



Cisco Crosswork Network Controller 7.0 Installation Guide

First Published: 2024-10-04

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.

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)

© 2024 Cisco Systems, Inc. All rights reserved.



CONTENTS

PART I

Get Started 11

CHAPTER 1

Overview 1

About this guide 1

Audience 1

Introduction 2

Security 3

CHAPTER 2

Plan Your Deployment 5

Before You Begin 5

Determine How Many VMs You Need 5

Identify the Resource Footprint 7

Special Considerations 9

CHAPTER 3

Choose Your Installation Workflow 11

Overview 11

Install Cisco Crosswork Network Controller on VMware vCenter 11

Install Cisco Crosswork Network Controller on AWS EC2 13

Install Cisco Crosswork Network Controller on a Single VM 15

PART II

Install Cisco Crosswork Network Controller on VMware vCenter 17

CHAPTER 4

Installation Prerequisites for VMware vCenter 19

Overview 19

Supported Network Topology Models 19

VMware Settings 24

Host VM Requirements	25
Crosswork Cluster VM Requirements	25
Crosswork Data Gateway VM Requirements	27
Crosswork TCP/UDP Port requirements	29
IP Address Restrictions	34

CHAPTER 5**Install Crosswork Cluster on VMware vCenter 37**

Installation Overview	37
Installation Parameters	37
Automate Application Installation Using Auto Action Functionality	43
Install Cisco Crosswork on VMware vCenter using the Cluster Installer Tool	47
Sample manifest templates for VMware vCenter	51
Manual Installation of Cisco Crosswork using vCenter vSphere UI	60
Build the OVF template	60
Deploy the template	70
Monitor Cluster Activation	73
Log into the Cisco Crosswork UI	76
Import Cluster Inventory	78
Troubleshoot the Cluster	78

CHAPTER 6**Install Crosswork Data Gateway on VMware vCenter 91**

Crosswork Data Gateway Installation Workflow	91
Crosswork Data Gateway Parameters and Deployment Scenarios	92
Install Crosswork Data Gateway using vCenter vSphere Client	105
Install Crosswork Data Gateway via OVF Tool	116
Sample Script for the Crosswork Data Gateway IPv4 Deployment	118
Sample Script for the Crosswork Data Gateway IPv6 Deployment	120
Sample Script for Crosswork Data Gateway Dual-Stack Deployment	121
Sample Script for Crosswork Data Gateway Dual-Stack Deployment with Geo-Redundancy	123
Log in and Log out of the Data Gateway VM	124
Access Crosswork Data Gateway VM from SSH	124
Access Crosswork Data Gateway through vCenter	125
Log Out of Crosswork Data Gateway VM	126
Crosswork Data Gateway Authentication and Enrollment	126

Crosswork Data Gateway Post-installation Tasks	127
Configure Timezone of the Data Gateway VM	127
Troubleshoot Crosswork Data Gateway Installation and Enrollment	128
Import Controller Signing Certificate File	132
View the Controller Signing Certificate File	132

PART III

Install Cisco Crosswork Network Controller on AWS EC2 135

CHAPTER 7
Installation Prerequisites for AWS EC2 137

Overview	137
Amazon EC2 Settings	137
Host VM Requirements	140
Crosswork Cluster VM Requirements	140
Crosswork Data Gateway VM Requirements	141
Crosswork TCP/UDP Port Requirements	143
IP Address Restrictions	147

CHAPTER 8
Install Cisco Crosswork Network Controller on AWS EC2 149

Installation Overview	149
Extract CF Template Image	149
Roles and Policy Permissions	151
Configure the CloudFormation (CF) Template Parameters	151
CF Template Parameters for Installing Cisco Crosswork Cluster VMs	152
CF Template Parameters for Installing Crosswork Data Gateway	158
CF Template Parameters for Installing NSO	161
CF Template Parameters for Installing Single Hybrid Cluster or Worker Node	162
Install Using Module Deployment Method	164
Install Cisco Crosswork Cluster on Amazon EC2	164
Install Crosswork Data Gateway on Amazon EC2	165
Auto-Configuration for Deploying Crosswork Data Gateway	167
Install Cisco NSO on Amazon EC2	170
Deploy an Additional Crosswork Cluster Node	171
Manage CF Template Deployment	171
Deploy a CF Template	172

- Monitor the Installation 173
- Accessing the Crosswork UI 173
- Crosswork Data Gateway Post-installation Tasks 174
 - Configure Timezone of the Data Gateway VM 174
 - Log in and Log out of the Data Gateway VM 176
 - Access Crosswork Data Gateway VM from SSH 176
 - Log out of Crosswork Data Gateway VM 176
 - Troubleshoot Crosswork Data Gateway Installation and Enrollment 176
 - Import Controller Signing Certificate File 179
 - View the Controller Signing Certificate File 180

PART IV **Install Crosswork Applications 181**

CHAPTER 9 **Install Crosswork Applications 183**

- Install Crosswork Applications 183

PART V **Integrate Cisco NSO and SR-PCE with Cisco Crosswork Network Controller 187**

CHAPTER 10 **Integrate Cisco NSO 189**

- NSO Integration Workflow 189
- Add Cisco NSO Providers 190
 - (Optional) Set up Cisco NSO Layered Service Architecture 193
- Install Cisco NSO Function Pack Bundles from Crosswork UI 193
 - View NSO Function Pack Bundles 194
 - Manage NSO Function Pack Bundles 195
 - Deploy NSO Function Pack Bundles 197
 - Troubleshoot the NSO Function Pack Installation 200
 - View NSO Function Pack Job History 201
 - Install NSO Function Packs Manually 202

CHAPTER 11 **Integrate SR-PCE 203**

- SR-PCE Integration Workflow 203
- Configure SR-PCE 203
 - Sample SR-PCE config 206

Add Cisco SR-PCE Providers 206

PART VI

Upgrade Cisco Crosswork Network Controller 211

CHAPTER 12

Upgrade Cisco Crosswork 213

Upgrade Overview 213

Upgrade Requirements 214

Upgrade Using Existing Hardware 216

Shut Down the Data Gateway VMs 217

Create Backup and Shut Down Cisco Crosswork 217

Install the latest version of the Crosswork Network Controller Cluster 220

Install the Crosswork Network Controller Applications 221

Migrate Crosswork Network Controller Backup 221

Upgrade Crosswork Data Gateway 223

Troubleshoot Crosswork Data Gateway Upgrade Issues 225

Post-upgrade Checklist 226

Upgrade Using Parallel Hardware 227

Deploy a new Crosswork Network Controller Cluster 227

Backup Cisco Crosswork Cluster 228

Update DNS Server and Run Migration 230

Add Crosswork Data Gateway to Cisco Crosswork 231

Shut Down the old Cisco Crosswork Cluster 233

Update Crosswork Network Controller applications (standalone activity) 234

PART VII

Uninstall Cisco Crosswork Network Controller 237

CHAPTER 13

Uninstall Cisco Crosswork 239

Uninstall the Crosswork Cluster 239

Delete the VM using the Cluster Installer Tool 239

Delete the VM using the vSphere UI 240

Uninstall Crosswork Data Gateway 240

Delete the Data Gateway VM from Cisco Crosswork 241

Delete Crosswork Data Gateway from the Crosswork Cluster 241

Uninstall Crosswork Applications 242

PART VIII	Enable Geo Redundancy	245
------------------	------------------------------	------------

CHAPTER 14	Geo Redundancy Overview	247
	Introduction	247

CHAPTER 15	Geo Redundancy Requirements	249
	Crosswork Cluster Requirements	249
	Crosswork Data Gateway Requirements	250
	Unified Endpoint Requirements	250
	Data Store Roles	250

CHAPTER 16	Enable Geo Redundancy Solution	253
	Geo Redundancy Workflow (Day 0)	253
	Connectivity Checks	255
	Enable Geo Redundancy	256
	Sample Cross Cluster Inventory Template	259
	View Cross Cluster Status	260
	Configure Cross Cluster Settings	262
	Configure Cross Cluster Notification Settings	265
	Geo Redundancy Scenarios	266
	Install Geo High Availability Crosswork Data Gateway	268
	Geo Redundancy Workflow (Day N)	268

CHAPTER 17	Geo Redundancy Switchover	271
	Perform Switchover	271
	Crosswork Optimization Engine License Count After a Switchover	275
	Geo Redundant Cluster Disaster Recovery	275
	Destruction of Standby Cluster	275
	Destruction of Active Cluster	275

CHAPTER 18	Upgrade to Geo Redundancy Solution	277
	Upgrade from Crosswork Network Controller 6.0 to 7.0 (Geo Redundant)	277
	Convert Single Instance NSO to NSO HA	279

Create Backup of the Cisco Crosswork Cluster	279
Install the Crosswork Network Controller Cluster and Applications	281
Run Migration	282
Install the Standby Cluster and Enable Geo Redundancy	283
Upgrade Crosswork Data Gateway 6.0 to 7.0 Geo Redundancy	284
Configure Controller IP for Crosswork Data Gateway	285
Update Providers	286
Complete Geo Redundancy Enablement	286

PART IX

Install Cisco Crosswork Network Controller on a Single VM	289
--	------------

CHAPTER 19

Install Cisco Crosswork Network Controller on a Single VM	291
Introduction	291
Installation Parameters	291
Installation Requirements	295
Install Crosswork Network Controller using the vCenter vSphere UI	300
Install Cisco Crosswork via the OVF Tool	306
Install Crosswork Network Controller using the Docker Installer Tool	309
Sample Manifest Template	312



PART I

Get Started

- [Overview, on page 1](#)
- [Plan Your Deployment, on page 5](#)
- [Choose Your Installation Workflow, on page 11](#)



CHAPTER 1

Overview

This chapter contains the following topics:

- [About this guide, on page 1](#)
- [Audience, on page 1](#)
- [Introduction, on page 2](#)
- [Security, on page 3](#)

About this guide

This guide explains the requirements and processes to install or upgrade Crosswork Network Controller solution.

This document does not cover the installation of integrated components (such as Cisco NSO or Cisco SR-PCE) that may already be installed or can be used independently. For more details about these components, please refer to their respective installation documentation.

Audience

This guide is for experienced network users and operators who want to install Crosswork Network Controller solution in their network. This guide assumes that you are familiar with the following:

- Using a Docker container
- Running scripts in Python
- Deploying an OVA file using VMware vCenter
- Deploying an OVA file using VMware OVF tool
- Amazon Web Services (AWS), Amazon EC2 concepts, and creation of CloudFormation templates

Introduction

Cisco Crosswork Network Controller

Cisco Crosswork Network Controller is a transport SDN controller that empowers customers to simplify and automate intent-based network service provisioning, health monitoring, and optimization in a multi-vendor network environment with a common GUI and API. Crosswork Network Controller simplifies operational workflows by consolidating both the service lifecycle and device management functions in a single integrated solution.

