



Cisco Crosswork Infrastructure 4.4 and Applications Installation Guide

First Published: 2022-10-31

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 NON-INFRINGEMENT 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.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022–2022 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Cisco Crosswork Overview	1
About this guide	1
Audience	1
Security	2
Introduction	2
Cisco Crosswork Product Portfolio	3
Integrated Components	4
Crosswork Installation Workflow	5

CHAPTER 2

Cisco Crosswork Installation Requirements	9
Requirements Overview	9
General Requirements (common for VMware and AWS)	9
Host VM Requirements	10
Crosswork Cluster VM Requirements	10
Crosswork Data Gateway VM Requirements	12
Port requirements	15
IP Address Restrictions	19
Integration Requirements for other Cisco Products	20
(Optional) Set up Cisco NSO Layered Service Architecture	22
Supported Web Browsers	23
Installation Requirements in VMware vCenter	23
VMware Resource Requirements	23
VMware Settings	25
Supported Network Topology Models	26
Installation Requirements in AWS EC2	31
AWS Resource Requirements	31

AWS EC2 Settings 33

CHAPTER 3

Install the Crosswork Cluster 35

Installation Parameters 35

Install Cisco Crosswork on VMware vCenter 39

Install Cisco Crosswork on VMware vCenter using Cluster Installer tool 39

Monitor the Installation 44

Known Limitations 45

Troubleshoot the Cluster 46

Manual Installation of Cisco Crosswork using vCenter vSphere UI 48

Build the template 49

Deploy the template 54

Install Crosswork Cluster on AWS EC2 57

Install Cisco Crosswork on AWS EC2 using CloudFormation Template 58

Install Crosswork Cluster on Amazon EC2 Manually 59

Log into the Cisco Crosswork UI 62

CHAPTER 4

Install Cisco Crosswork Data Gateway 65

Cisco Crosswork Data Gateway Installation Workflow 65

Cisco Crosswork Data Gateway Parameters and Deployment Scenarios 66

Install Cisco Crosswork Data Gateway Using vCenter vSphere Client 80

Install Cisco Crosswork Data Gateway Via OVF Tool 85

Install Crosswork Data Gateway on Amazon EC2 86

Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template 87

Install Crosswork Data Gateway on Amazon EC2 Manually 88

Crosswork Data Gateway Post-installation Tasks 91

Configure Timezone of the Crosswork Data Gateway VM 92

Log in and Log out of Crosswork Data Gateway VM 93

Access Crosswork Data Gateway VM from SSH 93

Access Crosswork Data Gateway Through vCenter 94

Log Out of Crosswork Data Gateway VM 94

Cisco Crosswork Data Gateway Authentication and Enrollment 94

Troubleshoot Crosswork Data Gateway Installation and Enrollment 95

Import Controller Signing Certificate File 98

View the Controller Signing Certificate File 99

CHAPTER 5

Install Crosswork Applications 101

Install Crosswork Applications 101

CHAPTER 6

Upgrade Cisco Crosswork 107

Cisco Crosswork Upgrade Workflow 107

Upgrade Requirements 108

Upgrade Using Same Hardware 109

Shut Down Cisco Crosswork Data Gateway VMs 110

Create Backup and Shut Down Cisco Crosswork 111

Install the Cisco Crosswork 4.4 Cluster 113

Install Cisco Crosswork 4.4 Applications 114

Migrate the Previous Cisco Crosswork backup to Cisco Crosswork 4.4 114

Upgrade to Crosswork Data Gateway 4.1 115

Troubleshoot Crosswork Data Gateway Upgrade Issues 118

Post-upgrade Checklist 119

Upgrade Using Parallel Hardware 120

Deploy a new Cisco Crosswork 4.4 Cluster 120

Backup Cisco Crosswork Cluster 121

Update DNS Server and Run Migration 123

Add Crosswork Data Gateway 4.1 to Cisco Crosswork 4.4 124

Shut Down the Previous Cisco Crosswork Cluster 127

Update a Crosswork Application (standalone activity) 128

CHAPTER 7

Uninstall Cisco Crosswork 131

Uninstall the Crosswork Cluster 131

Delete the VM using the Cluster Installer 131

Delete the VM using the vSphere UI 132

Uninstall Crosswork Data Gateway 132

Delete Crosswork Data Gateway VM from Cisco Crosswork 133

Uninstall Crosswork Applications 133

APPENDIX A

Sample deployment templates 135

[Sample manifest template for VMware vCenter](#) **135**

[Set seed node explicitly](#) **137**

[Sample CloudFormation template for installing Crosswork Cluster VMs on AWS EC2](#) **137**

[Sample CloudFormation Template for installing Crosswork Data Gateway on EC2](#) **152**



CHAPTER 1

Cisco Crosswork Overview

This chapter contains the following topics:

- [About this guide, on page 1](#)
- [Audience, on page 1](#)
- [Security, on page 2](#)
- [Introduction, on page 2](#)
- [Cisco Crosswork Product Portfolio, on page 3](#)
- [Integrated Components, on page 4](#)
- [Crosswork Installation Workflow, on page 5](#)

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, any of the Crosswork applications.

There are other components that integrate with Cisco Crosswork (see [Integrated Components, on page 4](#)), such as Cisco NSO or Cisco WAE, but they are NOT covered in this document. For integration steps, please refer to the [Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide](#). For more details about these components, please refer to their respective installation documentation.



Note While this guide includes instructions for installing Cisco Crosswork on Amazon EC2 platform, the EC2 deployment is only available as a limited-release deployment. Please contact the Cisco Product Management team for assistance.

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
- Amazon Web Services (AWS), Amazon EC2 concepts, and creation of CloudFormation templates

Security

Cisco takes great strides to ensure that all our products conform to the latest industry recommendations. We firmly believe that security is an end-to-end commitment and are here to help secure your entire environment. Please work with your Cisco account team to review the security profile of your network.

For details on how we validate our products, see [Cisco Secure Products and Solutions](#) and [Cisco Security Advisories](#).

If you have questions or concerns regarding the security of any Cisco products, please open a case with the Cisco Customer Experience team and include details about the tool being used and any vulnerabilities it reports.

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 the deployed applications. 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. Please work with the Cisco Customer Experience team to determine the number of nodes required 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 into its 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 the Cisco Customer Experience team for guidance on your deployment to best meet your needs.

The Crosswork Data Gateway is an integral part of the Crosswork solution being deployed. For this reason, this document explains Crosswork Data Gateway as a foundational component that must be installed in tandem with the Crosswork cluster. However, this document does not cover the installation of the other integrated components (such as Cisco NSO, Cisco SR-PCE, etc.) that may already be installed or can be used independently.

Cisco Crosswork Product Portfolio

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

Cisco Crosswork supports Cisco Crosswork Network Controller solution and its contents:

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.

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

Table 1: Cisco Crosswork Network Controller Packages

Package	Contents	Description
Cisco Crosswork Network Controller Essentials	Cisco Crosswork Optimization Engine	An application that provides closed-loop tracking of the network state and real-time network optimization in response to changes in network state, allowing operators to effectively maximize network capacity utilization, as well as increase service velocity.
	Cisco Crosswork Active Topology	A component of Crosswork Network Controller that enables visualization of topology and services on logical and geographical maps.

Package	Contents	Description
Cisco Crosswork Network Controller Advantage	Cisco Crosswork Optimization Engine	An application that provides closed-loop tracking of the network state and real-time network optimization in response to changes in network state, allowing operators to effectively maximize network capacity utilization, as well as increase service velocity.
	Cisco Crosswork Active Topology	A component of Crosswork Network Controller that enables visualization of topology and services on logical and geographical maps.
	Cisco Crosswork Service Health	An 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	An application 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	An application 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 Zero Touch Provisioning	A component of Cisco Crosswork Network Controller that streamlines onboarding and provisioning of Day 0 configuration resulting in faster deployment IOS-XR and IOS-XE devices at a lower operating cost.
	Element Management Functions	A library of functions that provides deep inventory collection, alarm management and image management using Inventory, Fault, and Software Image Management (SWIM) functions.

For information on the installation and configuration requirements of Cisco Crosswork products, see [Integration Requirements for other Cisco Products, on page 20](#).

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), external servers (TACACS+ and LDAP), DHCP server (when using Crosswork ZTP), Vitria, and external Kafka. The details about these specific integrations are addressed in the [Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide](#) or in the application guides.

Crosswork Installation Workflow

The following table describes the general workflow to install Crosswork components on your preferred datacenter.

Table 2: Crosswork Installation Workflow

Step	Action
1. Ensure that your environment meets all the requirements.	Refer to the guidelines in: <ul style="list-style-type: none"> • General Requirements (common for VMware and AWS), on page 9 • VMware: Installation Requirements in VMware vCenter, on page 23 • AWS EC2: Installation Requirements in AWS EC2, on page 31
2. Install or upgrade to the compatible version of NSO with the appropriate Function packs to support the applications you plan to use.	Follow the steps in Integration Requirements for other Cisco Products , on page 20.
3. Install the Cisco Crosswork cluster on your preferred datacenter platform.	Choose an installation method for your platform, and follow the relevant procedure: <ul style="list-style-type: none"> • VMware: <ul style="list-style-type: none"> • Using cluster installer tool: Install Cisco Crosswork on VMware vCenter using Cluster Installer tool, on page 39 • Manual Installation: Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 48 • AWS EC2: <ul style="list-style-type: none"> • Using CloudFormation template: Install Cisco Crosswork on AWS EC2 using CloudFormation Template, on page 58 • Manual Installation: Install Crosswork Cluster on Amazon EC2 Manually, on page 59

Step	Action
4. Verify if the installation was successful, and log into the Cisco Crosswork UI	Refer to the guidelines in: <ul style="list-style-type: none"> • Monitor the Installation, on page 44 (for VMware) • Log into the Cisco Crosswork UI, on page 62
5. Install the Crosswork Data Gateway on your preferred datacenter platform.	Choose the profile for the Cisco Crosswork Data Gateway VM (i.e., Standard, Standard with Extra Resources or Extended). See Mandatory deployment type for Crosswork Data Gateway, on page 12 for more information and install as per your preferred method: <ul style="list-style-type: none"> • VMware: <ul style="list-style-type: none"> • Using vSphere: Install Cisco Crosswork Data Gateway Using vCenter vSphere Client, on page 80 • Using OVF tool: Install Cisco Crosswork Data Gateway Via OVF Tool, on page 85 • AWS EC2: <ul style="list-style-type: none"> • Using CloudFormation template: Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template, on page 87 • Manual Installation: Install Crosswork Data Gateway on Amazon EC2 Manually , on page 88 <p>Note When entering the parameters for deployment, ensure that you add the correct parameters. If the parameter values are incorrect, you have to destroy the current Crosswork Data Gateway VM, create a new VM, and re-enroll the new VM with Cisco Crosswork.</p>
6. Complete the Crosswork Data Gateway post-installation tasks.	Follow the steps in Crosswork Data Gateway Post-installation Tasks, on page 91 .
7. Verify that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork.	Follow the steps in Cisco Crosswork Data Gateway Authentication and Enrollment, on page 94 . <p>After verifying that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork, set up the Crosswork Data Gateway for collection by creating a Crosswork Data Gateway pool. See Section: Create a Crosswork Data Gateway Pool in the Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide.</p> <p>Note If you plan to install multiple Cisco Crosswork Data Gateway VMs due to load or scale requirements or you wish to leverage Cisco Data Gateway High Availability, we recommend that you install all the Crosswork Data Gateway VMs first and then proceed with adding them to a Data Gateway pool.</p>

Step	Action
8. Install the Crosswork Applications	<p data-bbox="768 296 1458 323">Follow the steps in Install Crosswork Applications, on page 101.</p> <p data-bbox="768 342 1516 464">Important If you intend to use the Crosswork Network Controller solution (Essential or Advantage), install Crosswork Cluster and Crosswork Data Gateway, and then install the Crosswork applications in the following sequence:</p> <ol data-bbox="899 485 1516 730" style="list-style-type: none"><li data-bbox="899 485 1287 512">1. Crosswork Optimization Engine<li data-bbox="899 533 1243 560">2. Crosswork Active Topology<li data-bbox="899 581 1516 646">3. Crosswork Service Health (only available in Advantage bundle)<li data-bbox="899 667 1516 730">4. Cisco Element Management System (EMS) Services (only available in Advantage bundle) <p data-bbox="899 766 1516 888">Crosswork Change Automation, Crosswork Health Insights, and Crosswork Zero Touch Provisioning can be installed independently in any order and do not require any other application to be installed prior.</p>



CHAPTER 2

Cisco Crosswork Installation Requirements

This chapter contains the following topics:

- [Requirements Overview](#), on page 9
- [General Requirements \(common for VMware and AWS\)](#), on page 9
- [Installation Requirements in VMware vCenter](#), on page 23
- [Installation Requirements in AWS EC2](#), on page 31

Requirements Overview

Cisco Crosswork can be deployed in the following data centers:

- VMware vCenter
- Amazon Web Services Elastic Cloud Compute (AWS EC2)

Starting with the Cisco Crosswork 4.4 release, Crosswork deployment is no longer supported for the Cisco CSP platform. For more information, see [End-of-Life Announcement for the Cisco Cloud Services Platform Operating System](#).

This chapter explains the general installation requirements (such as VM requirements, port requirements, application requirements, etc.) that are common for all data centers along with the specific requirements needed for each data center to install Crosswork Infrastructure (cluster) and Crosswork Data Gateway.

The data center resources needed to operate other integrated components or applications (such as Cisco NSO, WAE, DHCP, and TFTP servers) are not addressed in this document. Please refer to the respective install documentation of those components for more details.

General Requirements (common for VMware and AWS)

The following requirements remain the same irrespective of the data center where you deploy Cisco Crosswork:

- [Host VM Requirements](#), on page 10
- [Port requirements](#), on page 15
- [IP Address Restrictions](#), on page 19

- [Integration Requirements for other Cisco Products, on page 20](#)
- [\(Optional\) Set up Cisco NSO Layered Service Architecture, on page 22](#)
- [Supported Web Browsers, on page 23](#)

Host VM Requirements

This section explains the resource requirements per VM to deploy the Crosswork Cluster and Crosswork Data Gateway.

- [Crosswork Cluster VM Requirements, on page 10](#)
- [Crosswork Data Gateway VM Requirements, on page 12](#)

Crosswork Cluster VM Requirements

The Crosswork cluster 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 (maximum up to 3 worker 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 the Cisco Customer Experience team for guidance on your deployment to best meet your needs.

The following table shows the VM requirements for various use cases and combinations of applications:

Table 3: Deployment Profiles

Deployment Size	Use case	Number of Cluster Nodes needed ¹
Large	Crosswork Network Controller Essentials package (Production environment)	3 Hybrid nodes + 1 Worker node
	Crosswork Network Controller Advantage package (Production environment) ²	Advantage package: 3 Hybrid nodes + 2 Worker nodes

¹ The number of nodes mentioned is only the minimum requirement. You can add more Worker nodes (maximum upto 3 worker nodes) as needed.

² The cluster resource estimation is under the assumption that you are using all the applications in the Crosswork Network Controller Advantage package.



Important

A Crosswork cluster with only 3 Hybrid VM nodes (without any Worker VM nodes) is more prone to data loss. If one of the Hybrid VM fails, it will result in impaired system performance, as the remaining 2 Hybrid VMs struggle to support all the pods being migrated from the failed VM. Having sufficient worker nodes in your cluster ensures that the load on the Hybrid VMs remains less, therefore, ensuring more VM resiliency. For assistance in adjusting VM Memory and CPU configuration post-installation, please contact the Cisco Customer Experience team.

The resources required per VM such as CPU, Memory, and Storage vary based on the datacenter where you are deploying. For more information, see the following topics:

- **VMware:** [Installation Requirements in VMware vCenter, on page 23](#)
- **AWS EC2:** [Installation Requirements in AWS EC2, on page 31](#)



Note For assistance in adjusting VM Memory and CPU configuration post installation, please contact the Cisco Customer Experience team.

The table below explains the network requirements per VM host:

Table 4: Network Requirements (per VM)

Requirement	Description
Network Connections	<p>For production deployments, we recommend that you use dual interfaces, one for the Management network and one for the Data network.</p> <p>For optimal performance, the Management and Data networks should use links configured at a minimum of 10 Gbps.</p>
IP Addresses	<p>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.</p> <p>When using single NIC: 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.</p> <p>When using dual NICs (one for the Management network and one for the Data network): A management and data IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and two additional IP addresses to be used as the Virtual IP (VIP) address (one for the Management network and one for the Data network).</p> <p>For example, in the case of a 3 VM cluster with a single NIC, you need 4 IP addresses, and in the case of a 3 VM cluster with dual NIC, you need 8 IP addresses (4 for management network and 4 for data network).</p> <p>Note</p> <ul style="list-style-type: none"> • 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 the 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.
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. <ul style="list-style-type: none"> • 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.
Backup Server	Cisco Crosswork will back up the configuration of the system to an external server using SCP. The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.

- 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.

Crosswork Data Gateway VM Requirements

This section provides information about the general guidelines and minimum requirements for installing Crosswork Data Gateway.

- [Mandatory deployment type for Crosswork Data Gateway, on page 12](#)
- [Crosswork Data Gateway VM Requirements, on page 13](#)

Mandatory deployment type for Crosswork Data Gateway

Cisco Crosswork Data Gateway supports the following on-premise deployment options:

- **On-Premise Standard** (default): Collectors only.
- **On-Premise Extended**: Collectors and offload services.



Attention The **On-Premise Standard with Extra Resources** profile is available as a limited-availability feature and must not be used while deploying Crosswork Data Gateway in your data center. Please contact the Cisco Customer Experience team for assistance.

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



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. Ensure that you manually rollback any Data Gateway global parameter changes before attempting to redeploy the Crosswork Data Gateway in order to switch profiles.

Table 5: Mandatory deployment type for Crosswork Data Gateway

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

Crosswork Data Gateway VM Requirements

The VM requirements Crosswork Data Gateway are listed in the following table.

Table 6: Crosswork Data Gateway Requirements for on-premise applications

Requirement	Description
Data Center	VMware. See Installation Requirements in VMware vCenter, on page 23 . Amazon EC2. See Installation Requirements in AWS EC2, on page 31 .

Requirement	Description			
Interfaces	<p>Minimum: 1</p> <p>Maximum: 3</p> <p>Cisco Crosswork Data Gateway can be deployed with either 1, 2, or 3 interfaces as per the combinations below:</p> <p>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.</p>			
	No. of NICs	vNIC0	vNIC1	vNIC2
	1	<ul style="list-style-type: none"> • Management Traffic • Control/Data Traffic • Device Access Traffic 	—	—
	2	<ul style="list-style-type: none"> • Management Traffic 	<ul style="list-style-type: none"> • Control/Data Traffic • Device Access Traffic 	—
	3	<ul style="list-style-type: none"> • Management Traffic 	<ul style="list-style-type: none"> • Control/Data Traffic 	<ul style="list-style-type: none"> • Device Access Traffic
	<ul style="list-style-type: none"> • Management traffic: for accessing the Interactive Console and passing the Control/Data information between servers (for example, a Crosswork application to Crosswork Data Gateway). • 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 access and data collection. <p>Note Due to security policies, traffic from subnets of a vNIC received on other vNICs is dropped. For example, in a 3 vNIC model setup, all device traffic (incoming and outgoing) must be routed through vNIC2. Crosswork Data Gateway drops device traffic received over vNIC0 and vNIC1.</p>			

Requirement	Description
IP Addresses	<p>1 or 2 IPv4 or IPv6 addresses based on the number of interfaces you choose to use. Including one additional IP address to be used as the Virtual IP (VIP) address. For more information, refer to the <i>Interfaces</i> section in the Table 27: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 66 table.</p> <p>Note Crosswork does not support dual stack configurations. Therefore, ALL addresses for the environment must be either IPv4 or IPv6.</p> <p>In a 3- NIC deployment, you will need to provide an IP address for Management interface (vNIC0) and Control/Data interface (vNIC1) only during installation. A virtual IP address for Device Access Traffic (vNIC2) is assigned when you create a Crosswork Data Gateway pool as explained in the Section: <i>Create a Crosswork Data Gateway Pool</i> in the Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide.</p>
NTP Servers	<p>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. Verify that the NTP IP address or host name is reachable on the network or installation will fail.</p> <p>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.</p>
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.
(optional) Proxy Server	<p>URL of an optional management network proxy server if your environment.</p> <p>If your environment requires an HTTP or HTTPS proxy in order to access URLs on the public Internet, you must configure a proxy server in order for the Cisco Crosswork Data Gateway to successfully connect to Cisco Crosswork</p>
(optional) Syslog Sever	The hostname or IPv4 or IPv6 address of an external syslog server.
(optional) Auditd Server	The hostname or IPv4 or IPv6 address of an external auditd server.

Port requirements

Crosswork Cluster Port Requirements

The following ports are needed by the Crosswork Cluster to operate correctly.



Note Crosswork cluster ports allow bidirectional flow of information.

Table 7: External Ports used by Crosswork Cluster

Port	Protocol	Used for
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)
30606	TCP	Docker Registry
30621	TCP	For FTP (available on data interface only). The additional ports used for file transfer are 31121 (TCP), 31122 (TCP), and 31123 (TCP). This port is available only when the supported application is installed on Cisco Crosswork and the FTP settings are enabled.
30622	TCP	For SFTP (available on data interface only) This port is available only when the supported application is installed on Cisco Crosswork and the SFTP settings are enabled.
49152:49370	TCP	GlusterFS

Table 8: Ports used by other Crosswork components

Port	Protocol	Used for
30602	TCP	to monitor the installation (Crosswork Network Controller)

Port	Protocol	Used for
30603	TCP	Crosswork Network Controller Web User interface (NGINX server listens for secure connections on port 443)
30607	TCP	Crosswork Data Gateway vitals collection
30608	TCP	Data Gateway gRPC channel with Data Gateway VMs
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.

Table 9: Destination Ports used by Crosswork Cluster

Port	Protocol	Used for
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

Crosswork Data Gateway Port Requirements

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

Inbound: Crosswork Data Gateway listens on the specified ports.

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

Table 10: 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



Note SCP port can be tuned.

Table 11: 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

Port	Protocol	Used for	Direction
6514	TLS	Syslog Collector	Inbound
9898	TCP	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.	
9514	UDP		
Site Specific Default ports differ from XR, XE to vendor. Check platform-specific documentation.	TCP	gNMI Collector	Outbound

Table 12: 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

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 13: Protected IP Subnets

IP Type	Subnet	Remarks
IPv4	172.17.0.0/16	Docker 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

Integration Requirements for other Cisco Products

This section explains the requirements to integrate with other Cisco Products.

Integrated Components

Ensure that you have installed compatible versions of the integrated components such as Cisco NSO, Cisco NED, and Cisco SR-PCE.

Table 14: Integrated Components - compatible versions

Software/Driver	Version
Cisco Network Services Orchestrator (Cisco NSO)	5.7.6 or higher 5.7.x version For install instructions, see the relevant NSO documentation . Additionally, for Cisco NSO LSA setup, see (Optional) Set up Cisco NSO Layered Service Architecture , on page 22.
Cisco Network Element Driver (NED) Note Cisco NEDs must be installed only for the device types and versions that you are managing. For example, if you are using NETCONF, then you must install the NED that corresponds to your IOS XR version(s). Similarly, Cisco IOS CLI NED must be installed if you have IOS devices in the network.	Cisco IOS XR: • CLI: 7.40.1 • NETCONF: 7.3.2, 7.315, 7.4.2, 7.5.2, 7.6, 7.7.1 Cisco IOS: • CLI: 6.77.9
Cisco Segment Routing Path Computation Element (SR-PCE)	Cisco IOS XR 7.7.1 For install instructions, see the Cisco IOS XRv 9000 Router Installation Guide .

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 on Cisco NSO to make the products compatible. The table below provides references to each FP installation procedure:

Table 15: List of mandatory Function Packs

Crosswork Product	Required Function Pack documentation
Crosswork Network Controller Essentials package <ul style="list-style-type: none"> Crosswork Optimization Engine Crosswork Active Topology 	<ul style="list-style-type: none"> Cisco NSO Transport SDN Function Pack Bundle 4.1.0 User Guide Cisco NSO Transport SDN Function Pack Bundle 4.1.0 Installation Guide Cisco Network Services Orchestrator DLM Service Pack 4.4.0 Installation Guide Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 4.4.0-116 Installation Guide

Crosswork Product	Required Function Pack documentation
Crosswork Network Controller Advantage package (combination of Crosswork Active Topology & Crosswork Optimization Engine) <ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • Cisco NSO Transport SDN Function Pack Bundle 4.1.0 User Guide • Cisco NSO Transport SDN Function Pack Bundle 4.1.0 Installation Guide • Cisco Network Services Orchestrator DLM Service Pack 4.4.0 Installation Guide • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 4.4.0-116 Installation Guide • Cisco Crosswork Change Automation NSO Function Pack 4.4.0 Installation Guide
Crosswork Health Insights	<ul style="list-style-type: none"> • Cisco Network Services Orchestrator DLM Service Pack 4.4.0 Installation Guide
Crosswork Change Automation	<ul style="list-style-type: none"> • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 4.4.0-116 Installation Guide • Cisco Crosswork Change Automation NSO Function Pack 4.4.0 Installation Guide
Crosswork Optimization Engine	<ul style="list-style-type: none"> • Cisco Network Services Orchestrator DLM Service Pack 4.4.0 Installation Guide • Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 4.4.0-116 Installation Guide

(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](#).

