Cisco Crosswork Infrastructure 4.3 and Applications Installation Guide

First Published: 2022-08-15

Last Modified: 2023-02-03

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CONTENTS

CHAPTER 1

CHAPTER 2

CHAPTER 3

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 other components that integrate with Cisco Crosswork (see Integrated Components, on page 2), such as Cisco NSO or Cisco WAE, 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. The total number of Hybrid and Worker nodes varies based on the size of the network and the applications being run work with Cisco Crosswork to scale the solution correctly for your needs.

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. 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 Customer Experience 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 and/or to discover devices in the network.

Cisco Crosswork can also integrate with other providers (such as Cisco WAE, Syslog and Alert) and servers (TACACS+ and LDAP). For more information, see the "Device Management" chapter in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*.

Cisco Crosswork Product Portfolio

Cisco Crosswork Infrastructure provides a flexible platform to deploy different products (Crosswork and non-Crosswork) where each product is downloaded and added to the platform.

The list of Crosswork products are:

- **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.

- **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.

Crosswork Network Controller applications are bundled as **Essentials** and **Advantage** packages.

Table 1: Crosswork Network Controller Packages

Crosswork Network Controller package	Contents
Essentials package	Crosswork Optimization Engine Crosswork Active Topology
Advantage package	Crosswork Optimization Engine Crosswork Active Topology Cisco Crosswork Service Health Cisco Crosswork Health Insights Cisco Crosswork Change Automation Crosswork Zero Touch Provisioning Element Management System (EMS) Services

Aside from Crosswork products, Crosswork Infrastructure supports deployment of the following non-Crosswork application:

- The **Cisco Evolved Programmable Network Manager (EPNM)** is designed to provide simplified, converged, end-to-end lifecycle management for carrier-grade networks. It provides device management, network service provisioning, and network assurance across core, edge, aggregation, and access networks consisting of a wide range of Cisco device families.

For information on the installation and configuration requirements of Cisco Crosswork products, see Installation Dependencies for Cisco Crosswork Products, on page 23.

Resource Allocation

Resource requirements for a cluster and each cluster VM node vary based on the Crosswork components that you use and the deployment size you select. The following tables contain an estimation of resources needed for each scenario:

Table 2: Cluster Requirements

Deployment Size	Use Case	Number of Nodes
Small	Lab only	3 Hybrid nodes
Large	Crosswork Network Controller Essentials package	3 Hybrid nodes + 1 Worker node (to ensure VM resiliency) You can add more Worker nodes as needed.
	Crosswork Network Controller Advantage package[1]	3 Hybrid nodes + 2 Worker nodes (to ensure VM resiliency) You can add more Worker nodes as needed.
Extra Large	Evolved Programmable Network Manager (EPNM)	3 Hybrid nodes + 2 Worker nodes (to ensure VM resiliency) You can add more Worker nodes as needed. **Note** Use of other Crosswork applications with EPNM is NOT currently supported.

[1] The cluster resource estimation is under the assumption that you are using all the applications in the Crosswork Network Controller Advantage package.

Note A cluster with only 3 Hybrid VM nodes (without any Worker VM nodes) is NOT resilient. If one of the VM fails, it will certainly result in an impaired system performance, as the remaining 2 VMs will not be able to support all the pods being migrated from the failed VM.

Table 3: Resource Footprint per VM node

Component	vCPU	Memory (RAM)	Network Interface Controller (NIC)	Storage
Crosswork Infrastructure	12	96 GB	10 Gbps	1 TB
CDG Standard	12	48 GB	10 Gbps	60 GB
CDG Extended	20	112 GB	10 Gbps	560 GB
NSO (Large)	24	132 GB	10 Gbps	1 TB
NSO (Small) [below 1k devices]	8	64 GB	10 Gbps	250 GB
SR-PCE	8	64 GB	10 Gbps	45 GB

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 4.3 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 standard 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. Please consult with your Cisco Customer Experience team for guidance on your deployment to best meet your needs.

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 needed to operate other integrated components or applications (such as Cisco NSO, WAE, or EPNM) are not addressed in this document. Please refer to the respective install documentation of those components for more details.

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 46.
- 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). As Cisco Crosswork cluster nodes place high demands on the VMs, you must not oversubscribe CPU or memory resources on the machines hosting the nodes.

- VMware Data Center Requirements, on page 8
- CSP Data Center Requirements, on page 9

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.

Note A single pair of network names is required for these networks to be used across all the physical host machines hosting the Crosswork VMs. The same network names must be used and configured on all the ESXi host machines.

- 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 (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 data center 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 requirements for each VM host.

The data center host platform (**VMware vCenter** or **Cisco CSP**) has to accommodate 3 Hybrid VMs (aside from any additional Worker nodes) of the following minimum configuration:

Table 4: CPU/Memory/Storage Profiles (per VM)

Deployment Size	Number of Nodes	vCPUs/CPU Cores	Memory	Storage	Minimum Clock Reservation
Small (for lab deployments only)	3 Hybrid nodes	8	48 GB RAM + (optional) 2 GB RAM disk	1 TB **Note** 10 GB (approximately) of additional storage is required for the Crosswork OVA (in **vCenter**), OR the Crosswork QCOW2 image on each CSP node (in **CSP**).	12 GHz
Large	**Essentials package:** 3 Hybrid nodes + 1 Worker node (to ensure VM resiliency) **Advantage package:** 3 Hybrid nodes + 2 Worker nodes (to ensure VM resiliency) You can add more Worker nodes as needed.	12	96 GB RAM		18 GHz
Extra Large (for EPNM only)	3 Hybrid nodes + 2 Worker nodes (to ensure VM resiliency) You can add more Worker nodes as needed. **Note** Use of other Crosswork applications with EPNM is NOT currently supported.	24	128 GB RAM		32 GHz

Note For assistance in adjusting VM Memory and CPU configuration post installation, please 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.

The table below explains the network requirements per VM host:

Table 5: Network Requirements (per VM)

Requirement	Description
Network Connections	For production deployments, we recommend that you use dual interfaces, one for the Management network and one for the Data network. For optimal performance, the Management and Data networks should use links configured at a minimum of 10 Gbps.
IP Addresses	2 IP subnets, one for the Management network and one for Data network, with one IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and one additional IP address to be used as the Virtual IP (VIP) address. A 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.

Requirement	Description
NTP Servers	The IPv4 or IPv6 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize the Crosswork application VM clock, devices, clients, and servers across your network. • Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached. • The ESXi hosts that will run the Crosswork application and Crosswork Data Gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors.
DNS Servers	The IPv4 or IPv6 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network. • Ensure that the DNS servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.
DNS Search Domain	The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.

Important Notes

- Cisco Crosswork Infrastructure and applications are built to run as a distributed collection of containers managed by Kubernetes. The number of containers varies as applications are added or deleted.
- Dual stack configuration is not supported in Crosswork Platform Infrastructure. Therefore, **all** addresses for the environment must be either IPv4 or IPv6.

IP Address Restrictions

Crosswork cluster uses the following IP ranges for internal communications. This cannot be changed. As a result, these subnets cannot be used for devices or other purposes within your network.

You are recommended to isolate your Crosswork cluster to ensure all the communications stay within the cluster. Please also ensure that address spaces do not overlap for any of the external integration points (e.g. connections to devices, connections to external servers that Crosswork is sending data to, connections to the NSO server, etc.).

Note This is applicable for cluster installation and for adding a static route.

Table 6: Protected IP Subnets

IP Type	Subnet	Remarks
IPv4	172.17.0.0/16	Docker Subnet (Infrastructure)
	10.244.0.0/16	Pod Subnet (Infrastructure)
	10.96.0.0/16	Service Subnet (Infrastructure)
	169.254.0.0/16	Link local address block
	127.0.0.0/8	Loopback address
	192.88.99.0/24	Reserved, previously used for relay servers to do IPv6 over IPv4
	240.0.0.0/4	Reserved for future use (previously class E block)
	224.0.0.0/4	MCAST-TEST-NET
	0.0.0.0/8	Current network, valid as source address only
IPv6	2001:db8:1::/64	Docker Subnet (Infrastructure)
	fdfb:85ef:26ff::/48	Pod Subnet (Infrastructure)
	fd08:2eef:c2ee::/110	Service Subnet (Infrastructure)
	::1/128	Loopback address
	fe80::/10	Link local
	ff00::/8	IPv6 Multicast
	2002::/16	Reserved, previously used for relay servers to do IPv6 over IPv4
	2001:0000::/32	Terredo tunnel and relay
	2001:20::/28	Used by ORCHID and not IPv6 routable
	100::/64	Discard prefix, used in specific use-cases not applicable to Crosswork Zero Touch Provisioning
	::/128	Unspecified address, cannot be assigned to hosts
	::ffff:0:0/96	IPv4 mapped addresses
	::ffff:0:0:0/96	IPv4 translated addresses

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 7: 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.
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.

Port	Protocol	Usage
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 8: 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

To access the Crosswork UI after installing the infrastructure, we recommend using either of the browsers which have been validated:

Table 9: 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 4.3 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
- Mandatory deployment type for Crosswork Data Gateway, on page 16

Mandatory deployment type for Crosswork Data Gateway

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

1. **On-Premise Standard** (default): Collectors only.
2. **On-Premise Extended**: Collectors and offload services.
3. **On-Premise Standard with Extra Resources**: Collectors and additional resources.

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 all of the Crosswork Data Gateways in your environment must be deployed in the Extended profile.

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

Table 10: 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)	On-Premise Standard
Crosswork Optimization Engine	On-Premise Standard
Crosswork Change Automation	On-Premise Extended
Crosswork Health Insights	On-Premise Extended
Crosswork Zero Touch Provisioning	On-Premise Standard
Crosswork Service Health (Automated Assurance)	On-Premise Extended
Cisco Evolved Programmable Network Manager	On-Premise Standard with Extra Resources

Crosswork Data Gateway VM Requirements

VM requirements for each type of deployment are listed in the following table. These requirements are same for both VMware and Cisco CSP, unless stated otherwise.

Note The VM resource requirements for Crosswork Data Gateway are different for each profile and cannot be modified. Therefore, if your requirements change, you must re-deploy the Crosswork Data Gateway to move from one profile to another.

Table 11: 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.
Memory	• On-Premise Standard: 48 GB • On-Premise Extended: 112 GB • On-Premise Standard with Extra Resources: 128 GB
Total Disk space	• On-Premise Standard: 60 GB • On-Premise Extended: 560 GB • On-Premise Standard with Extra Resources: 60 GB
vCPU	• On-Premise Standard: 12 • On-Premise Extended: 20 • On-Premise Standard with Extra Resources: 24

<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:
<b>Note</b> 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 UI 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.
<b>Note</b> 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.
</td></tr>
</table>

Requirement	Description
IP Addresses	1, 2, or 3 IPv4 or 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 of a 3 NIC VM, you will need to provide IP address for Management Traffic (vNIC0) and Control/Data Traffic (vNIC1) only. IP address for Device Access Traffic (vNIC2) is assigned during Crosswork Data Gateway pool creation as explained in the Section: *Create a Crosswork Data Gateway Pool* in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*. Depending on the number of NICs in your deployment, this virtual IP address would be: • An additional IP address on the Management Network for a single NIC deployment. • An additional IP address on the Data Network for 2 NIC deployment. • An IP address on the Southbound Network for 3 NIC deployment.
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 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 12: 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
30607	TCP	Crosswork Controller	Outbound

Table 13: 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 value. You can change this value after installation from the Cisco Crosswork UI. See Configure Crosswork Data Gateway Global Parameters for more information.	Inbound
9010	TCP	MDT Collector	Inbound
22	TCP	CLI Collector	Outbound
6514	TLS	Syslog Collector This is the default value. You can change this value after installation from the Cisco Crosswork UI. See Configure Crosswork Data Gateway Global Parameters for more information.	Inbound
9898	TCP		
9514	UDP		

Port	Protocol	Used for...	Direction
Site Specific Default ports differ from XR, XE to vendor. Check platform-specific documentation.	TCP	gNMI Collector	Outbound

Table 14: 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
Site Specific	Site Specific	Kafka and gRPC Destination	Outbound

Cisco NSO and NED Requirements

The following table explains the requirements for using Cisco Network Services Orchestrator:

Table 15: Supported Cisco NSO and NED versions

Software/Driver	Version
Cisco Network Services Orchestrator (Cisco NSO)	5.7.5.1 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 23 Additionally, for Cisco NSO LSA setup, see (Optional) Set up Cisco NSO Layered Service Architecture, on page 23.
Cisco Network Element Driver (NED)	**Cisco IOS XR:** • CLI: 7.39.5 • NETCONF: 7.3.2, 7.315, 7.4.2, 7.5.2, 7.6, 7.7 **Cisco IOS:** • CLI: 6.77.9

(Optional) Set up Cisco NSO Layered Service Architecture

This section is applicable only when you have opted for Cisco NSO Layered Service Architecture (LSA) deployment.

Cisco NSO LSA allows you to add arbitrarily many device nodes for improved memory and provisioning throughput. Large service providers or enterprises use Cisco NSO to manage services for millions of subscribers or users, ranging over several hundred thousand managed devices. To achieve this, you can design your services in the layered fashion called LSA.

To position Cisco Crosswork Network Controller 4.0 for large customers, the solution is made compatible with the existing Cisco NSO LSA architecture.

Follow these steps to decide when to use Cisco NSO LSA:

1. Check if the deployment is stand-alone or Cisco NSO LSA.
2. If the deployment is stand-alone, check the maximum memory that may be utilised. If the maximum memory that may be utilised is more than the current memory state, Cisco NSO LSA needs to be deployed.

Note Migration from stand-alone deployment to Cisco NSO LSA deployment is not currently supported.

To get a detailed information on Cisco NSO LSA and to set up Cisco NSO LSA, see NSO Layered Service Architecture.

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 16: List of mandatory Function Packs

Crosswork Product	Required Function Pack documentation
Crosswork Network Controller Essentials package • Crosswork Optimization Engine • Crosswork Active Topology	• Cisco NSO Transport SDN Function Pack Bundle 4.0.0 User Guide • Cisco NSO Transport SDN Function Pack Bundle 4.0.0 Installation Guide • Cisco Network Services Orchestrator DLM Service Pack 4.3.0 Installation Guide • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 4.3.0-51 Installation Guide

Crosswork Product	Required Function Pack documentation
Crosswork Network Controller Advantage package (combination of Crosswork Active Topology & Crosswork Optimization Engine) • Crosswork Optimization Engine • Crosswork Active Topology • Cisco Crosswork Service Health • Cisco Crosswork Health Insights • Cisco Crosswork Change Automation • Crosswork Zero Touch Provisioning • Element Management System (EMS) Services	• Cisco NSO Transport SDN Function Pack Bundle 4.0.0 User Guide • Cisco NSO Transport SDN Function Pack Bundle 4.0.0 Installation Guide • Cisco Network Services Orchestrator DLM Service Pack 4.3.0 Installation Guide • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 4.3.0-51 Installation Guide • Cisco Crosswork Change Automation NSO Function Pack 4.3.0 Installation Guide
Crosswork Health Insights	• Cisco Network Services Orchestrator DLM Service Pack 4.3.0 Installation Guide • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 4.3.0-51 Installation Guide • Cisco Crosswork Change Automation NSO Function Pack 4.3.0 Installation Guide
Crosswork Change Automation	
Crosswork Optimization Engine	• Cisco Network Services Orchestrator DLM Service Pack 4.3.0 Installation Guide • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 4.3.0-51 Installation Guide

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 17: 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.
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

This section introduces the different topology models, their corresponding network components that you can employ to install and use Cisco Crosswork. Each topology model has corresponding network components and connections that need to be installed in order to be functional.

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.

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

Figure 1: Cisco Crosswork - 1 NIC Network Topology

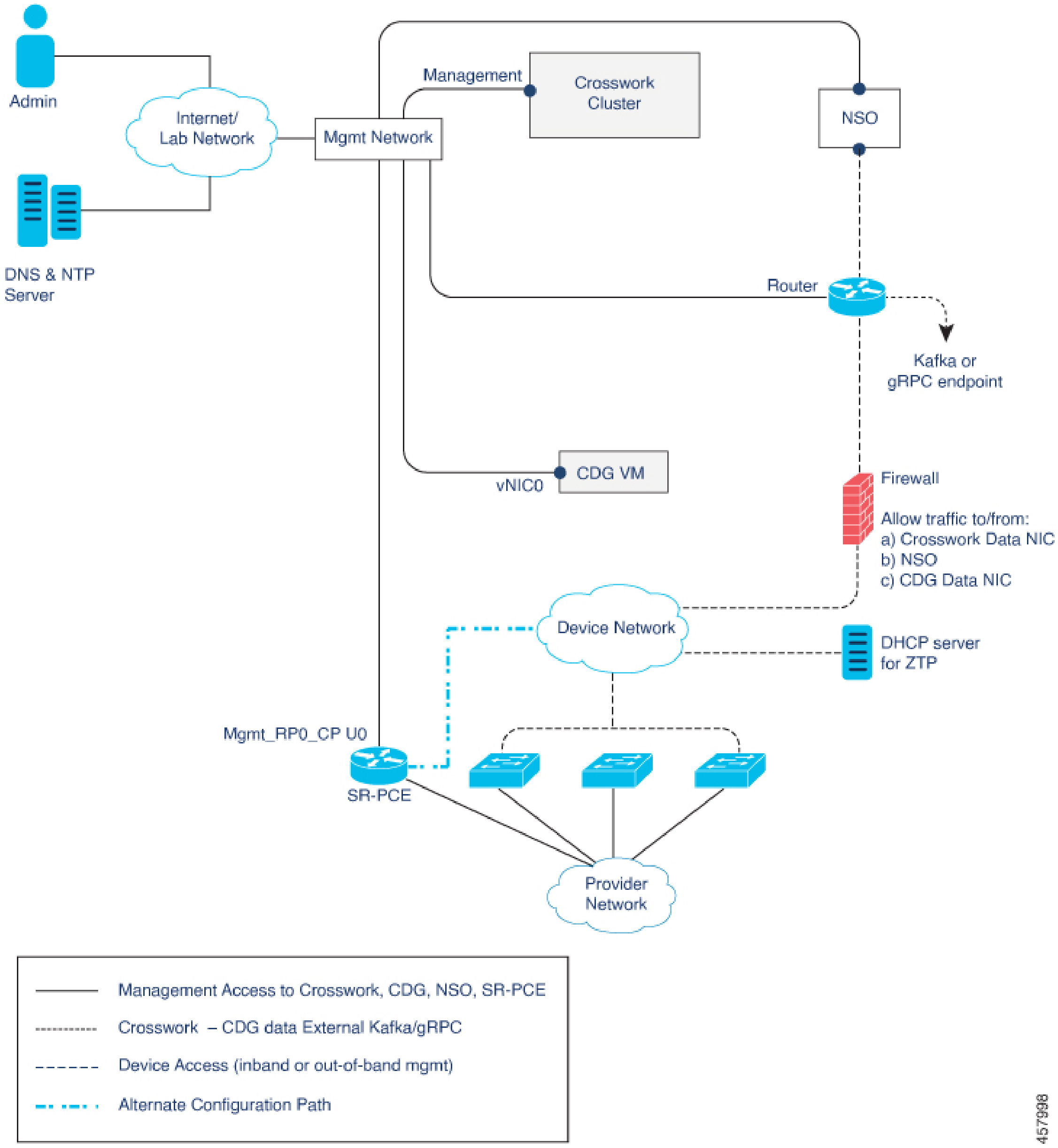


Figure 2: Cisco Crosswork - 2 NIC Network Topology

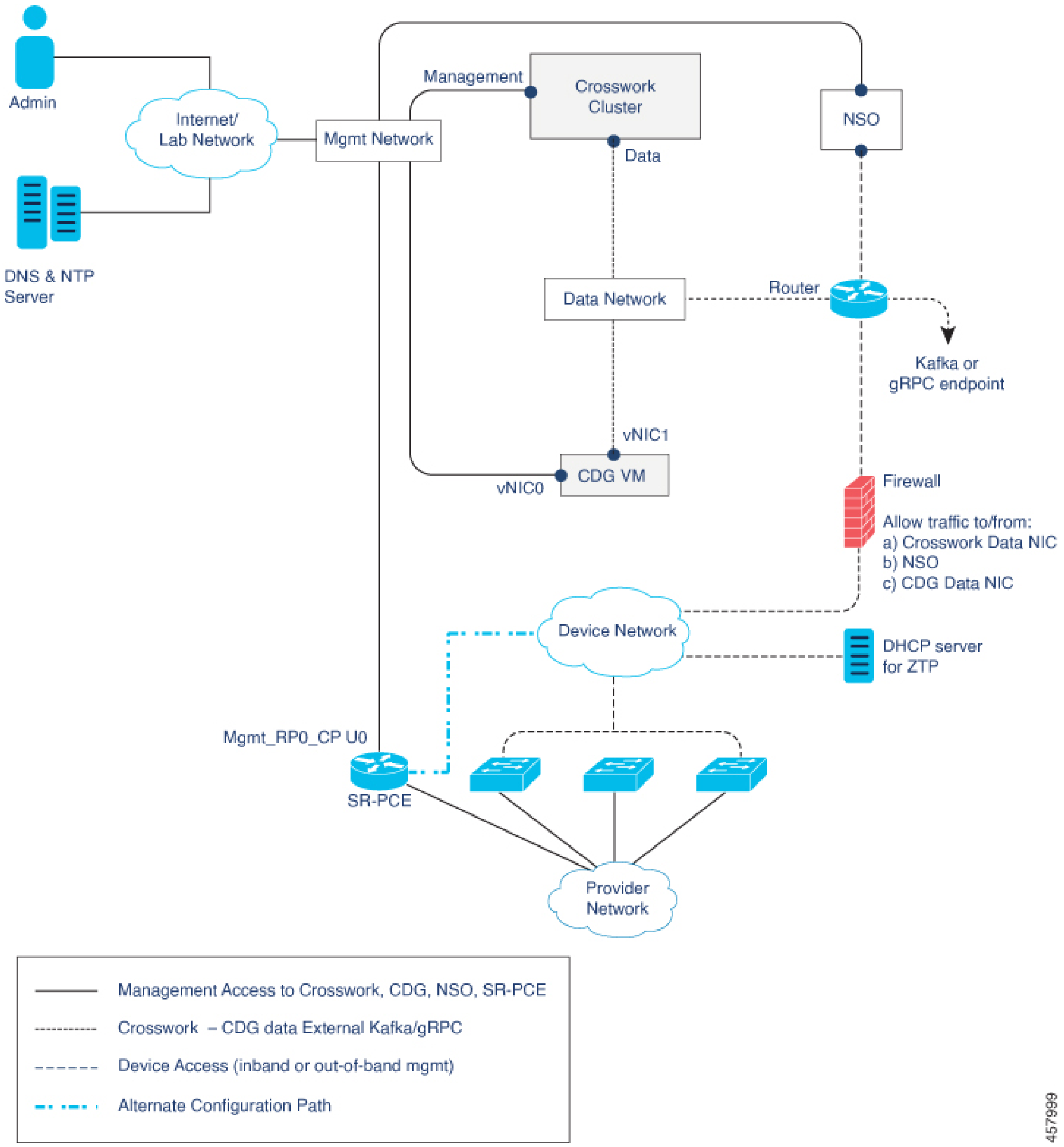


Figure 3: Cisco Crosswork - 3 NIC Network Topology

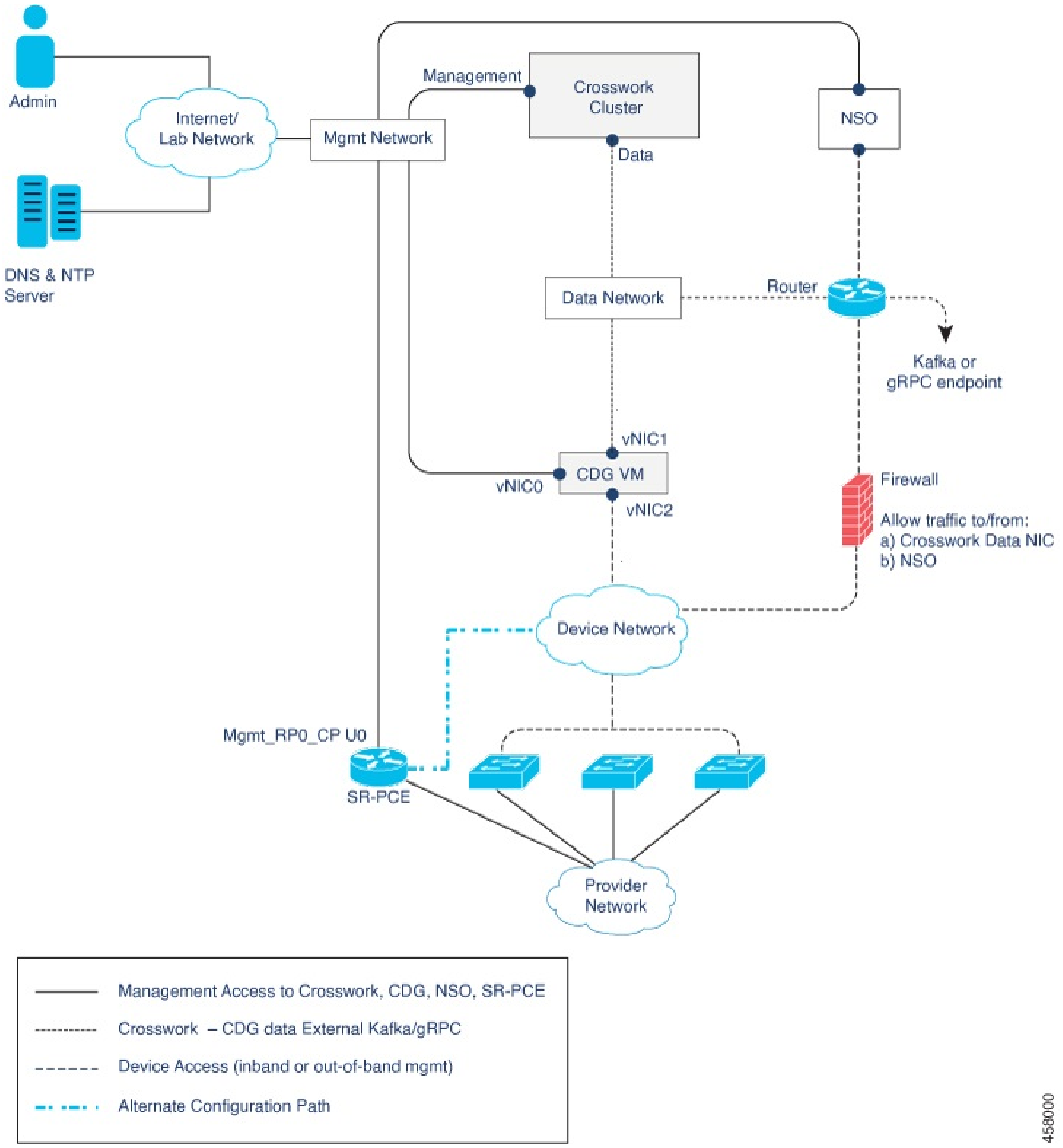


Table 18: Types of Network Traffic

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 19: 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 20: 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

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.

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). For more information on enabling Crosswork access to an SR-PCE instance as a device on the device network (shown as alternate path in the figures), please refer to the *Add Cisco SR-PCE Providers* topic in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*.

