafka/gRPC).

Traffic	Description
Device Access	Device configuration and management, and telemetry data being forwarded to the Crosswork Data Gateway.

Cisco Crosswork Virtual Machine (VM)

The Cisco Crosswork VM has the following vNIC deployment options:

Table 14: Cisco Crosswork vNIC deployment modes

No. of vNICs	vNIC	Description
1	Management	Management, Data, and Device access passing through a single NIC
2	Management	Management
	Data	Data and Device access

Cisco Crosswork Data Gateway VM

The Cisco Crosswork Data Gateway VM has the following vNIC deployment options:

Note If you use one interface on your Crosswork cluster, you must use only one interface on the Crosswork Data Gateway. If you use two interfaces on your Crosswork Cluster, then you can use two or three interfaces on the Crosswork Data Gateway as per your network requirements.

Table 15: Cisco Crosswork Data Gateway vNIC deployment modes

No. of vNICs	vNIC	Description
1	vNIC0	Management, Data, and Device access passing through a single NIC
2	vNIC0	Management
	vNIC1	Data and Device access
3	vNIC0	Management
	vNIC1	Data
	vNIC2	Device Access

Cisco Network Services Orchestrator (NSO) VM

The NSO VM has the following vNICs:

- Management: Used for Crosswork applications to reach NSO.

- Device Access: Used for NSO to reach devices or NSO Resource Facing Services (RFS).

Note Preference for the number of vNICs can vary from one deployment to another. The number of vNICs can be dependent on the security and traffic isolation needs of the deployment. Crosswork Data Gateway and Crosswork accommodates this variability by introducing a variable number of vNICs.

Routed and Device Networks

Connectivity between the various components should be accomplished via an external routing entity. The figures show various line styles suggesting possible routing domains within the routed network.

- Solid - Management routing domain.
- Dotted - Data/Control routing domain (information transferred between Cisco Crosswork and Cisco Crosswork Data Gateway, and other data destinations (external Kafka or gRPC)).
- Dashes - Device access routing domain (from Cisco Crosswork Data Gateway and NSO).
- Blue dashes - Alternate SR-PCE configuration path

The IP/subnet addressing scheme on each of these domains depends on the type of deployment.

Routing between domains is needed for Crosswork and NSO to reach the devices. However, proper firewall rules need to be in place to allow only select sources (for example, Crosswork and NSO) to reach the devices.

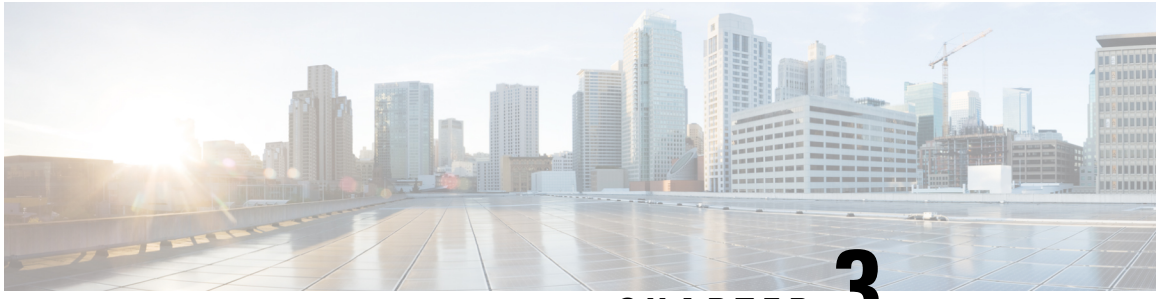
On the device network, devices can be reached in-band or using out-of-band management interfaces, depending on the local security policies of each deployment.

SR-PCE Configuration

The Segment Routing Path Computation Element (SR-PCE) is both a device and a Software-Defined Networking (SDN) controller. Some deployments may want to treat an SR-PCE instance as a device, in which case they would need access via the device network. Some deployments may want to treat an SR-PCE instance as an SDN controller and access it on the Management routing domain. Crosswork supports both models. By default, Crosswork will use **`eth0`** (Management) to access SR-PCE as an SDN controller on the Management domain (shown in the figures). To enable Crosswork access to an SR-PCE instance as a device on the device network (shown as alternate path in the figures): When adding an SR-PCE as a provider, add the **Property Key** and **Property Value** as **`outgoing-interface`** and **`eth1`** (Data) respectively.

ZTP Requirements

If you plan to use Zero Touch Provisioning, the device network needs to be equipped with a DHCP server (not provided with Cisco Crosswork). The devices must also have network connectivity to the Crosswork cluster as they will pull files (software and/or configuration) directly from the Crosswork cluster.



CHAPTER 3

Install the Crosswork Cluster

This chapter contains the following topics:

Available Installation Methods

The Cisco Crosswork cluster can be installed using the following methods:

- Install Cisco Crosswork using the Cluster Installer tool: Cluster installer tool is a one-time day 0 deployment tool that leverages VMware or Cisco CSP APIs to deploy all of the virtual machines needed to form your cluster and bring the system to an initial operational state. This is the recommended installation method.

  Note The installer tool will deploy the software and power on the virtual machines. If you wish to power on the virtual machines yourself, use the manual installation.

- Install Cisco Crosswork Manually: This option is available for deployments that cannot use the installer tool.

Installation Parameters

This section explains the important parameters that must be specified while installing the Crosswork cluster. Kindly ensure that you have relevant information to provide for each of the parameters mentioned in the table and that your environment meets all the requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.

Note Some of the below parameters are named differently depending upon the installation method (cluster installer tool or manual) and IP stack (IPv4 or IPv6) you choose. The aliases of such parameters are mentioned in the "*Also mentioned as*" column.

Parameter Name	Also mentioned as	Description
`ClusterName`		Name of the cluster file
`ClusterIPStack`	`CWIPv4Address`, `CWIPv6Address`	The IP stack protocol: IPv4 or IPv6
`ManagementIPAddress`	`ManagementIPv4Address`, `ManagementIPv6Address`	The Management IP address of the VM (IPv4 or IPv6).
`ManagementIPNetmask`	`ManagementIPv4Netmask`, `ManagementIPv6Netmask`	The Management IP subnet in dotted decimal format (IPv4 or IPv6).
`ManagementIPGateway`	`ManagementIPv4Gateway`, `ManagementIPv6Gateway`	The Gateway IP on the Management Network (IPv4 or IPv6). The address must be reachable, otherwise the installation will fail.
`ManagementVIP`		The Management Virtual IP for the cluster.
`ManagementVIPName`		Name of the Management Virtual IP for the cluster. This is an optional parameters used to reach Crosswork cluster Management VIP via DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server and must match the ManagementVIP and ManagementVIPName.
`DataIPAddress`	`DataIPv4Address`, `DataIPv6Address`	The Data IP address of the VM (IPv4 or IPv6).
`DataIPNetmask`	`DataIPv4Netmask`, `DataIPv6Netmask`	The Data IP subnet in dotted decimal format (IPv4 or IPv6).
`DataIPGateway`	`DataIPv4Gateway`, `DataIPv6Gateway`	The Gateway IP on the Data Network (IPv4 or IPv6). The address must be reachable, otherwise the installation will fail.
`DataVIP`		The Data Virtual IP for the cluster.
`DataVIPName`		Name of the Data Virtual IP for the cluster. This is an optional parameters used to reach Crosswork cluster Data VIP via DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server and must match the DataVIP and DataVIPName.
`DNS`	`DNSv4, DNSv6`	The IP address of the DNS server (IPv4 or IPv6). The address must be reachable, otherwise the installation will fail.

Parameter Name	Also mentioned as	Description
`NTP`		NTP server address or name. The address must be reachable, otherwise the installation will fail.
`DomainName`	`Domain`	The domain name used for the cluster
`CWusername`		Username to log into Cisco Crosswork.
`CWPassword`		Password to log into Cisco Crosswork.
`VMSize`		VM size for the cluster. Values are `small`(for lab deployments only) or `large`.
`VMName`		Name of the VM You will require at least 3 unique names (one for each VM).
`NodeType`	`VMType`	Indicates the type of VM. Choose either "Hybrid" or "Worker". **Note** The Crosswork cluster for 4.1 release requires at least three VMs operating in a hybrid configuration.
`IsSeed`		Choose "True" if this is the first VM being built in a new cluster. Choose "False" for all other VMs, or when rebuilding a failed VM.
`InitNodeCount`		Total number of nodes in the cluster including hybrid and worker nodes. The default value is 3.
`InitMasterCount`		Total number of hybrid nodes in the cluster. The default value is 3.
`BackupMinPercent`		Minimum percentage of the data disk space to be used for the size of the backup partition. The default value is 50 (valid range is from 1 to 80). Please use the default value unless recommended otherwise. **Note** The final backup partition size will be calculated dynamically. This parameter defines the minimum.
`ManagerDataFsSize`		Refers to the data disk size for Hybrid nodes (in Giga Bytes). This is an optional parameter and the default value is 450 (valid range is from 450 to 8000), if not explicitly specified. Please use the default value unless recommended otherwise.

Parameter Name	Also mentioned as	Description
`WorkerDataFsSize`		Refers to the data disk size for Worker nodes (in Giga Bytes). This is an optional parameter and the default value is 450 (valid range is from 450 to 8000), if not explicitly specified. Please use the default value unless recommended otherwise.
`ThinProvisioned`		Thin or thick provisioning for all disks. Set as "false" for live production deployments, and "true" for lab deployments.
`EnableHardReservations`		Determines the enforcement of VM CPU and Memory profile reservations. This is an optional parameter and the default value is `true`, if not explicitly specified. If set as `true`, the VM's resources are provided exclusively. In this state, the installation will fail if there are insufficient CPU cores, memory or CPU cycles. If set as `false` (only set for lab installations), the VM's resources are provided on best efforts. In this state, the installation will fail if there are insufficient CPU cores.
`RamDiskSize`	`ramdisk`	Size of the Ram disk. This parameter is only used for lab installations (value must be at least 2). When a non-zero value is provided for `RamDiskSize`, the `HSDatastore` value is not used.
VMware resource data		
`vCenterAddress`		The vCenter IP or host name.
`vCenterUser`		The username needed to log into vCenter.
`vCenterPassword`		The password needed to log into vCenter.
`DCname`		The name of the Data Center resource to use.
`MgmtNetworkName`		The name of the vCenter network to attach to the VM's Management interface.
`DataNetworkName`		The name of the vCenter network to attach to the VM's Data interface.
`Host`		The ESXi host or resource group name.
`Datastore`		The datastore name available to be used by this host or resource group.
`HSDatastore`		The high speed datastore available for this host or resource group.
`DCfolder`		The resource folder name on vCenter. Leave as empty if not used.

Parameter Name	Also mentioned as	Description
Cisco CSP resource data		
`name`	`Host`	Host name
`protocol`		Protocol used (e.g. "https")
`server`		Cisco CSP Server IP address
`username`		The username needed to log into Cisco CSP.
`password`		The password needed to log into Cisco CSP.
`insecure`		Default value is "true".
`MgmtNetworkName`		The name of the CSP network to attach to the VM's Management interface.
`DataNetworkName`		The name of the CSP network to attach to the VM's Data interface.

Install Cisco Crosswork using the Cluster Installer tool

This section describes how Cisco Crosswork is installed in VMware and Cisco CSP using the Cluster Installer tool.

- Install Cisco Crosswork on VMware vCenter , on page 32
- Install Cisco Crosswork on Cisco CSP, on page 35

The cluster installer tool is the recommended method to install Cisco Crosswork. It is a day 0 installation tool used to deploy the Crosswork cluster with user specified parameters supplied via a template file. The tool is run from a docker container which can be hosted on any docker capable platform including a regular PC/laptop. The docker container contains a set of template files which can be edited to provide the deployment specific data. Separate templates need to be used for vCenter and CSP deployments.

Note Docker version 19 or higher is recommended while using the cluster installer option. For more information on docker, see https://docs.docker.com/get-docker/

Few pointers to know when using the cluster installer tool:

- Make sure that your data center meets all the requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.
- The install script is safe to run multiple times. Upon error, input parameters can be corrected and re-run. However, it must be noted that running the tool multiple times may result in the deletion and re-creation of VMs.
- The edited template in the `/data` directory will contain sensitive information (VM passwords). The operator needs to manage access to this content. Erase them after use or when you quit the container.

- The `install.log`, `install_tf.log`, and `crosswork-cluster.tfstate` files will be created during the install and stored in the `/data` directory. If you encounter any trouble with the installation, provide these files to the Cisco Customer Experience team when opening a case.
- In case you are using the same installer tool for multiple Crosswork cluster installations, it is important to run the tool from different local directories, allowing for each deployment state files to be independent. The simplest way for doing so is to create on the host machine a local directory for each deployment on the host machine and map each one to the container accordingly.

Note In order to change install parameters or to correct parameters following installation errors, it is important to distinguish whether the installation has managed to deploy the VMs or not. Deployed VMs are evidenced by the output of the installer similar to:

```
vsphere_virtual_machine.crosswork-IPv4-vm["1"]: Creation complete after 2m50s
[id=4214a520-c53f-f29c-80b3-25916e6c297f]
```

In case of deployed VMs, changes to the CW VM settings or the Data Center host for a deployed VM are NOT supported. To change a setting using the installer when the deployed VMs are present, the clean operation needs to be run and the cluster redeployed.

A VM redeployment will delete the VM's data, hence caution is advised. We recommend you to perform VM parameter changes from the CW UI, or alternatively one VM at a time. Installation parameter changes that occur prior to any VM deployment, e.g. an incorrect vCenter parameter, can be performed by applying the change and simply re-running the install operation.

Install Cisco Crosswork on VMware vCenter

This section explains the procedure to install Cisco Crosswork on VMware vCenter using the cluster installer tool.

Before you begin

- Make sure that your environment meets all the vCenter requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.
- On running, the installer will upload the .ova file into the vCenter if it is not already present, and convert it into a VM template. After the installation is completed successfully, you can delete the template file from the vCenter UI (located under *VMs and Templates*) if the image is no longer needed.

Step 1 In your docker capable machine, create a directory where you will store everything you will use during the installation.

Step 2 Download the installer bundle (.tar.gz file) and the OVA file from cisco.com to the directory you created previously. For the purpose of these instructions, we will use the file names as **"cw-na-platform-4.1.0-38-installer-pkg.tar.gz"** and **"cw-na-platform-4.1.0-38-release-211108.ova"** respectively.

Step 3 Use the following command to unzip the installer bundle:

```
tar -xvf cw-na-platform-4.1.0-38-installer-pkg.tar.gz
```

The contents of the installer bundle is unzipped to a new directory (e.g. `cw-na-platform-4.1.0-38-installer`). This new directory will contain the installer image (e.g. **cw-na-platform-installer-4.1.0-38-release-211108.tar.gz**) and files necessary to validate the image.

Step 4 Navigate to the directory created in the previous step and use the following command to verify the signature of the installer image:

Note Use `python --version` to find out the version of python on your machine.

If you are using python 2.x, use the following command:

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

If you are using python 3.x, use the following command:

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

Note If you do not get a successful verification message, please contact the Cisco Customer Experience team.

Step 5 Use the following command to load the installer image file into your Docker environment.

```
docker load -i <.tar.gz file>
```

For example:

```
docker load -i cw-na-platform-installer-4.1.0-38-release-211108.tar.gz
```

The result will be a line similar to the following: (section we will need is underlined for clarity)

```
Loaded image ID: sha256:4a55858a7dd9a5fed7d0d46716e4c9525333525419e5517a4904093f01b3f165
```

Step 6 Launch the Docker container using the following command:

```
docker run --rm -it -v `pwd`:/data 4a55858a7dd9a5fed7d0d46716e4c9525333525419e5517a4904093f01b3f165
```

Note You do not have to enter that full value. In this case, "docker run --rm -it -v `pwd`:/data 4a5" was adequate. You only require enough of the image ID to uniquely identify the image you want to use for the installation.

Note In the above command, we are using the backtick (`). Do not use the single quote or apostrophe (') as the meaning to the shell is very different. By using the backtick (recommended), the template file and OVA will be stored in the directory where you are when you run the commands on your local disk, instead of inside the container.

```
My Machine% docker images
REPOSITORY                                          TAG       IMAGE ID       CREATED        SIZE
cw-na-platform-installer-4.1.0-38-release-211108    <none>    4a55858a7dd9   7 days ago     276MB
```

Step 7 Navigate to the directory with the VMware template.

```
cd /opt/installer/deployments/4.1.0/vcenter
```

Step 8 Copy the template file found under `/opt/installer/deployments/4.1.0/vcenter/deployment_template_tfvars` to the `/data` folder using a different name.

For example: `cp deployment_template_tfvars /data/deployment.tfvars`

For the rest of this procedure, we will use `deployment.tfvars` in all the examples.

Step 9 Edit the template file located in the `/data` directory, in a text editor, adding the necessary parameters:

- Crosswork cluster information such as VM size: Use "Small" for lab deployments, otherwise enter "Large". For more information, see the storage profiles in VM Host Requirements, on page 7.
- Unique Crosswork VM entries, including names, their IP addresses and node type settings.

  Note Use a strong VM Password (8 character long, including upper & lower case letters, numbers and one special character). The VM setup will fail if a weak password is used.

- vCenter access details and credentials, along with the assignment of the named Crosswork VMs to the Data Center resources.

Note A sample of the template file is posted at the end of this section. The file itself has two parts, the template that you need to fill in with the values for your environment and a set of example data to demonstrate how the information is formatted.

Step 10 From the terminal window, determine the container id and copy the OVA file to the `/data` directory in your container.

```
docker ps
CONTAINER ID     IMAGE            COMMAND       CREATED         STATUS         PORTS NAMES
1bda806bbd82     4a55858a7dd9     "/bin/sh"     3 hours ago     Up 3 hours     <port-name>
```

Note the container ID.

```
docker cp {image file name} {container id} :/data
```

For example: `docker cp cw-na-platform-4.1.0-38-release-211108.ova 1bda806bbd82:/data`

Step 11 Run the installer.

```
./cw-installer.sh install -p -m /data/<template file name> -o /data/<.ova file>
```

For example:

```
./cw-installer.sh install -p -m /data/deployment.tfvars -o
/data/cw-na-platform-4.1.0-38-release-211108.ova
```

Note If the installation fails, you should try rerunning the installation without the `-p` option. This will deploy the VMs serially rather than in parallel.

Step 12 Enter "yes" when prompted to accept the End User License Agreement (EULA).

Step 13 Enter "yes" when prompted to confirm the operation.

Note It is not uncommon to see some warnings like the following during the install:

```
Warning: Line 119: No space left for device '8' on parent controller '3'.
Warning: Line 114: Unable to parse 'enableMPTSupport' for attribute 'key' on element
'Config'.
```

If the install process proceeds to a successful conclusion (see sample output below), these warnings can be ignored.

Sample output:

```
cw_cluster_vms = <sensitive>
INFO: Copying day 0 state inventory to CW
INFO: Waiting for deployment status server to startup on 10.90.147.66. Elapsed time 0s,
retrying in 30s
Crosswork deployment status available at http://{VIP}:30602/grafana.monitoring
Once deployment is complete login to Crosswork via: https://{VIP}:30603/#/logincontroller

INFO: Cw Installer operation complete.
```

Example

See Sample manifest template for VMware vCenter, on page 123

What to do next

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the Installation, on page 52 to know how you can check the status of the installation.

Install Cisco Crosswork on Cisco CSP

This section explains the procedure to install Cisco Crosswork on Cisco CSP using the cluster installer tool.

Before you begin

- Make sure that your environment meets all the CSP requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.

Step 1 In your docker capable machine, create a directory where you will store everything you will use during the installation.

Step 2 Download the installer bundle (.tar.gz file) and the QCOW2 bundle (.tar.gz file) from cisco.com to the directory you created previously. For the purpose of these instructions, we will use the file names as **"cw-na-platform-4.1.0-38-installer-pkg.tar.gz"** and **"cw-na-platform-4.1.0-38-release-211108-qcow2-pkg.tar.gz"** respectively.

Step 3 Use the following command to unzip the installer bundle:

```
tar -xvf cw-na-platform-4.1.0-38-installer-pkg.tar.gz
```

The contents of the installer bundle is unzipped to a new directory (e.g. `cw-na-platform-4.1.0-38-installer`). This new directory will contain the installer image (e.g. **cw-na-platform-installer-4.1.0-38-release-211108.tar.gz**) and files necessary to validate the image.

Step 4 Navigate to the directory created in the previous step and use the following command to verify the signature of the installer image:

Note Use `python --version` to find out the version of python on your machine.

If you are using python 2.x, use the following command:

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

If you are using python 3.x, use the following command:

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

Note If you do not get a successful verification message, please contact the Cisco Customer Experience team.

Step 5 Use the following command to load the installer image file into your Docker environment.

```
docker load -i <.tar.gz file>
```

For example:

```
docker load -i cw-na-platform-installer-4.1.0-38-release-211108.tar.gz
```

The result will be a line similar to the following: (section we will need is underlined for clarity)

```
Loaded image ID: sha256:4a55858a7dd9a5fed7d0d46716e4c9525333525419e5517a4904093f01b3f165
```

Step 6 Launch the Docker container using the following command:

```
docker run --rm -it -v `pwd`:/data 4a55858a7dd9a5fed7d0d46716e4c9525333525419e5517a4904093f01b3f165
```

Note You do not have to enter that full value. In this case, "docker run --rm -it -v `pwd`:/data 4a5" was adequate. You only require enough of the image ID to uniquely identify the image you want to use for the installation.

Note In the above command, we are using the backtick (`). Do not use the single quote or apostrophe (') as the meaning to the shell is very different. By using the backtick (recommended), the template file and QCOW2 will be stored in the directory where you are when you run the commands on your local disk, instead of inside the container.

```
My Machine% docker images
REPOSITORY                                          TAG       IMAGE ID       CREATED        SIZE
cw-na-platform-installer-4.1.0-38-release-211108    <none>    4a55858a7dd9   7 days ago     276MB
```

Step 7 Navigate to the directory with the CSP template.

```
cd /opt/installer/deployments/4.1.0/csp
```

Step 8 Copy the template file found under `/opt/installer/deployments/4.1.0/csp/deployment_template_tfvars` to the `/data` folder using a different name.

For example: `cp deployment_template_tfvars /data/deployment.tfvars`

For the rest of this procedure, we will use `deployment.tfvars` in all the examples.

Step 9 Edit the template file located in the `/data` directory, in a text editor, adding the necessary parameters:

- Crosswork cluster information such as VM size: Use "Small" for lab deployments, otherwise enter "Large".
- Unique Crosswork VM entries, including names, their IP addresses and node type settings.

Note Use a strong VM Password (8 character long, including upper & lower case letters, numbers and one special character). The VM setup will fail if a weak password is used.

- Cisco CSP access details and credentials, along with the assignment of the named Crosswork VMs to the Cisco CSP host resources.

Note A sample of the template file is posted at the end of this section. The file itself has two parts, the template that you need to fill in with the values for your environment and a set of example data to demonstrate how the information is formatted.

Step 10 From the terminal window, unzip the QCOW2 bundle (.tar.gz file):

```
tar -xvf cw-na-platform-4.1.0-38-release-211108-qcow2-pkg.tar.gz
```

The contents of the QCOW2 bundle is unzipped to a new directory (e.g. `cw-na-platform-4.1.0-38-release-211108-qcow2`). This new directory will contain the QCOW2 image (e.g. **cw-na-platform-4.1.0-38-release-211108-qcow2.tar.gz**) and files necessary to validate the image.

Step 11 Navigate to the directory created in the previous step, and use the following command to verify the signature of the QCOW2 image:

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

Note If you do not get a successful verification message, please contact the Cisco Customer Experience team.

Step 12 Run the installer.

```
./cw-installer.sh install -t csp -m /data/<template file name> -o /data/<qcow2.tar.gz file> -p
```

For example:

```
./cw-installer.sh install -t csp m /data/deployment.tfvars -o
/data/cw-na-platform-4.1.0-38-release-211108-qcow2.tar.gz -p
```

Note If the installation fails, you should try rerunning the installation without the `-p` option. This will deploy the VMs serially rather than in parallel.

Step 13 Enter "yes" when prompted to accept the End User License Agreement (EULA).

Step 14 Enter "yes" when prompted to confirm the operation.

Example

See Sample manifest template for Cisco CSP, on page 124.

What to do next

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the Installation, on page 52 to know how you can check the status of the installation.

Install Cisco Crosswork Manually

This section describes how Cisco Crosswork can be manually installed in VMware and Cisco CSP.

- Manual Installation of Cisco Crosswork using vSphere UI, on page 38
- Manual Installation of Cisco Crosswork on Cisco CSP, on page 46

Manual Installation of Cisco Crosswork using vSphere UI

This section explains the procedure to manually install Cisco Crosswork on VMware vCenter using the vSphere UI. The procedure needs to repeated for each node in the cluster.

The manual installation workflow is broken into two parts. In the first part, you create a template. In the second part, you deploy the template as many times as needed to build the cluster of 3 hybrid nodes (typically) along with any worker nodes that your environment requires.

Before you begin

- Make sure that your environment meets all the vCenter requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.

Step 1 Download the latest available Cisco Crosswork image file (*.ova) to your system.

Step 2 With VMware ESXi running, log into the VMware vSphere Web Client. On the left navigation pane, choose the ESXi host on which you want to deploy the VM.

Step 3 Choose **Actions** > **Deploy OVF Template**.

Caution The default VMware vCenter deployment timeout is 15 minutes. The total time needed to deploy the OVA image file may take much longer than 15 minutes, depending on your network speed and other factors. If vCenter times out during deployment, the resulting VM will be unbootable. To prevent this, we recommend that you either set the vCenter deployment timeout to a much longer period (such as one hour), or unTAR the OVA file before continuing, and then deploy using the OVA's four separate Open Virtualization Format and Virtual Machine Disk component files: cw.ovf, cw_rootfs.vmdk, cw_dockerfs.vmdk, and cw_extrafs.vmdk.

Step 4 The VMware **Deploy OVF Template** window appears, with the first step, **1 - Select an OVF template**, highlighted. Click **Choose Files** to navigate to the location where you downloaded the OVA image file and select it. Once selected, the file name is displayed in the window.

Step 5 Click **Next**. The **Deploy OVF Template** window is refreshed, with **2 - Select a name and folder** now highlighted. Enter a name and select the respective Datacenter for the Cisco Crosswork VM you are creating.

We recommend that you include the Cisco Crosswork version and build number in the name, for example: Cisco Crosswork 4.0 Build 152.

Step 6 Click **Next**. The **Deploy OVF Template** window is refreshed, with **3 - Select a compute resource** highlighted. Select the host for your Cisco Crosswork VM.

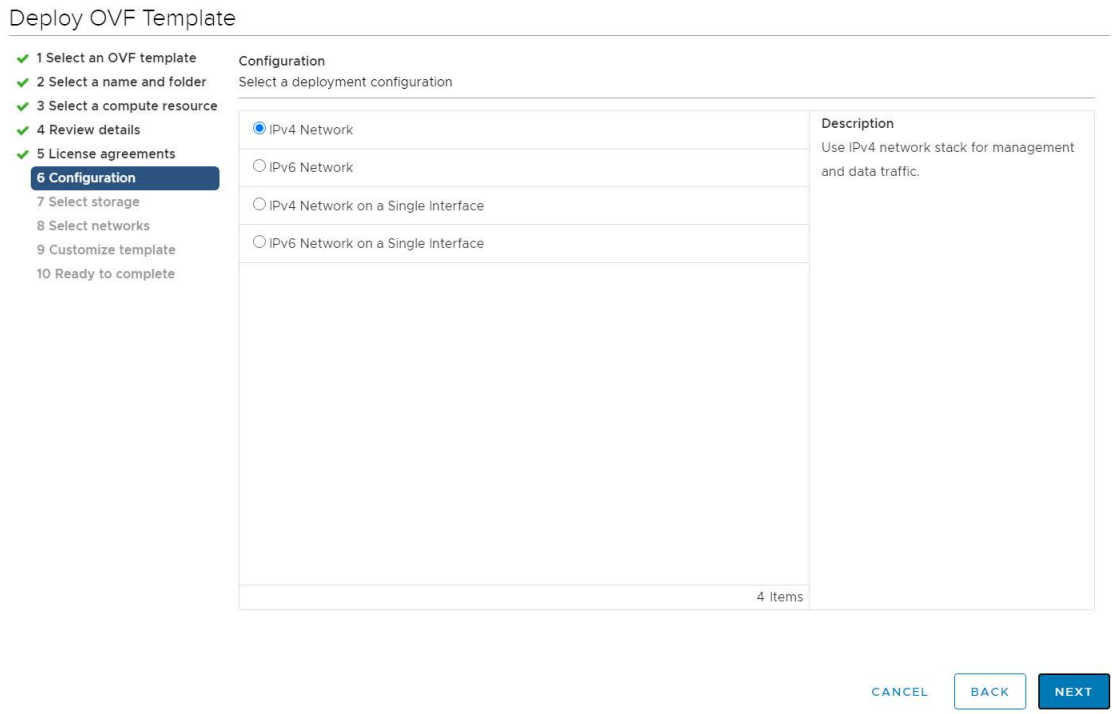
Step 7 Click **Next**. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. After the validation is complete, the **Deploy OVF Template** window is refreshed, with **4 - Review details** highlighted.

Step 8 Review the OVF template that you are deploying. Note that this information is gathered from the OVF, and cannot be modified.

Step 9 Click **Next**. The **Deploy OVF Template** window is refreshed, with **5 - License agreements** highlighted. Review the End User License Agreement and click the **I accept all license agreements** checkbox.