For more information on the Crosswork Network Controller solution components and packages, please refer to the [Crosswork Network Controller 7.0 Release Notes](#).

Cisco Crosswork Infrastructure

Cisco Crosswork Infrastructure is a resilient and scalable platform on which all Crosswork components can be deployed. The infrastructure is based on a cluster architecture to ensure extensibility, scalability, and high availability. It supports deployment in VMware and AWS EC2 environments. Cisco Crosswork can be deployed as a cluster with associated VMs (like NSO and WAE) and optionally a second cluster for geo redundancy, or as a single VM with limited device capacity.

A cluster deployment includes three hybrid VMs or nodes, with the option to add more worker nodes based on application needs (see [Determine How Many VMs You Need, on page 5](#) for more information). For optimal node configuration, consulting the Cisco Customer Experience team is recommended.

A single VM deployment operates supported functions on one machine, offering limited redundancy. In this setup, Crosswork Network Controller includes Cisco Crosswork Infrastructure, Embedded Collectors, and the Element Management Functions application integrated together to support the targeted use cases.

For more information on the various deployment options, please refer to [Plan Your Deployment, on page 5](#).



Note In this guide, Cisco Crosswork Infrastructure will be referred to as "Cisco Crosswork".

Crosswork Data Gateway

Cisco Crosswork integrates with data gateways to collect information from managed devices and forward it to Cisco Crosswork, with optional forwarding to external destinations. The applications analyze this information for various use cases, including topology visualization, service health monitoring, element management, and optimizing network performance. The utilization of forwarded data by third-party applications is beyond the scope of this guide.

Forwarding data to external destinations requires an additional license. For information on licensing requirements, see the *Licensing Requirements for External Collection Jobs* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#). For information on how to enable Crosswork to forward data to an external destinations, see the *Create and Manage External Data Destinations* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

The number of data gateways deployed in your network depends on factors such as the number of devices, the volume of data being collected, the overall topology, and your redundancy requirements. Each data gateway is deployed on an individual VM. For guidance on your deployment to best meet your needs, please consult with the Cisco Customer Experience team.

Crosswork Data Gateway is an integral part of the Crosswork solution being deployed, and it does not require a separate license. Therefore, this document explains the data gateway as a foundational component that must be installed in tandem with the Crosswork Infrastructure.

Cisco Integrated Components

Cisco Crosswork Network Service Orchestrator (NSO) functions as the provider for Cisco Crosswork to configure the devices according to their expected functions, including optionally configuring MDT sensor paths for data collection. NSO provides the important functions of device management, configuration and maintenance services.

Cisco Segment Routing Path Computation Element (SR-PCE) is configured to run on either a physical or virtual device that runs IOS-XR. The SR-PCE supports both Segment Routing Traffic Engineering (SR-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 paths for TE tunnels and/or to discover devices in the network.

Components that supports integration with Crosswork Network Controller

- TACACS+, LDAP, and RADIUS servers (see *Set Up User Authentication* in [Cisco Crosswork Network Controller 7.0 Administration Guide](#) for more information).
- DHCP server (when using Crosswork ZTP).
- External Kafka (for external data collection destinations).
- External gRPC (for external data collection destinations).
- Storage server that supports SCP for storage of backups.

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.



CHAPTER 2

Plan Your Deployment

This chapter contains the following topics:

- [Before You Begin, on page 5](#)

Before You Begin

This section explains the decisions you need to make before installing Crosswork Network Controller solution on your preferred platform.

1. [Determine How Many VMs You Need, on page 5](#)
2. [Identify the Resource Footprint, on page 7](#)
3. [Special Considerations, on page 9](#)

After completing the planning in the above steps, follow the relevant installation workflow steps for your platform:

- **For VMware vCenter:** [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- **For AWS EC2:** [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

Starting with the Crosswork Network Controller version 4.1, 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](#).

Determine How Many VMs You Need



Attention

This topic is applicable only when you need to deploy Crosswork Network Controller as a cluster. In case of single VM deployment, see [Install Cisco Crosswork Network Controller on a Single VM, on page 291](#)

After finalizing the Crosswork Network Controller package/tier that meets the needs of your production environment, use the table below to determine the number of VMs required to deploy the Crosswork cluster and the type of data gateways to be deployed.

This is a crucial step as each Crosswork Network Controller package can impact the overall resources needed.



Note Geo redundancy solution requires double the number of VMs. For more information, see [Enable Geo Redundancy, on page 245](#) section.

Crosswork Network Controller is available in the following packages:

Table 1: Crosswork Network Controller packages

Cisco Crosswork Network Controller package 1	Contents	Crosswork Data Gateway Deployment 2	Recommended number of cluster VMs 3
Essentials	Element Management Functions	On-Premise Standard (default): Collectors only.	3 Hybrid nodes
Advantage	Cisco Crosswork Optimization Engine	On-Premise Standard (default): Collectors only.	3 Hybrid nodes + 2 Worker nodes
	Cisco Crosswork Active Topology	On-Premise Standard (default): Collectors only.	
	Cisco Crosswork Service Health	On-Premise Extended: Collectors and offload services.	
Add-on	Cisco Crosswork Change Automation	On-Premise Extended: Collectors and offload services.	3 Hybrid nodes + 2 Worker nodes
	Cisco Crosswork Health Insights	On-Premise Extended: Collectors and offload services.	

¹ There are licensing implications for different packages, please consult your Cisco Account team to understand which packages and licenses are required for your use cases.

² The VM resource requirements for Crosswork Data Gateway are different for each type and cannot be modified. Therefore, if your requirements change, you must re-deploy the Crosswork Data Gateway to move from one type to another. For more information, see the *Redeploy a Crosswork Data Gateway VM* section in the [Crosswork Network Controller 7.0 Administration Guide](#).

³ The number of VMs mentioned is the recommended count. You can add more Worker nodes (maximum up to three worker nodes) as needed. If your requirements exceed the recommended count, please contact the Cisco Customer Experience team.

Ensure that you have sufficient worker nodes in your cluster. You can always check the load in your cluster and choose to add new worker nodes post installation. For more information, see the *Deploy New Cluster Nodes* section in the [Crosswork Network Controller 7.0 Administration Guide](#).

Identify the Resource Footprint

Once you determine the Crosswork applications you want and the number of VMs you will need to deploy to host them, ensure that you have the resources needed for them. The resources required per VM such as CPU, Memory, and Storage vary based on the data center where your VMs will be hosted (VMware or AWS).

The tables in this topic explain the resource requirements per VM to deploy Crosswork Hybrid or Worker nodes, Crosswork Data Gateways, NSO, and SR-PCE (refer to the table relevant to your platform).



Note

- The resources listed for NSO are higher than for other NSO use cases due to the additional requirements Crosswork Network Controller places on NSO.
 - The NSO footprint depends on the type of deployment, standalone or LSA.
 - The SR-PCE count will depend on the number of head-ends that need to be managed
 - The values in **Storage** column is the space needed for storing Crosswork files and does not consider any additional overhead that may be required (for example, RAID configuration).
 - The storage required for each backup will vary based on the your cluster size, applications in the cluster, and the scale requirements.
 - Upgrade of the cluster (using parallel hardware) temporarily requires double the total disk space used by the cluster. See [Upgrade Using Parallel Hardware, on page 227](#) for more information.
 - The number of data gateways needed depends on the number of devices you have in your network and the level of redundancy you want (1:n up to 1:1). To determine the number of Crosswork Data Gateways needed, contact the Cisco Customer Experience team.
-

Crosswork Resource Footprint for VMware



Note

- Ensure that you have a docker-capable host to load the Crosswork installer tool.
-



Important

As Cisco Crosswork cluster nodes place high demands on the VMs, ensure that you have not oversubscribed CPU or memory resources on the machines hosting the nodes.

Table 2: Crosswork Resource Footprint for VMware

Component	vCPU	Clock Freq (GHz)	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data disks)
Crosswork Hybrid or Worker node	12 Minimum clock reservation: 18 GHz	>= 2.20	96 GB	10 Gbps	1 TB
Crosswork Data Gateway On-Premise Standard	12	>= 2.20	48 GB	10 Gbps	70 GB (50 GB + 20 GB)
Crosswork Data Gateway On-Premise Extended	20	>= 2.20	112 GB	10 Gbps	570 GB (50 GB + 520 GB)
Cisco NSO	16	>= 2.20	128 GB	10 Gbps	1 TB
Cisco SR-PCE Note This is the requirement for running a Cisco XRv9K with SR-PCE functionality enabled.	8	>= 2.20	24 GB	10 Gbps	70 GB
Basic SCP Server (for storing backups)	-	-	-	-	At least 25 GB (recommended)

Crosswork Resource Footprint for AWS EC2

When deploying in AWS EC2, choose an EC2 instance size that meets or surpasses the resource requirements listed below:

Table 3: Crosswork Resource Footprint for AWS EC2

Component	vCPU	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data Disks)
Crosswork Hybrid or Worker node	12	96 GB	10 Gbps	1 TB
Crosswork Data Gateway On-Premise Standard	12	64 GB	10 Gbps	70 GB (50 GB + 20GB)
Crosswork Data Gateway On-Premise Extended	24	128 GB	10 Gbps	570 GB (50 GB + 520 GB)
Cisco NSO	16	128 GB	10 Gbps	1 TB

Component	vCPU	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data Disks)
Cisco SR-PCE Note This is the requirement for running a Cisco XRv9K with SR-PCE functionality enabled.	8	24 GB	10 Gbps	70 GB
Basic SCP Server (for storing backups)	-	-	-	At least 25 GB (recommended)

Additional Resource Requirements:

- 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 15, 000 RPM.
- The VM data store(s) need to have disk access latency < 10 ms or > 5000 IOPS.

Special Considerations

In addition to the above instructions, there may be certain setup options that you need to consider before you begin the installation.

- **Check versions of NSO and SR-PCE** – Please see the [Crosswork Network Controller 7.0 Release Notes](#) to know the NSO and SR-PCE versions compatible with Crosswork Network Controller.
- **Are you going to use self-signed certificates?** – if yes, you need to make the certificates available. For more information on the type of certificates supported and how to manage them, see the *Manage Certificates* section in the [Crosswork Network Controller 7.0 Administration Guide](#).
- **Do you plan to integrate Crosswork with external authentication servers?**– Integration with TACACS+ or other external authentication servers will require you to have credentials created for the Crosswork user accounts and roles.
- **In Crosswork Data Gateway, do you want to configure a Syslog server to collect the syslog?**– if yes, then provide the host name or IPv4 or IPv6 address of an external syslog server. Or, you have the option to configure the syslog server using the interactive console after the installation is complete.
- **In Crosswork Data Gateway, do you want to configure an Auditd server to collect the event logs?**– if yes, then provide the host name or IPv4 or IPv6 address of an external auditd server. As an alternative, you have the option to configure the auditd server using the interactive console after the installation is complete.
- **Do you plan to enable the automatic execution of linked playbooks?** – If yes, you must enable Playbook Job Scheduling and disable Credential Prompting for playbook execution in the Network Automation settings window. For more information, see the *Enable Automatic Playbook Execution* topic in the [Cisco Crosswork Network Controller 7.0 Closed-Loop Network Automation](#) guide.