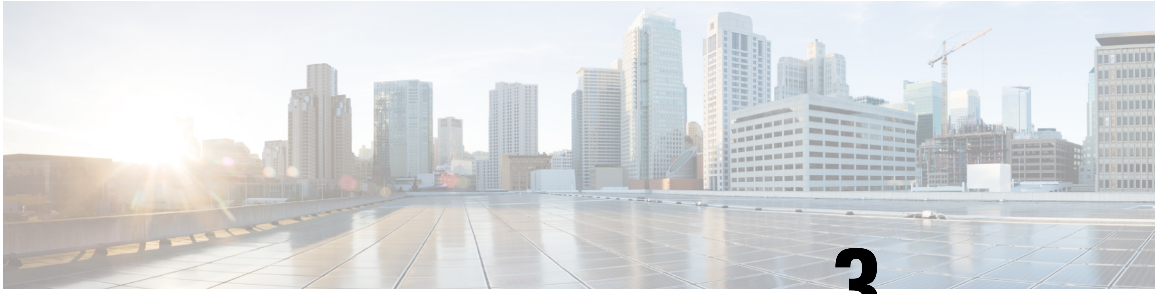
ZTP Requirements

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.

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).



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 7.

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. Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!). While they satisfy the criteria, such passwords are weak and will result in the failure of VM setup. You are recommended to use a password with more characters and complex combinations.
`VMSize`		VM size for the cluster. Values are `small`(for lab deployments only), `large`, or `extra 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 4.3 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.

Parameter Name	Also mentioned as	Description
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.
WorkerDataFsSize		Refers to the data disk size for Worker nodes (in Gigabytes). 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 (see VM Host Requirements, on page 10 for more information). 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.
OP_Status		The state for this VM. To indicate a running status, the value must be 2 (`#OP_Status = 2`). This is an optional parameter. This parameter is used (uncommented) only for manually importing the inventory without using the installer.
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.

Parameter Name	Also mentioned as	Description
`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.
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 37
- Install Cisco Crosswork on Cisco CSP, on page 41

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 7.

- 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. Store them in a secure environment or edit them to remove the passwords.

- 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 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 Crosswork 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. For more information, see Delete the VM using the Cluster Installer, on page 141.

A VM redeployment will delete the VM's data, hence caution is advised. We recommend you to perform VM parameter changes from the Crosswork 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.

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 data center.

- 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.
- 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. If your data center requires the use of VLANs you can use the manual install process instead of the installer.
- 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. When making modifications after the initial deployment of the cluster, ensure that you capture the inventory information. For more information, see the "Manage Clusters" chapter in the *Crosswork Infrastructure 4.3 and Applications Administration Guide*.
- 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.

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 7.
- 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.

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

Note If you are using a Mac, please ensure that the directory name is in lower case.

Step 2 Download the installer bundle (.bin 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-installer-4.3.0-88-release-220809.signed.bin"** and **"cw-na-platform-4.3.0-88-release-220809_SHA256_signed.ova"** respectively.

Step 3 Extract and validate the contents of the installer bundle:

a) Use the following command from a Linux-based machine with access to Cisco network:

```
$ sh <image.signed.bin>
```

The contents of the installer bundle is validated and extracted to the new directory.

Example:

```
[test@cw-build sample]$ sh cw-na-platform-installer-4.3.0-88-release-220809.signed.bin
Unpacking...
Verifying signature...
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of cw-na-platform-installer-4.3.0-88-release-220809.tar.gz
 using CW-CCO_RELEASE.cer
```

b) If the **sh** command fails due to any network connectivity issues, you can use the following command to skip verification and extract the bundle.

```
$ sh <image.signed.bin> --skip-verification
```

This new directory will contain the installer image (e.g. **cw-na-platform-installer-4.3.0-88-release-220809.tar.gz**) and files necessary to validate the image.

Example:

```
[test@cw-build sample]$ sh cw-na-platform-installer-4.3.0-88-release-220809.signed.bin
--skip-verification
Unpacking...
[test@cw-build sample]$ ls
CW-CCO_RELEASE.cer            cisco_x509_verify_release.py3
cw-na-platform-installer-4.3.0-88-release-220809.tar.gz            README
cisco_x509_verify_release.py  cw-na-platform-installer-4.3.0-88-release-220809.signed.bin
cw-na-platform-installer-4.3.0-88-release-220809.tar.gz.signature
```

Review the contents of the README file in order to understand everything that is in the package. Use the following command to manually 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 to validate the file:

```
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 to validate the file:

```
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 4 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-4.3.0-88-release-220809.tar.gz
```

Step 5 Run Docker image list or Docker images command to get the "image ID" (which is needed in the next step).

For example:

```
docker image list
```

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

```
My Machine% docker images
REPOSITORY                      TAG                                                 IMAGE ID
   CREATED        SIZE
dockerhub.cisco.com/cw-installer  cw-na-platform-installer-4.3.0-88-release-220809   a4570324fad30
  7 days ago     276MB
```

Note Pay attention to the "CREATED" time stamp in the table presented when you run Docker image list, as you might have other images present from the installation of prior releases. If you wish to remove these, the `docker rm {image id}` command can be used.

Step 6 Launch the Docker container using the following command:

```
docker run --rm -it -v `pwd`:/data {image id of the installer container}
```

To run the image loaded in our example, the command would be:

```
docker run --rm -it -v `pwd`:/data a4570324fad30
```

Note

- You do not have to enter that full value. In this case, "docker run --rm -it -v `pwd`:/data a45" was adequate. You only require enough of the image ID to uniquely identify the image you want to use for the installation.

- 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.

- 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>
    ```

- 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>
  ```

Note The Docker command provided will use the current directory to store the template and ova file used during the install. If you encounter either of the following errors you should trying running Docker from a different directory.

Error 1:

```
% docker run --rm -it -v `pwd`:/data a45
docker: invalid reference format: repository name must be lowercase.
See 'docker run --help'
```

Error 2:

```
docker: Error response from daemon: Mounts denied: approving /Users/Desktop: file does not
 exist
ERRO[0000] error waiting for container: context canceled
```

Step 7 Navigate to the directory with the VMware template.

```
cd /opt/installer/deployments/4.3.0/vcenter
```

Step 8 Copy the template file found under `/opt/installer/deployments/4.3.0/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.

Edit the template file to match your planned deployment. Refer to the table for details on the required and optional fields and proper settings. The template also includes an example (starting at line 210 in this release) that you can reference for proper formatting. The example is more compact due tot he removal of descriptive comments

Step 9 Edit the template file located in the `/data` directory in a text editor, to match your planned deployment. Refer to the Installation Parameters, on page 31 table for details on the required and optional fields and their proper settings:

- Crosswork cluster information such as VM size: Use "Small" for lab deployments, otherwise enter "Large" or "Extra Large". For more information, see the storage profiles in VM Host Requirements, on page 10.
- Unique Crosswork VM entries, including names, their IP addresses and node type settings.

  Note Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!). While they satisfy the criteria, such passwords are weak and will result in the failure of VM setup. You are recommended to use a password with more characters and complex combinations.

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

The Sample manifest template for VMware vCenter, on page 147 includes an example that you can reference for proper formatting.

Step 10 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-4.3.0-88-release-220809_SHA256_signed.ova
```

Step 11 Enter "yes" when prompted to accept the End User License Agreement (EULA).

Step 12 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.
```

Note If the installation fails due to a timeout, you should try rerunning the installation (step 12) without the `-p` option. This will deploy the VMs serially rather than in parallel.

If the installation fails (with or without the -p), open a case with Cisco and provide the .log files that were created during the install, to Cisco for review. The two most common reasons for the install to fail are: (a) password that is not adequately complex, and (b) errors in the template file.

If the installer fails for any other reason (for example, mistyped IP address), correct the error and rerun the install script.

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 63 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 7.

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 (.bin file) and the QCOW2 bundle (.bin 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-installer-4.3.0-88-release-220809.signed.bin"** and **"cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin"** respectively.

Step 3 Extract and validate the contents of the installer bundle:

a) Use the following command from a Linux-based machine with access to Cisco network:

```
$ sh <image.signed.bin>
```

The contents of the installer bundle is validated and extracted to the new directory.

Example:

```
[test@cw-build sample]$ sh cw-na-platform-installer-4.3.0-88-release-220809.signed.bin
Unpacking...
Verifying signature...
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of cw-na-platform-installer-4.3.0-88-release-220809.tar.gz
 using CW-CCO_RELEASE.cer
```

b) If the **sh** command fails due to any network connectivity issues, you can use the following command to skip verification and extract the bundle.

```
$ sh <image.signed.bin> --skip-verification
```

This new directory will contain the installer image (e.g. **cw-na-platform-installer-4.3.0-88-release-220809.tar.gz**) and files necessary to validate the image.

Example:

```
[test@cw-build sample]$ sh cw-na-platform-installer-4.3.0-88-release-220809.signed.bin
--skip-verification
Unpacking...
[test@cw-build sample]$ ls
CW-CCO_RELEASE.cer            cisco_x509_verify_release.py3
cw-na-platform-installer-4.3.0-88-release-220809.tar.gz            README
cisco_x509_verify_release.py  cw-na-platform-installer-4.3.0-88-release-220809.signed.bin
cw-na-platform-installer-4.3.0-88-release-220809.tar.gz.signature
```

Review the contents of the README file in order to understand everything that is in the package. Use the following command to manually 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 to validate the file:

```
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 to validate the file:

```
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 4 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-4.3.0-88-release-220809.tar.gz
```

Step 5 Run Docker image list or Docker images command to get the "image ID" (which is needed in the next step).

For example:

```
docker image list
```

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

```
My Machine% docker images
REPOSITORY                        TAG                                                   IMAGE ID
   CREATED        SIZE
dockerhub.cisco.com/cw-installer  ccw-na-platform-installer-4.3.0-88-release-220809   a4570324fad30
  7 days ago     276MB
```

Note Pay attention to the "CREATED" time stamp in the table presented when you run Docker image list, as you might have other images present from the installation of prior releases. If you wish to remove these, the `docker rm {image id}` command can be used.

Step 6 Launch the Docker container using the following command:

```
docker run --rm -it -v `pwd`:/data {image id of the installer container}
```

To run the image loaded in our example, the command would be:

```
docker run --rm -it -v `pwd`:/data a4570324fad30
```

Note

- You do not have to enter that full value. In this case, "docker run --rm -it -v `pwd`:/data a45" was adequate. You only require enough of the image ID to uniquely identify the image you want to use for the installation.
- 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.
- 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>
    ```
- 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>
  ```

Note The Docker command provided will use the current directory to store the template and ova file used during the install. If you encounter either of the following errors you should trying running Docker from a different directory.

Error 1:

```
% docker run --rm -it -v `pwd`:/data a45
docker: invalid reference format: repository name must be lowercase.
See 'docker run --help'
```

Error 2:

```
docker: Error response from daemon: Mounts denied: approving /Users/Desktop: file does not
 exist
ERRO[0000] error waiting for container: context canceled
```

Step 7 Navigate to the directory with the CSP template.

`cd /opt/installer/deployments/4.3.0/csp`

Step 8 Copy the template file found under `/opt/installer/deployments/4.3.0/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, to match your planned deployment. Refer to the Installation Parameters, on page 31 table for details on the required and optional fields and their proper settings:

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

  Note Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!). While they satisfy the criteria, such passwords are weak and will result in the failure of VM setup. You are recommended to use a password with more characters and complex combinations.

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

The Sample manifest template for Cisco CSP, on page 148 includes an example that you can reference for proper formatting.

Step 10 From the terminal window, extract and validate the contents of the QCOW2 bundle (.bin file):

a) Use the following command from a Linux-based machine with access to Cisco network:

```
$ sh <image.signed.bin>
```

The contents of the QCOW2 bundle is validated and extracted to the new directory.

Example:

```
[test@cw-build sample]$ sh cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin
Unpacking...
Verifying signature...
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
```

```
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz using
 CW-CCO_RELEASE.cer
```

b) If the **sh** command fails due to any network connectivity issues, you can use the following command to skip verification and extract the bundle.

```
$ sh <image.signed.bin> --skip-verification
```

This new directory will contain the QCOW2 image (e.g. **cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz**) and files necessary to validate the image.

Example:

```
[test@cw-build sample]$ sh cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin
--skip-verification
Unpacking...
[test@cw-build sample]$ ls
CW-CCO_RELEASE.cer            cisco_x509_verify_release.py3
cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz            README
cisco_x509_verify_release.py  cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin
cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz.signature
```

Review the contents of the README file in order to understand everything that is in the package. Use the following command to manually 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 to validate the file:

```
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 to validate the file:

```
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 11 Run the installer.

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

For example:

```
./cw-installer.sh install -t csp -p -m /data/deployment.tfvars -o
/data/cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz
```

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 If the installation fails due to a timeout, you should try rerunning the installation (step 14) without the `-p` option. This will deploy the VMs serially rather than in parallel.

If the installation fails (with or without the -p), open a case with Cisco and provide the .log files that were created during the install, to Cisco for review. The two most common reasons for the install to fail are: (a) password that is not adequately complex, and (b) errors in the template file.

If the installer fails for any other reason (for example, mistyped IP address), correct the error and rerun the install script.

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 63 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 46
- Manual Installation of Cisco Crosswork on Cisco CSP, on page 55

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:

1. Build the template, on page 47
2. Deploy the template, on page 52

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.

Note If the template already exists and you need to rebuild or deploy a Worker node, you can directly go to deploying the template (the second part of this procedure).

Before you begin:

- Make sure that your environment meets all the vCenter requirements specified under Cisco Crosswork Infrastructure Requirements, on page 7.

Build the template

Before you begin

- Make sure that your environment meets all the vCenter requirements specified under Cisco Crosswork Infrastructure Requirements, on page 7.
- 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.

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 Review and confirm that your network settings meet the requirements.

Step 4 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 document the choices they are going to make (such as IP address, gateway, DNS server, etc.) so that you can enter the information quickly and avoid any issues with the VMware configuration.

Step 5 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 6 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 7 Click **Next**. The **Deploy OVF Template** window is refreshed, with **3 - Select a compute resource** highlighted. Select the host for your Cisco Crosswork VM.

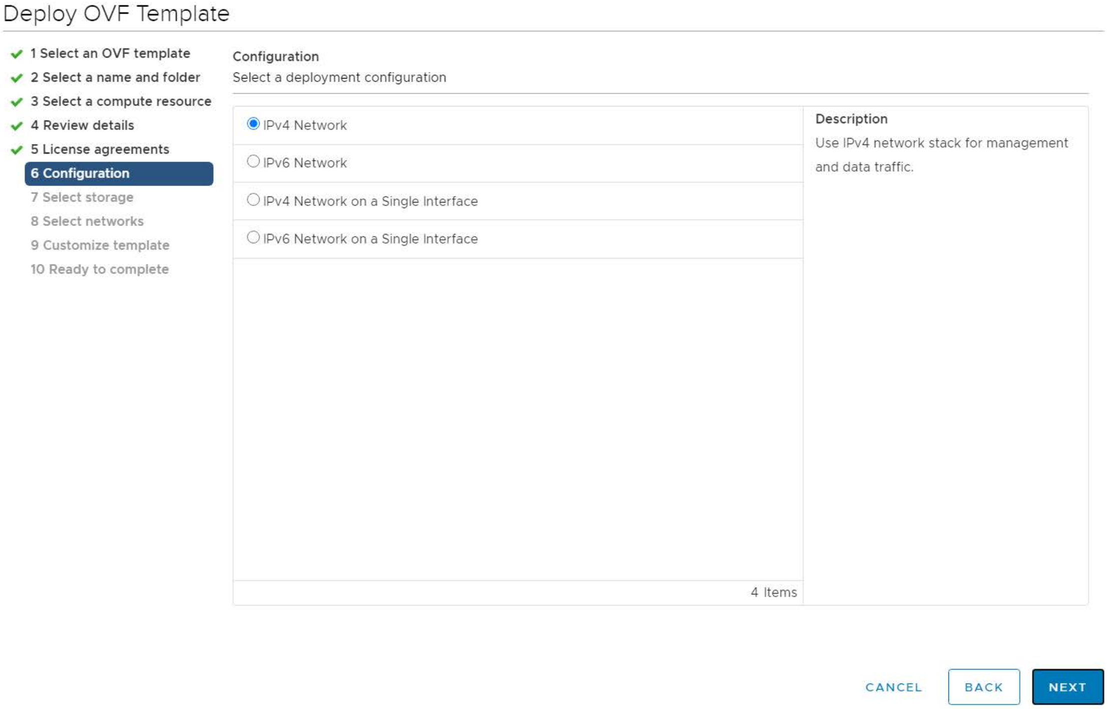
Step 8 Click **Next**. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. After the validation is complete, the **Deploy OVF Template** window is refreshed, with **4 - Review details** highlighted.

Step 9 Review the OVF template that you are deploying. Note that this information is gathered from the OVF, and cannot be modified.

Step 10 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 11 Click **Next** The **Deploy OVF Template** window is refreshed, with **6 - Configuration** highlighted. Choose the desired deployment configuration.

Figure 4: Select a deployment configuration



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Configuration

Select a deployment configuration

● IPv4 Network

○ IPv6 Network

○ IPv4 Network on a Single Interface

○ IPv6 Network on a Single Interface

4 Items

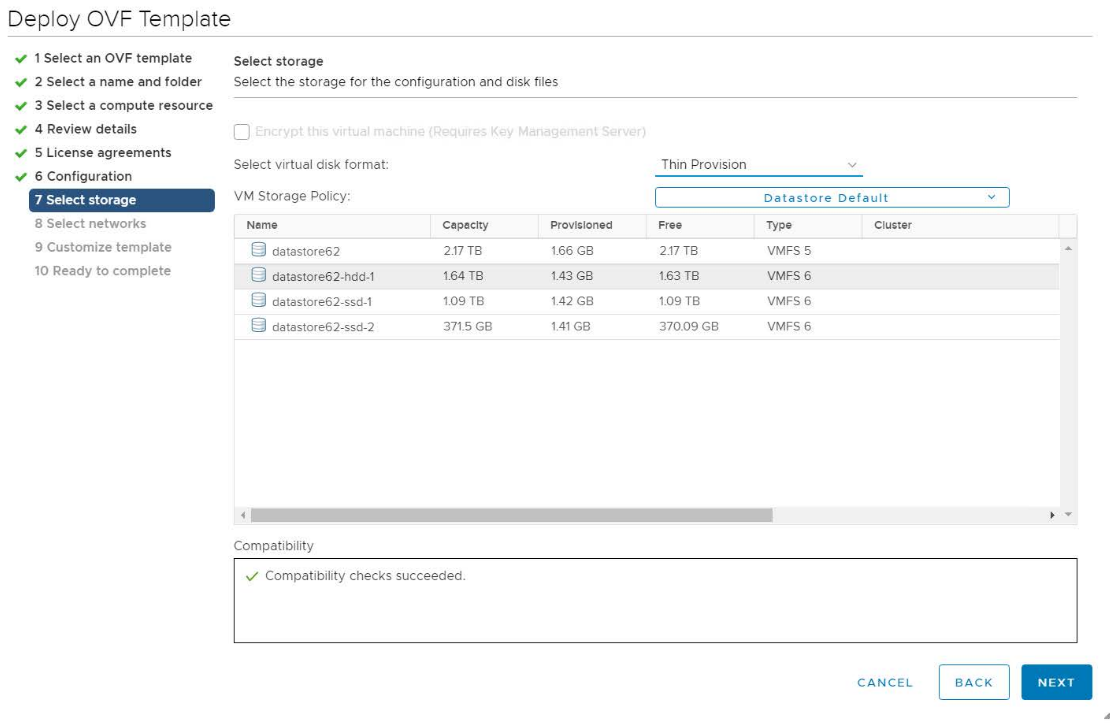
Description

Use IPv4 network stack for management and data traffic.

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 12 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



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
datastore62	2.17 TB	1.66 GB	2.17 TB	VMFS 5	
datastore62-hdd-1	1.64 TB	1.43 GB	1.63 TB	VMFS 6	
datastore62-ssd-1	1.09 TB	1.42 GB	1.09 TB	VMFS 6	
datastore62-ssd-2	371.5 GB	1.41 GB	370.09 GB	VMFS 6	

Compatibility

✓ Compatibility checks succeeded.

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.

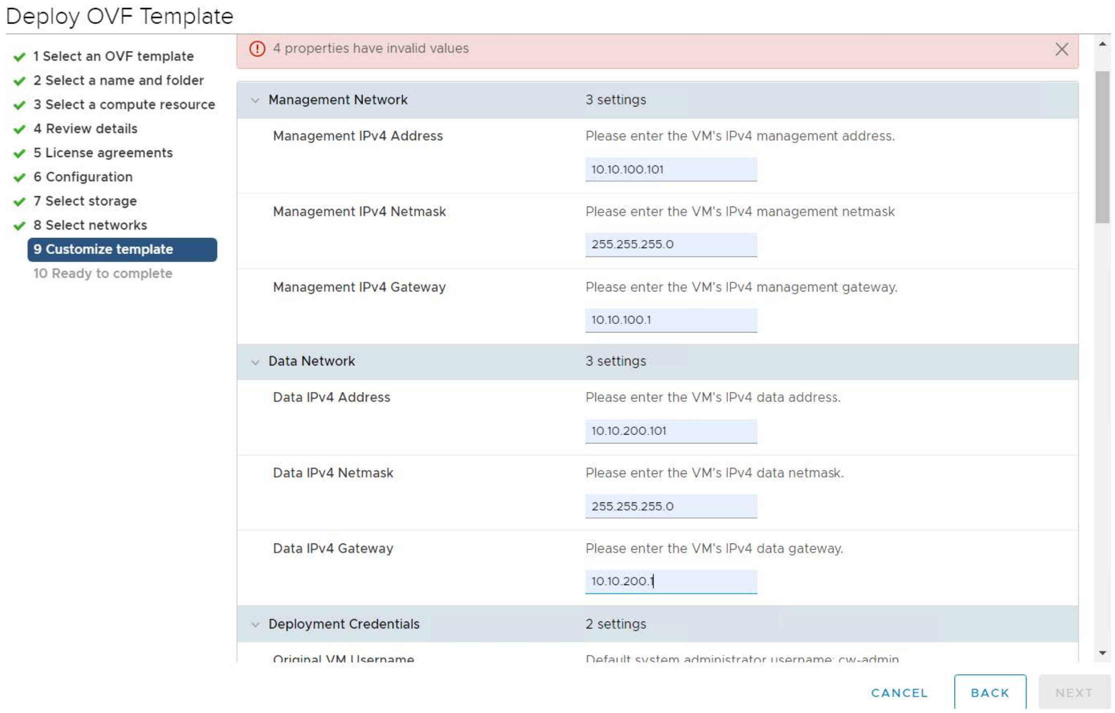
Step 13 Click **Next**. The **Deploy OVF Template** window is refreshed, with **8 - Select networks** highlighted. From the **Data Network** and **Management Network** drop-down lists, choose an appropriate destination network.

Step 14 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



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 License agreements
✓ 6 Configuration
✓ 7 Select storage
✓ 8 Select networks
9 Customize template
10 Ready to complete

4 properties have invalid values

Management Network	3 settings
Management IPv4 Address	Please enter the VM's IPv4 management address. 10.10.100.101
Management IPv4 Netmask	Please enter the VM's IPv4 management netmask 255.255.255.0
Management IPv4 Gateway	Please enter the VM's IPv4 management gateway. 10.10.100.1
Data Network	3 settings
Data IPv4 Address	Please enter the VM's IPv4 data address. 10.10.200.101
Data IPv4 Netmask	Please enter the VM's IPv4 data netmask. 255.255.255.0
Data IPv4 Gateway	Please enter the VM's IPv4 data gateway. 10.10.200.1
Deployment Credentials	2 settings
Original VM Username	Default system administrator username: cw-admin

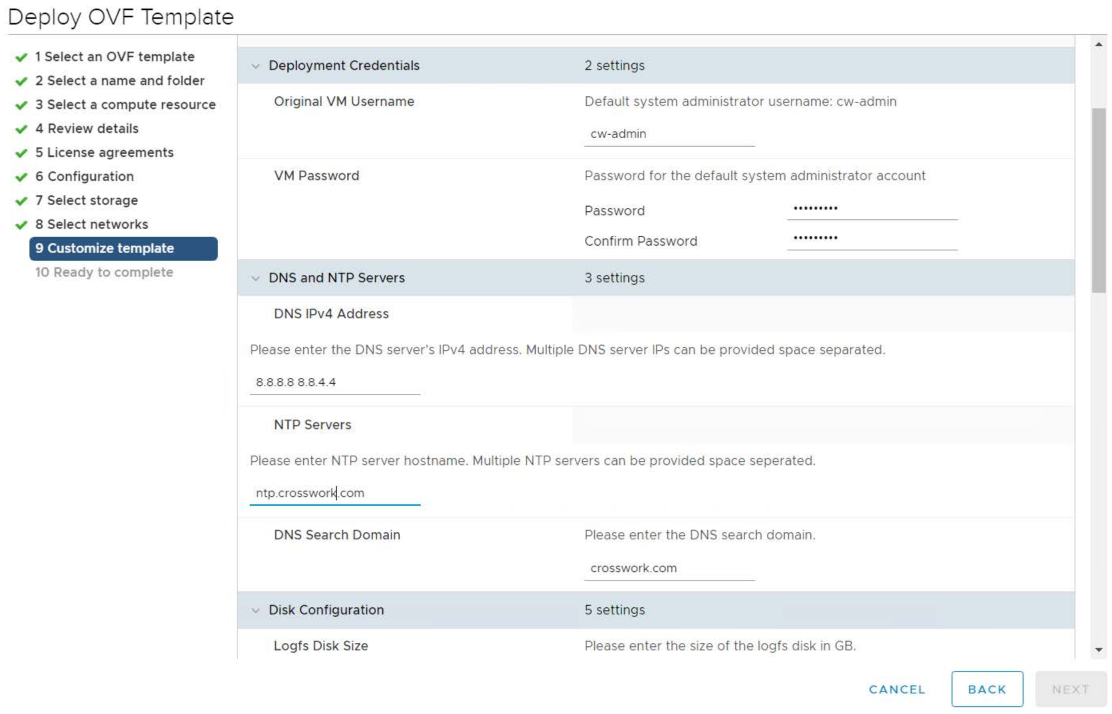
Note **Data Network** settings are not displayed if you have selected the **IPv4 on a Single Interface** or **IPv6 on a Single Interface** configuration.

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

Note Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!). While they satisfy the criteria, such passwords are weak and will result in the failure of VM setup. You are recommended to use a password with more characters and complex combinations.

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.



Deploy OVF Template

Deployment Credentials — 2 settings

Original VM Username — Default system administrator username: cw-admin

cw-admin

VM Password — Password for the default system administrator account

Password: •••••••••

Confirm Password: •••••••••

DNS and NTP Servers — 3 settings

DNS IPv4 Address

Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated.

8.8.8.8 8.8.4.4

NTP Servers

Please enter NTP server hostname. Multiple NTP servers can be provided space seperated.

ntp.crosswork.com

DNS Search Domain — Please enter the DNS search domain.

crosswork.com

Disk Configuration — 5 settings

Logfs Disk Size — Please enter the size of the logfs disk in GB.

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.