Step 10 Click **Next** The **Deploy OVF Template** window is refreshed, with **6 - Configuration** highlighted. Choose the desired deployment configuration.

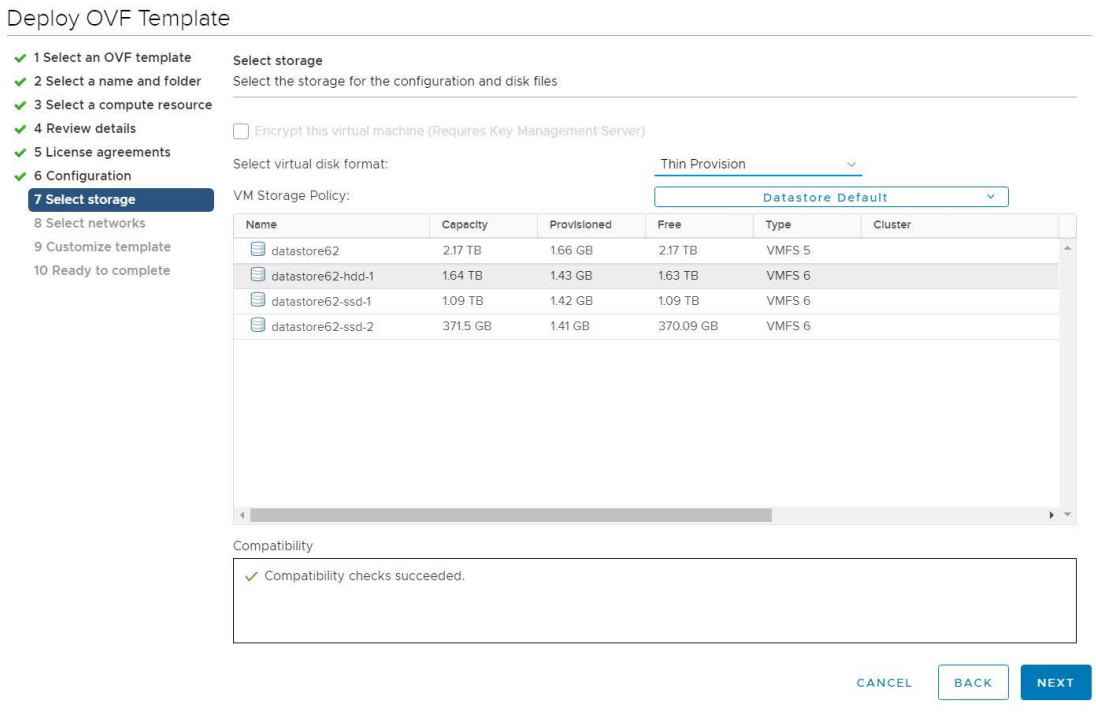
Figure 4: Select a deployment configuration



Note If Cisco Crosswork is deployed using a single interface, then Cisco Crosswork Data Gateway must be deployed using a single interface as well (only required for lab deployments).

Step 11 Click **Next**. The **Deploy OVF Template** window is refreshed, with **7 - Select Storage** highlighted. Choose the relevant option from the **Select virtual disk format** drop-down list. From the table, choose the datastore you want to use, and review its properties to ensure there is enough available storage.

Figure 5: Select Storage



Note For production deployment, choose the **Thick provision eager zeroed** option because this will preallocate disk space and provide the best performance. For lab purposes, we recommend the **Thin provision** option because it saves disk space.

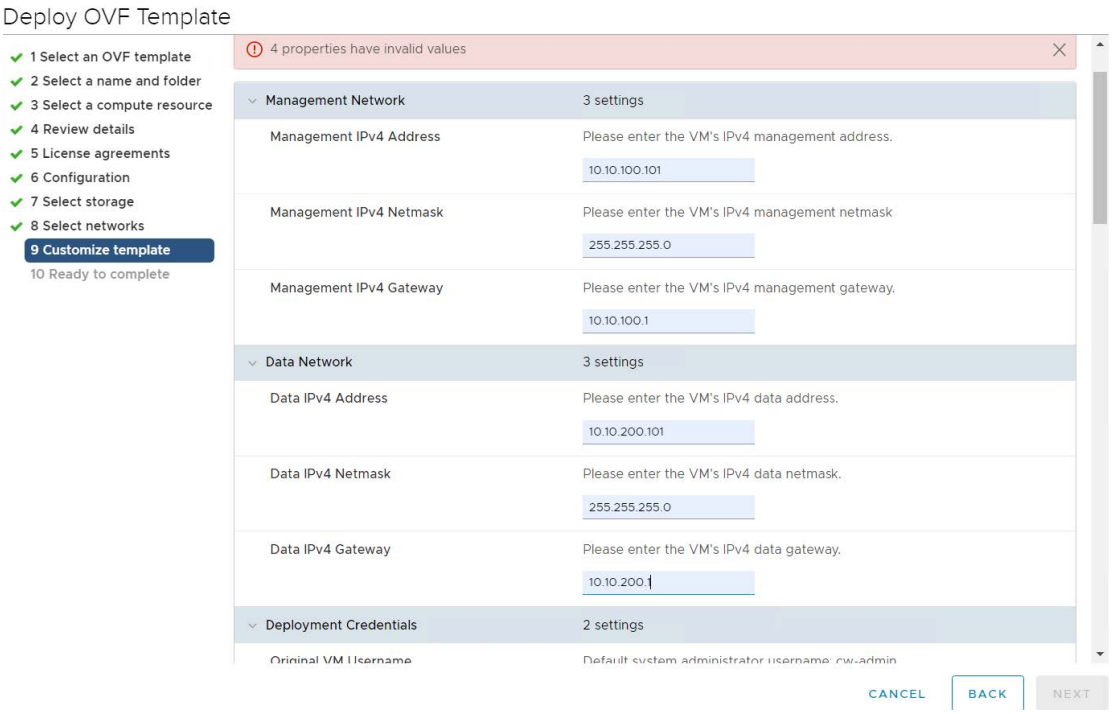
Step 12 Click **Next**. The **Deploy OVF Template** window is refreshed, with **8 - Select networks** highlighted. From the **Data Network** and **Management Network** drop-down lists, choose an appropriate destination network.

Step 13 Click **Next**. The **Deploy OVF Template** window is refreshed, with **9 - Customize template** highlighted.

a) Expand the **Management Network** settings. Provide information for the IPv4 or IPv6 deployment (as per your selection).

b) Expand the **Data Network** settings. Provide information for the IPv4 or IPv6 deployment (as per your selection).

Figure 6: Customize template settings

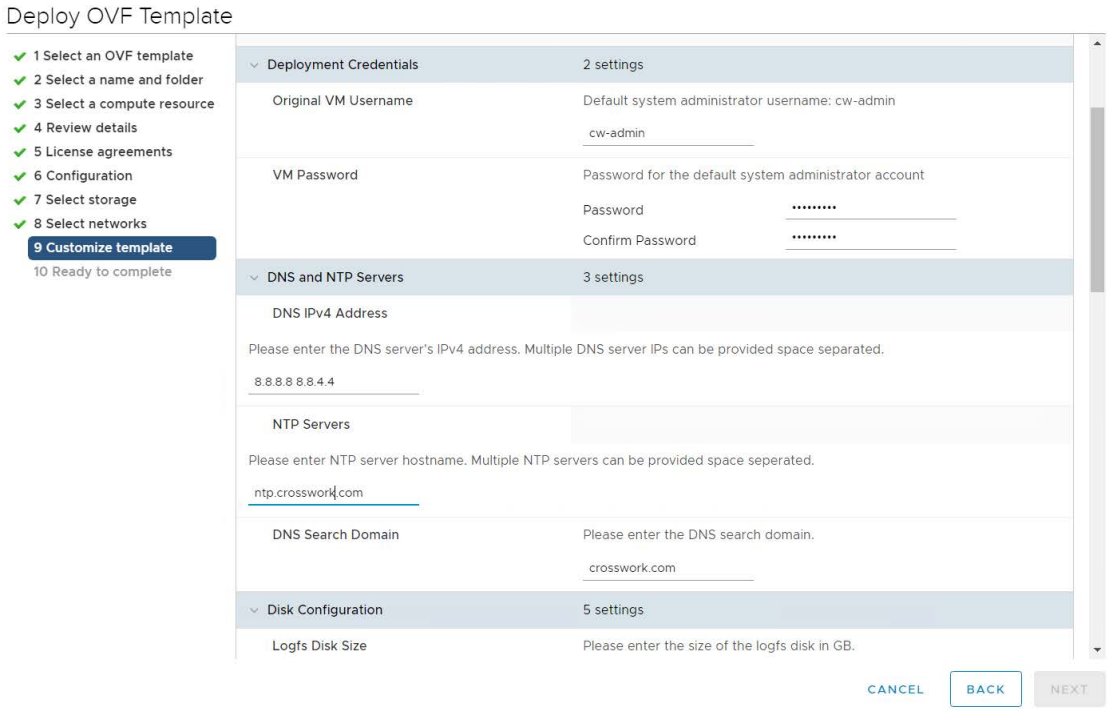


Note **Data Network** settings are not displayed if you have selected the **IPv4 on a Single Interface** or **IPv6 on a Single Interface** configuration.

c) Expand the **Deployment Credentials** settings. Enter relevant values for the VM Username and Password.

d) Expand the **DNS and NTP Servers** settings. According to your deployment configuration (IPv4 or IPv6), the fields that are displayed are different. Provide information in the following three fields:

- **DNS IP Address**: The IP addresses of the DNS servers you want the Cisco Crosswork server to use. Separate multiple IP addresses with spaces.
- **DNS Search Domain**: The name of the DNS search domain.
- **NTP Servers**: The IP addresses or host names of the NTP servers you want to use. Separate multiple IPs or host names with spaces.



Note The DNS and NTP servers must be reachable using the network interfaces you have mapped on the host. Otherwise, the configuration of the VM will fail.

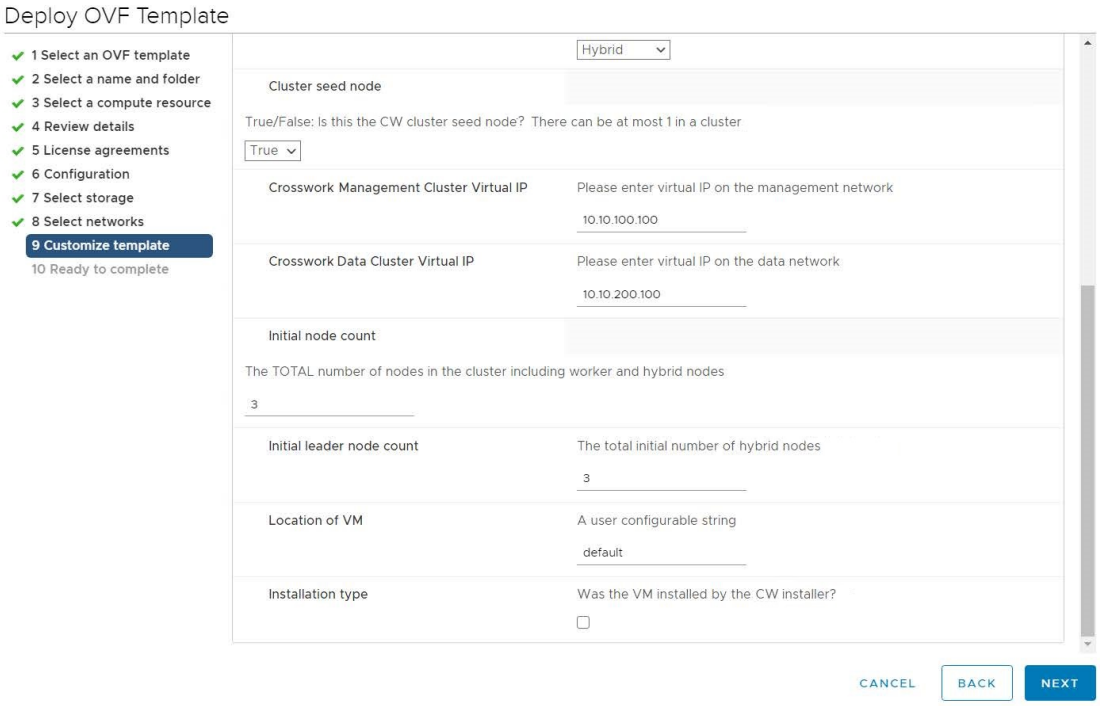
e) The default **Disk Configuration** settings should work for most environments. Change the settings only if you are instructed to by the Cisco Customer Experience team.

f) Expand **Crosswork Configuration** and enter your legal disclaimer text (users will see this text if they log into the CLI).

g) Expand **Crosswork Cluster Configuration**. Provide relevant values for the following fields:

- **VM Type**:
  - Choose **Hybrid** if this is one of the 3 hybrid nodes.
  - Choose **Worker** if this is a worker node.
- **Cluster Seed node**:
  - Choose **True** if this is the first VM being built in a new cluster.
  - Choose **False** for all other VMs, or when rebuilding a failed VM.
- **Crosswork Management Cluster Virtual IP**: Enter the Management Virtual IP address and Management Virtual IP DNS name.
- **Crosswork Data Cluster Virtual IP**: Enter the Data Virtual IP address. and the Data Virtual IP DNS name.
- **Initial node count**: Default value is 3.
- **Initial leader node count**: Default value is 3.

- **Location of VM**: Enter the location of VM.
- **Installation type**:
  - *For new cluster installation*: Do not select the checkbox.
  - *Replacing a failed VM*: Select the checkbox if this VM is being installed to replace a failed VM.



Step 14 Click **Next**. The **Deploy OVF Template** window is refreshed, with **10 - Ready to Complete** highlighted.

Step 15 Review your settings and then click **Finish** if you are ready to begin deployment. Wait for the deployment to finish before continuing. To check the deployment status:

a) Open a VMware vCenter client.

b) In the **Recent Tasks** tab of the host VM, view the status of the **Deploy OVF template** and **Import OVF package** jobs.

Step 16 To finalize the template creation, select the host and right-click on the newly installed VM and select **Template** > **Convert to Template**. A prompt confirming the action is displayed. Click **Yes** to confirm. The template is created under the **VMs and Templates** tab in the vSphere Client UI.

This is the end of the first part of the manual installation workflow. In the second part, use the newly created template to build the cluster VMs.

Step 17 To build the VM, right-click on the newly created template and select **New VM from This Template**.

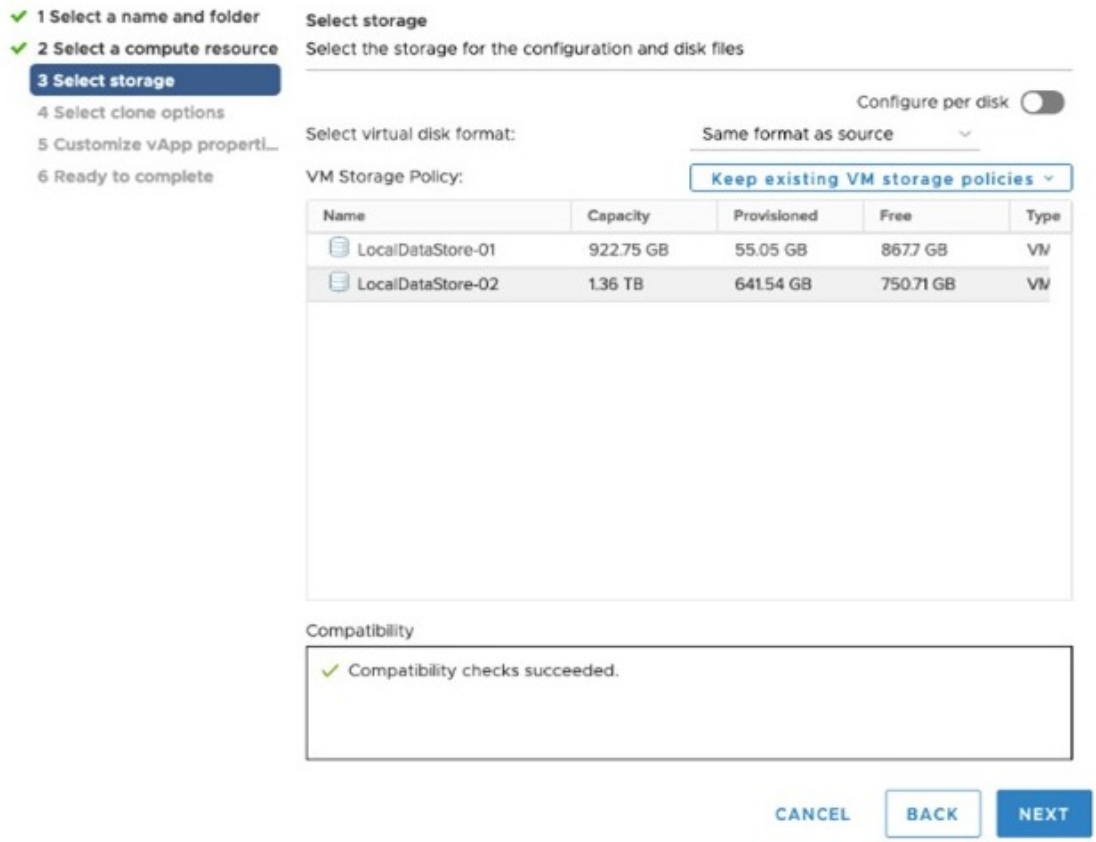
Step 18 The VMware **Deploy From Template** window appears, with the first step, **1 - Select a name and folder**, highlighted. Enter a name and select the respective Datacenter for the VM.

Step 19 Click **Next**. The **Deploy From Template** window is refreshed, with **2 - Select a compute resource** highlighted. Select the host for your Cisco Crosswork VM.

Step 20 Click **Next**. The **Deploy From Template** window is refreshed, with **3 - Select Storage** highlighted. Choose **Same format as source** option as the virtual disk format (recommended).

If you are using a single data store: Select the data store you wish to use, and click **Next**.

Figure 7: Select Storage - single data store

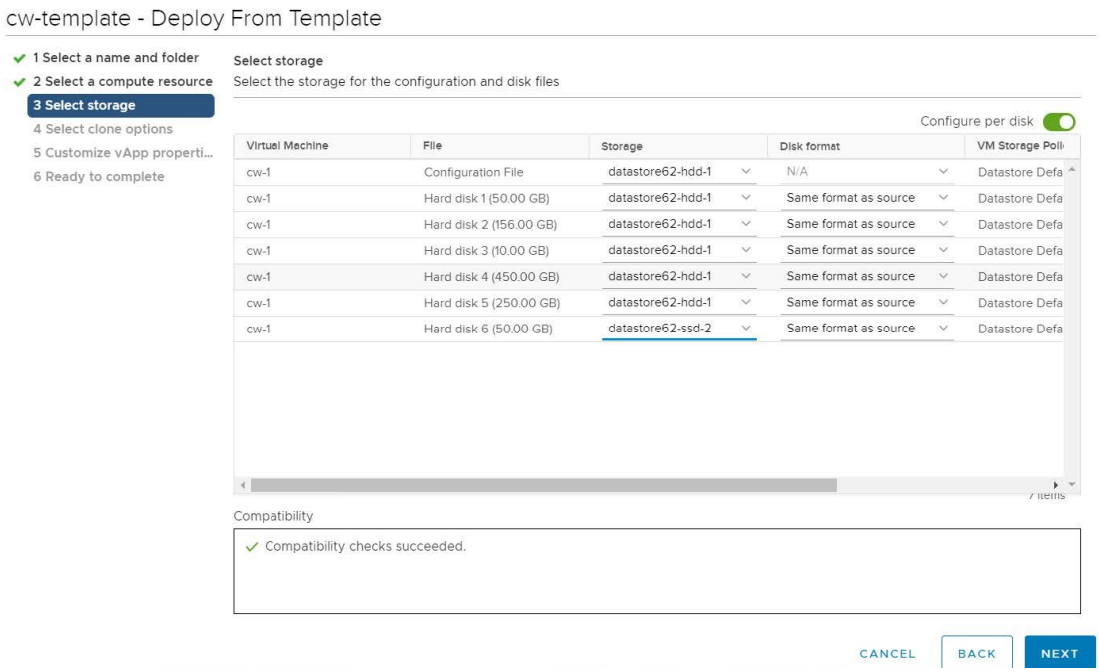


If you are using two data stores (regular and high speed):

- Enable **Configure per disk** option.
- Select regular data store as the **Storage** setting for all the disks except disk 6.
- Select high speed (ssd) data store as the **Storage** setting for disk 6.

  Note This disk must have 50 GB of free storage space.

Figure 8: Select Storage - Configure per disk



- Click **Next**.

Step 21 The **Deploy From Template** window is refreshed, with **4 - Select clone options** highlighted. You can choose further clone options here.

(Optional) Perform the following steps to configure the disk, memory and Extensive Firmware Interface (EFI) boot settings:

- Choose **Customize this virtual machine's hardware** and click **Next**. The **Edit Settings** dialog box is displayed.
- Under **Virtual Hardware** tab, enter the relevant values (see VM Host Requirements, on page 7) for **CPU** and **Memory**.
- Under **VM Options** tab, expand **Boot Options**, select **EFI** as the Firmware, and check the **Secure Boot** checkbox.

Step 22 Click **Next**. The **Deploy From Template** window is refreshed, with **5 - Customize vApp properties** highlighted. The vApp properties from the template is already populated in this window. You need to check the following fields:

- **Cluster Seed node**:
  - Choose **True** if this is the first VM being built in a new cluster.
  - Choose **False** for all other VMs, or when rebuilding a failed VM.
- **Management Network settings**: Enter correct IP values for each VM in the cluster.
- **Data Network settings**: Enter correct IP values for each VM in the cluster.
- **Crosswork Management Cluster Virtual IP**: The Virtual IP will remain same for each cluster node.
- **Crosswork Data Cluster Virtual IP**: The Virtual IP will remain same for each cluster node.

- **Deployment Credentials**: Enter same deployment credentials for each VM in the cluster.

Note If this VM is being deployed to replace a failed VM, the IP and other settings must match the machine being replaced.

Step 23 Click **Next**. The **Deploy From Template** window is refreshed, with **6 - Ready to complete** highlighted. Review your settings and then click **Finish** if you are ready to begin deployment.

Step 24 Repeat from **Step 17** to **Step 23** to deploy the remaining VMs in the cluster.

Step 25 You can now power on Cisco Crosswork VMs to complete the deployment process. The VM selected as the cluster seed node must be powered on first, followed by the remaining VMs (after a delay of few minutes). To power on, expand the host's entry, click the Cisco Crosswork VM, and then choose **Actions** > **Power** > **Power On**.

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the Installation, on page 52 to know how you can check the status of the installation.

Note If you are running this procedure to replace a failed VM, then you can check the status from the Cisco Crosswork GUI (go to **Administration** > **Crosswork Manager** and click on the cluster tile to check the *Crosswork Cluster* status.

Manual Installation of Cisco Crosswork on Cisco CSP

This section explains the procedure to manually install Crosswork cluster hybrid nodes and worker nodes on Cisco CSP.

Note While deploying worker nodes, set the `VMType` value in the `ovf-env.xml` file as **Worker**.

Step 1 Prepare the Cisco Crosswork service image for upload to Cisco CSP:

a) Download and extract the Cisco Crosswork `qcow2` build from cisco.com to your local machine or a location on your local network that is accessible to your Cisco CSP.

The build is a tarball of the `qcow2` file and the template file (.tpl).

Note The procedure requires `ovf-env.xml` file. You must create it using the template file found in the build.

b) Open the `ovf-env.xml` file and modify the parameters as per your installation requirements.

Below is an example of how the `ovf-env.xml` file looks like:

```
<?xml version="1.0" encoding="UTF-8"?>
<Environment>
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:ve="http://www.cisco.com/schema/ovfenv"
     oe:id=""
   <PlatformSection>
      <Kind>Cisco CSP</Kind>
      <Version>2.8</Version>
```

```
      <Vendor>Cisco</Vendor>
      <Locale>en</Locale>
   </PlatformSection>
   <PropertySection>
         <Property oe:key="CWIPv4Address" oe:value="0.0.0.0"/>
         <Property oe:key="CWIPv6Address" oe:value="::0"/>
         <Property oe:key="CWPassword" oe:value="{{.CWPassword}}"/>
         <Property oe:key="CWUsername" oe:value="{{.CWUsername}}"/>
         <Property oe:key="ClusterName" oe:value="{{.ClusterName}}"/>
         <Property oe:key="CwInstaller" oe:value="True"/>
         <Property oe:key="DNSv4" oe:value="{{.DNSv4}}"/>
         <Property oe:key="DNSv6" oe:value="{{.DNSv6}}"/>
         <Property oe:key="DataIPv4Address" oe:value="{{.DataIPv4Address}}"/>
         <Property oe:key="DataIPv4Gateway" oe:value="{{.DataIPv4Gateway}}"/>
         <Property oe:key="DataIPv4Netmask" oe:value="{{.DataIPv4Netmask}}"/>
         <Property oe:key="DataIPv6Address" oe:value="{{.DataIPv6Address}}"/>
         <Property oe:key="DataIPv6Gateway" oe:value="{{.DataIPv6Gateway}}"/>
         <Property oe:key="DataIPv6Netmask" oe:value="{{.DataIPv6Netmask}}"/>
         <Property oe:key="DataVIP" oe:value="{{.DataVIP}}"/>
         <Property oe:key="Deployment" oe:value="{{.Deployment}}"/>
         <Property oe:key="Disclaimer" oe:value="{{.Disclaimer}}"/>
         <Property oe:key="Domain" oe:value="{{.Domain}}"/>
         <Property oe:key="InitMasterCount" oe:value="{{.InitMasterCount}}"/>
         <Property oe:key="InitNodeCount" oe:value="{{.InitNodeCount}}"/>
         <Property oe:key="IsSeed" oe:value="{{.IsSeed}}"/>
         <Property oe:key="K8Orch" oe:value=""/>
         <Property oe:key="ManagementIPv4Address" oe:value="{{.ManagementIPv4Address}}"/>
         <Property oe:key="ManagementIPv4Gateway" oe:value="{{.ManagementIPv4Gateway}}"/>
         <Property oe:key="ManagementIPv4Netmask" oe:value="{{.ManagementIPv4Netmask}}"/>
         <Property oe:key="ManagementIPv6Address" oe:value="{{.ManagementIPv6Address}}"/>
         <Property oe:key="ManagementIPv6Gateway" oe:value="{{.ManagementIPv6Gateway}}"/>
         <Property oe:key="ManagementIPv6Netmask" oe:value="{{.ManagementIPv6Netmask}}"/>
         <Property oe:key="ManagementVIP" oe:value="{{.ManagementVIP}}"/>
         <Property oe:key="NSOProvider" oe:value="False"/>
         <Property oe:key="NTP" oe:value="{{.NTP}}"/>
         <Property oe:key="VMType" oe:value="{{.VMType}}"/>
         <Property oe:key="corefs" oe:value="20"/>
         <Property oe:key="ddatafs" oe:value="200"/>
         <Property oe:key="logfs" oe:value="10"/>
         <Property oe:key="ramdisk" oe:value="{{.RamDiskSize}}"/>
   </PropertySection>
</Environment>
```

Note Only one node in the cluster must have `IsSeed` set to True.

Step 2 Upload Cisco Crosswork service image to Cisco CSP:

a) Log into the Cisco CSP.

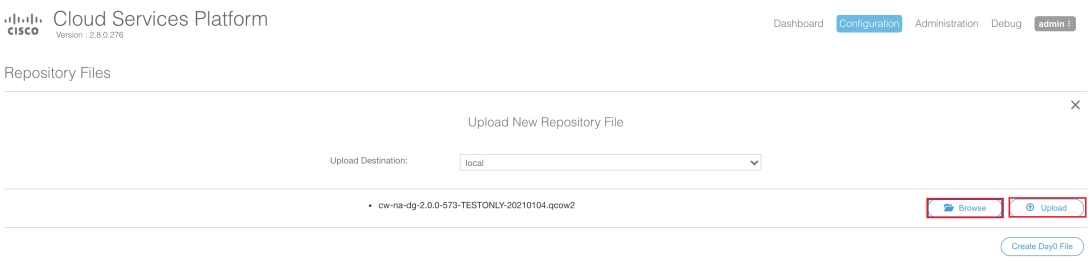
b) Go to **Configuration** > **Repository**.

c) On the **Repository Files** page, Click [+] button.

d) Select an **Upload Destination**.

e) Click **Browse**, navigate to the `qcow2` file, click **Open** and then **Upload**.

Repeat this step to upload `ovf-env.xml` file.



After the file is uploaded, the file name and other relevant information are displayed in the **Repository Files** table.

Step 3 Create Cisco Crosswork VM:

a) Go to **Configuration** > **Services**.

b) On the **Service** page, click [+] button.