Supported Web Browsers

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

Table 16: Supported Web Browsers

Browser	Version
Google Chrome (recommended)	92 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 4.4 and Applications Administration Guide](#).

Installation Requirements in VMware vCenter

- [VMware Resource Requirements, on page 23](#)
- [VMware Settings, on page 25](#)
- [Supported Network Topology Models, on page 26](#)

VMware Resource Requirements

This section explains the resource requirements needed for each VM to deploy Crosswork in VMware.



Important Ensure that you have installed compatible versions of Cisco NSO and Cisco SR-PCE, and have installed all mandatory Function Packs.

The following table shows the VM requirements for various use cases and combinations of applications:

Table 17: VM Requirements in VMware

Component	vCPU	Clock Freq (GHz)	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data disk)
Crosswork Infrastructure	12	>= 2.20	96 GB	10 Gbps Minimum clock reservation: 18 GHz	1 TB
CDG On-Premise Standard	12	>= 2.20	48 GB	10 Gbps	70 GB (50 GB + 20 GB)
CDG On-Premise Extended	20	>= 2.20	112 GB	10 Gbps	570 GB (50 GB + 520 GB)
Cisco NSO 3	16	>= 2.20	128 GB	10 Gbps	1 TB
Cisco SR-PCE 4	8	>= 2.20	24 GB	10 Gbps	70 GB

³ NSO footprint depends on the type of deployment, standalone or non-LSA

⁴ SR-PCE count will depend on the number of head-ends that need to be managed



Note The disk requirements does not include RAID configuration as this may change based on your production requirements.

Things to note for Crosswork Infrastructure VMs:

- In addition to the storage for each VM, additional space will be needed in the datacenter to store the build images, application packages, and backups.
- 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.
- Ensure you have configured a SCP server with sufficient storage (at least 25 GB) to make backups of Cisco Crosswork.

VMware Settings

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. For more information on manual installation, see [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 48](#).

- 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).
- The machine where you run the installer must have network connectivity to the vCenter data center 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 [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 48](#).
- 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.
- 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

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.

Supported Network Topology Models

This section introduces the different topology models, their corresponding network components that you can employ to deploy and use Cisco Crosswork in VMware. 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

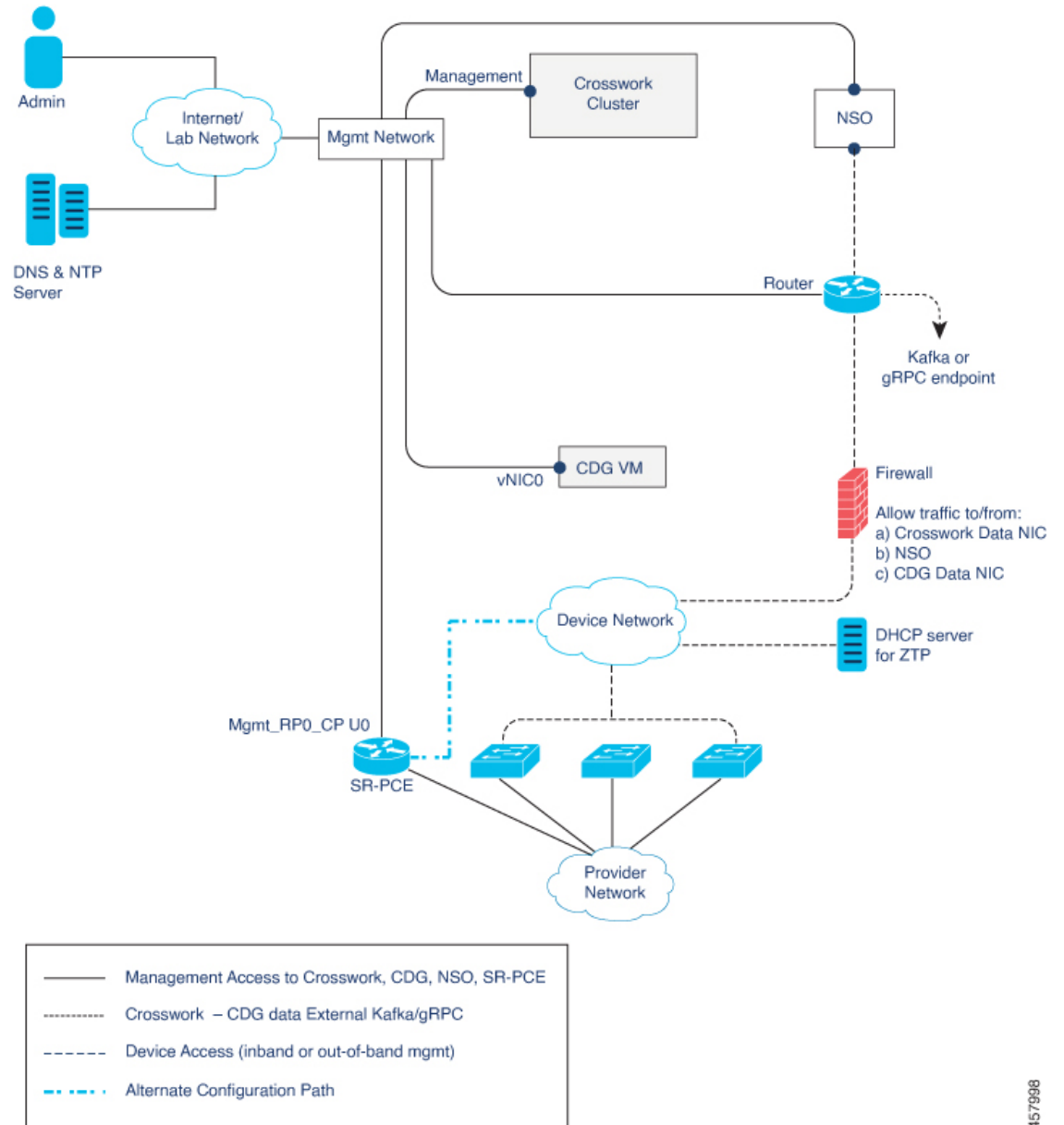
The IP/subnet addressing scheme on each of these domains depends on the type of deployment.

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.

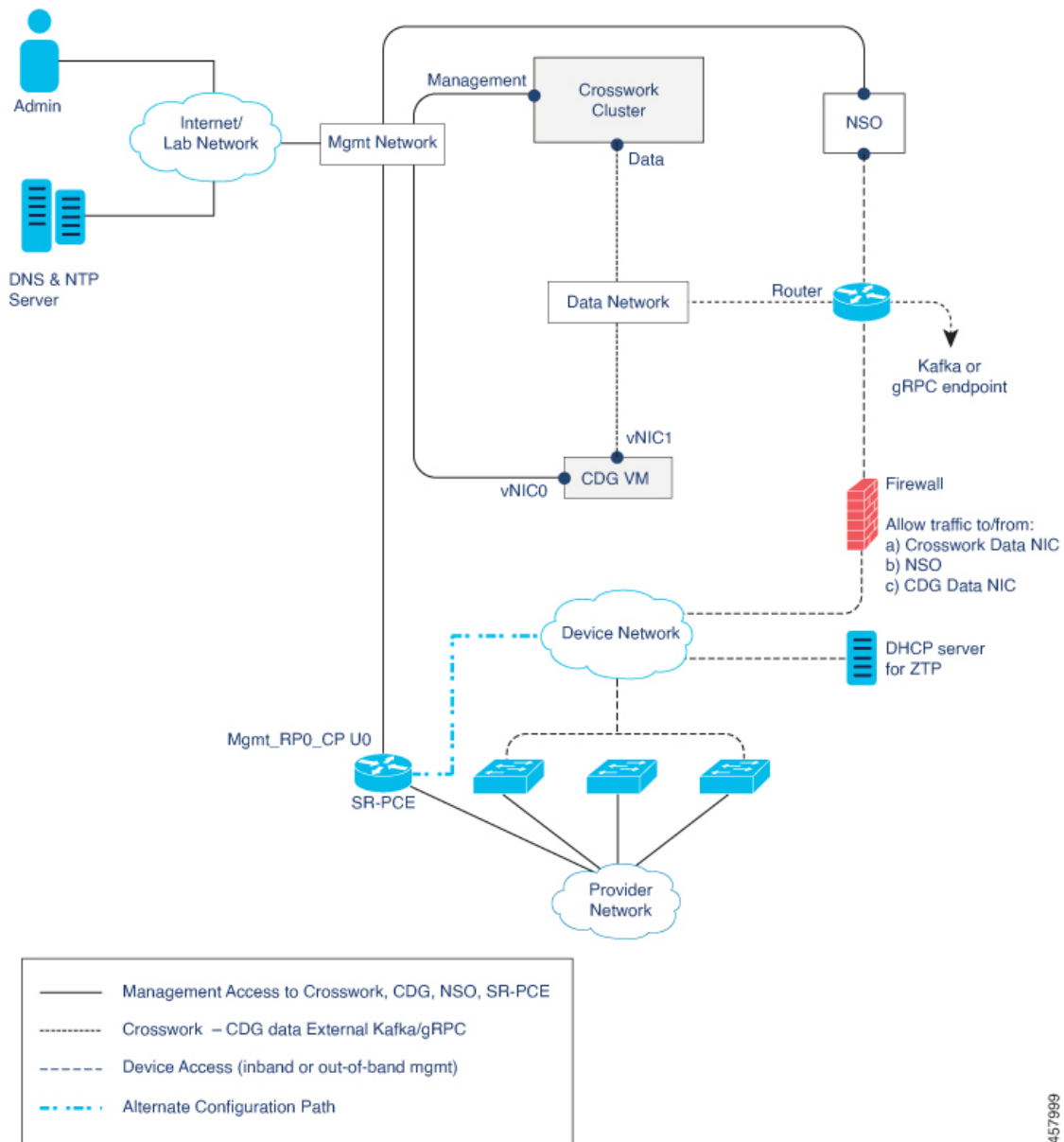
There are three types of traffic flowing between the network components, are explained below:

Figure 1: Cisco Crosswork - 1 NIC Network Topology



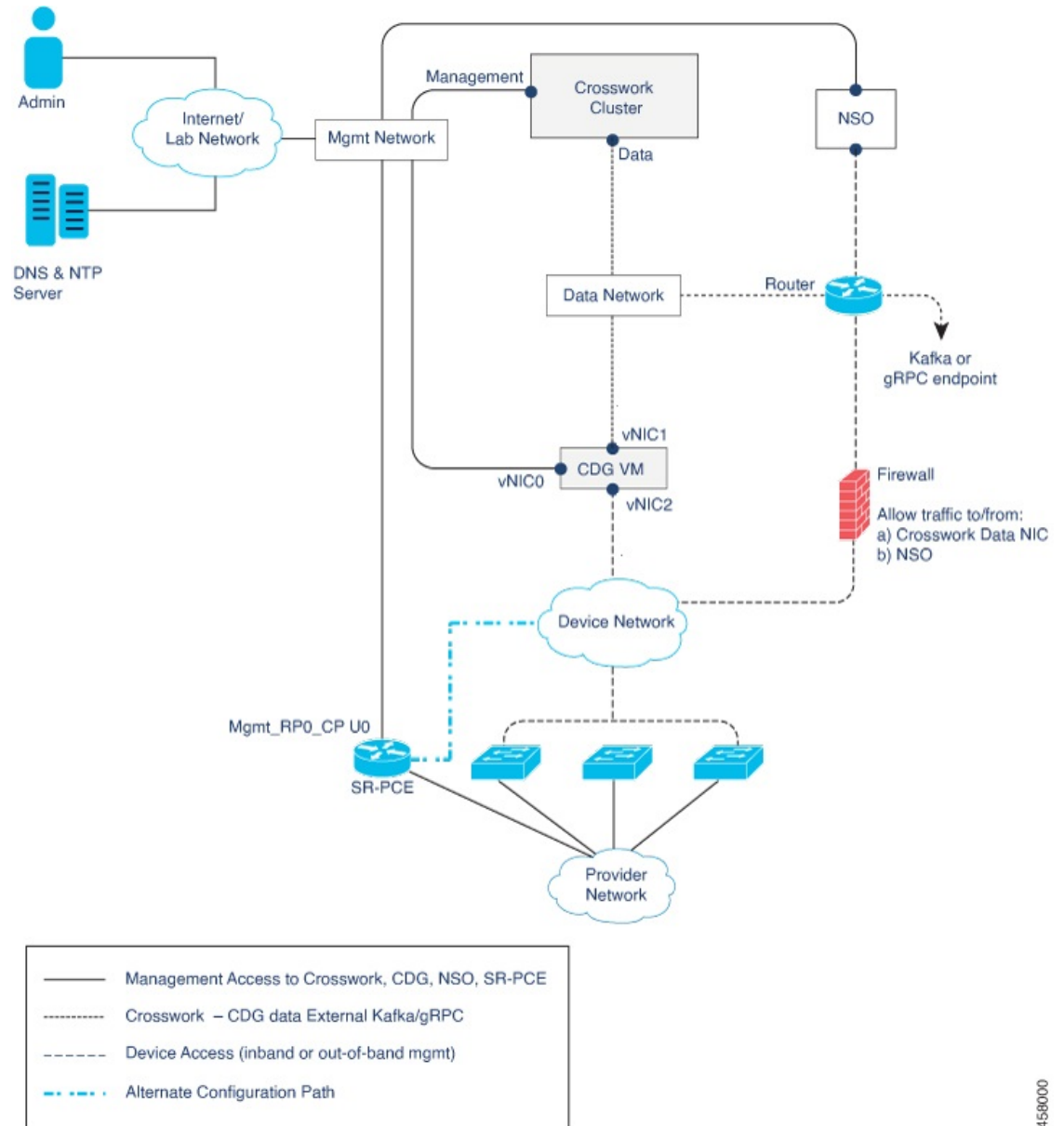
457998

Figure 2: Cisco Crosswork - 2 NIC Network Topology



457989

Figure 3: Cisco Crosswork - 3 NIC Network Topology



458000

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 4.4 and Applications Administration Guide](#).

ZTP Requirements

If you plan to use Zero Touch Provisioning, the device network needs to be equipped with DHCP and TFTP servers (not provided with Cisco Crosswork). All ZTP options require DHCP, PNP also requires the TFTP server too. 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. For more information on Zero Touch Provisioning concepts and features, please refer to the *Zero Touch Provisioning* chapter in the [Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide](#).

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).

Installation Requirements in AWS EC2

Amazon Web Services Elastic Compute Cloud (AWS EC2) is a web service that provides resizable computing capacity that you use to build and host Crosswork.

- [AWS Resource Requirements, on page 31](#)
- [AWS EC2 Settings, on page 33](#)

Crosswork can be deployed in AWS EC2 using the following methods:

- **Using CloudFormation:** The CloudFormation process is faster and less error-prone than the manual procedure to build the cluster, however you must have the necessary skills to prepare a CloudFormation template with details of the cluster deployment.
- **Manually deploying each VM:** The manual deployment process is simpler, but it takes time and must be repeated for each VM in your cluster. The manual process requires a smaller scripts ("user data") which must be created for each VM in your cluster.

AWS Resource Requirements

This section explains the resource requirements needed for each VM to deploy Crosswork in Amazon EC2.



Important Ensure that you have installed compatible versions of Cisco NSO and Cisco SR-PCE, and have installed all mandatory Function Packs. For more information, see the [Integration Requirements for other Cisco Products](#), on page 20.

The following table shows the VM requirements for various use cases and combinations of applications:

Table 21: VM Requirements in Amazon

Component	vCPU	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data Disk)
Crosswork Infrastructure	12 Minimum clock reservation: 18 GHz	96 GB	10 Gbps	1 TB
CDG On-Premise Standard	12	64 GB	10 Gbps	70 GB (50 GB + 20GB)
CDG On-Premise Extended	24	128 GB	10 Gbps	570 GB (50 GB + 520 GB)
Cisco NSO 5	16	128 GB	10 Gbps	1 TB
Cisco SR-PCE 6	8	24 GB	10 Gbps	70 GB

⁵ NSO footprint depends on the type of deployment, standalone or non-LSA

⁶ SR-PCE count will depend on the number of head-ends that need to be managed

Things to note for Crosswork Infrastructure VMs:

- In addition to the storage for each VM, additional space will be needed in the datacenter to store the build images, application packages, and backups.
- 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.
- One or more VM data stores need to have disk access latency of < 10 ms.
- Upgrade of the cluster temporarily requires double the total disk space used by the cluster.
- Ensure you have configured an SCP server with sufficient storage (at least 25 GB) to make backups of Cisco Crosswork.

AWS EC2 Settings

This section describes the settings that must be configured to install Crosswork cluster and Crosswork Data Gateway on AWS EC2.



Attention Most of the requirements discussed in this section are AWS EC2 concepts and not imposed exclusively by Crosswork.

Requirement	Description
VPC & Subnets	<p>VPC (Virtual Private Cloud) is created and configured with dedicated subnets for Crosswork and Crosswork Data Gateway (Management, Data, and Device) interfaces. Ensure that you do not violate Restrictions, on page 19 section.</p> <p>Note The Crosswork cluster does not support launching instances in multiple availability zones. All instances are linked to the same availability zone.</p>
Endpoints	<p>An endpoint is created in your VPC with the following parameters:</p> <ul style="list-style-type: none"> • Service name: EC2 service for the region (availability zone) where you are deploying. • Private DNS names: Enabled • Endpoint type: Interface • Under Subnets, specify the management subnet that you intend to use for the installation. For the other subnets for the Crosswork VM and the Crosswork Data Gateway VM, ensure that you specify subnets that the endpoint has access to the subnets.
IAM role	<p>A role is created in Identity and Access Management (IAM) with relevant permission policies and permissions with credentials that are valid for short durations. Roles can be assumed by entities.</p> <p>Note</p> <ul style="list-style-type: none"> • The minimum permissions required for a Crosswork role are ec2:AssignPrivateIpAddresses and ec2:UnassignPrivateIpAddresses. • The trust policy for your role must have the "Action": "sts:AssumeRole".
Key pairs	Key pairs (private keys used to log into the VMs) are created and configured.
Placement Groups	<p>A placement group of <i>Cluster</i> strategy is created.</p> <p>In a <i>cluster</i> placement group, instances are logically grouped in a single availability zone to increase network throughput.</p> <p>This requirement is required only for launching the Crosswork cluster instances.</p>

Requirement	Description
IP addresses	<p>Crosswork cluster: 2 IP subnets, one for the Management network and one for Data network, w node being deployed (Hybrid or Worker) and one additional IP address to be used as the Virtual requires Worker nodes, you will need a Management and Data IP address for each Worker node</p> <p>When using single NIC, you require one IP address (IPv4 or IPv6) for each node being deployed IP address to be used as the Virtual IP (VIP) address. When using dual NICs (one for the Manag network), you require a management and data IP address (IPv4 or IPv6) for each node being depl IP addresses to be used as the management and data Virtual IP (VIP) address.</p> <p>For example, in the case of a 3 VM cluster with a single NIC, you need 4 IP addresses, and in th you need 8 IP addresses (4 for management network and 4 for data network).</p> <p>Crosswork Data Gateway: IP addresses for Management Traffic and Data Traffic only. IP add during Crosswork Data Gateway pool creation as explained in the Section: <i>Create a Crosswork L Infrastructure 4.4 and Applications Administration Guide</i>.</p> <ul style="list-style-type: none"> • The IP addresses must be able to reach the gateway address for the network where Cisco C or the installation will fail. • At this time, your IP allocation is permanent and cannot be changed without re-deploymen Customer Experience team.
Security group	A security group must be created and configured to specify which ports or traffic are allowed. F Port requirements, on page 15 .
Instance type	<p>The resource profile for your instance deployment.</p> <p>Crosswork Cluster:</p> <ul style="list-style-type: none"> • Select m5.4xlarge for demos or lab deployments. • Select m5.8xlarge for production deployments. <p>Crosswork Data Gateway (production and lab deployments):</p> <ul style="list-style-type: none"> • Standard - Select m5.4xlarge • Extended - Select m5.8xlarge
CloudFormation (CF) template	<p>The CF template (.yaml) files for Crosswork cluster and Crosswork Data Gateway VMs that mus CloudFormation templates procedure. For more information, see:</p> <ul style="list-style-type: none"> • Install Cisco Crosswork on AWS EC2 using CloudFormation Template, on page 58 • Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template, on pag
User data	<p>The VM-specific parameters script that must be specified during the manual installation proced</p> <ul style="list-style-type: none"> • Install Crosswork Cluster on Amazon EC2 Manually , on page 59 • Install Crosswork Data Gateway on Amazon EC2 Manually , on page 88



CHAPTER 3

Install the Crosswork Cluster

This chapter contains the following topics:

- [Installation Parameters](#), on page 35
- [Install Cisco Crosswork on VMware vCenter](#), on page 39
- [Install Crosswork Cluster on AWS EC2](#), on page 57
- [Log into the Cisco Crosswork UI](#), on page 62

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 Installation Requirements](#), on page 9.



Note Some of the below parameters may be named differently depending upon the destination platform (vCenter or Amazon EC2), the installation method (automated or manual), and IP stack (IPv4 or IPv6) you choose.



Note Secure ZTP and Secure Syslog require the Crosswork cluster to be deployed with FQDN.

Table 22: General parameters

Parameter Name	Description
ClusterName	Name of the cluster file
ClusterIPStack	The IP stack protocol: IPv4 or IPv6
ManagementIPAddress	The Management IP address of the VM (IPv4 or IPv6).
ManagementIPNetmask	The Management IP subnet in dotted decimal format (IPv4 or IPv6).
ManagementIPGateway	The Gateway IP on the Management Network (IPv4 or IPv6). The address must be reachable, otherwise the installation will fail.

Parameter Name	Description
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	The Data IP address of the VM (IPv4 or IPv6).
DataIPNetmask	The Data IP subnet in dotted decimal format (IPv4 or IPv6).
DataIPGateway	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	The IP address of the DNS server (IPv4 or IPv6). The address must be reachable, otherwise the installation will fail.
NTP	NTP server address or name. The address must be reachable, otherwise the installation will fail.
DomainName	The domain name used for the cluster.
CWusername	Username to log into Cisco Crosswork. This is an optional parameter.
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. Value is <code>large</code> .
VMName	Name of the VM You will require at least 3 unique names (one for each VM).
VMType	Indicates the type of VM. Choose either "Hybrid" or "Worker". Note The Crosswork cluster for 4.5 release requires at least three VMs operating in a hybrid configuration.

Parameter Name	Description
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. This parameter is optional for installing using the cluster installer tool.
InitNodeCount	Total number of nodes in the cluster including Hybrid and Worker nodes. The default value is 3. This parameter is optional for installing using the cluster installer tool.
InitMasterCount	Total number of Hybrid nodes in the cluster. The default value is 3. This parameter is optional for installing using the cluster installer tool.
BackupMinPercent	Minimum percentage of the data disk space to be used for the size of the backup partition. The default value is 50 (valid range is from 1 to 80). Please use the default value unless recommended otherwise. Note The final backup partition size will be calculated dynamically. This parameter defines the minimum.
ManagerDataFsSize	Refers to the data disk size for Hybrid nodes (in Giga Bytes). This is an optional parameter and the default value is 450 (valid range is from 450 to 8000), if not explicitly specified. Please use the default value unless recommended otherwise.
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 VMware Resource Requirements, on page 23 for more information). This is an optional parameter and the default value is <code>true</code> , if not explicitly specified. If set as <code>true</code> , 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 <code>false</code> (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	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 <code>RamDiskSize</code> , the <code>HSDatastore</code> value is not used.

Parameter Name	Description
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.
SchemaVersion	The configuration Manifest schema version
LogFsSize	Log partition size (in Giga Bytes). Minimum value is 10 GB and Maximum value is 1000 GB.

Table 23: VMware template parameters

Parameter Name	Description
vCenterAddress	The vCenter IP or host name.
vCenterUser	The username needed to log into vCenter.
vCenterPassword	The password needed to log into vCenter.
DCname	The name of the Data Center resource to use.
MgmtNetworkName	The name of the vCenter network to attach to the VM's Management interface.
DataNetworkName	The name of the vCenter network to attach to the VM's Data interface.
Host	The ESXi host or resource group name.
Datastore	The datastore name available to be used by this host or resource group.
HSDatastore	The high speed datastore available for this host or resource group.
DCfolder	The resource folder name on vCenter. Leave as empty if not used.
Cw_VM_Image	The name of Crosswork cluster VM image in vCenter. If left blank, the name is generated from the uploaded image.
HostedCwVMs	The IDs of the VMs to be hosted by the ESXi host or resource. These have to match to the Crosswork cluster VM.

Table 24: Amazon EC2 template parameters

Parameter Name	Description
ManagementPeerIPs	The Management IP addresses of all the deployed VMs.
DataPeerIPs	The Data IP addresses of all the deployed VMs.
AwsIamRole	The Identity and Access Management (IAM) user id created for by your AWS account administrator to build the cluster virtual machines.

Parameter Name	Description
K8sServiceNetwork	The network address for the kubernetes service network. The CIDR range is fixed to '/16'. This is an optional parameter.
K8sPodNetwork	The network address for the kubernetes pod network. The CIDR range is fixed to '/16'. This is an optional parameter.