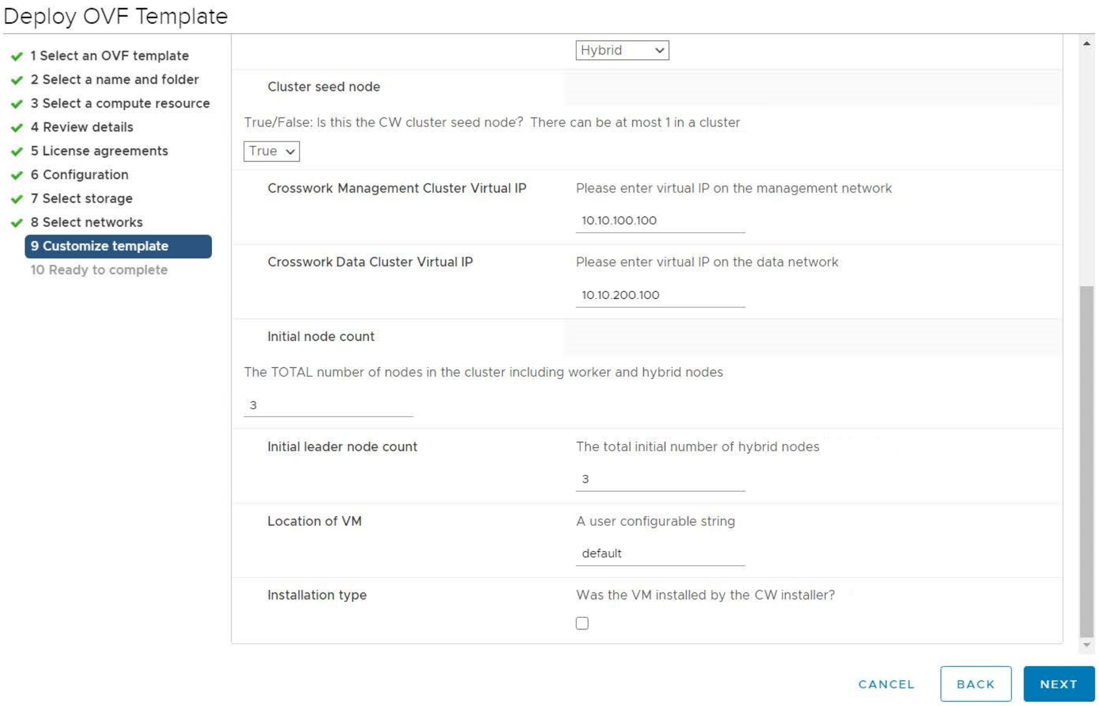
e) The default **Disk Configuration** settings should work for most environments. Change the settings only if you are instructed to by the Cisco Customer Experience team.

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.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- 9 Customize template
- 10 Ready to complete

Hybrid

Cluster seed node

True/False: Is this the CW cluster seed node? There can be at most 1 in a cluster

True

Crosswork Management Cluster Virtual IP — Please enter virtual IP on the management network: 10.10.100.100

Crosswork Data Cluster Virtual IP — Please enter virtual IP on the data network: 10.10.200.100

Initial node count

The TOTAL number of nodes in the cluster including worker and hybrid nodes: 3

Initial leader node count — The total initial number of hybrid nodes: 3

Location of VM — A user configurable string: default

Installation type — Was the VM installed by the CW installer? □

Step 15 Click **Next**. The **Deploy OVF Template** window is refreshed, with **10 - Ready to Complete** highlighted.

Step 16 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 17 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.

Deploy the template

Step 1 To build the VM, right-click on the newly created template and select **New VM from This Template**.

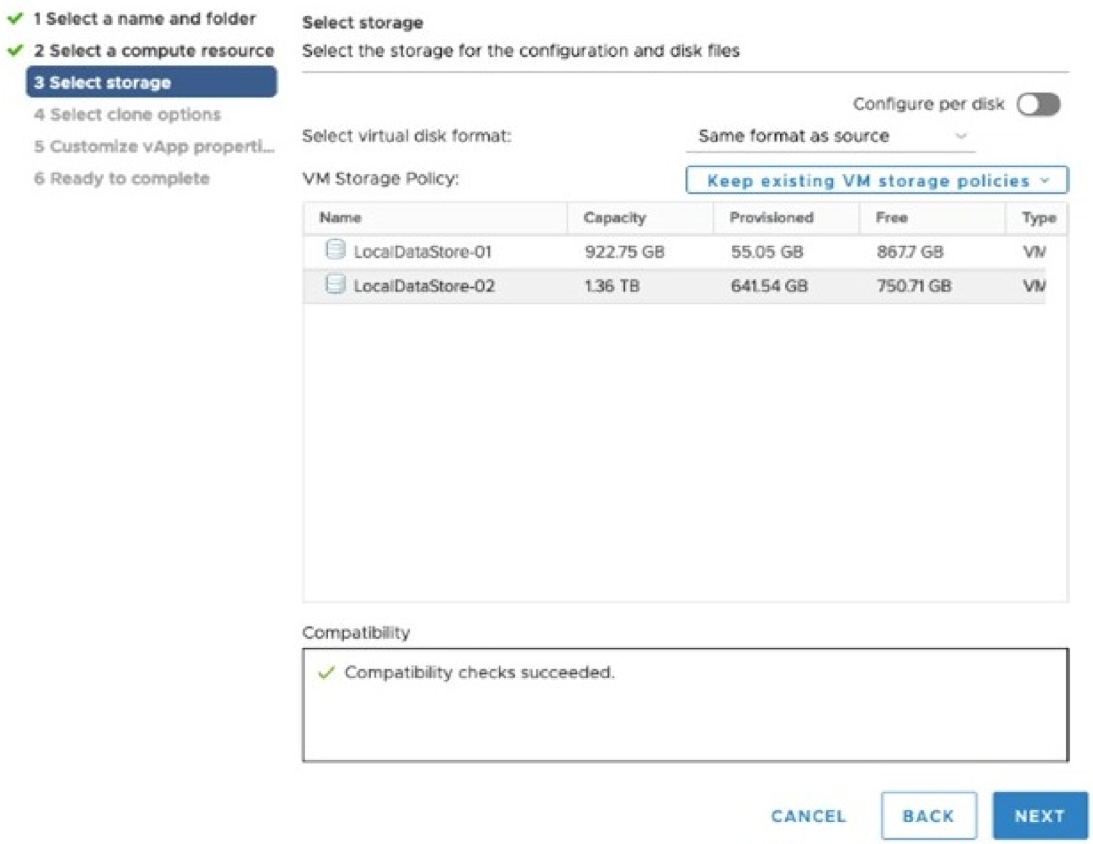
Step 2 The VMware **Deploy From Template** window appears, with the first step, **1 - Select a name and folder**, highlighted. Enter a name and select the respective Datacenter for the VM.

Step 3 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 4 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



✓ 1 Select a name and folder
✓ 2 Select a compute resource
3 Select storage
4 Select clone options
5 Customize vApp properti...
6 Ready to complete
CANCEL
BACK
NEXT

Select storage
Select the storage for the configuration and disk files

Configure per disk

Select virtual disk format: Same format as source

VM Storage Policy: Keep existing VM storage policies

Name	Capacity	Provisioned	Free	Type
LocalDataStore-01	922.75 GB	55.05 GB	867.7 GB	VM
LocalDataStore-02	1.36 TB	641.54 GB	750.71 GB	VM

Compatibility

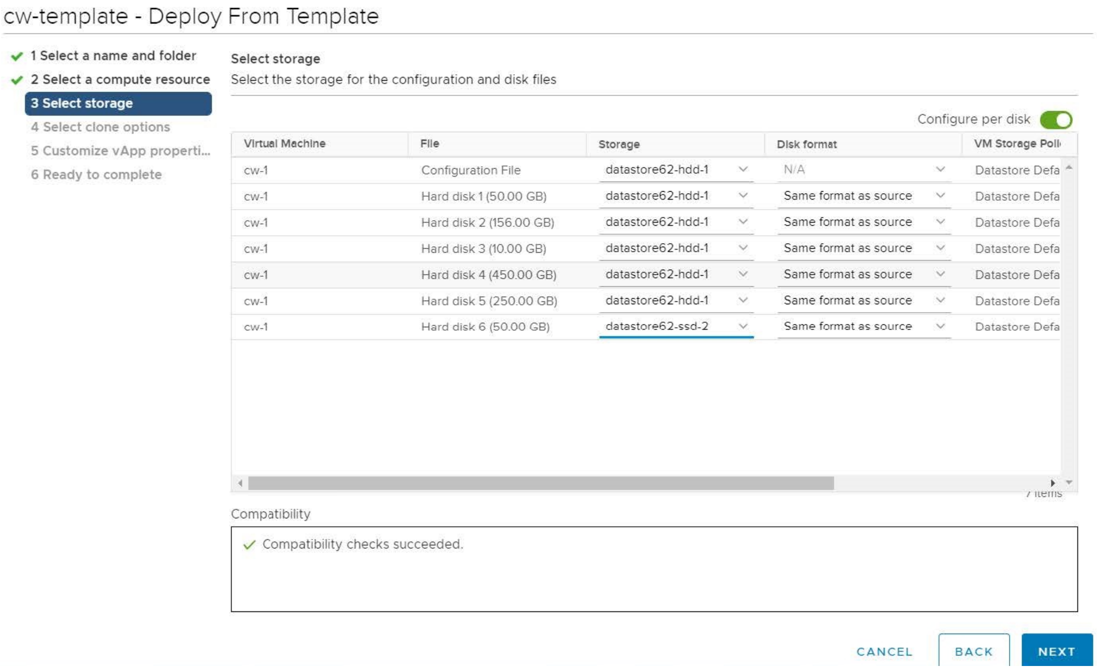
✓ Compatibility checks succeeded.

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



cw-template - Deploy From Template

✓ 1 Select a name and folder
✓ 2 Select a compute resource
3 Select storage
4 Select clone options
5 Customize vApp properti...
6 Ready to complete

Select storage
Select the storage for the configuration and disk files

Configure per disk ●

Virtual Machine	File	Storage	Disk format	VM Storage Poli
cw-1	Configuration File	datastore62-hdd-1	N/A	Datastore Defa
cw-1	Hard disk 1 (50.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 2 (156.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 3 (10.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 4 (450.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 5 (250.00 GB)	datastore62-hdd-1	Same format as source	Datastore Defa
cw-1	Hard disk 6 (50.00 GB)	datastore62-ssd-2	Same format as source	Datastore Defa

7 items

Compatibility

✓ Compatibility checks succeeded.

- Click **Next**.

Step 5 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:

Note The default configuration for the template is the small configuration. For non-lab environments, you need to go and reconfigure the hardware to use the proper amount of memory and CPU resources.

- 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 10) for **CPU** and **Memory**.
- Under **VM Options** tab, expand **Boot Options**, select **EFI** as the Firmware, and check the **Secure Boot** checkbox.

  Note If you are only deploying Hybrid nodes, you do not need to change the hardware settings.

Step 6 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 7 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 8 Repeat from **Step 1** to **Step 7** to deploy the remaining VMs in the cluster.

Step 9 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 63 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.

Note If you are using this process to build a new Worker node, no additional work is required after the node is powered on. The node will register with the existing Kubernetes cluster.

For more information on how the resources are allocated to the Worker node, see the "Rebalance Cluster Resources" section in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*.

Manual Installation of Cisco Crosswork on Cisco CSP

The manual installation of Crosswork on the Cisco CSP is needed when your deployment is not compatible with the installer tool. One common reason for this is the use of VLANs in the network configuration, and this section will use that use case as the basis for the manual install. If you are using this process for other reasons, please work with Cisco customer experience team to make sure you are making the proper adjustments to address your use case.

This following procedure explains how to manually install Crosswork cluster Hybrid nodes and Worker nodes on Cisco CSP.

Step 1 **Download and validate the Crosswork image for Cisco CSP:**

a) Download the QCOW2 bundle (*.bin file) 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 file name as **"cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin"**.

b) Use the following command from a Linux-based machine to extract and validate the contents of the QCOW2 bundle (.bin file):

```
$ sh <image.signed.bin>
```

The contents of the installer bundle is validated and extracted to the new directory.

Example:

```
[test@cw-build sample]$ sh cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin
Unpacking...
Verifying signature...
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz using
 CW-CCO_RELEASE.cer
```

c) If the **sh** command fails due to any network connectivity issues, you can use the following command to skip verification and extract the bundle.

```
$ sh <image.signed.bin> --skip-verification
```

This new directory will contain the QCOW2 image (e.g. **cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz**) and files necessary to validate the image.

Example:

```
[test@cw-build sample]$ sh cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin
--skip-verification
Unpacking...
[test@cw-build sample]$ ls
CW-CCO_RELEASE.cer            cisco_x509_verify_release.py3
cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz            README
cisco_x509_verify_release.py  cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin
cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz.signature
```

Review the contents of the README file in order to understand everything that is in the package. Use the following command to manually 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 to validate the file:

```
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 to validate the file:

```
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.

d) Add the QCOW2 bundle (**cw-na-platform-4.3.0-88-release-220809-qcow2.signed.bin**) to the repository.

When added, the package will uncompressed and added as the following files: rootfs.qcow2, extrasfs.qcow2, dockerfs.qcow2, and the sample template file.

Step 2 **Create the template file for each VM in your cluster:**

a) Download the sample template file (.xml file) from the repository, and use it to build template files for each VM node in your cluster (for example, you need three template files for a cluster of 3 Hybrid VMs). For the sake of this procedure, the template files will be referred as `ovf-env-1.xml` (for the seed node), `ovf-env-2.xml`, and `ovf-env-3.xml`

Note Only one of the nodes should have the `IsSeed` variable set to `true`.

The other template files will be the same except for the IP addresses, and the seed node setting (which will be `false`. Update the values for the second and third nodes and save as unique files.

Note While deploying Worker nodes, set the `VMType` variable in the template file as `Worker`.

Below is an example of the template file (`ovf-env-1.xml`) to create the seed node:

```
&lt;?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="CWPassword" oe:value="trial@12345"/>
        <Property oe:key="CWUsername" oe:value="admin"/>
        <Property oe:key="ClusterName" oe:value="crosswork_cluster1"/>
        <Property oe:key="CwInstaller" oe:value="True"/>
        <Property oe:key="DNSv4" oe:value="171.70.21.183"/>
        <Property oe:key="DNSv6" oe:value=""/>
        <Property oe:key="DataIPv4Address" oe:value="192.168.5.43"/>
        <Property oe:key="DataIPv4Gateway" oe:value="192.168.5.1"/>
        <Property oe:key="DataIPv4Netmask" oe:value="255.255.255.0"/>
        <Property oe:key="DataIPv6Address" oe:value=""/>
        <Property oe:key="DataIPv6Gateway" oe:value=""/>
        <Property oe:key="DataIPv6Netmask" oe:value=""/>
        <Property oe:key="DataVIP" oe:value="192.168.5.41"/>
        <Property oe:key="DataVIPName" oe:value=""/>
        <Property oe:key="Deployment" oe:value="cw_ipv4"/>
        <Property oe:key="Disclaimer" oe:value="Cisco Crosswork"/>
        <Property oe:key="Domain" oe:value="cisco.com"/>
        <Property oe:key="InitMasterCount" oe:value="3"/>
        <Property oe:key="InitNodeCount" oe:value="5"/>
        <Property oe:key="IsSeed" oe:value="True"/>
        <Property oe:key="K8Orch" oe:value=""/>
        <Property oe:key="ManagementIPv4Address" oe:value="10.195.165.43"/>
        <Property oe:key="ManagementIPv4Gateway" oe:value="10.195.165.1"/>
        <Property oe:key="ManagementIPv4Netmask" oe:value="255.255.255.0"/>
        <Property oe:key="ManagementIPv6Address" oe:value=""/>
        <Property oe:key="ManagementIPv6Gateway" oe:value=""/>
        <Property oe:key="ManagementIPv6Netmask" oe:value=""/>
        <Property oe:key="ManagementVIP" oe:value="10.195.165.41"/>
        <Property oe:key="ManagementVIPName" oe:value=""/>
        <Property oe:key="NSOProvider" oe:value="False"/>
        <Property oe:key="NTP" oe:value="ntp.esl.cisco.com"/>
        <Property oe:key="VMType" oe:value="Hybrid"/>
        <Property oe:key="corefs" oe:value="20"/>
        <Property oe:key="ddatafs" oe:value="450"/>
        <Property oe:key="logfs" oe:value="10"/>
        <Property oe:key="ramdisk" oe:value="0"/>
        <Property oe:key="bckup_min_percent" oe:value="50"/>
    </PropertySection>
</Environment>
```

Note Since a Crosswork cluster requires at least 3 VMs in hybrid configuration, you will always need a minimum of three template files. If you decide to add additional Worker nodes, ensure to create corresponding template files for each of them.

b) Unzip the QCOW2 file (**cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz**).

```
tar -xvf cw-na-platform-4.3.0-88-release-220809-qcow2.tar.gz
```

When uncompressed, it will get expanded into 3 files:

```
cw-na-platform-4.3.0-88-release-220809_dockerfs.qcow2
cw-na-platform-4.3.0-88-release-220809_extrafs.qcow2
cw-na-platform-4.3.0-88-release-220809_rootfs.qcow2
```

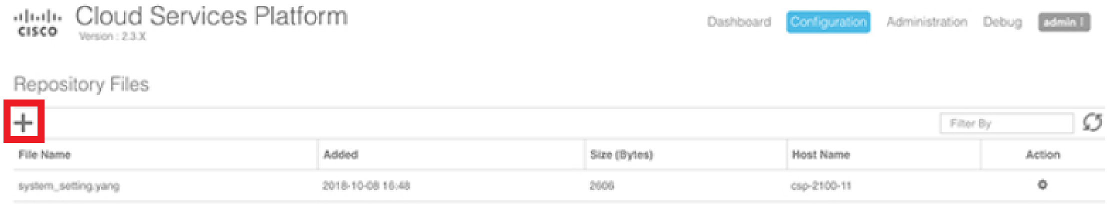
Step 3 **Upload the template files to Cisco CSP:**

Upload the templates for each cluster VM and the three .qcow2 file (see Step 2) into the repository on the Cisco CSP.

a) Log into the Cisco CSP.

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

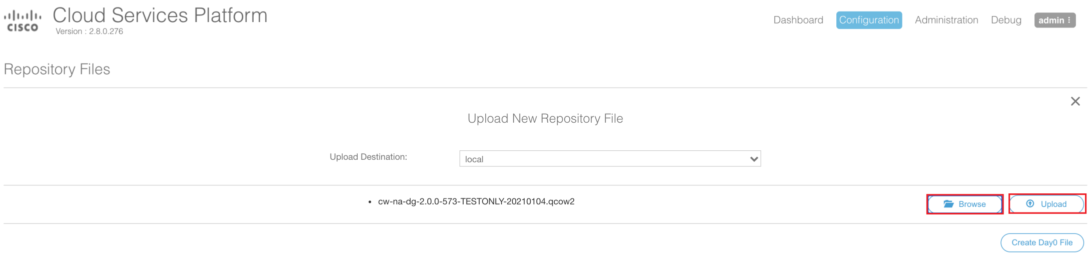
c) On the **Repository Files** page, Click ⊞ button.



File Name	Added	Size (Bytes)	Host Name	Action
system_setting.yang	2018-10-08 16:48	2606	csp-2100-11	⚙

d) Select an **Upload Destination**.

e) Click **Browse**, navigate to the `qcow2` file, click **Open** and then **Upload**. After the file is uploaded, the file name and other relevant information are displayed in the **Repository Files** table.



Upload Destination: local

- cw-na-dg-2.0.0-573-TESTONLY-20210104.qcow2

Repeat this step to upload all three `.qcow2` files (`rootfs.qcow2, extrasfs.qcow2, dockerfs.qcow2`) and for each of the template files created for each VM in the cluster.

Step 4 Create Cisco Crosswork VM:

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

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

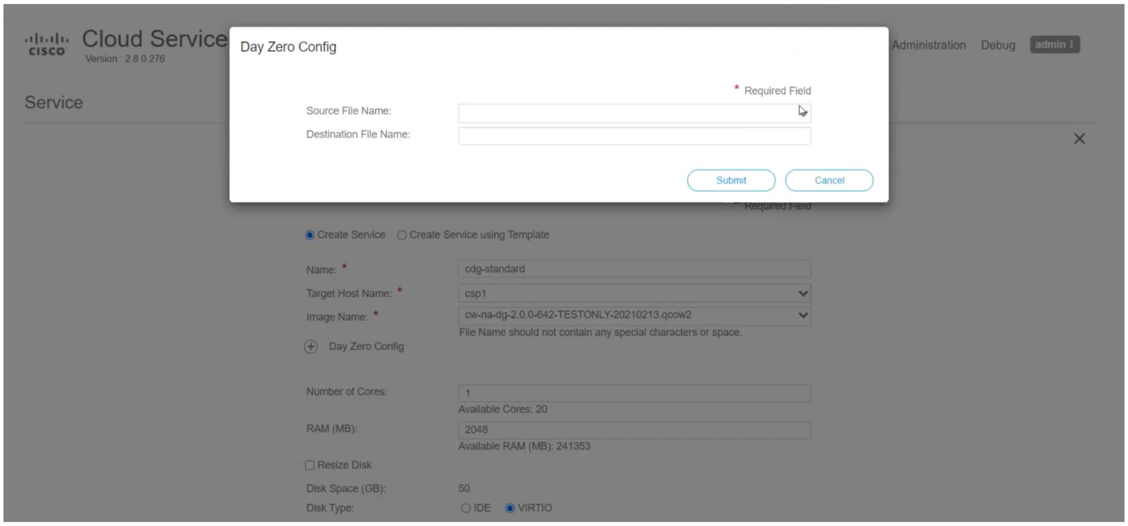
c) Check **Create Service** option.

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 `rootfs.qcow2` image.

e) Click **Day Zero Config**.



Day Zero Config

* Required Field

Source File Name:

Destination File Name:

● Create Service ○ Create Service using Template

Name: * cdg-standard

Target Host Name: * csp1

Image Name: * cw-na-dg-2.0.0-642-TESTONLY-20210213.qcow2

File Name should not contain any special characters or space.

Number of Cores: 1

Available Cores: 20

RAM (MB): 2048

Available RAM (MB): 241353

□ Resize Disk

Disk Space (GB): 50

Disk Type: ○ IDE ● VIRTIO

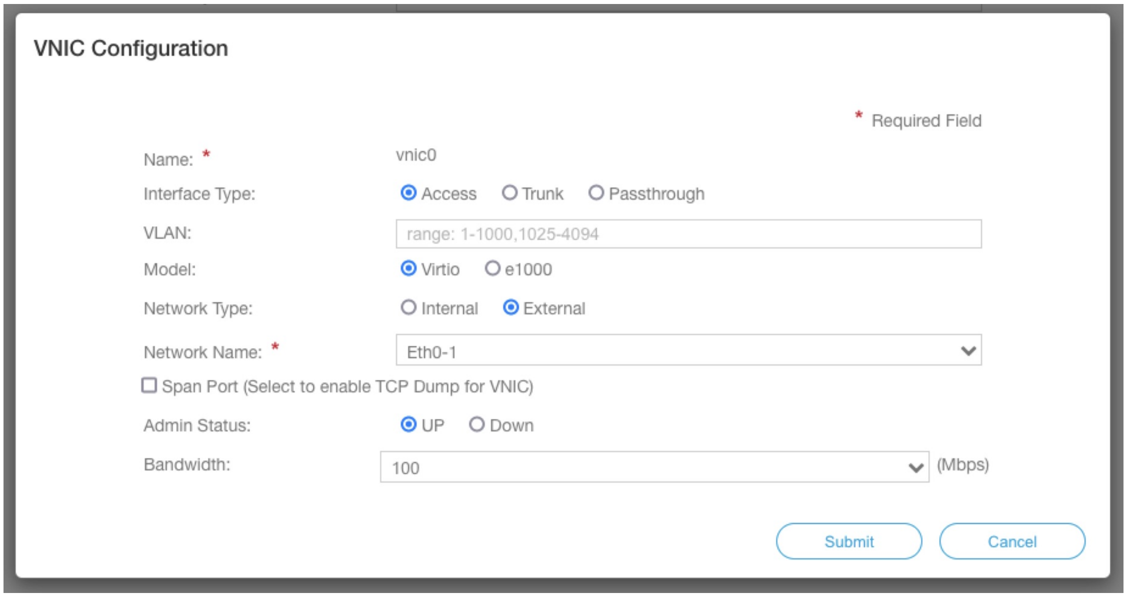
In the **Day Zero Config** dialog box, do the following:

1. From the **Source File Name** drop-down list, select a day0 configuration file (`ovf-env-1.xml` 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 Extra Large: 24
RAM (MB)	Small: 49152 Large: 98304 Extra Large: 131072

g) Click **VNIC**.



VNIC Configuration

* Required Field

Name: * vnic0

Interface Type: ● Access ○ Trunk ○ Passthrough

VLAN: range: 1-1000,1025-4094

Model: ● Virtio ○ e1000

Network Type: ○ Internal ● External

Network Name: * Eth0-1

□ Span Port (Select to enable TCP Dump for VNIC)

Admin Status: ● UP ○ Down

Bandwidth: 100 (Mbps)

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

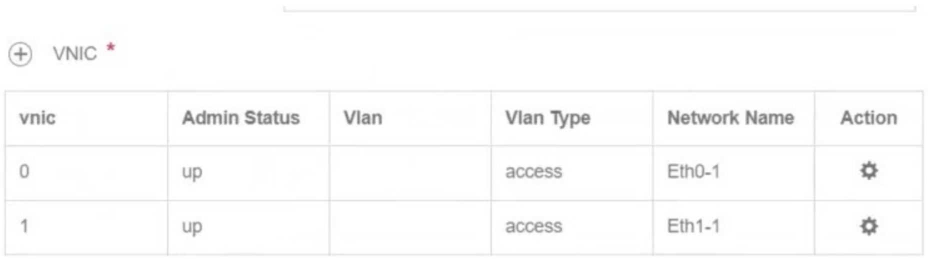
Note The VNIC Name is set by default.

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
vnic1	Eth1-1

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

After you have added vNIC0 and vNIC1, the VNIC table will look like this:

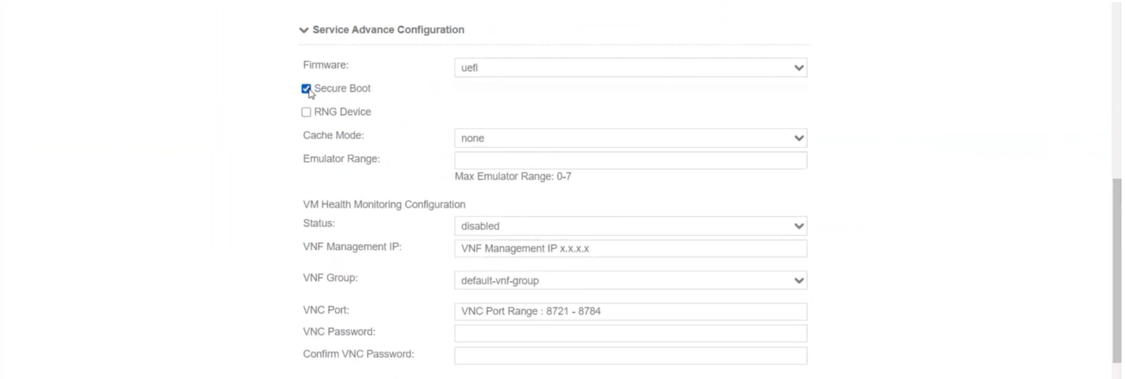


⊕ VNIC *

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

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

Check the **Secure Boot** checkbox.