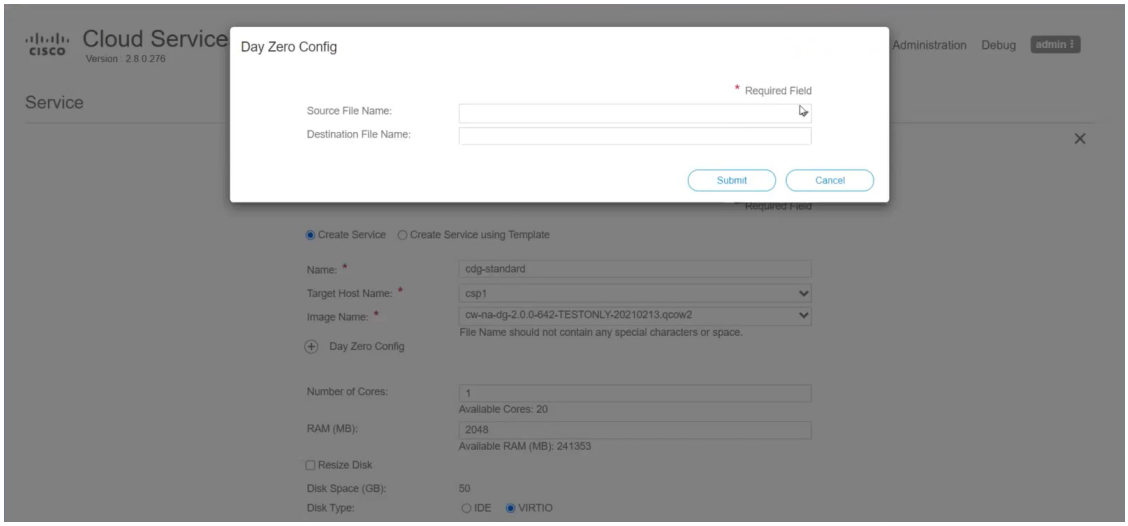
c) Check **Create Service** option.

The **Create Service Template** page is displayed.

d) Enter the values for the following fields:

Field	Description
Name	Name of the VM.
Target Host Name	Choose the target host on which you want to deploy the VM.
Image Name	Select the `qcow2` image.

e) Click **Day Zero Config**.



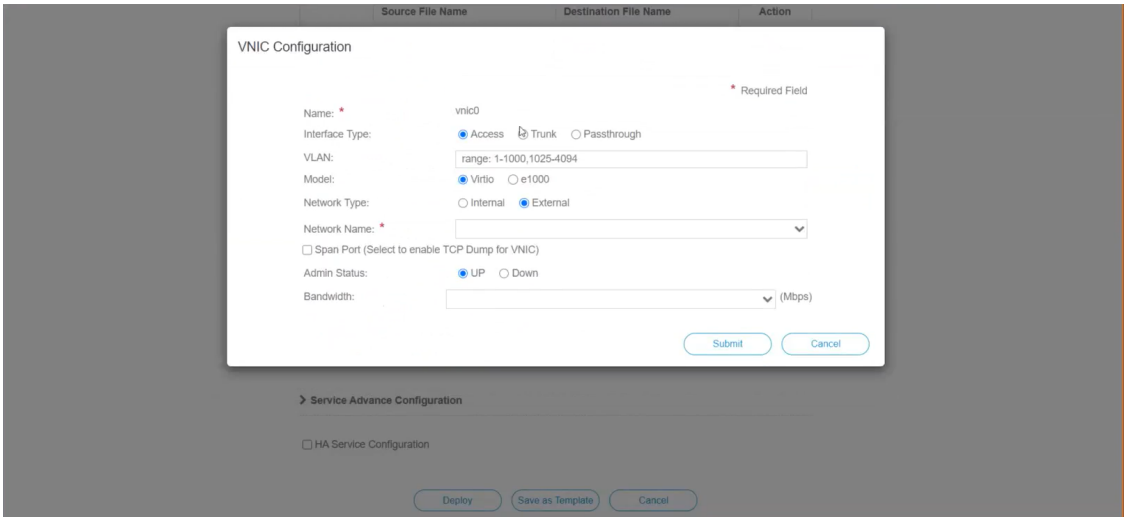
In the **Day Zero Config** dialog box, do the following:

1. From the **Source File Name** drop-down list, select a day0 configuration file i.e., the `ovf-env.xml` file that you modifed and uploaded earlier.
2. In the **Destination File Name** field, specify the name of the day0 destination text file. This must always be "ovf-env.xml".
3. Click **Submit**.

f) Enter the values for the following fields:

Field	Description
Number of CPU Cores	Small: 8 Large: 12
RAM (MB)	Small: 49152 Large: 98304

g) Click **VNIC**.



In the **VNIC Configuration** dialog box, perform the following:

Note The VNIC Name is set by default.

1. Select the **Interface Type** as **Access**.
2. Select the **Model** as **Virtio**.
3. Select the **Network Type** as **External**.
4. Select **Network Name**:

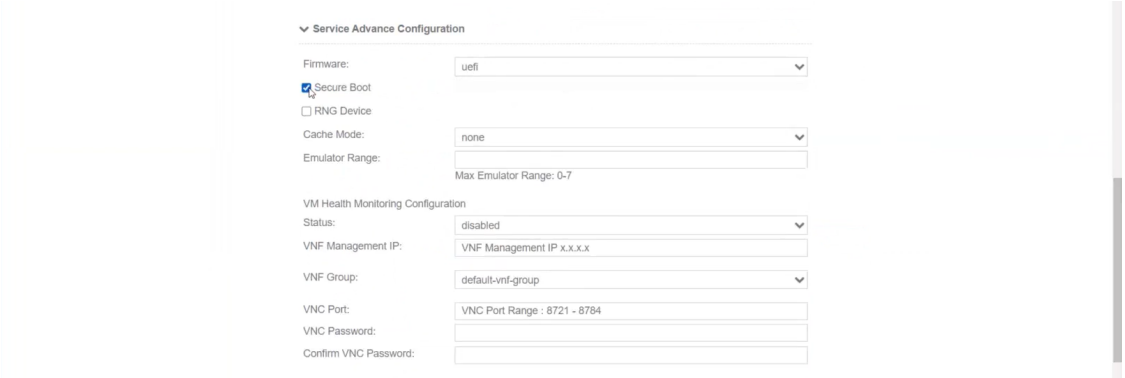
For VNIC...	Select...
vnic0	Eth0-1

For VNIC...	Select...
vnic1	Eth1-1

5. Select **Admin Status** as **UP**.
6. Click **Submit**.
7. Repeat Steps **i** to **vi** for vNIC1 and vNIC2.

After you have added all three vNICs, the VNIC table will look like this:

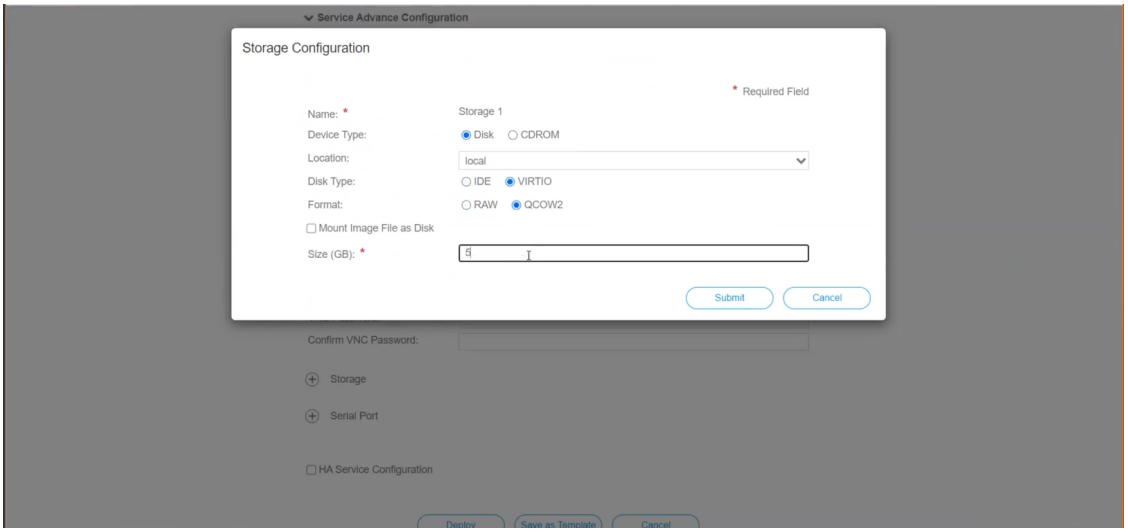
h) Expand the **Service Advance Configuration** and for **Firmware**, select **uefi** from the drop-down. Check the **Secure Boot** checkbox.



i) Click **Storage**. In the **Storage Configuration** dialog box, fill the following fields:

Field	Description
Name	Name of the storage. This is specified by default.
Device Type	Select **Disk**.
Location	Select **local**.
Disk Type	Select **VIRTIO**.
Format	Select **QCOW2**.

Field	Description
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size (**5** for Standard and **500** for Extended.)

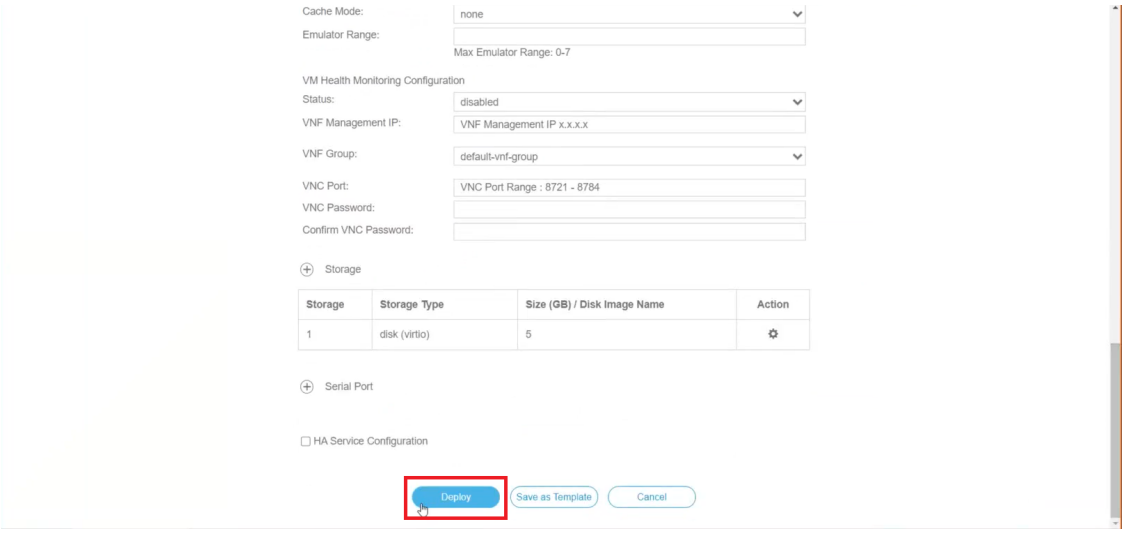


Note You have to configure 3 disks of different sizes:

- Disk 0: 10 GB
- Disk 1: 400 GB
- Disk 2: 50 GB

When you have completed the storage configuration, click **Submit**.

j) Click **Deploy**.



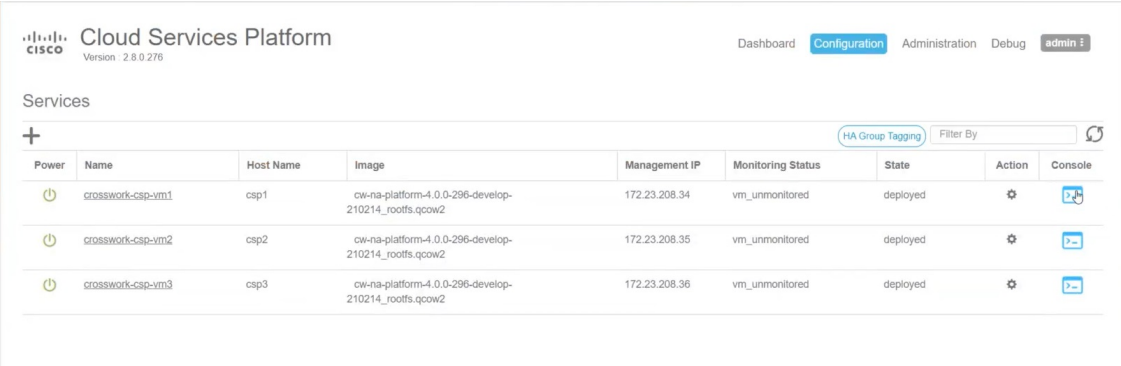
You will see a similar message once the service has successfully deployed. Click **Close**.

Step 4 Repeat **Step 1** to **Step 3** for each VM in the cluster.

Step 5 Deploy Cisco Crosswork VM:

a) Go to **Configuration** > **Services**.

b) In the **Services** table, click the console icon under **Console** column for the Cisco Crosswork VM you created above.



What to do next

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the Installation, on page 52 to know how you can check the status of the installation.

Monitor the Installation

This section explains how to monitor and verify if the installation has completed successfully. As the installer builds and configures the cluster it will report progress. The installer will prompt you to accept the license agreement and then ask if you want to continue the install. After you confirm, the installation will progress and any errors will be logged in either `installer.log` or `installer_tf.log`.

Note During installation, Cisco Crosswork will create a special administrative ID (**virtual machine (VM) administrator**, with the username *cw-admin*, and the default password *cw-admin*). The administrative username is reserved and cannot be changed. The first time you log in using this administrative ID, you will be prompted to change the password. Data center administrators use this ID to log into and troubleshoot the Crosswork application VM. You will use it to verify that the VM has been properly set up.

The following is a list of critical steps in the process that you can watch for to be certain that things are progressing as expected:

1. The installer uploads the crosswork image file (OVA file in vCenter & QCOW2 file in CSP) to the data center.
2. The installer creates the VMs, and displays a success message (e.g. "Creation Complete") after each VM is created.

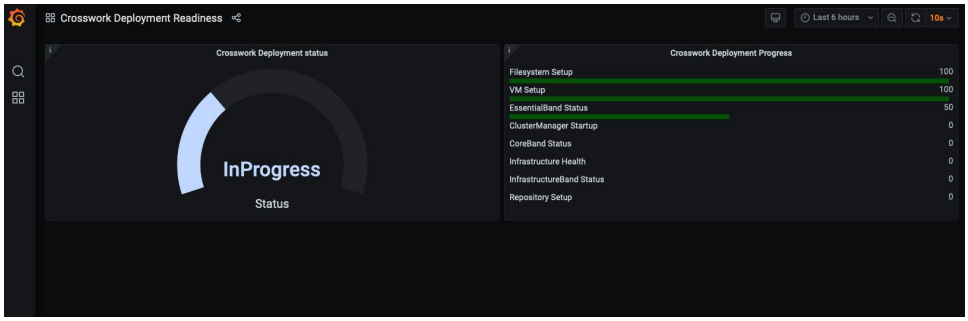
Note For VMware deployments, this activity can also be monitored from the vSphere UI.

3. After the VMs are created successfully, the Crosswork cluster will be created.
4. Once the cluster is created and becomes accessible, a success message (e.g. "CW Installer operation complete") will be displayed on the screen.

Once the VMs are built and powered on (either automatically when the installer completes, or after you power on the VMs during the manual installation) the Kubernetes cluster is built and the containers that make up Crosswork are started. You can monitor startup progress using the following methods:

- **Using browser accessible dashboard:** While the cluster is being created, you can monitor the setup process from a browser accessible dashboard. The URL for this grafana dashboard (in the format `http://{VIP}:30603/grafana.monitoring`) is displayed once the installer completes. Please note that this URL is temporary and will be available only for a limited time (around 30 minutes). At the end of the deployment, the grafana dashboard will report a "Ready" status. If the URL is inaccessible, you can use the other methods described in this section to monitor the installation process.

  Figure 9: Crosswork Deployment Readiness



- **Using the console:** You can also check the progress from the console of one of the hybrid VMs by using SSH to the Virtual IP address, switching to super user, and running `kubectl get nodes` (to see if the nodes are ready) and `kubectl get pods` (to see the list of active running pods) commands. Repeat the `kubectl get pods` command until you see `robot-ui` in the list of active pods. At this point, you can try to access the Cisco Crosswork UI.

After the Cisco Crosswork UI becomes accessible, you can also monitor the status from the UI. For more information, see Log into the Cisco Crosswork UI, on page 54.

Failure Scenario

In the event of a failue scenario (listed below), contact the Cisco Customer Experience team and provide the `installer.log` and `installer_tf.log` files (there will be one per VM) for review:

- Installation is incomplete
- Installation is completed, but the VMs are not functional
- Installation is completed, but you are directed to check `firstboot.log` file

Log into the Cisco Crosswork UI

Once the cluster activation and startup have been completed, you can check if all the nodes are up and running in the cluster from the Cisco Crosswork UI. Perform the following steps to log into the Cisco Crosswork UI and and check the cluster health:

Note If the Cisco Crosswork UI is not accessible, during installation, please access the host's console from the VMware or CSP UI to confirm if there was any problem in setting up the VM. When logging in, if you are directed to review the `firstboot.log` file, please check the file to determine the problem. If you are able to identify the error, rectify it and rerun the installer. If you require assistance, please contact the Cisco Customer Experience team.

Note You can log into the Crosswork UI using DNS name as well.

Step 1 Launch one of the supported browsers (see Supported Web Browsers, on page 12).

Step 2 In the browser's address bar, enter:

```
https://<Crosswork Management Network Virtual IP (IPv4)>:30603/
```

or

```
https://[<Crosswork Management Network Virtual IP (IPv6)>]:30603/
```

Note Please note that the IPv6 address in the URL must be enclosed with brackets.

Note You can also log into the Crosswork UI using DNS name.

The **Log In** window opens.

Note When you access the Cisco Crosswork for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco Crosswork server. After you add a security exception, the browser accepts the server as a trusted site in all future login attempts. If you want to use a CA signed certificate, see the "Manage Certificates" section in the *Cisco Crosswork Infrastructure 4.1 and Applications Administrator Guide*.

Step 3 Log into the Cisco Crosswork as follows:

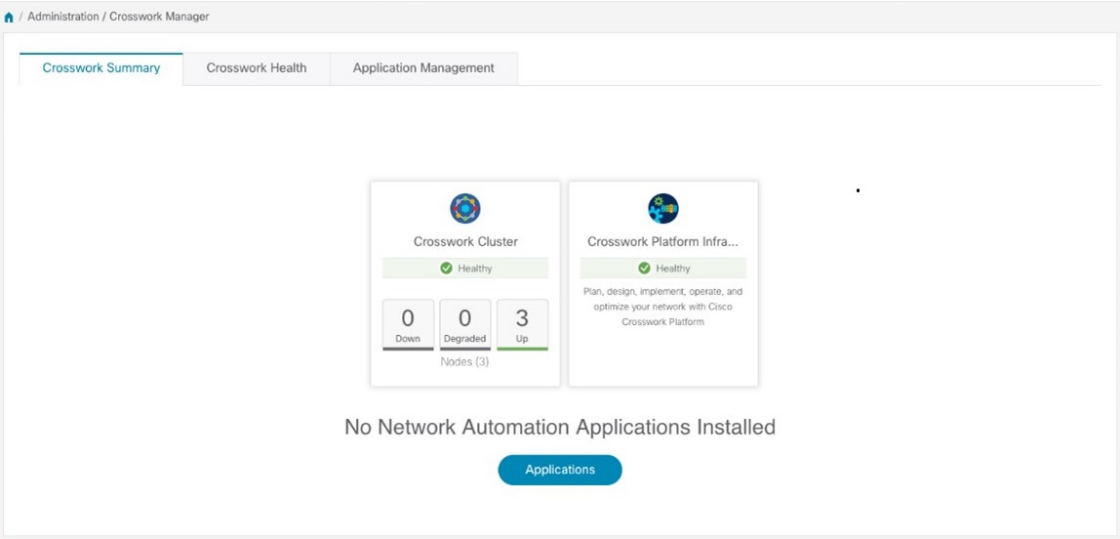
a) Enter the Cisco Crosswork administrator username **admin** and the default password **admin**.

b) Click **Log In**.

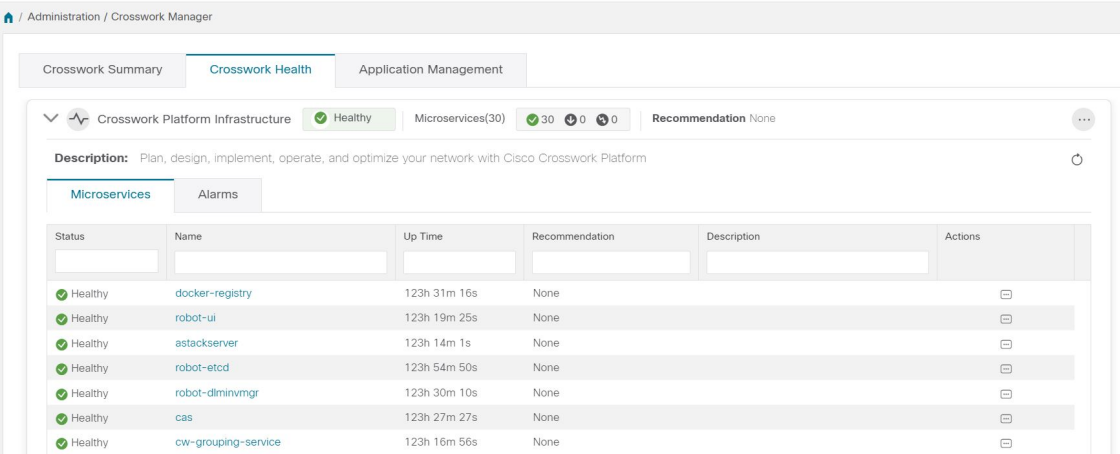
c) When prompted to change the administrator's default password, enter the new password in the fields provided and then click **OK**.

Note Use a strong password (8 character long, including upper & lower case letters, numbers and one special character).

The **Crosswork Manager** window is displayed.



Step 4 (Optional) Click on the **Crosswork Health** tab, and click on the **Crosswork Infrastructure** tile to view the health status of the microservices running on Cisco Crosswork.



Known Limitations

These following scenarios are the caveats for installing the Cisco Crosswork using the cluster installer tool.

- The vCenter host VMs defined must use the same network names (vSwitch) across all hosts in the DC.
- The vCenter storage folders, i.e. datastores organized under a virtual folder structure, are not supported currently. Please ensure that the datastores referenced are not grouped under a folder.
- When deploying a IPv6 cluster, the installer needs to run on an IPv6 enabled container/VM. This requires additionally configuring the docker daemon before running the installer, using the following method:
  - **Linux hosts (ONLY)**: Run the docker container in host networking mode by adding the "–network host" flag to the docker run command line.

```
docker run --network host <remainder of docker run options>
```

- The cluster installer does not configure VMs with VLAN interfaces. As a result, CSP interfaces have to be untrunked with no tagged VLANs used for Management and Data networks. CSP allows non-VLAN tagged interfaces to be shared between multiple VMs, which allows for a more optimal interface assignment when deploying Crosswork and Crosswork Data Gateway VMs on the same CSP.
- Any VMs that are not created by the day 0 installer (for example, manually brought up VMs), cannot be changed either by the day 0 installer or via the Crosswork UI later. Similarly, VMs created via the Crosswork UI cannot be modified using the day 0 installer.
- Crosswork does not support dual stack configurations, and all addresses for the environment must be either IPv4 or IPv6. However, vCenter UI provides a service where a user accessing via IPv4 can upload images to the IPv6 ESXi host. Cluster installer cannot use this service. Follow either of the following workarounds for IPv6 ESXi hosts:
  1. Upload the OVA template image manually, via the GUI and convert it to template.
  2. Run the cluster installer from an IPv6 enabled machine. To do this, configure the docker daemon to map an IPv6 address into the docked container.
- Centos/RHEL hosts, by default, enforce a strict SELinux policy which does not allow the installer container to read from or write to the mounted data volume. On such hosts, run the docker volume command with the Z option as shown below:

  ```
  docker run --rm -it -v `pwd`:/data:Z <remainder of docker options>
  ```

Troubleshoot the Cluster

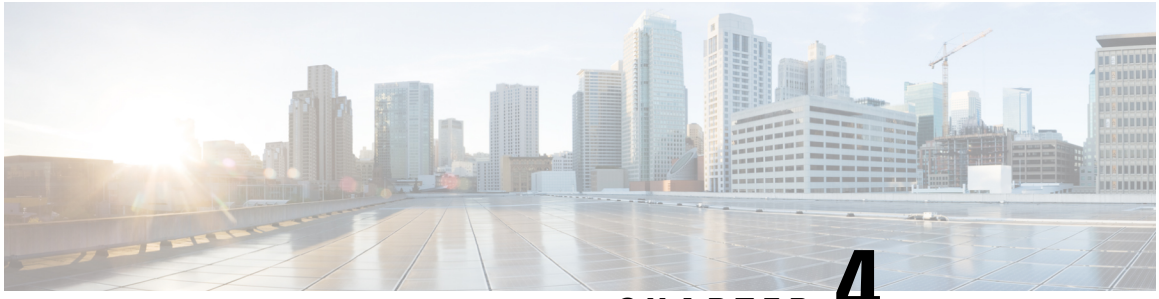
By default, the installer displays progress data on the command line. The install log is fundamental in identifying the problems, and it is copied into the `/data` directory.

Scenario	Possible Resolution
Missing or invalid parameters	The installer provides a clue as regards to the issue; however, in case of errors in the manfiest file HCL syntax, these can be misguiding. If you see "Type errors", check the formatting of the configuration manifest. The manifest file can also be passed as a simple JSON file. Use the following converter to validate/convert: https://www.hcl2json.com/
Image upload takes a long time or upload is interrupted.	The image upload duration depends on the link and datastore performance and can be expected to take around 10 minutes or more. It is best *not* to interrupt the process, which automatically ceases. However, if an upload is interrupted, the user needs to manually remove the partially uploaded image file from vCenter via the vSphere UI.
vCenter authorization	The vCenter user needs to have authorization to perform the actions as described in Cisco Crosswork Installation Requirements, on page 5.

Scenario	Possible Resolution
Floating VIP address is not reachable	The VRRP protocol requires unique router_id advertisments to be present on the network segment. By default, Crosswork uses the ID 169 on the management and ID 170 on the data network segments. A symptom of conflict, if it arises, is that the VIP address is not reachable. Remove the conflicting VRRP router machines or use a different network.
Crosswork VM is not allowing to log in	The password specified is not strong enough. Change the configuration manfiest and redeploy.
Error conditions such as: *Error: Error locking state: Error acquiring the state lock: resource temporarily unavailable* *Error: error fetching virtual machine: vm not found* *Error: Invalid index*	These errors are common when re-running the installer after an initial run is interrupted (Control C, or TCP timeout, etc). Remediation steps are: **1.** Run the clean operation (`./cw-installer.sh clean -m <your manifest here>`) OR remove the VM files manually from the vCenter. **2.** Remove the state file (`rm /data/crosswork-cluster.tfstate`) and retry.
Deployment fails with: *Failed to validate Crosswork cluster initialization.*	The clusters' seed VM is either unreachable or one or more of the cluster VMs have failed to get properly configured. **1.** Check whether the VM is reachable, and collect logs from `/var/log/firstBoot.log` and `/var/log/vm_setup.log` **2.** Check the status of the other cluster nodes.

The VMs are deployed but the Crosswork cluster is not being formed.	A successful deployment allows the operator logging in to the VIP or any cluster IP address to run the following command to get the status of the cluster:
	`sudo kubectl get nodes`
	A healthy output for a 3-node cluster is:
	`NAME STATUS ROLES AGE VERSION`
	`172-25-87-2-hybrid.cisco.com Ready master 41d v1.16.4`
	`172-25-87-3-hybrid.cisco.com Ready master 41d v1.16.4`
	`172-25-87-4-hybrid.cisco.com Ready master 41d v1.16.4`
	In case of a different output, collect the following logs: `/var/log/firstBoot.log` and `/var/log/vm_setup.log`
	In addition, for any cluster nodes not displaying the Ready state, collect:
	`sudo kubectl describe node <name of node>`

Scenario	Possible Resolution
The following error is displayed while uploading the image: *govc: The provided network mapping between OVF networks and the system network is not supported by any host.*	The Dswitch on the vCenter is misconfigured. Please check whether it is operational and mapped to the ESXi hosts.
The VMs take a long time to deploy	The disk load on the vCenter plays a major role in cloning VM. To ease loaded systems, it is possible to run the VM install operations in a serialized manner. On higher performance systems, run the deployment in parallel by passing the [-p] flag.
VMs deploy but install fails with *Error: timeout waiting for an available IP address*	Most likely cause would be an issue in the VM parameters provided or network reachability. Enter the VM host through the vCenter console. and review and collect the following logs: `/var/log/firstBoot.log` and `/var/log/vm_setup.log`
On cluster node failure, the VIP is not transferred to the remaining nodes	Ensure that switch or the vCenter Dswitch connected the VMs allows IP address movement (Allow Forged Transmits in vCenter). For more information, see Data Center Requirements, on page 5.
When deploying on a vCenter, the following error is displayed towards the end of the VM bringup: Error processing disk changes post-clone: *disk.0: ServerFaultCode: NoPermission: RESOURCE (vm-14501:2000), ACTION (queryAssociatedProfile): RESOURCE (vm-14501), ACTION (PolicyIDByVirtualDisk)*	Enable Profile-driven storage. Query permissions for the vCenter user at the root level (i.e. for all resources) of the vCenter.
Installer reports plan to add more resources than the current numbr of VMs	Other than the Crosswork cluster VMs, the installer tracks a couple of other meta-resources. Thus, when doing an installation of, say a 3-VM cluster, the installer may report a "plan" to add more resources than the number of VMs.
On running or cleaning, installer reports *Error: cannot locate virtual machine with UUID "xxxxxxx": virtual machine with UUID "xxxxxxxx" not found*	To resolve, remove the `/data/crosswork-cluster.tfstate` file. The installer uses the `tfstate` file stored as `/data/crosswork-cluster.tfstate` to maintain the state of the VMs it has operated upon. If a VM is removed outside of the installer, that is through the vCenter UI, this state is out of synchronization.



CHAPTER 4

Install Cisco Crosswork Data Gateway

This chapter contains the following topics:

Install Cisco Crosswork Data Gateway

This procedure can be used for installing the first Cisco Crosswork Data Gateway or for adding additional Cisco Crosswork Data Gateway VMs.