Install Cisco Crosswork on VMware vCenter

This section describes how Cisco Crosswork is installed on VMware vCenter:

- [Install Cisco Crosswork on VMware vCenter using Cluster Installer tool , on page 39:](#)

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.

- [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 48](#)

Install Cisco Crosswork on VMware vCenter using Cluster Installer tool

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



Attention The file names mentioned in this topic are sample names and may differ from the actual file names in [cisco.com](https://www.cisco.com).

Before you begin

Few pointers to know when using the cluster installer tool:

- Make sure that your environment meets all the vCenter requirements specified under [Crosswork Cluster VM Requirements, on page 10](#) and [Installation Requirements in VMware vCenter, on page 23](#).
- 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 and the vCenter password). 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 the 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.
- Docker version 19 or higher is required while using the cluster installer option. For more information on Docker, see <https://docs.docker.com/get-docker/>
- 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 131](#).

- A VM redeployment will delete the VM's data, hence caution is advised. We recommend you 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.



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.

Step 1 In your vCenter datacenter, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch. In the virtual switch, select **Edit > Security**, and configure the following DVS port group properties:

- Set **Promiscuous mode** as *Reject*
- Set **MAC address changes** as *Reject*

Confirm the settings and repeat the process for each virtual switch used in the cluster.

Step 2 In your Docker capable machine, create a directory where you will store everything you will use during this installation.

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

Step 3 Download the installer bundle (.tar.gz file) and the OVA file from [cisco.com](https://www.cisco.com) to the directory you created previously. For the purpose of these instructions, we will use the file names as "**cw-na-platform-4.4.0-signed-installer.tar.gz**" and "**cw-na-platform-4.4.0-250-release-221027.ova**" respectively.

Step 4 Use the following command to unzip the installer bundle:

```
tar -xvf cw-na-platform-4.4.0-signed-installer.tar.gz
```

The contents of the installer bundle is unzipped to a new directory (e.g. `cw-na-platform-4.4.0-signed-installer`). This new directory will contain the installer image (e.g. `cw-na-platform-installer-4.4.0-250-release-221027.tar.gz`) and files necessary to validate the image.

Step 5 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.

Step 6 Navigate to the directory created in the previous step and use the following command to verify the signature of the installer image:

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

If you are using python 2.x, use the following command 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 7 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-4.4.0-250-release-221027.tar.gz
```

Step 8 Run Docker image list or Docker images command to get the "image ID" (which is needed in the next step).

For example:

```
docker images
```

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-4.4.0-250-release-221027  a4570324fad30
      7 days ago        276MB
```

Note Pay attention to the "CREATED" time stamp in the table presented when you run `docker images`, 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 9 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. Docker requires 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 on your local disk when you run the commands, 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 read the template and the ova files, and to write the log files used during the install. If you encounter either of the following errors you should move the files to a directory where the path is in lowercase (all lowercase, no spaces or other special characters).

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 10

Navigate to the directory with the VMware template.

```
cd /opt/installer/deployments/4.4.0/vcenter
```

Step 11

Copy the template file found under

/opt/installer/deployments/4.4.0/vcenter/deployment_template_tfvars to the /data folder using a different name.

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

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

Step 12

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 35](#) table for details on the required and optional fields and their proper settings. The [Sample manifest template for VMware vCenter, on page 135](#) includes an example that you can reference for proper formatting. The example is more compact due to the removal of descriptive comments:

- Crosswork cluster information such as VM size: Use "Large" for production environments. For more information, see the storage profiles in [Crosswork Cluster VM 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.

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

Step 13 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-4.4.0-250-release-221027.ova
```

Step 14 Read, and then enter "yes" when prompted to accept the End User License Agreement (EULA).

Step 15 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/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark  
  
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 13) without the `-p` option. This will deploy the VMs serially rather than in parallel.

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

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.

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 44](#) 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 possible 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 credentials that you provided in the template during the install. In case the installer is unable to apply the credentials, it creates the administrative ID 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) to the vCenter 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.



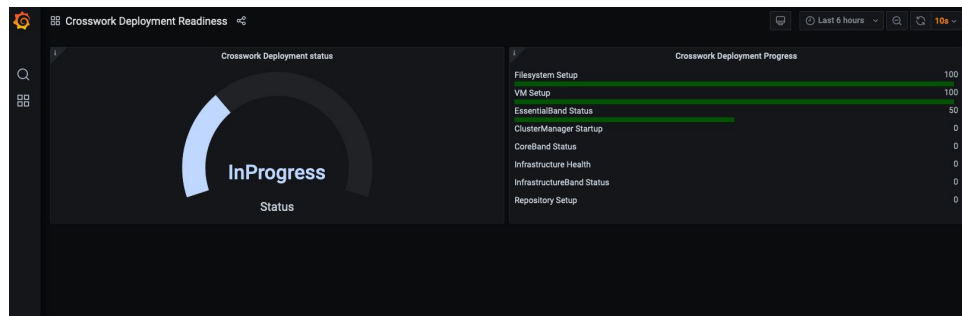
Note For VMware deployments, this activity can also be monitored from the vSphere UI.

3. After each VM is created, it is powered on (either automatically when the installer completes, or after you power on the VMs during the manual installation). The parameters specified in the template are applied to the VM, and it is rebooted. The VMs are then registered by Kubernetes to form the cluster.
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.

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}:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark`) 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 4: Crosswork Deployment Readiness



- **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. In the latter case, after logging in specify the `cs-admin` to be used, then switch to super user (`sudo su -` command) 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 62](#).

Failure Scenario

In the event of a failure 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.

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.

- 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 4.4 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.

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 written into the `/data` directory.

Scenario	Possible Resolution
Missing or invalid parameters	<p>The installer provides a clue as regards to the issue; however, in case of errors in the manifest file HCL syntax, these can be misleading. If you see "Type errors", check the formatting of the configuration manifest.</p> <p>The manifest file can also be passed as a simple JSON file. Use the following converter to validate/convert: https://www.hcl2json.com/</p>
Certificate Error	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.
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. 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 Installation Requirements in VMware vCenter, on page 23 .
Floating VIP address is not reachable	The VRRP protocol requires unique router_id advertisements 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.

Scenario	Possible Resolution																				
Crosswork VM is not allowing to log in	The password specified is not strong enough. Change the configuration manifest and redeploy.																				
Error conditions such as: <i>Error: Error locking state: Error acquiring the state lock: resource temporarily unavailable</i> <i>Error: error fetching virtual machine: vm not found</i> <i>Error: Invalid index</i>	These errors are common when re-running the installer after an initial run is interrupted (Control C, or TCP timeout, etc). Remediation steps are: <ol style="list-style-type: none"> 1. Run the clean operation (<code>./cw-installer.sh clean -m <your manifest here></code>) OR remove the VM files manually from the vCenter. 2. Remove the state file (<code>rm /data/crosswork-cluster.tfstate</code>) and retry. 																				
Deployment fails with: <i>Failed to validate Crosswork cluster initialization.</i>	The clusters' seed VM is either unreachable or one or more of the cluster VMs have failed to get properly configured. <ol style="list-style-type: none"> 1. Check whether the VM is reachable, and collect logs from <code>/var/log/firstBoot.log</code> and <code>/var/log/vm_setup.log</code> 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: <pre>sudo kubectl get nodes</pre> A healthy output for a 3-node cluster is: <table border="1"> <thead> <tr> <th>NAME</th> <th>STATUS</th> <th>ROLES</th> <th>AGE</th> <th>VERSION</th> </tr> </thead> <tbody> <tr> <td>172-25-87-2-hybrid.cisco.com v1.16.4</td> <td>Ready</td> <td>master</td> <td>41d</td> <td></td> </tr> <tr> <td>172-25-87-3-hybrid.cisco.com v1.16.4</td> <td>Ready</td> <td>master</td> <td>41d</td> <td></td> </tr> <tr> <td>172-25-87-4-hybrid.cisco.com v1.16.4</td> <td>Ready</td> <td>master</td> <td>41d</td> <td></td> </tr> </tbody> </table> In case of a different output, collect the following logs: <code>/var/log/firstBoot.log</code> and <code>/var/log/vm_setup.log</code> In addition, for any cluster nodes not displaying the Ready state, collect: <pre>sudo kubectl describe node <name of node></pre>	NAME	STATUS	ROLES	AGE	VERSION	172-25-87-2-hybrid.cisco.com v1.16.4	Ready	master	41d		172-25-87-3-hybrid.cisco.com v1.16.4	Ready	master	41d		172-25-87-4-hybrid.cisco.com v1.16.4	Ready	master	41d	
NAME	STATUS	ROLES	AGE	VERSION																	
172-25-87-2-hybrid.cisco.com v1.16.4	Ready	master	41d																		
172-25-87-3-hybrid.cisco.com v1.16.4	Ready	master	41d																		
172-25-87-4-hybrid.cisco.com v1.16.4	Ready	master	41d																		
The following error is displayed while uploading the image: <i>govc: The provided network mapping between OVF networks and the system network is not supported by any host.</i>	The Dswitch on the vCenter is misconfigured. Please check whether it is operational and mapped to the ESXi hosts.																				

Scenario	Possible Resolution
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 <i>Error: timeout waiting for an available IP address</i>	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 VMware Settings, on page 25 .
When deploying on a vCenter, the following error is displayed towards the end of the VM bringup: Error processing disk changes post-clone: <i>disk.0: ServerFaultCode: NoPermission: RESOURCE (vm-14501:2000), ACTION (queryAssociatedProfile): RESOURCE (vm-14501), ACTION (PolicyIDByVirtualDisk)</i>	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 <i>Error: cannot locate virtual machine with UUID "xxxxxxx": virtual machine with UUID "xxxxxxx" not found</i>	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.

Manual Installation of Cisco Crosswork using vCenter vSphere UI

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

The manual installation workflow is broken into two parts:

1. [Build the template, on page 49](#)
2. [Deploy the template, on page 54](#)

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).



Important In case of manual installation of Crosswork Cluster, you must import a cluster inventory file (.tfvars file) to the Crosswork UI. The inventory file (a sample can be downloaded from the Crosswork UI) will contain information about the VMs in your cluster along with the data center parameters. Cisco Crosswork cannot deploy or remove VM nodes in your cluster until you complete this operation. For more information, see the *Import Cluster Inventory* topic in the [Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide](#).

Before you begin:

- Make sure that your environment meets all the vCenter requirements specified under [Crosswork Cluster VM Requirements, on page 10](#) and [Installation Requirements in VMware vCenter, on page 23](#).

Build the template

- 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** In the vSphere UI, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch. In the virtual switch, select **Edit > Security**, and configure the following DVS port group properties:
- Set **Promiscuous mode** as *Reject*
 - Set **MAC address changes** as *Reject*
- Confirm the settings and repeat the process for each virtual switch used in the cluster.
- Step 4** Review and confirm that your network settings meet the requirements.
- Step 5** 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 6** 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 7** 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 8** 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 9** 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 10** Review the OVF template that you are deploying. Note that this information is gathered from the OVF, and cannot be modified.
- Step 11** 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 12** Click **Next**. The **Deploy OVF Template** window is refreshed, with **6 - Configuration** highlighted. Choose the desired deployment configuration.

Figure 5: 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

	Description
<input checked="" type="radio"/> IPv4 Network	Use IPv4 network stack for management and data traffic.
<input type="radio"/> IPv6 Network	
<input type="radio"/> IPv4 Network on a Single Interface	
<input type="radio"/> IPv6 Network on a Single Interface	

4 Items

CANCEL BACK NEXT

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 recommended for lab deployments).

- Step 13** 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 6: 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.

CANCEL BACK NEXT

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 14 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 15 Click **Next**. The **Deploy OVF Template** window is refreshed, with **9 - Customize template** highlighted.

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

Figure 7: Customize template settings

Deploy OVF Template

4 properties have invalid values

- ✓ 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

Network	Settings
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 custom administrator username: cw-admin

CANCEL BACK NEXT

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

<ul style="list-style-type: none"> ✓ 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 <li style="background-color: #005596; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<div style="border: 1px solid #ccc; padding: 5px;"> <div style="background-color: #e6f2ff; padding: 2px; margin-bottom: 5px;"> Deployment Credentials 2 settings </div> <div style="border-bottom: 1px solid #ccc; padding: 5px;"> <p>Original VM Username Default system administrator username: cw-admin</p> <p><input type="text" value="cw-admin"/></p> </div> <div style="border-bottom: 1px solid #ccc; padding: 5px;"> <p>VM Password Password for the default system administrator account</p> <p>Password <input type="password" value="....."/></p> <p>Confirm Password <input type="password" value="....."/></p> </div> <div style="background-color: #e6f2ff; padding: 2px; margin-bottom: 5px;"> DNS and NTP Servers 3 settings </div> <div style="border-bottom: 1px solid #ccc; padding: 5px;"> <p>DNS IPv4 Address</p> <p>Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated.</p> <p><input type="text" value="8.8.8.8 8.8.4.4"/></p> </div> <div style="border-bottom: 1px solid #ccc; padding: 5px;"> <p>NTP Servers</p> <p>Please enter NTP server hostname. Multiple NTP servers can be provided space separated.</p> <p><input type="text" value="ntp.crosswork.com"/></p> </div> <div style="border-bottom: 1px solid #ccc; padding: 5px;"> <p>DNS Search Domain Please enter the DNS search domain.</p> <p><input type="text" value="crosswork.com"/></p> </div> <div style="background-color: #e6f2ff; padding: 2px; margin-bottom: 5px;"> Disk Configuration 5 settings </div> <div style="padding: 5px;"> <p>Logfs Disk Size Please enter the size of the logfs disk in GB.</p> </div> </div>
--	--

CANCEL
BACK
NEXT

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?

CANCEL
BACK
NEXT

Step 16 Click **Next**. The **Deploy OVF Template** window is refreshed, with **10 - Ready to Complete** highlighted.

Step 17 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 18 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 8: Select Storage - single data store

The screenshot shows the 'Select storage' step in the VMware Deploy From Template wizard. On the left, a progress list shows steps 1 through 6, with step 3 'Select storage' highlighted. The main area is titled 'Select storage' and contains the instruction 'Select the storage for the configuration and disk files'. There are two options for virtual disk format: 'Same format as source' (selected) and 'Configure per disk' (disabled). Below this is a 'VM Storage Policy' section with a dropdown menu set to 'Keep existing VM storage policies'. A table lists two 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

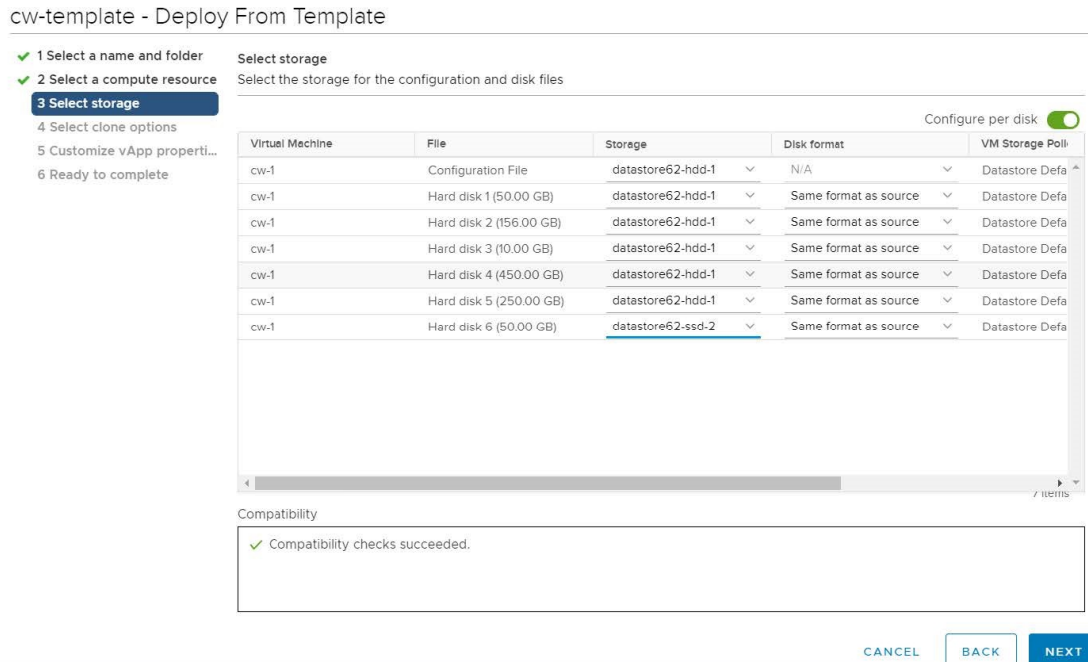
At the bottom, a 'Compatibility' section shows a green checkmark and the text 'Compatibility checks succeeded.' At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

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 9: Select Storage - Configure per disk



- 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 For non-lab environments, you need to 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 [Crosswork Cluster VM 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 (Optional) Use the **Reservation** field under the **Virtual Hardware** tab to set reservation for the VM's CPU allocation (in MHz) and memory profile (in MB).

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 44](#) 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* topic in the *Cisco Crosswork Infrastructure 4.5 and Applications Administration Guide*.

What to do next

After you login to Crosswork UI, please import the cluster inventory file (.tfvars file). For more information, see the *Import Cluster Inventory* topic in the *Cisco Crosswork Infrastructure 4.5 and Applications Administration Guide*.

Install Crosswork Cluster on AWS EC2

This section describes how Cisco Crosswork is installed on Amazon Web Services Elastic Cloud Compute (AWS EC2). For more information on the prerequisites, see [AWS EC2 Settings, on page 33](#).



Attention This document expects the user to be familiar with Amazon Web Services (AWS), Amazon EC2 concepts, and CloudFormation templates.

- [Install Cisco Crosswork on AWS EC2 using CloudFormation Template, on page 58](#)
- [Install Crosswork Cluster on Amazon EC2 Manually , on page 59](#)

Install Cisco Crosswork on AWS EC2 using CloudFormation Template

Amazon CloudFormation (CF) allows you to create stacks via a structured template (.yaml file), referred to in this section as the CF template. The CF template contains parameter details of all your VMs, and the prerequisite Amazon Web Services (AWS) settings. During the process, the CF template is uploaded into the AWS UI and CloudFormation provisions the resources that are described in your template to install the Crosswork VMs.

The CloudFormation process is faster and less error-prone than the manual procedure to build the cluster.



Note The terms 'stack' and 'instance' refers to cluster and VM respectively.

For more information on the CF template, see [Sample CloudFormation template for installing Crosswork Cluster VMs on AWS EC2, on page 137](#).



Important The CF template (.yaml file) referenced in this section contains the details to install a Crosswork cluster with 3 VMs. Please note that it is only a sample, and you will create a different CF template according to your production preferences and execute it as per the steps mentioned in this section.

Before you begin

Make sure that you have met all the requirements specified in [AWS EC2 Settings, on page 33](#).

-
- Step 1** Log in to AWS and search for the CloudFormation service. The CloudFormation dashboard opens.
- Step 2** Click **Stacks** from the side menu.
All existing stacks in the environment are displayed here.
- Step 3** Click **Create Stack > With new resources (standard)**.
The **Create Stack** window is displayed.
- Step 4** In **Step 1 - Specify template**, select the following settings:
- Under **Prepare template**, select **Template is ready**.
 - Under **Template source**, select **Upload a template file**.
 - Click **Choose file**, and select your CF template (.yaml file).
- Note** (Optional) Click **View in Designer** to view a visual representation of the execution flow in your CF template.
- Click **Next**.
- Step 5** In **Step 2 - Specify stack details**, enter relevant values for the stack name and each parameter field, and click **Next**.

Note The parameter field names visible in this window are defined by the parameters in your CF template. Generally, these fields include the AWS concepts mentioned in [AWS EC2 Settings, on page 33](#).

Step 6 In **Step 3 - Configure stack options**, enter the relevant values for the settings. Click **Next** to continue.

Note The stack options are not exclusive for installing Crosswork and can be configured based on your production preferences.

Step 7 In **Step 4- Review**, review the settings you have selected.

Step 8 Click the acknowledgement checkbox at the bottom, and click **Create stack** to initiate the stack creation.

Step 9 Navigate to the Stacks window (see step 2), to see the list of stacks. Select the stack you configured (status will be CREATE_IN_PROGRESS).

The stack details are displayed on the right side of the window.

Step 10 In your stack window, click on the each tab to view the status of the creation. For example, the **Outputs** tab displays if the IP addresses are assigned correctly to each interface in your Crosswork cluster.

Note Once a stack is created, export names are assigned to the VIP parameters (Data VIP and Management VIP), and they can be used to reference them in other CF templates. Changes to these export names are automatically updated downstream in the other stacks.

Step 11 Once the stack creation is completed (status will be CREATE_COMPLETE), click on the **Resources** tab, and click the Physical ID of the first instance in your stack (seed VM node).

The Instances window is displayed with details of the selected instance.

Step 12 Click **Connect** (top right corner). The **Connect to instance** window is displayed.

Step 13 Click on the **EC2 serial console** tab. Click **Connect** to connect to the console of the VM.

Step 14 Log in using the credentials specified in `CWUsername` and `CWPassword` parameters.

Step 15 Run the `kubectl get nodes` command to check if the VMs are available.

Install Crosswork Cluster on Amazon EC2 Manually

Follow the steps below to install Crosswork Cluster on Amazon EC2:

Before you begin

Make sure that you have met all the requirements specified in [AWS EC2 Settings, on page 33](#).



Attention

- The Launch instance workflow offers a wide range of launch options that you can set based on your preferences. The following procedure only addresses the mandatory settings that must be configured for the successful deployment of your Crosswork instance.
- The following procedure addresses the launching of Crosswork cluster with 3 VM instances. This procedure can also be used to launch a Worker VM node by setting the `VMType` as "Worker".

Step 1 Download the Crosswork AMI (Amazon Machine Image) file from cisco.com to a location accessible from your Amazon Web Services (AWS).

Step 2 Prepare the user data for Crosswork Cluster VMs (see sample below):

Attention This is a sample user data for a seed VM. Please use it as a reference to create user data based on your production preferences. You need to create similar user data for each VM in your cluster.