Service Advance Configuration

Firmware: uefi

☑ Secure Boot

☐ RNG Device

Cache Mode: none

Emulator Range:

Max Emulator Range: 0-7

VM Health Monitoring Configuration

Status: disabled

VNF Management IP: VNF Management IP x.x.x.x

VNF Group: default-vnf-group

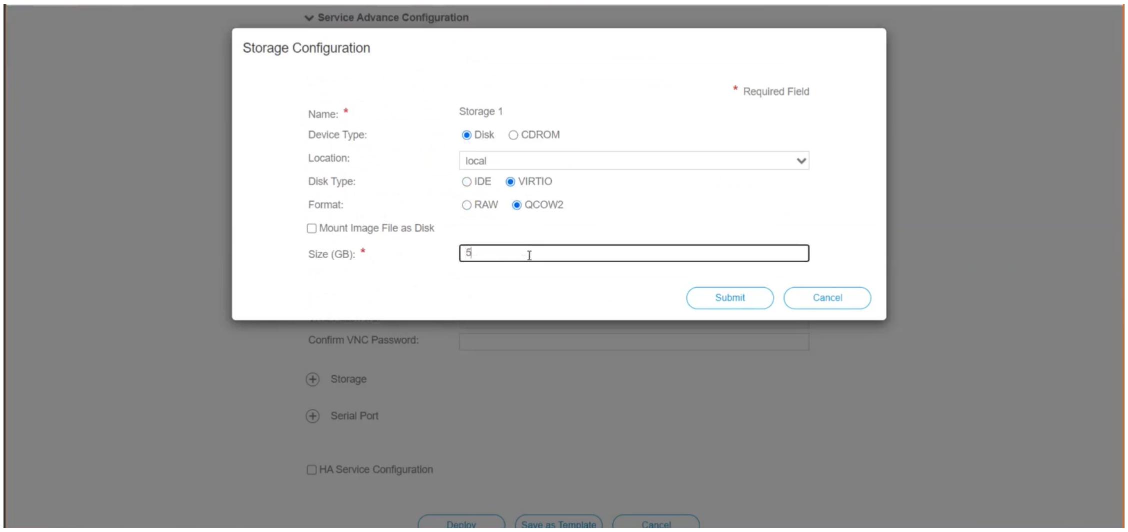
VNC Port: VNC Port Range : 8721 - 8784

VNC Password:

Confirm VNC Password:

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**. **Note** The disks get created for you when you pick the template file (.xml file). You can accept the default value, or edit the values if directed to use more disks.
Location	Select **local**.
Disk Type	Select **VIRTIO**.
Format	Select **QCOW2**.
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size.



Service Advance Configuration

Storage Configuration

* Required Field

Name: * Storage 1

Device Type: ● Disk ○ CDROM

Location: local

Disk Type: ○ IDE ● VIRTIO

Format: ○ RAW ● QCOW2

□ Mount Image File as Disk

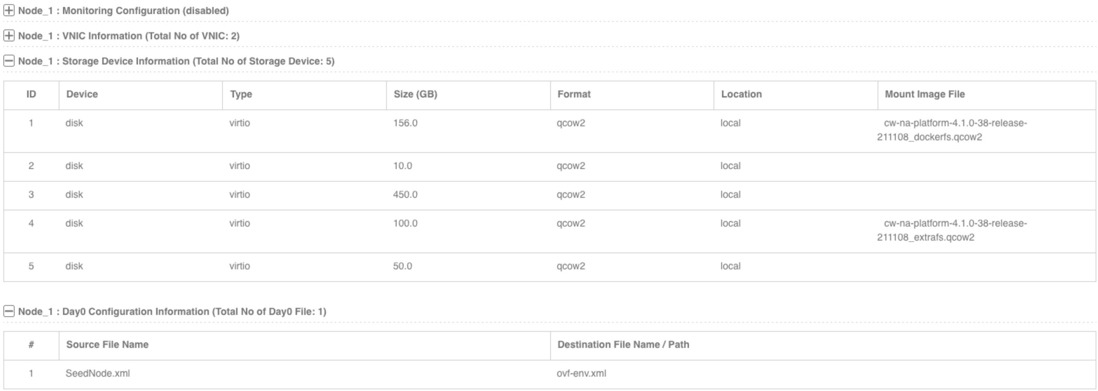
Size (GB): * 5

Note You have to configure 5 disks of different sizes, and two of them will be mapped to the .qcow2 files (`extrasfs.qcow2, dockerfs.qcow2`).

- Disk 1: 156 GB (mapped to `dockerfs.qcow2`)
- Disk 2: 10 GB
- Disk 3: 450 GB
- Disk 4: 100 GB (mapped to `extrasfs.qcow2`)
- Disk 5: 50 GB

The disk 0 gets set for the base OS in a different section.

Figure 9: Sample Storage Allocation



⊞ Node_1 : Monitoring Configuration (disabled)

⊞ Node_1 : VNIC Information (Total No of VNIC: 2)

⊟ Node_1 : Storage Device Information (Total No of Storage Device: 5)

ID	Device	Type	Size (GB)	Format	Location	Mount Image File
1	disk	virtio	156.0	qcow2	local	cw-na-platform-4.1.0-38-release-211108_dockerfs.qcow2
2	disk	virtio	10.0	qcow2	local	
3	disk	virtio	450.0	qcow2	local	
4	disk	virtio	100.0	qcow2	local	cw-na-platform-4.1.0-38-release-211108_extrafs.qcow2
5	disk	virtio	50.0	qcow2	local	

⊟ Node_1 : Day0 Configuration Information (Total No of Day0 File: 1)

#	Source File Name	Destination File Name / Path
1	SeedNode.xml	ovf-env.xml

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

j) Click **Deploy**.

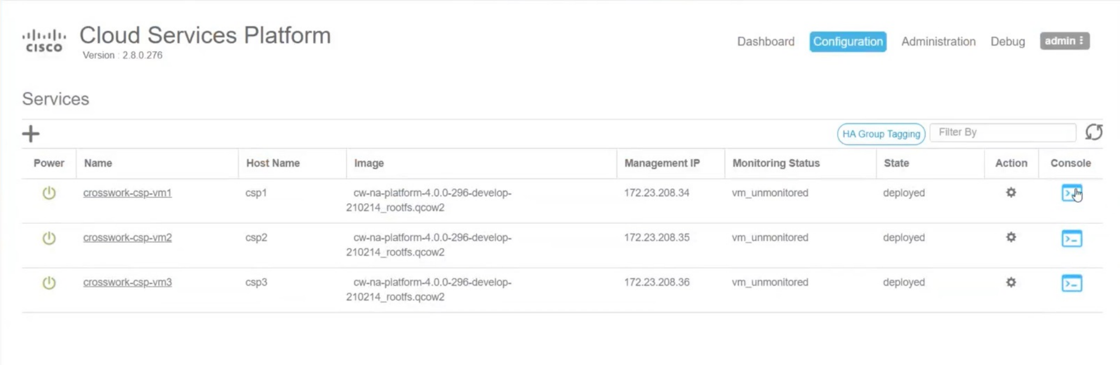
You will see a message once the service has successfully deployed. Click **Close**.

Step 5 Repeat **Step 4** for each VM in the cluster.

Step 6 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.



Power	Name	Host Name	Image	Management IP	Monitoring Status	State	Action	Console
⏻	crosswork-csp-vm1	csp1	cw-na-platform-4.0.0-296-develop-210214_rootfs.qcow2	172.23.208.34	vm_unmonitored	deployed	⚙	>_
⏻	crosswork-csp-vm2	csp2	cw-na-platform-4.0.0-296-develop-210214_rootfs.qcow2	172.23.208.35	vm_unmonitored	deployed	⚙	>_
⏻	crosswork-csp-vm3	csp3	cw-na-platform-4.0.0-296-develop-210214_rootfs.qcow2	172.23.208.36	vm_unmonitored	deployed	⚙	>_

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 63 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`. If the VMs get built and are able to boot, the errors in applying the operator specified configuration will be logged on the VM in the /var/log/firstboot.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.

Note 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.

2. The installer creates the VMs, and displays a success message (e.g. "Creation Complete") after each VM is created.

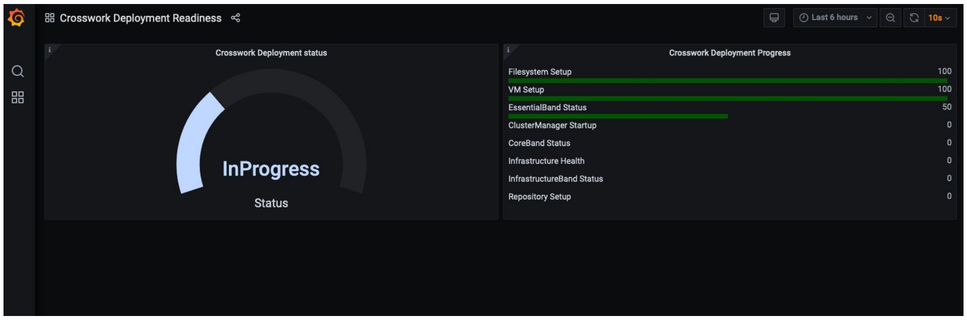
   Note For VMware deployments, this activity can also be monitored from the vSphere UI.

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. "Crosswork Installer operation complete") will be displayed and the installer script will exit and return you to a prompt 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 10: Crosswork Deployment Readiness

  Crosswork Deployment Readiness

  Crosswork Deployment status

  InProgress

  Status

  Crosswork Deployment Progress

  Filesystem Setup 100
  VM Setup 100
  EssentialBand Status 50
  ClusterManager Startup 0
  CoreBand Status 0
  Infrastructure Health 0
  InfrastructureBand Status 0
  Repository Setup 0

- **Using the console:** You can also check the progress from the console of one of the hybrid VMs or by using SSH to the Virtual IP address, then after logging in switch to super user and run `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 65.

Failure Scenario

In the event of a failue scenario (listed below), contact the Cisco Customer Experience team and provide the `installer.log`, `installer_tf.log`, and `firstBoot.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 `/var/log/firstBoot.log` or `/opt/robot/bin/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 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 15).

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 that was configured during the install.

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 4.3 and Applications Administrator Guide*.

Step 3 Log into the Cisco Crosswork as follows:

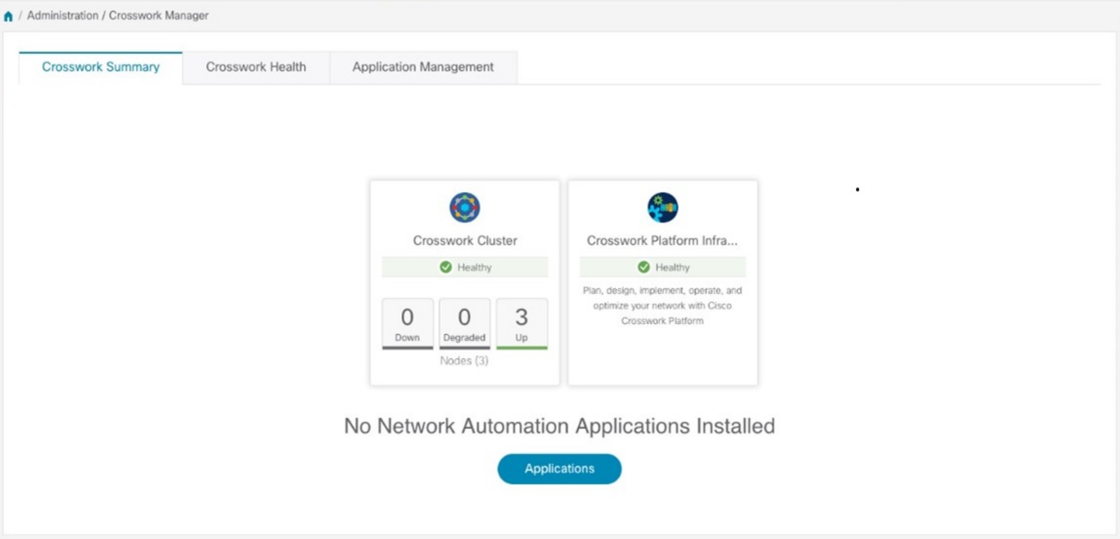
a) Enter the Cisco Crosswork administrator username **admin** and the default password **admin**.

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**.

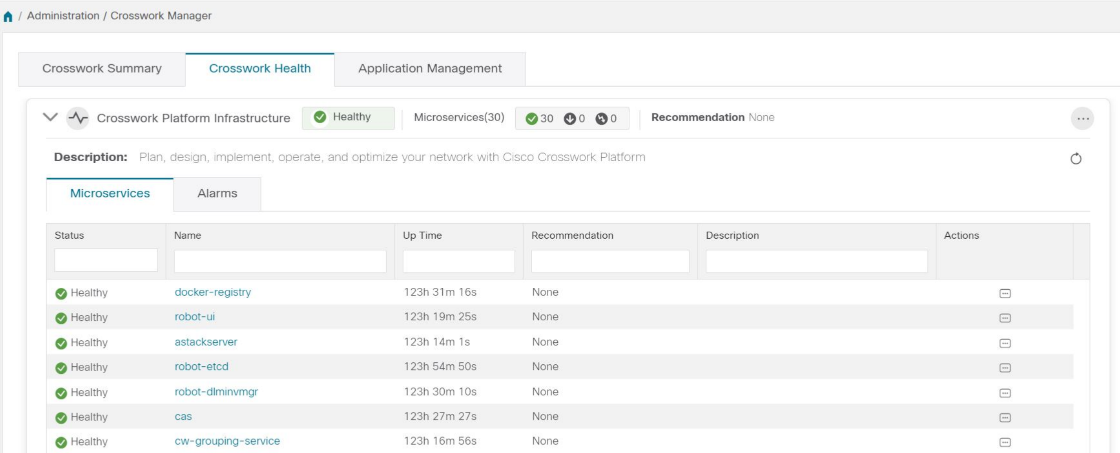
Note Use a strong VM Password (minimum 8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words (for example, C!sco123 or Cwork321!). You are recommended to use a password with more characters and complex combinations.

The **Crosswork Manager** window is displayed.



/ Administration / Crosswork Manager
Crosswork Summary
Crosswork Health
Application Management
Crosswork Cluster
Healthy
0 Down
0 Degraded
3 Up
Nodes (3)
Crosswork Platform Infra...
Healthy
Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform
No Network Automation Applications Installed
Applications

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.



Description: Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Status	Name	Up Time	Recommendation	Description	Actions
✓ Healthy	docker-registry	123h 31m 16s	None		⋯
✓ Healthy	robot-ui	123h 19m 25s	None		⋯
✓ Healthy	astackserver	123h 14m 1s	None		⋯
✓ Healthy	robot-etcd	123h 54m 50s	None		⋯
✓ Healthy	robot-dlminvmgr	123h 30m 10s	None		⋯
✓ Healthy	cas	123h 27m 27s	None		⋯
✓ Healthy	cw-grouping-service	123h 16m 56s	None		⋯

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 7.
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.

Scenario	Possible Resolution
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>`

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 8.

Scenario	Possible Resolution
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 16.

2. Install Cisco Crosswork Data Gateway on your preferred platform:

VMware	Install Cisco Crosswork Data Gateway Using vCenter vSphere Client, on page 84
	Install Cisco Crosswork Data Gateway Via OVF Tool, on page 89
Cisco CSP	Install Cisco Crosswork Data Gateway on Cisco CSP, on page 91

3. Set timezone on Cisco Crosswork Data Gateway VM. See Configure Timezone of the Crosswork Data Gateway VM, on page 101.

4. Verify Cisco Crosswork Data Gateway enrollment with Cisco Crosswork. See Cisco Crosswork Data Gateway Authentication and Enrollment, on page 104.

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 addresses 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 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 4.3 and Applications Administration Guide*.

The **dg-admin** and **dg-oper** user accounts are reserved usernames and cannot be changed. You can change the password in the console for both the accounts. See Section *Change Passphrase Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*. In case of lost or forgotten passwords, destroy the current VM, you have to create a new VM, and re-enroll the new VM with Cisco Crosswork.

In the following table:

* Denotes the mandatory parameters. Parameters without this mark are optional. You can choose them based on your deployment scenario. Deployment scenarios are explained (wherever applicable) in the **Additional Information** column.

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

Table 21: 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 Gateway VMs.	
Deployment	`Deployment`	Parameter that conveys the type of controller application that CDG is deployed with. For an on-premise installation, choose either: • `onpremise-standard` • `onpremise-standard-plus` • `onpremise-extended` The default value is `onpremise-standard`.	The deployment parameter for the profile **On-Premise Standard with Extra Resources** is `onpremise-standard-plus`. You 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. The default number of interfaces for the deployment options—Standard, Standard Plus, and Extended are 3.	You can choose to use either 1, 2, or 3 vNICs as per the following combinations: **Important** If you use one vNIC in your Crosswork cluster, use only one vNIC in the Crosswork Data Gateway. If you use two vNICs in your Crosswork Cluster, then you can use two or three vNICs in 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, data traffic through vNIC1, and device data on vNIC2.

Name	Parameter	Description	Additional Information
AllowRFC8190*	`AllowRFC8190`	Choose how to validate interface addresses that fall in a usable RFC 8190 range. Options are `True`, `False`, or `Ask`, where the initial configuration scripts prompts for confirmation. The default value is `True` to automatically allow interface addresses in an RFC 8190 range.	
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`	Passphrase of SCP user to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	

Name	Parameter	Description	Additional Information
Data Disk Size	`DGAppdataDisk`	Size in GB of a second data disk. Default value of this parameter in each profile is: • 10 GB for Standard. • 10 GB for Standard Plus • 510 GB for Extended.	
Passphrase			
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 In a 3-NIC deployment, you need to provide IP address for Management Traffic (vNIC0) and Control/Data Traffic (vNIC1) only. IP address for Device Access Traffic (vNIC2) is assigned during Crosswork Data Gateway pool creation as explained in the Section: *Create a Crosswork Data Gateway Pool* in the *Cisco Crosswork Infrastructure 4.3 and Applications Administration Guide*. **Note** • Selecting **None** in both IPv4 Method and the IPv6 Method fields of the vNIC results in a nonfunctional deployment. • VMware vCenter does not require the vNIC2 details and does not ask for this value during deployment.			
vNIC IPv4 Address			

Name	Parameter	Description	Additional Information

vNIC IPv4 Method*
For example, the parameter name for vNIC0 is vNIC0 IPv4 Method.
	`Vnic0IPv4Method`
	`Vnic1IPv4Method`
	`Vnic2IPv4Method`
		Method in which the interface is assigned an IPv4 address - `None`, `Static`, or `DHCP`.
		The default value is `None`.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for the vNIC IPv4 parameters. Proceed to enter information in the vNIC IPv6 Address parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			• **DHCP**: The vNIC IPv4 Address parameter values are assigned automatically. Do not change these values.

vNIC IPv4 Address	`Vnic0IPv4Address`
	`Vnic1IPv4Address`
	`Vnic2IPv4Address`
		IPv4 address of the interface.	

vNIC IPv4 Netmask	`Vnic0IPv4Netmask`
	`Vnic1IPv4Netmask`
	`Vnic2IPv4Netmask`
		IPv4 netmask of the interface in dotted quad format.	

vNIC IPv4 Skip Gateway	`Vnic0IPv4SkipGateway`
	`Vnic1IPv4SkipGateway`
	`Vnic2IPv4SkipGateway`
		The default value is `False`.
		Setting this to `True` skips configuring a gateway.	

vNIC IPv4 Gateway	`Vnic0IPv4Gateway`
	`Vnic1IPv4Gateway`
	`Vnic2IPv4Gateway`
		IPv4 address of the vNIC gateway.	

vNIC IPv6 Address			

Name	Parameter	Description	Additional Information

vNIC IPv6 Method*	`Vnic0IPv6Method`
	`Vnic1IPv6Method`
	`Vnic2IPv6Method`
		Method in which the vNIC interface is assigned an IPv6 address - `None`, `Static`, or `DHCP`.
		The default value is `None`.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for the vNIC IPv6 parameters. Enter information in the vNIC IPv4 Address parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			• **DHCP**:
			Values for the vNIC IPv6 Address parameters are assigned automatically.
			Do not change the VnicxIPv6Address default values.

vNIC IPv6 Address	`Vnic0IPv6Address`
	`Vnic1IPv6Address`
	`Vnic2IPv6Address`
		IPv6 address of the interface.	

vNIC IPv6 Netmask	`Vnic0IPv6Netmask`
	`Vnic1IPv6Netmask`
	`Vnic2IPv6Netmask`
		IPv6 prefix of the interface.	

vNIC IPv6 Skip Gateway	`Vnic0IPv6SkipGateway`
	`Vnic1IPv6SkipGateway`
	`Vnic2IPv6SkipGateway`
		Options are `True` or `False`.
		Selecting `True` skips configuring a gateway.	

vNIC IPv6 Gateway	`Vnic0IPv6Gateway`
	`Vnic1IPv6Gateway`
	`Vnic2IPv6Gateway`
		IPv6 address of the vNIC gateway.	

DNS Servers			
DNS Address*	`DNS`	Space delimited list of IPv4 or IPv6 addresses of the DNS servers accessible from the management interface.	
DNS Search Domain*	`Domain`	DNS search domain	
DNS Security Extensions *	`DNSSEC`	Options are `False`, `True`, or `Allow-Downgrade`. The default value is `False` Select `True` to use DNS security extensions.	

Name	Parameter	Description	Additional Information
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`. Select `True` to use multicast DNS. The default value is `False`.	If you choose Resolve, only resolution support is enabled. Responding is disabled.
Link-Local Multicast Name Resolution*	`LLMNR`	Options are `False`, `True`, `Opportunistic`, or `Resolve`. The default value is `False`. Select `True` to use link-local multicast name resolution.	If you choose Resolve, only resolution support is enabled. Responding is disabled.
NTPv4 Servers			
NTPv4 Servers*	`NTP`	Space-delimited list of IPv4, IPv6 addresses, or hostnames of the NTPv4 servers accessible in 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 nonfunctional 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.

Name	Parameter	Description	Additional Information
Use NTPv4 Authentication	`NTPAuth`	Select `True` to use NTPv4 authentication. The default value is `False`.	
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`	Options are `True` and `False`. Select `True` to send syslog messages to a remote host. The default value is `False`.	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 the following settings: • Use Remote Syslog Server • Syslog Server Address • Syslog Server Port • Syslog Server Protocol **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`	Hostname, IPv4, or IPv6 address of a syslog server accessible in 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. The default port number is 514.	
Syslog Server Protocol	`SyslogProtocol`	Options are `UDP` or `TCP` to send the syslog. The default value is `UDP`.	
Use Syslog over TLS?	`SyslogTLS`	Select `True` to use TLS to encrypt syslog traffic. The default value is `False`.	
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.	

Name	Parameter	Description	Additional Information
Remote Auditd Server			
Use Remote Auditd Server*	`UseRemoteAuditd`	Options are `True` and `False`. The default value is `False`.. Select `True` to send auditd messages 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. The default port is 60.	
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.	

Name	Parameter	Description	Additional Information
Controller Signing Certificate File URI*	`ControllerSignCertChain`	PEM formatted root cert of Cisco Crosswork to validate signing certs retrieved 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 enroll automatically with Cisco Crosswork. 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 108.
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.	

Name	Parameter	Description	Additional Information
Proxy Server URL	`ProxyURL`	URL of the HTTP 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`	Comma-delimited list of addresses and hostnames that will not use 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.	

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 We have included sample images of Cisco Crosswork Data Gateway on-premise Standard deployment in the procedure.

Step 1 Download the Cisco Crosswork Data Gateway 4.0 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 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* Table 21: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 72 for list of mandatory and optional parameters.

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**.

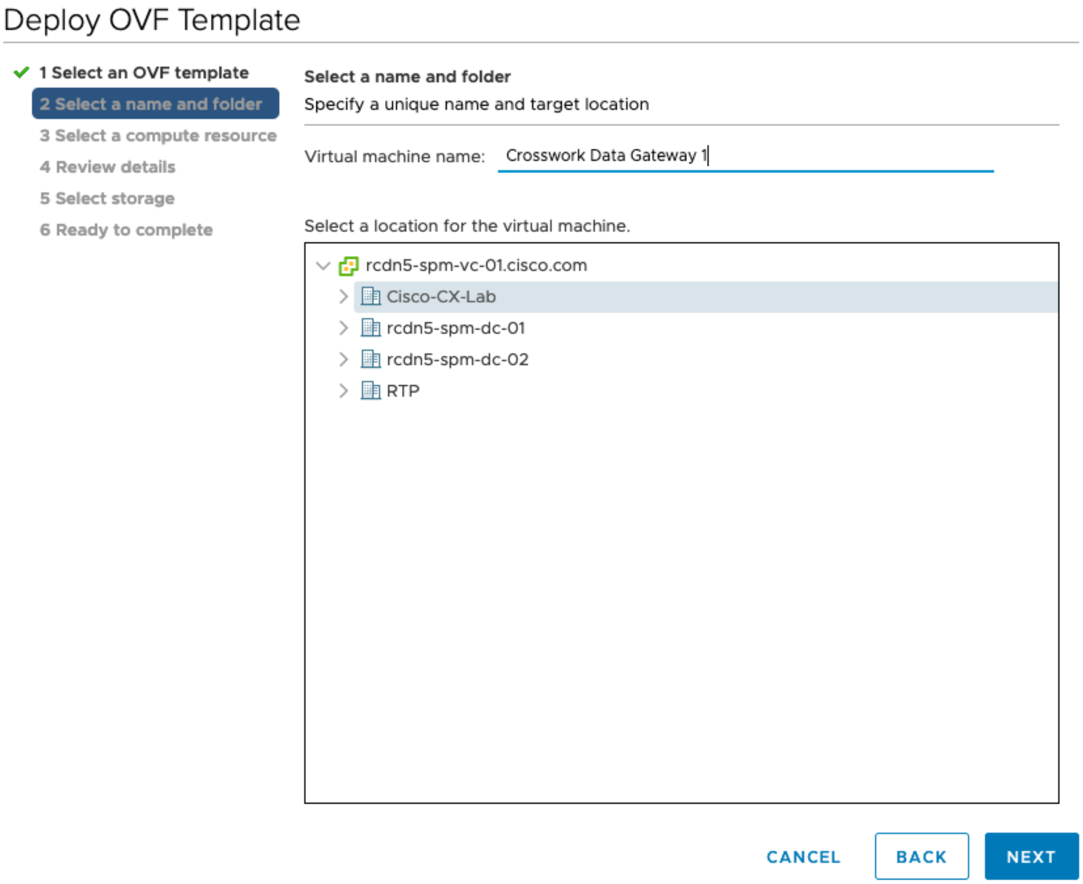
a) Click **Browse** to navigate to the location where you downloaded the OVA image file and select it.

Once selected, the file name 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 data center under which the VM will reside.


Deploy OVF Template

✓ 1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Ready to complete

Select a name and folder

Specify a unique name and target location

Virtual machine name: Crosswork Data Gateway 1

Select a location for the virtual machine.

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**.

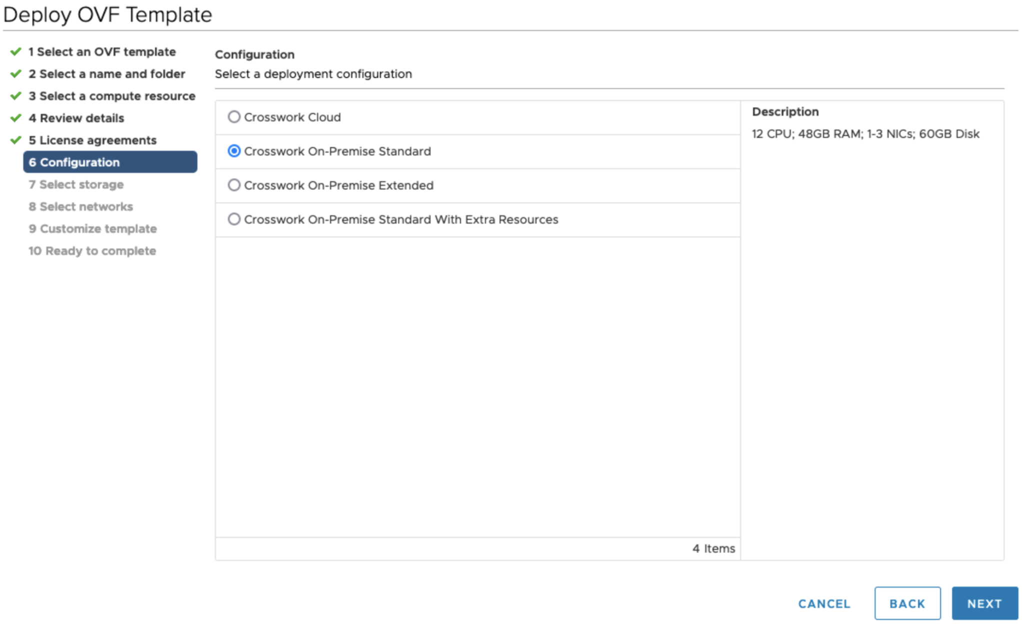
Take a moment to review the OVF template you are deploying.