Note If you are re-deploying Cisco Crosswork Data Gateway with Cisco Crosswork, delete the previous Cisco Crosswork entry for auto-enrollment to work.

Cisco Crosswork Data Gateway Deployment and Set Up Workflow

To deploy and set up Crosswork Data Gateway VM for use with Cisco Crosswork, follows these steps:

1. Choose the deployment type for Cisco Crosswork Data Gateway i.e., Standard or Extended. See Cisco Crosswork Data Gateway Requirements, on page 12.
2. Install Cisco Crosswork Data Gateway on your preferred platform:

VMware	Install Cisco Crosswork Data Gateway Using vCenter vSphere Client, on page 70
	Install Cisco Crosswork Data Gateway Via OVF Tool, on page 76
Cisco CSP	Install Cisco Crosswork Data Gateway on Cisco CSP, on page 78

3. Set timezone on Cisco Crosswork Data Gateway VM. See Configure Timezone of the Crosswork Data Gateway VM, on page 87.

4. Verify Cisco Crosswork Data Gateway enrollment with Cisco Crosswork. See Cisco Crosswork Data Gateway Authentication and Enrollment, on page 90.

After verifying that the Cisco Crosswork Data Gateway has successfully enrolled with Cisco Crosswork, create a Cisco Crosswork Data Gateway pool and add the Cisco Crosswork Data Gateway VMs to the pool.

Note If you are going to have multiple Cisco Crosswork Data Gateways due to load or scale and/or you wish to leverage Cisco Data Gateway High Availability, it is recommended that you install all the Cisco Crosswork Data Gateway VMs and then add them to a Data Gateway pool.

Cisco Crosswork Data Gateway Parameters and Deployment Scenarios

Before you begin installing the Crosswork Data Gateway, go through this section to read about the deployment parameters and possible deployment scenarios.

Crosswork Data Gateway supports either IPv4 or IPv6 for all interfaces. Cisco Crosswork does not support dual stack configurations. Therefore, plan ALL addresses for the environment as either IPv4 or IPv6.

During installation, Cisco Crosswork Data Gateway creates two default user accounts:

- Cisco Crosswork Data Gateway administrator, with the username, **dg-admin** and the password set during installation. The administrator uses this ID to log in and troubleshoot Cisco Crosswork Data Gateway.
- Cisco Crosswork Data Gateway operator, with the username, **dg-oper** and the password set during installation. The **dg-oper** user has permissions to perform all ‘read’ operations and limited ‘action’ commands.
- To know what operations an admin and operator can perform, see Section *Supported User Roles* in the *Cisco Crosswork Infrastructure 4.1 and Applications Administration Guide*.

The **dg-admin** and **dg-oper** user accounts are reserved usernames and cannot be changed. You can change the password from the console for both the accounts. See Section *Change Passphrase Cisco Crosswork Infrastructure 4.1 and Applications Administration Guide*. In case of lost or forgotten passwords, you have to create a new VM, destroy the current VM, and re-enroll the new VM with Cisco Crosswork.

In the following table:

* Denotes the mandatory parameters. Other parameters are optional. You can choose them based on deployment scenario you require. We have explained deployment scenarios wherever applicable in the **Additional Information** column.

** Denotes parameters that you can enter during install or address later using additional procedures.

Table 16: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Name	Parameter	Description	Additional Information
Host Information			

Name	Parameter	Description	Additional Information
Hostname*	`Hostname`	Name of the Cisco Crosswork Data Gateway VM specified as a fully qualified domain name (FQDN). **Note** In larger systems, you are likely to have more than one Cisco Crosswork Data Gateway VM. The hostname must, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	`Description`	A detailed description of the Cisco Crosswork Data Gateway.	
Label	`Label`	Label used by Cisco Crosswork to categorize and group multiple Cisco Crosswork Data Gateways.	
Deployment	Deployment	Parameter that conveys the controller type. For On-premise installation , choose either `onpremise-standard` or `onpremise-extended`. Default value is `onpremise-standard`.	This parameter is pre-defined for CSP installation. You will need to specify this value for OVF tool installation.

Name	Parameter	Description	Additional Information
Active vNICs*	`ActiveVnics`	Number of vNICs to use for sending traffic.	You can choose to use either 1, 2, or 3 vNICs as per the following combinations: **Note** If you use one vNIC on your Crosswork cluster, use only one interface on the Crosswork Data Gateway. If you use two vNICs on your Crosswork Cluster, then you can use two or three vNICs on the Crosswork Data Gateway. • **1** - sends all traffic through vNIC0. • **2** - sends management traffic through vNIC0 and all data traffic through vNIC1. • **3** - sends management traffic through vNIC0, Northbound data through vNIC1, and Southbound data on vNIC2.
AllowRFC8190 *	`AllowRFC8190`	Automatically allow addresses in an RFC 8190 range. Options are `yes`, `no` or `ask`, where the initial configuration scripts prompts for confirmation. The default value is `yes`.	

Name	Parameter	Description	Additional Information
Private Key URI	`DGCertKey`	SCP URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	Cisco Crosswork uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation. However, if you want to use third-party or your own certificate files, then enter these three parameters. Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (user:host:/path/to/file). **Note** The host with the URI files must be reachable on the network (from the vNIC0 interface via SCP) and files must be present at the time of install.
Certificate File URI	`DGCertChain`	SCP URI to PEM formatted signing certificate chain for this VM. You can retrieve this using SCP (user@host:path/to/file).	
Certificate File and Key Passphrase	`DGCertChainPwd`	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	
Data Disk Size	`DGAppdataDisk`	Size in GB of a second data disk. Default size is 5GB for Standard and 500GB for Extended.	
Passphrase			

Name	Parameter	Description	Additional Information
dg-admin Passphrase*	`dg-adminPassword`	The password you have chosen for the dg-admin user. Password must be 8-64 characters.	
dg-oper Passphrase*	`dg-operPassword`	The password you have chosen for the dg-oper user. Password must be 8-64 characters.	
Interfaces **Note** You must select either an IPv4 or IPv6 address. Selecting **None** in both **vNICx IPv4 Method** field and **vNICx IPv6 Method** field results in a non-functional deployment.			
vNICx IPv4 Address (VNIC0, VNIC1, and VNIC2 based on the number of interfaces you choose to use)			
vNICx IPv4 Method* For example, the parameter name for vNIC0 is vNIC0 IPv4 Method.	`VnicxIPv4Method` For example, the parameter name for vNIC0 is `Vnic0IPv4Method`.	Method by which the vNICx interface gets its IPv4 address.	The default value for **Method** is **None**. If you choose to use IPv4 address, select **Method** as **Static** and enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields.
vNICx IPv4 Address	`VnicxIPv4Address`	IPv4 address of the vNICx interface.	
vNICx IPv4 Netmask	`VnicxIPv4Netmask`	IPv4 netmask of the vNICx interface in dotted quad format.	
vNICx IPv4 Skip Gateway	`VnicxIPv4SkipGateway`	Options are `yes` or `no`. Selecting `yes` skips configuring a gateway.	
vNICx IPv4 Gateway	`VnicxIPv4Gateway`	IPv4 address of the vNICx gateway.	
vNICx IPv6 Address (VNIC0, VNIC1, and VNIC2 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information
vNICx IPv6 Method* For example, the parameter for vNIC0 is vNIC0 IPv6 Method.	`VnicxIPv6Method` For example, the parameter for vNIC0 is `Vnic0IPv6Method`.	Method by which the vNICx interface gets its IPv6 address.	The default value for **Method** is **None**. If you choose to use IPv6 address, select **Method** as **Static** and enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields.
vNICx IPv6 Address	`VnicxIPv6Address`	IPv6 address of the vNICx interface.	
vNICx IPv6 Netmask	`VnicxIPv6Netmask`	IPv6 prefix of the vNICx interface.	
vNICx IPv6 Skip Gateway	`VnicxIPv6SkipGateway`	Options are `yes` or `no`. Selecting `yes` skips configuring a gateway.	
vNICx IPv6 Gateway	`VnicxIPv6Gateway`	IPv6 address of the vNICx gateway.	
DNS Servers			
DNS Address*	`DNS`	Space-delimited list of IPv4/IPv6 addresses of the DNS server accessible from the management interface.	
DNS Search Domain*	`Domain`	DNS search domain	
DNS Security Extensions *	`DNSSEC`	Options are False, True, Allow-Downgrade. The default value is False. Select True to use DNS security extensions.	
DNS over TLS*	`DNSTLS`	Options are False, True, and Opportunistic. The default value is False. Select True to use DNS over TLS.	
Multicast DNS*	`mDNS`	Options are False, True and Resolve. The default value is False. Select True to use multicast DNS.	If you choose Resolve, only resolution support is enabled. Responding is disabled.
Link-Local Multicast Name Resolution*	`LLMNR`	Options are False, True, Opportunistic and Resolve. By default, this is set to False. Select True to use link-local multicast name resolution.	If you choose Resolve, only resolution support is enabled. Responding is disabled.

Name	Parameter	Description	Additional Information
NTPv4 Servers			
NTPv4 Servers*	`NTP`	NTPv4 server list. Enter space-delimited list of IPv4/IPv6 addresses or hostnames of the NTPv4 servers accessible from the management interface.	You must enter a value here, such as pool.ntp.org. NTP server is critical for time synchronization between Crosswork Data Gateway VM, Crosswork, and devices. Using a non-functional or dummy address may cause issues when Cisco Crosswork and Crosswork Data Gateway try to communicate with each other. If you are not using an NTP server, ensure that time gap between Crosswork Data Gateway and Crosswork is not more than 10 minutes. Else, Crosswork Data Gateway fails to connect.
Use NTPv4 Authentication	`NTPAuth`	Select Yes to use NTPv4 authentication.	
NTPv4 Keys	`NTPKey`	Key IDs to map to the server list. Enter space-delimited list of Key IDs.	
NTPv4 Key File URI	`NTPKeyFile`	SCP URI to the chrony key file.	
NTPv4 Key File Passphrase	`NTPKeyFilePwd`	Password of SCP URI to the chrony key file.	
Remote Syslog Server			

Name	Parameter	Description	Additional Information
Use Remote Syslog Server*	`UseRemoteSyslog`	Select Yes to send syslog messages to a remote host.	Configuring an external syslog server sends service events (CLI/MDT/SNMP/gNMI) to the external syslog server. Otherwise, they are logged only to the Cisco Crosswork Data Gateway VM. If you want to use an external syslog server, specify these seven settings. **Note** The host with the URI files must be reachable on the network (from vNIC0 interface via SCP) and files must be present at the time of install.
Syslog Server Address	`SyslogAddress`	IPv4 or IPv6 address of a syslog server accessible from the management interface. **Note** If you are using an IPv6 address, surround the address with square brackets ([1::1]).	
Syslog Server Port	`SyslogPort`	Port number of the syslog server.	
Syslog Server Protocol	`SyslogProtocol`	Use UDP or TCP when sending syslog. Default value is UDP.	
Use Syslog over TLS?	`SyslogTLS`	Select Yes to use TLS to encrypt syslog traffic.	
Syslog TLS Peer Name	`SyslogPeerName`	Syslog server hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	`SyslogCertChain`	PEM formatted root cert of syslog server retrieved using SCP.	
Syslog Certificate File Passphrase	`SyslogCertChainPwd`	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Server			

Name	Parameter	Description	Additional Information
Use Remote Auditd Server*	`UseRemoteAuditd`	Select Yes to send Auditd message to a remote host	If desired, you can configure an external remote auditd server to send Cisco Crosswork Data Gateway VM change audit notifications. Specify these three settings to use an external Auditd server.
Auditd Server Address	`AuditdAddress`	Hostname, IPv4, or IPv6 address of an optional Auditd server	
Auditd Server Port	`AuditdPort`	Port number of an optional Auditd server.	
Controller and Proxy Settings			
Crosswork Controller IP*	`ControllerIP`	The Virtual IP address or the hostname of Cisco Crosswork Cluster. **Note** If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).	This is required if you are providing a controller signing certificate file URI.
Crosswork Controller Port*	`ControllerPort`	Port of the Cisco Crosswork controller. The default port is 30607	
Controller Signing Certificate File URI*	`ControllerSignCertChain`	PEM formatted root cert of Cisco Crosswork to validate signing certs retrived using SCP. Cisco Crosswork generates the PEM file and is available at the following location: `cw-admin@<Crosswork_VM_Management_IP_Address>:/home/cw-admin/controller.pem`	Crosswork Data Gateway requires the Controller Signing Certificate File to become functional. If you specify these parameters during the installation, the certificate file is imported once Crosswork Data Gateway boots up for the first time. If you do not specify these parameters during installation, then import the certificate file manually by following the procedure Import Controller Signing Certificate File, on page 93.

Name	Parameter	Description	Additional Information
Controller SSL/TLS Certificate File URI	`ControllerTlsCertChain`	Cisco Crosswork Controller PEM formatted SSL/TLS certificate file retrieved using SCP.	
Controller Certificate File Passphrase*	`ControllerCertChainPwd`	Password of SCP user (cw-admin) to retrieve Cisco Crosswork certificate chain.	
Proxy Server URL	`ProxyURL`	URL of management network proxy server.	Crosswork Data Gateway must connect to the Internet via TLS, and a proxy server may be required if it is not present in your environment. If you want to use a proxy server, specify these parameters.
Proxy Server Bypass List	`ProxyBypass`	Space-delimited list of subnets and domains that should not be sent to the proxy server.	
Authenticated Proxy Username	`ProxyUsername`	Username for authenticated proxy servers.	
Authenticated Proxy Passphrase	`ProxyPassphrase`	Passphrase for authenticated proxy servers.	
HTTPS Proxy SSL/TLS Certificate File URI	`ProxyCertChain`	HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP.	
HTTPS Proxy SSL/TLS Certificate File Passphrase	`ProxyCertChainPwd`	Password of SCP user to retrieve proxy certificate chain.	
Collector Listening Ports			The default port values can be changed either during install or changed later from the Interactive Menu (**Change Current System Settings** > **c Configure Collector Server Port**) of the Crosswork Data Gateway VM.
SNMP trap port**	`PortSNMPTrap`	SNMP trap port. The default port is 1062.	
Syslog UDP port**	`PortSyslogUDP`	Syslog UDP port. The default port is 9514.	
Syslog TCP port**	`PortSyslogTCP`	Syslog TCP port. The default port is 9898.	
Syslog TLS port**	`PortSyslogTLS`	Syslog TLS port. The default port is 6514.	

Note If you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,

```
-P55 user@host:path/to/file
```

Where 55 is a custom port.

Install Cisco Crosswork Data Gateway Using vCenter vSphere Client

Follow the steps to install Cisco Crosswork Data Gateway using vCenter vSphere Client:

Note The example images shown are only of Cisco Crosswork Data Gateway On-Premise Standard deployment.

Step 1 Download the Cisco Crosswork Data Gateway 2.0 image file from cisco.com (*.ova).

Warning The default VMware vCenter deployment timeout is 15 minutes. If the time taken to fill the OVF template exceeds 15 minutes, vCenter times out and you will have to start over again. To prevent this, it is recommended that you plan for the installation by having the necessary parameters and requirements ready. Refer to the *Table* #unique_36 unique_36_Connect_42_table_m3h_vtb_p4b.

Step 2 Connect to vCenter vSphere Client. Then select **Actions** > **Deploy OVF Template**

Step 3 The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 Select template**.

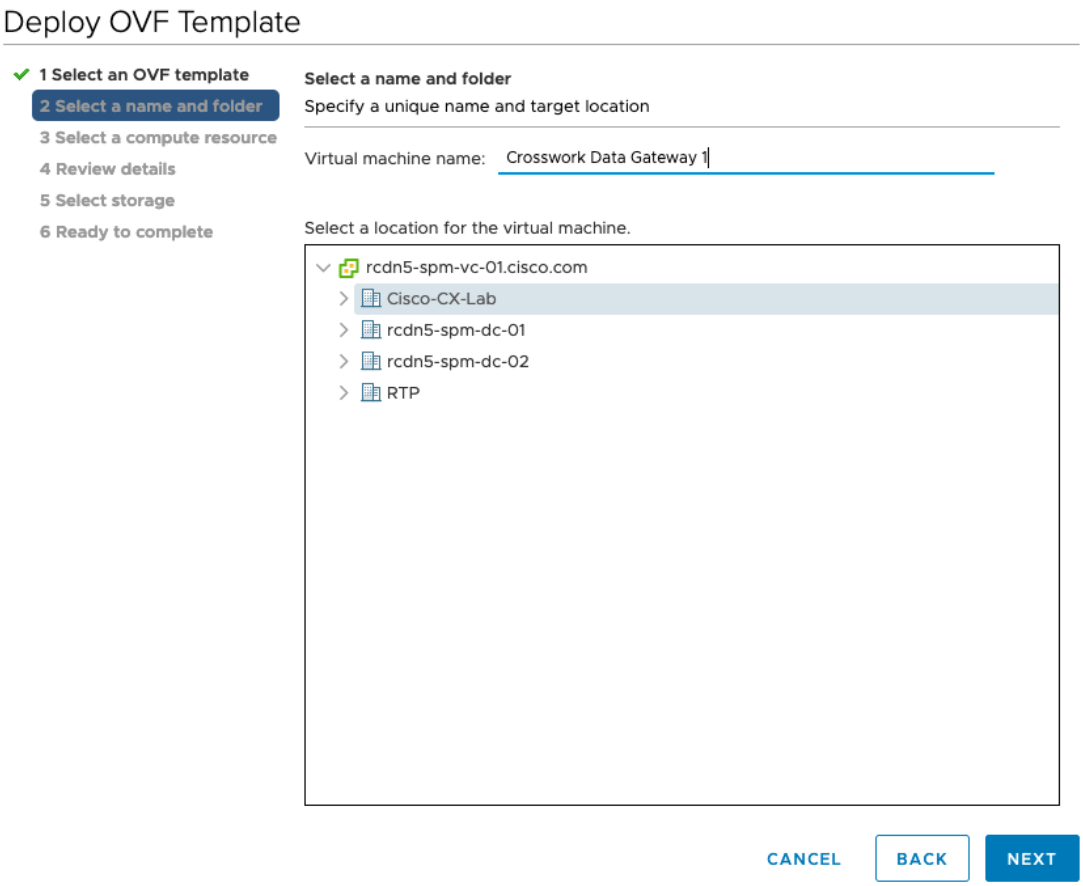
a) Click **Browse** to navigate to the location where you downloaded the OVA image file and select it.

Once selected, the filename is displayed in the window.

Step 4 Click **Next** to go to **2 Select name and location**, as shown in the following figure.

a) Enter a name for the VM you are creating.

b) In the **Select a location for the virtual machine** list, choose the datacenter under which the VM will reside.



Step 5 Click **Next** to go to **3 Select a resource**. Choose the VM's host.

Step 6 Click **Next**. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. When the validation is complete, the wizard moves to **4 Review details**. Review the OVA's information and then click **Next**.

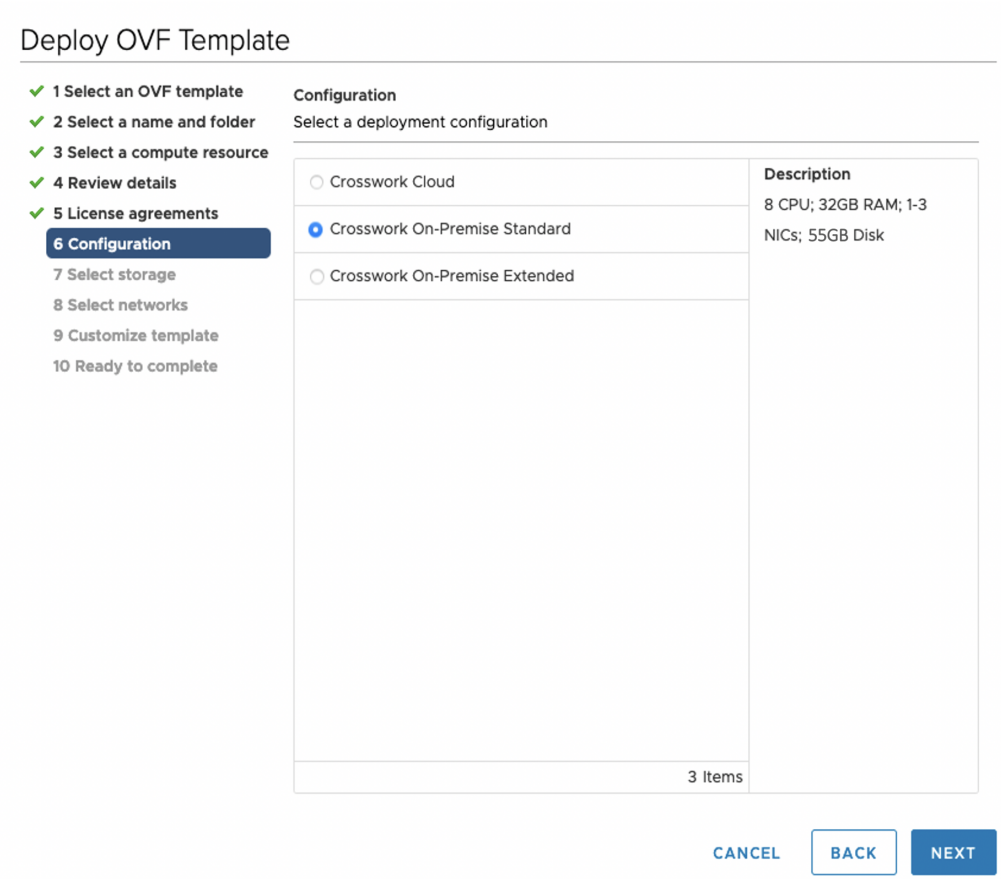
Take a moment to review the OVF template you are deploying.

Note This information is gathered from the OVF and cannot be modified.

Step 7 Click **Next** to go to **5 accept license agreements**. Review the End User License Agreement and click **Accept**.

Step 8 Click **Next** to go to **6 Select configuration**, as shown in the following figure. Select the type of configuration you want i.e., either **Crosswork On-Premise Standard** or **Crosswork On-Premise Extended**.

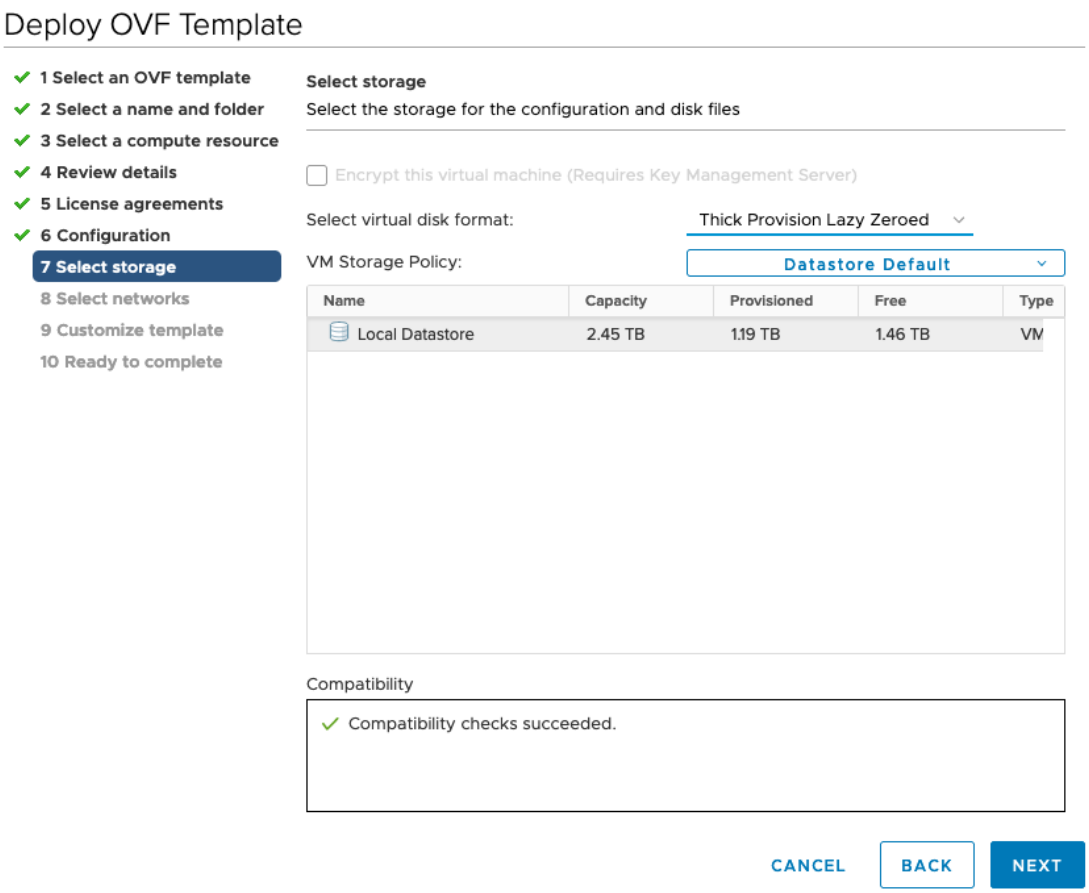
Note You must choose **Crosswork On-Premise Extended** if you plan to use Crossowork Data Gateway with Crosswork Health Insights.



Step 9 Click **Next** to go to **7 Select storage**, as shown in the following figure.

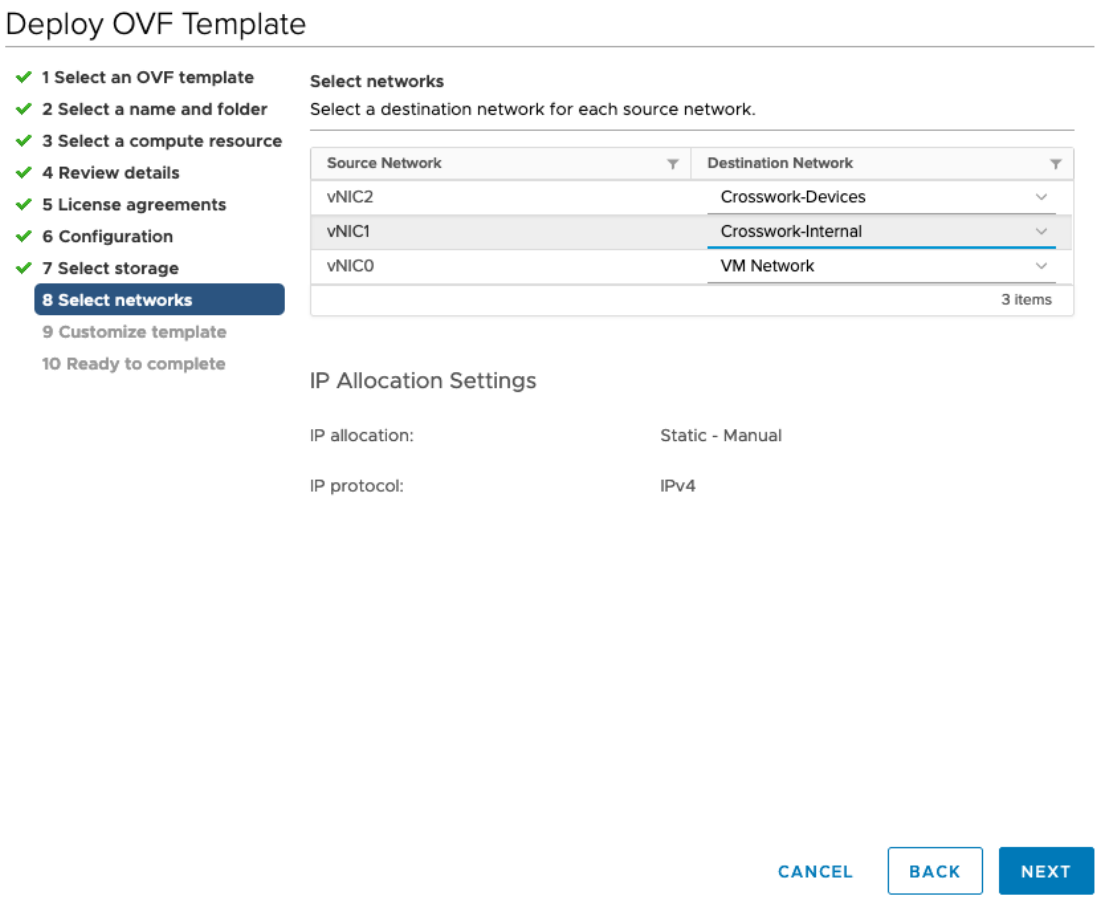
a) Cisco recommends that you select **Thick provision lazy zeroed** from the **Select virtual disk format** drop-down list.

b) From the **Datastores** table, choose the datastore you want to use and review its properties to ensure there is enough available storage.