CHAPTER 3

Choose Your Installation Workflow

This chapter contains the following topics:

- [Overview, on page 11](#)
- [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)
- [Install Cisco Crosswork Network Controller on a Single VM, on page 15](#)

Overview

This chapter outlines the installation workflows for each of the supported deployment options: VMware, AWS, and Single VM.

The workflows give a high-level description of the tasks necessary to install the Crosswork Network Controller and to integrate it with the required components of the solution. Integration with optional components is addressed in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

These workflow steps should be used as your primary installation guidepost and roadmap for the end to end installation of Crosswork Network Controller. After completing each detailed step, it is recommended that you refer to the workflow chart for the next step to perform.



Note The entire installation can typically take up to a few hours based on the size of your deployment profile and the performance characteristics of your hardware.

Please see the [Crosswork Network Controller 7.0 Release Notes](#) to know the NSO and SR-PCE versions compatible with Crosswork Network Controller.

Install Cisco Crosswork Network Controller on VMware vCenter

Before you begin:

- Ensure you have identified the Crosswork components you need and arranged for the resources required to complete the installation. If not, please refer to the guidelines in [Plan Your Deployment, on page 5](#).

The following table describes the stages to install Crosswork Network Controller on VMware vCenter.

Table 4: Crosswork Installation Workflow

Step	Action
Prepare for installation	
1. Ensure that your VMware environment meets all the requirements.	Refer to the guidelines in Installation Prerequisites for VMware vCenter , on page 19.
Install the Crosswork cluster	
2. Install the Cisco Crosswork cluster on VMware vCenter.	Install using your preferred method: <ul style="list-style-type: none"> • <i>Using cluster installer tool:</i> Install Cisco Crosswork on VMware vCenter using the Cluster Installer Tool, on page 47 • <i>Manual Installation:</i> Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 60
3. 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 Cluster Activation, on page 73 • Log into the Cisco Crosswork UI, on page 76
Install Crosswork Data Gateway	
4. Install one or more data gateway instances on VMware vCenter.	Choose the profile for the data gateway VM (Standard or Extended) and install as per your preferred method: <ul style="list-style-type: none"> • <i>Using vSphere:</i> Install Crosswork Data Gateway using vCenter vSphere Client, on page 105 • <i>Using OVF tool:</i> Install Crosswork Data Gateway via OVF Tool, on page 116 <p>Note If you plan to install multiple data gateway VMs due to load or scale requirements, or you wish to leverage Data Gateway High Availability, you are recommended to install all the data gateway VMs first and then proceed with adding them to a data gateway pool.</p>
5. Verify that the data gateway VM or multiple VMs have enrolled successfully with Crosswork Network Controller.	Follow the steps in Crosswork Data Gateway Authentication and Enrollment , on page 126. After verifying that the data gateway VM has enrolled successfully with Cisco Crosswork, set up the data gateway for collection by creating a data gateway pool. See the <i>Create a Crosswork Data Gateway Pool</i> section in Cisco Crosswork Network Controller 7.0 Administration Guide .
6. Complete the data gateway post-installation tasks.	Follow the steps in Crosswork Data Gateway Post-installation Tasks , on page 127.

Step	Action
Install the Cisco Crosswork Applications	
7. Install the Crosswork Applications	Follow the instructions in Install Crosswork Applications, on page 183 .
Integrate NSO with Crosswork	
8. Do you have Cisco NSO already installed?	<p>If yes, proceed to step 9.</p> <p>If no, please follow the system install instructions in the NSO Installation Guide.</p> <p>Note The NSO requirements for Crosswork integration exceed those specified in the NSO installation document.</p>
9. Add NSO Provider and verify that it is reachable	Follow the instructions in Add Cisco NSO Providers, on page 190 .
10. Install the latest NSO Function Packs	Follow the instructions in Install Cisco NSO Function Pack Bundles from Crosswork UI, on page 193 .
Integrate SR-PCE with Crosswork	
11. Is your SR-PCE installed?	<p>If yes, please proceed to step 12.</p> <p>If no, please choose the type of SR-PCE you wish to use (physical or virtual device) and follow the appropriate instructions to get the device (or virtual device) deployed. For more information, see the Cisco IOS XRv 9000 Router Installation Guide for the XR device you are going to use as your PCE.</p> <p>Note For the rest of the document, we will refer to the physical or virtual device(s) as the SR-PCE(s).</p>
12. Configure SR-PCE	Follow the instructions in Configure SR-PCE, on page 203 .
13. Add SR-PCE Provider and verify that it is reachable.	Follow the instructions in Add Cisco SR-PCE Providers, on page 206 .
14. (Recommended) Create a backup of your Crosswork Network Controller.	Follow the instructions in <i>Manage Backups</i> chapter in Cisco Crosswork Network Controller 7.0 Administration Guide .

After completing the installation, please refer to the [Cisco Crosswork Network Controller 7.0 Administration Guide](#) to carry out the post-installation operations.

Install Cisco Crosswork Network Controller on AWS EC2

Before you begin:

- Ensure you have identified the Crosswork components you need and arranged for the resources required to complete the installation. If not, please refer to the guidelines in [Plan Your Deployment, on page 5](#).

Crosswork Network Controller enables you to selectively install components of the Cisco Crosswork solution, including hybrid and worker nodes for the Crosswork cluster, one or more data gateways, and NSO, based on your deployment needs.

The following table describes the stages to install Crosswork Network Controller on AWS EC2 using CloudFormation (CF) templates.

Table 5: Crosswork Installation Workflow

Step	Action
Prepare for installation	
1. Ensure that your AWS EC2 environment meets all the requirements.	Refer to the guidelines in Installation Prerequisites for AWS EC2, on page 137 Installation Prerequisites for AWS EC2, on page 137 .
2. Extract the CF template package	Follow the instructions in Extract CF Template Image, on page 149 .
Install Crosswork components	
3. Module deployment: Install the Cisco Crosswork components using module deployment.	Install the Crosswork components individually: <ul style="list-style-type: none"> • Install the Crosswork cluster: Install Cisco Crosswork Cluster on Amazon EC2, on page 164 • Install one or more data gateway(s): Install Crosswork Data Gateway on Amazon EC2, on page 165 Crosswork Data Gateway is deployed with the default parameter values if you missed configuring the values during deployment. For more information, see Auto-Configuration for Deploying Crosswork Data Gateway, on page 167. • Install Cisco NSO: Install Cisco NSO on Amazon EC2, on page 170
4. Verify the installation and access Crosswork UI	Refer to the guidelines in Accessing the Crosswork UI, on page 173
Install the Crosswork Applications	
5. Install the Crosswork Applications	Follow the instructions in Install Crosswork Applications, on page 183 .
Integrate NSO with Crosswork	
6. Install the NSO Function Packs	Follow the instructions in Install Cisco NSO Function Pack Bundles from Crosswork UI, on page 193 .
7. Add NSO Provider and verify that is reachable.	Follow the instructions in Add Cisco NSO Providers, on page 190 .
Integrate SR-PCE with Crosswork	

Step	Action
8. Is your SR-PCE installed?	If yes, please proceed to step 9. If no, please select the SR-PCE type (for AWS) and follow the relevant install instructions in the Cisco IOS XRv 9000 Router Installation Guide .
9. Configure SR-PCE	Follow the instructions in Configure SR-PCE, on page 203 .
10. Add SR-PCE Provider and verify that SR-PCE is reachable.	Follow the instructions in Add Cisco SR-PCE Providers, on page 206 .
11. (Recommended) Create a backup of your Crosswork Network Controller.	Follow the instructions in <i>Manage Backups</i> chapter in the Cisco Crosswork Network Controller 7.0 Administration Guide .

After completing the installation, please refer to the [Cisco Crosswork Network Controller 7.0 Administration Guide](#) to carry out the post-installation operations.

Install Cisco Crosswork Network Controller on a Single VM

This topic explains the stages to install Crosswork Network Controller on a single VM or node. For the single VM deployment, Crosswork Network Controller consists of the Cisco Crosswork Infrastructure, Embedded Collectors, and the Element Management Functions application bundled together in a package.

Table 6: Crosswork Installation Workflow

Step	Action
Prepare for installation	
1. Ensure that your VMware environment meets all the requirements for single VM deployment.	Refer to the guidelines in Installation Requirements, on page 295 .
Install Crosswork	
2. Install the Crosswork Network Controller on VMware vCenter.	Install using your preferred method: <ul style="list-style-type: none"> • <i>Manual Installation:</i> Install Crosswork Network Controller using the vCenter vSphere UI, on page 300 • <i>Using the OVF tool:</i> Install Cisco Crosswork via the OVF Tool, on page 306 • <i>Using cluster installer tool:</i> Install Crosswork Network Controller using the Docker Installer Tool, on page 309
3. (Recommended) Create a backup of your Crosswork Network Controller.	Follow the instructions in <i>Manage Backups</i> chapter in Cisco Crosswork Network Controller 7.0 Administration Guide .

After completing the installation, please refer to the [Cisco Crosswork Network Controller 7.0 Administration Guide](#) to carry out the post-installation operations.



PART II

Install Cisco Crosswork Network Controller on VMware vCenter

- [Installation Prerequisites for VMware vCenter, on page 19](#)
- [Install Crosswork Cluster on VMware vCenter, on page 37](#)
- [Install Crosswork Data Gateway on VMware vCenter, on page 91](#)



CHAPTER 4

Installation Prerequisites for VMware vCenter

This chapter contains the following topics:

- [Overview, on page 19](#)
- [Supported Network Topology Models, on page 19](#)
- [VMware Settings, on page 24](#)
- [Host VM Requirements, on page 25](#)
- [Crosswork TCP/UDP Port requirements, on page 29](#)
- [IP Address Restrictions, on page 34](#)

Overview

This chapter explains the general (such as VM requirements, port requirements, application requirements, etc.) and platform-specific prerequisites to install each Crosswork component.

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

Supported Network Topology Models

This section introduces the different topology models supported when deploying Cisco Crosswork and the other solution components on a data center using VMware.