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 from **Crosswork On-Premise Standard**, **Crosswork On-Premise Extended**, and **Crosswork On-Premise Standard with Extra Resources**. See Mandatory deployment type for Crosswork Data Gateway, on page 16 for more information.

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



Deploy OVF Template

Configuration

Select a deployment configuration

○ Crosswork Cloud

● Crosswork On-Premise Standard

○ Crosswork On-Premise Extended

○ Crosswork On-Premise Standard With Extra Resources

4 Items

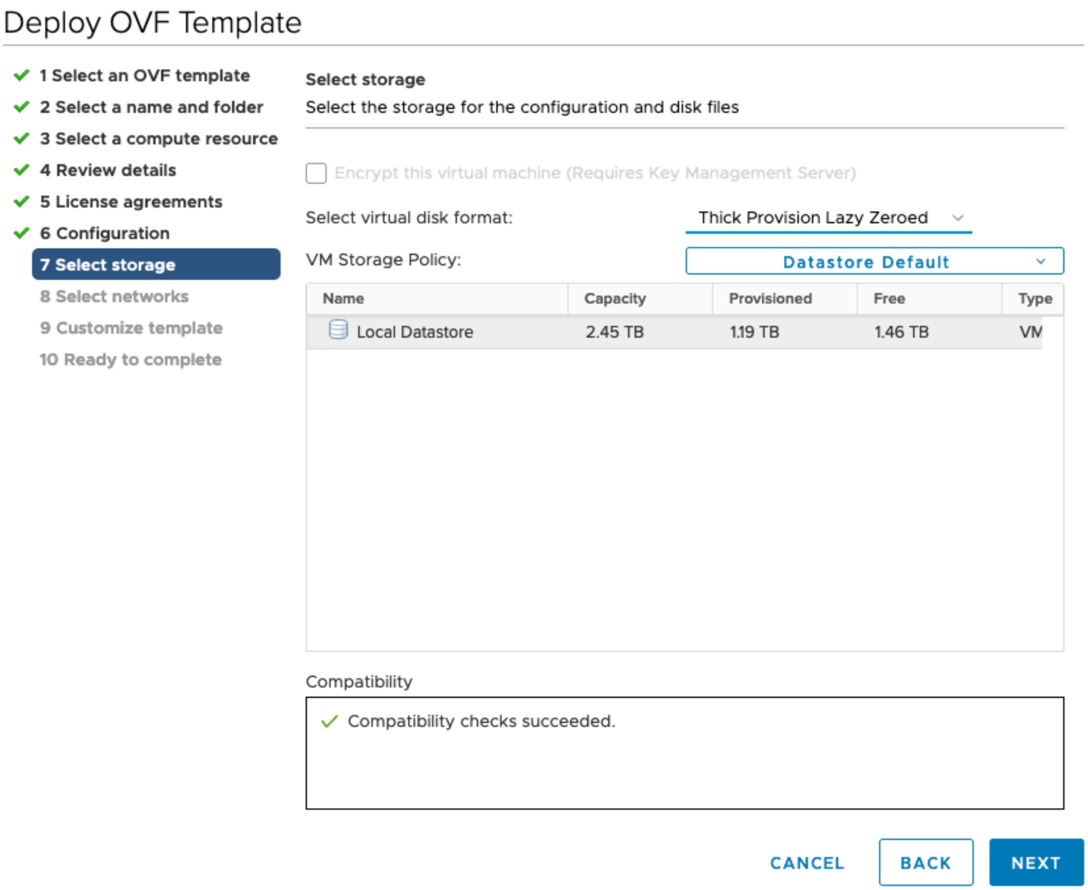
Description

12 CPU; 48GB RAM; 1-3 NICs; 60GB Disk

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 data store you want to use and review its properties to ensure there is enough available storage.



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type
Local Datastore	2.45 TB	1.19 TB	1.46 TB	VM

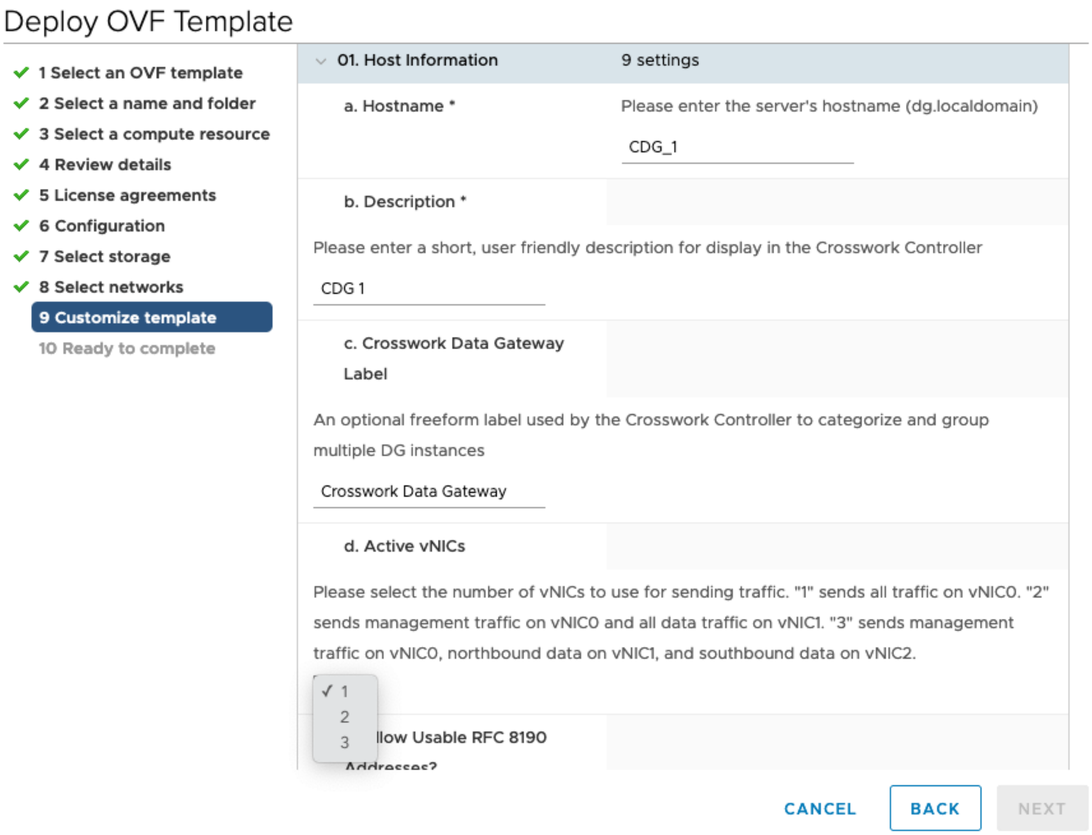
Compatibility

✓ Compatibility checks succeeded.

Step 10 Click **Next** to go to **8 Select networks**, as shown in the following figure. In the drop-down 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*: Table 21: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 72.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 License agreements
✓ 6 Configuration
✓ 7 Select storage
✓ 8 Select networks
9 Customize template
10 Ready to complete

01. Host Information — 9 settings

a. Hostname * — Please enter the server's hostname (dg.localdomain)
CDG_1

b. Description *
Please enter a short, user friendly description for display in the Crosswork Controller
CDG 1

c. Crosswork Data Gateway Label
An optional freeform label used by the Crosswork Controller to categorize and group multiple DG instances
Crosswork Data Gateway

d. Active vNICs
Please select the number of vNICs to use for sending traffic. "1" sends all traffic on vNIC0. "2" sends management traffic on vNIC0 and all data traffic on vNIC1. "3" sends management traffic on vNIC0, northbound data on vNIC1, and southbound data on vNIC2.
✓ 1
2
3

llow Usable RFC 8190 Addresses?

CANCEL BACK NEXT

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.

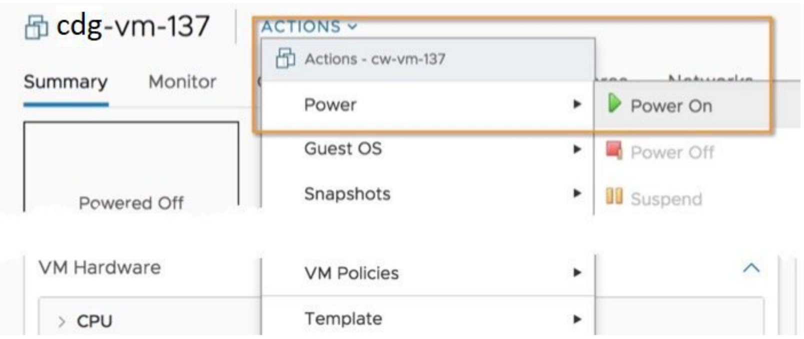
Step 13 Wait for the deployment to finish before continuing. To check the deployment status:

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 log in 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. Make changes to these settings at your own risk.

What to do next

Log in to Cisco Crosswork Data Gateway VM Via vCenter:

1. Locate the VM in vCenter and then right click and select **Open Console**.
2. Enter user name (**`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 log in, the Crosswork 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 the list of mandatory and optional parameters in the command/script as per your requirement and run the OVF Tool. Refer *Table* Table 21: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 72.

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="<image download url>"

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

ActiveVnics="3"

Hostname="<Hostname>"
Vnic0IPv4Address="<Vnic0_ipv4_address>"
Vnic0IPv4Gateway="<Vnic0_ipv4_gateway>"
Vnic0IPv4Netmask="<Vnic0_ipv4_netmask>"
Vnic0IPv4Method="Static"
Vnic1IPv4Address="<Vnic1_ipv4_address>"
Vnic1IPv4Gateway="<Vnic1_ipv4_gateway>"
Vnic1IPv4Netmask="<Vnic1_ipv4_netmask>"
Vnic1IPv4Method="Static"

DNS="<DNS_IP_address>"
NTP="<NTP Server>"
Domain="cisco.com"

ControllerIP="<Controller_IP_Address>"
ControllerPort="<Controller Port"
ControllerSignCertChain="<controller_certificate>"
ControllerCertChainPwd="<password"

Description="Description for Cisco Crosswork Data Gateway VM"
Label="Label for Cisco Crosswork Data Gateway VM"
```

```
dg_adminPassword="<dg-admin_password>"
dg_operPassword="<dg-oper_password>"


ProxyUsername="<username_for_proxy>"
ProxyPassphrase="<password_for_proxy>"


SyslogAddress="<syslog_server_address>"
SyslogPort=<syslog_server_port>
SyslogProtocol="<syslog_server_protocol>"
SyslogTLS=False
SyslogPeerName="<syslog_server_peer_name>"
SyslogCertChain="<syslog_server_root_certificate>"
SyslogCertChainPwd="<password>"

# Please replace this information according to your vcenter setup
VCENTER_LOGIN="<vCenter login details>"
VCENTER_PATH="<vCenter path>"
DS="<DS details>"

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**

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 that you have created containing the command and arguments, run the following command:

```
./cdgovfdeployVM197
```

Once the VM powers up, log into the VM. See Login into Crosswork Data Gateway VM. After you log in, the Crosswork 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) Refer to the *Crosswork Data Gateway 4.0.0 Release notes for On-premise Applications* and download the 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-4.0.0-55-release-20220809.uefi.signed.bin"**.

b) Extract the content of the bin file to the current directory.

```
sh cw-na-dg-4.0.0-55-release-20220809.uefi.signed.bin
```

This command verifies the authenticity of the product. The directory contains the following files as shown here:

```
CDG-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cw-na-dg-4.0.0-55-release-20220809.uefi.tar.gz
README
cisco_x509_verify_release.py
cw-na-dg-4.0.0-55-release-20220809.uefi.signed.bin
cw-na-dg-4.0.0-55-release-20220809.uefi.tar.gz.signature
```

If you encounter any network connectivity issues, skip this verification and perform a manual verification as explained in Step 1 (e).

```
sh cw-na-dg-4.0.0-55-release-20220809.uefi.signed.bin --skip-verification
```

c) Review the contents of the README file in order to understand everything that is in the package and how it will be validated in the following steps.

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

e) 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.

If you are using Python 2.x, use the following command to validate the file:

```
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 to validate the file:

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

f) Unzip the QCOW2 file (**cw-na-dg-4.0.0-55-release-20220809.uefi.tar.gz**) with the following command:

```
tar -xvf cw-na-dg-4.0.0-32-release-20220518.uefi.tar.gz
```

This creates a new directory that will contain the `config.txt` file.

Step 2 **Prepare Cisco Crosswork Data Gateway Service Image for upload to Cisco CSP:**

a) 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 72.

Use these values for the following parameters:

- Deployment
  - Use "Crosswork On-Premise" for Crosswork On-Premise.
- Profile
  - Use "Standard" for Standard deployment.
  - Use "Standard Plus" for Standard Plus 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=
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
```

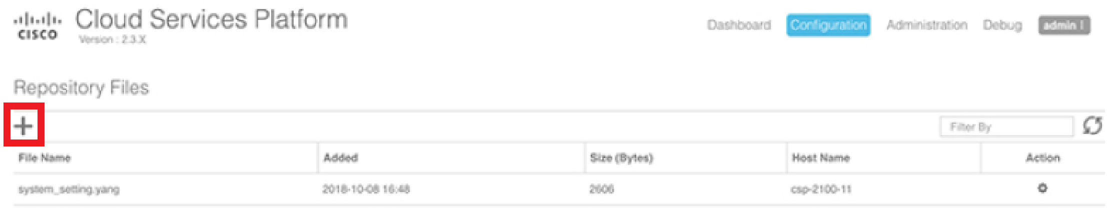
b) Repeat the previous step to create a `config.txt` file for each Crosswork Data Gateway that you plan to deploy (for example, CDG1.txt, CDG2.txt).

Step 3 **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.

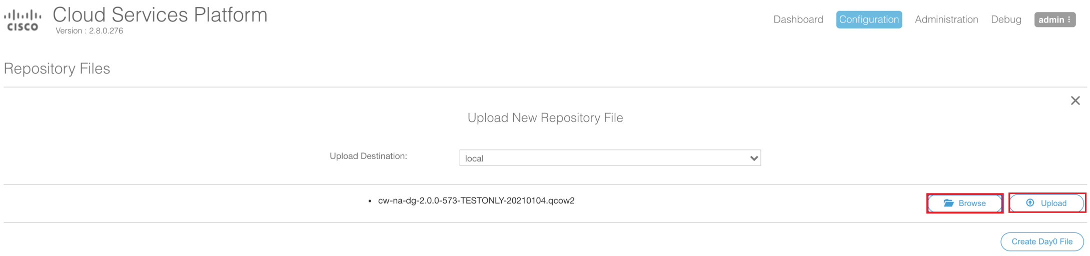


File Name	Added	Size (Bytes)	Host Name	Action
system_setting.yang	2018-10-08 16:48	2606	csp-2100-11	⚙

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.



Upload Destination: local

- cw-na-dg-2.0.0-573-TESTONLY-20210104.qcow2

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

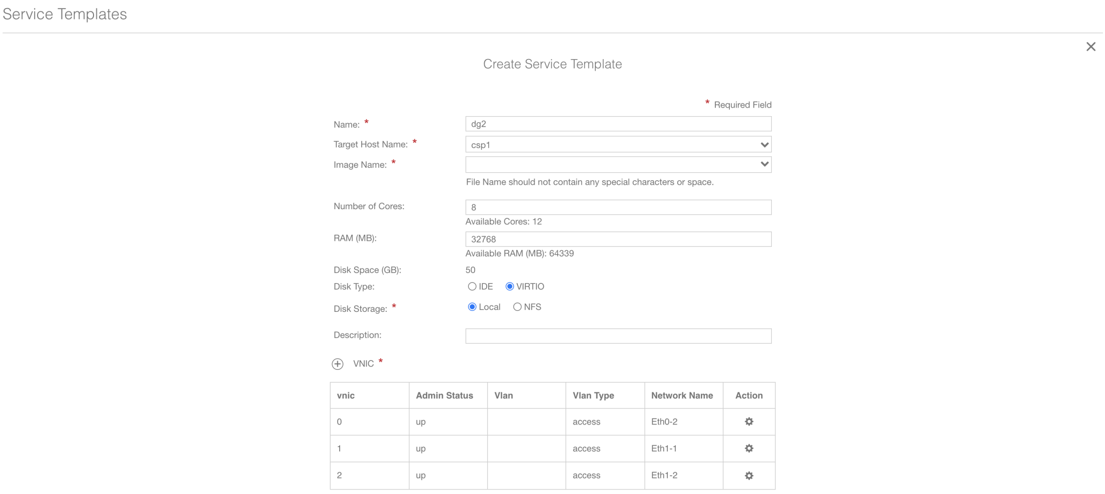
Step 4 **Create Crosswork Data Gateway VM:**

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

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

c) Check **Create Service** option.

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



Service Templates

Create Service Template

* Required Field

Name: * dg2

Target Host Name: * csp1

Image Name: *

File Name should not contain any special characters or space.

Number of Cores: 8

Available Cores: 12

RAM (MB): 32768

Available RAM (MB): 64339

Disk Space (GB): 50

Disk Type: ○ IDE ● VIRTIO

Disk Storage: * ● Local ○ NFS

Description:

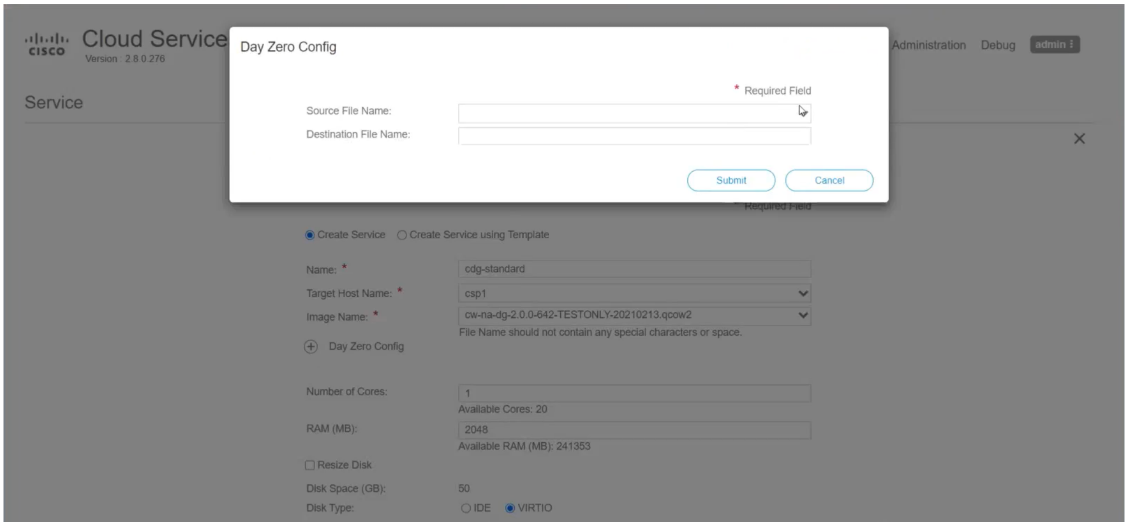
VNIC *

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

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 (`cw-na-dg-4.0.0-18-release-20210409`).

e) Click **Day Zero Config**.



Day Zero Config

* Required Field

Source File Name:

Destination File Name:

● Create Service ○ Create Service using Template

Name: * cdg-standard

Target Host Name: * csp1

Image Name: * cw-na-dg-2.0.0-642-TESTONLY-20210213.qcow2

File Name should not contain any special characters or space.

Day Zero Config

Number of Cores: 1

Available Cores: 20

RAM (MB): 2048

Available RAM (MB): 241353

□ Resize Disk

Disk Space (GB): 50

Disk Type: ○ IDE ● VIRTIO

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

1. From the **Source File Name** drop-down list, select the `config.txt` file that you created for the Crossswork Data Gateway being deployed.

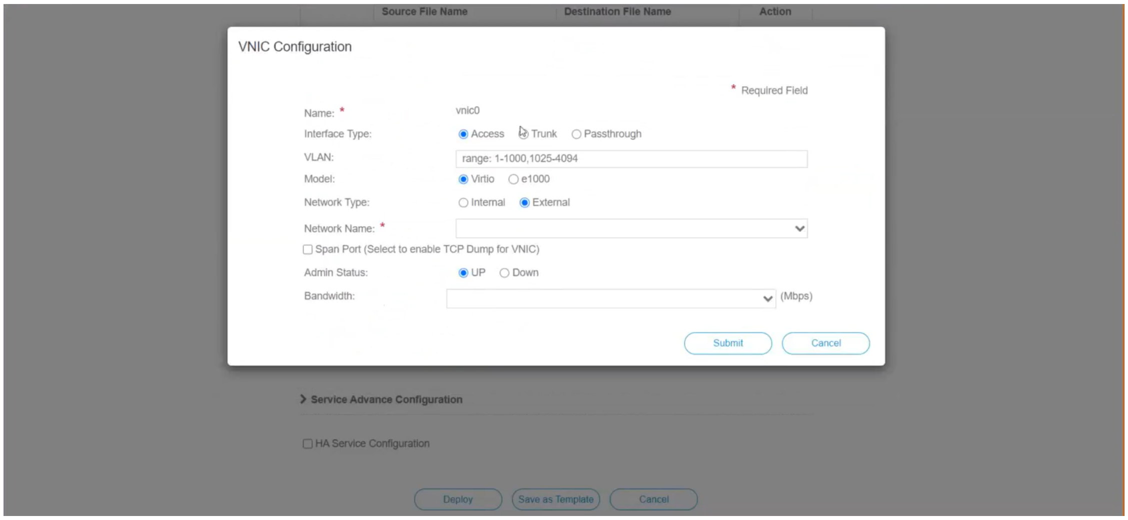
2. In the **Destination File Name** field, specify the name of the day0 destination text file. This must always be "config.txt".

3. Click **Submit**.

f) Enter the values for the following fields:

Field	Description
Number of Cores	Standard: 12 Standard Plus: 20 Extended: 24
RAM (MB)	Standard: 48 Standard Plus: 112 Extended: 128

g) Click + next to **VNIC**.



Source File Name | Destination File Name | Action

VNIC Configuration

* Required Field

Name: * vnic0

Interface Type: ● Access ○ Trunk ○ Passthrough

VLAN: range: 1-1000,1025-4094

Model: ● Virtio ○ e1000

Network Type: ○ Internal ● External

Network Name: *

□ Span Port (Select to enable TCP Dump for VNIC)

Admin Status: ● UP ○ Down

Bandwidth: (Mbps)

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

Note The VNIC Name is set by default.

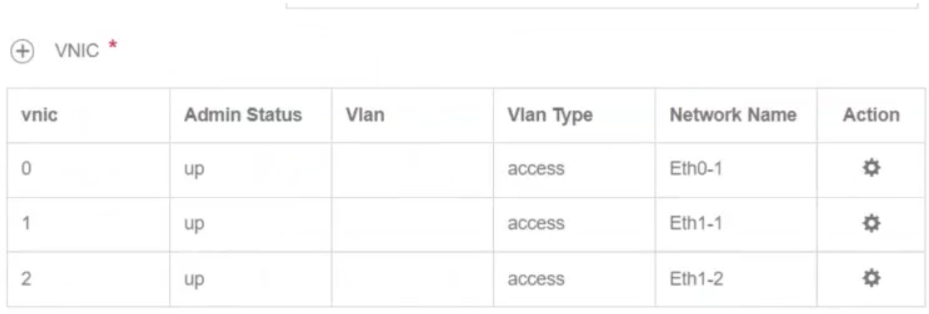
1. Select the **Interface Type** as **Access**.

2. Select the **Model** as **Virtio**.

3. Select the **Network Type** as **External**.

4. Select **Network Name**:

   For a Crosswork Data Gateway that is configured to use 3 VNICs, the configuration will look similar to the following table:



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	⚙

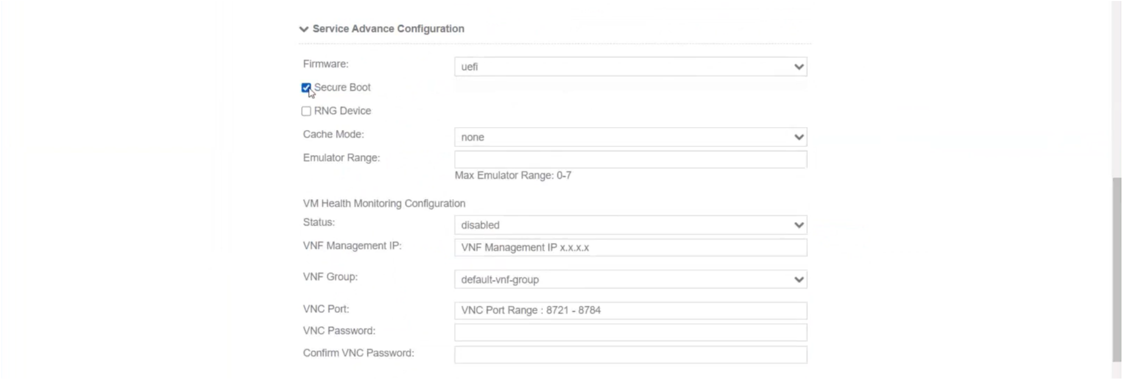
5. Select **Admin Status** as **UP**.

6. Click **Submit**.

7. Repeat Steps **G** (including all the substeps) for each interface you plan to use on the Crosswork Data Gateway (1,2,or 3).

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

Check the **Secure Boot** checkbox.



Service Advance Configuration

Firmware: uefi

☑ Secure Boot

☐ RNG Device

Cache Mode: none

Emulator Range:

Max Emulator Range: 0-7

VM Health Monitoring Configuration

Status: disabled

VNF Management IP: VNF Management IP x.x.x.x

VNF Group: default-vnf-group

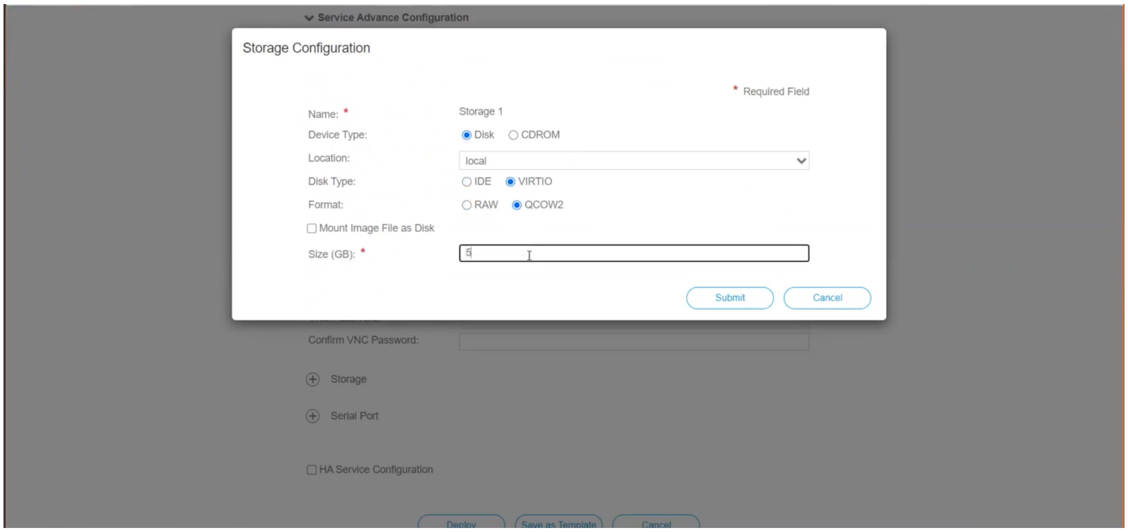
VNC Port: VNC Port Range : 8721 - 8784

VNC Password:

Confirm VNC Password:

i) Click **Storage**.