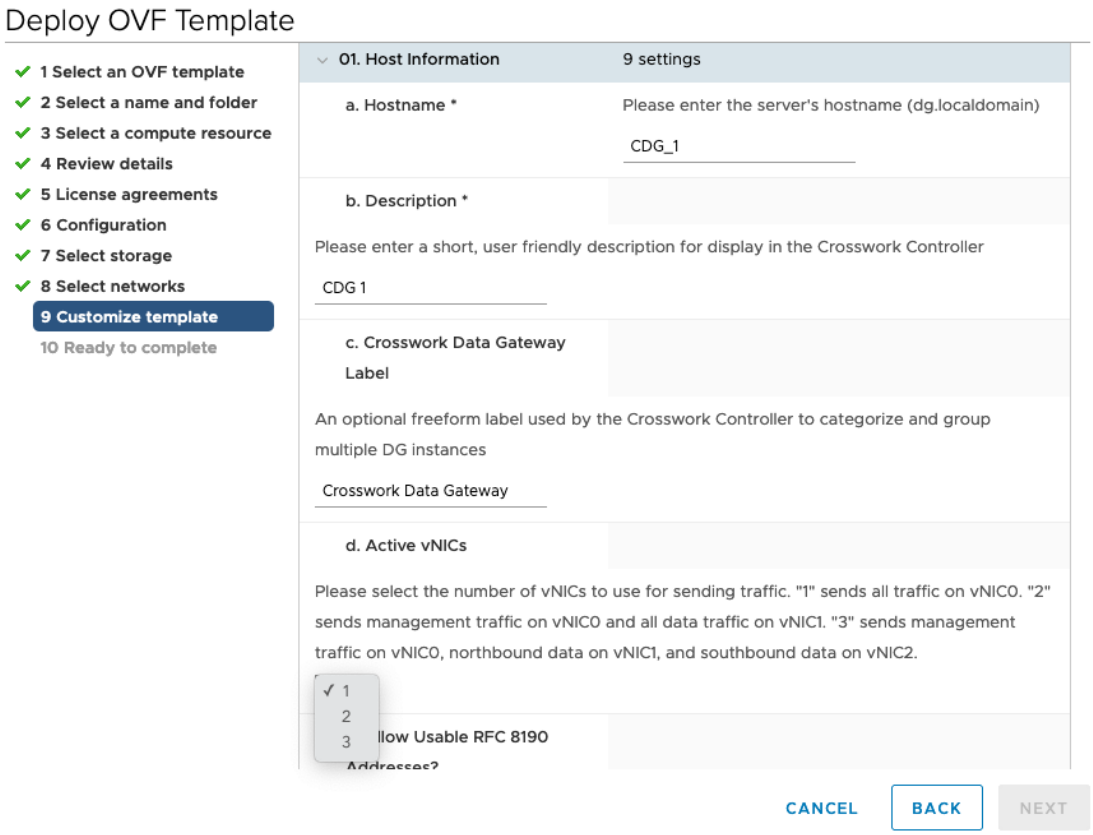


Step 10 Click **Next** to go to **8 Select networks**, as shown in the following figure. In the dropdown table at the top of the page, choose the appropriate destination network for each source network, **vNIC2**, **vNIC1**, and **vNIC0** respectively.

Note Starting with **vNIC0**, select a destination network for vNICs that will be used and leave unused vNICs set to the default value.



Step 11 Click **Next** to go to **9 Customize template**, with the **Host Information Settings** already expanded. Enter the information for the parameters as explained in *Table* #unique_36 unique_36_Connect_42_table_m3h_vtb_p4b.



Step 12 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish** if you are ready to begin deployment.

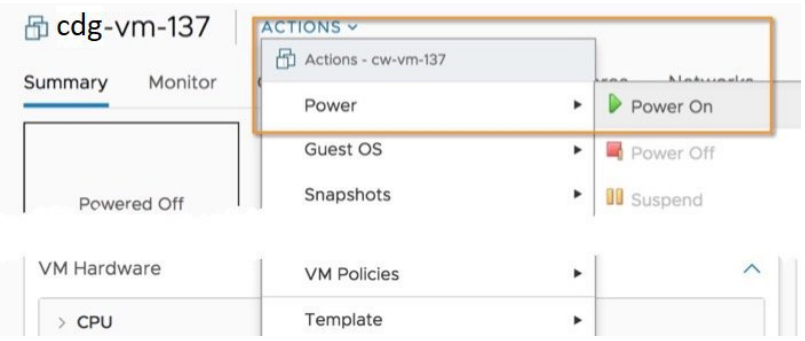
Step 13 Wait for the deployment to finish before continuing. To check the deployment status:

a) Open the vCenter vSphere client.

b) In the **Recent Tasks** tab for the host VM, view the status for the **Deploy OVF template** and **Import OVF package** jobs.

Wait for the deployment status to become 100%. You can now proceed to power on the VM.

Step 14 Once the deployment status is 100%, power on the VM to complete the deployment process. Expand the host's entry so you can click the VM and then choose **Actions** > **Power** > **Power On**, as shown in the following figure:



Wait for at least 5 minutes for the VM to come up and then login via vCenter or SSH as explained below.

Warning Changing the VM's network settings in vCenter may have significant unintended consequences, including but not limited to the loss of static routes and connectivity. The settings have been validated to provide the best network performance and any changes are done at your own risk.

What to do next

Login to Cisco Crosswork Data Gateway VM Via vCenter:

1. Locate the VM in vCenter and then right click and select **Open Console**.
2. Enter username (`dg-admin` or `dg-oper` as per the role assigned to you) and the corresponding password (the one that you created during installation process) and press **Enter**.

After you login, the Crossway Data Gateway should present you with the welcome screen and options menu indicating that the installation completed successfully. Log out and proceed with the post-installation tasks explained in the next section.

Install Cisco Crosswork Data Gateway Via OVF Tool

You can modify mandatory/optional parameters in the command/script as per your requirement and run the OVF Tool. Refer *Table* #unique_36 unique_36_Connect_42_table_m3h_vtb_p4b.

Below is a sample if you plan to run the OVF tool with a script:

```
#!/usr/bin/env bash

# robot.ova path
ROBOT_OVA_PATH="https://engci-maven.cisco.com/artifactory/cdg-group/build/2.0.0_dg200_7_2021-03-31_18-00-00/image/cw-na-dg-2.0.0-7-TESTONLY-20210331.ova"

VM_NAME="dg-32"
DM="thin"
Deployment="onpremise-standard"

ActiveVnics="3"

Hostname="dg-32.cisco.com"
Vnic0IPv4Address="172.23.213.32"
Vnic0IPv4Gateway="172.23.213.1"
Vnic0IPv4Netmask="255.255.255.0"
Vnic0IPv4Method="Static"
Vnic1IPv4Address="32.32.32.32"
Vnic1IPv4Gateway="32.32.32.1"
Vnic1IPv4Netmask="255.255.255.0"
Vnic1IPv4Method="Static"

DNS="171.70.168.183"
NTP="ntp.esl.cisco.com"
Domain="cisco.com"

ControllerIP="172.23.213.10"
ControllerPort="30607"
ControllerSignCertChain="cw-admin@172.23.213.10:/home/cw-admin/controller.pem"
ControllerCertChainPwd="Cwork123!"

Description="Description for Cisco Crosswork Data Gateway for 32"
Label="Label for Cisco Crosswork Data Gateway dg-32"
```

```
dg_adminPassword="cisco123"
dg_operPassword="cisco123"


ProxyUsername="cisco"
ProxyPassphrase="cisco123"


SyslogAddress="127.0.0.1"
SyslogPort=514
SyslogProtocol="UDP"
SyslogTLS=False
SyslogPeerName="combo-46.cisco.com"
SyslogCertChain="root@172.23.213.46:/root/stproxy/proxycert/CA.pem"
SyslogCertChainPwd="cisco123"

# Please replace this information according to your vcenter setup
VCENTER_LOGIN="administrator%40vsphere.local:Vtsisco%40123%21@172.23.213.21"
VCENTER_PATH="DC1/host/172.23.213.8"
DS="datastore1 (5)"

ovftool --acceptAllEulas --X:injectOvfEnv --skipManifestCheck --overwrite --noSSLVerify
--powerOffTarget --powerOn \
--allowExtraConfig --extraConfig:firmware=efi --extraConfig:uefi.secureBoot.enabled=true \
--datastore="$DS" --diskMode="$DM" \
--name=$VM_NAME \
--net:"vNIC0=VM Network" \
--net:"vNIC1=DPortGroupVC-2" \
--net:"vNIC2=DPortGroupVC-1" \
--deploymentOption=$Deployment \
--prop:"ControllerIP=$ControllerIP" \
--prop:"ControllerPort=$ControllerPort" \
--prop:"ControllerSignCertChain=$ControllerSignCertChain" \
--prop:"ControllerCertChainPwd=$ControllerCertChainPwd" \
--prop:"Hostname=$Hostname" \
--prop:"Description=$Description" \
--prop:"Label=$Label" \
--prop:"ActiveVnics=$ActiveVnics" \
--prop:"Vnic0IPv4Address=$Vnic0IPv4Address" \
--prop:"Vnic0IPv4Gateway=$Vnic0IPv4Gateway" \
--prop:"Vnic0IPv4Netmask=$Vnic0IPv4Netmask" \
--prop:"Vnic0IPv4Method=$Vnic0IPv4Method" \
--prop:"Vnic1IPv4Address=$Vnic1IPv4Address" \
--prop:"Vnic1IPv4Gateway=$Vnic1IPv4Gateway" \
--prop:"Vnic1IPv4Netmask=$Vnic1IPv4Netmask" \
--prop:"Vnic1IPv4Method=$Vnic1IPv4Method" \
--prop:"DNS=$DNS" \
--prop:"NTP=$NTP" \
--prop:"dg-adminPassword=$dg_adminPassword" \
--prop:"dg-operPassword=$dg_operPassword" \
--prop:"Domain=$Domain" $ROBOT_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"
```

Step 1 Open a command prompt.

Step 2 Navigate to the location where you installed the OVF Tool.

Step 3 Run the OVF Tool in one of the following ways:

a) **Using the command**

The command contains the location of the source OVF file and location of the vmx file that will be created as a result of executing the command:

```
ovftool <location_of_source_ovf_file> <location_of_vmx_file>
```

For example,

```
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds="datastore130-2"
 --deploymentOption="onpremise-standard" --diskMode="thin" --prop:"ControllerIP=<controller-ip>"
 --prop:"ControllerPort=30607" --prop:"ControllerSignCertChain=<location of controller.pem file>"

--prop:"ControllerCertChainPwd=<password>" --overwrite --powerOffTarget --powerOn
--noSSLVerify --allowExtraConfig --extraConfig:firmware=efi
--extraConfig:uefi.secureBoot.enabled=true --name="cdg147.cisco.com"
--prop:"Hostname=cdg147.cisco.com" --prop:"Description=CDG Base VM for Automation"
--net:"vNIC0=VM Network" --prop:"Vnic0IPv4Method=Static"
--prop:"Vnic0IPv4Address=<vNIC 0 IPv4 address>" --prop:"Vnic0IPv4Netmask=<vNIC0 IPv4 netmask>"
--prop:"Vnic0IPv4Gateway=<vNIC 0 IPv4 gateway>" --net:"vNIC1=DPG991"
--prop:"Vnic1IPv4Method=Static" --prop:"Vnic1IPv4Address=<vNIC1 IPv4 address>"
--prop:"Vnic1IPv4Netmask=<vNIC1 IPv4 netmask>" --prop:"Vnic1IPv4Gateway=<vNIC1 IPv4 gateway>"
--net:"vNIC2=DPG999" --prop:"dg-adminPassword=<password>"
--prop:"dg-operPassword=<password>" --prop:"DNS=<DNS address>"
--prop:"NTP=<NTP>"
--prop:"Domain=cisco.com" <image download url> vi://<username>:<password>'@<IP address>/DC/host/<IP
 address>
```

b) **Using the script**

If you want to execute the script thast you have created containing the command and arguments, run the following command:

```
root@cxcloudctrl:/opt# ./cdgovfdeployVM197
```

Once the VM powers up, log into the VM. See Login into Crosswork Data Gateway VM. After you login, the Crossway Data Gateway should present you with the welcome screen and options menu indicating that the installation completed successfully. Log out and proceed with the post-installation tasks explained in the next section.

Install Cisco Crosswork Data Gateway on Cisco CSP

Follow the steps to install Cisco Crosswork Data Gateway on Cisco CSP:

Step 1 **Download the Cisco Crosswork Data Gateway `qcow2` package:**

a) Download Cisco Crosswork Data Gateway `qcow2` package from cisco.com to your local machine or a location on your local network that is accessible to your Cisco CSP. For the purpose of these instructions, we will use the package name **"cw-na-dg-2.0.0-18-release-qcow2-pkg.tar.gz"**.

b) Unzip the `qcow2` package with the following command:

```
tar -xvf cw-na-dg-2.0.0-18-release-qcow2-pkg.tar.gz
```

The content of the `qcow2` package is unzipped to a new directory (e.g. `cw-na-dg-2.0.0-18-release-qcow2`).

This new directory will contain the Cisco Crosswork Data Gateway `qcow2` build (e.g. **cw-na-dg-2.0.0-18-release-20210409.tar.gz**) and other files necessary to validate the build.

Step 2 **(optional) Verify the Cisco Crosswork Data Gateway `qcow2` package:**

a) Navigate to the directory created in the previous step.

b) Use the following command to verify the signature of the build:

Note The machine where the script is being run needs HTTP access to cisco.com. Please contact Cisco Customer Experience team if access to cisco.com is not possible due to security restrictions, or if you did not get a successful verification message after running the script.

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s <.tar.gz.signature file>
-v dgst -sha512
```

Note The cisco_x509_verify_release.py script is only compatible with python 2. Instead of using the provided script, you can also calculate and verify the md5 or SHA512 checksum of the file originally downloaded from Cisco against the checksum posted on Cisco.com.

Step 3 **Prepare Cisco Crosswork Data Gateway Service Image for upload to Cisco CSP:**

a) The Cisco Crosswork Data Gateway `qcow2` build is a tarball of the `qcow2` and `config.txt` files. Unzip the `.tar.gz` (e.g. **cw-na-dg-2.0.0-18-release-20210409.tar.gz**) with the following command:

```
tar -xvf ccw-na-dg-2.0.0-18-release-20210409.tar.gz
```

b) Open the `config.txt` file and modify the parameters as per your installation requirements. See Section Cisco Crosswork Data Gateway Parameters and Deployment Scenarios, on page 60.

Following parameters have pre-defined values:

- Deployment
  - Use "Crosswork On-Premise" for Crosswork On-Premise.
- Profile
  - Use "Standard" for standard deployment.
  - Use "Extended" for extended deployment.

Below is an example of how the `config.txt` file looks like:

```
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=
ControllerIP=changeme
ControllerPort=30607
ControllerSignCertChain=
ControllerTlsCertChain=
Deployment=Crosswork On-Premise
Description=changeme
DGAppdataDisk=5
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=changeme
DNSSEC=False
DNSTLS=False
Domain=changeme
EnrollmentPassphrase=
EnrollmentURI=
Hostname=changeme
Label=
LLMNR=False
mDNS-False
NTP=changeme
```

```
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
PortSNMPTrap=1062
PortSyslogTCP=9898
PortSyslogTLS=6514
PortSyslogUDP=9514
Profile=Standard
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=
SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=0.0.0.0
Vnic0IPv4Gateway=0.0.0.1
Vnic0IPv4Method=None
Vnic0IPv4Netmask=0.0.0.0
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=::0
Vnic0IPv6Gateway=::1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
Vnic1IPv4Address=0.0.0.0
Vnic1IPv4Gateway=0.0.0.1
Vnic1IPv4Method=None
Vnic1IPv4Netmask=0.0.0.0
Vnic1IPv4SkipGateway=False
Vnic1IPv6Address=::0
Vnic1IPv6Gateway=::1
Vnic1IPv6Method=None
Vnic1IPv6Netmask=64
Vnic1IPv6SkipGateway=False
Vnic2IPv4Address=0.0.0.0
Vnic2IPv4Gateway=0.0.0.1
Vnic2IPv4Method=None
Vnic2IPv4Netmask=0.0.0.0
Vnic2IPv4SkipGateway=False
Vnic2IPv6Address=::0
Vnic2IPv6Gateway=::1
Vnic2IPv6Method=None
Vnic2IPv6Netmask=64
Vnic2IPv6SkipGateway=False
dg-adminPassword=changeme
dg-operPassword=changeme
```

Step 4 **Upload Cisco Crosswork Data Gateway Service Image to Cisco CSP:**

a) Log into the Cisco CSP.

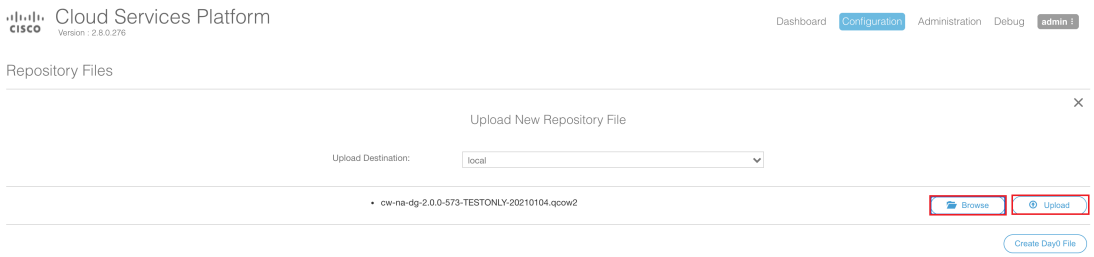
b) Go to **Configuration** > **Repository**.

c) On the **Repository Files** page, Click ⊞ button.

d) Select an **Upload Destination**.

e) Click **Browse**, navigate to the `qcow2` file, click **Open** and then **Upload**.

Repeat this step to upload `config.txt` file.



After the file is uploaded, the file name and other relevant information are displayed in the **Repository Files** table.

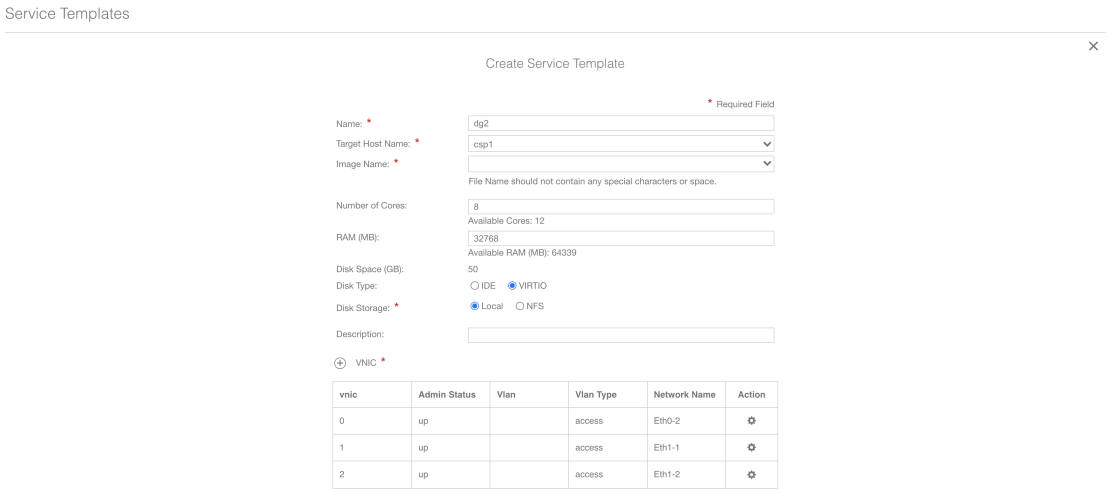
Step 5 **Create Crosswork Data Gateway VM:**

a) Go to **Configuration** > **Services**.

b) On the **Service** page, click ⊞ button.

c) Check **Create Service** option.

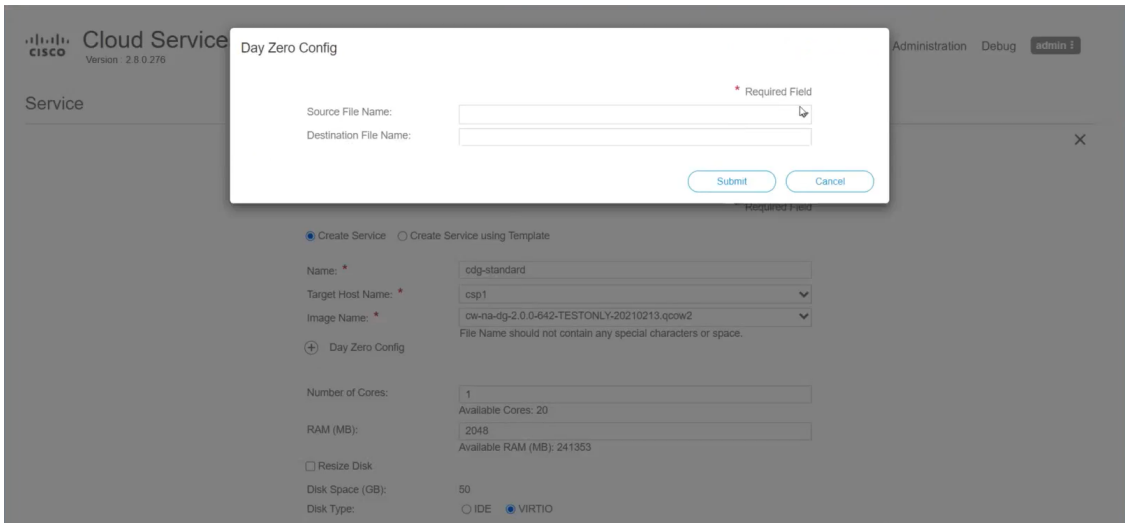
The **Create Service Template** page is displayed.



d) Enter the values for the following fields:

Field	Description
Name	Name of the VM.
Target Host Name	Choose the target host on which you want to deploy the VM.
Image Name	Select the `qcow2` image.

e) Click **Day Zero Config**.



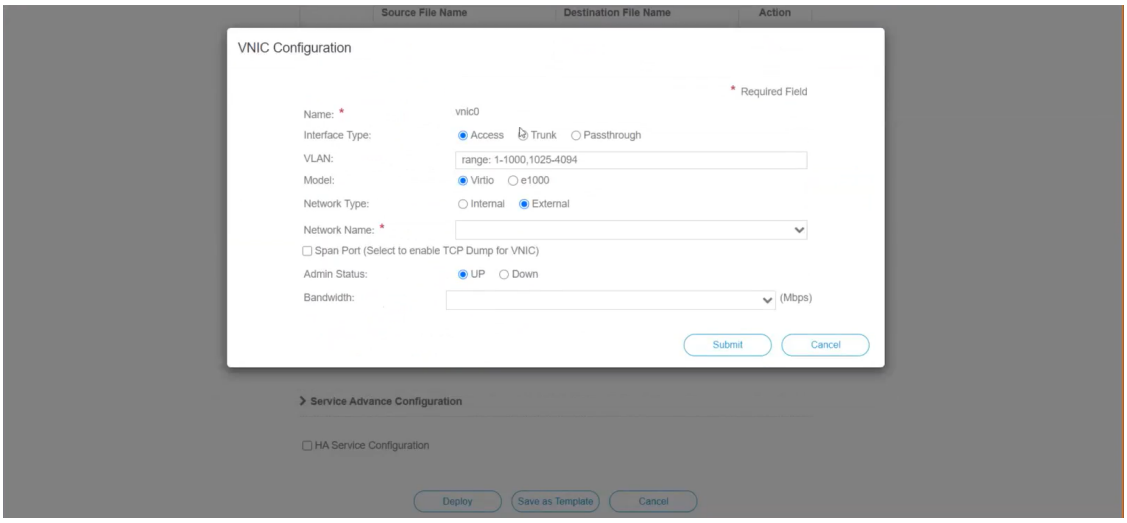
In the **Day Zero Config** dialog box, do the following:

1. From the **Source File Name** drop-down list, select a day0 configuration file i.e., the `config.txt` file that you modifed and uploaded earlier.
2. In the **Destination File Name** field, specify the name of the day0 destination text file. This must always be "config.txt".
3. Click **Submit**.

f) Enter the values for the following fields:

Field	Description
Number of Cores	Standard: 8 Extended: 16
RAM (MB)	Standard: 32768 Extended: 98304

g) Click **VNIC**.



In the **VNIC Configuration** dialog box, do the following:

Note The VNIC Name is set by default.

1. Select the **Interface Type** as **Access**.
2. Select the **Model** as **Virtio**.
3. Select the **Network Type** as **External**.
4. Select **Network Name**:

For VNIC...	Select...
vnic0	Eth0-1
vnic1	Eth1-1
vnic2	Eth1-2

5. Select **Admin Status** as **UP**.
6. Click **Submit**.
7. Repeat Steps **i** to **vi** for vNIC1 and vNIC2.

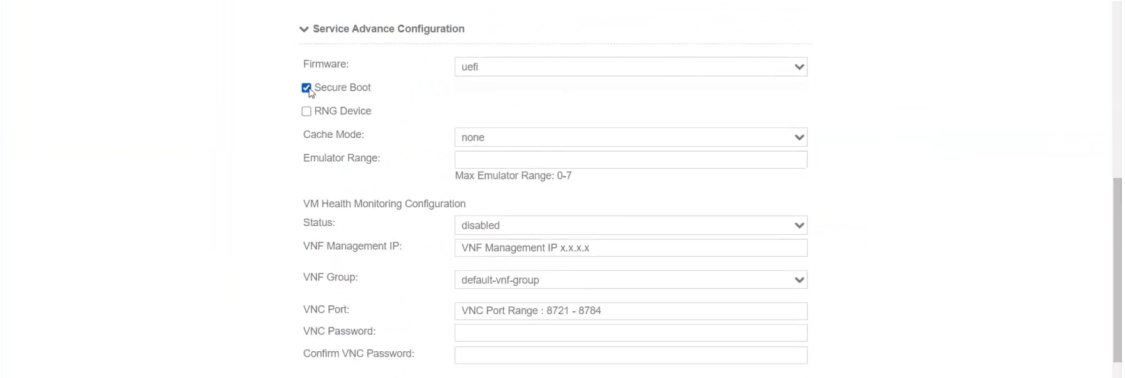
After you have added all three vNICs, the VNIC table will look like this:

VNIC *

vnic	Admin Status	Vlan	Vlan Type	Network Name	Action
0	up		access	Eth0-1	
1	up		access	Eth1-1	
2	up		access	Eth1-2	

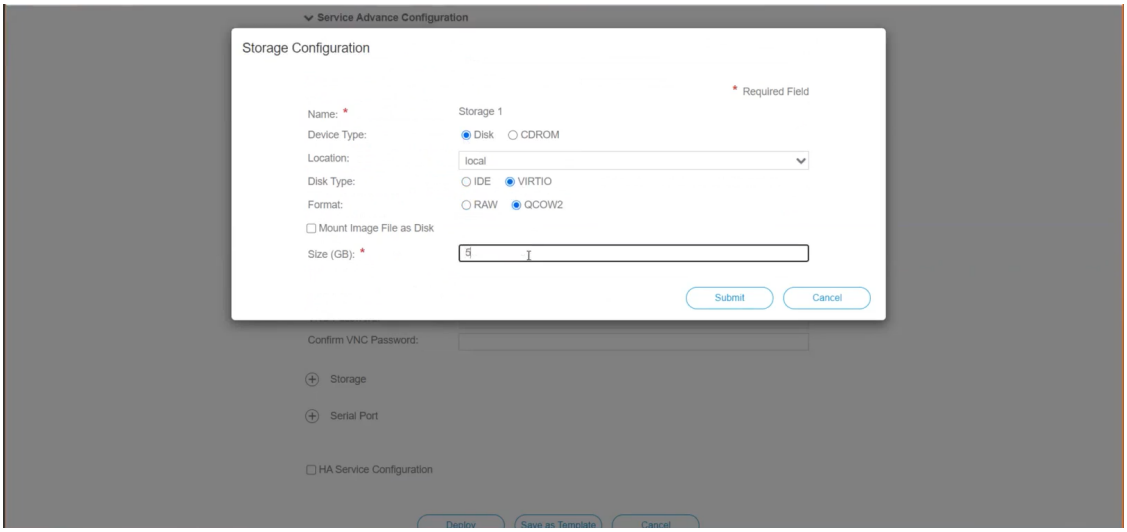
h) Expand the **Service Advance Configuration** and for **Firmware**, select **uefi** from the drop-down.

Check the **Secure Boot** checkbox.



i) Click **Storage**.

In the **Storage Configuration** dialog box, do the following:

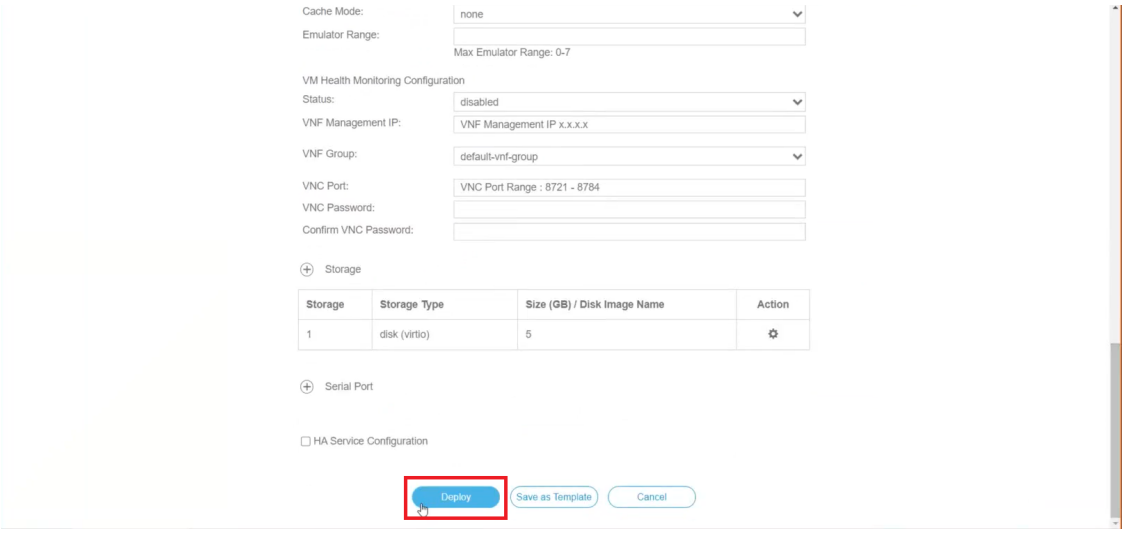


Field	Description
Name	Name of the storage. This is specified by default.

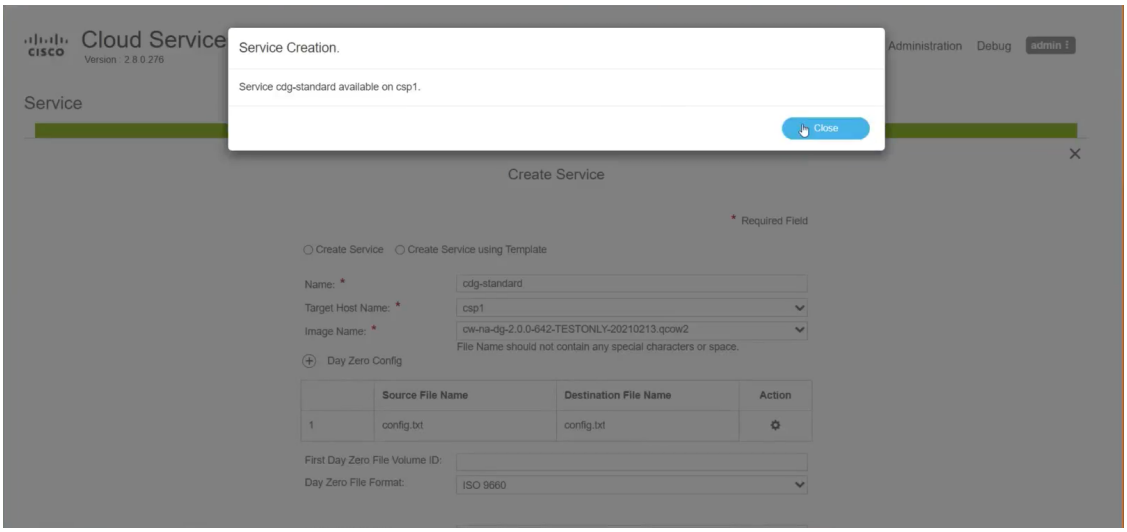
Field	Description
Device Type	Select **Disk**.
Location	Select **local**.
Disk Type	Select **VIRTIO**.
Format	Select **QCOW2**.
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size (**5** for Standard and **500** for Extended.)

When you are done with the storage configuration, click **Submit**.

j) Click **Deploy**.



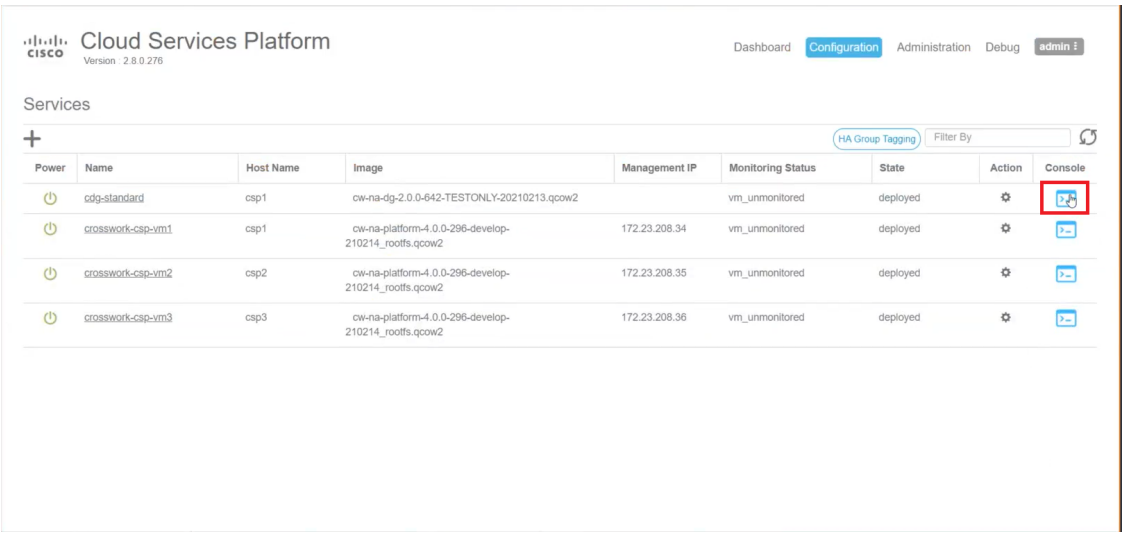
You will see a similar message once the service has successfully deployed. Click **Close**.



Step 6 **Deploy Cisco Crosswork Data Gateway service:**

a) Go to **Configuration** > **Services**.

b) In the **Services** table, click the console icon under **Console** column for the Cisco Crosswork Data Gateway service you created above.



c) The **noVNC** window opens. Click **Connect** option in the top right corner.

d) Once the Cisco Crosswork Data Gateway service connects, enter username and password.

The Cisco Crosswork Data Gateway console is available.

After you login, the Crossway Data Gateway should present you with the welcome screen and options menu indicating that the installation completed successfully.

Crosswork Data Gateway Post-installation Tasks

After installing Cisco Crosswork Data Gateway, configure the timezone and log out of the Croosswork Data Gateway VM.

- Configure Timezone of the Crosswork Data Gateway VM, on page 87
- Log Out of Crosswork Data Gateway VM, on page 90

Configure Timezone of the Crosswork Data Gateway VM

The Crosswork Data Gateway VM first launches with default timezone as UTC. Update the timezone with your geographical area so that all Crosswork Data Gateway processes (including the showtech logs) reflect the timestamp corresponding to the location you have chosen.

Step 1 In Crosswork Data Gateway VM interactive menu, select **Change Current System Settings**.

Step 2 Select **9 Timezone**.

Step 3 Select the geographic area in which you live.