Routed and Device Networks

The following table describes the types of traffic that comes from the Crosswork Network Controller. This traffic can use dual NICs.

Table 7: Types of Crosswork Network Traffic

Traffic	Description
Management	For accessing the UI and Crosswork Network Controller command line, and passing information between servers (for example, Cisco Crosswork to Crosswork Data Gateway or NSO).

Traffic	Description
Data	Data and configuration transfer between Cisco Crosswork and Crosswork Data Gateway and other data destinations (external Kafka/gRPC).
Device Access	The device access that the servers (Crosswork, NSO, Crosswork Data Gateway, or others) use to communicate with the managed devices in the network.

Connectivity between the various components should be accomplished via an external routing entity. The Network Topology figures in this section 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 Crosswork Data Gateway, and other data destinations (external Kafka or gRPC)).
- Dashes - Device access routing domain (from Crosswork Data Gateway and NSO).
- Blue dotted/dashed line - 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.



Important

- It is vital to have secure firewalls between Crosswork Network Controller and the network devices. However, the firewalls are not provided by Crosswork Network Controller and must be set up separately by the user. This topic highlights what application flows need to be allowed through the user-provided firewall system.
- 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.

Crosswork Cluster Configurations

The supported configurations are:

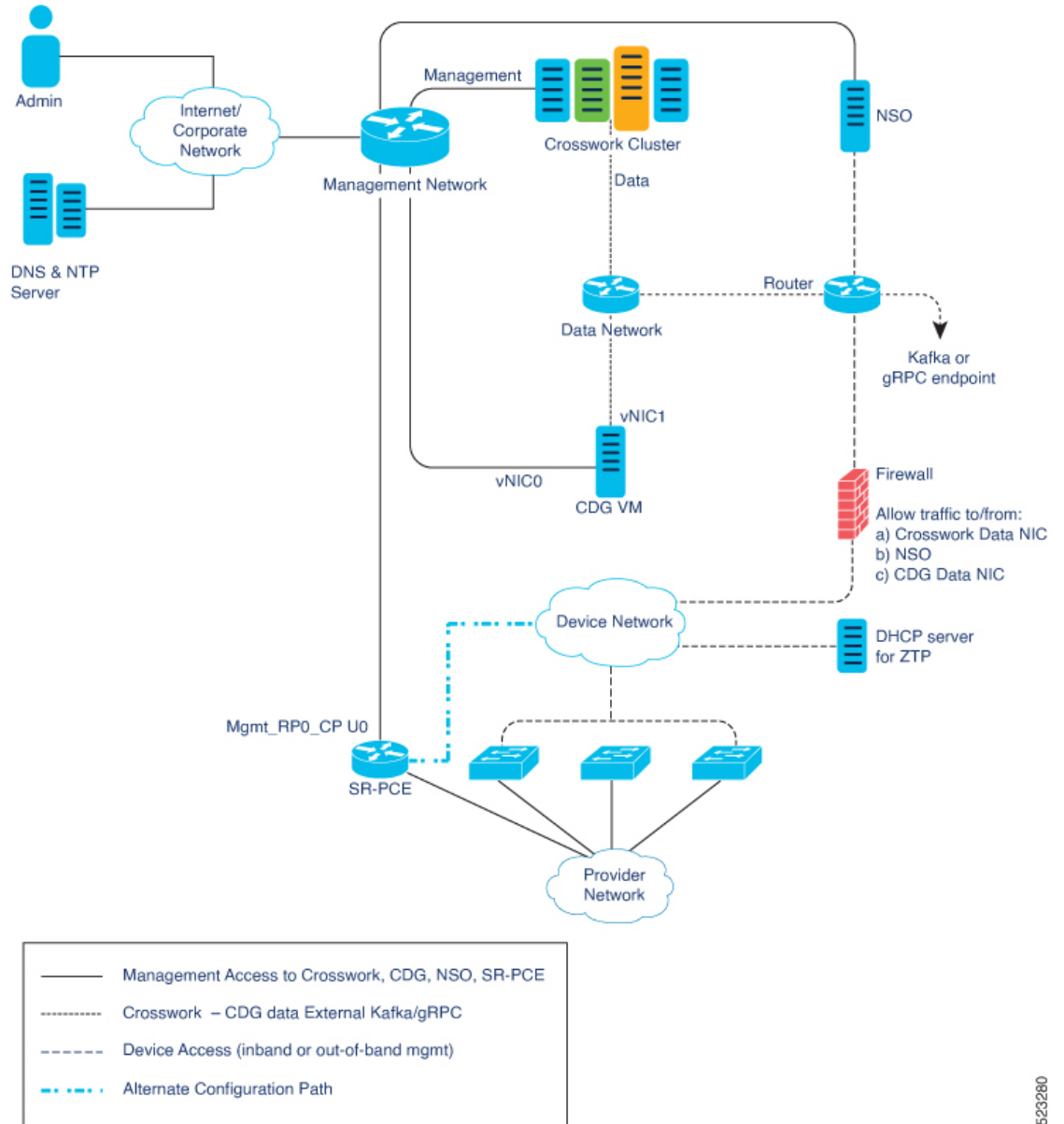
The supported configurations are:

- **2 NIC Network Topology:** The Crosswork cluster, Crosswork Data Gateway, NSO, and SR-PCE use one network interface to communicate between their management interfaces, a second interface to pass the data between Crosswork Network Controller and Crosswork Data Gateway, and a routed interface to communicate with the network devices.
- **3 NIC Network Topology:** The Crosswork Data Gateway, NSO, and SR-PCE use one network interface to communicate between their management interfaces, a second interface to pass the data between Crosswork Network Controller and Crosswork Data Gateway, and a third interface for Crosswork Data Gateway to communicate with the network devices.



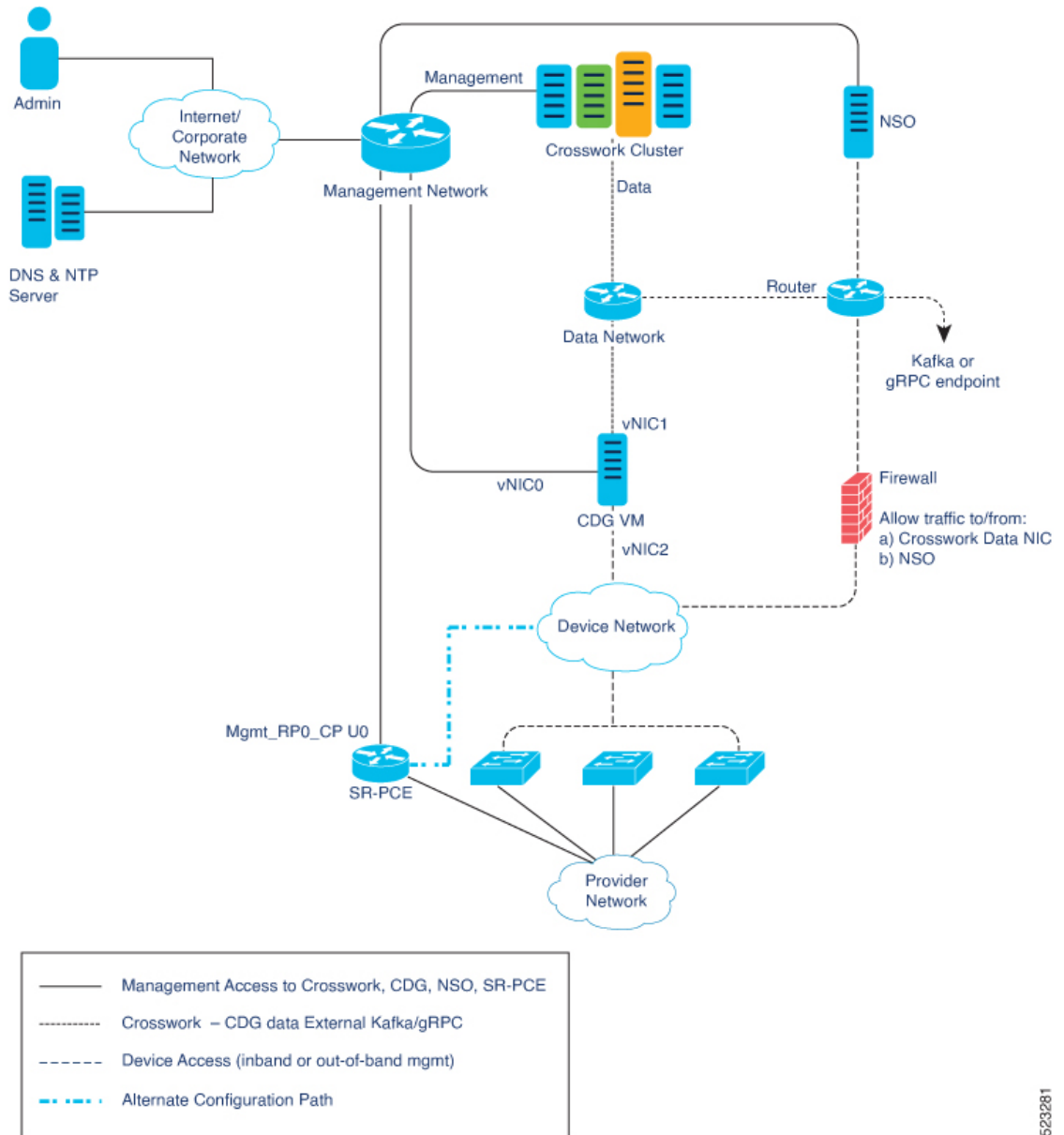
Note For simplicity, all these diagrams depict NSO using a management interface and a device-facing interface. Other configurations are also possible.

Figure 1: Cisco Crosswork - 2 NIC Network Topology



523280

Figure 2: Cisco Crosswork - 3 NIC Network Topology



523281

Cisco Crosswork Virtual Machine (VM)

The Cisco Crosswork VM has the following vNIC deployment options:

Table 8: Cisco Crosswork vNIC deployment modes

No. of vNICs	vNIC	Description
2	Management	Management
	Data	Data and Device access

Crosswork Data Gateway VM

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



Note 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.

Preference for the number of vNICs can vary from one deployment to another. The number of vNICs can depend on the security and traffic isolation needs of the deployment.

Table 9: Crosswork Data Gateway default vNIC deployment modes

No. of vNICs	vNIC	Roles
2	vNIC0	Default Gateway, Administration, External Logging, and Management traffic.
	vNIC1	Control, Northbound External Data, and Southbound Data traffic.
3	vNIC0	Default Gateway, Administration, External Logging, and Management traffic.
	vNIC1	Control and Northbound External Data traffic.
	vNIC2	Southbound Data traffic

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 [Add Cisco SR-PCE Providers, on page 206](#).