```
<PropertySection>
  <Property oe:key="CWPassword" oe:value="{CNCSSHPassword}"/>
  <Property oe:key="CWUsername" oe:value="cw-admin"/>
  <Property oe:key="CwInstaller" oe:value="False"/>
  <Property oe:key="DNSv4" oe:value="169.254.169.253"/>
  <Property oe:key="DNSv6" oe:value=":0"/>
  <Property oe:key="DataIPv4Address" oe:value="10.10.2.201"/>
  <Property oe:key="DataIPv4Gateway" oe:value="10.10.2.1"/>
  <Property oe:key="DataIPv4Netmask" oe:value="255.255.255.0"/>
  <Property oe:key="DataIPv6Address" oe:value=":0"/>
  <Property oe:key="DataIPv6Gateway" oe:value=":1"/>
  <Property oe:key="DataIPv6Netmask" oe:value="64"/>
  <Property oe:key="DataVIP" oe:value="10.10.2.200"/>
  <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="3"/>
  <Property oe:key="IsSeed" oe:value="True"/>
  <Property oe:key="K8Orch" oe:value=""/>
  <Property oe:key="ManagementIPv4Address" oe:value="10.10.1.201"/>
  <Property oe:key="ManagementIPv4Gateway" oe:value="10.10.1.1"/>
  <Property oe:key="ManagementIPv4Netmask" oe:value="255.255.255.0"/>
  <Property oe:key="ManagementIPv6Address" oe:value=":0"/>
  <Property oe:key="ManagementIPv6Gateway" oe:value=":1"/>
  <Property oe:key="ManagementIPv6Netmask" oe:value="64"/>
  <Property oe:key="ManagementVIP" oe:value="10.10.1.200"/>
  <Property oe:key="NTP" oe:value="169.254.169.123"/>
  <Property oe:key="ManagerPeerIPs" oe:value="10.10.1.201 10.10.1.202 10.10.1.203"/>
  <Property oe:key="DataPeerIPs" oe:value="10.10.2.201 10.10.2.202 10.10.2.203"/>
  <Property oe:key="AwsIamRole" oe:value="SITEC2FullAccess"/>
  <Property oe:key="VMLocation" oe:value="default"/>
  <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="ssd" oe:value="50"/>
</PropertySection>
```

Step 3 Log in to AWS and search for the EC2 service. The EC2 dashboard is displayed.

Step 4 Click on **Launch Instance**. The **Launch an instance** window is displayed.

Step 5 Under **Name and tags**, provide a name for the instance deployment. You can also provide additional tags, if you choose.

Step 6 Under **Application and OS Images**, click on the **My AMI** tab, select **Owned by me**. Browse the dropdown list and select the Crosswork AMI file that you downloaded earlier.

Step 7 Under **Instance type**, select the resource profile for your instance. In case of production deployments, you are recommended to select **m5.8xlarge**.

Step 8 Under **Key Pair**, create a new key pair or select the key pair you created earlier.

Step 9 Under **Network Settings**, click **Edit** and make the following changes:

- a) Under **VPC**, select the relevant VPC.
- b) Under **Subnet**, provide the Management subnet that you created earlier.
- c) Set **Auto-assign public IP** as **Disabled**.
- d) Under **Firewall**, create a security group or select the security group you created earlier.
- e) Under **Advanced network configuration**, enter relevant values for **Network interface 1**.
 - **Description**: Provide a description.
 - **Primary IP**: Specify the Management IP address of your VM.
- f) Click **Add network interface**, and enter relevant values for **Network interface 2**.
 - **Description**: Provide a description
 - **Subnet**: Select the Data subnet that you created earlier.
 - **Security group**: Select the security group you created earlier.
 - **Primary IP**: Specify the Data IP address of your VM.

Note When you add a network interface, some fields (such as Subnet and Security group) may be prepopulated with values. Ensure that the values are consistent with the values you have selected earlier.

Step 10

Under **Configure Storage**, create the storage partitions for your instance. By default, three storage volumes added by AWS (click **Advanced** to view for more details). For Crosswork cluster, you need to add three additional custom storage volumes. Click on **Add new volume**, and specify the following values for each new volume:

Table 25: Configure Storage

Volume No.	Device Name	Size
Volume 4	/dev/sdc	10
Volume 5	/dev/sdd	450
Volume 6	/dev/sdm	10

Note You are recommended to use either gp3 or gp2 as **volume type** for optimum experience.

Step 11

Under **Advanced details**, enter the following mandatory information:

- a) Under **IAM instance profile**, create a new IAM profile or browse the dropdown and select the IAM role you created earlier.
- b) Under **Placement Group**, create a new placement group (*Cluster* strategy) or browse the dropdown and select the placement group you created earlier.
- c) Set **Metadata accessible** field as **Enabled**.
- d) Set **Metadata version** field as **V1 and V2 (token optional)**.
- e) Set **Metadata response hop limit** as **2**.
- f) In the **User data** field, paste the template containing the parameters for your VM.

Note If you are providing the VM parameters in a base64 encoded format instead of text, select the corresponding checkbox.

Step 12

Click **Launch instance**. A message is displayed about successfully initiating the launch of the instance.

- Step 13** Repeat steps 3 to 12 for the remaining VM instances in your cluster.
- Step 14** After all instances are launched, go to the EC2 dashboard, and click on **Instances** (on the side menu) to view the launched instances. The instances window is displayed. You can search for the instance using the name, attributes or tags.
- Note** After all VM instances are launched correctly, it can take a while (minimum of 45 minutes) for the VMs to be ready and functional.
- Step 15** To verify the installation, select your seed VM and click **Connect** (top right corner). The **Connect to instance** window is displayed.
- Step 16** Click on the **EC2 serial console** tab. Click **Connect** to connect to the console of the VM.
- Step 17** Log in using the credentials specified in `CWUsername` and `CWPassword` parameters.
- Step 18** Run the `kubectl get nodes` command to check if the VMs are available.

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 AWS EC2 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.

Step 1 Launch one of the supported browsers (see [Supported Web Browsers](#), on page 23).

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.

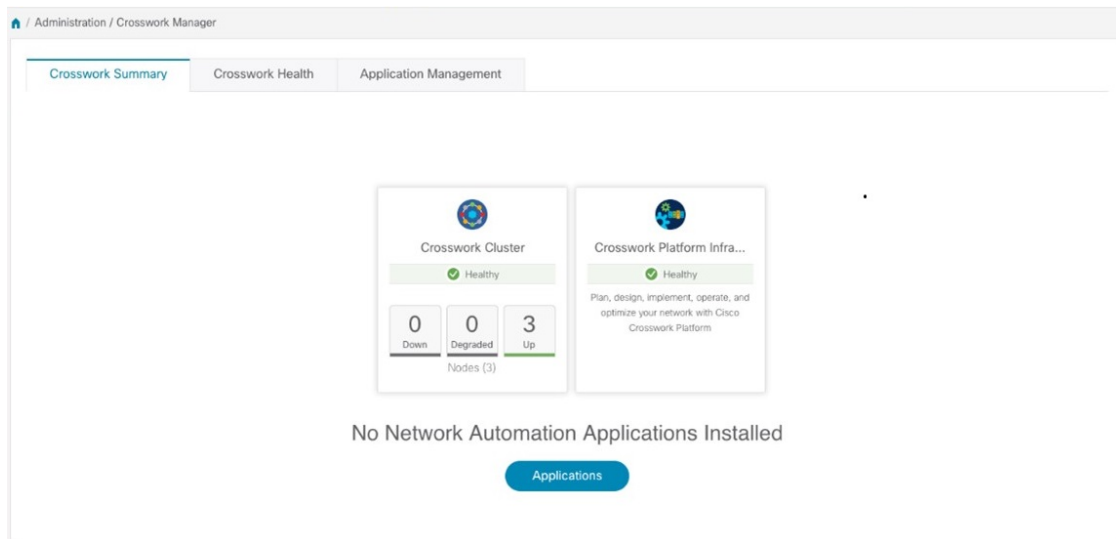
Note When you access the Cisco Crosswork for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco Crosswork server. After you add a security exception, the 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 4.4 and Applications Administrator Guide*.

Step 3 Log into the Cisco Crosswork as follows:

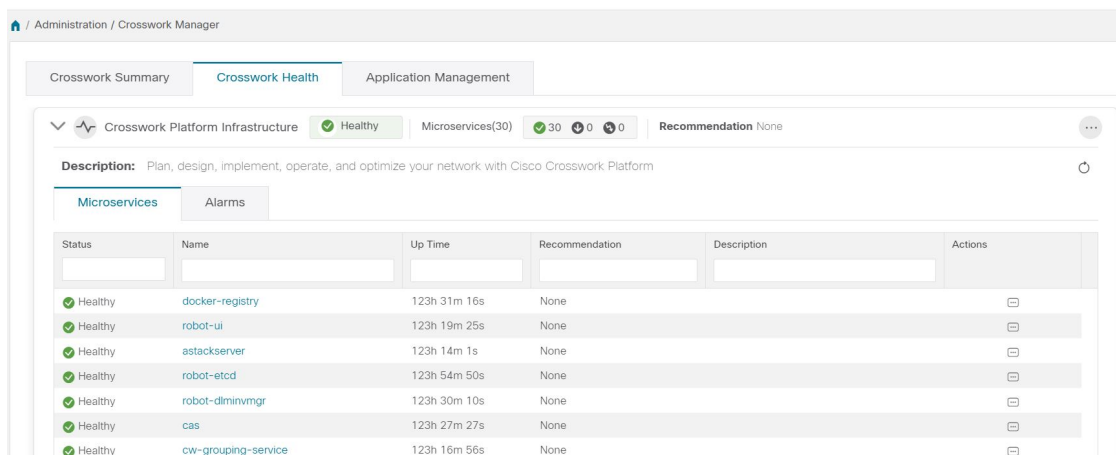
- Enter the Cisco Crosswork administrator username **admin** and the default password **admin**.
- Click **Log In**.
- When prompted to change the administrator's default password, enter the new password in the fields provided and then click **OK**.

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.



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.





CHAPTER 4

Install Cisco Crosswork Data Gateway

This chapter contains the following topics:

- [Cisco Crosswork Data Gateway Installation Workflow, on page 65](#)
- [Crosswork Data Gateway Post-installation Tasks, on page 91](#)
- [Log in and Log out of Crosswork Data Gateway VM, on page 93](#)
- [Cisco Crosswork Data Gateway Authentication and Enrollment, on page 94](#)
- [Troubleshoot Crosswork Data Gateway Installation and Enrollment, on page 95](#)

Cisco Crosswork Data Gateway Installation Workflow

Cisco Crosswork Data Gateway is installed as a VM called Base VM (containing only enough software to register itself with Cisco Crosswork). Use this procedure to install the first Cisco Crosswork Data Gateway VM or for adding additional Cisco Crosswork Data Gateway VMs.



Note If you are redeploying the same Cisco Crosswork Data Gateway with Cisco Crosswork, delete the previous Crosswork Data Gateway entry from the Virtual Machine table under Data Gateway Management. For information on how to delete a Crosswork Data Gateway VM, see [Delete Crosswork Data Gateway VM from Cisco Crosswork, on page 133](#).

To install Crosswork Data Gateway VM for use with Cisco Crosswork, follow these steps:

1. Choose the deployment profile for the Crosswork Data Gateway VM. See [Crosswork Data Gateway VM Requirements, on page 12](#).
2. Install Cisco Crosswork Data Gateway on your preferred platform:

Table 26: Crosswork Data Gateway installation options

VMware	Install Cisco Crosswork Data Gateway Using vCenter vSphere Client, on page 80
	Install Cisco Crosswork Data Gateway Via OVF Tool, on page 85
Amazon EC2	Install Crosswork Data Gateway on Amazon EC2, on page 86

3. Complete the post-installation tasks mentioned in the section [Crosswork Data Gateway Post-installation Tasks, on page 91](#)
4. Verify that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork. See [Cisco Crosswork Data Gateway Authentication and Enrollment, on page 94](#).

After verifying that the Crosswork Data Gateway VM has enrolled successfully with Cisco Crosswork, set up the Crosswork Data Gateway for collection by creating a Crosswork Data Gateway pool. See Section: *Create a Crosswork Data Gateway Pool in the Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide*.



Note If you plan to install multiple Cisco Crosswork Data Gateway VMs due to load or scale requirements or you wish to leverage Cisco Data Gateway High Availability, we recommend that you install all the Crosswork Data Gateway VMs first and then proceed with adding 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 4.4 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 4.4 and Applications Administration Guide*. In case of lost or forgotten passwords, destroy the current VM, you have to create a new VM, and reenroll 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 27: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Name	Parameter	Description	Additional Information
Host Information			

Name	Parameter	Description	Additional Information
Hostname*	Hostname	<p>Name of the Cisco Crosswork Data Gateway VM specified as a fully qualified domain name (FQDN).</p> <p>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.</p>	
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	<p>Parameter that conveys the type of controller application that CDG is deployed with. For an on-premise installation, choose either:</p> <ul style="list-style-type: none"> • onpremise-standard • onpremise-extended <p>The default value is onpremise-standard.</p>	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.	<p>You can choose to use either 1, 2, or 3 vNICs as per the following combinations:</p> <p>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.</p> <ul style="list-style-type: none"> • 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	<p>Choose how to validate interface addresses that fall in a usable RFC 8190 range. Options are <code>True</code>, <code>False</code>, or <code>Ask</code>, where the initial configuration scripts prompts for confirmation.</p> <p>The default value is <code>True</code> to automatically allow interface addresses in an RFC 8190 range.</p>	
Private Key URI	DGCertKey	<p>SCP URI to private key file for session key signing. You can retrieve this using SCP (<code>user@host:path/to/file</code>).</p>	<p>Cisco Crosswork uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation.</p>
Certificate File and Key Passphrase	DGCertChainPwd	<p>Passphrase of SCP user to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.</p>	<p>However, if you want to use third party or your own certificate files, then enter these parameters.</p> <p>Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (<code>user:host:/path/to/file</code>).</p> <p>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.</p>

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: <ul style="list-style-type: none"> • 20 GB for Standard. • 520 GB for Extended. 	
AwsIamRole	AwsIamRole	AWS IAM role name for EC2 installation.	A role created in Identity and Access Management (IAM) in the AWS environment with relevant permissions.
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			
<p>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: <i>Create a Crosswork Data Gateway Pool</i> in the <i>Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide</i>.</p>			
<p>Note</p> <ul style="list-style-type: none"> • 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. • Amazon EC2 mandates entering an IP address for the vNIC2 interface when Crosswork Data Gateway is deployed using 3 NICs. This is an AWS EC2 requirement and not imposed by Crosswork. 			
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.	<p>If you have selected Method as:</p> <ul style="list-style-type: none"> • 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 - <code>None</code> , <code>Static</code> , or <code>DHCP</code> . The default value is <code>None</code> .	<p>If you have selected Method as:</p> <ul style="list-style-type: none"> • 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 <code>VnicxIPv6Address</code> 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 <code>True</code> or <code>False</code> . Selecting <code>True</code> 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 <code>False</code> , <code>True</code> , or <code>Allow-Downgrade</code> . The default value is <code>False</code> . Select <code>True</code> to use DNS security extensions.	

Name	Parameter	Description	Additional Information
DNS over TLS*	DNSTLS	Options are <code>False</code> , <code>True</code> , and <code>Opportunistic</code> . The default value is <code>False</code> . Select <code>True</code> to use DNS over TLS.	
Multicast DNS*	mDNS	Options are <code>False</code> , <code>True</code> , and <code>Resolve</code> . Select <code>True</code> to use multicast DNS. The default value is <code>False</code> .	If you choose <code>Resolve</code> , only resolution support is enabled. Responding is disabled.
Link-Local Multicast Name Resolution*	LLMNR	Options are <code>False</code> , <code>True</code> , <code>Opportunistic</code> , or <code>Resolve</code> . The default value is <code>False</code> . Select <code>True</code> to use link-local multicast name resolution.	If you choose <code>Resolve</code> , 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 <code>pool.ntp.org</code> . 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 <code>True</code> to use NTPv4 authentication. The default value is <code>False</code> .	
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 <code>True</code> and <code>False</code> . Select <code>True</code> to send syslog messages to a remote host. The default value is <code>False</code> .	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: <ul style="list-style-type: none"> • 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]).	
Syslog Server Port	SyslogPort	Port number of the syslog server. The default port number is 514.	
Syslog Server Protocol	SyslogProtocol	Options are <code>UDP</code> or <code>TCP</code> to send the syslog. The default value is <code>UDP</code> .	
Use Syslog over TLS?	SyslogTLS	Select <code>True</code> to use TLS to encrypt syslog traffic. The default value is <code>False</code> .	
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 <code>True</code> and <code>False</code> . The default value is <code>False</code> . Select <code>True</code> 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	<p>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:</p> <p><code>cert/crosswork/management/peem/cert/certChain</code></p>	<p>Crosswork Data Gateway requires the Controller Signing Certificate File to enroll automatically with Cisco Crosswork.</p> <p>If you specify these parameters during the installation, the certificate file is imported once Crosswork Data Gateway boots up for the first time.</p> <p>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 98.</p>
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. Note This parameter applies to the Crosswork Data Gateway cloud deployment.	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. Note This parameter applies to the Crosswork Data Gateway cloud deployment.	
Authenticated Proxy Username	ProxyUsername	Username for authenticated proxy servers. Note This parameter applies to the Crosswork Data Gateway cloud deployment.	
Authenticated Proxy Passphrase	ProxyPassphrase		

Name	Parameter	Description	Additional Information
		Passphrase for authenticated proxy servers. Note This parameter applies to the Crosswork Data Gateway cloud deployment.	
HTTPS Proxy SSL/TLS Certificate File URI	ProxyCertChain	HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP. Note This parameter applies to the Crosswork Data Gateway cloud deployment.	
HTTPS Proxy SSL/TLS Certificate File Passphrase	ProxyCertChainPwd	Password of SCP user to retrieve proxy certificate chain. Note This parameter applies to the Crosswork Data Gateway cloud deployment.	



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 4.1 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 27: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 66](#) 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**.

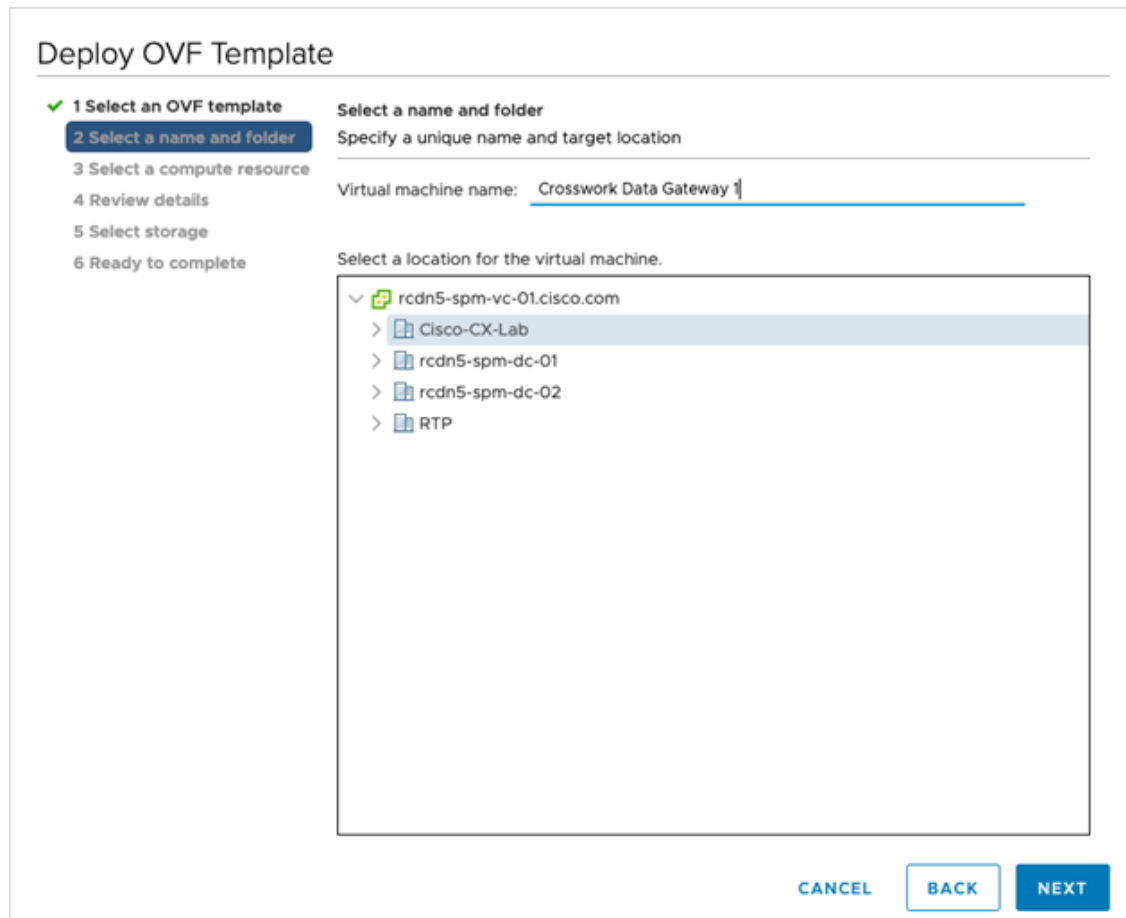
a) Click **Browse** to navigate to the location where you downloaded the OVA image file and select it.

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.



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** and **Crosswork On-Premise Extended**. See [Mandatory deployment type for Crosswork Data Gateway, on page 12](#) for more information.

Attention The **On-Premise Standard with Extra Resources** profile is available as a limited-availability feature and must not be used while deploying Crosswork Data Gateway. Please contact the Cisco Customer Experience team for assistance.

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

	Description
<input type="radio"/> Crosswork Cloud	
<input checked="" type="radio"/> Crosswork On-Premise Standard	12 CPU; 48GB RAM; 1-3 NICs; 60GB Disk
<input type="radio"/> Crosswork On-Premise Extended	
<input type="radio"/> Crosswork On-Premise Standard With Extra Resources	

4 Items

CANCEL BACK NEXT

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

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

CANCEL BACK NEXT

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 27: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios*, on page 66.

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

Allow Usable RFC 8190
 Address?

CANCEL BACK NEXT

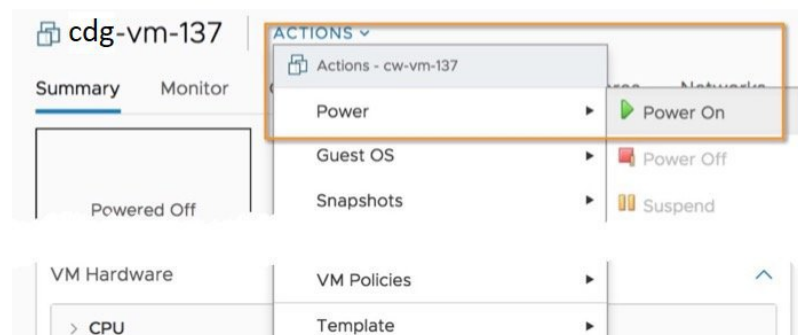
Step 12 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish** if you are ready to begin deployment.

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

- Open the vCenter vSphere client.
- 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 to the Table: [Table 27: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 66](#) for the list of installation parameters and their default values.



Note Ensure that you specify all the required mandatory and optional parameters with the desired values when you build the script. Parameters that are not included in the script will be considered with their default values for deployment.

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

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

VM_NAME='VM_NAME'
DM='thin'
DS='Datastore name'
Vcenter='Vcenter IP'
Host='Vcenter Host IP'
DC='DC Name'
CwIpv4Mgmt='CW IP'
ManagementIPv4Address='CDG IP'
ManagementIPv4Netmask='Netmask address'
ManagementIPv4Gateway='Management Gateway IP'
NorthDataIPv4Address='Northbound IP'
NorthDataIPv4Netmask='Netmask address'
NorthDataIPv4Gateway='Data Gateway IP'
DNSv4='DNS IP'
NTP='NTP FQDN'
Domain='Domain name'
CtrlerCertChainPwd='Controller Password'
DgAdminPwd='Admin user password'
DgOperPwd='Oper user password'
CdgDomain='CDG hostname'
MgmtNetwork='Standard Network'
SouthDataNetwork='Southbound port group name'
```

```

NorthDataNetwork='Northbound port group name'
DeploymentOption='Deployment Option'
VcenterUser='Vcenter username'
VcenterPwd='Vcenter password'
ImageFilePath='CDG Image Path'

ovftool --version
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv --overwrite --powerOffTarget
--powerOn --noSSLVerify --allowExtraConfig \
--ds=$DS \
--deploymentOption="{DeploymentOption}" \
--diskMode=$DM \
--name="{VM_NAME}" \
--prop:"ControllerIP=${CwIpv4Mgmt}" \
--prop:"ControllerPort=30607" \
--prop:"ControllerSignCertChain=cw-admin@${CwIpv4Mgmt}:/home/cw-admin/controller.pem" \
--prop:"ControllerCertChainPwd=${CtrlerCertChainPwd}" \
--prop:"Hostname=${CdgDomain}" \
--prop:"Description=CDG Base VM for Automation" \
--prop:"Vnic0IPv4Method=Static" \
--prop:"Vnic0IPv4Address=${ManagementIPv4Address}" \
--prop:"Vnic0IPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"Vnic0IPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"Vnic1IPv4Method=Static" \
--prop:"Vnic1IPv4Address=${NorthDataIPv4Address}" \
--prop:"Vnic1IPv4Netmask=${NorthDataIPv4Netmask}" \
--prop:"Vnic1IPv4Gateway=${NorthDataIPv4Gateway}" \
--prop:"dg-adminPassword=${DgAdminPwd}" \
--prop:"dg-operPassword=${DgOperPwd}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--net:"vNIC0=${MgmtNetwork}" \
--net:"vNIC1=${NorthDataNetwork}" \
--net:"vNIC2=${SouthDataNetwork}" \
$ImageFilePath \
vi://$VcenterUser:$VcenterPwd@$Vcenter/$DC/host/$Host

```

-
- Step 1** Open a command prompt.
 - Step 2** Navigate to the location where you installed the OVF Tool.
 - Step 3** Install the VM by executing the script that you created containing the command and arguments.

```
./<script_file>
```

For example,

```
root@cxcdgctrl:/opt# ./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 Crosswork Data Gateway on Amazon EC2

You can install the Crosswork Data Gateway on Amazon EC2 in one of the following ways:

- [Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template, on page 87.](#)
- [Install Crosswork Data Gateway on Amazon EC2 Manually , on page 88.](#)

Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template

Installing Crosswork Data Gateway on EC2 using CloudFormation (CF) templates involves creating a template (YAML formatted text file) which describes the VM resources and their properties. Whenever you create a stack, CloudFormation provisions the resources that are described in your template and installs the VMs.

A sample CF template is attached [Sample CloudFormation Template for installing Crosswork Data Gateway on EC2](#) for your reference.

Before you begin

- Ensure that you have met the requirements specified in the section [AWS EC2 Settings, on page 33.](#)
- All the Cisco Crosswork VMs have been installed.

-
- Step 1** Log in to AWS and search for the CloudFormation service. The CloudFormation dashboard opens.
- Step 2** Click **Stacks** from the side menu.
- All existing stacks in the environment are displayed here.
- Step 3** In **Step 1 - Specify template**, select the following settings:
- a) Under **Prepare template**, select **Template is ready**.
 - b) Under **Template source**, select **Upload a template file**.
 - c) Click **Choose file**, and select your CF template (.yaml file).
 - d) Click **Next**.
- Step 4** In **Step 2 - Specify stack details**, enter relevant values for the stack name and each parameter field, and click **Next**.
- Note** The parameter field names visible in this window are defined by the parameters in the CF template.
- Step 5** In **Step 3 - Configure stack options**, enter the relevant values for the settings based on your production preferences. Click **Next** to continue.
- Step 6** In **Step 4 - Review**, review the settings you have configured.
- Step 7** Select the acknowledgment checkbox, and click **Create stack** to start the VM installation.
-

Verify that the VMs were installed successfully

1. In the CloudFormation dashboard, click **Stacks** from the side menu to view the list of stacks.
2. Select the stack you installed. The stack details are displayed on the right. Click on each tab in this window to view details of the stack creation.

The status of the stack in the **Events** tab will be **CREATE_IN_PROGRESS**
3. After the stack has been created:
 - The status of the stack changes to **CREATE_COMPLETE** and the **Logical ID** displays the stack name.

- The **Resources** tab displays details of the all the resources that the CF template has created, including the physical IDs.
 - The **Output** tab has details of the VM's interface IP addresses.
4. Click the **Physical ID** of the VM instance in your stack.
Doing this will open the Instances window in the EC2 dashboard with details of the selected VM instance.
 5. Click **Connect** (top right corner).
 6. In the **Connect to instance** window that appears, click the **EC2 Serial Control** tab and click **Connect**.
 7. Click on the **EC2 serial console** tab. Click **Connect** to connect to the console of the VM.
 8. Log in to the VM as a `dg-admin` or `dg-oper` user using the password you configured.
The Interactive Console of the VM is displayed on successful login.

Install Crosswork Data Gateway on Amazon EC2 Manually

Follow these steps to install Crosswork Data Gateway on EC2.



Note

- The Launch Instance workflow offers a wide range of launch options that you can configure based on your requirements. The following procedure lists the mandatory settings that must be configured to install the Crosswork Data Gateway VM successfully.
- The steps in this procedure explain the installation of an Extended Crosswork Data Gateway VM with 3 interfaces.

Before you begin

Ensure that you have the following information ready before deploying the Crosswork Data Gateway VMs :

- Ensure that you have met the requirements specified in [AWS EC2 Settings, on page 33](#).
- All the Cisco Crosswork VMs have been installed.
- Decide the number of Crosswork Data Gateway VM instances to install.
- Have the Crosswork Data Gateway AMI image saved in a location accessible to your AWS.

Step 1 Prepare the user data for the Crosswork Data Gateway VMs.

- a) Prepare the user data for Crosswork Data Gateway VMs. See [Cisco Crosswork Data Gateway Parameters and Deployment Scenarios](#) for more information about the parameters. Sample user data for a VM is attached here for your reference. Important parameters have been highlighted.