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



Name: * Storage 1

Device Type: ● Disk ○ CDROM

Location: local

Disk Type: ○ IDE ● VIRTIO

Format: ○ RAW ● QCOW2

□ Mount Image File as Disk

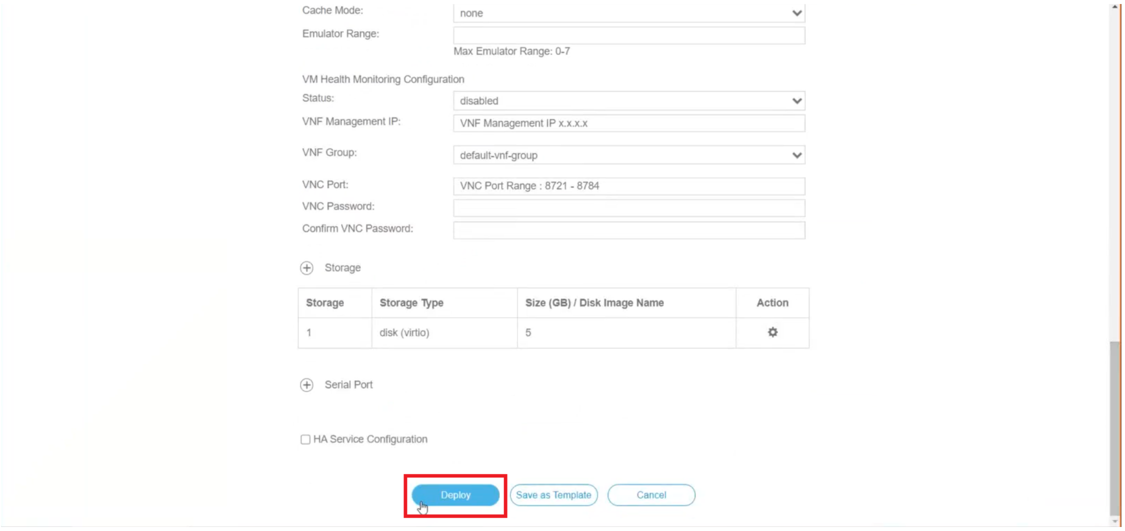
Size (GB): * 5

□ HA Service Configuration

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**.
Mount image file as disk?	Leave this unchecked.
Size (GB)	Enter the disk size (**10** for Standard, **5** for Standard Plus, and **510** for Extended.)

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

j) Click **Deploy**.



Cache Mode:	none
Emulator Range:	 Max Emulator Range: 0-7

VM Health Monitoring Configuration

Status:	disabled
VNF Management IP:	VNF Management IP x.x.x.x
VNF Group:	default-vnf-group
VNC Port:	VNC Port Range : 8721 - 8784
VNC Password:	
Confirm VNC Password:	

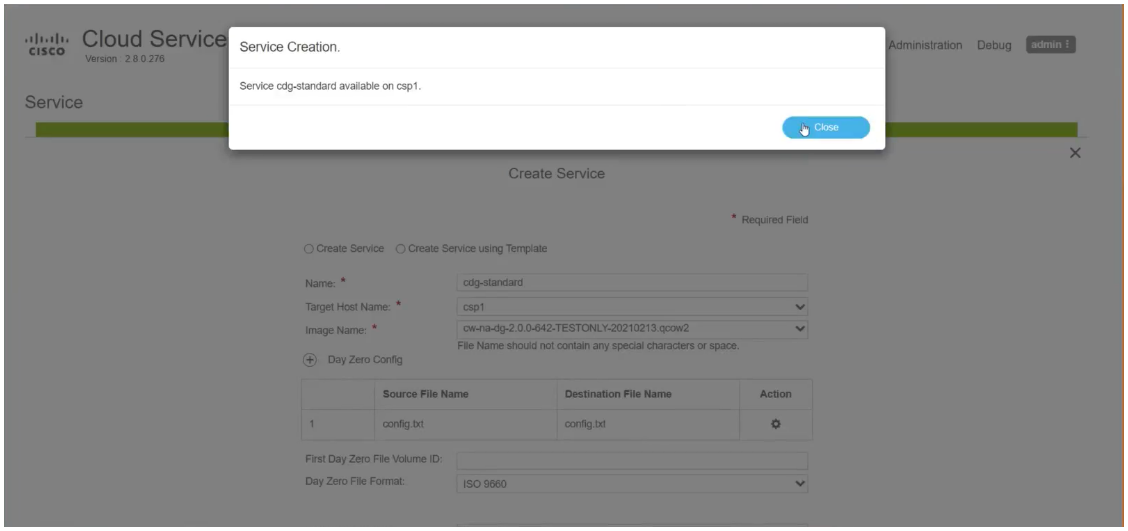
⊕ Storage

Storage	Storage Type	Size (GB) / Disk Image Name	Action
1	disk (virtio)	5	⚙

⊕ Serial Port

□ HA Service Configuration

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



Service Creation.

Service cdg-standard available on csp1.

Create Service

* Required Field

○ Create Service ○ Create Service using Template

Name: *	cdg-standard
Target Host Name: *	csp1
Image Name: *	cw-na-dg-2.0.0-642-TESTONLY-20210213.qcow2 File Name should not contain any special characters or space.

⊕ Day Zero Config

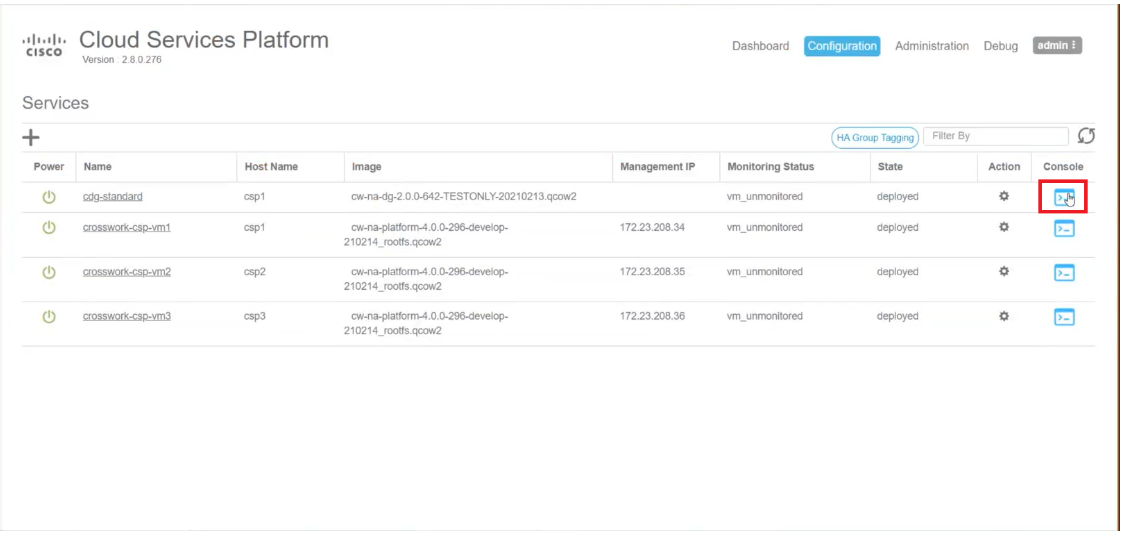
	Source File Name	Destination File Name	Action
1	config.txt	config.txt	⚙

First Day Zero File Volume ID:	
Day Zero File Format:	ISO 9660

Step 5 **Deploy Cisco Crosswork Data Gateway service:**

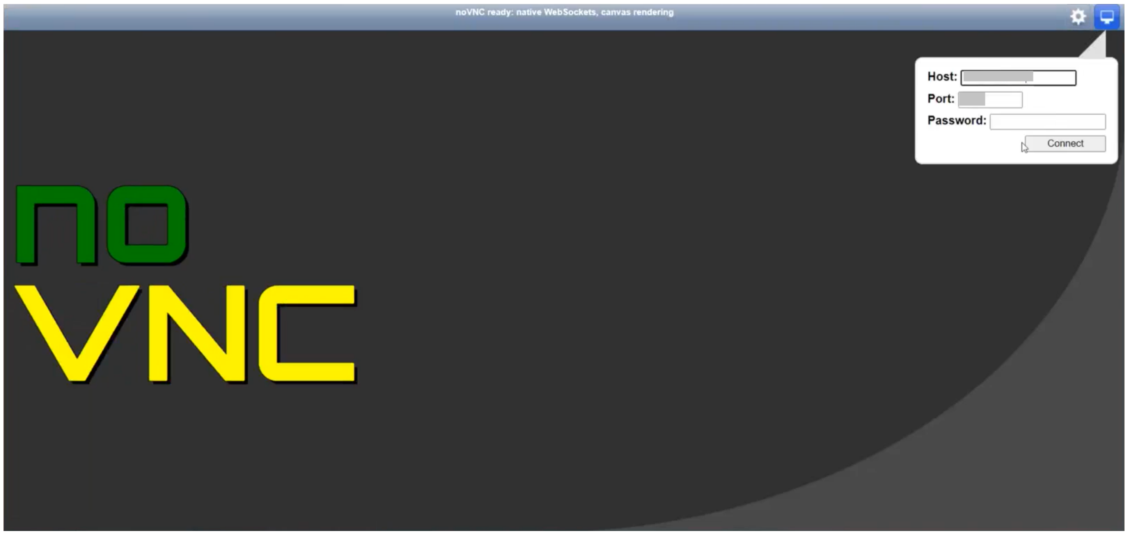
a) Go to **Configuration** > **Services**.

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



Power	Name	Host Name	Image	Management IP	Monitoring Status	State	Action	Console
⏻	cdg-standard	csp1	cw-na-dg-2.0.0-642-TESTONLY-20210213.qcow2		vm_unmonitored	deployed	⚙	>_
⏻	crosswork-csp-vm1	csp1	cw-na-platform-4.0.0-296-develop-210214_rootfs.qcow2	172.23.208.34	vm_unmonitored	deployed	⚙	>_
⏻	crosswork-csp-vm2	csp2	cw-na-platform-4.0.0-296-develop-210214_rootfs.qcow2	172.23.208.35	vm_unmonitored	deployed	⚙	>_
⏻	crosswork-csp-vm3	csp3	cw-na-platform-4.0.0-296-develop-210214_rootfs.qcow2	172.23.208.36	vm_unmonitored	deployed	⚙	>_

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



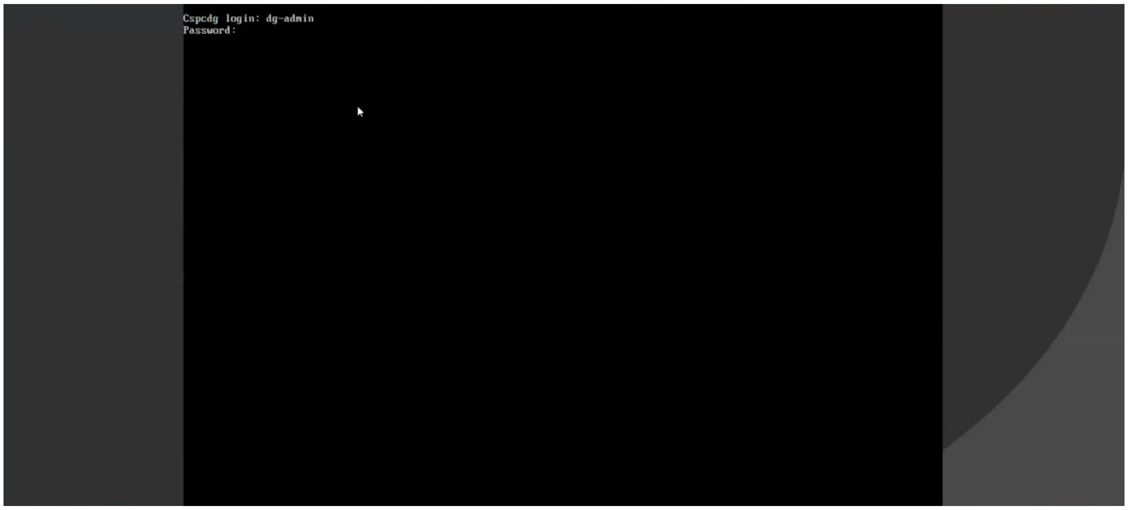
noVNC ready: native WebSockets, canvas rendering

Host:

Port:

Password:

d) Enter user name and password after the Crosswork Data Gateway server connects.



```
Cspcdg login: dg-admin
Password:
```

The Cisco Crosswork Data Gateway console is available.

After you log in, Crossway Data Gateway presents you with the welcome screen and the Interactive Console to indicate that the installation has 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 101
- Log Out of Crosswork Data Gateway VM, on page 104

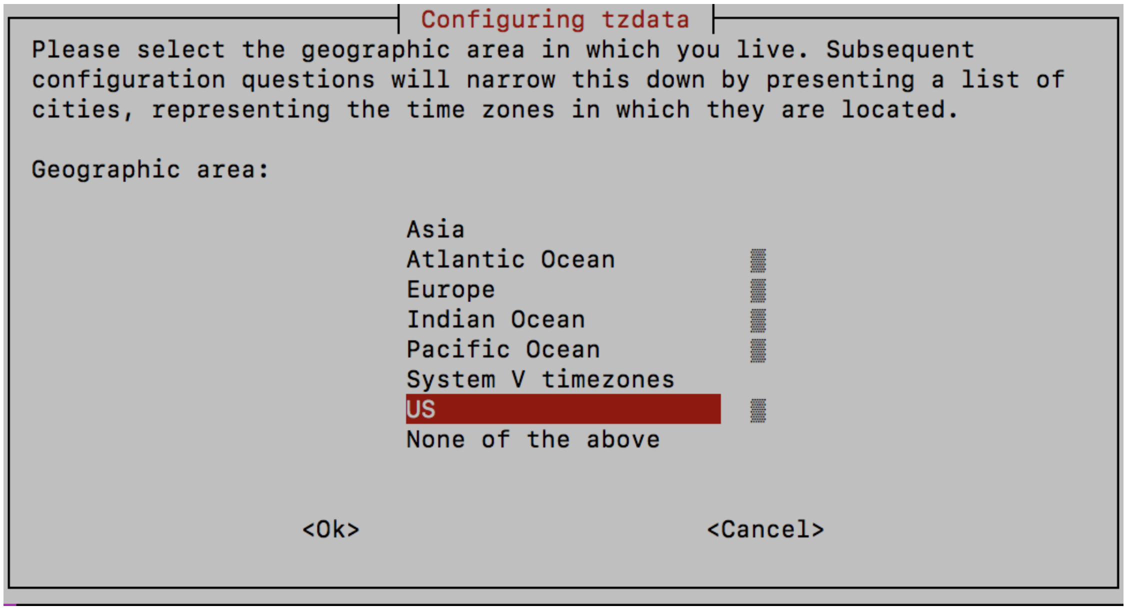
Configure Timezone of the Crosswork Data Gateway VM

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.



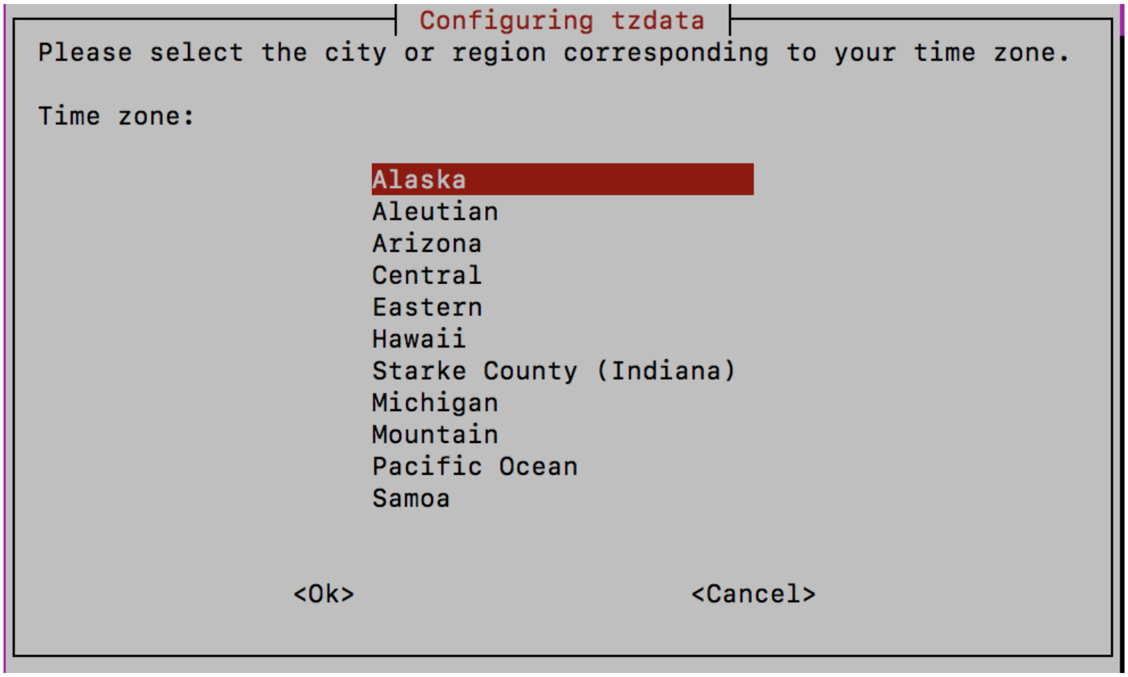
```
Configuring tzdata
Please select the geographic area in which you live. Subsequent
configuration questions will narrow this down by presenting a list of
cities, representing the time zones in which they are located.

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 in to the Crosswork Data Gateway VM in one of the following ways:

- Access Crosswork Data Gateway VM from SSH, on page 103
- Access Crosswork Data Gateway Through vCenter, on page 103
- Access Crosswork Data Gateway Through Cisco CSP, on page 104

To log out of the Crosswork Data Gateway VM, see Log Out of Crosswork Data Gateway VM, on page 104.

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.

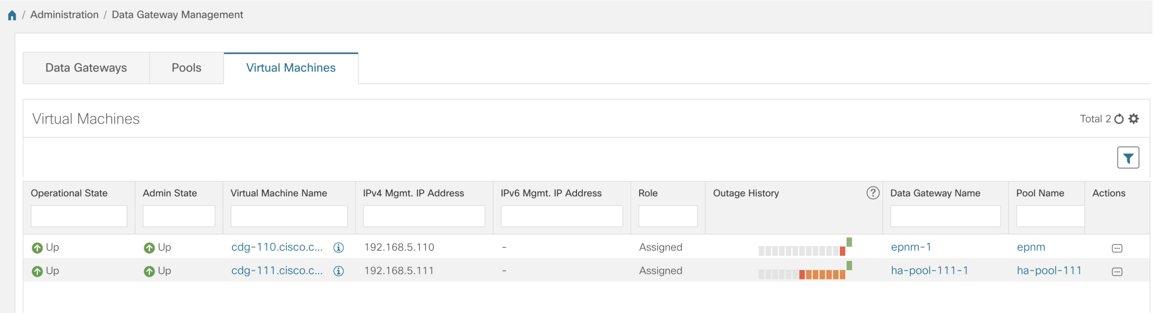
To verify if the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork:

1. Log into the Cisco Crosswork UI. See Log into the Cisco Crosswork UI, on page 65.
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.



Operational State	Admin State	Virtual Machine Name	IPv4 Mgmt. IP Address	IPv6 Mgmt. IP Address	Role	Outage History	Data Gateway Name	Pool Name	Actions
Up	Up	cdg-110.cisco.c...	192.168.5.110	-	Assigned		epnm-1	epnm	
Up	Up	cdg-111.cisco.c...	192.168.5.111	-	Assigned		ha-pool-111-1	ha-pool-111	

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 show-tech (**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 22: 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"	

Issue	Action
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**. The show-tech is now encrypted with a file extension ending with .tar.xz. 3. Run the following command to decrypt the show-tech file. `openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string>` 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"	
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.

Issue	Action
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 password).

The certificate file is imported.

Step 6 Verify that the certificate was installed successfully. SeeView the Controller Signing Certificate File, on page 109.

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 (*.tar.gz) 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.

The Crosswork Network Controller applications are packaged as **Essentials** and **Advantage** bundles (*.bin) in cisco.com.

Table 23: Crosswork Network Controller Packages

Crosswork Network Controller Essentials package	Crosswork Network Controller Advantage package
Crosswork Optimization Engine Crosswork Active Topology	Crosswork Optimization Engine Crosswork Active Topology Cisco Crosswork Service Health Cisco Crosswork Health Insights Cisco Crosswork Change Automation Crosswork Zero Touch Provisioning Cisco Element Management System (EMS) Services

Before you begin

Ensure that all requirements of your application are met. For more information, see Installation Dependencies for Cisco Crosswork Products, on page 23.

Important If you intend to use the Crosswork Network Controller solution and have downloaded and added the solution package (Essential or Advantage), please follow the installation sequence below:

- Crosswork Optimization Engine must be installed before installing Crosswork Active Topology.
- Crosswork Active Topology must be installed before installing Crosswork Service Health or Common EMS Service.

Crosswork Change Automation, Crosswork Health Insights, and Crosswork Zero Touch Provisioning can be installed independently, in any order, with or without Crosswork Optimization Engine and/or Crosswork Active Topology.

Step 1 **Download and validate the CAPP files:**

a) Navigate to cisco.com and locate the application CAPP files that you require.

b) If you are planning to use Crosswork Network Controller, download the relevant package (*.bin). For the purpose of these instructions, we will use the file name as **"cw-na-cncadvantage-4.0.0-51-release-220809.signed.bin"**.

To validate the downloaded bundle file, use the following command from a Linux-based machine with access to Cisco network:

```
$ sh <image.signed.bin>
```

Example:

```
[test@cw-build sample]$ sh  cw-na-cncadvantage-4.0.0-51-release-220809.signed.bin
Unpacking...
Verifying signature...
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of cw-na-cncadvantage-4.0.0-51-release-220809.tar.gz using
CW-CCO_RELEASE.cer
```

If the **sh** command fails due to any network connectivity issues, you can use the following command to skip verification and extract the bundle.

```
$ sh <image.signed.bin> --skip-verification
```

This new directory will contain the installer image (e.g. **cw-na-platform-installer-4.3.0-88-release-220809.tar.gz**) and files necessary to validate the image.

Example:

```
[test@cw-build sample]$ sh cw-na-cncadvantage-4.0.0-51-release-220809.signed.bin --skip-verification
Unpacking...
[test@cw-build sample]$ ls
CW-CCO_RELEASE.cer             cisco_x509_verify_release.py3
cw-na-cncadvantage-4.0.0-51-release-220809.tar.gz              README
cisco_x509_verify_release.py   cw-na-cncadvantage-4.0.0-51-release-220809.signed.bin
cw-na-cncadvantage-4.0.0-51-release-220809.tar.gz.signature
```

Use the following command to manually 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 to validate the file:

```
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 to validate the file:

```
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.

c) If you are planning to use individual CAPP files, hover over the relevant file and copy the MD5 or SHA512 checksum to your clip board.

Download the CAPP files to a server that can be reached from the Crosswork server. Run a tool of your choice to calculate the checksum, and the compare the checksum value in your dowloaded file with the value you copied in the clip board.

For example, on a MAC you can use the **md5** command to calculate the MD5 sum on a file:

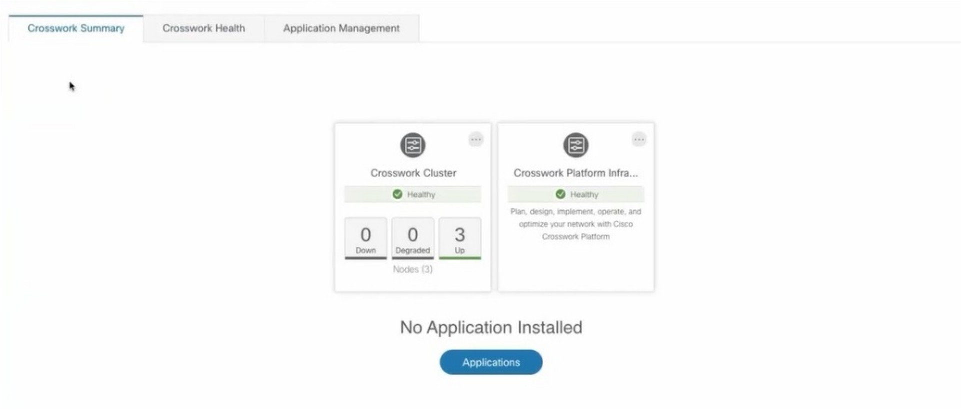
```
md5 cw-na-ztp-3.0.3-3-release-220614.tar.gz
```