ZTP Requirements

If you plan to use Zero Touch Provisioning, the device network needs to be equipped with a DHCP server (not provided as part of Cisco Crosswork). Some forms of ZTP also require a TFTP server (not provided as part of Cisco Crosswork). Additionally, all devices that use ZTP must 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 Network Controller 7.0 Device Lifecycle Management*.

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).

VMware Settings

The following requirements are mandatory if you are planning to install Crosswork Network Controller using the cluster installer tool. If your vCenter data center does not meet these requirements, the VMs have to be deployed individually. For more information on manual installation, see [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 60](#).

- Hypervisor and vCenter supported:
 - VMware vCenter Server 8.0 (U2c or later) and ESXi 8.0 (U2b or later)
 - VMware vCenter Server 7.0 (U3p or later) and ESXi 7.0 (U3p or later)
- Crosswork Network Controller supports only VMFS and NFS datastore types.
- If you plan to use the docker installer tool, 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 60](#).
- Crosswork Network Controller cluster VMs (Hybrid nodes and Worker nodes) must be hosted on hardware with Hyper Threading disabled.
- As Crosswork Network Controller cluster nodes place high demands on the VMs, ensure that you have not oversubscribed 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. This prevents the host from being a single point of failure and improves solution resilience.
- Ensure that profile-driven storage is enabled by the vCenter admin user. Query permissions for the vCenter user at the root level (for all resources) of the vCenter.
- 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 (latency with RTT <= 10 ms).



Note The same network names must be used and configured on all the ESXi host machines hosting the Crosswork VMs.

- To allow use of VRRP (Virtual Router Redundancy Protocol), the DVS Port group needs to be set as follows:

Property	Value
Promiscuous mode	Reject
MAC address changes	Reject

- The VRRP protocol requires unique router_id advertisements to be present on the network segment. The IDs can vary based on the deployment. For example, Crosswork usually uses the ID 169 on the management and ID 170 on the data network segments when multicast is used in discovery. If there is a symptom of conflict such as the VIP address not being reachable, check if any of the router IDs is duplicated and remove the conflicting VRRP router machines or use a different network.
- 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 a new disk on the data center or VM folder.
 - Resource: Assign a VM to a resource pool on the destination host, cluster, or resource pool.
 - Datastore: Allocate space on the destination datastore or datastore folder.
 - Network: Assign the 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.

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 25](#)
- [Crosswork Data Gateway VM Requirements, on page 27](#)

Crosswork Cluster VM Requirements

The Crosswork cluster consists of three VMs or nodes operating in a hybrid configuration. This is the minimum configuration necessary to support the applications in a standard network. Additional VMs or nodes in a worker configuration can be added during the installation or later to scale your deployment. For more information on VM count for each Crosswork Network Controller package, see [Table 1: Crosswork Network Controller packages, on page 6](#). Please consult with the Cisco Customer Experience team for guidance on your deployment to best meet your needs.

The table below explains the network requirements per VM host:

Table 10: 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 with a latency of less than 10 milliseconds.</p>
IP Addresses	<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 cluster with 3 hybrid VMs and 1 worker VM with a dual NIC, you need 10 IP addresses (5 for management network and 5 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 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.
NTP Server	<p>The IPv4 or IPv6 addresses or host names of the NTP server 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.</p> <p>Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.</p>
DNS Servers	<p>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.</p> <p>Ensure that the DNS servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.</p>
DNS Search Domain	<p>The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.</p>
Backup Server	<p>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.</p>

Requirement	Description
FQDN (Optional)	<p>The installation process supports using either a VIP (Virtual IP address) or a FQDN (Fully Qualified Domain Name) to access the cluster.</p> <p>If you choose to use the FQDN, you will need one for the Management and one for the Data network.</p> <p>Note Secure ZTP and Secure Syslog require the Crosswork cluster to be deployed with FQDN.</p>

Cisco Crosswork Infrastructure and applications are built to run as a distributed collection of containers managed by Kubernetes.

Crosswork Data Gateway VM Requirements

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

- [Selecting the Crosswork Data Gateway Deployment Type, on page 27](#)
- [Crosswork Data Gateway VM Requirements, on page 28](#)

Selecting the Crosswork Data Gateway Deployment Type

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

Table 11: Crosswork Data Gateway deployment types

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	On-Premise Extended

The VM resource requirements for Crosswork Data Gateway differ based on the deployment type and cannot be modified. If your resource needs change, you must redeploy the data gateway to transition from one type to another.

For information on redeployment, see the *Redeploy a Crosswork Data Gateway VM* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

Crosswork Data Gateway VM Requirements

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

Table 12: Crosswork Data Gateway Requirements for on-premise applications

Requirement	Description			
Data Center	VMware. See Installation Prerequisites for VMware vCenter , on page 19.			
Interfaces	Minimum: 2 Maximum: 3 Crosswork Data Gateway can be deployed with 2 or 3 interfaces as per the combinations below: Note If you use two interfaces on your Crosswork Cluster, then you can use two, or three interfaces on the data gateway as per your network requirements.			
	No. of NICs	vNIC0	vNIC1	vNIC2
	2	Management Traffic	<ul style="list-style-type: none"> Control/Data Traffic Device Access Traffic 	—
	3	Management Traffic	Control/Data Traffic	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 Crosswork Data Gateway and Crosswork applications and other external data destinations. Device access traffic: for device access and data collection. 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 default vNIC2. Crosswork Data Gateway drops device traffic received over vNIC0 and vNIC1.			

Requirement	Description
IP Addresses	<p>1 or 2 IPv4 or IPv6 addresses based on the number of interfaces you choose to use.</p> <p>An additional IP address to be used as the Virtual IP (VIP) address. For each active data gateway, a unique VIP is required.</p> <p>For more information, refer to the <i>Interfaces</i> section in the Table 26: Crosswork Data Gateway Deployment Parameters and Scenarios, on page 93.</p> <p>Note In a 3-NIC deployment, you need to provide an IP address for Management interface (vNIC0) and Control/Data interface (vNIC1) during installation. A virtual IP address for Device Access Traffic (vNIC2) is assigned when you create a data gateway to a pool as explained in the <i>Create a Crosswork Data Gateway Pool</i> section in Cisco Crosswork Network Controller 7.0 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 else the installation fails.</p> <p>Also, the ESXi hosts that run the Crosswork application and 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 fails 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.
FQDN	The FQDN addresses are configured for Amazon EC2 deployments.
Internet Control Message Protocol (ICMP)	The Crosswork uses ICMP in the communications with Crosswork Data Gateway. Ensure that the firewall between Crosswork and Crosswork Data Gateway passes this traffic.

Crosswork TCP/UDP Port requirements

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



Note All IP addresses (including Virtual IP addresses) between Crosswork Cluster, Crosswork applications, and Crosswork Data Gateway need to be reachable (to be pinged to/from) between each other.

Crosswork Cluster Port Requirements

The following TCP/UDP port numbers need to be allowed through any external firewall or access-list rules deployed by the data center administrator. Depending on the NIC deployment, these ports may be applicable to only one or both NICs.



Note Crosswork cluster ports allow bidirectional flow of information.

Table 13: External Ports used by Crosswork Cluster

Port	Protocol	Used for	Location (in 2 NIC deployment)
22	TCP	Remote SSH traffic	Management Network / vNIC0
179	TCP	Calico BGP (Kubernetes)	Management Network / vNIC0
500, 4500	UDP	IPSec	Management Network / vNIC0
2379/2380	TCP	Kubernetes etcd	Management Network / vNIC0
6443	TCP	kube-apiserver (Kubernetes)	Management Network / vNIC0
9100	TCP	Kubernetes metamonitoring	Management Network / vNIC0
10250	TCP	kubelet (Kubernetes)	Management Network / vNIC0
24007	TCP	GlusterFS	Management Network / vNIC0
30603	TCP	User interface (NGINX server listens for secure connections on port 443)	Management Network / vNIC0
30606	TCP	Docker Registry	Management Network / vNIC0
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.	Data Network / vNIC1
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.	Data Network / vNIC1
49152:49370	TCP	GlusterFS	Management Network / vNIC0

Table 14: Ports used by other Crosswork components

Port	Protocol	Used for	Location (in 2 NIC deployment)
30180, 30190	TCP	Used in geo HA deployments for database replication (PQ binary protocol), and are secured by SSL.	Management Network / eth0
30602	TCP	To monitor the installation (Crosswork Network Controller)	Management Network / vNIC0
30604	TCP	Used for Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server	Management Network / vNIC0
30607	TCP	Crosswork Data Gateway vitals collection	Data Network / vNIC1
30608	TCP	Crosswork Data Gateway gRPC channel with Data Gateway VMs	Data Network / vNIC1
30609	TCP	Used by the Expression Orchestrator (Crosswork Service Health)	Management Network / vNIC0
30610	TCP	Used by the Metric Scheduler (Crosswork Service Health)	Management Network / vNIC0
30611	TCP	Used by the Expression Tracker component (Crosswork Service Health)	Management Network / vNIC0
30617	TCP	Used for Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server	Management Network / vNIC0
30620	TCP	Used to receive plug-and-play HTTP traffic on the ZTP server	Management Network / vNIC0
30649	TCP	To set up and monitor data gateway collection status	Data Network / vNIC1
30650	TCP	The astack gRPC channel with astack-client running on the data gateway VMs	Data Network / vNIC1
30993, 30994, 30995	TCP	Crosswork Data Gateway sending the collected data to Crosswork Kafka destination	Data Network / vNIC1

Table 15: Destination Ports used by Crosswork Cluster

Port	Protocol	Used for	Location (in 2 NIC deployment)
7	TCP/UDP	Discover endpoints using ICMP	Management Network / vNIC0
22	TCP	Initiate SSH connections with managed devices	Management Network / vNIC0
53	TCP/UDP	Connect to DNS	Management Network / vNIC0
123	UDP	Network Time Protocol (NTP)	Management Network / vNIC0
830	TCP	Initiate NETCONF	Management Network / vNIC0

Port	Protocol	Used for	Location (in 2 NIC deployment)
2022	TCP	Used for communication between Crosswork and Cisco NSO (for NETCONF)	Management Network / vNIC0
8080	TCP	REST API to SR-PCE	Management Network / vNIC0
8888	TCP	Used for communication between Crosswork and Cisco NSO (for HTTPS)	Management Network / vNIC0
20243	TCP	Used by the DLM Function Pack for communication between DLM and Cisco NSO	Management Network / vNIC0
20244	TCP	Used to internally manage the DLM Function Pack listener during a Reload Packages scenario on Cisco NSO	Management Network / vNIC0

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 16: 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 17: Ports to be Opened for Device Access Traffic

Port	Protocol	Used for	Direction
161	UDP	SNMP Collector	Outbound

Port	Protocol	Used for	Direction
1062	UDP	SNMP Trap Collector This is the default value. You can change this value after installation from the Cisco Crosswork UI. See Configure Crosswork Data Gateway Global Parameters for more information.	Inbound
9010	TCP	MDT Collector	Inbound
22	TCP	CLI Collector	Outbound
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 4	TCP	gNMI Collector	Outbound

⁴ For default port information of a device, see the platform-specific documentation. Ensure that port number on the device is the same as that configured on **Device Management > Network Devices > Edit Device**

Table 18: 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 5	Site Specific	Kafka and gRPC Destination	Outbound

⁵ You cannot modify the port numbers of system-created destinations as they are created with predefined ports. To modify the user-defined destination ports, edit the port number from **Administration > Data Collector(s) Global Settings > Data destinations > Edit destination**.