```
AwsIamRole=changeme
ActiveVnics=3
AllowRFC8190=Yes
AuditdAddress=
AuditdPort=60
ControllerCertChainPwd=changeme
```

```

ControllerIP=
ControllerPort=30607
ControllerSignCertChain=cw-admin@<controller-IP>:/home/cw-admin/controller.pem
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=Extended
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 //IP address of management interface
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 //IP address of data interface
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 //leave unchanged to default value.
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 the user data for each Crosswork Data VM that you plan to install.

Step 2 Install the Crosswork Data Gateway VM.

- a) Log in to AWS and search for the EC2 service. The EC2 dashboard opens.
- b) Navigate to **Launch Instance** pane on the dashboard and click **Launch Instance** > **Launch Instance**.
- A **Launch an Instance** window appears.
- c) In the **Name and tags** section, enter the name of the Crosswork Data Gateway VM.
- d) In the **Application and OS Images (Amazon Machine Image)** section, click **My AMIs** > **Owned by me** and select the Crosswork Data Gateway AMI image in the **Amazon Machine Image (AMI)** field.
- e) In the **Instance type** section, select the following instance types (both production and lab environment) based on the profile of the Crosswork Data VM you are deploying.

- **m5.4xlarge** - for a Standard VM.
- **m5.8xlarge** - for an Extended VM.

- f) In the **Key pair (login)** section, select a **Key pair name** from the drop-down list.

Note Cisco Crosswork does not support key-based authentication. This is an AWS requirement and will not be used by Cisco Crosswork.

- g) In the **Network Settings** section, click **Edit**.

1. Enter values in the following fields:

- **VPC** - Select the appropriate VPC for your environment.
- **Subnet** - Select the subnet that you wish to assign to the management interface.
- **Auto-assign public IP** - Select **Disabled**.
- **Firewall (security groups)** - Specify a security group for the VM. You can create a security group or use an existing security group that you have already created.

After you have entered the details above, under **Advanced network configuration**, a **Network Interface1** is automatically created.

2. Update the **Description**, **Primary IP** (vNIC0 IP address from the user data), **Subnet**, **Security groups**.
3. Click **Add network interface** and add details for a second interface (corresponds to vNIC1) and a third interface (vNIC2) of the VM.

Important Please note that the user data for the VM does not have an IP address for vNIC2 as this is assigned during pool creation. It is an AWS requirement to assign an IP address each time a network interface is created. You can either enter an IP address in the **Primary IP** field (static IP) of the third interface or leave it blank (AWS assigns an IP automatically).

- h) In the **Configure Storage** section, click **Advanced** and click **Add new volume** to add an additional partition for your VM. Update the following fields for the newly created volume.
- **Device name** - /device/sdb
 - **Size (GiB)** - 20 GB (Standard CDG) or 520 GB (Extended CDG)
 - **Volume type** - We recommend using gp2 or gp3.
- i) In the **Advanced Settings** section, update the following fields.
- **IAM instance profile** - Select the AWS IAM role that you had specified in the user data or create a new role.
 - **Metadata accessible** - Enabled.
 - **Metadata version** - V1 and V2 (token optional)
 - **Metadata response hop limit** - 2
 - **User data** - Copy the user data that you had prepared in Step 1 and paste it within the window here. If you are providing the parameters in a base64 encoded format, select the check box.
- Note** Ensure that there are no leading white spaces when you paste the user data otherwise the deployment will fail.

Step 3 Click **Launch Instance**. AWS EC2 initiates the installation of the VM.

Step 4 Repeat steps 2 to 4 to install the remaining VMs.

Verify that the VMs were installed successfully

1. In the EC2 dashboard, click **Instances** from the menu on the left to view the VMs that were deployed. You can search for the VMs using the name, attributes or tags.
Wait for about 20 minutes for the VMs to be deployed.
2. After the VMs are launched successfully, they have the **Instance State** as **Running**.
3. To verify that the VMs were installed successfully, select a VM and click **Connect** (top right corner).
4. In the **Connect to instance** window that appears, click the **EC2 Serial Control** tab and click **Connect**.
5. Log in to the VM as a `dg-admin` or `dg-oper` user using the password you configured in the user data. The Interactive Console of the VM is displayed on successful login.

Crosswork Data Gateway Post-installation Tasks

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

- [Configure Timezone of the Crosswork Data Gateway VM, on page 92](#)
- [Log Out of Crosswork Data Gateway VM, on page 94](#)

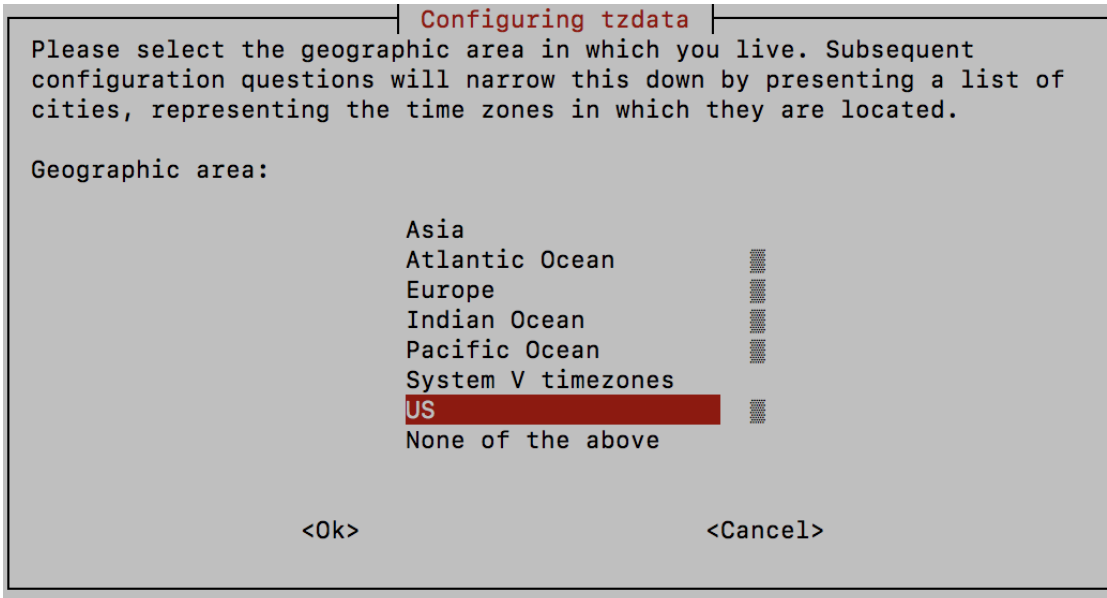
Configure Timezone of the Crosswork Data Gateway VM

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.

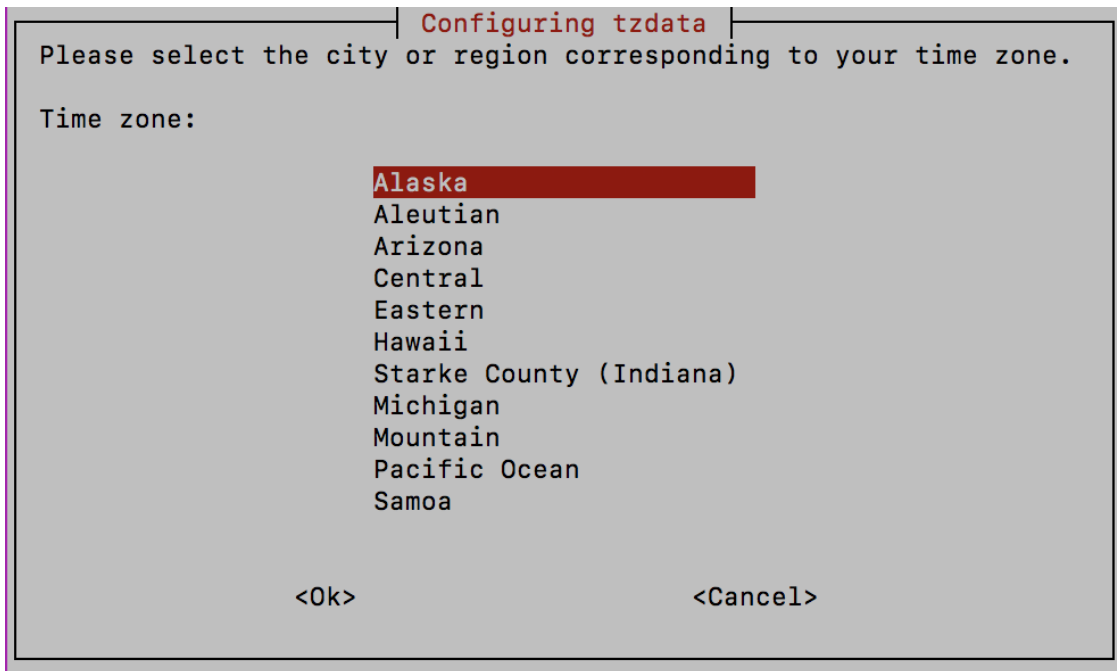
Step 1 In Crosswork Data Gateway VM interactive menu, select **Change Current System Settings**.

Step 2 Select **9 Timezone**.

Step 3 Select the geographic area in which you live.



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



- 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 93](#)
- [Access Crosswork Data Gateway Through vCenter, on page 94](#)

To log out of the Crosswork Data Gateway VM, see [Log Out of Crosswork Data Gateway VM, on page 94](#).

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 administrator 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**.

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 62](#).
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.

For information about the different operational states of the VMs, see Section: *Overview of Cisco Crosswork Data Gateway* in the *Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide*.

Operational State	Admin State	Virtual Machine Name	IP4 Mgmt. IP Address	IP6 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 be 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 > 2 Run show-tech**) and check for the reason in `controller-gateway` logs. For more information on how to collect show-tech logs, see [Collect show-tech logs from the Interactive Console](#). If there are session establishment or certificate related issues, ensure that the `controller.pem` certificate is uploaded using the Interactive Console.

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 28: Troubleshooting the Installation/Enrollment

Issue	Action
1. Cannot enroll Crosswork Data Gateway with Cisco Crosswork	
<p>Crosswork Data Gateway cannot be enrolled with Cisco Crosswork due to an NTP issue, i.e., there is a clock-drift between the two.</p> <p>The clock-drift might be with either Crosswork Data Gateway or Cisco Crosswork.</p> <p>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.</p> <p>Sync the clock time on the host and retry.</p>	<ol style="list-style-type: none"> 1. Log into the Crosswork Data Gateway VM. 2. From the main menu, select 5 Troubleshooting > 2 Run show-tech. <p>Enter the destination to save the tarball containing logs and vitals and click OK.</p> <p>The show-tech is now encrypted with a file extension ending with .tar.xz.</p> <ol style="list-style-type: none"> 3. Run the following command to decrypt the show-tech file. <pre>openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string></pre> <p>In the show-tech logs (in file <code>session.log</code> at location <code>/opt/dg/log/controller-gateway/session.log</code>), if you see the error <code>UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid</code>, then there is a clock-drift between Crosswork Data Gateway and Cisco Crosswork.</p> <ol style="list-style-type: none"> 3. From the main menu, go to 3 Change Current System Settings > 1 Configure NTP. <p>Configure NTP to sync with the clock time on the Cisco Crosswork server and try re-enrolling Crosswork Data Gateway.</p>
2. Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals"	

Issue	Action
<p>Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals" due to certificate errors.</p>	<ol style="list-style-type: none"> 1. Log into the Crosswork Data Gateway VM. 2. From the main menu, select 5 Troubleshooting > 2 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. <pre>openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted filename> -pass pass:<encrypt string></pre> <p>In the show-tech logs (in file <code>gateway.log</code> at location <code>/opt/dg/log/controller-gateway/gateway.log</code>), if you see certificate errors, then re-upload the Controller Signing Certificate, as explained in the steps below:</p> <ol style="list-style-type: none"> 1. From the main menu, select 3 Change Current System Settings > 7 Import Certificate. 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.
<p>3. Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "gRPC connection cannot be established"</p>	
<p>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.</p>	<ol style="list-style-type: none"> 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: <ol style="list-style-type: none"> a. From the main menu, select 5 Troubleshooting and click OK. b. From the Troubleshooting menu, select 4 Reboot VM and click OK. c. Once the reboot is complete, check if the Crosswork Data Gateway's operational status is Up.
<p>Crosswork Data Gateway goes into Error state</p>	<p>Check the vNIC values in the OVF template in case of vCenter.</p>

Issue	Action
Crosswork Data Gateway enrollment with 1 NIC Cisco Crosswork fails	<p>Check the vNIC values in the OVF template in case of vCenter. If ActiveVnics property is missing for 1 NIC and 2 NIC, Crosswork Data Gateway tries to deploy 3 NICs by default.</p> <p>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.</p>
Crosswork Data Gateway deploys Standard profile instead of Extended profile	<p>Check the <code>Deployment</code> parameter in the OVF template in case of vCenter. If <code>Deployment</code> parameter mismatches or does not exist for an Extended profile, then Crosswork Data Gateway deploys the Standard profile by default.</p>

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 or reinstalled 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. See [View the Controller Signing Certificate File, on page 99](#).

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.

View the Controller Signing Certificate File



CHAPTER 5

Install Crosswork Applications

This chapter contains the following topics:

- [Install Crosswork Applications, on page 101](#)

Install Crosswork Applications

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

Every crosswork application is bundled in a particular format unique to Crosswork known as CAPP (Crosswork APPLICATION). The application CAPP files (*.tar.gz) are downloaded from [cisco.com](https://www.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 bundled as **Essentials** and **Advantage** packages in [cisco.com](https://www.cisco.com).

Table 29: Crosswork Network Controller Packaging

Package	Contents
Crosswork Network Controller Essentials	Crosswork Optimization Engine Crosswork Active Topology
Crosswork Network Controller Advantage	Crosswork Optimization Engine Crosswork Active Topology Crosswork Service Health Crosswork Health Insights 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 [Integration Requirements for other Cisco Products, on page 20](#).



Important If you intend to use the Crosswork Network Controller solution (Essential or Advantage), install Crosswork Cluster and Crosswork Data Gateway, and then install the Crosswork applications in the following sequence:

1. Crosswork Optimization Engine
2. Crosswork Active Topology
3. Crosswork Service Health (only available in Advantage bundle)
4. Cisco Element Management System (EMS) Services (only available in Advantage bundle)

Crosswork Change Automation, Crosswork Health Insights, and Crosswork Zero Touch Provisioning can be installed independently in any order and do not require any other application to be installed prior.

Step 1 Download and validate the CAPP files:

- a) Navigate to [cisco.com](https://www.cisco.com) and download the application CAPP files that you require and the relevant signature file to a directory in your machine. For the purpose of these instructions, we will use the file names "**cw-na-cncadvantage-4.1.0-374-release-221027.tar.gz**" and "**cnc-4.1.0-capp-signatures.tar.gz**" respectively.
- b) Decompress the signature file

```
tar -xvf <signature file>
```

Example:

```
[test@cw-build sample]% tar -xvf cnc-4.1.0-capp-signatures.tar.gz
x README
x CW-CCO_RELEASE.cer
x cisco_x509_verify_release.py3
x cisco_x509_verify_release.py
x cw-na-ztp-4.1.0-229-release-221025.tar.gz.signature
x cw-na-common-ems-services-4.1.0-127-release-221025.tar.gz.signature
x cw-na-cat-4.1.0-225-release-221024.tar.gz.signature
x cw-na-aa-4.1.0-262-release-221026.tar.gz.signature
x cw-na-cncadvantage-4.1.0-374-release-221027.tar.gz.signature
x cw-na-cncessential-4.1.0-401-release-221026.tar.gz.signature
```

- c) Use python script to validate the signature of each file you plan to use.

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
```

Example:

```
[test@cw-build sample]% python cisco_x509_verify_release.py3 -s
cw-na-cncadvantage-4.1.0-374-release-221027.tar.gz.signature -i
cw-na-cncadvantage-4.1.0-374-release-221027.tar.gz -e CW-CCO_RELEASE.cer
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/innespace.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-4.1.0-374-release-221027.tar.gz using
CW-CCO_RELEASE.cer
```

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

- d) 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 downloaded file with the value you copied in the clip board.

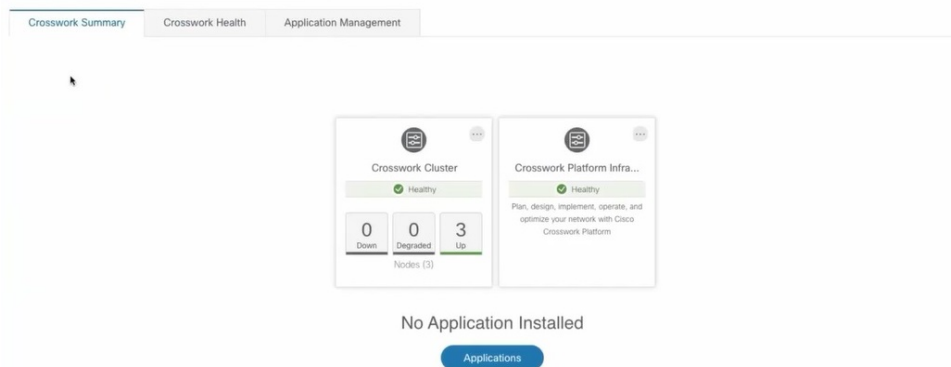
For example, on a MAC you can use the **md5** command to calculate the MD5 sum on a file:

```
md5 <.tar.gz>
```

Verify that the result value matches with the posted value on [cisco.com](https://www.cisco.com).

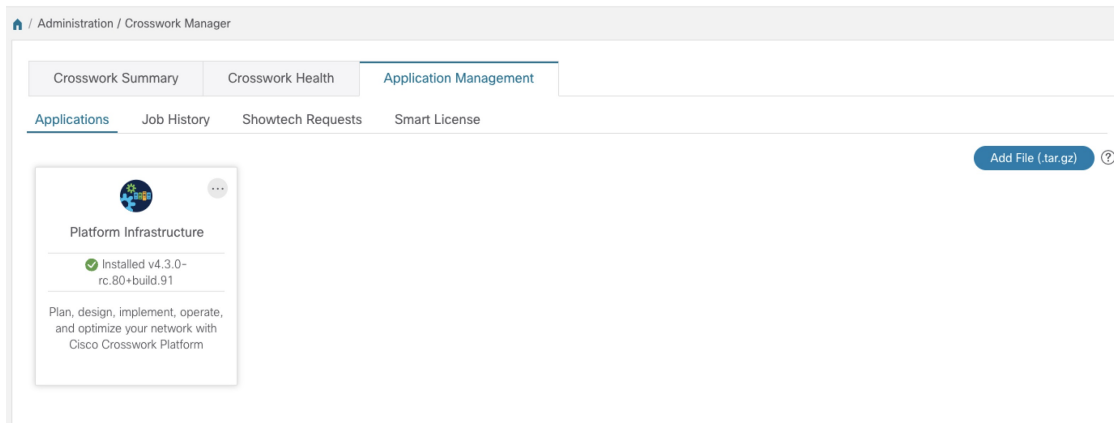
Step 2 Add the downloaded CAPP file to Crosswork:

- 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.



You can click on the tiles to get more information.

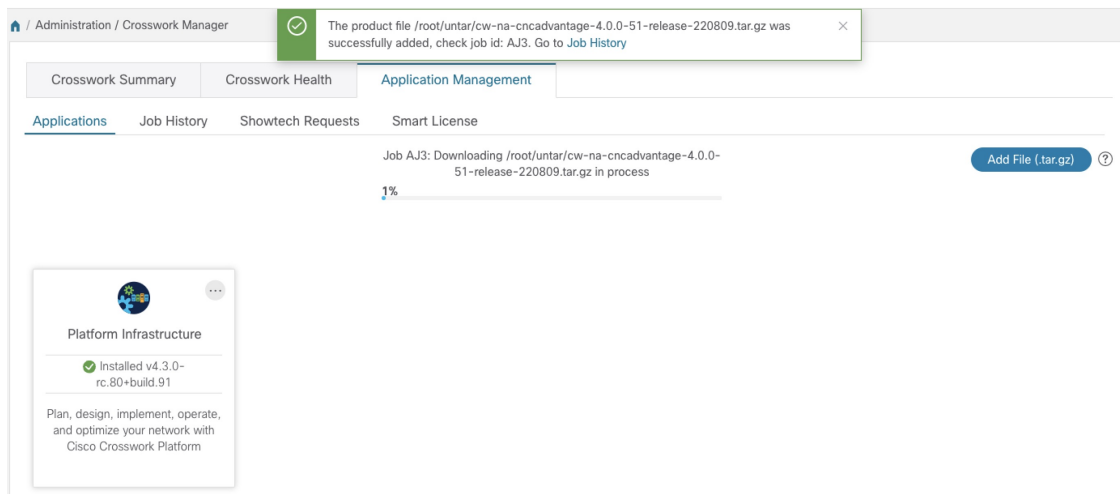
- b) To install an application or application bundle, click on **Applications** button. Alternately, click on the **Application Management** tab.



- 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**.

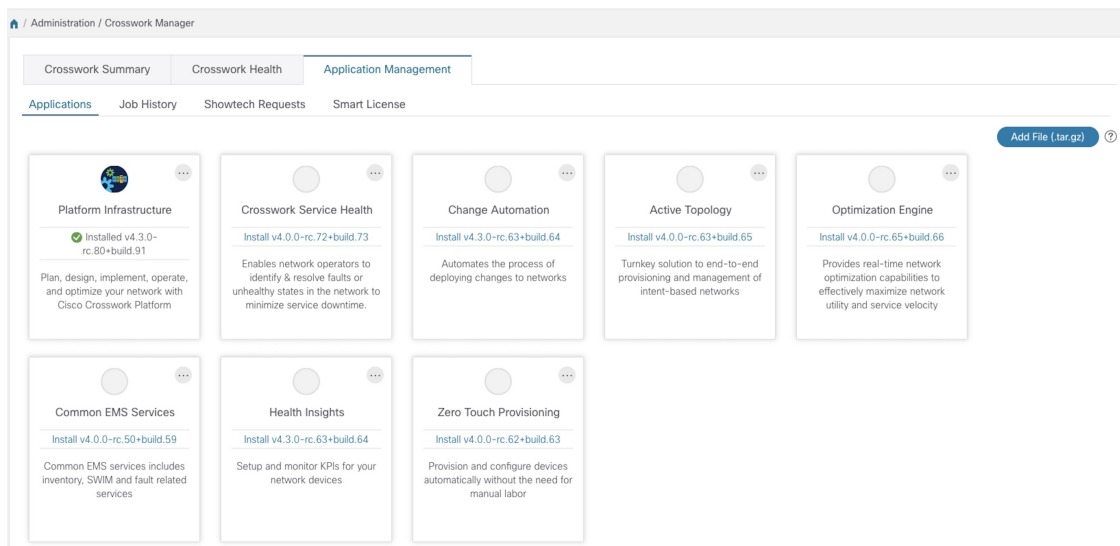
The dialog box is titled 'Add File (.tar.gz) via Secure Copy' and has a close button (X) in the top right corner. It contains several input fields: 'Server Path/Location' with a placeholder 'Network/server_name/directory/file name', 'Host Name/IP Address', 'Port' with the value '22', 'Username', and 'Password' with a toggle icon. There is a checkbox labeled 'Automatically clean all repository files before adding new one'. At the bottom right, there are two buttons: 'Add' and 'Cancel'.

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




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.



Step 3 Install the Application CAPP file:

- 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, on page 107](#)
- [Upgrade Requirements, on page 108](#)
- [Upgrade Using Same Hardware, on page 109](#)
- [Upgrade Using Parallel Hardware, on page 120](#)
- [Update a Crosswork Application \(standalone activity\) , on page 128](#)

Cisco Crosswork Upgrade Workflow

This section provides the high-level workflow for upgrading Cisco Crosswork to the latest version. This includes upgrading Cisco Crosswork cluster, Cisco Crosswork Data Gateway and Crosswork Applications within a single maintenance window.

You can upgrade Cisco Crosswork in the following methods:

1. [Upgrade Using Same Hardware, on page 109](#)
2. [Upgrade Using Parallel Hardware, on page 120](#)

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 an earlier version has the following limitations:

- License tags are not auto-registered as part of the upgrade operation. You must register them manually after the upgrade.
- 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 earlier version of Cisco Crosswork are not migrated, and need to be updated manually on the new version post migration.
- Any user roles with administrative privileges in the earlier version of Cisco Crosswork must be assigned new permissions after the upgrade to continue being administrative users.
- 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 discrepancy.

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 128.

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 an earlier version of Crosswork Optimization Engine and want to upgrade to Crosswork Optimization Engine 4.1, 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 4.1 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 4.4 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 VMs, on page 110](#)
2. [Create Backup and Shut Down Cisco Crosswork, on page 111](#)

3. [Install the Cisco Crosswork 4.4 Cluster, on page 113](#)



Note While the cluster installation is in progress, you must upgrade NSO to version 5.7.6. 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 version 7.7.1.

4. [Install Cisco Crosswork 4.4 Applications, on page 114](#)



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 Previous Cisco Crosswork backup to Cisco Crosswork 4.4, on page 114](#)

6. [Upgrade to Crosswork Data Gateway 4.1, on page 115](#)

7. [Post-upgrade Checklist, on page 119](#)

Shut Down Cisco Crosswork Data Gateway 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 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 4.1, on page 115](#).

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

Step 2 Shut down the Crosswork Data Gateway VMs.

- a) Log in to the Crosswork Data Gateway VM. See [Access Crosswork Data Gateway VM from SSH, on page 93](#).

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

This is the second stage of the upgrade workflow. Creating a backup is a prerequisite when upgrading your current version of Cisco Crosswork to a new 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 the current version of Cisco Crosswork, download a copy of the package to your system. You will need to upload the package after you complete migrating to Cisco Crosswork 4.4. See [Post-upgrade Checklist, on page 119](#) for more information.
- If you have modified the current version of Cisco Crosswork to include third-party device types, you must download the third-party device configuration file, and re-apply it to Cisco Crosswork 4.4. 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 108.

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 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 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 4.4 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 5.7.6](#).

Install the Cisco Crosswork 4.4 Cluster

This is the third stage of the upgrade workflow. After the successful backup of the old version of Cisco Crosswork, proceed to install Cisco Crosswork 4.4 cluster.



Note The number of VM nodes installed in Cisco Crosswork 4.4 must be equal or more than the number of VM nodes in the old version of Cisco Crosswork.



Note While the cluster installation is in progress, you must upgrade NSO to version 5.7.6. 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 version 7.7.1 (see *Crosswork Network Controller 4.1 Release Notes* for details).

Before you begin

- Make sure that your environment meets all the requirements specified under [Cisco Crosswork Installation Requirements, on page 9](#).

Step 1 Install Cisco Crosswork 4.4 cluster using any of the installation methods described in [Install the Crosswork Cluster, on page 35](#).

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.
- From the Cisco Crosswork main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
 - 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 4.4 Applications

This is the fourth stage of the upgrade workflow. After the successful installation of Cisco Crosswork 4.4 cluster, proceed to install Cisco Crosswork 4.4 applications.



Note You can only install 4.4 versions of the Cisco Crosswork applications that were backed up during [Create Backup and Shut Down Cisco Crosswork](#), on page 111.

- Step 1** Install Cisco Crosswork 4.4 applications using the steps described in [Install Crosswork Applications](#), on page 101.
- Step 2** After the applications are successfully installed, check the health of the Cisco Crosswork 4.4 cluster.
- From the Cisco Crosswork main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
 - Click **Crosswork Cluster** tile to view the health details of the cluster.

Migrate the Previous Cisco Crosswork backup to Cisco Crosswork 4.4

This is the fifth stage of the upgrade workflow. After the successfully installing Cisco Crosswork 4.4 applications, proceed to migrate the backup of earlier version of Cisco Crosswork on Cisco Crosswork 4.4 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](#), on page 111.
- The name and path of the backup file created in [Create Backup and Shut Down Cisco Crosswork](#), on page 111.
- 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, on page 111](#).

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

Step 3 **Migrate the previous Cisco Crosswork backup on the Cisco Crosswork 4.4 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, on page 111](#)) 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 4.4 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 4.1

This is the final stage of the upgrade workflow. Ensure that the migration is complete and Cisco Crosswork 4.4 UI is available before you proceed with installing Crosswork Data Gateway (CDG) 4.1.



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 the old Crosswork Data Gateway VMs with Crosswork Data Gateway 4.1 VMs in the network.



Important Step 8 in this procedure requires you log out of Cisco Crosswork 4.4 and log in again after verifying the deployment and enrollment of the 4.1 CDG VMs with Cisco Crosswork 4.4. 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 4.4 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 4.1 VMs with the same number and the same information (management interface importantly) as the old Crosswork Data Gateway VMs. Follow the steps in the [Cisco Crosswork Data Gateway Installation Workflow, on page 65](#).
- 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 4.1 VMs are enrolled with Cisco Crosswork 4.4 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 the previous version of Cisco Crosswork, 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 the previous version of Cisco Crosswork.

Note You can also verify the pool details by clicking on the pool name.

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

Step 7

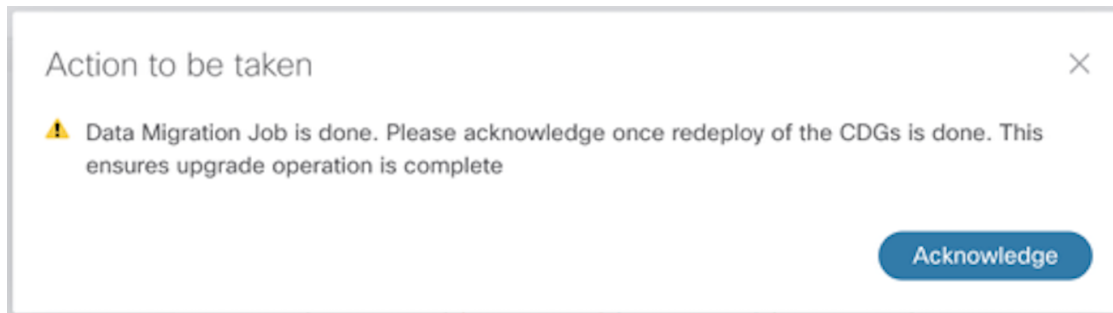
Verify that devices are attached to the Crosswork Data Gateways 4.1 in the Cisco Crosswork 4.4 UI.

- Navigate to the **Administration > Data Gateway Management** page.
- Check the **Attached Device Count** of the Crosswork Data Gateway.

Step 8

Log out of Cisco Crosswork 4.4 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.



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 4.1 VMs are enrolled with Cisco Crosswork 4.4.
- 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	<ol style="list-style-type: none"> 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 .	<ol style="list-style-type: none"> 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 4.4. 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.	<ol style="list-style-type: none"> 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 4.4 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 discrepancy.
- Navigate to **Administration > Collection Jobs** in Cisco Crosswork 4.4 UI and delete the duplicate system jobs.

Status	App ID	Context ID	Action
Successful	cw.dminvmgr0	dim/cli-collector/group/reachability/subscription	⊙
Successful	cw.dminvmgr	dim/cli-collector/group/reachability/subscription	⊙
Degraded	cw.dminvmgr	dim/snmp-collector/group/subscription	⊙
Degraded	cw.dminvmgr	dim/cli-collector/group/te-tunnel-id/subscription	⊙
Degraded	cw.dminvmgr0	dim/cli-collector/group/te-tunnel-id/subscription	⊙
Degraded	cw.dminvmgr0	dim/snmp-collector/group/subscription	⊙
Degraded	cw.dminvmgr0	dim/cli-collector/group/showclock/subscription	⊙
Deleting	cw.dminvmgr	dim/cli-collector/group/showclock/subscription	⊙

- Verify that the collection jobs are running on the Crosswork Data Gateway 4.1 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 4.4.
- (Optional) Based on your network requirements, download the relevant map files from cisco.com and re-upload them to Cisco Crosswork 4.4.
- (Optional) If any NSO device onboarding policy was set in the previous version of Cisco Crosswork, you must update the policy with new Network Element Drivers (NED) on the NSO.
- (Optional) Re-apply any third-party device configurations (used in the previous version of Cisco Crosswork) to Cisco Crosswork 4.4.
- 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 108](#).

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 4.4 using new hardware. This method relies on installing the Cisco Crosswork 4.4 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 4.4 Cluster, on page 120](#)



Note While the cluster installation is in progress, you must upgrade NSO to version 5.7.6. 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 version 7.7.1 (see the *Crosswork Network Controller 4.1 Release Notes* for details).

2. [Backup Cisco Crosswork Cluster, on page 121](#)
3. [Update DNS Server and Run Migration , on page 123](#)
4. [Add Crosswork Data Gateway 4.1 to Cisco Crosswork 4.4, on page 124](#)
5. [Shut Down the Previous Cisco Crosswork Cluster, on page 127](#)

Deploy a new Cisco Crosswork 4.4 Cluster

Install Cisco Crosswork 4.4 cluster and applications on a new set of VMs in parallel.



Note Cisco Crosswork 4.4 must be installed with the same FQDN and same number of nodes as in the old version of Cisco Crosswork.

Before you begin

- Make sure that your environment meets all the requirements specified under [Cisco Crosswork Installation Requirements, on page 9](#).

-
- Step 1** Install Cisco Crosswork 4.4 cluster using any of the installation methods described in [Install the Crosswork Cluster, on page 35](#).
- 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.
- From the Cisco Crosswork main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
 - 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 the old version of Cisco Crosswork. For more information, see [Install Crosswork Applications, on page 101](#).
- Step 5** After the applications are successfully installed, check the health of the Cisco Crosswork 4.4 cluster.
-

Backup Cisco Crosswork 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 the previous version of Cisco Crosswork, download a copy of the package to your system. You will need to upload the package after you complete migrating to Cisco Crosswork 4.4. See [Post-upgrade Checklist, on page 119](#) for more information.

- If you have modified the previous version of Cisco Crosswork to include third-party device types, you must download the third-party device configuration file, and re-apply it to Cisco Crosswork 4.4. 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 108.



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:**

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

Step 4 **Create a backup:**

- From the Cisco Crosswork main menu, choose **Administration > Backup and Restore**.
- Click **Actions > Backup** to display the **Backup** dialog box with the destination server details prefilled.
- Provide a relevant name for the backup in the **Job Name** field.
- 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.

- 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 4.4 and Applications Administration Guide](#) instead of the instructions here.

- 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.

- (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 the previous version of Cisco Crosswork cluster to the <new_VIP> of Cisco Crosswork 4.4 cluster.

Step 2 Navigate to the UI of the Cisco Crosswork 4.4 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 Cluster, on page 121](#).

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

Step 4 **Migrate the old Cisco Crosswork backup on the Cisco Crosswork 4.4 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 Cluster, on page 121](#)) 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 4.4 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 discrepancy.

Add Crosswork Data Gateway 4.1 to Cisco Crosswork 4.4

Ensure that the migration is complete and Cisco Crosswork 4.4 UI is available before you proceed with installing Crosswork Data Gateway (CDG) 4.1.



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 4.1 VMs in the network.



Important Step 6 in this procedure requires you log out of Cisco Crosswork 4.4 and log in again after verifying the deployment and enrollment of the 4.1 CDG VMs with Cisco Crosswork 4.4. 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 4.4 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 4.1 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 [Cisco Crosswork Data Gateway Installation Workflow, on page 65](#).
- 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 4.1 VMs are enrolled with Cisco Crosswork 4.4 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.

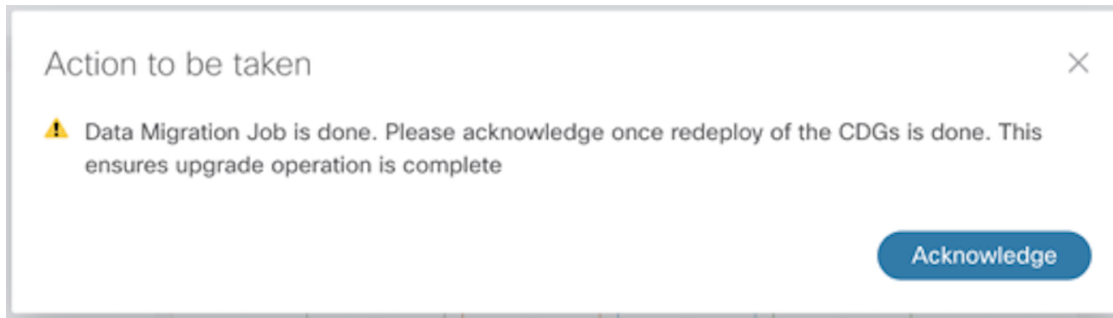
For example, the Crosswork Data Gateway pool in the following image contains two VMs, where the active VM is 172.23.247.78

Step 7 Verify that devices are attached to the Crosswork Data Gateways 4.1 in the Cisco Crosswork 4.4 UI.

- Navigate to the **Administration > Data Gateway Management** page.
- Check the **Attached Device Count** of the Crosswork Data Gateway.

Step 8 Log out of Cisco Crosswork 4.4 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 .



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 4.1 VMs are enrolled with Cisco Crosswork 4.4.
- 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 the Previous Cisco Crosswork Cluster

Before you begin

Gather the following information before shutting down the previous version of Cisco Crosswork:

- 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):

- Log into the VMware vSphere Web Client.
- In the **Navigator** pane, right-click the VM that you want to shut down.
- Choose **Power > Power Off**.
- Wait for the VM status to change to **Off**.
- Wait for 30 seconds and repeat steps 1a to 1d for each of the remaining VMs.

Step 2 Shut down the Crosswork Data Gateway VMs.

- Log in to the previous version of Crosswork Data Gateway VM. See [Access Crosswork Data Gateway VM from SSH, on page 93](#).

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 5.7.6](#).

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-4.0.3-3-release-220614.tar.gz
```

```
ff47a72ed7dc4fc4be388db3a43fa13f
```

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

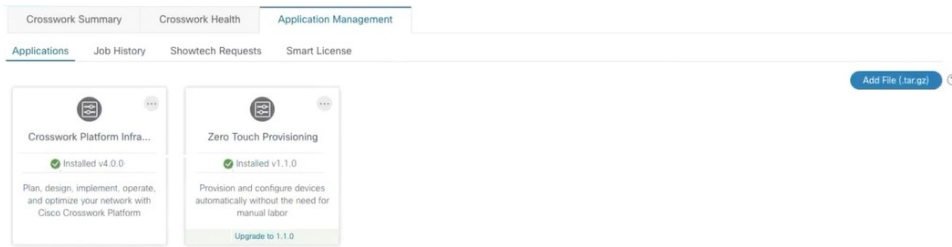
Step 2 Click on **Administration > Crosswork Manager**, and select the **Application Management** tab.

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.

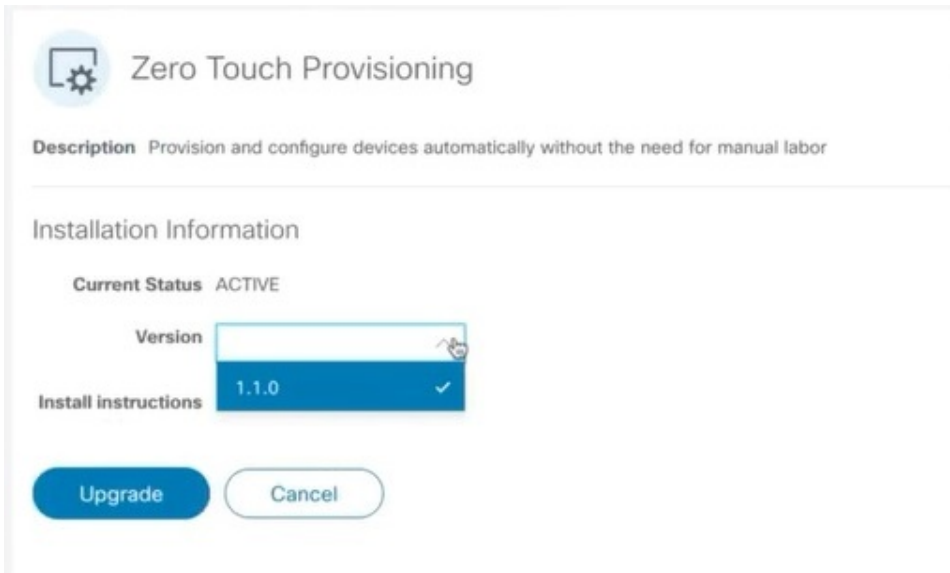


The upgrade progress is displayed on the application tile.

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**.



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, on page 131](#)
- [Uninstall Crosswork Data Gateway, on page 132](#)
- [Uninstall Crosswork Applications, on page 133](#)

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 131](#)
- [Delete the VM using the vSphere UI, on page 132](#)

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 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>
```

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.

Add `-o` option to remove the Cisco Crosswork image template from the data center.

For example:

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

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

Step 6 (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. For more information, see *Delete Cisco Crosswork Data Gateway VM from Cisco Crosswork* in [Cisco Crosswork Infrastructure 4.4 and Applications Administration Guide](#).
 - Delete the Crosswork Data Gateway VM from Cisco Crosswork as described in this chapter.

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.

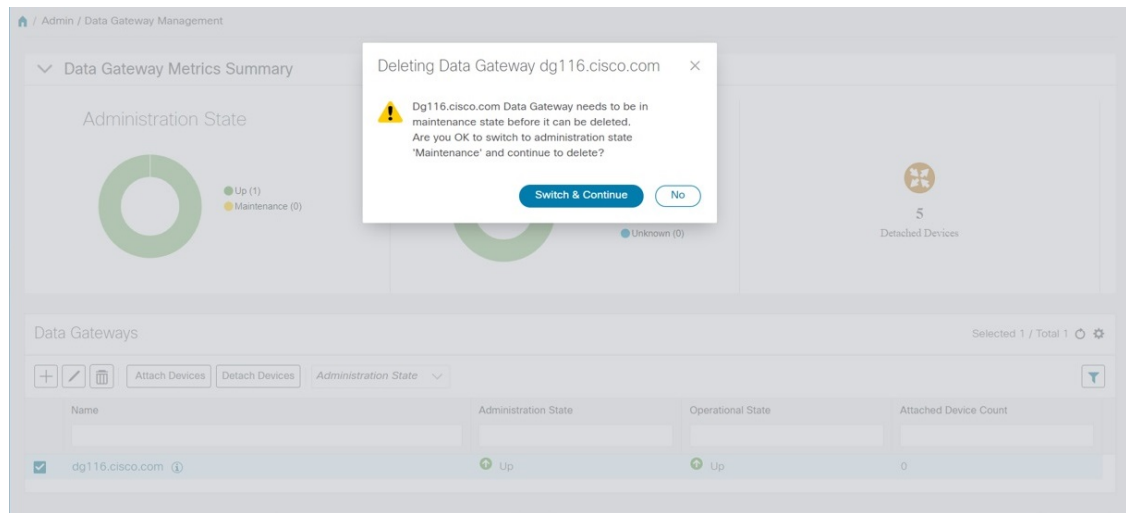
- [Delete Crosswork Data Gateway VM from Cisco Crosswork, on page 133](#)

Delete Crosswork Data Gateway VM from Cisco Crosswork

Before you begin

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

- Step 1** Log into Cisco Crosswork UI.
- Step 2** From the navigation panel, select **Administration > Data Gateway Management**.
Click on the **Virtual Machines** tab.
- Step 3** In the **Virtual Machines** list, find the Crosswork Data Gateway VM you want to delete and click  under **Actions** column.
Click **Delete**.
- Step 4** If the Crosswork Data Gateway VM is not in maintenance state, Cisco Crosswork prompts you to switch it to maintenance state. Click **Switch to maintenance & continue**.



The Crosswork Data Gateway VM is deleted.

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.



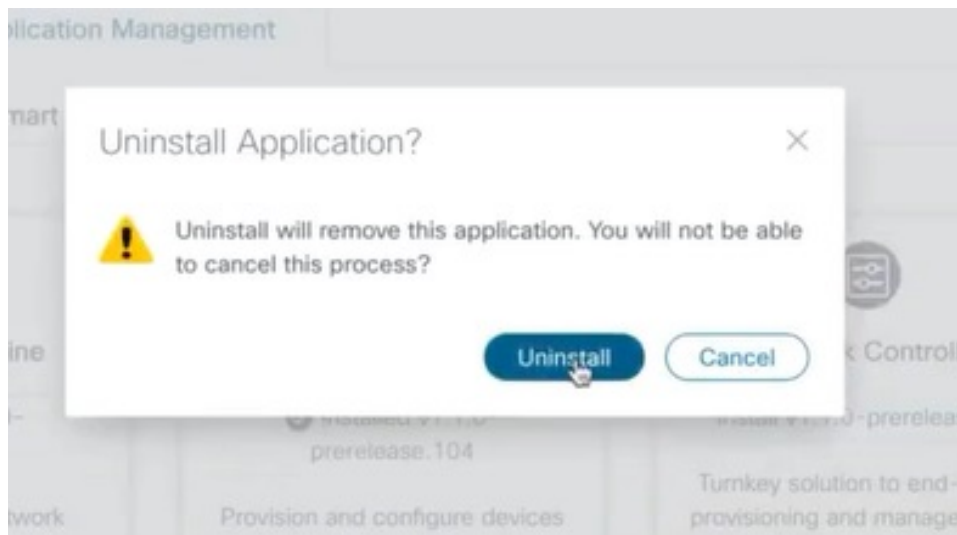
Attention Crosswork Active Topology (if installed) must be uninstalled before you can uninstall Crosswork Optimization Engine.

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.

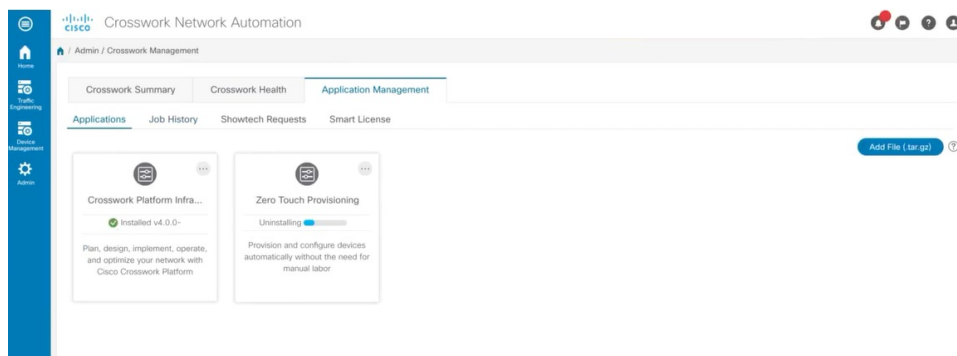
Step 2 Click  on the application tile that you want to uninstall, and select the **Uninstall** option from the drop down list.

A pop-up is displayed to confirm the action.



Step 3 Click **Uninstall** to confirm.

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



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

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



APPENDIX **A**

Sample deployment templates

This appendix contains the following topics:



Note The templates in this appendix are samples for your reference and do not contain real values.

- [Sample manifest template for VMware vCenter, on page 135](#)
- [Set seed node explicitly, on page 137](#)
- [Sample CloudFormation template for installing Crosswork Cluster VMs on AWS EC2, on page 137](#)
- [Sample CloudFormation Template for installing Crosswork Data Gateway on EC2, on page 152](#)

Sample manifest template for VMware vCenter

The following example deploys a Crosswork cluster containing 3 Hybrid nodes and 2 worker nodes.



Note In case you are using resource pools, please note that individual ESXi host targeting 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  
*****  
  
ClusterIPStack = "IPv4"  
ManagementVIP = "172.25.87.94"  
ManagementIPNetmask = "255.255.255.192"  
ManagementIPGateway = "172.25.87.65"  
DataVIP = "192.168.123.94"  
DataIPNetmask = "255.255.255.0"  
DataIPGateway = "0.0.0.0"  
DNS = "171.70.168.183"  
DomainName = "cisco.com"  
CWPassword = "****"  
VMSize = "Large"  
NTP = "ntp.cisco.com"  
CloneTimeOut = 90  
ManagerDataFsSize = 450  
ThinProvisioned = true
```

```

BackupMinPercent = 50
EnableHardReservations = false
ManagerDataFsSize = 450
WorkerDataFsSize = 450

CwVMs = {
  "0" = {
    VMName = "vm0",
    ManagementIPAddress = "172.25.87.82",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.82",
    NodeType = "Hybrid"
  },
  "1" = {
    VMName = "vm1",
    ManagementIPAddress = "172.25.87.83",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.83",
    NodeType = "Hybrid"
  },
  "2" = {
    VMName = "vm2",
    ManagementIPAddress = "172.25.87.84",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.84",
    NodeType = "Hybrid"
  },
  "3" = {
    VMName = "vmworker",
    ManagementIPAddress = "172.25.87.85",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.84",
    NodeType = "Worker"
  },
  "4" = {
    VMName = "vmworker2",
    ManagementIPAddress = "172.25.87.86",
    DataIPAddress = "0.0.0.0",
    DataIPAddress = "192.168.123.86",
    NodeType = "Worker"
  },
}

/***** vCentre Resource Data with Cw VM assignment *****/

VCentreDC = {
  VCentreAddress = "172.25.87.90",
  VCentreUser = administrator@vsphere.local,
  VCentrePassword = "*****",
  DCname = "dc-cr",
  MgmtNetworkName = "VM Network",
  DataNetworkName = "DPortGroup10",
  VMs = [
    {
      HostedCwVMs = [
        "0",
        "1",
        "2",
        "3", "4"
      ]
    }
  ],
}

```

```

    Host = "172.25.87.93",
    Datastore = "datastore3"
  HSDatastore = "datastore3",
},]
}

```

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_mgr_nodes = 2
#Default Max number of manager nodes
  max_mgr_nodes = 3
#Default seed node key name
  default_seed_node = "0"
}

```

Sample CloudFormation template for installing Crosswork Cluster VMs on AWS EC2



Attention The following CF template (.yaml file) contains the details to install a Crosswork cluster with 3 VMs. Please note that it is only a sample, and you can always create a different CF template according to your production preferences and execute it as per the steps mentioned in this section. This document assumes that you are familiar with AWS and the CloudFormation concepts, and as such, the CF template creation is out of the scope of this document.