```
ff47a72ed7dc4fc4be388db3a43fa13f
```

Verify that the result value matches with the posted value on cisco.com.

Step 2 **Add the downloaded CAPP file to Crosswork:**

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

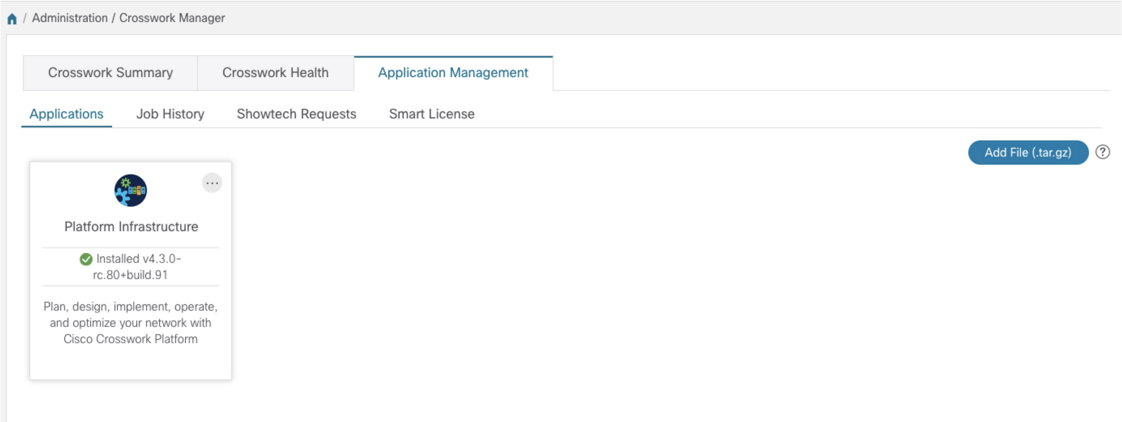


Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

No Application Installed

You can click on the tiles to get more information.

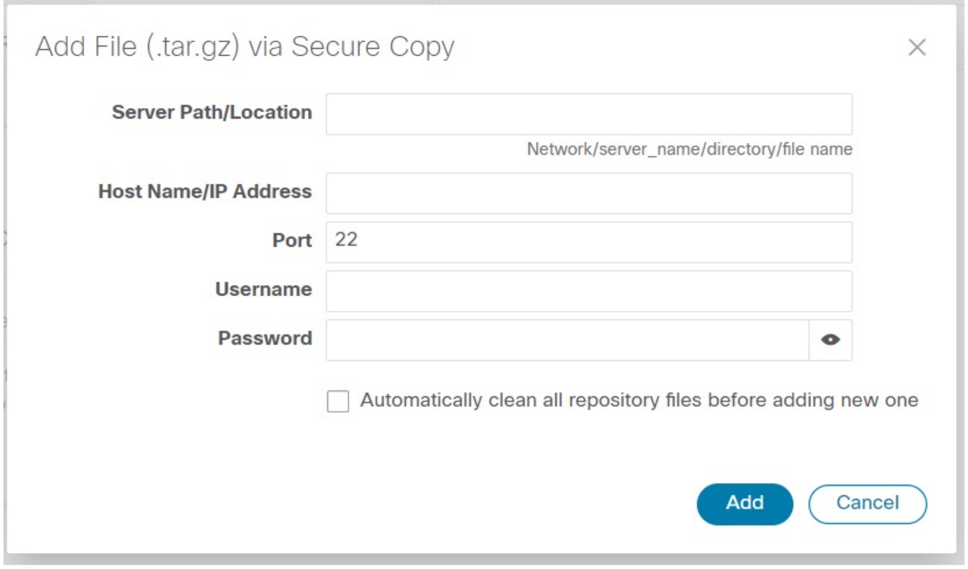
b) To install an application or application bundle, click on **Applications** button. Alternately, click on the **Application Management** tab.



Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

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

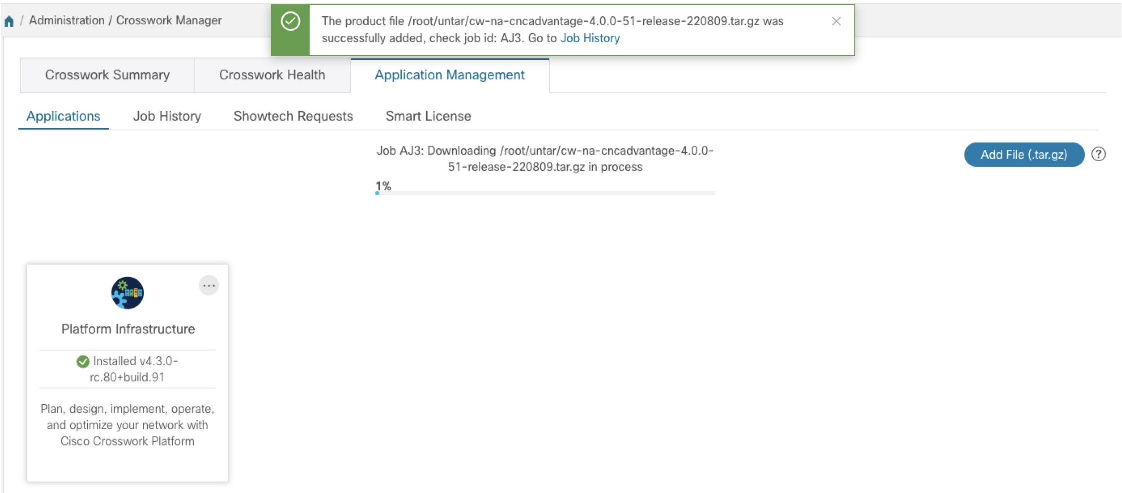
d) In the Add File dialog box, enter the relevant information and click **Add**.


Add File (.tar.gz) via Secure Copy
Server Path/Location
Network/server_name/directory/file name
Host Name/IP Address
Username
Password
Add
Cancel

Port: 22

□ Automatically clean all repository files before adding new one

The add operation progress is displayed on the **Applications** screen. You can also view the installation progress in the **Job History** tab.



The product file /root/untar/cw-na-cncadvantage-4.0.0-51-release-220809.tar.gz was successfully added, check job id: AJ3. Go to Job History

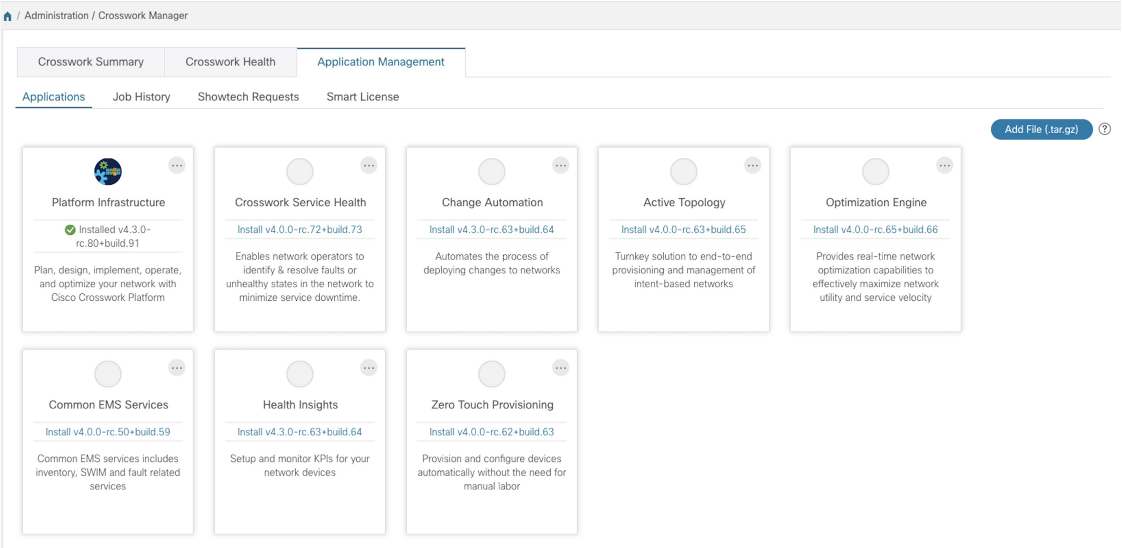
Job AJ3: Downloading /root/untar/cw-na-cncadvantage-4.0.0-51-release-220809.tar.gz in process

Installed v4.3.0-rc.80+build.91

Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Note When loading an application bundle (**Essentials** or **Advantage**), the loading process may stop at 50% for a while depending on the resources your host platform has available.

The newly added application file (or application files, if you added a bundle) is displayed as a tile on the **Applications** screen.



Platform Infrastructure — Installed v4.3.0-rc.80+build.91 — Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Crosswork Service Health — Install v4.0.0-rc.72+build.73 — Enables network operators to identify & resolve faults or unhealthy states in the network to minimize service downtime.

Change Automation — Install v4.3.0-rc.63+build.64 — Automates the process of deploying changes to networks

Active Topology — Install v4.0.0-rc.63+build.65 — Turnkey solution to end-to-end provisioning and management of intent-based networks

Optimization Engine — Install v4.0.0-rc.65+build.66 — Provides real-time network optimization capabilities to effectively maximize network utility and service velocity

Common EMS Services — Install v4.0.0-rc.50+build.59 — Common EMS services includes inventory, SWIM and fault related services

Health Insights — Install v4.3.0-rc.63+build.64 — Setup and monitor KPIs for your network devices

Zero Touch Provisioning — Install v4.0.0-rc.62+build.63 — Provision and configure devices automatically without the need for manual labor

Step 3 **Install the Application CAPP file:**

a) Click on the **Install** prompt on the application tile. You can also click ⋯ on the tile, and select the **Install** option from the drop down list.

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.

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.

b) 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 4 Repeat step 3 for installing any remaining applications.

Step 5 (Optional) Click ⋯ on the application tile, and select the **View Details** option to view details of the installed application.

Step 6 Once an application (or all applications) have been installed, check the health of the environment to make sure all the applications are healthy. It can take up to an hour for all the processes that make launch and for the applications to report as healthy. If after an hour a newly installed application is not healthy after an hour, contact the Cisco Customer Experience team.

CHAPTER 6

Upgrade Cisco Crosswork

This chapter contains the following topics:

Cisco Crosswork Upgrade Workflow

This section provides the high-level workflow for upgrading Cisco Crosswork from release 4.1 to release 4.3. This includes upgrading Cisco Crosswork cluster, Cisco Crosswork Data Gateway and Crosswork Applications to Release 4.3, within a single maintenance window.

You can upgrade to Cisco Crosswork 4.3 in the following methods:

1. Upgrade Using Same Hardware, on page 119
2. Upgrade Using Parallel Hardware, on page 129

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 4.1 to 4.3 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.
- After a successful migration, you must perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepency.

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 137.

Upgrade Requirements

This section explains the requirements for upgrading the Cisco Crosswork if you are using the Crosswork Optimization Engine.

If you have enabled feature packs (LCM, Bandwidth Optimization, or BWoD) in Crosswork Optimization Engine 3.0 and want to upgrade to Crosswork Optimization Engine 4.0, you must perform the following tasks prior to upgrading:

LCM and Bandwidth Optimization (BWOpt)

- From the LCM or Bandwidth Optimization **Configuration** page:

  1. Set the **Delete Tactical SR Policies when Disabled** option to **False**. This task must be done prior to disabling LCM or BWOpt so that tactical polices deployed by LCM or BWOpt remain in the network after the upgrade.

  2. Set the **Enable** option to **False**. If LCM or BWOpt remains enabled, there is a chance that tactical policies may be deleted after the upgrade.

  3. Note all options (Basic and Advanced) in the LCM or BWOpt **Configuration** page so that you can confirm the same configuration has been migrated after the upgrade.

- Export the current list of interfaces managed by LCM or BWOpt (**Traffic Engineering** > **Local Congestion Mitigation** or **Bandwidth Optimization** > **Interface Threshold** > **Export** icon). Confirm the interfaces are valid by reimporting the CSV file without errors. For more information, see "Add Individual Interface Thresholds" in the Cisco Crosswork Optimization Engine 4.0 User Guide.

- After the upgrade, wait until the **Traffic Engineering** page shows all the nodes and links before enabling LCM or BWOpt.

Note:

After the system is stable and before enabling domains for LCM, confirm that the migration of previously monitored interfaces has completed and that each domain has the expected configuration options.

1. Navigate to **Administration** > **Alarms** > **All** > **Events** and enter **LCM** to filter the **Source** column.

2. Look for the following event: "Migration complete. All migrated LCM interfaces and policies are mapped to their IGP domains". If this message does not appear wait for the **Congestion Check Interval** period (set in the LCM **Configuration** page), then restart LCM (**Administration** > **Crosswork Manager** > **Optimization Engine** > **optima-lcm** > **...** > **Restart**).

3. Wait until the optima-lcm service changes from Degraded to Healthy state.

4. For each domain, navigate to the **Configuration** page and verify the options have been migrated successfully. If the domain configurations are incorrect, restart LCM (**Administration** > **Crosswork Manager** > **Optimization Engine** > **optima-lcm** > **...** > **Restart**).

5. Check the **Events** page for the event mentioned above and the **Configuration** page to verify the options.

Note

- If the confirmation message does not appear or domain configuration options are incorrect, then contact Cisco Technical support and provide them with showtech information and the exported Link Management CSV file.
- You can also manually add missing interfaces that were previously monitored or update domain configuration options *after* the system is stable.

BWoD

- Set the **Enable** option to **False**. If BWoD remains enabled, there is a chance that tactical policies may be deleted after the upgrade.
- Note all options (Basic and Advanced) in the BWoD **Configuration** page so that you can confirm the same configuration has been migrated after the upgrade.
- After the upgrade, wait until the **Traffic Engineering** page shows all the nodes and links before enabling BWoD.

Upgrade Using Same Hardware

This section explains how to migrate to Cisco Crosswork 4.3 using the existing cluster.

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 3.0 VMs, on page 120
2. Create Backup and Shut Down Cisco Crosswork 4.1, on page 120
3. Install the Cisco Crosswork 4.3 Cluster, on page 123

   Note

   While the cluster installation is in progress, you must upgrade NSO to version 5.7.5.1. The process to upgrade NSO is not covered in this document. For more information, see the relevant Cisco NSO documentation. Additionally, if you are planning to use Cisco Optimization Engine individually or as part of the Cisco Network Controller solution, upgrade your SR-PCE to the supported version as mentioned in the Crosswork Network Controller Release Notes.

4. Install Cisco Crosswork 4.3 Applications, on page 123

   Note

   You are recommended to download and validate the application CAPP files (See Install Crosswork Applications) before starting the actual upgrade process. This will reduce your system downtime as opposed to downloading the CAPP files midway through the upgrade process.

5. Migrate the Cisco Crosswork 4.1 backup to Cisco Crosswork 4.3, on page 124

6. Upgrade to Crosswork Data Gateway 4.0, on page 125

7. Post-upgrade Checklist, on page 128

Shut Down Cisco Crosswork Data Gateway 3.0 VMs

This is the first stage of the upgrade workflow.

Note When Crosswork Data Gateway VMs are shut down, 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 4.1 UI. In the **Pools** tab, for each pool listed here, take a screenshot to make a note of the active, spare, and unassigned VMs in the pool. This information is useful during Upgrade to Crosswork Data Gateway 4.0, on page 125.

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

Step 2 Shut down the Crosswork Data Gateway 3.0 VMs.

a) Log in to the Crosswork Data Gateway 3.0 VM. See Access Crosswork Data Gateway VM from SSH, on page 103.

   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 4.1

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.
- After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.
- 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 4.1, download a copy of the package to your system. You will need to upload the package after you complete migrating to Cisco Crosswork 4.3. See Post-upgrade Checklist, on page 128 for more infomation.
- If you have modified Cisco Crosswork 4.1 to include third-party device types, you must download the third-party device configuration file, and re-apply it to Cisco Crosswork 4.3. 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** > **Domain Identifier <domain_id>** > **Interface Thresholds** > **Export** OR **Traffic Engineering** > **Bandwidth Optimization** > **Interface Thresholds** > **Export** icon). Follow the steps documented in Upgrade Requirements, on page 118.

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 4.1 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 4.1 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 4.3 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. 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 After the backup operation is completed, navigate to the destination SCP server directory and ensure that the backup file is created. You will require this backup file in the later stages of the upgrade process.

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 5.7.5.1.

Install the Cisco Crosswork 4.3 Cluster

This is the third stage of the upgrade workflow. After the successful backup of Cisco Crosswork 4.1, proceed to install Cisco Crosswork 4.3 cluster.

Note The number of VM nodes installed in Cisco Crosswork 4.3 must be equal or more than the number of VM nodes in Cisco Crosswork 4.1.

Note While the cluster installation is in progress, you must upgrade NSO to version 5.7.5.1. The process to upgrade NSO is not covered in this document. For more information, see the relevant Cisco NSO documentation. Additionally, if you are planning to use Cisco Optimization Engine individually or as part of the Cisco Network Controller solution, upgrade your SR-PCE to the supported version as mentioned in the Crosswork Network Controller Release Notes.

Before you begin

- Make sure that your environment meets all the requirements specified under Cisco Crosswork Infrastructure Requirements, on page 7.

Step 1 Install Cisco Crosswork 4.3 cluster using any of the installation methods described in Install the Crosswork Cluster, on page 31.

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 4.3 Applications

This is the fourth stage of the upgrade workflow. After the successful installation of Cisco Crosswork 4.3 cluster, proceed to install Cisco Crosswork 4.3 applications.

Note You can only install 4.3 versions of the Cisco Crosswork applications that were backed up during Create Backup and Shut Down Cisco Crosswork 4.1, on page 120.

Step 1 Install Cisco Crosswork 4.3 applications using the steps described in Install Crosswork Applications, on page 111.

Step 2 After the applications are successfully installed, check the health of the Cisco Crosswork 4.3 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 4.1 backup to Cisco Crosswork 4.3

This is the fifth stage of the upgrade workflow. After the successfully installing Cisco Crosswork 4.3 applications, proceed to migrate the backup of Cisco Crosswork 4.1 on Cisco Crosswork 4.3 cluster.

Before you begin

Before you begin, ensure that you have:

- The hostname or IP address and the port number of a secure destination SCP server used in Create Backup and Shut Down Cisco Crosswork 4.1, on page 120.
- The name and path of the backup file created in Create Backup and Shut Down Cisco Crosswork 4.1, on page 120.
- User credentials with file read and write permissions to the directory.

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 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 4.1, on page 120.

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

Step 3 **Migrate the Cisco Crosswork 4.1 backup on the Cisco Crosswork 4.3 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 4.1, on page 120) 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, please wait for a few minutes and 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 might become temporarily unavailable during the data migration operation. When the Crosswork UI is down, you can view the job status in the Grafana dashboard. The Grafana link is available as *View Data Migration Process Dashboard* option on the right side of the Job Details window.

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

Step 4 After the data migration is successfully completed, check the health of the Cisco Crosswork 4.3 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 Crosswork Data Gateway 4.0

This is the final stage of the upgrade workflow. Ensure that the migration is complete and Cisco Crosswork 4.3 UI is available before you proceed with installing Crosswork Data Gateway (CDG) 4.0.

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.

Crosswork Data Gateway functions as a passive device in the network. The Crosswork Data Gateway upgrade process consists of the following steps replacing all Crosswork Data Gateway 3.0 VMs with Crosswork Data Gateway 4.0 VMs in the network.

Important Step 8 in this procedure requires you log out of Cisco Crosswork 4.3 and log in again after verifying the deployment and enrollment of the 4.0 CDG VMs with Cisco Crosswork 4.3. After you log in, an **Action to be taken** window appears prompting you to confirm that the upgrade is complete. Do not click **Acknowledge** unless you have completed all the verification steps mentioned in Step 3, Step 4 and Step 5 in the procedure.

Step 1 Log out of Cisco Crosswork 4.3 and log in again.

Step 2 After you log in, an **Action to be taken** window appears. Close this window and do not click **Acknowledge**.

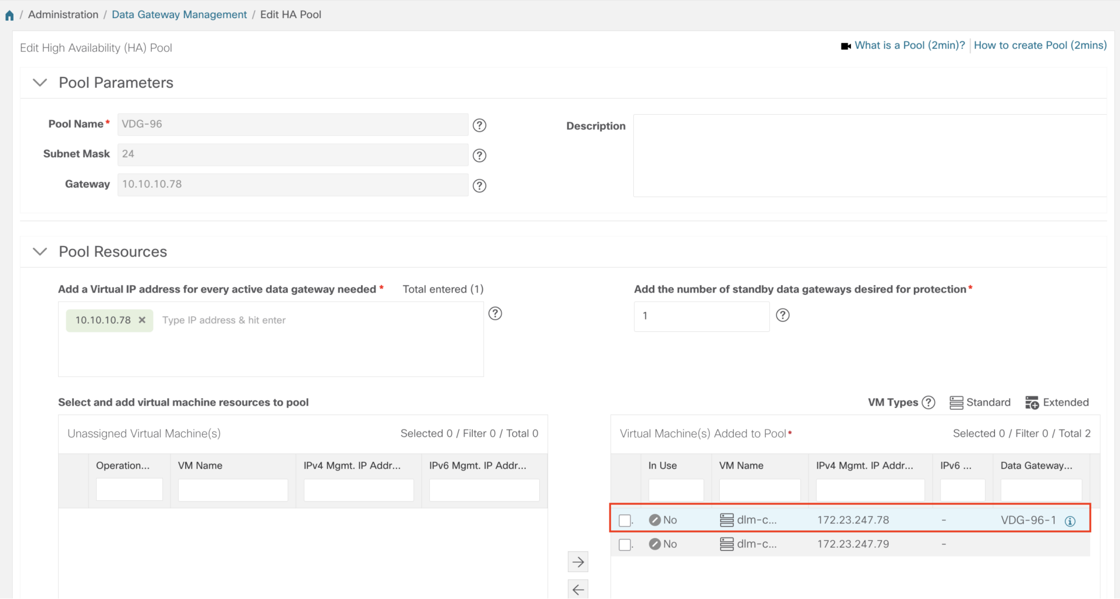
Step 3 Install new Cisco Crosswork Data Gateway 4.0 VMs with the same number and the same information (management interface importantly) as the Crosswork Data Gateway 3.0 VMs. Follow the steps in the Install Cisco Crosswork Data Gateway, on page 71.

Step 4 Wait for about 5 minutes and navigate to **Administration** > **Data Gateway Management**.

Step 5 Check the **Virtual Machines** tab to verify that the new Crosswork Data Gateway 4.0 VMs are enrolled with Cisco Crosswork 4.3 and have the **Admin State** as **Up** and **Operational State** as **Not Ready**.

Step 6 After the **Operational State** of the VMs changes to **Ready**, navigate to the **Pools** tab and verify that all the Crosswork Data Gateway pools from Cisco Crosswork 4.1, are listed here. Edit each Crosswork Data Gateway pool to verify that the active Crosswork Data Gateway is same as one that you noted in Cisco Crosswork 4.1.

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


/ Administration / Data Gateway Management / Edit HA Pool
Edit High Availability (HA) Pool
What is a Pool (2min)? | How to create Pool (2mins)
Pool Parameters
Pool Resources
Select and add virtual machine resources to pool
VM Types
Standard
Extended
Unassigned Virtual Machine(s)
Virtual Machine(s) Added to Pool*

Pool Name* VDG-96

Subnet Mask 24

Gateway 10.10.10.78

Description

Add a Virtual IP address for every active data gateway needed* Total entered (1)

10.10.10.78 × Type IP address & hit enter

Add the number of standby data gateways desired for protection* 1

Unassigned Virtual Machine(s) — Selected 0 / Filter 0 / Total 0

Operation...	VM Name	IPv4 Mgmt. IP Addr...	IPv6 Mgmt. IP Addr...

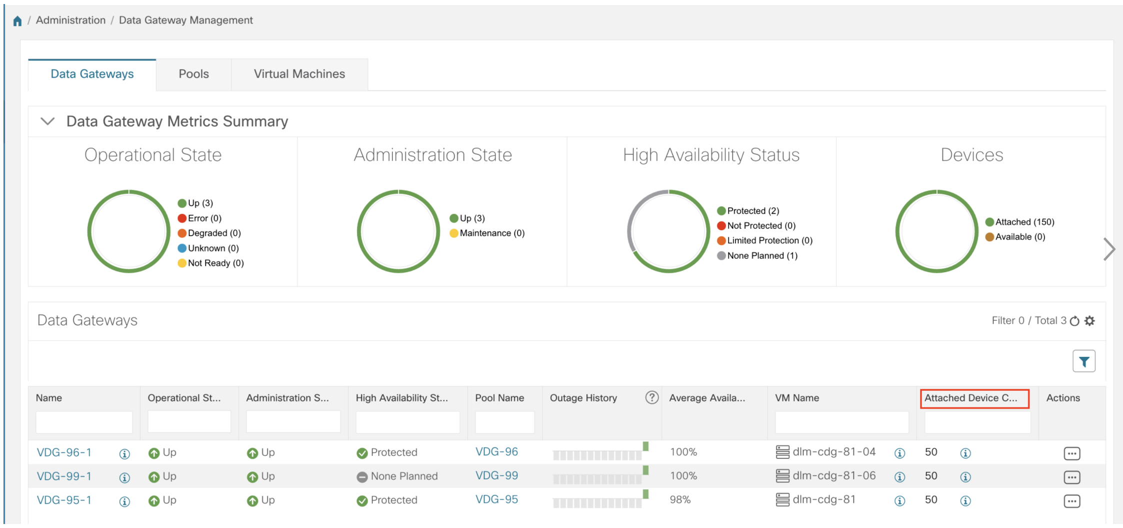
Virtual Machine(s) Added to Pool* — Selected 0 / Filter 0 / Total 2

	In Use	VM Name	IPv4 Mgmt. IP Addr...	IPv6 ...	Data Gateway...
□	No	dlm-c...	172.23.247.78	-	VDG-96-1
□	No	dlm-c...	172.23.247.79	-	

Step 7 **Verify that devices are attached to the Crosswork Data Gateways 4.0 in the Cisco Crosswork 4.3 UI.**

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

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

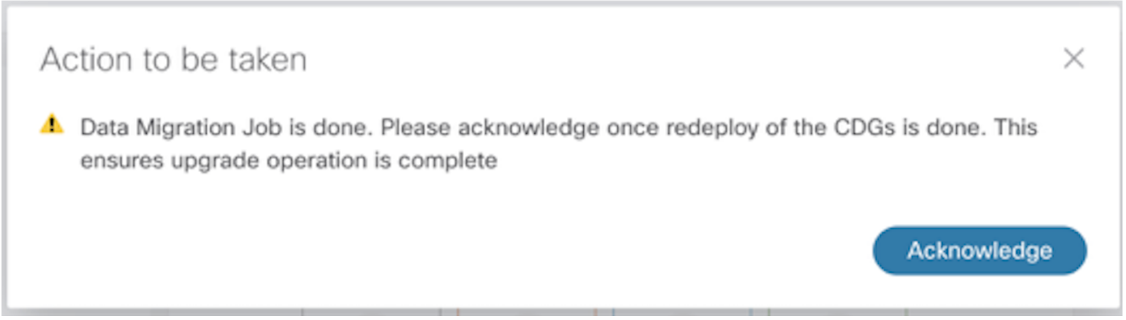


Data Gateways — Filter 0 / Total 3

Name	Operational St...	Administration S...	High Availability St...	Pool Name	Outage History	Average Availa...	VM Name	Attached Device C...	Actions
VDG-96-1	Up	Up	Protected	VDG-96		100%	dlm-cdg-81-04	50	⋯
VDG-99-1	Up	Up	None Planned	VDG-99		100%	dlm-cdg-81-06	50	⋯
VDG-95-1	Up	Up	Protected	VDG-95		98%	dlm-cdg-81	50	⋯

Step 8 Log out of Cisco Crosswork 4.3 and log in again.

Step 9 After you log in, Cisco Crosswork presents you with the following window prompting for confirmation that the VMs. Click **Acknowledge** in the pop up that appears .



Action to be taken

⚠ Data Migration Job is done. Please acknowledge once redeploy of the CDGs is done. This ensures upgrade operation is complete

Important Do not click **Acknowledge** unless you have verified that the VMs are in the **Up**/**Not Ready** state. Doing so will result in VMs having the state as **Error**. See Troubleshoot Crosswork Data Gateway Upgrade Issues.

Step 10 (Optional) Move Cisco NSO out of maintenance or read-only mode.