IP Address Restrictions

Crosswork cluster uses specific IP ranges for internal communications by default, which cannot be used for other devices or purposes within your network. It is recommended to isolate your Crosswork cluster to ensure all communications remain internal and that there are no address space overlaps with external integration points (e.g., connections to devices, external servers, or the NSO server).

If these default IP ranges conflict with your network, collaborate with the Cisco Customer Experience team for assistance in modifying the settings before deployment.



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



Note The default values for the `K8sServiceNetwork` (10.96.0.0) and `K8sPodNetwork` (10.244.0.0) parameters can be changed.

Table 19: 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, 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

IP Type	Subnet	Remarks
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, 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

What to do next:

- For installation instructions on VMware, see [Install Crosswork Cluster on VMware vCenter, on page 37](#).
- For installation instructions on AWS EC2, see [Install Cisco Crosswork Network Controller on AWS EC2, on page 149](#).
- For installation instructions for Single VM deployment, see [Install Cisco Crosswork Network Controller on a Single VM, on page 291](#).



CHAPTER 5

Install Crosswork Cluster on VMware vCenter

This chapter contains the following topics:

- [Installation Overview, on page 37](#)
- [Installation Parameters, on page 37](#)
- [Install Cisco Crosswork on VMware vCenter using the Cluster Installer Tool, on page 47](#)
- [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 60](#)
- [Monitor Cluster Activation, on page 73](#)
- [Log into the Cisco Crosswork UI, on page 76](#)
- [Import Cluster Inventory, on page 78](#)
- [Troubleshoot the Cluster, on page 78](#)

Installation Overview

Crosswork Network Controller Crosswork Cluster can be installed using the following methods:

- **Cluster Installer Tool:** The cluster installer tool 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 template file which is edited to provide the deployment specific data.
- **Manual Installation (via the VMware UI):** This option is available for deployments that cannot use the installer tool.

The installer tool method is the preferred option as it is faster and easier to use.

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 [Installation Prerequisites for VMware vCenter, on page 19](#).

The settings recommended in the table represent the least complex configuration. If you encounter network conflicts or wish to implement more advanced security settings (e.g., self-signed certificates), please work with the Cisco Customer Experience team to ensure you are prepared to make the necessary changes for your cluster.

**Attention**

- Please use the latest template file that comes with the Crosswork installer tool.
- Secure ZTP and Secure Syslog require the Crosswork cluster to be deployed with FQDN.

**Note**

In case of dual stack deployment, you need to configure the following fields:

- ManagementIPv4Address, ManagementIPv4Netmask, ManagementIPv4Gateway, ManagementVIPv4
- ManagementIPv6Address, ManagementIPv6Netmask, ManagementIPv6Gateway, ManagementVIPv6
- DataIPv4Address, DataIPv4Netmask, DataIPv4Gateway, DataVIPv4
- DataIPv6Address, DataIPv6Netmask, DataIPv6Gateway, DataVIPv6
- DNSv4, DNSv6

Table 20: General parameters

Parameter Name	Description
ClusterName	Name of the cluster file.
ClusterIPStack	The IP stack protocol: IPv4, IPv6, or DUALSTACK.
ManagementIPv4Address ManagementIPv6Address	The Management IP address of the VM (IPv4 and/or IPv6).
ManagementIPv4Netmask ManagementIPv6Netmask	The Management IP subnet in dotted decimal format (IPv4 and/or IPv6).
ManagementIPv4Gateway ManagementIPv6Gateway	The Gateway IP on the Management Network (IPv4 and/or IPv6). The address must be reachable, otherwise the installation will fail.
ManagementVIPv4 ManagementVIPv6	The Management Virtual IP address (IPv4 and/or IPv6) for the cluster.
ManagementVIPName	Name of the Management Virtual IP for the cluster. This is an optional parameter 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.
DataIPv4Address DataIPv6Address	The Data IP address of the VM (IPv4 and/or IPv6).
DataIPv4Netmask DataIPv6Netmask	The Data IP subnet in dotted decimal format (IPv4 and/or IPv6).
DataIPv4Gateway DataIPv6Gateway	The Gateway IP on the Data Network (IPv4 and/or IPv6). The address must be reachable, otherwise the installation will fail.
DataVIPv4 DataVIPv6	The Data Virtual IP address (IPv4 and/or IPv6) for the cluster.

Parameter Name	Description
DataVIPName	Name of the Data Virtual IP for the cluster. This is an optional parameter 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.
DNSv4 DNSv6	The IP address of the DNS server (IPv4 and/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.
CWPassword	Password to log into Cisco Crosswork. Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and at least one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words. While they satisfy the criteria, such passwords are weak and will be rejected resulting in failure to setup the VM.
VMSize	VM size for the cluster. If left empty, the default value ("Large") is selected.
VMName	Name of the VM. A unique VM name is required for each node on the cluster (Hybrid or Worker).
NodeType	Indicates the type of VM. Choose either "Hybrid" or "Worker". Note The Crosswork cluster requires at least three VMs operating in a hybrid configuration.
IsSeed	Choose "True" if this is the first VM being built in a new cluster. Choose "False" for all other VMs, or when rebuilding a failed VM. 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. Set this to match the number of VMs (nodes) you are going to deploy. For more information on VM count, see Table 1: Crosswork Network Controller packages, on page 6 . This parameter is optional for installing using the cluster installer tool.
InitLeaderCount	Total number of Hybrid nodes in the cluster. The default value is 3. This parameter is optional for installing using the cluster installer tool.

Parameter Name	Description
BackupMinPercent	<p>Minimum percentage of the data disk space to be used for the size of the backup partition. The default value is 35 (valid range is from 1 to 80).</p> <p>Please use the default value unless recommended otherwise.</p> <p>Note The final backup partition size will be calculated dynamically. This parameter defines the minimum.</p>
ManagerDataFsSize	<p>Refers to the data disk size for Hybrid nodes (in Giga Bytes). This is an optional parameter and the default value is 485 (valid range is from 485 to 8000), if not explicitly specified.</p> <p>Please use the default value unless recommended otherwise.</p>
WorkerDataFsSize	<p>Refers to the data disk size for Worker nodes (in Gigabytes). This is an optional parameter and the default value is 485 (valid range is from 485 to 8000), if not explicitly specified.</p> <p>Please use the default value unless recommended otherwise.</p>
ThinProvisioned	Set to "false" for production deployments.
EnableHardReservations	<p>Determines the enforcement of VM CPU and Memory profile reservations (see Installation Prerequisites for VMware vCenter, on page 19 for more information). This is an optional parameter and the default value is <code>true</code>, if not explicitly specified.</p> <p>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.</p> <p>If set as <code>false</code> (only set for lab installations), the VM's resources are provided on best efforts. In this state, insufficient CPU cores can impact performance or cause installation failure.</p>
RamDiskSize	<p>Size of the Ram disk.</p> <p>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.</p>
OP_Status	<p>This optional parameter is used (uncommented) to import inventory post manual deployment of Crosswork cluster.</p> <p>The parameter refers to the state for this VM. To indicate a running status, the value must be 2 (<code>#OP_Status = 2</code>). For more information, see Import Cluster Inventory, on page 78.</p>

Parameter Name	Description
SchemaVersion	<p>The configuration Manifest schema version. This indicates the version of the installer to use with this template.</p> <p>Schema version should map to the version packaged with the sample template in the cluster installer tool on cisco.com. You should always build a new template from the default template provided with the release you are deploying, as template requirements may change from one release to the next.</p>
LogFsSize	<p>Log partition size (in Giga Bytes). Minimum value is 20 GB and Maximum value is 1000 GB. You are recommended to use the default value.</p>
Timezone	<p>Enter the timezone. Input is a standard IANA time zone (for example, "America/Chicago").</p> <p>If left blank, the default value (UTC) is selected.</p> <p>This is an optional parameter.</p> <p>Note The timestamp in Kafka log messages represents the NSO server time. To avoid any mismatch between the Crosswork server time and the NSO event time, ensure you update the NSO server time before changing the <code>Timezone</code> parameter in Crosswork.</p>
EnableSkipAutoInstallFeature	<p>Any pods marked as skip auto install will not be brought up until a dependent application/pod explicitly asks for it.</p> <p>If left blank, the default value ("False") is selected.</p>
EnforcePodReservations	<p>Enforces minimum resource reservations for the pod.</p> <p>If left blank, the default value ("True") is selected.</p>
K8sServiceNetwork	<p>The network address for the kubernetes service network. By default, the CIDR range is fixed to '10.96.0.0/16'. If you wish to change this default value, please work with the Cisco Customer Experience team.</p>
K8sPodNetwork	<p>The network address for the kubernetes pod network. By default, the CIDR range is fixed to '10.224.0.0/16'. If you wish to change this default value, please work with the Cisco Customer Experience team.</p>
DefaultApplicationResourceProfile	<p>Resource profile for application pods. If left blank, resource profile defaults to the deployment's VM profile (recommended option).</p>
DefaultInfraResourceProfile	<p>Resource profile for infra pods. If left blank, resource profile defaults to the deployment's VM profile (recommended option).</p>
IsRunDiagnosticsScriptForCheck	<p>Used to enable/disable execution of the diagnostic script. The values are "true" (default value) and "false".</p> <p>You are recommended to select the default value.</p>

Parameter Name	Description
IgnoreDiagnosticsCheckFailure	<p>Used to set the system response in case of a diagnostic check failure.</p> <p>If set to "true" (default value), the diagnostic check is ignored and installation will continue. If set to "false", the installation is terminated.</p> <p>You are recommended to select the default value.</p> <p>Note</p> <ul style="list-style-type: none"> The log files (<code>diagnostic_stdout.log</code> and <code>diagnostic_stderr.log</code>) can be found at <code>/var/log</code>. The result from each diagnostic execution is kept in a file at <code>/home/cw-admin/diagnosis_report.txt</code>. Use diagnostic all command to invoke the diagnostic manually on day N. Use diagnostic history command to view previous test report.