```
┤ Configuring tzdata ├
Please select the geographic area in which you live. Subsequent
configuration questions will narrow this down by presenting a list of
cities, representing the time zones in which they are located.

Geographic area:

                        Asia
                        Atlantic Ocean
                        Europe
                        Indian Ocean
                        Pacific Ocean
                        System V timezones
                        US
                        None of the above

                 <Ok>                      <Cancel>
```

Step 4 Select the city or region corresponding to your timezone.

```
┤ Configuring tzdata ├
Please select the city or region corresponding to your time zone.

Time zone:

                    Alaska
                    Aleutian
                    Arizona
                    Central
                    Eastern
                    Hawaii
                    Starke County (Indiana)
                    Michigan
                    Mountain
                    Pacific Ocean
                    Samoa

                <Ok>                     <Cancel>
```

Step 5 Select **OK** to save the settings.

Step 6 Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone.

Step 7 Log out of the Crosswork Data Gateway VM.

Log in and Log out of Crosswork Data Gateway VM

You can log into the Crosswork Data Gateway VM in one of the following ways:

- Access Crosswork Data Gateway VM from SSH, on page 89
- Access Crosswork Data Gateway Through vCenter, on page 89
- Access Crosswork Data Gateway Through Cisco CSP, on page 90

To log out of the Crosswork Data Gateway VM:

- Log Out of Crosswork Data Gateway VM, on page 90

Access Crosswork Data Gateway VM from SSH

The SSH process is protected from brute force attacks by blocking the client IP after a number of login failures. Failures such as incorrect username or password, connection disconnect, or algorithm mismatch are counted against the IP. Up to 4 failures within a 20 minute window will cause the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures will cause the blocked time to be increased. Each client IP is tracked separately.

Follow these steps to login to the Cisco Crosswork Data Gateway VM from SSH.

Step 1 From your work station with network access to the Cisco Crosswork Data Gateway management IP, run the following command:

ssh <username>@<ManagementNetworkIP>

where **ManagementNetworkIP** is the management network IP address.

For example,

To login as adminstrator user: **ssh dg-admin@<ManagementNetworkIP>**

To login as operator user: **ssh dg-oper@<ManagementNetworkIP>**

The Crosswork Data Gateway flash screen opens prompting for password.

Step 2 Input the corresponding password (the one that you created during installation process) and press **Enter**.

If you are unable to access the Cisco Crosswork Data Gateway VM, there is an issue with your network configuration settings. From the console check the network settings. If they are incorrect, it is best to delete the Cisco Crosswork Data Gateway VM and re-install with the correct network settings.

Access Crosswork Data Gateway Through vCenter

Follow these steps to log in via vCenter:

Step 1 Locate the VM in vCenter and then right click and select **Open Console**.

The Crosswork Data Gateway console comes up.

Step 2 Enter username (`dg-admin` or `dg-oper` as per the role assigned to you) and the corresponding password (the one that you created during installation process) and press **Enter**.

Access Crosswork Data Gateway Through Cisco CSP

Follow the steps to launch Crosswork Data Gateway on Cisco CSP:

Step 1 Log into your Cisco CSP.

Step 2 Go to **Configuration** > **Services**. The **Service** table shows the current status of services.

Step 3 Find your Crosswork Data Gateway service in the **Service Name** column.

Click on the **Console** icon under **Console** column to launch the service.

Step 4 In the Crosswork Data Gateway login prompt, enter your username and password and press **Enter**. Crosswork Data Gateway interactive menu is displayed.

Log Out of Crosswork Data Gateway VM

To log out, select option **l Logout** from the Main Menu and press Enter or click **OK**.

Cisco Crosswork Data Gateway Authentication and Enrollment

Once the Crosswork Data Gateway is installed, it identifies itself and enrolls with Cisco Crosswork automatically. Cisco Crosswork then instantiates a new Crosswork Data Gateway instance in its database and waits for a "first-sign-of-life" from the Crosswork Data Gateway VM.

After the connectivity is established, the Crosswork Data Gateway instance confirms the identity of the controller application (Cisco Crosswork) and offers its own proof of identity via signed certificates. Cisco Crosswork Data Gateway then downloads the configuration files and functional images (collection profiles) from Cisco Crosswork.

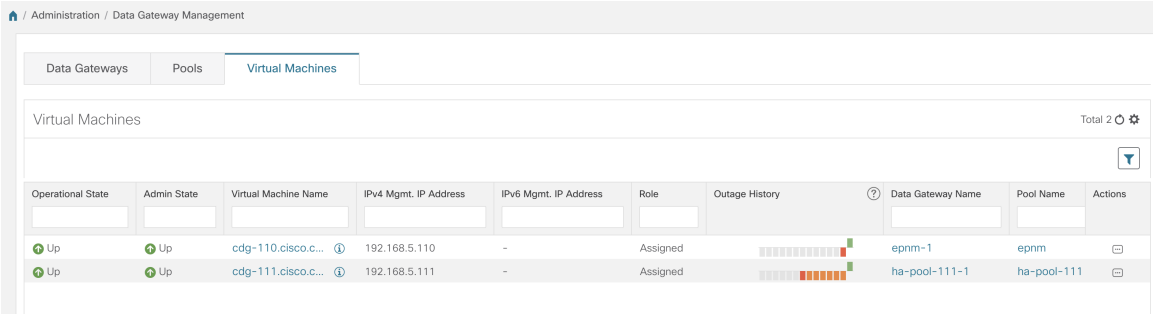
To verify if the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork:

1. Log into the Cisco Crosswork UI. See Log into the Cisco Crosswork UI, on page 54.
2. Navigate to **Administration** > **Data Gateway Management**.
3. Click on **Virtual Machines** tab.

   All the Cisco Crosswork Data Gateway VMs that have successfully enrolled with Cisco Crosswork are displayed here.

Newly installed Crosswork Data Gateway VMs have the **Operational State** as "Degraded". After enrolling successfully with Cisco Crosswork, the **Operational State** changes to **Not Ready**. While it depends on the bandwidth between the Crosswork Data Gateway VMs and Cisco Crosswork, this operation typically takes less than 5 minutes.

Note Cisco Crosswork Data Gateway VMs that were previously onboarded and still have the **Operational State** as **Degraded** need to be investigated. Contact Cisco Customer Experience team for assistance.



Click the Refresh icon in the **Virtual Machines** pane to refresh the pane and reflect the latest **Operational State** of the Crosswork Data Gateway VMs.

Note Crosswork Data Gateway VMs that have the **Role** as **Unassigned** must be assigned to a pool before they can used. A Cisco Crosswork Data Gateway VM is your physical Crosswork Data Gateway. You cannot attach or detach devices to it. Devices can be attached only to a Cisco Crosswork Data Gateway pool.

Troubleshoot Crosswork Data Gateway Installation and Enrollment

If Crosswork Data Gateway fails to auto-enroll with Cisco Crosswork, you can collect Crosswork Data Gateway showtech (**Main menu** > **5 Troubleshooting** > **Run show-tech**) and check for the reason in `controller-gateway` logs. If there are session establishment/certificate related issues, ensure that the `controller.pem` certificate is uploaded using the interactive menu.

The following table lists common problems that might be experienced while installing or enrolling Crosswork Data Gateway, and provides approaches to identifying the source of the problem and solving it.

Table 17: Troubleshooting the Installation/Enrollment

Issue	Action
1. Cannot enroll Crosswork Data Gateway with Cisco Crosswork	

Issue	Action
Crosswork Data Gateway cannot be enrolled with Cisco Crosswork due to an NTP issue, i.e., there is a clock-drift between the two. The clock-drift might be with either Crosswork Data Gateway or Cisco Crosswork. Also, on the NTP servers for Cisco Crosswork and Crosswork Data Gateway, the initial time is set to the ESXi server. For this reason, the ESXi server must also have NTP configured. Sync the clock time on the host and retry.	1. Log into the Crosswork Data Gateway VM. 2. From the main menu, go to **5 Troubleshooting** > **Run show-tech**. Enter the destination to save the tarball containing logs and vitals and click **OK**. In the show-tech logs (in file `session.log` at location `/cdg/logs/components/controller-gateway/session.log`), if you see the error `UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid`, then there is a clock-drift between Crosswork Data Gateway and Cisco Crosswork. 3. From the main menu, go to **3 Change Current System Settings** > **1 Configure NTP**. Configure NTP to sync with the clock time on the Cisco Crosswork server and try re-enrolling Crosswork Data Gateway.
2. Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals"	
Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals" due to certificate errors.	1. Log into the Crosswork Data Gateway VM. 2. From the main menu, select **5 Troubleshooting** > **Run show-tech**. Enter the destination to save the tarball containing logs and vitals and click **OK**. In the show-tech logs (in file `gateway.log` at location `/cdg/logs/components/controller-gateway/gateway.log`), if you see certificate errors, then re-upload the Controller Signing Certificate, as explained in the steps below: 1. From the main menu, select **3 Change Current System Settings** > **7 Import Certification**. 2. From the **Import Certificates** menu, select **1 Controller Signing Certificate File** and click **OK**. 3. Enter the SCP URI for the certificate file and click **OK**.
3. Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established"	

Issue	Action
Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established" due to certificate errors.	1. Re-upload the certificate file as explained in the troubleshooting scenario **2.** above. 2. Reboot the Crosswork Data Gateway VM following the steps below: a. From the main menu, select **5 Troubleshooting** and click **OK**. b. From the Troubleshooting menu, select **7 Reboot VM** and click **OK**. c. Once the reboot is complete, check if the Crosswork Data Gateway's operational status is **Up**.
Crosswork Data Gateway goes into Error state	Check the vNIC values in the OVF template in case of vCenter and config.txt in case of Cisco CSP.
Crosswork Data Gateway enrollment with 1 NIC Cisco Crosswork fails	Check the vNIC values in the OVF template in case of vCenter and config.txt in case of Cisco CSP. If ActiveVnics property is missing for 1 NIC and 2 NIC, Crosswork Data Gateway tries to deploy 3 NICs by default. Due to this, Crosswork Data Gateway enrollment with 1 NIC Cisco Crosswork fails post deployment with error in gateway.log that Crosswork Data Gateway expected 1 NIC, but it is not 1 NIC.
Crosswork Data Gateway deploys standard profile instead of extended	Check the deploymentoption property in the OVF template in case of vCenter and config.txt in case of Cisco CSP. If "deploymentoption" property mismatches or does not exist for extended profile template, then Crosswork Data Gateway deploys standard profile.

Import Controller Signing Certificate File

The Controller Certificate file is automatically imported after the VM boots. You will need to perform this step manually for the following reasons:

- You have not specified **Controller Signing Certificate File URI** under the **Controller Settings** during installation.
- Cisco Crosswork was upgraded and you need to authenticate and enroll Crosswork Data Gateway with Cisco Crosswork.

Follow these steps to import controller signing certificate file.

Step 1 From the Cisco Crosswork Data Gateway VM's Interactive Menu, select **3 Change Current System Settings**.

The **Change System Settings** menu opens.

Step 2 Select **7 Import Certificate**.

Step 3 From **Import Certificates** menu, select **1 Controller Signing Certificate File**.

Step 4 Enter the SCP URI for the certificate file.

An example URI is given below:

```
cw-admin@{server ip}:/home/cw-admin/controller.pem
```

Step 5 Enter the SCP passphrase (the SCP user pasword).

The certificate file is imported.

Step 6 Verify that the certificate was installed successfully. See View the Controller Signing Certificate File, on page 94.

View the Controller Signing Certificate File

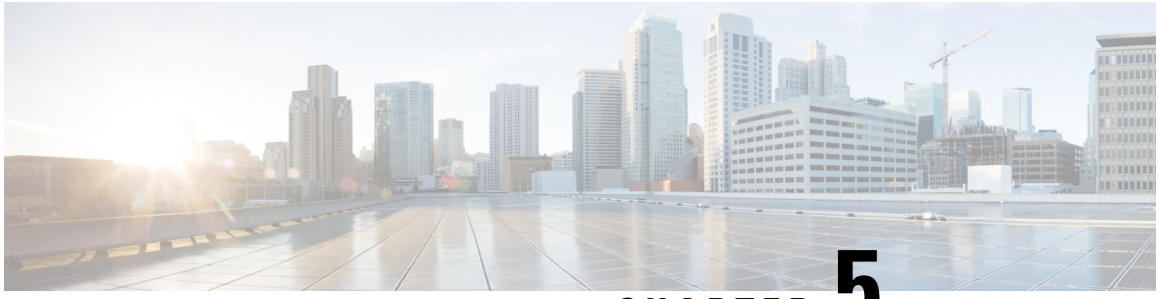
Follow the steps to view the signing certificate.

Step 1 From the Crosswork Data Gateway VM's interactive menu, select **2 Show System Settings**.

Step 2 From the **Show Current System Settings** menu, select **7 Certificates**.

Step 3 Select **2 Controller Signing Certificate File**.

Crosswork Data Gateway displays the default certificate if no new certificate has been imported. Otherwise, it displays the new certificate if it was successfully imported.



CHAPTER 5

Install Crosswork Applications

This chapter contains the following topics:

Install Crosswork Applications

This section explains how to install a Cisco Crosswork application from the Cisco Crosswork UI.

Every crosswork application is packaged in a particular format unique to Crosswork known as CAPP (Crosswork APPlication). The application CAPP files are downloaded from cisco.com to a machine reachable from the Cisco Crosswork server, and added to the Crosswork UI where it can be installed. You need to have the credentials that will allow you to copy the CAPP files from that machine.

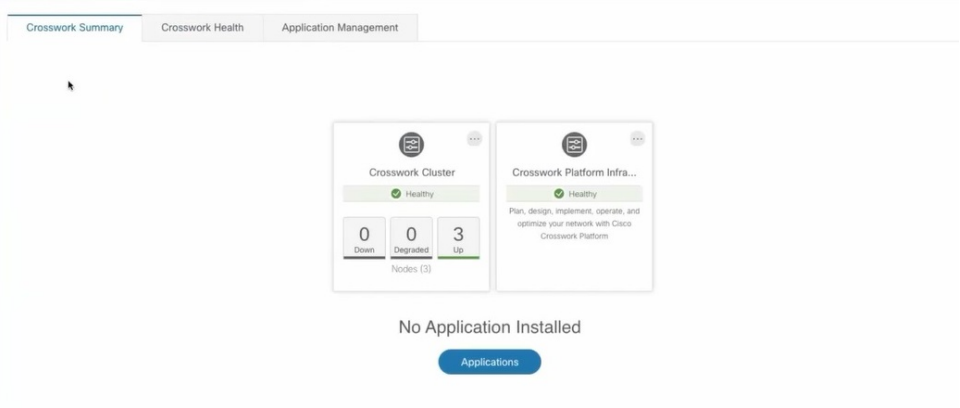
Before you begin

Ensure that all requirements of your application are met. For more information, see Installation Dependencies for Cisco Crosswork Products, on page 18.

Note Installation of Crosswork Service Health (Automated Assurance) will fail if Crosswork Active Topology is not already installed.

Step 1 Download or copy the CAPP files from cisco.com to a server that can be reached from the CW server.

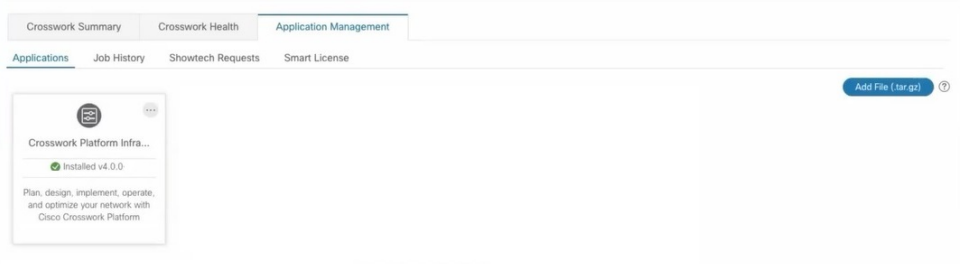
Step 2 Log into Cisco Crosswork and in the homepage, click on **Administration** > **Crosswork Management**. The **Crosswork Summary** page is displayed with Crosswork Cluster and Crosswork Platform Infrastructure tiles.



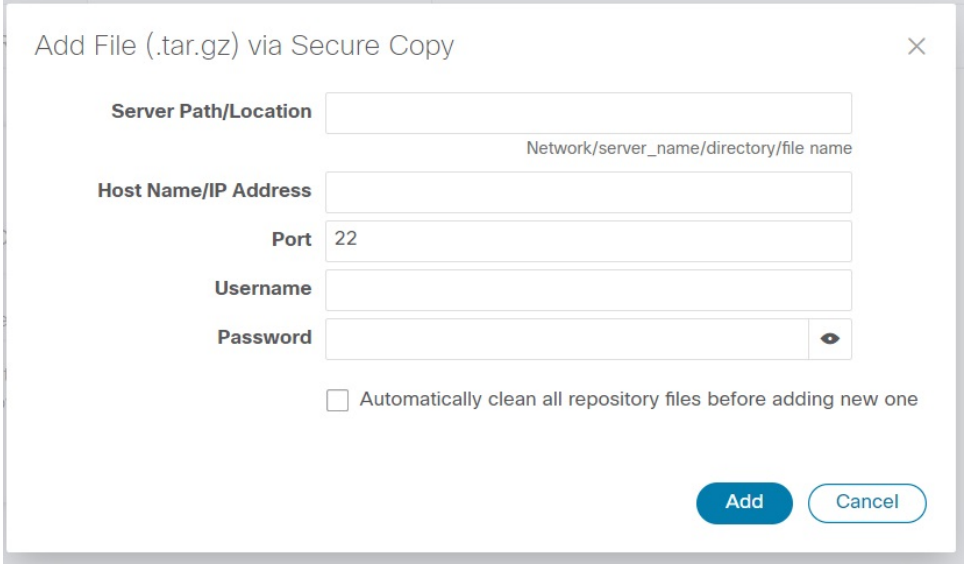
You can click on the tiles to get more information.

Step 3 To install an application, click on **Applications** button. Alternately, click on the **Application Management** tab.

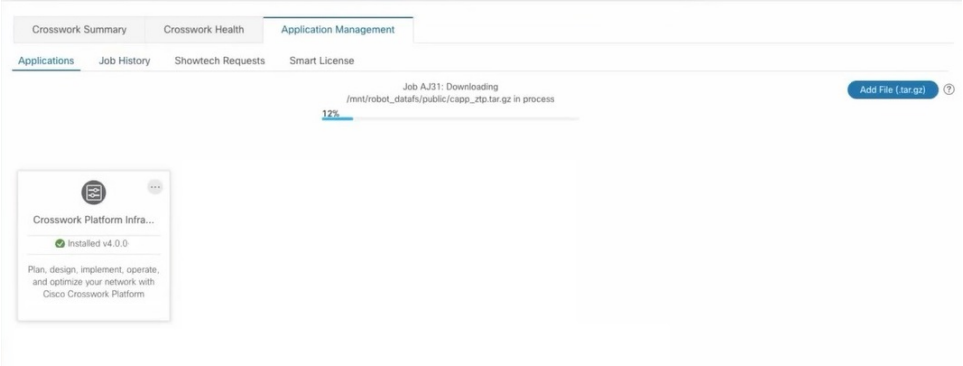
Step 4 In the Application Management screen, select the **Applications** tab, and click on the **Add File (.tar.gz)** option to add a CAPP file.



Step 5 In the Add File dialog box, enter the relevant information and click **Add**.

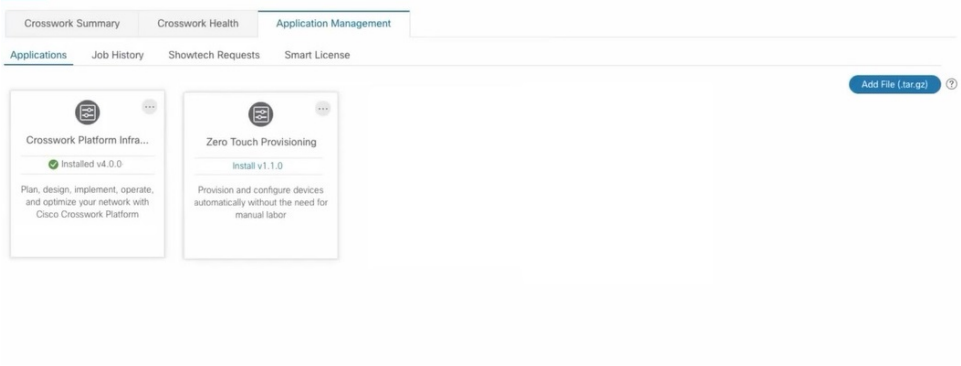


The add operation progress is displayed on the **Applications** screen.

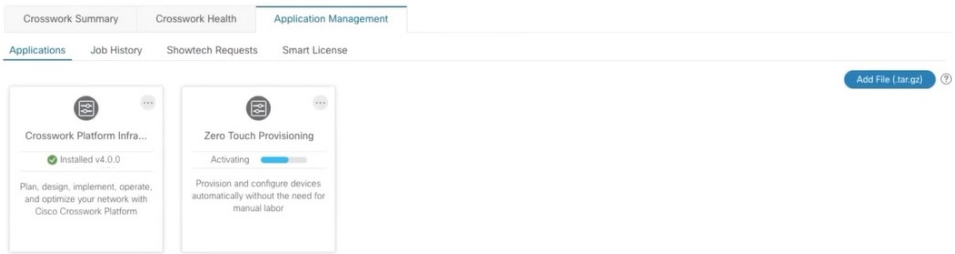


Note You can add a new CAPP file while another CAPP file is being added. The system will add each file in sequence, and the current CAPP file that is added will be displayed on the screen.

Step 6 The newly added application (CAPP file) is displayed as a tile on the **Applications** screen. To install, click on the Install prompt on the tile. You can also click ··· on the tile, and select the **Install** option from the drop down list.

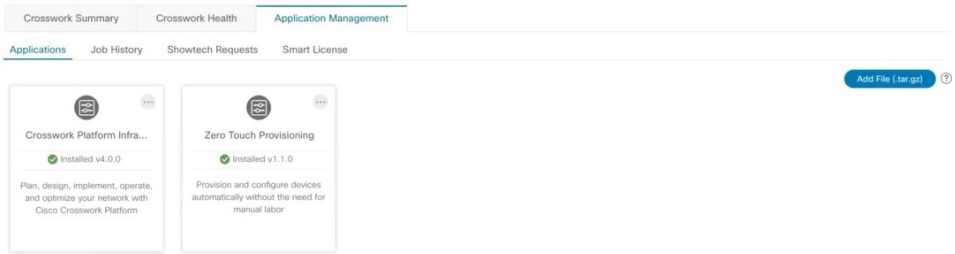


The progress of installation is displayed on the application tile. You can also view the installation progress in the **Job History** tab.



The application is now installed. You can observe the change in the application tile icon. Once an application is installed, all the related-resources, UI screens and menu options are dynamically loaded in the Crosswork UI.

You can initiate multiple installs by clicking the install option in the application tiles. The system will install the CAPP files in sequence, and the progress of current CAPP being will be displayed on the screen. The applications are that are in queue to be installed will have the status as "Install pending"

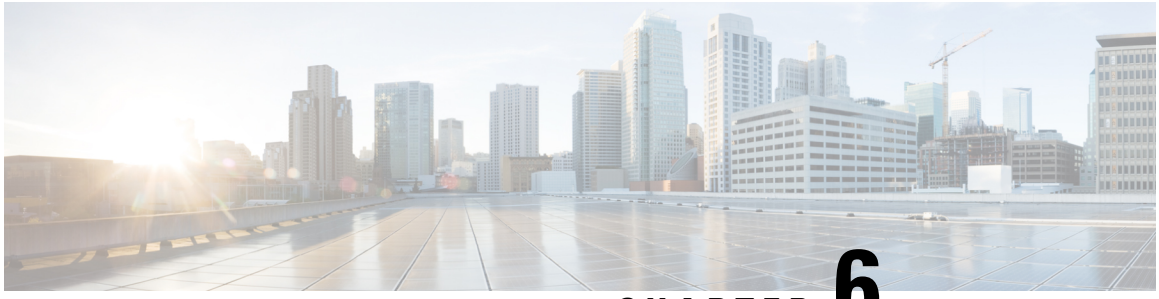


Note Once an application is installed, the 90-day evaluation period will automatically start. You can register the application with your Cisco Smart Account in the the **Smart License** tab.

Step 7 After an application is installed, it must be activated to become functional. The first-time installation also activates a CAPP file. However, if the activation fails after a successful installation, you can manually activate the application. To manually activate an application, click the ··· on the application tile, and select **Activate**.

Step 8 Repeat steps 6 to 8 for adding more applications.

Step 9 (Optional) Click ··· on the application tile, and select the **View Details** option to view details of the installed application.



CHAPTER 6

Upgrade Cisco Crosswork

This chapter contains the following topics:

Cisco Crosswork 4.0 to 4.1 Upgrade Workflow

This section provides the high-level workflow for upgrading Cisco Crosswork from release 4.0 to release 4.1. This includes upgrading Cisco Crosswork cluster, Cisco Crosswork Data Gateway and Crosswork Applications to Release 4.1, within a single maintenance window.

Each stage in this upgrade workflow must be executed in sequence, and is explained in detail in later sections of this chapter. The stages are:

1. Shut Down Cisco Crosswork Data Gateway 2.0 VMs, on page 100
2. Create Backup and Shut Down Cisco Crosswork 4.0, on page 100
3. Install the Cisco Crosswork 4.1 Cluster, on page 103

Note While the cluster installation is in progress, you must upgrade NSO to version 5.5.2.12. The process to up NSO is not covered in this document. For more information, see the documentation for Cisco NSO 5.5 Additionally, if you are planning to use Cisco Optimization Engine individually or as part of the Cisco Ne Controller solution, upgrade your SR-PCE to the supported version as mentioned in the Crosswork Ne Controller Release Notes.

4. Install Cisco Crosswork 4.1 Applications, on page 103
5. Migrate the Cisco Crosswork 4.0 backup to Cisco Crosswork 4.1, on page 104
6. Upgrade to Cisco Crosswork Data Gateway 3.0, on page 105
7. Post-upgrade Checklist, on page 111

The time taken for the entire upgrade window can vary based on size of your deployment profile and the performance characteristics of your hardware.

Warning Migration of Cisco Crosswork from 4.0 to 4.1 has the following limitations:

- Third-party device configuration in Device Lifecycle Management (DLM) and Cisco NSO is not migrated, and needs to be re-applied on the new Cisco Crosswork version post migration.
- Custom user roles (Read-Write/Read) created in Cisco Crosswork 4.0 are not migrated, and need to be updated manually on the new version post migration.
- Crosswork Health Insights KPI alert history is not retrieved as part of the migration.

Crosswork applications can be independently updated from the Cisco Crosswork UI in case of minor updates or patch releases. For more information, see Update a Crosswork Application (standalone activity) , on page 113.

Shut Down Cisco Crosswork Data Gateway 2.0 VMs

This is the first stage of the upgrade workflow.

Note When Crosswork Data Gateway VMs are shut down, the data will not be forwarded to data destinations. Check with the application providers to determine if any steps are needed to avoid alarms or other problems.

Before you begin

Take screenshots of the all the tabs in the **Data Gateway Management** page to keep a record of the list of Crosswork Data Gateways, **Attached Device Count** in the Cisco Crosswork 4.0 UI. In the **Pools** tab, for each pool listed here, take a screenshot to make a note of the active, spare, and unassigned VM in the pool. This information is useful during Upgrade to Cisco Crosswork Data Gateway 3.0, on page 105.

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 Shut down the Cisco Crosswork Data Gateway 2.0 VMs.

a) Log in to the Crosswork Data Gateway VM. See Access Crosswork Data Gateway VM from SSH, on page 89.

Crosswork Data Gateway launches an Interactive Console after you login successfully.

b) Choose **5 Troubleshooting**.

c) From the **Troubleshooting** menu, choose **5 Shutdown VM** to shut down the VM.

Create Backup and Shut Down Cisco Crosswork 4.0

This is the second stage of the upgrade workflow. Creating a backup is a prerequisite when upgrading your Cisco Crosswork to a new software version.

Note We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Cisco Crosswork while the backup operation is running.

Before you begin

Follow these guidelines whenever you create a backup:

- Cisco Crosswork will back up the configuration of the system to an external server using SCP. Before you begin you need to have the following configuration in place and information about the SCP server available:
  - The hostname or IP address and the port number of a secure SCP server.
  - A preconfigured path on the SCP server where the backup will be stored.
  - User credentials with file read and write permissions to the directory.
  - The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.
- Ensure that you have configured a destination SCP server to store the backup files. This configuration is a one-time activity.
- Both the Cisco Crosswork cluster and the SCP server must be in the same IP environment. For example: If Cisco Crosswork is communicating over IPv6, so must the backup server.
- Keep a record of the list of Crosswork applications you have installed in the current version of Cisco Crosswork, as you can only install those applications after migrating to the new version of Cisco Crosswork.
- If you have onboarded a custom MIB package in Cisco Crosswork 4.0, download a copy of the package to your system. You will need to upload the package after you complete migrating to Cisco Crosswork 4.1. See Post-upgrade Checklist, on page 111 for more infomation.
- If you have modified Cisco Crosswork 4.0 to include third-party device types, you must download the third-party device configuration file, and re-apply it to Cisco Crosswork 4.1. The device configuration file is located on the cluster node (at `/mnt/cw_glusterfs/bricks/brick3/sys-oids.yaml`) and on the pod (at `/mnt/backup/sys-oids.yaml`).
- If Cisco Crosswork Optimization Engine has feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) that are enabled, you must disable them before proceeding. You must also, if available, export the current list of interfaces managed by LCM or BWOpt (**Traffic Engineering > Local Congestion Mitigation** or **Bandwidth Optimization > Link Management > Export** icon). Follow the steps documented in "Upgrade Crosswork Optimization Engine Feature Packs" in the latest *Cisco Crosswork Optimization Engine Release Notes*.

Step 1 Check and confirm that all the VMs are healthy and running in your cluster.

Step 2 **Configure an SCP backup server:**

a) From the Cisco Crosswork 4.0 main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the **Edit Destination** dialog box. Make the relevant entries in the fields provided.
c) Click **Save** to confirm the backup server details.

Step 3 **Create a backup:**

a) From the Cisco Crosswork 4.0 main menu, choose **Administration** > **Backup and Restore**.

b) Click **Actions** > **Backup** to display the **Backup** dialog box with the destination server details prefilled.

c) Provide a relevant name for the backup in the **Job Name** field.

d) If any of the VMs or applications are not in **Healthy** state, but you want to create the backup, check the **Force** check box.

Note The **Force** option must be used only after consultation with the Cisco Customer Experience team.

e) Uncheck the **Backup NSO** checkbox if you don't want to include Cisco NSO data in the backup.

If you do want to include Cisco NSO data in the Cisco Crosswork backup process, follow the instructions given in **Backup Cisco Crosswork with Cisco NSO** section in the *Cisco Crosswork Infrastructure 4.1 and Applications Administration Guide* instead of the instructions here.

f) Complete the remaining fields as needed.

If you want to specify a different remote server upload destination: Edit the pre-filled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

g) (Optional) Click **Verify Backup Readiness** to verify that Cisco Crosswork has enough free resources to complete the backup. Cisco Crosswork will also confirm that none of the applications are being updated, if the remote destination is correctly defined and the if applications are healthy. If the verifications are successful, Cisco Crosswork displays a warning about the time-consuming nature of the operation. Click **OK**.

If the verification is unsuccessful, please contact the Cisco Customer Experience team for assistance.

h) Click **Start Backup** to start the backup operation. Cisco Crosswork creates the corresponding backup job set and adds it to the job list. The Job Details panel reports the status of each backup step as it is completed.

i) To view the progress of a backup job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note If you do not see your backup job in the list, refresh the **Backup and Restore Job Sets** table.

j) If the backup fails during upload to the remote server: In the **Job Details** panel, just under the Status icon, click the **Upload backup** button to retry the upload.

Note Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path and so on). This is indicated by failure of the task **`uploadBackupToRemote`**). If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

Step 4 After a successful backup, shut down the Cisco Crosswork cluster by powering down the VMs hosting each node (start with the Hybrid VMs):

a) Log into the VMware vSphere Web Client.

b) In the **Navigator** pane, right-click the VM that you want to shut down.

c) Choose **Power** > **Power Off**.

d) Wait for the VM status to change to **Off**.

e) Wait for 30 seconds and repeat steps 4a to 4d for each of the remaining VMs.

Step 5 Move Cisco NSO into read-only mode to avoid any unintended updates to Cisco NSO during the upgrade.

Use the following command to move NSO to read-only mode:

```
ncs_cmd -c maapi_read_only
```

For more information, please refer to the documentation for Cisco NSO 5.4.2.

Install the Cisco Crosswork 4.1 Cluster

This is the third stage of the upgrade workflow. After the successful backup of Cisco Crosswork 4.0, proceed to install Cisco Crosswork 4.1 cluster.

Note The number of nodes installed in Cisco Crosswork 4.1 must be equal or more than the number of nodes in Cisco Crosswork 4.0.

Before you begin

- Make sure that your environment meets all the requirements specified under Cisco Crosswork Infrastructure Requirements, on page 5.

Step 1 Install Cisco Crosswork 4.1 cluster using any of the installation methods described in Install the Crosswork Cluster, on page 27.

Note During installation, Cisco Crosswork will create a special administrative ID (**virtual machine (VM) administrator**, with the username *cw-admin*, and the default password *cw-admin*). The administrative username is reserved and cannot be changed. The first time you log in using this administrative ID, you will be prompted to change the password. Data center administrators use this ID to log into and troubleshoot the Crosswork application VM. You will use it to verify that the VM has been properly set up.

Step 2 After the installation is completed, log into the Cisco Crosswork UI and check if all the nodes are up and running in the cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the details of the cluster such as resource utilization by node, the IP addresses in use, whether each node is a hybrid or worker, and so on.

Install Cisco Crosswork 4.1 Applications

This is the fourth stage of the upgrade workflow. After the successful installation of Cisco Crosswork 4.1 cluster, proceed to install Cisco Crosswork 4.1 applications.

Note You can only install 4.1 versions of the Cisco Crosswork applications that were backed up during Create Backup and Shut Down Cisco Crosswork 4.0, on page 100.

Step 1 Install Cisco Crosswork 4.1 applications using the steps described in Install Crosswork Applications, on page 95.

Step 2 After the applications are successfully installed, check the health of the Cisco Crosswork 4.1 cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Migrate the Cisco Crosswork 4.0 backup to Cisco Crosswork 4.1

This is the fifth stage of the upgrade workflow. After the successfully installing Cisco Crosswork 4.1 applications, proceed to migrate the backup of Cisco Crosswork 4.0 on Cisco Crosswork 4.1 cluster.

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of a secure SCP server.
- The name and path of the backup file created in Create Backup and Shut Down Cisco Crosswork 4.0, on page 100.
- User credentials with file read and write permissions to the directory.

Step 1 **Configure an SCP backup server:**

a) From the main menu, choose **Administration** > **Backup and Restore**.

b) Click **Destination** to display the **Edit Destination** dialog box.

c) Make the relevant entries in the fields provided.

Note In the **Remote Path** field, please provide the location of the backup created in Create Backup and Shut Down Cisco Crosswork 4.0, on page 100.

d) Click **Save** to confirm the backup server details.

Step 2 **Migrate the Cisco Crosswork 4.0 backup on the Cisco Crosswork 4.1 cluster:**

a) From the Cisco Crosswork main menu, choose **Administration** > **Backup and Restore**.

b) Click **Actions** > **Data Migration** to display the **Data Migration** dialog box with the destination server details prefilled.

c) Provide the name of the data migration backup (created in Create Backup and Shut Down Cisco Crosswork 4.0, on page 100) in the **Backup File Name** field.

d) If you want to perform the data migration backup despite any Cisco Crosswork application or microservice issues, check the **Force** check box.

e) Click **Start Migration** to start the data migration operation. Cisco Crosswork creates the corresponding data migration job set and adds it to the **Backup and Restore Job Sets** table. The Job Details panel reports the status of each backup step as it is completed.

Note If you do not see your job in the list, refresh the **Backup and Restore Job Sets** table.

f) To view the progress of a data migration job: Enter the job details (such as Status or Job Type) in the search fields in the **Backup and Restore Job Sets** table. Then click on the job set you want.

The **Job Details** panel displays information about the selected job set, such as the job Status, Job Type, and Start Time. If there's a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note Crosswork UI and Grafana monitoring might become temporarily unavailable during the data migration operation.

g) If the data migration fails in between, you need to restart the procedure from step 1.

Step 3 After the data migration is successfully completed, check the health of the Cisco Crosswork 4.1 cluster.

a) From the Cisco Crosswork main menu, choose **Administration** > **Crosswork Manager** > **Crosswork Summary**.

b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Upgrade to Cisco Crosswork Data Gateway 3.0

This is the final stage of the Crosswork 4.0 to Crosswork 4.1 upgrade workflow. Before you proceed, ensure that you have completed all the steps from the previous stages in the upgrade workflow.

Note This procedure is required only for a Cisco Crosswork Data Gateway Base VM upgrade. Upgrade of other components, such as collectors, is performed by Cisco Crosswork.

Cisco Crosswork Data Gateway functions as a passive device in the network. The Crosswork Data Gateway upgrade process consists of shutting down the Crosswork Data Gateway 2.0 VMs and replacing this with the Crosswork Data Gateway 3.0 VMs.

Pools and device mapping information are migrated to the 3.0 VMs by running the Migration Utility API:

https://<VIP>:30603/crosswork/inventory/v1/dg/vdg/migrate

The Migration Utilty API in DLM is an accumulative API. You can safely run it multiple times.

Step 1 Install new Cisco Crosswork Data Gateway 3.0 VMs with the same number and the same information (management interface importantly) as the Crosswork Data Gateway 2.0 VMs. Follow the steps in the Install Cisco Crosswork Data Gateway, on page 59.

Step 2 Ensure that the new Cisco Crosswork Data Gateway VMs have enrolled with Cisco Crosswork and have the Administration state **Up** and Operational state as **Not Ready**. See Cisco Crosswork Data Gateway Authentication and Enrollment, on page 90.

Step 3 Move Cisco NSO out of maintenance or read-only mode. For more information, see Related Documentation for 5.5.2.9.

```
ncs_cmd -c maapi_read_write
```

Step 4 (Optional) If you have onboarded a custom MIB package in Cisco Crosswork 4.0, upload the custom MIB package that you had downloaded (as instructed in Create Backup and Shut Down Cisco Crosswork 4.0, on page 100). For information on how to do this, see Section: Add a Custom Software Package in the *Cisco Crosswork Infrastructure 4.1 Applications and Administration Guide*. After uploading the custom MIB package, do the following checks:

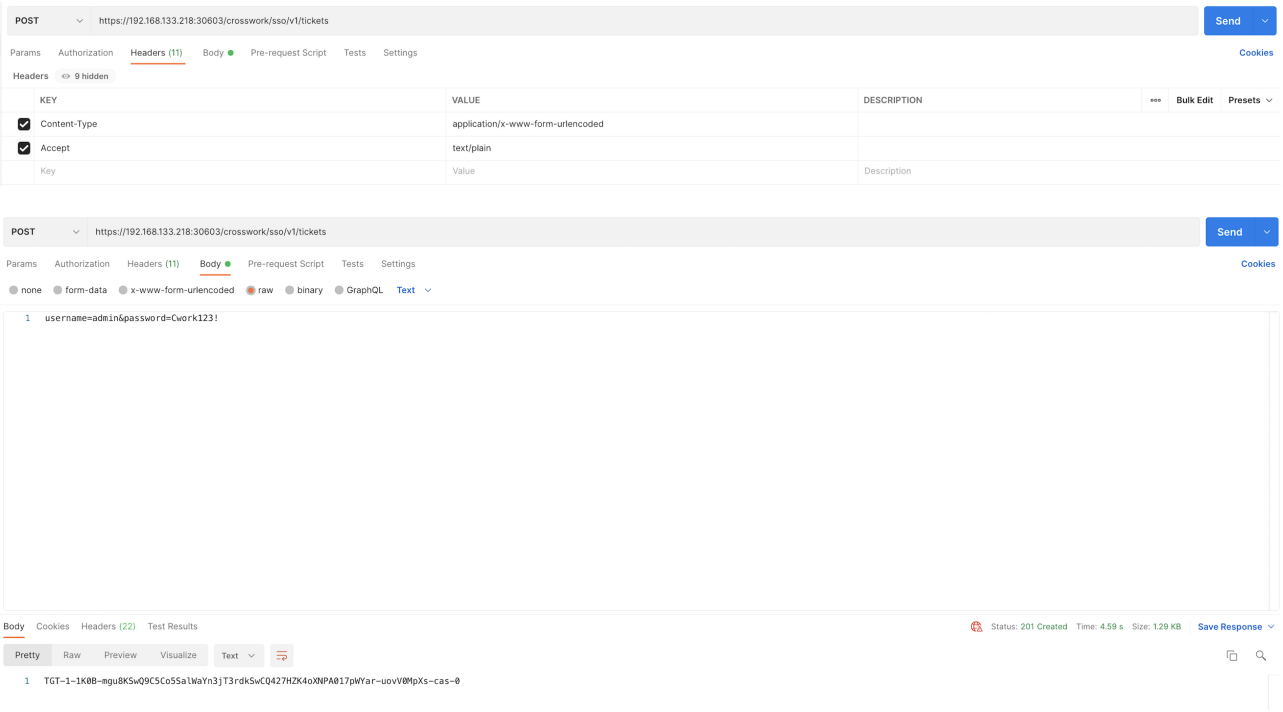
- Restart **robot-alerting**, **robot-fleet** and **pulse** micro-services.
- Disable all the KPIs which were using the custom MIB package.
- After the jobs are successfully disabled, enable all the KPIs that are using custom KPIs.

Step 5 **Fetch the JWT token to run the Migration Utility API.**

Note You can use any tool to perform the API calls. For the purpose of these instructions, we have used POSTMAN.

a) Run the following API to get the TGT.

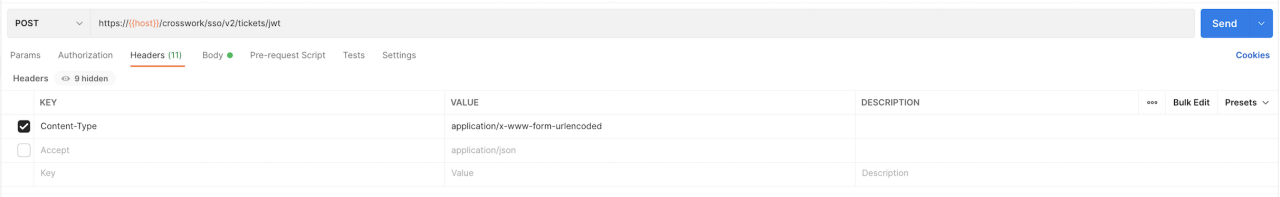
```
https://<VIP>:30603/crosswork/sso/v1/tickets


HTTP method: POST
Headers:
    Content-Type: application/x-www-form-urlencoded
    Accept: text/plain
Body:
    username=<Cisco Crosswork UI login username>
    password-<Cisco Crosswork UI login password>
```

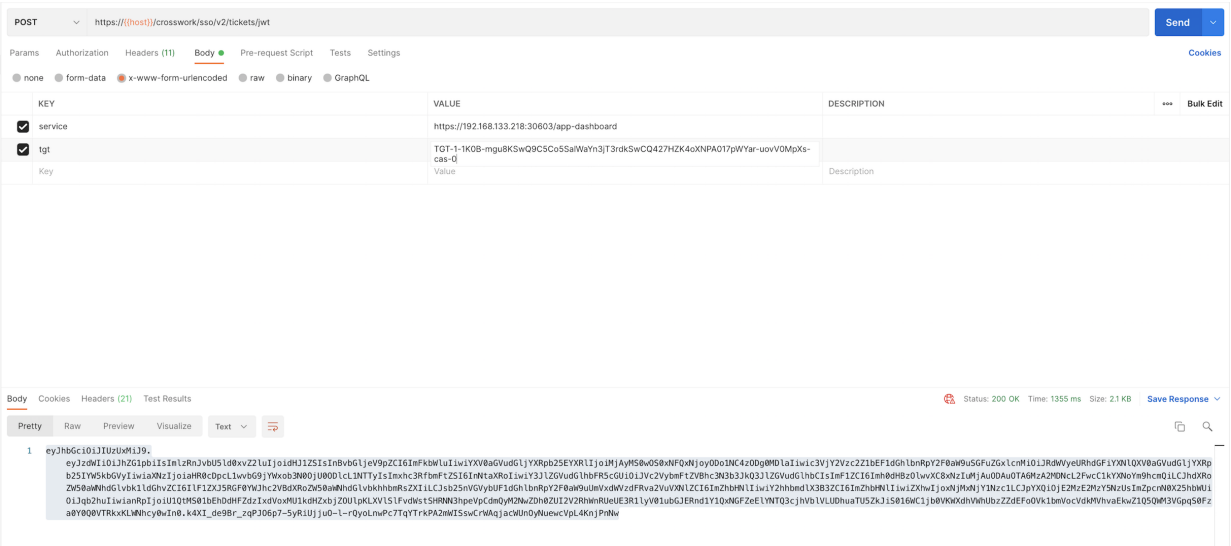


b) Get the JWT after getting the TGT.

```
https://<VIP>:30603/crosswork/sso/v2/tickets/jwt
```

```
HTTP method:POST
Headers:
    Content-Type: application/x-www-form-urlencoded
    Accept: text/plain
Body:
    service=https://<VIP>:30603/app-dashboard
    tgt=<TGT from step a>
```

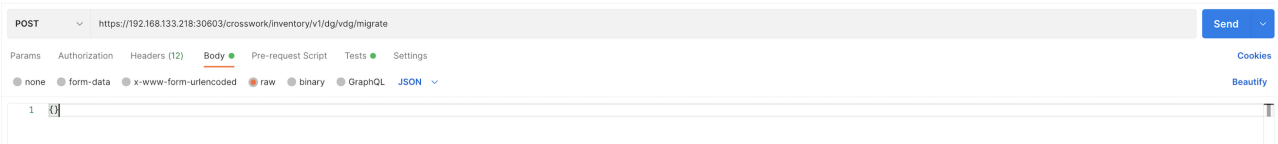


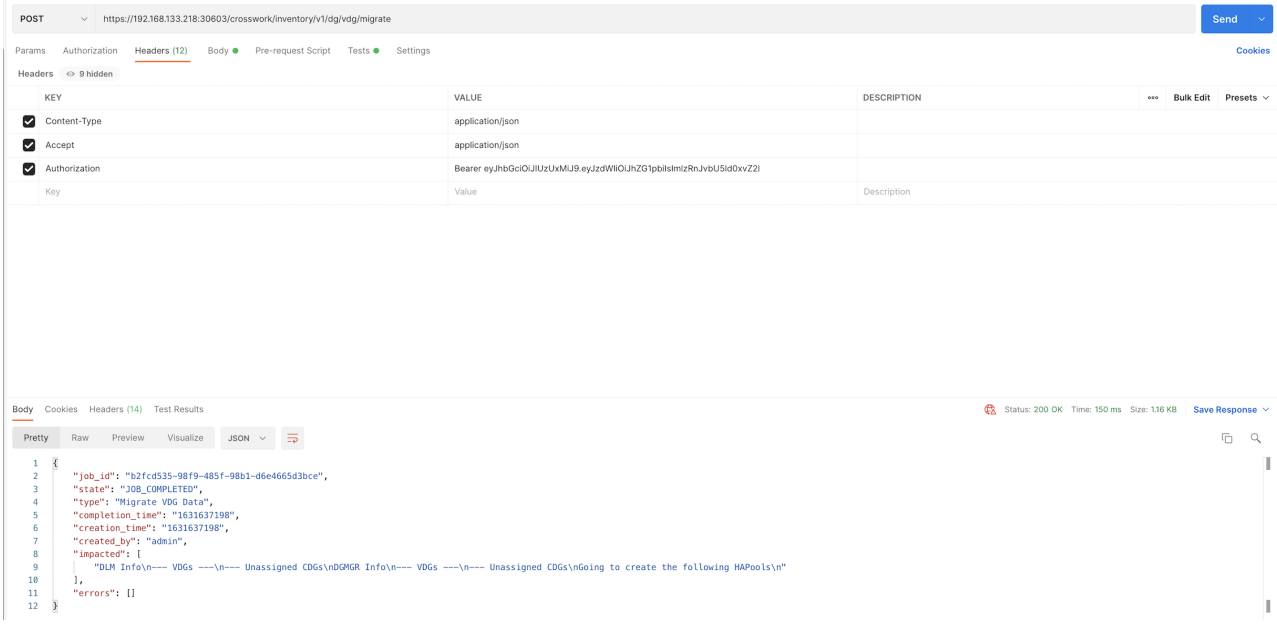


Step 6 Create Crosswork Data Gateway pools by executing the Migration utility API.

API: `https://<VIP>:30603/crosswork/inventory/v1/dg/vdg/migrate`