```
ncs_cmd -c maapi_read_write
```

After the upgrade is complete:

- Crosswork Data Gateway 4.0 VMs are enrolled with Cisco Crosswork 4.3.
- All destinations, Crosswork Data Gateway pools, device mapping information can be viewed on the Cisco Crosswork UI with the upgraded Crosswork Data Gateway VMs.
- Collection jobs start again automatically with the new Cisco Crosswork Data Gateway VMs.

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	Recommended Action
Some of the Crosswork Data Gateway VMs are in **Error** or **Degraded** state because you clicked **Acknowledge** before the VMs came to the **Up**/**Not Ready** state	1. Wait for the Crosswork Data Gateway VMs to have the state as **Up** or **Not Ready** state. 2. Once the VMs have the state as **Up** or **Not Ready**, delete all Crosswork Data Gateway pools and create them again.
Some of the Crosswork Data Gateway VMs are in **Error** or **Degraded** state because you clicked **Acknowledge** before the VMs came to the **Up**/**Not Ready** state. The state of the VMs did not change to **Up**/ **Ready** and they are still in **Error**.	1. Delete all Crosswork Data Gateway pools. 2. Check if the VMs now have the state as **Up** or **Not Ready**. 3. If the VMs are still in a state of **Error**, manually re-enroll the VMs with Cisco Crosswork 4.3. See Re-enroll Crosswork Data Gateway for more information.

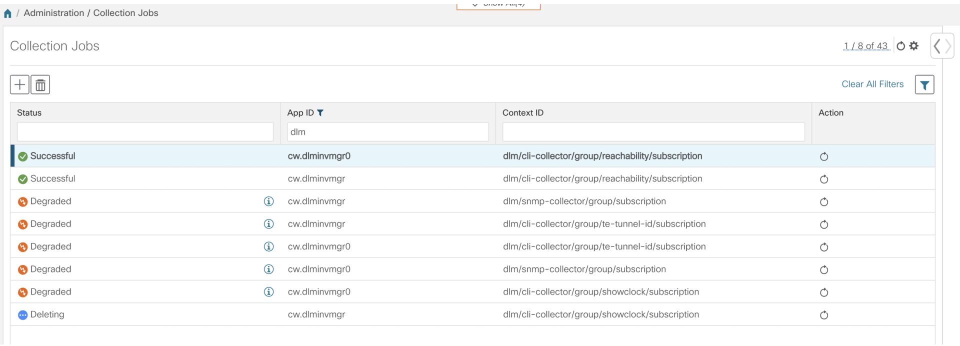
Issue	Recommended Action
Crosswork Data Gateways VMs are stuck in the **Degraded** state with Image manager being in exited state. The list of components for the Crosswork Data Gateway either do not show Image manager or show it in an exited state.	1. In the Cisco Crosswork UI, navigate to **Data Gateway Management** > **Virtual Machines**. 2. Click the Crosswork Data Gateway that is degraded. 3. Click **Actions** and click **Reboot**.

Post-upgrade Checklist

After the upgrade to Cisco Crosswork 4.3 is completed, check the health of the new cluster. If your cluster is healthy, perform the following activities:

- Perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepency.

- Navigate to **Administration** > **Collection Jobs** in Cisco Crosswork 4.3 UI and delete the duplicate system jobs.



Status	App ID	Context ID	Action
	dlm		
✓ Successful	cw.dlminvmgr0	dlm/cli-collector/group/reachability/subscription	⟳
✓ Successful	cw.dlminvmgr	dlm/cli-collector/group/reachability/subscription	⟳
Degraded ⓘ	cw.dlminvmgr	dlm/snmp-collector/group/subscription	⟳
Degraded ⓘ	cw.dlminvmgr	dlm/cli-collector/group/te-tunnel-id/subscription	⟳
Degraded ⓘ	cw.dlminvmgr0	dlm/cli-collector/group/te-tunnel-id/subscription	⟳
Degraded ⓘ	cw.dlminvmgr0	dlm/snmp-collector/group/subscription	⟳
Degraded ⓘ	cw.dlminvmgr0	dlm/cli-collector/group/showclock/subscription	⟳
Deleting	cw.dlminvmgr	dlm/cli-collector/group/showclock/subscription	⟳

- Verify that the collection jobs are running on the Crosswork Data Gateway 4.0 VMs in the **Administration** > **Collection Jobs** page.

- Verify the restored AAA data by logging in using default credentials, and configure custom user roles (Read-Write/Read) in Cisco Crosswork 4.3.

- (Optional) Based on your network requirements, download the relevant map files from cisco.com and re-upload them to Cisco Crosswork 4.3.

- (Optional) If any NSO device onboarding policy was set in Cisco Crosswork 4.1, 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 4.1) to Cisco Crosswork 4.3.

- If you are using Crosswork Change Automation, verify that all the stock and custom playbooks are migrated successfully.

- If you are using Crosswork Health Insights, verify that the the collection to the external destination is working. Also, check if the alert dashboard is displaying the correct data.

- 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 Requirements, on page 118.

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

Upgrade Using Parallel Hardware

This section explains how to migrate to Cisco Crosswork 4.3 using new hardware. This method relies on installing the Cisco Crosswork 4.3 cluster on new hardware in parallel while the data from the old Cisco Crosswork cluster is being backed up. This method is faster but requires twice the amount of resources for creating the new cluster in parallel.

The stages of the parallel upgrade workflow are:

1. Deploy a new Cisco Crosswork 4.3 Cluster, on page 129

Note While the cluster installation is in progress, you must upgrade NSO to version 5.7.5.1. The process to upgrade NSO is not covered in this document. For more information, see the relevant Cisco NSO documentation. Additionally, if you are planning to use Cisco Optimization Engine individually or as part of the Cisco Network Controller solution, upgrade your SR-PCE to the supported version as mentioned in the Crosswork Network Controller Release Notes.

2. Backup Cisco Crosswork 4.1 Cluster, on page 130
3. Update DNS Server and Run Migration , on page 132
4. Add Crosswork Data Gateway 4.0 to Cisco Crosswork 4.3, on page 133
5. Shut Down Cisco Crosswork 4.1 Cluster, on page 136

Deploy a new Cisco Crosswork 4.3 Cluster

Install Cisco Crosswork 4.3 cluster and applications on a new set of VMs in parallel.

Note Cisco Crosswork 4.3 must be installed with the same FQDN and same number of nodes as in Cisco Crosswork 4.1.

Before you begin

- Make sure that your environment meets all the requirements specified under Cisco Crosswork Infrastructure Requirements, on page 7.

Step 1 Install Cisco Crosswork 4.3 cluster using any of the installation methods described in Install the Crosswork Cluster, on page 31.

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 by navigating to https://<NEW_VIP>:30603.

Step 3 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.

Step 4 Install the applications which were part of Cisco Crosswork 4.1. For more information, see Install Crosswork Applications, on page 111.

Step 5 After the applications are successfully installed, check the health of the Cisco Crosswork 4.3 cluster.

Backup Cisco Crosswork 4.1 Cluster

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 4.1, download a copy of the package to your system. You will need to upload the package after you complete migrating to Cisco Crosswork 4.3. See Post-upgrade Checklist, on page 128 for more infomation.

- If you have modified Cisco Crosswork 4.1 to include third-party device types, you must download the third-party device configuration file, and re-apply it to Cisco Crosswork 4.3. 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** > **Domain Identifier <domain_id>** > **Interface Thresholds** > **Export** OR **Traffic Engineering** > **Bandwidth Optimization** > **Interface Thresholds** > **Export** icon). Follow the steps documented in Upgrade Requirements, on page 118.

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.

Step 1 Launch the Cisco Crosswork UI by using a browser and navigating to https://<FQDN>:30603

Step 2 Check and confirm that all the VMs are healthy and running in your cluster.

Step 3 **Configure an SCP backup server:**

a) From the Cisco Crosswork 4.1 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 4 **Create a backup:**

a) From the Cisco Crosswork 4.1 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 4.3 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**.

Update DNS Server and Run Migration

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 .
- User credentials with file read and write permissions to the directory.

Step 1 Update the DNS server to point the FQDN of Cisco Crosswork 4.1 cluster to the new_VIP of Cisco Crosswork 4.3 cluster.

Step 2 Navigate to the UI of the new 4.3 cluster using https://<new_VIP>:30603.

Step 3 **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 Backup Cisco Crosswork 4.1 Cluster, on page 130.

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

Step 4 **Migrate the Cisco Crosswork 4.1 backup on the Cisco Crosswork 4.3 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 Backup Cisco Crosswork 4.1 Cluster, on page 130) 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 5 After the data migration is successfully completed, check the health of the Cisco Crosswork 4.3 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.

Note After a successful migration, please perform a hard refresh or browser cache deletion before proceeding to use the system. Failing to do this step can result in data discrepency.

Add Crosswork Data Gateway 4.0 to Cisco Crosswork 4.3

Ensure that the migration is complete and Cisco Crosswork 4.3 UI is available before you proceed with installing Crosswork Data Gateway (CDG) 4.0.

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.

Crosswork Data Gateway functions as a passive device in the network. The Crosswork Data Gateway upgrade process consists of replacing all Crosswork Data Gateway 3.0 VMs with Crosswork Data Gateway 4.0 VMs in the network.

Important Step 6 in this procedure requires you log out of Cisco Crosswork 4.3 and log in again after verifying the deployment and enrollment of the 4.0 CDG VMs with Cisco Crosswork 4.3. After you log in, an **Action to be taken** window appears prompting you to confirm that the upgrade is complete. Do not click **Acknowledge** unless you have completed all the verification steps mentioned in Step 3, Step 4 and Step 5 in the procedure.

Step 1 Log out of Cisco Crosswork 4.3 and log in again.

Step 2 After you log in, an **Action to be taken** window appears. Close this window and do not click **Acknowledge**.

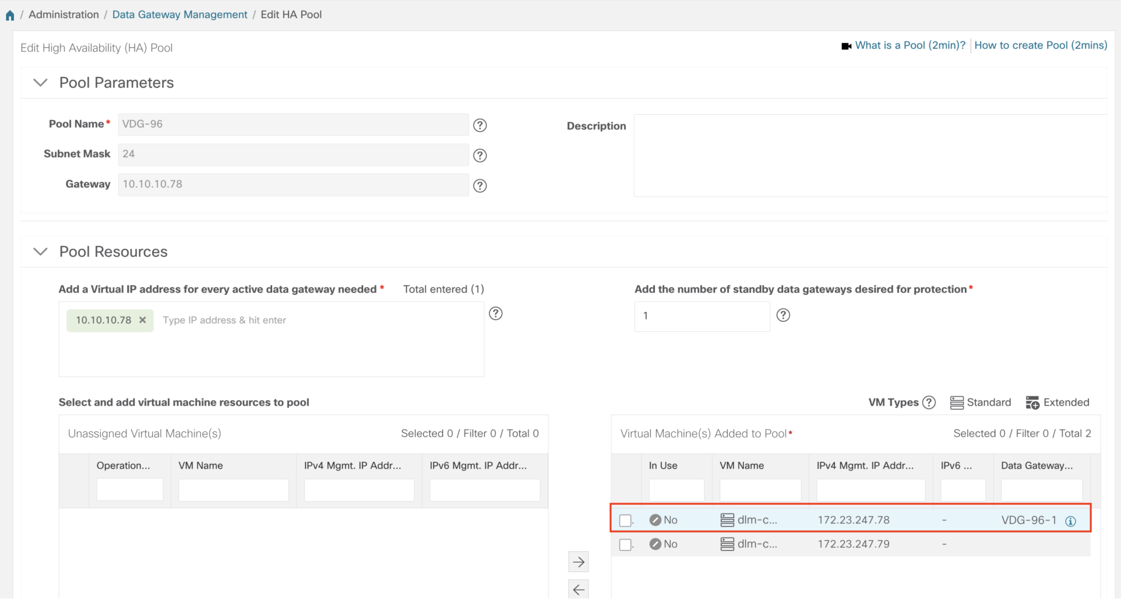
Step 3 Install new Cisco Crosswork Data Gateway 4.0 VMs with the same number and the same information (management interface importantly) as the Crosswork Data Gateway 3.0 VMs. Follow the steps in the Install Cisco Crosswork Data Gateway, on page 71.

Step 4 Wait for about 5 minutes and navigate to **Administration** > **Data Gateway Management**.

Step 5 Check the **Virtual Machines** tab to verify that the new Crosswork Data Gateway 4.0 VMs are enrolled with Cisco Crosswork 4.3 and have the **Admin State** as **Up** and **Operational State** as **Not Ready**.

Step 6 After the **Operational State** of the VMs changes to **Ready**, navigate to the **Pools** tab and verify that all the Crosswork Data Gateway pools from Cisco Crosswork 4.1, are listed here. Edit each Crosswork Data Gateway pool to verify that the active Crosswork Data Gateway is same as one that you noted in Cisco Crosswork 4.1.

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


Administration / Data Gateway Management / Edit HA Pool
Edit High Availability (HA) Pool
What is a Pool (2min)? | How to create Pool (2mins)
Pool Parameters
Pool Resources
Unassigned Virtual Machine(s)
Selected 0 / Filter 0 / Total 0
Virtual Machine(s) Added to Pool*
Selected 0 / Filter 0 / Total 2
VM Types
Standard
Extended

Pool Name* VDG-96
Subnet Mask 24
Gateway 10.10.10.78
Description

Add a Virtual IP address for every active data gateway needed* Total entered (1)
10.10.10.78 ✕ Type IP address & hit enter

Add the number of standby data gateways desired for protection*
1

Select and add virtual machine resources to pool

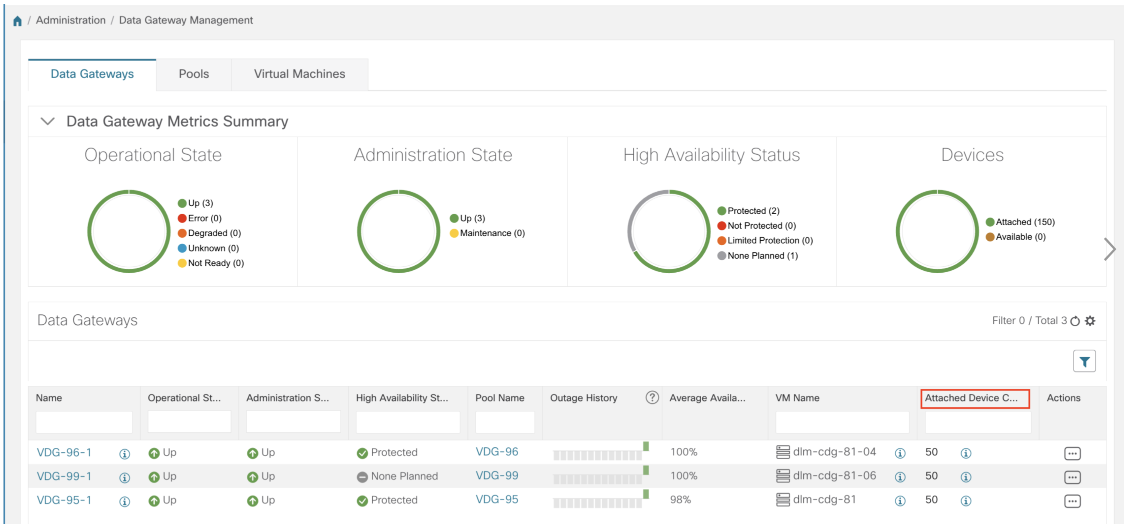
Operation...	VM Name	IPv4 Mgmt. IP Addr...	IPv6 Mgmt. IP Addr...

	In Use	VM Name	IPv4 Mgmt. IP Addr...	IPv6 ...	Data Gateway...
□	No	dlm-c...	172.23.247.78	-	VDG-96-1
□	No	dlm-c...	172.23.247.79	-	

Step 7 **Verify that devices are attached to the Crosswork Data Gateways 4.0 in the Cisco Crosswork 4.3 UI.**

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

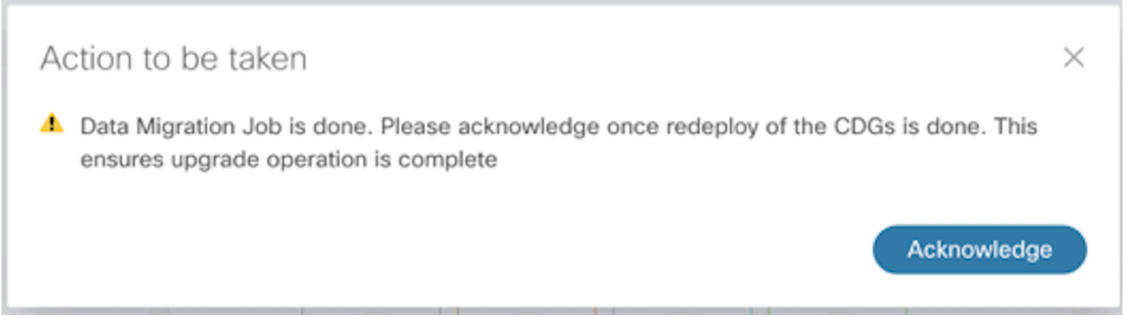
b) Check the **Attached Device Count** of the Crosswork Data Gateway.



Name	Operational St...	Administration S...	High Availability St...	Pool Name	Outage History	Average Availa...	VM Name	Attached Device C...	Actions
VDG-96-1	Up	Up	Protected	VDG-96		100%	dlm-cdg-81-04	50	⋯
VDG-99-1	Up	Up	None Planned	VDG-99		100%	dlm-cdg-81-06	50	⋯
VDG-95-1	Up	Up	Protected	VDG-95		98%	dlm-cdg-81	50	⋯

Step 8 Log out of Cisco Crosswork 4.3 and log in again.

Step 9 After you log in, Cisco Crosswork presents you with the following window prompting for confirmation that the VMs .Click **Acknowledge** in the pop up that appears .



Action to be taken

Data Migration Job is done. Please acknowledge once redeploy of the CDGs is done. This ensures upgrade operation is complete

Important Do not click **Acknowledge** unless you have verified that the VMs are in the **Up**/**Not Ready** state. Doing so will result in VMs having the state as **Error**. See Troubleshoot Crosswork Data Gateway Upgrade Issues.

Step 10 (Optional) Move Cisco NSO out of maintenance or read-only mode.

```
ncs_cmd -c maapi_read_write
```

After the upgrade is complete:

- Crosswork Data Gateway 4.0 VMs are enrolled with Cisco Crosswork 4.3.
- All destinations, HA Pools, device mapping information can be viewed on the Cisco Crosswork UI with the upgraded Crosswork Data Gateway VMs.
- Jobs start again automatically with the new Cisco Crosswork Data Gateway VMs.

Shut Down Cisco Crosswork 4.1 Cluster

Before you begin

Gather the following information before shutting down the Cisco Crosswork 4.1:

- All the IP addresses in the cluster.
- All the IP addresses of the CDGs.

Step 1 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 1a to 1d for each of the remaining VMs.

Step 2 Shut down the Crosswork Data Gateway 3.0 VMs.

a) Log in to the Crosswork Data Gateway 3.0 VM. See Access Crosswork Data Gateway VM from SSH, on page 103.

   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.

Step 3 (Optional) 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 5.7.5.1.

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 **Download and validate the CAPP files:**

a) Navigate to cisco.com and locate the CAPP files (.tar.gz) that you require.
b) Hover over the file and copy the MD5 or SHA512 checksum to your clip board.
c) Download the CAPP files to a server that can be reached from the Crosswork server.
d) Run a tool of your choice to calculate the checksum, and the compare the checksum value in your dowloaded file with the value you copied in the clip board.

For example, on a MAC you can use the **md5** command to calculate the MD5 sum on a file:

```
md5 cw-na-ztp-3.0.3-3-release-220614.tar.gz
```

```
ff47a72ed7dc4fc4be388db3a43fa13f
```

Verify that the result value matches with the posted value on cisco.com.

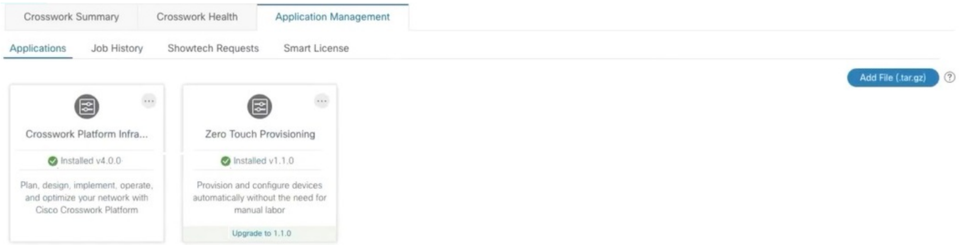
Step 2 Click on **Administration** > **Crosswork Manager**, and select the **Application Management** tab.

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

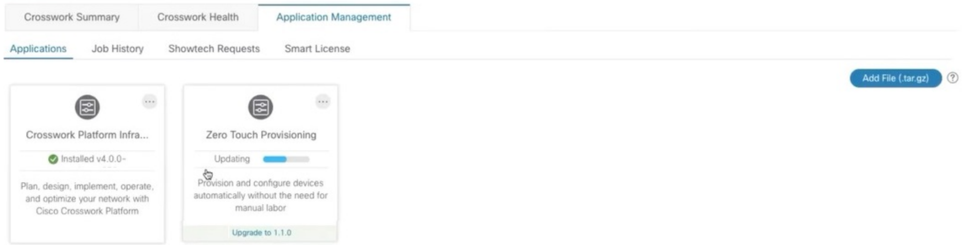
Step 3 Click on the **Add File (.tar.gz)** option to add the application CAPP file that you had downloaded.

Step 4 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.

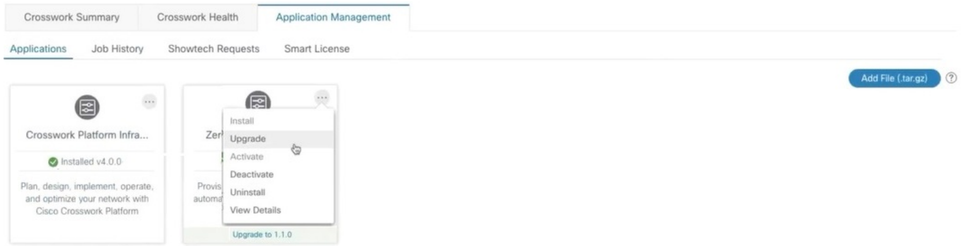


Step 5 To upgrade, click the Upgrade prompt and the new version of the application is installed.

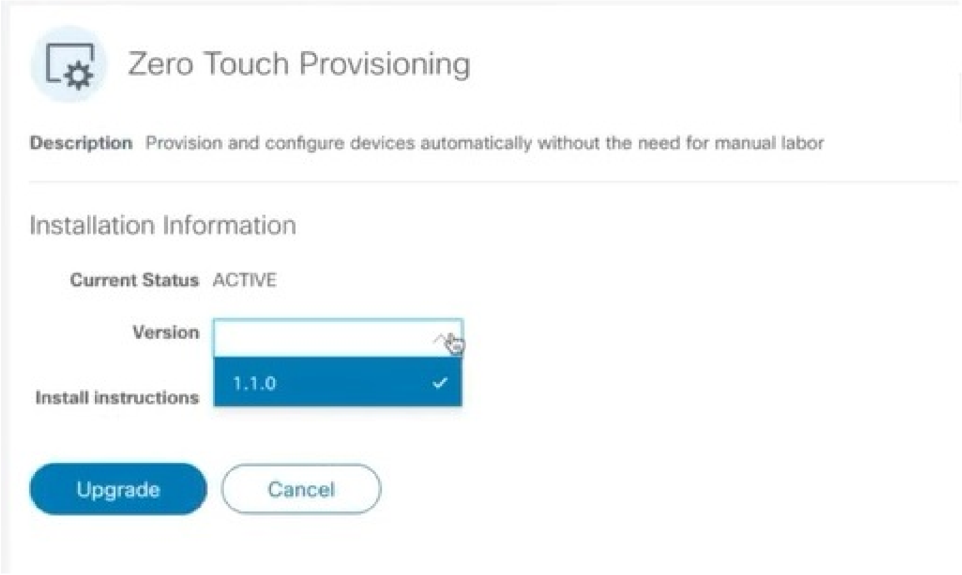

Crosswork Summary
Crosswork Health
Application Management
Applications
Job History
Showtech Requests
Smart License
Add File (.tar.gz)
Crosswork Platform Infra...
Installed v4.0.0-
Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform
Zero Touch Provisioning
Updating
Provision and configure devices automatically without the need for manual labor
Upgrade to 1.1.0

The upgrade progress is displayed on the application tile.

Step 6 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**.


Zero Touch Provisioning

Description Provision and configure devices automatically without the need for manual labor

Installation Information

Current Status ACTIVE

Version 1.1.0 ✓

Install instructions

Step 7 (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, on page 141
- Delete the VM using the vSphere UI, on page 142

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 143.

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 143
- Delete Crosswork Data Gateway Service from Cisco CSP, on page 144

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.

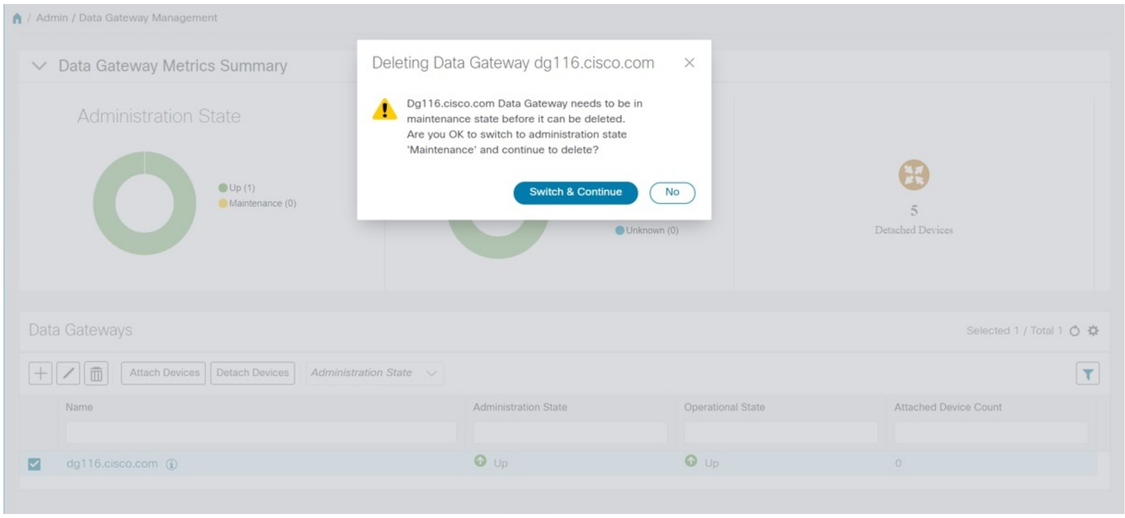
Step 2 From the navigation panel, select **Administration** > **Data Gateway Management**.

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**.



Deleting Data Gateway dg116.cisco.com

Dg116.cisco.com Data Gateway needs to be in maintenance state before it can be deleted. Are you OK to switch to administration state 'Maintenance' and continue to delete?

	Name	Administration State	Operational State	Attached Device Count
☑	dg116.cisco.com	Up	Up	0

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.

⚠

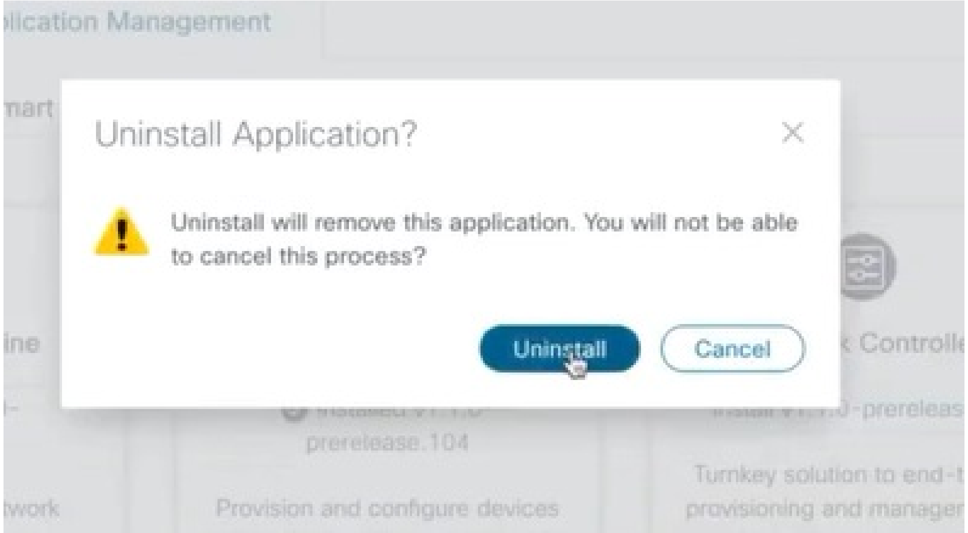
Attention Crosswork Active Topology (if installed) must be uninstalled before you can uninstall Crosswork Optimization Engine.

Step 1 Click on **Admin** > **Crosswork Manager**, 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.

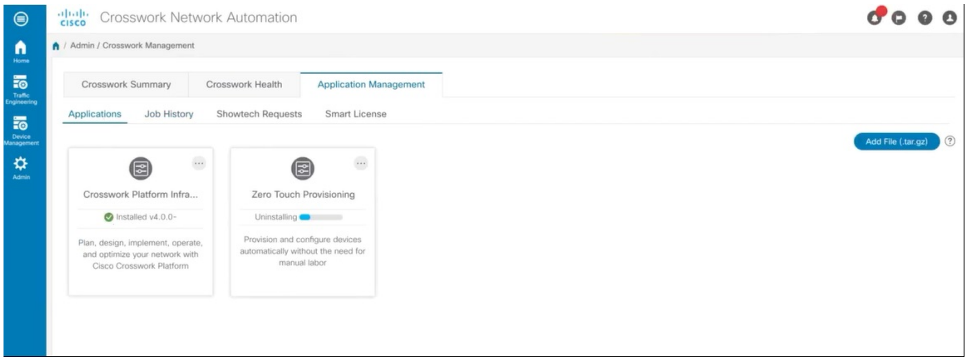
A pop-up is displayed to confirm the action.



Uninstall will remove this application. You will not be able to cancel this process?

Step 3 Click **Uninstall** to confirm.

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



Plan, design, implement, operate, and optimize your network with Cisco Crosswork Platform

Provision and configure devices automatically without the need for manual labor

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.

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"
}
```