Table 21: 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	<p>The name of the Data Center resource to use.</p> <p>Example: DCname = "WW-DCN-Solutions"</p>
MgmtNetworkName	<p>The name of the vCenter network to attach to the VM's Management interface.</p> <p>This network must already exist in VMware or the installation will fail.</p>
DataNetworkName	<p>The name of the vCenter network to attach to the VM's Data interface.</p> <p>This network must already exist in VMware or the installation will fail.</p>
Host	<p>The ESXi host, or ONLY the vcenter cluster/resource group name where the VM is to be deployed.</p> <p>The primary option is to use the host IP or name (all the hosts should be under the data center). If the hosts are under a cluster in the data center, only provide the cluster name (all hosts within the cluster will be picked up).</p> <p>The subsequent option is to use a resource group. In this case, a full path should be provided.</p> <p>Example: Host = "Main infrastructure/Resources/00_trial"</p>

Parameter Name	Description
Datastore	The datastore name available to be used by this host or resource group. The primary option is to use host IP or name. The subsequent option is to use a resource group. Example: Datastore = "SDRS-DCNSOL-prodexsi/bru-netapp-01_FC_Prodesx_ds_15"
HSDatastore	The high speed datastore available for this host or resource group. When not using a highspeed data store, set to same value as Datastore.
DCfolder	The resource folder name on vCenter. To be used if you do not have root access as a VMware user, or when you need to create VMs in separate folders for maintenance purposes. You must provide the complete path as value for the DCfolder. Example: DCfolder = "/WW-DCN-Solutions/vm/00_trial" Please contact your VMware administrator for any queries regarding the complete folder path. Leave as empty if not used.
Cw_VM_Image	The name of Crosswork cluster VM image in vCenter. This value is set as an option when running the cluster installer tool and does not need to be set in the template file.
HostedCwVMs	The IDs of the VMs to be hosted by the ESXi host or resource.

After you have decided the installation parameters values for Crosswork Network Controller, choose the method you prefer and begin your deployment:

- [Install Cisco Crosswork on VMware vCenter using the Cluster Installer Tool, on page 47](#)
- [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 60](#)

Automate Application Installation Using Auto Action Functionality

The auto action functionality is an optional method that enables you to automate the installation and activation of applications as needed during the cluster installation using a day-0 installer. Designed to simplify the installation process, this option can be configured with the Docker installer, direct OVA installation, and the OVF tool.

To enable auto action, you must configure a definition file (JSON format) that lists the tar bundles to be imported and activated. The JSON file is submitted alongside the day-0 installer and overrides the default file bundled in the OVA during installation.



Note The auto action functionality is supported only for day-0 deployments of non-geo HA cluster builds. Please ensure that the file path specified in the auto action file (the location on your local machine where the files are downloaded) is accessible from the Crosswork cluster.

The auto action definition file customizes two CAPP actions:

- **Add to repository** (`add_to_repository_requests`): The auto action functionality supports HTTP, HTTPS, and SCP protocols with basic authentication (HTTP/HTTPS) to add the application file (CAPP file) to the repository.

Sample script demonstrating all supported options for adding to the repository:

```
{
  "auto_action": {
    "add_to_repository_requests": [
      {
        "file_location": {
          "uri_location": {
            "uri":
"https://example.com/path/to/cw-na-element-management-functions-7.0.0.tar.gz",
            "basic_auth": {
              "username": "user",
              "password": "xxxx"
            }
          }
        }
      },
      {
        "file_location": {
          "uri_location": {
            "uri": "https://example.com/path/to/cw-na-hi-7.0.0.tar.gz"
          }
        }
      },
      {
        "file_location": {
          "scp_location": {
            "remote_file": "/example/cw-na-hi-7.0.0.tar.gz",
            "ssh_config": {
              "remote_host": "x.x.x.x",
              "username": "root",
              "password": "xxxxxx",
              "port": 22
            }
          }
        }
      }
    ],
  }
}
```

- **Activate** (`install_activate_requests`): The CAPP files to be installed and activated are identified using the **version** and **id** parameters.

Example:

```
"auto_action": {
  "install_activate_requests": [
    {
      "package_identifier": {
        "_comment": "Part of advantage capp",
        "version": "7.0.0",
        "id": "capp-coe"
      }
    },
  ],
}
```

Using Docker Installer

While installing via the docker installer, if the JSON file is successfully validated, the installation will proceed. If there are syntax errors in the file, you will be prompted with an error message, and the installation will be halted. Once the errors are corrected, you can retry the installation.

Syntax to execute the auto action file:

```
./cw-installer.sh install -p -m /data/<template file name> -a <path to json def file> -o /data/<.ova file>
```

Example:

```
./cw-installer.sh install -m /data/deployment.tfvars -a https://example.com/path/to/crosswork_auto_action.json -o /data/signed-cw-na-platform-7.0.0-114-release-240831.ova
```

Using vCenter UI or OVF tool

While installing via the vCenter UI, the CDATA JSON content is validated in the backend. If there are syntax errors in the data, the auto action instructions are skipped and Crosswork Cluster is installed as per the regular installation workflow.

vCenter and the OVF tool do not support the direct upload of JSON format files due to issues with handling special characters. To resolve this, you must compress the JSON file and enclose it in CDATA format.

```
<![CDATA[{auto action json compressed content}]]>
```



Note The CDATA example below has line breaks for the purpose of readability. During production deployment, kindly execute the CDATA without any line breaks.

Example:

```
<![CDATA[{"auto_action":{"add_to_repository_requests":[{"file_location":{"uri_location":{"uri":"<file path>/<filename.tar.gz>"}]}], "install_activate_requests":[{"package_identifer":{"id":"capp-coe","version":"7.0.0"}}]}}]]>
```

Sample auto action definition file



Note Make sure to replace the placeholder values (e.g., //example.com/path/to/cw-na-cncessential-7.0.0-240831.tar.gz, username, password, id, and version) with actual values relevant to your environment.

```
{
  "auto_action": {
    "add_to_repository_requests": [
      {
        "file_location": {
          "uri_location": {
            "uri":
"https://example.com/path/to/cw-na-cncessential-7.0.0-240831.tar.gz"
          }
        }
      },
      {
        "file_location": {
```

```

        "uri_location": {
            "uri":
"https://example.com/path/to/cw-na-cncadvantage-7.0.0-240831.tar.gz"
        }
    },
    {
        "file_location": {
            "uri_location": {
                "uri":
"https://example.com/path/to/cw-na-cncaddon-7.0.0-240831.tar.gz"
            }
        }
    }
],
"install_activate_requests": [
    {
        "package_identifier": {
            "_comment": "Part of essentials capp",
            "version": "7.0.0",
            "id": "capp-common-ems-services"
        }
    },
    {
        "package_identifier": {
            "_comment": "Part of advantage capp",
            "version": "7.0.0",
            "id": "capp-cat"
        }
    },
    {
        "package_identifier": {
            "_comment": "Part of advantage capp",
            "version": "7.0.0",
            "id": "capp-coe"
        }
    },
    {
        "package_identifier": {
            "_comment": "Part of advantage capp",
            "version": "7.0.0",
            "id": "capp-aa"
        }
    },
    {
        "package_identifier": {
            "_comment": "Part of add on capp",
            "version": "7.0.0",
            "id": "capp-ca"
        }
    },
    {
        "package_identifier": {
            "_comment": "Part of add on capp",
            "version": "7.0.0",
            "id": "capp-hi"
        }
    }
]
}
}
}

```

Install Cisco Crosswork on VMware vCenter using the Cluster Installer Tool

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



Note The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware.

Before you begin

Pointers to know when using the cluster installer tool:

- Make sure that your environment meets all the vCenter requirements specified in [Installation Prerequisites for VMware vCenter, on page 19](#).
- If you intend to use a dual stack configuration for your deployment, make sure that the host machine running the Docker installer meets the following requirements:
 - It must have an IPv6 address from the same prefix as the Crosswork Management IPv6 network, or be able to route to that network. To verify this, try pinging the Gateway IP of the Management IPv6 network from the host. To utilize the host's IPv6 network, use the parameter `--network host` when running the Docker installer.
 - Confirm that the provided IPv6 network CIDR and gateway are valid and reachable.
- 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 the templates used for your install in a secure environment or edit them to remove the passwords after the install is complete.
- The `install.log`, `install_tf.log`, and `.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.
- The install script is safe to run multiple times. Upon error, input parameters can be corrected and rerun. Running the cluster installer tool multiple times may result in the deletion and re-creation of VMs.
- In case you are using the same cluster 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 tool 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 Tool, on page 239](#).
- 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.
- If you want to use the auto action functionality, the definition file (JSON format) must be specified while executing the OVA file. For more information, see [Automate Application Installation Using Auto Action Functionality, on page 43](#).

Known limitations:

These following scenarios are the caveats for installing the Crosswork cluster 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 or 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.
- vCenter UI provides a service where a user accessing via IPv4 can upload images to the IPv6 ESXi host. Cluster installer tool cannot use this service. Follow either of the following workarounds for IPv6 ESXi hosts:
 1. Install the OVA template image manually (for more information, see [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 60](#)).
 2. Run the cluster installer tool from an IPv6 enabled machine. To do this, configure the Docker daemon to map an IPv6 address into the docked container.



Note The cluster 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 data center, 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 **signed-cw-na-platform-installer-7.0.0-85-release700-240823.tar.gz** and **signed-cw-na-platform-7.0.0-85-release700-240823.ova** respectively.

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).

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

```
tar -xvf signed-cw-na-platform-installer-7.0.0-85-release700-240823.tar.gz
```

The contents of the installer bundle are unzipped to a new directory (e.g. `signed-cw-na-platform-installer-7.0.0-85-release700`). This new directory will contain the installer image (**cw-na-platform-installer-7.0.0-85-release700-240823.tar.gz**) and files necessary to validate the image.

Step 5 Change the directory to the directory created by opening the file and then 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 Use the following command to verify the signature of the installer image:

- Ensure you have python installed. If not, go to [python.org](https://www.python.org) and download the version of python that is appropriate for your work station.
- Use `python --version` to find out the version of python on your machine.
- Depending on the python version use one of these commands to validate the file.

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
```

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-7.0.0-85-release700-240823.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-7.0.0-85-release700-240823  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 image 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 or dual stack 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>
```

Step 10 Navigate to the directory with the VMware template.

```
cd /opt/installer/deployments/7.0.0/vcentre
```

Step 11 Copy the template file found under

`/opt/installer/deployments/7.0.0/vcentre/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 37](#) table for details on the required and optional fields and their proper settings. The [Sample manifest templates for VMware vCenter, on page 51](#) includes an example that you can reference for proper formatting. The example is more compact due to the removal of descriptive comments:

Step 13 From the `/opt/installer` directory, run the installer.