```

Description: "Sample CF Template for deploying Cisco Crosswork cluster VMs, with single hybrid, on EC2"

```

```

Metadata:
  AWS::CloudFormation::Interface:
    ParameterGroups:
      -
        Label:
          default: "Cw Network Configuration"
    Parameters:
      - VpcId
      - SecGroup

```

```

- CwSSHPassword
- CwAmiId
- CwMgmtSubnetId
- CwMgmtSubnetNetmask
- CwMgmtSubnetGateway
- CwMgmtVIP
- InterfaceDeploymentMode
- CwDataSubnetId
- CwDataSubnetNetmask
- CwDataSubnetGateway
- CwDataVIP
- Label:
  default: "Cw VM customization"
  Parameters:
    - InstanceType
    - DataDiskSize
    - K8sServiceNetwork
    - K8sPodNetwork
- Label:
  default: "OPTIONAL - VM IP addressing"
  Parameters:
    - Cw1MgmtIP
    - Cw1DataIP
    - Cw2MgmtIP
    - Cw2DataIP
    - Cw3MgmtIP
    - Cw3DataIP

Parameters:
  VpcId:
    Type: AWS::EC2::VPC::Id
    Description: VpcId of your existing Virtual Private Cloud (VPC)
    ConstraintDescription: Must be the VPC Id of an existing Virtual Private Cloud.

  SecGroup:
    Type: AWS::EC2::SecurityGroup::Id
    Description: Pre-created security group to be applied. Must allow ingress access for
ports 22, 30160:31560

  CwMgmtSubnetId:
    Type: AWS::EC2::Subnet::Id
    Description: Select the management subnet for the Crosswork VMs

  CwMgmtSubnetNetmask:
    Type: String
    Description: Enter the management subnet netmask in dotted decimal form, eg 255.255.255.0

    Default: "255.255.255.0"
    AllowedPattern: (\d{1,3})\.\d{1,3}\.\d{1,3}\.\d{1,3}

  CwMgmtSubnetGateway:
    Type: String
    Description: Enter the management default gateway on the selected management subnet.
This is typically the first address on the subnet.
    AllowedPattern: (\d{1,3})\.\d{1,3}\.\d{1,3}\.\d{1,3}

  CwMgmtVIP:
    Type: String
    Description: OPTIONAL - Specify a free address on the management subnet to be used as
the VIP. If not specified an address will be assigned automatically.
    AllowedPattern: ((\d{1,3})\.\d{1,3})\.\d{1,3}\.\d{1,3})|^$
    Default: ""

  CwDataSubnetId:

```



```

    Type: AWS::EC2::Subnet::Id
    Description: Select the data subnet for the Crosswork VMs. In single interface deployments
    select the same subnet as for the management interface.

InterfaceDeploymentMode:
  Type: String
  Description: Select 1 (Management only) or 2 (Management + Data) interface deployment
  mode.
  AllowedValues:
    - 1
    - 2

CwDataSubnetNetmask:
  Type: String
  Description: Enter the data subnet netmask in dotted decimal form, eg 255.255.255.0.
  Ignored when deploying in single interface mode.
  Default: "255.255.255.0"
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})

CwDataSubnetGateway:
  Type: String
  Description: Enter the management default gateway on the selectec data subnet. This is
  typically the first address on the subnet. Ignored when deploying in single interface mode.

  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})
  Default: '0.0.0.0'

CwDataVIP:
  Type: String
  Description: OPTIONAL - Specify a free address on the data subnet to be used as the
  VIP. If not specified an address will be assigned automatically.
  AllowedPattern: ((\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3}))|^$
  Default: ""

CwAmiId:
  Type: AWS::EC2::Image::Id
  Description: Provide Crosswork AMI ID.

# MgmtPublicIP:
#   Type: String
#   Description: Enter your public IP. Will be use to restrict CNC SSH and UI access to
  this IP only
#   Default: 0.0.0.0/0

CwSSHPassword:
  Type: String
  Description: Enter CNC SSH Password. NOTE; Use of external secret store is recommended.

  NoEcho: True

InstanceType:
  Description: Enter EC2 instance type for the node instances.Default is m5.4xlarge.
  Type: String
  AllowedValues:
    - m5.4xlarge
    - m5.8xlarge
    - m5.2xlarge
    - m5.12xlarge
    - m5d.4xlarge
    - m5d.8xlarge
    - m5d.2xlarge
    - m5d.12xlarge
    - m5n.4xlarge
    - m5n.8xlarge

```

```

- m5n.2xlarge
- m5n.12xlarge
- r5.4xlarge
- r5.8xlarge
- r5.2xlarge
- r5.12xlarge
- c5.4xlarge
- c5.8xlarge
- c5.2xlarge
- c5.12xlarge
- m5zn.2xlarge
- m5zn.3xlarge
- m5zn.4xlarge
Default: m5.4xlarge

DataDiskSize:
  Description: Cw data disk size.
  Type: Number
  MinValue: 450
  Default: 450

K8sServiceNetwork:
  Type: String
  Description: "OPTIONAL - Enter the network address for the k8s service network. The
CIDR range is fixed to '/16'."
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})
  Default: '10.96.0.0'

K8sPodNetwork:
  Type: String
  Description: "OPTIONAL - Enter the network address for the k8s pod network. The CIDR
range is fixed to '/16'."
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})
  Default: '10.244.0.0'

Cw1MgmtIP:
  Type: String
  Description: OPTIONAL - Specify a free address on the management subnet. If not specified
an address will be assigned automatically.
  AllowedPattern: ((\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3}))|^$
  Default: ""

Cw1DataIP:
  Type: String
  Description: OPTIONAL - Specify a free address on the data subnet. If not specified an
address will be assigned automatically.
  AllowedPattern: ((\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3}))|^$
  Default: ""

Cw2MgmtIP:
  Type: String
  Description: OPTIONAL - Specify a free address on the management subnet. If not specified
an address will be assigned automatically.
  AllowedPattern: ((\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3}))|^$
  Default: ""

Cw2DataIP:
  Type: String
  Description: OPTIONAL - Specify a free address on the data subnet. If not specified an
address will be assigned automatically.
  AllowedPattern: ((\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3}))|^$
  Default: ""

Cw3MgmtIP:

```

```

    Type: String
    Description: OPTIONAL - Specify a free address on the management subnet. If not specified
    an address will be assigned automatically.
    AllowedPattern: ((\d{1,3})\.\d{1,3})\.\d{1,3})\.\d{1,3})|^$
    Default: ""

    Cw3DataIP:
    Type: String
    Description: OPTIONAL - Specify a free address on the data subnet. If not specified an
    address will be assigned automatically.
    AllowedPattern: ((\d{1,3})\.\d{1,3})\.\d{1,3})\.\d{1,3})|^$
    Default: ""

    CwClusterPlacementStrategy:
    Type: String
    Description: Specify the EC2 instance placement strategy. Default 'cluster' ensures
    maximum throughput.
    Default: cluster
    AllowedValues:
    - cluster
    - partition
    - spread

    Conditions:
    DeployDataInterface: !Not
    - !Equals
    - !Ref InterfaceDeploymentMode
    - "1"

    SetMgmtVIP: !Not
    - !Equals
    - !Ref CwMgmtVIP
    - ""

    SetDataVIP: !Not
    - !Equals
    - !Ref CwDataVIP
    - ""

    SetCw1IP0: !Not
    - !Equals
    - !Ref Cw1MgmtIP
    - ""

    SetCw1IP1: !Not
    - !Equals
    - !Ref Cw1DataIP
    - ""

    SetCw2IP0: !Not
    - !Equals
    - !Ref Cw2MgmtIP
    - ""

    SetCw2IP1: !Not
    - !Equals
    - !Ref Cw2DataIP
    - ""

    SetCw3IP0: !Not
    - !Equals
    - !Ref Cw3MgmtIP
    - ""

```

```

SetCw3IP1: !Not
- !Equals
- !Ref Cw3DataIP
- ""

Resources:
  EC2ENIRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      Policies:
        - PolicyName: eni-modification
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
                  - ec2:DescribeNetworkInterfaces
                  - ec2:AssignPrivateIpAddresses
                  - ec2:UnassignPrivateIpAddresses
                Resource: "*"

  CwPlacementGroup:
    Type: AWS::EC2::PlacementGroup
    Properties:
      Strategy: !Sub ${CwClusterPlacementStrategy}

  CwEC2IamInstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      InstanceProfileName: !Sub ${AWS::StackName}-CwEC2IamInstanceProfile
      Path: "/cw/"
      Roles:
        - !Ref EC2ENIRole

  CwInstance1MgmtInterface:
    Type: AWS::EC2::NetworkInterface
    Properties:
      Description: "VM1-Mgmt-eth0"
      GroupSet:
        #- !Ref 'SSHSecurityGroup'
        - !Ref SecGroup
      PrivateIpAddresses:
        !If
        - SetCw1IP0
        - !If
          - SetMgmtVIP
          - - Primary: false
            PrivateIpAddress: !Ref CwMgmtVIP
          - Primary: true
            PrivateIpAddress: !Ref Cw1MgmtIP
        - - Primary: true
          PrivateIpAddress: !Ref Cw1MgmtIP
        - !If
          - SetMgmtVIP
          - - Primary: false

```

```

        PrivateIpAddress: !Ref CwMgmtVIP
        - !Ref 'AWS::NoValue'
    SecondaryPrivateIpAddressCount:
    !If
    - SetMgmtVIP
    - !Ref 'AWS::NoValue'
    - !If
    - SetCw1IP0
    - !Ref 'AWS::NoValue'
    - 1
    SubnetId: !Ref CwMgmtSubnetId
    Tags:
    - Key: Name
      Value: Cw-VM1-eth0

CwInstance1DataInterface:
Type: AWS::EC2::NetworkInterface
Properties:
  Description: "VM1-Data-eth1"
  GroupSet:
    #- !Ref 'SSHSecurityGroup'
    - !Ref SecGroup
  PrivateIpAddresses:
    !If
    - SetCw1IP1
    - !If
    - SetDataVIP
    - - Primary: false
      PrivateIpAddress: !Ref CwDataVIP
    - Primary: true
      PrivateIpAddress: !Ref Cw1DataIP
    - - Primary: true
      PrivateIpAddress: !Ref Cw1DataIP
    - !If
    - SetDataVIP
    - - Primary: false
      PrivateIpAddress: !Ref CwDataVIP
    - !Ref 'AWS::NoValue'
  SecondaryPrivateIpAddressCount:
    !If
    - SetDataVIP
    - !Ref 'AWS::NoValue'
    - !If
    - SetCw1IP1
    - !Ref 'AWS::NoValue'
    - 1
  SubnetId: !Ref CwDataSubnetId
  Tags:
  - Key: Name
    Value: Cw-VM1-eth1
  Condition: DeployDataInterface

CwInstance2MgmtInterface:
Type: AWS::EC2::NetworkInterface
Properties:
  Description: "VM2-Mgmt-eth0"
  GroupSet:
    #- !Ref 'SSHSecurityGroup'
    - !Ref SecGroup
  PrivateIpAddresses:
    !If
    - SetCw2IP0
    - - Primary: true
      PrivateIpAddress: !Ref Cw2MgmtIP

```

```

    - !Ref 'AWS::NoValue'
  SubnetId: !Ref CwMgmtSubnetId
  Tags:
    - Key: Name
      Value: Cw-VM2-eth0

CwInstance2DataInterface:
  Type: AWS::EC2::NetworkInterface
  Properties:
    Description: "VM2-Data-eth1"
    GroupSet:
      #- !Ref 'SSHSecurityGroup'
      - !Ref SecGroup
    PrivateIpAddresses:
      !If
        - SetCw2IP1
        - - Primary: true
          PrivateIpAddress: !Ref Cw2DataIP
      - !Ref 'AWS::NoValue'
    SubnetId: !Ref CwDataSubnetId
  Tags:
    - Key: Name
      Value: VM2-eth1
  Condition: DeployDataInterface

CwInstance3MgmtInterface:
  Type: AWS::EC2::NetworkInterface
  Properties:
    Description: "VM3-Mgmt-eth0"
    GroupSet:
      #- !Ref 'SSHSecurityGroup'
      - !Ref SecGroup
    PrivateIpAddresses:
      !If
        - SetCw3IP0
        - - Primary: true
          PrivateIpAddress: !Ref Cw3MgmtIP
      - !Ref 'AWS::NoValue'
    SubnetId: !Ref CwMgmtSubnetId
  Tags:
    - Key: Name
      Value: VM3-eth0

CwInstance3DataInterface:
  Type: AWS::EC2::NetworkInterface
  Properties:
    Description: "VM3-Data-eth1"
    GroupSet:
      #- !Ref 'SSHSecurityGroup'
      - !Ref SecGroup
    PrivateIpAddresses:
      !If
        - SetCw3IP1
        - - Primary: true
          PrivateIpAddress: !Ref Cw3DataIP
      - !Ref 'AWS::NoValue'
    SubnetId: !Ref CwDataSubnetId
  Tags:
    - Key: Name
      Value: VM3-eth1
  Condition: DeployDataInterface

# SSHSecurityGroup:
# #

```

```

http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-security-group.html
#   Type: AWS::EC2::SecurityGroup
#   Properties:
#     VpcId: !Ref "VpcId"
#     GroupDescription: Enable access to CNC VMs
#     Tags:
#       - Key: Name
#         Value: "Cw-SG-1"
#     SecurityGroupIngress:
#       # Must allow 22 and all of the service port range 30160:31560
#       #   - CidrIp: !Ref CwMgmtSubnetId
#       #     FromPort: 22
#       #     IpProtocol: tcp
#       #     ToPort: 22
#       #   - CidrIp: !Ref CwMgmtSubnetId
#       #     FromPort: 30603
#       #     IpProtocol: tcp
#       #     ToPort: 30603
#     - CidrIp: 10.0.0.0/8
#       FromPort: -1
#       IpProtocol: -1
#       ToPort: -1

#EC2 Launch Template Creation
CommonCwLaunchTemplate:
  Type: AWS::EC2::LaunchTemplate
  Properties:
    LaunchTemplateName: !Sub CommonCwLaunchTemplate-${AWS::StackName}
    LaunchTemplateData:
      InstanceType: !Ref 'InstanceType'
      ImageId: !Ref 'CwAmiId'
      IamInstanceProfile:
        Name: !Ref CwEC2IamInstanceProfile
      EbsOptimized: True
#     InstanceMarketOptions:
#     MarketType: spot
      Placement:
        GroupName: !Ref CwPlacementGroup
      BlockDeviceMappings:
        - Ebs:
            VolumeSize: 50
            VolumeType: standard
            DeleteOnTermination: True
            Encrypted: False
            #Iops: 1000
            DeviceName: /dev/sda1
        - Ebs:
            VolumeSize: 10
            DeleteOnTermination: True
            VolumeType: gp3
            DeviceName: /dev/sdc
        - Ebs:
            VolumeSize: !Ref DataDiskSize
            DeleteOnTermination: True
            VolumeType: gp3
            Iops: 6000
            DeviceName: /dev/sdd
        - Ebs:
            VolumeSize: 10
            VolumeType: gp3
            DeleteOnTermination: True
            #Iops: 6000
            DeviceName: /dev/sdm
        - Ebs:

```

```

        VolumeSize: 156
        DeleteOnTermination: True
        VolumeType: gp3
        Iops: 6000
        DeviceName: /dev/sdf
    - Ebs:
        VolumeSize: 250
        DeleteOnTermination: True
        VolumeType: gp3
        DeviceName: /dev/sdg
    MetadataOptions:
        HttpPutResponseHopLimit: 2
    PrivateDnsNameOptions:
        EnableResourceNameDnsARecord: True
    TagSpecifications:
    - ResourceType: instance
      Tags:
    - Key: cisco-bu-group
      Value: "spnaa"
    - Key: cisco-bu-owner
      Value: ""
    - Key: cisco-bu-project-name
      Value: "Crosswork"
    - Key: cisco-bu-release
      Value: "440"
    - Key: cisco-bu-role
      Value: "test"
    - Key: cisco-ops-runtime-optin
      Value: "in"
    - Key: cisco-ops-runtime-policy
      Value: "mon-fri"
    - Key: cisco-ops-timezone
      Value: "PST"
    - Key: cisco-sec-internetfacing
      Value: "false"

    CwInstance1:
    #
    http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-instance.html

    Type: AWS::EC2::Instance
    DependsOn:
    - CommonCwLaunchTemplate
    Properties:
    LaunchTemplate:
    Version: 1
    LaunchTemplateId: !Ref CommonCwLaunchTemplate
    NetworkInterfaces: !If
    - DeployDataInterface
    - - NetworkInterfaceId: !Ref CwInstance1MgmtInterface
      DeviceIndex: "0"
    - NetworkInterfaceId: !Ref CwInstance1DataInterface
      DeviceIndex: "1"
    - - NetworkInterfaceId: !Ref CwInstance1MgmtInterface
      DeviceIndex: "0"
    Tags:
    - Key: Name
      Value: Cw-EC2-VM1
    UserData: !Base64
    Fn::Join:
    - ''
    - - !Sub |
      <?xml version="1.0" encoding="UTF-8"?>
      <Environment

```



```

    <PlatformSection>
      <Kind>EC2</Kind>
    </PlatformSection>
    <PropertySection>
      <Property oe:key="CWPassword" oe:value="\${CwSSHPassword}"/>
      <Property oe:key="CWUsername" oe:value="cw-admin"/>
    - Fn::Join:
      - ""
      - - '<Property oe:key="AwsIamRole" oe:value="'
        - !Ref EC2ENIRole
        - '"/>'
        - "\n"
    - !Sub |
      <Property oe:key="IsSeed" oe:value="True"/>
      <Property oe:key="VMType" oe:value="Hybrid"/>
      <Property oe:key="ManagementIPv4Address"
oe:value="\${CwInstance1MgmtInterface.PrimaryPrivateIpAddress}"/>
      <Property oe:key="ManagementIPv4Gateway" oe:value="\${CwMgmtSubnetGateway}"/>

      <Property oe:key="ManagementIPv4Netmask" oe:value="\${CwMgmtSubnetNetmask}"/>

      <Property oe:key="ManagementIPv6Address" oe:value="::0"/>
      <Property oe:key="ManagementIPv6Gateway" oe:value="::1"/>
      <Property oe:key="ManagementIPv6Netmask" oe:value="64"/>
      <Property oe:key="ManagerPeerIPs"
oe:value="\${CwInstance1MgmtInterface.PrimaryPrivateIpAddress}
\${CwInstance2MgmtInterface.PrimaryPrivateIpAddress}
\${CwInstance3MgmtInterface.PrimaryPrivateIpAddress}"/>
      - Fn::Join:
        - ""
        - - '<Property oe:key="ManagementVIP" oe:value="'
          - Fn::Select: [0, Fn::GetAtt: [CwInstance1MgmtInterface,
SecondaryPrivateIpAddresses]]
          - '"/>'
          - "\n"
    - !If
      - DeployDataInterface
      # Join statement to construct the Data Interface configs
      - Fn::Join:
        - "\n"
        - - Fn::Sub: |
          <Property oe:key="DataIPv4Address"
oe:value="\${CwInstance1DataInterface.PrimaryPrivateIpAddress}"/>
          <Property oe:key="DataIPv4Netmask" oe:value="\${CwDataSubnetNetmask}"/>

          <Property oe:key="DataIPv4Gateway" oe:value="\${CwDataSubnetGateway}"/>

          <Property oe:key="DataPeerIPs"
oe:value="\${CwInstance1DataInterface.PrimaryPrivateIpAddress}
\${CwInstance2DataInterface.PrimaryPrivateIpAddress}
\${CwInstance3DataInterface.PrimaryPrivateIpAddress}"/>
          - Fn::Join:
            - ""
            - - '<Property oe:key="DataVIP" oe:value="'
              - Fn::Select: [0, Fn::GetAtt: [CwInstance1DataInterface,
SecondaryPrivateIpAddresses]]
              - '"/>'
              - "\n"
      # Default settings when no data interface is present
      - |
        <Property oe:key="DataIPv4Address" oe:value="0.0.0.0"/>
        <Property oe:key="DataIPv4Netmask" oe:value="255.255.255.0"/>
        <Property oe:key="DataIPv4Gateway" oe:value="0.0.0.0"/>
        <Property oe:key="DataVIP" oe:value="0.0.0.0"/>

```

```

        <Property oe:key="DataPeerIPs" oe:value=""/>
- !Sub |
  <Property oe:key="NTP" oe:value="169.254.169.123"/>
  <Property oe:key="DNsv4" oe:value="169.254.169.253"/>
  <Property oe:key="DNsv6" oe:value="::0"/>
  <Property oe:key="Domain" oe:value=""/>
  <Property oe:key="InitMasterCount" oe:value="3"/>
  <Property oe:key="InitNodeCount" oe:value="3"/>
  <Property oe:key="VMLocation" oe:value="AWS"/>
  <Property oe:key="DataIPv6Address" oe:value="::0"/>
  <Property oe:key="DataIPv6Gateway" oe:value="::1"/>
  <Property oe:key="DataIPv6Netmask" oe:value="64"/>
  <Property oe:key="Deployment" oe:value="cw_ipv4"/>
  <Property oe:key="Disclaimer" oe:value="Cisco Crosswork"/>
  <Property oe:key="K8Orch" oe:value=""/>
  <Property oe:key="CwInstaller" oe:value="False"/>
  <Property oe:key="corefs" oe:value="20"/>
  <Property oe:key="ddatafs" oe:value="\${DataDiskSize}"/>
  <Property oe:key="logfs" oe:value="10"/>
  <Property oe:key="ramdisk" oe:value="0"/>
  <Property oe:key="ssd" oe:value="50"/>
  <Property oe:key="K8sServiceNetworkV4" oe:value="\${K8sServiceNetwork}"/>
  <Property oe:key="K8sPodNetworkV4" oe:value="\${K8sPodNetwork}"/>
</PropertySection>
</Environment>

CwInstance2:
#
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-instance.html

Type: AWS::EC2::Instance
DependsOn:
- CommonCwLaunchTemplate
Properties:
LaunchTemplate:
  Version: 1
  LaunchTemplateId: !Ref CommonCwLaunchTemplate
NetworkInterfaces: !If
- DeployDataInterface
- - NetworkInterfaceId: !Ref CwInstance2MgmtInterface
  DeviceIndex: "0"
- - NetworkInterfaceId: !Ref CwInstance2DataInterface
  DeviceIndex: "1"
- - NetworkInterfaceId: !Ref CwInstance2MgmtInterface
  DeviceIndex: "0"
Tags:
- Key: Name
  Value: Cw-EC2-VM2
UserData: !Base64
'Fn::Join':
- ''
- - !Sub |
  <?xml version="1.0" encoding="UTF-8"?>
  <Environment
  <PlatformSection>
  <Kind>EC2</Kind>
  </PlatformSection>
  <PropertySection>
  <Property oe:key="CWPASSWORD" oe:value="\${CwSSHPASSWORD}"/>
  <Property oe:key="CWUsername" oe:value="cw-admin"/>
  </PropertySection>
  </Environment>
- Fn::Join:
- ""
- - '<Property oe:key="AwsIamRole" oe:value="'
  - !Ref EC2ENIRole

```

```

- '"/>'
- "\n"
- !Sub |
  <Property oe:key="IsSeed" oe:value="False"/>
  <Property oe:key="VMType" oe:value="Hybrid"/>
  <Property oe:key="ManagementIPv4Address"
oe:value="\${CwInstance2MgmtInterface.PrimaryPrivateIpAddress}"/>
  <Property oe:key="ManagementIPv4Gateway" oe:value="\${CwMgmtSubnetGateway}"/>

  <Property oe:key="ManagementIPv4Netmask" oe:value="\${CwMgmtSubnetNetmask}"/>

  <Property oe:key="ManagementIPv6Address" oe:value="::0"/>
  <Property oe:key="ManagementIPv6Gateway" oe:value="::1"/>
  <Property oe:key="ManagementIPv6Netmask" oe:value="64"/>
  <Property oe:key="ManagerPeerIPs"
oe:value="\${CwInstance1MgmtInterface.PrimaryPrivateIpAddress}
\${CwInstance2MgmtInterface.PrimaryPrivateIpAddress}
\${CwInstance3MgmtInterface.PrimaryPrivateIpAddress}"/>
  - Fn::Join:
    - ""
    - - '<Property oe:key="ManagementVIP" oe:value="'
      - Fn::Select: [0, Fn::GetAtt: [CwInstance1MgmtInterface,
SecondaryPrivateIpAddresses]]
      - '"/>'
      - "\n"
  - !If
    - DeployDataInterface
    # Join statement to construct the Data Interface configs
    - Fn::Join:
      - "\n"
      - - Fn::Sub: |
          <Property oe:key="DataIPv4Address"
oe:value="\${CwInstance2DataInterface.PrimaryPrivateIpAddress}"/>
          <Property oe:key="DataIPv4Netmask" oe:value="\${CwDataSubnetNetmask}"/>