```
HTTP method:POST
Headers:
    Authorization:Bearer <JWT from step 4b>
    Content-Type: application/json
Body:
{} //empty json needs to be sent
```





Note The API response will always have the status code as 200. The API response body contains a full report with the following details:

- Crosswork Data Gateway Pools that have been created successfully.
- Crosswork Data Gateway Pools that have not been created and the reason they have not been created.
- Crosswork Data Gateway Pools that already exist and are ready for device migration.

Copy the report that is returned inside the Migration Utility API. This report is useful during troubleshooting in case there are issues.

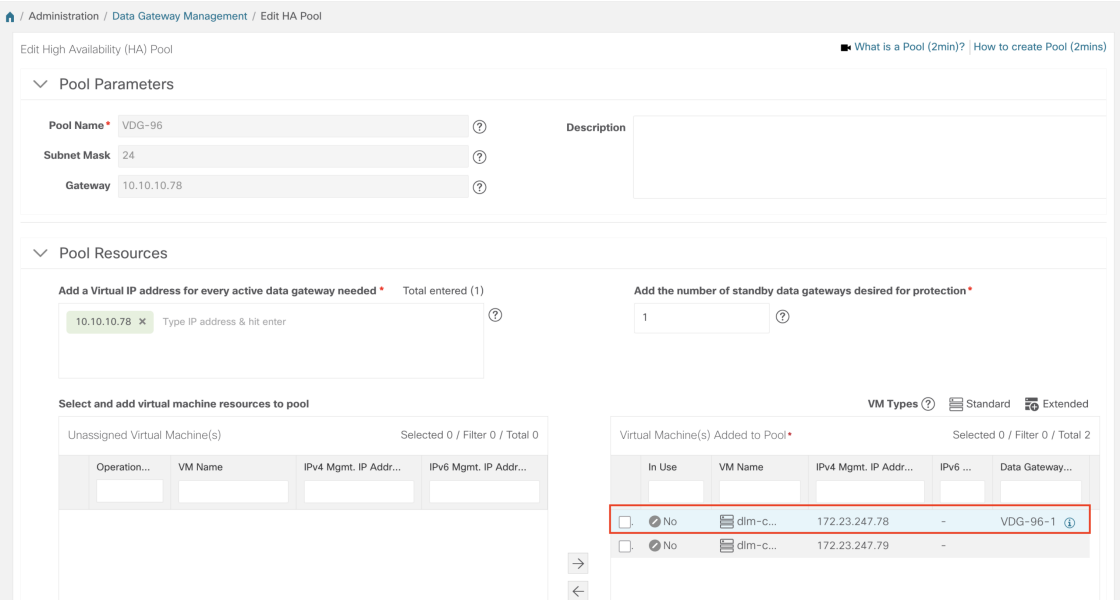
Step 7 **Verify that all Crosswork Data Gateway Pools have been created.**

a) Navigate to **Administration** > **Data Gateway Management** in Cisco Crosswork UI.

b) Verify that all the Crosswork Data Gateway Pools from Cisco Crosswork 4.0, are listed under the **Data Gateways** tab.

c) In the **Pools** tab, edit each Crosswork Data Gateway pool to verify that the active Crosswork Data Gateway is same as one that you noted in Cisco Crosswork 4.0.

For example, the Crosswork Data Gateway pool in the following image contains two VMs, where the active VM is 172.23.247.78



Note If there issues such as, Crosswork Data Gateway pool has not been created or a different VM is selected as active instead of the VM that was active in Cisco Crosswork 4.0 deployment, check for the issue in the API report generated in response to the API call. Refer to the Section: Troubleshoot Crosswork Data Gateway Upgrade Issues, on page 110 for troubleshooting and suggested workarounds for the issue.

Step 8 **Attach devices to Crosswork Data Gateways 3.0 using Migration Utility API**

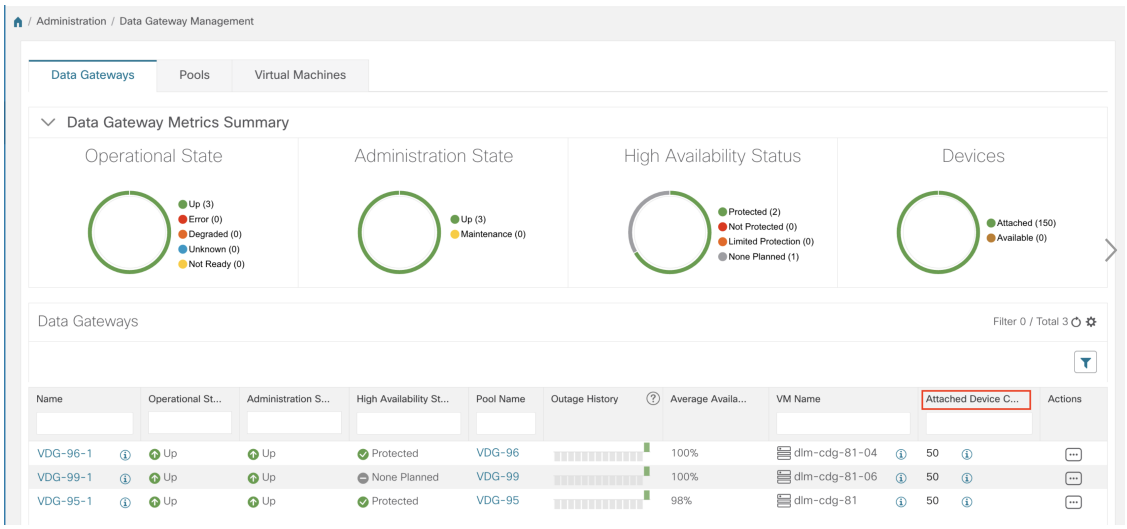
Map the devices from Crosswork Data Gateways 2.0 to the newly created Crosswork Data Gateways 3.0 in Cisco Crosswork 4.1 by running the Migration Utility API (as explained earlier in Step 5).

Running the Migration Utility API this time validates the Crosswork Data Gateways and attaches all devices to the corresponding Crosswork Data Gateways from Cisco Crosswork 4.0.

Step 9 **Verify that devices are attached to the Crosswork Data Gateways 3.0 in the Cisco Crosswork 4.1 UI.**

a) Navigate to the **Administration** > **Data Gateway Management** page.

b) Check the **Attached Device Count** of the Crosswork Data Gateway.



Note In case of issues (such as a missing Crosswork Data Gateway pool or a pool that does not have any devices attached to it), see Section: Troubleshoot Crosswork Data Gateway Upgrade Issues, on page 110.

Troubleshoot Crosswork Data Gateway Upgrade Issues

The following table lists common problems that might be experienced when upgrading the Crosswork Data Gateway, and provides approaches to identifying the source of the problem and solving it.

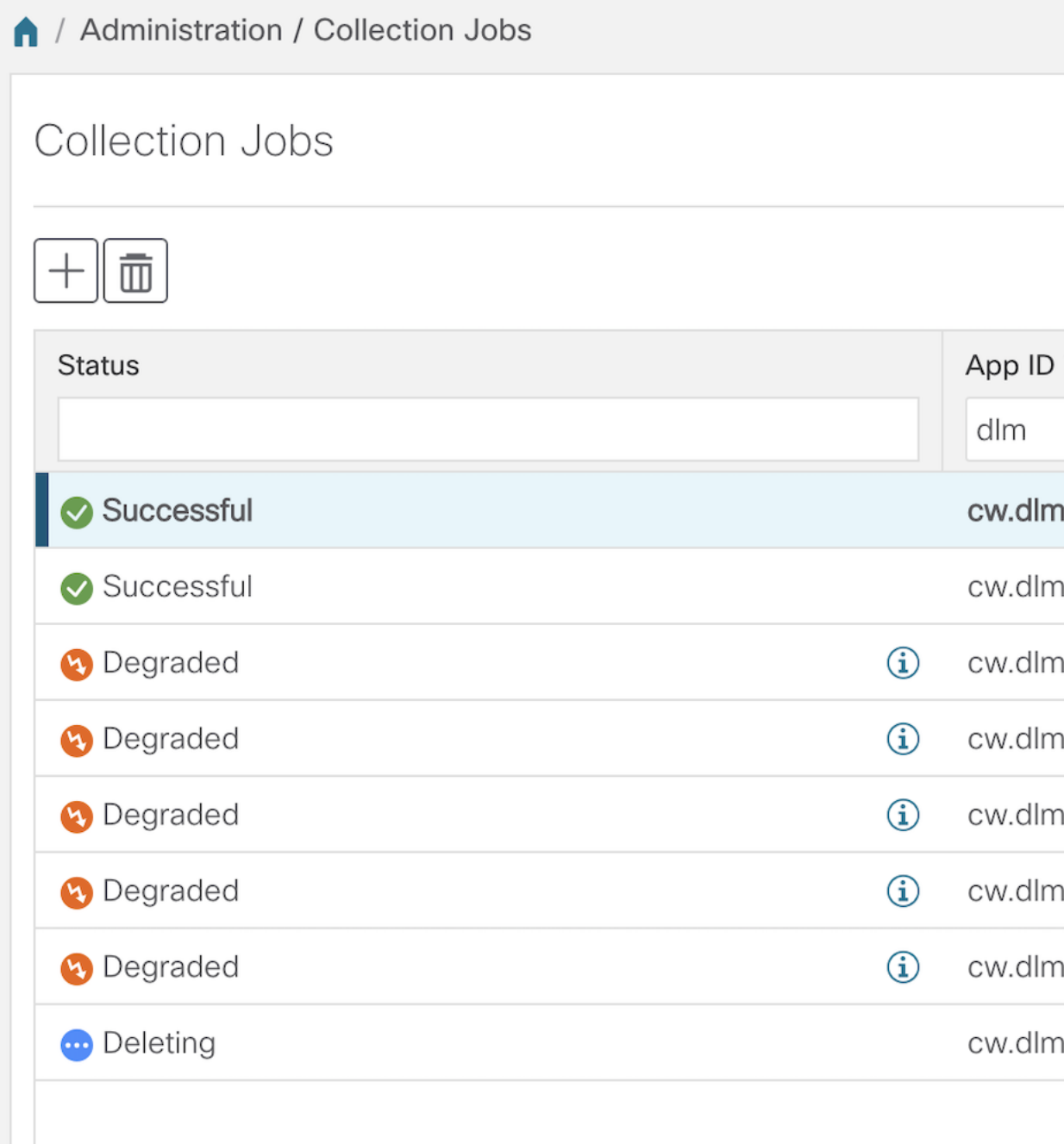
Issue	Symptom	Recommended Action
1. Forgot to enroll one or more Crosswork Data Gateway 3.0 VMs.	One of the Crosswork Data Gateway pools has not been created.	Enroll the missing Crosswork Data Gateways and repeat the data migration steps in (Step 5 onwards) in the section Upgrade to Cisco Crosswork Data Gateway 3.0, on page 105.
2. Some of the Crosswork Data Gateway VMs were in **Error** or **Degraded** state when executing the migration procedure	One of the Crosswork Data Gateway pools has not been created.	Wait for the Crosswork Data Gateway VMs to have the state as **Up** or **Not Ready** state. Take action if necessary to get the VM to **Not Ready** state. Repeat the Crosswork Data Gateway data migration steps as described (Step 5 onwards) in the section Upgrade to Cisco Crosswork Data Gateway 3.0, on page 105.

Issue	Symptom	Recommended Action
3. Crosswork Data Gateway pool has been created with the correct VMs, but a different VM is selected as active from the one that was active in the Cisco Crosswork 4.0 deployment.	A different VM is selected as active in the Crosswork Data Gateway pool.	**1.** Edit the Crosswork Data Gateway Pool to remove all VMs except the one that should be active per the Cisco Crosswork 4.0 deployment and save the pool. **2.** Edit the Crosswork Data Gateway pool again to add back all the VMs you removed from the pool and save the pool.
4. Crosswork Data Gateway does not have any devices attached to it even after running the VDG migration utility multiple times.	No devices are attached to the Crosswork Data Gateway.	**1.** Edit the Crosswork Data Gateway Pool to remove any VMs that were defined as Standy in Cisco Crosswork 4.0 deployment and save the pool. **2.** Repeat Step 6 and Step 7 as described in the section Upgrade to Cisco Crosswork Data Gateway 3.0, on page 105. **3.** Edit the Crosswork Data Gateway pool and add back the standby VMs to the pool and save the pool.

Post-upgrade Checklist

After the upgrade to Cisco Crosswork 4.1 is completed, check the health of the new cluster. If your cluster is healthy, perform the following activities:

- Navigate to **Administration** > **Collection Jobs** in Cisco Crosswork 4.1 UI and delete the duplicate system jobs.



- Verify that the collection jobs are running on the Crosswork Data Gateway 3.0 VMs in the **Administration** > **Collection Jobs** page. At this point, you can delete the 2.0 VMs.
- Verify the restored AAA data by logging in using default credentials, and configure custom user roles (Read-Write/Read) in Cisco Crosswork 4.1.
- (Optional) Based on your network requirements, download the relevant map files from cisco.com and re-upload them to Cisco Crosswork 4.1.

- (Optional) If any NSO device onboarding policy was set in Cisco Crosswork 4.0, you must update the policy with new Network Element Drivers (NED) on the NSO.
- (Optional) Re-apply any third-party device configurations (used in Cisco Crosswork 4.0) to Cisco Crosswork 4.1.
- If you are using Crosswork Optimization Engine, perform the following actions:
  - Upgrade the software versions in your devices as per the supported Cisco IOS XE/XR versions documented in the Cisco Crosswork Optimization Engine Release Notes.
  - Verify feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) using the instructions in "Upgrade Crosswork Optimization Engine Feature Packs" in the latest Cisco Crosswork Optimization Engine Release Notes.

If you encounter errors in any of the above activities, please contact the Cisco Customer Experience team.

Update a Crosswork Application (standalone activity)

This section explains how to independently update a Crosswork application from the Cisco Crosswork UI in case of minor updates or patch releases. This procedure is not part of the upgrade workflow discussed in the earlier sections.

Before you begin, ensure that you:

- Take a backup of your data (using the backup/restore functionality) before any critical upgrade.
- Download the latest version of the Crosswork APPlication file (CAPP) from cisco.com to your local machine.

Note Crosswork does not support the downgrade operation of a CAPP file. However, if you want to go back to an older application version, you can uninstall the application and install the older version of the application. In case of a downgrade, you are advised to take a backup of your data prior to the operation.

Step 1 Click on **Administration** > **Crosswork Management**, and select the **Application Management** tab.

The Crosswork Platform Infrastructure and any applications that are added are displayed here as tiles.

Step 2 Click on the **Add File (.tar.gz)** option to add the application CAPP file that you had downloaded.

Step 3 In the Add File dialog box, enter the relevant information and click **Add**.

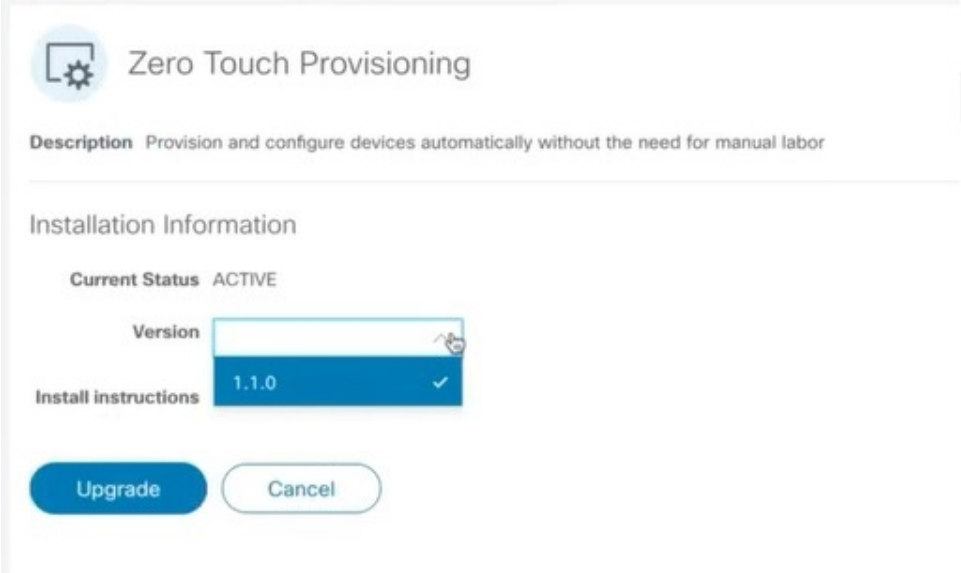
Once the CAPP file is added, you can observe the existing application tile (in this example, Zero Touch Provisioning) displaying an upgrade prompt.

Step 4 To upgrade, click the Upgrade prompt and the new version of the application is installed.

The upgrade progress is displayed on the application tile.

Step 5 Alternately, click ··· on the tile, and select the **Upgrade** option from the drop down list.

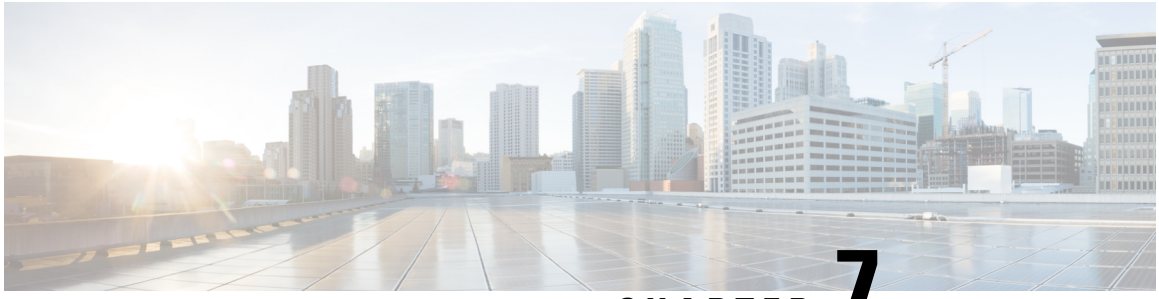
In the Upgrade screen, select the new version that you want to upgrade to, and click **Upgrade**.



Step 6 (Optional) Click on **Job History** to see the progress of the upgrade operation.

Note During an upgrade operation, typically only the components that have changed between the existing CAPP file and the new CAPP file are installed, as the new version may continue to use the most of the resources of the older version. This ensures a quick operation that happens without disruption to the current system and session.

Note During an upgrade, the application that is being updated will be unavailable until the update is completed. During this time, any other users using the application will be notified via an alarm about the upgrade.



CHAPTER 7

Uninstall Cisco Crosswork

This chapter contains the following topics:

Uninstall the Crosswork Cluster

This section explains the various methods to uninstall the Cisco Crosswork cluster.

Delete the VM using the Cluster Installer

In case of a failed installation, the cluster installer tool is used to cleanup or delete any previously created VMs based on the cluster-state. this is a critical activity during failed deployments. Any changes made to the VM settings or the data center host requires a cleanup operation before redeployment.

Note The cleanup procedure is similar for both vCenter and CSP deployments, with the only exception being the addition of "-t csp" option when running a CSP cleanup.

Note The installer cleanup option will delete the cluster deployment based on the inventory in `/data` directory.

Step 1 Enter the directory storing the deployment info.

For example, `_cd ~/cw-cluster`.

Step 2 Run the container on the host.

```
docker run --rm -it -v `pwd`:/data <cw-installer docker container>
```

Note Add the "-t csp" option when running a CSP cleanup.

Step 3 Edit the copy of the template file (for example, `v4.tfvars`) in a text editor, adding the data center access parameters. Remaining parameters can be provided with dummy values, or entered on the command line during the execution of the operation.

Step 4 Run the `_cw-installer.sh install_` script with the clean directive along with the deployment manifest using the `-m` flag. For example:

```
./cw-installer.sh clean -m /data/deployment.tfvars
```

Step 5 Enter "yes" when prompted to confirm the operation.

Step 6 (Optional) In addition to removing the VMs, adding the `-o` option to the clean directive will also remove the Cisco Crosswork image template from the data center.

Example:

```
./cw-installer.sh clean -m/data/deployment.tfvars -o
```

Step 7 (Optional) To clean the cluster quickly (without verification), users can run the installer using the following command:

```
docker run --rm -it -v `pwd`:/data <cw installer docker image> -exec './cw-installer.sh clean -m
/data/deployment.tfvars'
```

Delete the VM using the vSphere UI

This section explains the procedure to delete a VM from vCenter. This procedure is used to delete any Cisco Crosswork application VM.

Note

- Be aware that this procedure deletes all your app data.
- **If you want to delete Crosswork Data Gateway only**, ensure you have done the following:
  - Detach the devices from the Crosswork Data Gateway VM you want to delete. The procedure to detach devices from a Crosswork Data Gateway is described in the Section: *Delete Cisco Crosswork Data Gateway VM from Cisco Crosswork* in *Cisco Crosswork Infrastructure 4.0 and Applications Administration Guide*.
  - Delete the Crosswork Data Gateway VM from Cisco Crosswork as described in Delete Crosswork Data Gateway VM from Cisco Crosswork, on page 119.

Step 1 Log into the VMware vSphere Web Client.

Step 2 In the **Navigator** pane, right-click the app VM that you want to remove and choose **Power** > **Power Off**.

Step 3 Once the VM is powered off, right-click the VM again and choose **Delete from Disk**.

The VM is deleted.

Uninstall Crosswork Data Gateway

This section explains the methods to remove Cisco Crosswork Data Gateway.

- Delete Crosswork Data Gateway VM from Cisco Crosswork, on page 119
- Delete Crosswork Data Gateway Service from Cisco CSP, on page 120

Delete Crosswork Data Gateway VM from Cisco Crosswork

Before you begin

The Crosswork Data Gateway VM you want to delete must be in maintenance mode.

Step 1 Log into Cisco Crosswork UI.

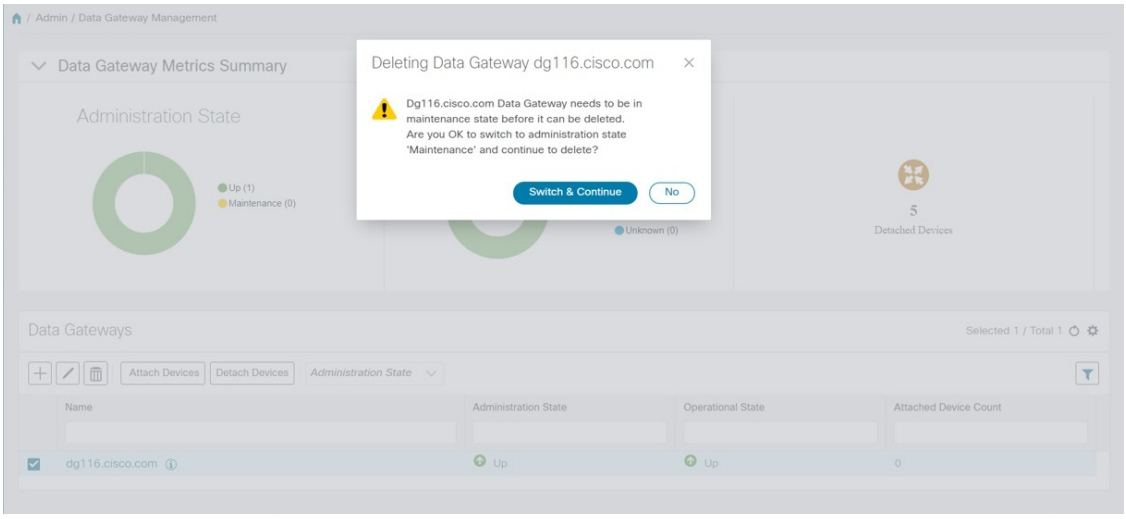
Step 2 From the navigation panel, select **Administration** > **Data Gateway Management**.

Click on the **Virtual Machines** tab.

Step 3 In the **Virtual Machines** list, find the Crosswork Data Gateway VM you want to delete and click ⋯ under **Actions** column.

Click **Delete**.

Step 4 If the Crosswork Data Gateway VM is not in maintenance state, Cisco Crosswork prompts you to switch it to maintenance state. Click **Switch to maintenance & continue**.



The Crosswork Data Gateway VM is deleted.

Delete Crosswork Data Gateway Service from Cisco CSP

Follow the steps to delete the Crosswork Data Gateway Service from Cisco CSP:

Before you begin

Ensure that you have deleted the Crosswork Data Gateway from Crosswork Cloud as described in the *Section: Delete Crosswork Data Gateways* of the respective Crosswork Cloud application user guide.

Step 1 Log into your Cisco CSP.

Step 2 Go to **Configuration** > **Services**.

The **Service** table shows the current status of the services.

Step 3 Find your service instance in the **Service Name** column and click **Delete** under the **Action** column.

Uninstall Crosswork Applications

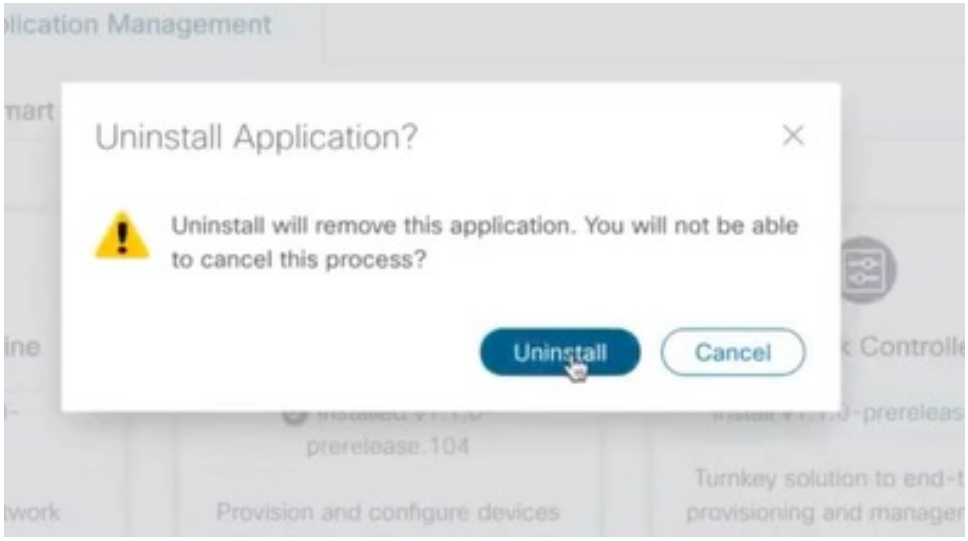
This section explains how to uninstall an application in the Crosswork UI. The **Uninstall** option removes the application, application-specific menus and associated data.

Step 1 Click on **Admin** > **Crosswork Management**, and select the **Application Management** tab.

The Crosswork Platform Infrastructure and any applications that are added are displayed here as tiles.

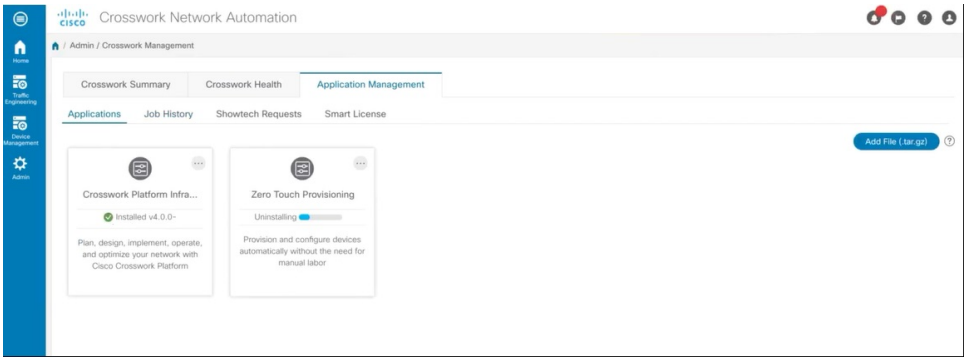
Step 2 Click ··· on the application tile that you want to uninstall, and select the **Uninstall** option from the drop down list.

A pop-up is displayed to confirm the action.



Step 3 Click **Uninstall** to confirm.

The selected application is uninstalled and the application tile is modified to reflect the same.



You can also view the progress of uninstallation in the Job History window (**Application Management** > **Job History**). If the uninstall fails, you can reattempt using the relevant options in the Job History window.

Note The uninstall operation does not remove the CAPP file from the repository. The CAPP file will remain visible in the Crosswork UI, in case user wants to install in the future.

Note

APPENDIX A

Manifest template for Cluster deployment

This appendix contains the following topics:

Sample manifest template for VMware vCenter

The following example might be used for a lab as it deploys the 3 hybrid nodes with two of the VMs on the same host and the third VM on a second host using the small configuration.

Note In case you are using resource pools, please note that individual ESXi host targetting is not allowed and vCenter is responsible for assigning the VM to a host in the resource pool. If vCenter is not configured with resource pools, then the exact ESXi host path must be passed.

```
*******
vCenter Example
********

//#********* Crosswork Cluster Data *********#

Cw_VM_Image = ""
ClusterIPStack = "IPv4"
ManagementVIP = "17.25.87.94"
ManagementIPNetmask = "255.255.255.192"
ManagementIPGateway = "17.25.87.65"
DataVIP = "192.168.123.94"
DataIPNetmask = "255.255.255.0"
DataIPGateway = "0.0.0.0"
DNS = "17.70.168.183"
DomainName = "somedomain.com"
CWPassword = "AStr0ngPa33!"
VMSize = "Small"
NTP = "ntp.com"
BackupMinPercent = 50
ThinProvisioned = true
ManagerDataFsSize = 450
WorkerDataFsSize = 450

#********* Crosswork VM Data Map *********
```

```
CwVMs = {
"0" = {
VMName = "vm1",
ManagementIPAddress = "17.25.87.82",
DataIPAddress = "192.168.123.82",
NodeType = "Hybrid"
},
"1" = {
VMName = "vm2",
ManagementIPAddress = "17.25.87.83",
DataIPAddress = "192.168.123.83",
NodeType = "Hybrid"
},
"2" = {
VMName = "vm3",
ManagementIPAddress = "17.25.87.84",
DataIPAddress = "192.168.123.84",
NodeType = "Hybrid"
}
}


#********* vCenter Resource Data with Cw VM assignment *********

VcenterDC = {
VcenterAddress = "17.25.87.90",
VcenterUser = "administrator@vsphere.local",
VcenterPassword = "vcenterPass",
DCname = "dc-cr",
MgmtNetworkName = "VM Network",
DataNetworkName = "DPortGroup10",
DCfolder = "",
VMs = [{
HostedCwVMs = ["0","1"],
Host = "17.25.87.93",
Datastore = "datastore3",
HSDatastore = "ssddatastore",
},
{
HostedCwVMs = ["2"],
Host = "17.25.87.92",
Datastore = "datastore2"
HSDatastore = "ssddatastore",
}
]
}
```

Sample manifest template for Cisco CSP

The following example might be used for a lab as it deploys the 3 hybrid nodes with two of the VMs on the same host and the third VM on a second host using the small configuration.

```
//*******
//CSP Example
//********

//#********* Crosswork Cluster Data  *********#

  ClusterName = "day0-cluster"
  Cw_VM_Image           = ""
  ManagementVIP     = "17.25.87.94"
```

```
  ManagementIPNetmask = "255.255.255.192"
  ManagementIPGateway = "17.25.87.65"
  DataVIP           = "192.168.123.94"
  DataIPNetmask       = "255.255.255.0"
  DataIPGateway       = "0.0.0.0"
  DNS                 = "17.70.168.183"
  DomainName            = "somedomain.com"
  CWPassword            = "AStr0ngPa33!"
  VMSize                = "Small"
  NTP                   = "ntp.com"
  ClusterIPStack        = "IPv4"
  BackupMinPercent      = 50
  ThinProvisioned     = false
  ManagerDataFsSize = 450
  WorkerDataFsSize  = 450

  RamDiskSize = 0

#********* Crosswork VM Data Map *********

CwVMs = {
  "0" = {
    VMName                = "vm1",
    ManagementIPAddress = "17.25.87.82",
    DataIPAddress       = "192.168.123.82",
    NodeType               = "Hybrid"
  },
  "1" = {
    VMName                = "vm2",
    ManagementIPAddress = "17.25.87.83",
    DataIPAddress       = "192.168.123.83",
    NodeType               = "Hybrid"
  },
  "2" = {
    VMName                = "vm3",
    ManagementIPAddress = "17.25.87.84",
    DataIPAddress       = "192.168.123.84",
    NodeType               = "Hybrid"
  }
}


#********* CSP Resource Data with Cw VM assignment *********

CSPCluster = {
  hosts = [{
    name = "host1",
    protocol = "https",
    server = "10.0.0.102",
    username = "admin",
    password = "Spass",
    insecure = true
  },
  {
    name = "host2",
    protocol = "https",
    server = "10.0.0.108",
    username = "admin",
    password = "Spass",
    insecure = true
  }]
  VMs = [{
    HostedCwVMs = ["0","1"],
    Host = "host1",
```

```
    MgmtNetworkName = "Eth1-1",
    DataNetworkName = "Eth1-2"
  },
    {
      HostedCwVMs = ["2"],
      Host = "host2",
      MgmtNetworkName = "Eth0-1",
      DataNetworkName = "Eth9-1"
    }
  ]
}
```

Set seed node explicitly

The cluster installer tool, by default, selects the first VM (VM 0) as the seed node. You can set the seed node explicitly by adding the following section to the manifest template (.tfvars file) indicating the unique key of the seed node.

Note You are recommended not to modify the default seed node value unless advised to do so by the Cisco Customer Experience team.

```
cluster_settings = {
#Default Minimum number of nodes in inventory
    min_inventory     = 3
#Default Max number of nodes in inventory
    max_inventory     = 9
#Default Min number of manager nodes
    min_mngr_nodes    = 2
#Default Max number of manager nodes
    max_mngr_nodes    = 3
#Default seed node key name
    default_seed_node = "0"
}
```