          <Property oe:key="DataIPv4Gateway" oe:value="\${CwDataSubnetGateway}"/>

          <Property oe:key="DataPeerIPs"
oe:value="\${CwInstance1DataInterface.PrimaryPrivateIpAddress}
\${CwInstance2DataInterface.PrimaryPrivateIpAddress}
\${CwInstance3DataInterface.PrimaryPrivateIpAddress}"/>
          - Fn::Join:
            - ""
            - - '<Property oe:key="DataVIP" oe:value="'
              - Fn::Select: [0, Fn::GetAtt: [CwInstance1DataInterface,
SecondaryPrivateIpAddresses]]
              - '"/>'
              - "\n"
          # Default settings when no data interface is present
          - |
            <Property oe:key="DataIPv4Address" oe:value="0.0.0.0"/>
            <Property oe:key="DataIPv4Netmask" oe:value="255.255.255.0"/>
            <Property oe:key="DataIPv4Gateway" oe:value="0.0.0.0"/>
            <Property oe:key="DataVIP" oe:value="0.0.0.0"/>
            <Property oe:key="DataPeerIPs" oe:value=""/>
      - !Sub |
        <Property oe:key="NTP" oe:value="169.254.169.123"/>
        <Property oe:key="DNSv4" oe:value="169.254.169.253"/>
        <Property oe:key="DNSv6" oe:value="::0"/>
        <Property oe:key="Domain" oe:value=""/>
        <Property oe:key="InitMasterCount" oe:value="3"/>
        <Property oe:key="InitNodeCount" oe:value="3"/>
        <Property oe:key="VMLocation" oe:value="AWS"/>
        <Property oe:key="DataIPv6Address" oe:value="::0"/>

```

```

    <Property oe:key="DataIPv6Gateway" oe:value="::1"/>
    <Property oe:key="DataIPv6Netmask" oe:value="64"/>
    <Property oe:key="Deployment" oe:value="cw_ipv4"/>
    <Property oe:key="Disclaimer" oe:value="Cisco Crosswork"/>
    <Property oe:key="K8Orch" oe:value=""/>
    <Property oe:key="CwInstaller" oe:value="False"/>
    <Property oe:key="corefs" oe:value="20"/>
    <Property oe:key="ddatafs" oe:value="\${DataDiskSize}"/>
    <Property oe:key="logfs" oe:value="10"/>
    <Property oe:key="ramdisk" oe:value="0"/>
    <Property oe:key="ssd" oe:value="50"/>
    <Property oe:key="K8sServiceNetworkV4" oe:value="\${K8sServiceNetwork}"/>
    <Property oe:key="K8sPodNetworkV4" oe:value="\${K8sPodNetwork}"/>
  </PropertySection>
</Environment>

CwInstance3:
#
http://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/aws-properties-ec2-instance.html

Type: AWS::EC2::Instance
Properties:
  LaunchTemplate:
    Version: 1
    LaunchTemplateId: !Ref CommonCwLaunchTemplate
  NetworkInterfaces: !If
    - DeployDataInterface
    - - NetworkInterfaceId: !Ref CwInstance3MgmtInterface
      DeviceIndex: "0"
    - - NetworkInterfaceId: !Ref CwInstance3DataInterface
      DeviceIndex: "1"
    - - NetworkInterfaceId: !Ref CwInstance3MgmtInterface
      DeviceIndex: "0"
  Tags:
    - Key: Name
      Value: Cw-EC2-VM3
  UserData: !Base64
    'Fn::Join':
      - ''
      - - !Sub |
          <?xml version="1.0" encoding="UTF-8"?>
          <Environment
            <PlatformSection>
              <Kind>EC2</Kind>
            </PlatformSection>
            <PropertySection>
              <Property oe:key="CWPassword" oe:value="\${CwSSHPasssword}"/>
              <Property oe:key="CWUsername" oe:value="cw-admin"/>
            </PropertySection>
          </Environment>
      - Fn::Join:
          - ""
          - - '<Property oe:key="AwsIamRole" oe:value="'
            - !Ref EC2ENIRole
            - '"/>'
            - "\n"
      - !Sub |
          <Property oe:key="IsSeed" oe:value="False"/>
          <Property oe:key="VMType" oe:value="Hybrid"/>
          <Property oe:key="ManagementIPv4Address"
            oe:value="\${CwInstance3MgmtInterface.PrimaryPrivateIpAddress}"/>
          <Property oe:key="ManagementIPv4Gateway" oe:value="\${CwMgmtSubnetGateway}"/>
          <Property oe:key="ManagementIPv4Netmask" oe:value="\${CwMgmtSubnetNetmask}"/>
          <Property oe:key="ManagementIPv6Address" oe:value="::0"/>

```

```

        <Property oe:key="ManagementIPv6Gateway" oe:value="::1"/>
        <Property oe:key="ManagementIPv6Netmask" oe:value="64"/>
        <Property oe:key="ManagerPeerIPs"
oe:value="${CwInstance1MgmtInterface.PrimaryPrivateIpAddress}
${CwInstance2MgmtInterface.PrimaryPrivateIpAddress}
${CwInstance3MgmtInterface.PrimaryPrivateIpAddress}"/>
    - Fn::Join:
      - ""
      - - '<Property oe:key="ManagementVIP" oe:value="'
        - Fn::Select: [0, Fn::GetAtt: [CwInstance1MgmtInterface,
SecondaryPrivateIpAddresses]]
        - '"/>'
        - "\n"
    - !If
      - DeployDataInterface
      # Join statement to construct the Data Interface configs
      - Fn::Join:
        - "\n"
        - - Fn::Sub: |
            <Property oe:key="DataIPv4Address"
oe:value="${CwInstance3DataInterface.PrimaryPrivateIpAddress}"/>
            <Property oe:key="DataIPv4Netmask" oe:value="${CwDataSubnetNetmask}"/>

            <Property oe:key="DataIPv4Gateway" oe:value="${CwDataSubnetGateway}"/>

            <Property oe:key="DataPeerIPs"
oe:value="${CwInstance1DataInterface.PrimaryPrivateIpAddress}
${CwInstance2DataInterface.PrimaryPrivateIpAddress}
${CwInstance3DataInterface.PrimaryPrivateIpAddress}"/>
            - Fn::Join:
              - ""
              - - '<Property oe:key="DataVIP" oe:value="'
                - Fn::Select: [0, Fn::GetAtt: [CwInstance1DataInterface,
SecondaryPrivateIpAddresses]]
                - '"/>'
                - "\n"
            # Default settings when no data interface is present
            - |
                <Property oe:key="DataIPv4Address" oe:value="0.0.0.0"/>
                <Property oe:key="DataIPv4Netmask" oe:value="255.255.255.0"/>
                <Property oe:key="DataIPv4Gateway" oe:value="0.0.0.0"/>
                <Property oe:key="DataVIP" oe:value="0.0.0.0"/>
                <Property oe:key="DataPeerIPs" oe:value=""/>
            - !Sub |
                <Property oe:key="NTP" oe:value="169.254.169.123"/>
                <Property oe:key="DNSv4" oe:value="169.254.169.253"/>
                <Property oe:key="DNSv6" oe:value="::0"/>
                <Property oe:key="Domain" oe:value=""/>
                <Property oe:key="InitMasterCount" oe:value="3"/>
                <Property oe:key="InitNodeCount" oe:value="3"/>
                <Property oe:key="VMLocation" oe:value="AWS"/>
                <Property oe:key="DataIPv6Address" oe:value="::0"/>
                <Property oe:key="DataIPv6Gateway" oe:value="::1"/>
                <Property oe:key="DataIPv6Netmask" oe:value="64"/>
                <Property oe:key="Deployment" oe:value="cw_ipv4"/>
                <Property oe:key="Disclaimer" oe:value="Cisco Crosswork"/>
                <Property oe:key="K8Orch" oe:value=""/>
                <Property oe:key="CwInstaller" oe:value="False"/>
                <Property oe:key="corefs" oe:value="20"/>
                <Property oe:key="ddatafs" oe:value="${DataDiskSize}"/>
                <Property oe:key="logfs" oe:value="10"/>
                <Property oe:key="ramdisk" oe:value="0"/>
                <Property oe:key="ssd" oe:value="50"/>
                <Property oe:key="K8sServiceNetworkV4" oe:value="${K8sServiceNetwork}"/>

```

```

    <Property oe:key="K8sPodNetworkV4" oe:value="\${K8sPodNetwork}"/>
  </PropertySection>
</Environment>

```

Outputs:

```

CrossworkClusterStack:
  Description: The Name of the Cw cluster stack
  Value: !Sub ${AWS::StackName}
CrossworkManagementVIP:
  Value:
    Fn::Select: [0, Fn::GetAtt: [CwInstance1MgmtInterface, SecondaryPrivateIpAddresses]]

Export:
  Name: !Sub ${AWS::StackName}-Cw-MgmtVIP
CrossworkManagementIP1:
  Value: !Sub ${CwInstance1MgmtInterface.PrimaryPrivateIpAddress}
CrossworkManagementIP2:
  Value: !Sub ${CwInstance2MgmtInterface.PrimaryPrivateIpAddress}
CrossworkManagementIP3:
  Value: !Sub ${CwInstance3MgmtInterface.PrimaryPrivateIpAddress}
CrossworkDataVIP:
  Value:
    Fn::Select: [0, Fn::GetAtt: [CwInstance1DataInterface, SecondaryPrivateIpAddresses]]
Export:
  Name: !Sub ${AWS::StackName}-Cw-DataVIP
  Condition: DeployDataInterface
CrossworkDataIP1:
  Value: !Sub ${CwInstance1DataInterface.PrimaryPrivateIpAddress}
  Condition: DeployDataInterface
CrossworkDataIP2:
  Value: !Sub ${CwInstance2DataInterface.PrimaryPrivateIpAddress}
  Condition: DeployDataInterface
CrossworkDataIP3:
  Value: !Sub ${CwInstance3DataInterface.PrimaryPrivateIpAddress}
  Condition: DeployDataInterface

```

Sample CloudFormation Template for installing Crosswork Data Gateway on EC2



Attention The CF template (.yaml file) displayed in this section contains the details to install a Standard Crosswork Data Gateway with a single interface. Please note that it is only a sample, and you can always create a different CF template according to your production preferences and execute it as per the steps mentioned in this section. This document assumes that a user of this procedure is familiar with AWS and the CloudFormation concepts, and as such, the CF template creation is out of the scope of this document.

```
Description: "Sample template for deploying CDG4.1 VMs - v4.4"
```

Metadata:

```

AWS::CloudFormation::Interface:
  ParameterGroups:
    -
      Label:
        default: "Cw Network Configuration"
      Parameters:
        - VpcId

```

- SecGroup
- CDGSSHPassword
- CDGAmiId
- CNCControllerIP
- CNCControllerPassword
- InterfaceDeploymentMode
- CDGInterface0SubnetId
- CDGInterface0Gateway
- CDGInterface0SubnetNetmask
- CDGInterface1SubnetId
- CDGInterface1Gateway
- CDGInterface1SubnetNetmask
- CDGInterface2SubnetId
- CDGInterface2Gateway
- CDGInterface2SubnetNetmask

Parameters:**VpcId:**

Type: AWS::EC2::VPC::Id

Description: VpcId of your existing Virtual Private Cloud (VPC)

ConstraintDescription: Must be the VPC Id of an existing Virtual Private Cloud.

CDGAmiId:

Type: AWS::EC2::Image::Id

Description: Provide CDG AMI ID

CDGSSHPassword:

Type: String

NoEcho: True

Description: Enter the SSH password to be configured on the CDG

SecGroup:

Type: AWS::EC2::SecurityGroup::Id

Description: Pre-created security group to be applied. Must allow ingress access for ports 22, 30160:31560

CNCControllerPassword:

Type: String

NoEcho: True

Description: Enter the cw-admin user password used to access CNC/Cw Controller

DataDiskSize:

Description: Cw data disk size.

Type: Number

MinValue: 20

Default: 50

CDGProfile:

Type: String

Description: Deployment profile of the CDG

AllowedValues:

- Standard

- Extended

Default: Standard

InstanceType:

Description: Enter EC2 instance type for the node instances. Default is m5zn.3xlarge.

Type: String

AllowedValues:

- m5.4xlarge

- m5.8xlarge

- m5.12xlarge

- m5d.4xlarge

- m5d.8xlarge

```

- m5d.12xlarge
- r5.4xlarge
- r5.8xlarge
- r5.12xlarge
- c5.4xlarge
- c5.8xlarge
- c5.12xlarge
- m5zn.3xlarge
Default: m5zn.3xlarge

InterfaceDeploymentMode:
  Type: String
  Description: Select the single (all traffic), dual (Management + Data) or triple
(Management + Data + Control) interface deployment mode.
  AllowedValues:
    - 1
    - 2
    - 3

CDGInterface0SubnetId:
  Type: AWS::EC2::Subnet::Id
  Description: Select the first interface subnet for the CDG VM.

CDGInterface0Gateway:
  Type: String
  Description: Enter the default gateway on the selected subnet. This is typically the
first address on the subnet.
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})

CDGInterface1SubnetId:
  Type: AWS::EC2::Subnet::Id
  Description: Select the first interface subnet for the CDG VM. Ignored if not using
dual interface mode.

CDGInterface1Gateway:
  Type: String
  Description: Enter the default gateway on the selected subnet. This is typically the
first address on the subnet.
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})
  Default: "0.0.0.1"

CDGInterface2SubnetId:
  Type: AWS::EC2::Subnet::Id
  Description: Select the first interface subnet for the CDG VM. Ignored if not using
triple interface mode.

CDGInterface2Gateway:
  Type: String
  Description: Enter the default gateway on the selected subnet. This is typically the
first address on the subnet.
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})
  Default: "0.0.0.1"

CDGInterface0IPAddress:
  Type: String
  Description: OPTIONAL - Enter a *free* IP address on the 1st subnet. If set to "0.0.0.0",
an IP address will be allocated automatically .
  Default: "0.0.0.0"
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})|^$

CDGInterface0SubnetNetmask:
  Type: String
  Description: Enter the subnet netmask in dotted decimal form, eg 255.255.255.0.
  Default: "255.255.255.0"

```



```

    AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})

CDGInterface1IPAddress:
  Type: String
  Description: OPTIONAL - Enter a *free* IP address on the 2nd subnet. If set to 0.0.0.0,
an IP address will be allocated automatically.
  Default: "0.0.0.0"
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})|^$

CDGInterface1SubnetNetmask:
  Type: String
  Description: Enter the subnet netmask in dotted decimal form, eg 255.255.255.0. Ignored
if not using dual interface mode.
  Default: "255.255.255.0"
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})

CDGInterface2IPAddress:
  Type: String
  Description: OPTIONAL - Enter a *free* IP address on the 3rd subnet. If set to 0.0.0.0,
an IP address will be allocated automatically.
  Default: "0.0.0.0"
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})|^$

CDGInterface2SubnetNetmask:
  Type: String
  Description: Enter the subnet netmask in dotted decimal form, eg 255.255.255.0. Ignored
if not using triple interface mode.
  Default: "255.255.255.0"
  AllowedPattern: (\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3})

CNCControllerIP:
  Type: String
  Description: Specify the address of the Crosswork CDG controller
  AllowedPattern: ((\d{1,3})\.\(\d{1,3})\.\(\d{1,3})\.\(\d{1,3}))|^$
  Default: ""

Conditions:
  DeployInterface0: !Equals
    - !Ref InterfaceDeploymentMode
    - "1"

  DeployInterface1: !Or
    - Fn::Equals:
      - !Ref InterfaceDeploymentMode
      - "2"
    - Fn::Equals:
      - !Ref InterfaceDeploymentMode
      - "3"

  DeployInterface2: !Equals
    - !Ref InterfaceDeploymentMode
    - "3"

  Setif0IP: !Not
    - !Equals
      - !Ref CDGInterface0IPAddress
      - "0.0.0.0"

  Setif1IP: !And
    - !Not
      - !Equals
        - !Ref CDGInterface1IPAddress
        - "0.0.0.0"
    - !Not

```

```

    - !Condition DeployInterface0

Setif2IP: !And
  - !Not
    - !Equals
      - !Ref CDGInterface2IPAddress
      - "0.0.0.0"
  - !Not
    - !Condition DeployInterface0
  - !Not
    - !Condition DeployInterface1

Resources:
  EC2ENIRole:
    Type: AWS::IAM::Role
    Properties:
      AssumeRolePolicyDocument:
        Version: "2012-10-17"
        Statement:
          - Effect: Allow
            Principal:
              Service:
                - ec2.amazonaws.com
            Action:
              - 'sts:AssumeRole'
      Policies:
        - PolicyName: eni-modification
          PolicyDocument:
            Version: '2012-10-17'
            Statement:
              - Effect: Allow
                Action:
                  - ec2:DescribeNetworkInterfaces
                  - ec2:AssignPrivateIpAddresses
                  - ec2:UnassignPrivateIpAddresses
                Resource: "*"

  CDGEC2IamInstanceProfile:
    Type: AWS::IAM::InstanceProfile
    Properties:
      InstanceProfileName: !Sub ${AWS::StackName}-CDG-EC2IamInstanceProfile
      Path: "/cdg/"
      Roles:
        - !Ref EC2ENIRole

  CDG1VNIC0:
    Type: AWS::EC2::NetworkInterface
    Properties:
      Description: "CDG1-VNIC0"
      GroupSet:
        - !Ref SecGroup
      PrivateIpAddresses: !If
        - Setif0IP
          - Primary: true
            PrivateIpAddress: !Ref CDGInterface0IPAddress
        - !Ref 'AWS::NoValue'
      SubnetId: !Ref CDGInterface0SubnetId
      Tags:
        - Key: Name
          Value: !Sub ${AWS::StackName}-CDG1-VNIC0

  CDG1VNIC1:
    Type: AWS::EC2::NetworkInterface
    Properties:

```

```

Description: "CDG1-VNIC1"
GroupSet:
  - !Ref SecGroup
PrivateIpAddresses: !If
  - Setif1IP
    - - Primary: true
      PrivateIpAddress: !Ref CDGInterface1IPAddress
  - !Ref 'AWS::NoValue'
SubnetId: !Ref CDGInterface1SubnetId
Tags:
  - Key: Name
    Value: !Sub ${AWS::StackName}-CDG1-VNIC1
Condition: DeployInterface1

CDG1VNIC2:
Type: AWS::EC2::NetworkInterface
Properties:
  Description: "CDG1-VNIC2"
  GroupSet:
    - !Ref SecGroup
  PrivateIpAddresses: !If
    - Setif2IP
      - - Primary: true
        PrivateIpAddress: !Ref CDGInterface2IPAddress
    - !Ref 'AWS::NoValue'
  SubnetId: !Ref CDGInterface2SubnetId
  Tags:
    - Key: Name
      Value: !Sub ${AWS::StackName}-CDG1-VNIC2
  Condition: DeployInterface2

CommonLaunchTemplateCDG4:
Type: AWS::EC2::LaunchTemplate
Properties:
  LaunchTemplateName: !Sub ${AWS::StackName}-CommonLaunchTemplateCDG4
  LaunchTemplateData:
    InstanceType: !Ref InstanceType
    ImageId: !Ref "CDGAmiId"
    BlockDeviceMappings:
      - Ebs:
          VolumeSize: !Ref DataDiskSize
          DeleteOnTermination: True
          VolumeType: standard
          DeviceName: /dev/sdb
    MetadataOptions:
      HttpPutResponseHopLimit: 2
  IamInstanceProfile:
    Arn: !GetAtt
      - CDGEC2IamInstanceProfile
      - Arn

CDGInstance:
Type: AWS::EC2::Instance
Properties:
  LaunchTemplate:
    Version: 1
    LaunchTemplateId: !Ref CommonLaunchTemplateCDG4
  NetworkInterfaces: !If
    - DeployInterface2
      - - NetworkInterfaceId: !Ref CDG1VNIC0
        DeviceIndex: "0"
      - NetworkInterfaceId: !Ref CDG1VNIC1
        DeviceIndex: "1"

```

```

- NetworkInterfaceId: !Ref CDG1VNIC2
  DeviceIndex: "2"
- !If
- DeployInterface1
- - NetworkInterfaceId: !Ref CDG1VNIC0
  DeviceIndex: "0"
  - NetworkInterfaceId: !Ref CDG1VNIC1
  DeviceIndex: "1"
- - NetworkInterfaceId: !Ref CDG1VNIC0
  DeviceIndex: "0"
Tags:
- Key: Name
  Value: !Sub ${AWS::StackName}-CDG4.0
UserData: !Base64
Fn::Join:
- ''
- - !Sub |
    AwsIamRole=${EC2ENIRole}
    ActiveVnics=${InterfaceDeploymentMode}
    AllowRFC8190=Yes
    AuditdAddress=
    AuditdPort=60
    ControllerCertChainPwd=${CNCControllerPassword}
    ControllerIP=${CNCControllerIP}
    ControllerPort=30607

ControllerSignCertChain=cw-admin@${CNCControllerIP}:/home/cw-admin/controller.pem
ControllerTlsCertChain=
Deployment=Crosswork On-Premise
Description=${AWS::StackName}-CDG4.1-1
DGAppdataDisk=5
DGCertChain=
DGCertChainPwd=
DGCertKey=
DNS=169.254.169.253
DNSSEC=False
DNSTLS=False
Domain=
EnrollmentPassphrase=
EnrollmentURI=
Hostname=${AWS::StackName}-CDG4.1
Label=
LLMNR=False
mDNS=False
NTP=169.254.169.123
NTPAuth=False
NTPKey=
NTPKeyFile=
NTPKeyFilePwd=
PortSNMPTrap=1062
PortSyslogUDP=9514
PortSyslogTCP=9898
PortSyslogTLS=6514
Profile=${CDGProfile}
ProxyBypass=
ProxyCertChain=
ProxyCertChainPwd=
ProxyPassphrase=
ProxyURL=
ProxyUsername=
SyslogAddress=
SyslogCertChain=
SyslogCertChainPwd=
SyslogPeerName=

```

```

SyslogPort=514
SyslogProtocol=UDP
SyslogTLS=False
UseRemoteAuditd=False
UseRemoteSyslog=False
Vnic0IPv4Address=${CDG1VNIC0.PrimaryPrivateIpAddress}
Vnic0IPv4Gateway=${CDGInterface0Gateway}
Vnic0IPv4Method=Static
Vnic0IPv4Netmask=${CDGInterface0SubnetNetmask}
Vnic0IPv4SkipGateway=False
Vnic0IPv6Address=:0
Vnic0IPv6Gateway=:1
Vnic0IPv6Method=None
Vnic0IPv6Netmask=64
Vnic0IPv6SkipGateway=False
- !If
- DeployInterface1
- !Sub |
  Vnic1IPv4Address=${CDG1VNIC1.PrimaryPrivateIpAddress}
  Vnic1IPv4Gateway=${CDGInterface1Gateway}
- |
  Vnic1IPv4Address=0.0.0.0
  Vnic1IPv4Gateway=0.0.0.1
- !Sub |
  Vnic1IPv4Method=Static
  Vnic1IPv4Netmask=${CDGInterface1SubnetNetmask}
  Vnic1IPv4SkipGateway=False
  Vnic1IPv6Address=:0
  Vnic1IPv6Gateway=:1
  Vnic1IPv6Method=None
  Vnic1IPv6Netmask=64
  Vnic1IPv6SkipGateway=False
- !If
- DeployInterface2
- !Sub |
  Vnic2IPv4Address=${CDG1VNIC2.PrimaryPrivateIpAddress}
  Vnic2IPv4Gateway=${CDGInterface2Gateway}
- |
  Vnic2IPv4Address=0.0.0.0
  Vnic2IPv4Gateway=0.0.0.1
- !Sub |
  Vnic2IPv4Method=None
  Vnic2IPv4Netmask=${CDGInterface2SubnetNetmask}
  Vnic2IPv4SkipGateway=False
  Vnic2IPv6Address=:0
  Vnic2IPv6Gateway=:1
  Vnic2IPv6Method=None
  Vnic2IPv6Netmask=64
  Vnic2IPv6SkipGateway=False
  dg-adminPassword=${CDGSSHPassword}
  dg-operPassword=${CDGSSHPassword}

```

Outputs:

```

CDGStack:
  Description: The Name of the CDG cluster stack
  Value: !Sub ${AWS::StackName}
CDGInterface0IPAddress:
  Value: !Sub ${CDG1VNIC0.PrimaryPrivateIpAddress}
CDGInterface1IPAddress:
  Value: !Sub ${CDG1VNIC1.PrimaryPrivateIpAddress}
  Condition: DeployInterface1
CDGInterface2IPAddress:
  Value: !Sub ${CDG1VNIC2.PrimaryPrivateIpAddress}
  Condition: DeployInterface2

```