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

For example:

```
./cw-installer.sh install -p -m /data/deployment.tfvars -o /data/signed-cw-na-platform-7.0.0-85-release700-240823.ova -y
```

Important If you want to use the auto action functionality, the definition file (JSON format) must be specified while executing the OVA file in the following format:

```
./cw-installer.sh install -p -m /data/<template file name> -a <path to json def file> -o /data/<.ova file>
```

Step 14 Read, and then enter "yes" if you accept the End User License Agreement (EULA). Otherwise, exit the installer and contact your Cisco representative.

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 in the `/data` directory (and the local directory where you launched the installer docker container), 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

- See [Monitor Cluster Activation, on page 73](#) to know how you can check the status of the installation.
- See [Troubleshoot the Cluster, on page 78](#) for common troubleshooting scenarios.

Sample manifest templates for VMware vCenter

This topic contains manifest template examples for various scenarios of Crosswork cluster deployment.



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 VMs to host(s) in the resource pool.

Example 1: To deploy a cluster (3 hybrid nodes, 2 worker nodes) on 2 hosts

The following example deploy Crosswork cluster with Hosts specified:

```
#See at the end of the file for a configured sample

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

# The name of the Crosswork Cluster.
ClusterName      = "CW-Cluster-01"

# Provide name of Cw VM image in vcenter or leave empty
# When empty the image name will be populated from the uploaded image
Cw_VM_Image = "" # Line added automatically by installer.

# The IP stack protocol: IPv4 or IPv6 or DUALSTACK
ClusterIPStack   = "IPv4"

# The Management Virtual IP for the cluster
ManagementVIP    = "x.x.x.x"

# Optional: The Management Virtual IP host-name
ManagementVIPName = ""

# The Management IP subnet in dotted decimal format for ipv4 or prefix length for ipv6
ManagementIPNetmask = "x.x.x.x"

# The Gateway IP on the Management Network
ManagementIPGateway = "x.x.x.x"

# The Data Virtual IP for the cluster. Use 0.0.0.0 or ::0 to disable
DataVIP          = "x.x.x.x"

# Optional: The Data Virtual IP host-name
DataVIPName = ""

# The Data IP subnet in dotted decimal format for ipv4 or prefix length for ipv6
# Provided any regular mask when not in use
DataIPNetmask    = "x.x.x.x"

# The Gateway IP on the Management Network
DataIPGateway    = "x.x.x.x"

# The IP address of the DNS server
DNS              = "x.x.x.x"

# The domain name to use for the cluster
DomainName       = "cisco.com"

# Sets the cw-admin user ssh login password for all VMs in the cluster
# The password MUST be of min length 8 and strong
CWPassword       = "*****"

# Sets the VM size for the cluster.
# Options are: Small | Large.
VMSize           = "Large"

# NTP server address or name
NTP              = "x.x.x.x"

# Configuration Manifest schema version
SchemaVersion    = "7.0.0"

# Data disk size for Manager/Hybrid nodes in GB. Min 485 Max 8000
```

```

ManagerDataFsSize = 485
# Data disk size for Worker nodes in GB. Min 485 Max 8000
WorkerDataFsSize = 485

// Thin or thick provisioning for all disks. Set to true for thin provisioning, false for
thick
ThinProvisioned = true

# Log partition size in GB. Min 20 Max 1000
LogFsSize = 20

# Minimum percentage of the data disk space to be used for the size of the backup partition

# Note: The final backup partition size will be calculated dynamically. This parameter
defines the minimum.
# Valid range 1 - 80
BackupMinPercent = 35

# Enforces VM profile reservations as "hard"
EnableHardReservations = true

# FOR DEMO USE ONLY - NOT TO BE USED IN PRODUCTION DEPLOYMENTS
# Ram disk size in GB
RamDiskSize          = 10

/***** Crosswork VM Data Map *****/
# Configure named entries for each Cw VM.
# Number of Hybrid VMs minimum: 3; maximum: 3
# Number of Worker VMs minimum: 2; maximum: 3

CwVMs = {
  # Seed VMs' data.
  # IMPORTANT: A VM with id "0" MUST be present in the initial day0 install manifest and
  its role MUST be
  # set to either MASTER or HYBRID.
  "0" = {

    # This VM's name
    VMName          = "CW_Node_0",

    # This VMs' management IP address
    ManagementIPAddress = "x.x.x.x",

    # This VMs' data IP address. Use 0.0.0.0 or ::0 to disable
    DataIPAddress    = "x.x.x.x",

    # This Cw VM's type - use "Hybrid" for initial install
    NodeType         = "Hybrid",

    # The state for this VM; 2 = running. Only uncomment when doing a manual inventory
import
    #Op_Status = 2
  },

  # Second VMs' data
  "1" = {
    # This VM's name
    VMName          = "CW_Node_1",

    # This VMs' management IP address
    ManagementIPAddress = "x.x.x.x",

    # This VMs' data IP address

```

```

    DataIPAddress      = "x.x.x.x",

    # This Cw VM's type - use "Hybrid" for initial install
    NodeType           = "Hybrid",

    # The state for this VM; 2 = running. Only uncomment when doing a manual inventory
import
    #Op_Status = 2
  },

  # Third VMs' data
  "2" = {
    # This VM's name
    VMName           = "CW_Node_2",

    # This VMs' management IP address
    ManagementIPAddress = "x.x.x.x",

    # This VMs' data IP address
    DataIPAddress     = "x.x.x.x",

    # This Cw VM's type - use "Hybrid" for initial install
    NodeType           = "Hybrid",

    # The state for this VM; 2 = running. Only uncomment when doing a manual inventory
import
    #Op_Status = 2
  },

  # Worker VMs' data
  "3" = {
    # This VM's name
    VMName           = "CW_Node_3",

    # This VMs' management IP address
    ManagementIPAddress = "x.x.x.x",

    # This VMs' data IP address
    DataIPAddress     = "x.x.x.x",

    # This Cw VM's type - use "Worker"
    NodeType           = "Worker",

    # The state for this VM; 2 = running. Only uncomment when doing a manual inventory
import
    #Op_Status = 2
  },

  # Worker VMs' data
  "4" = {
    # This VM's name
    VMName           = "CW_Node_4",

    # This VMs' management IP address
    ManagementIPAddress = "x.x.x.x",

    # This VMs' data IP address
    DataIPAddress     = "x.x.x.x",

    # This Cw VM's type - use "Worker"
    NodeType           = "Worker",

    # The state for this VM; 2 = running. Only uncomment when doing a manual inventory
import
    #Op_Status = 2
  }

```

```

    },
  }

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

VCenterDC = {

  # The vcenter IP or host name
  VCenterAddress = "x.x.x.x",

  # The username to use for logging into vcenter
  VCenterUser = "Cisco_User",

  # The vcenter password for the user
  VCenterPassword = "Test123!",

  # The name of the Data Centre resource to use
  DCname = "Cisco-Crosswork",

  # The name of the vcenter network to attach to the Cw VM Management interface
  # NOTE: Escape any special characters using their URL escape codes, eg use "%2f" instead
  # of "/"
  MgmtNetworkName = "VM Network",

  # The name of the vcenter network to attach to the Cw VM Data interface.
  # Leave empty if not used.
  # NOTE: Escape any special characters using their URL escape codes, eg use "%2f" instead
  # of "/"
  DataNetworkName = "Crosswork-Internal",

  # The resource folder name on vcenter. Leave empty if not used.
  DCfolder = "",

  # List of the vcenter host resources along with the VMs names
  # that each that each resource will host. Add additional stanzas, separated by a ','
  # for each additional ESXi host or resource
  VMs = [{

    # The ESXi host, or ONLY the vcenter cluster/resource group name.
    Host = "x.x.x.x",

    # The datastore name available to be used by this host or resource group.
    Datastore = "Datastore-1",

    # The high speed datastore available for this host or resource group.
    # Set to same value as Datastore if unsure.
    HSDatastore = "Datastore-1"

    # The ids of the VMs to be hosted by the above ESXi host or resource. These have to
    # match to the Cw VM
    # ids specified in the Cw VM map. Separate multiple VMs the given
    # host with a ',', eg ["0","1"].
    HostedCwVMs = ["0","1","2"]

  },
  {
    Host = "x.x.x.x"
    Datastore = "Datastore-2"
    HSDatastore = "Datastore-2"
    HostedCwVMs =["3","4"]
  }
  ]
}

```

Example 2: To deploy a cluster (3 hybrid, 2 workers) in a Resource Group

The following example deploys Crosswork cluster with resource groups:

```

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

ClusterName      = "CW-cluster-01"
# When empty the image name will be populated from the uploaded image
Cw_VM_Image = "" # Line added automatically by installer.
ClusterIPStack   = "IPv4"
ManagementVIP    = "x.x.x.x"
ManagementVIPName = ""
ManagementIPNetmask = "x.x.x.x"
ManagementIPGateway = "x.x.x.x"
DataVIP          = "x.x.x.x"
DataVIPName     = ""
DataIPNetmask    = "x.x.x.x"
DataIPGateway    = "x.x.x.x"
DNS              = "x.x.x.x"
DomainName       = "cisco.com"

# Kubernetes Service Network Customization - The default network '10.96.0.0'.
# NOTE: The CIDR range is fixed '/16', no need to enter.
# Only IPv4 is supported, IPv6 customization is NOT supported.
K8sServiceNetwork = "10.96.0.0"

# Kubernetes Service Network Customization - The default network '10.244.0.0'.
# NOTE: The CIDR range is fixed '/16', no need to enter.
# Only IPv4 is supported, IPv6 customization is NOT supported.
K8sPodNetwork = "10.244.0.0"

CWPassword       = "Test1234!"
VMSize           = "Large"
NTP              = "x.x.x.x"
SchemaVersion    = "7.0.0"

# Data disk size for Manager/Hybrid nodes in GB. Min 485 Max 8000
ManagerDataFsSize = 485
# Data disk size for Worker nodes in GB. Min 485 Max 8000
WorkerDataFsSize = 485

// Thin or thick provisioning for all disks. Set to true for thin provisioning, false for thick
ThinProvisioned = true

# Log partition size in GB. Min 20 Max 1000
LogFsSize = 20

# Minimum percentage of the data disk space to be used for the size of the backup partition

# Note: The final backup partition size will be calculated dynamically. This parameter
defines the minimum.
# Valid range 1 - 80
BackupMinPercent = 35

# Enforces VM profile reservations as "hard"
EnableHardReservations = "false"

# FOR DEMO USE ONLY - NOT TO BE USED IN PRODUCTION DEPLOYMENTS
# Ram disk size in GB
RamDiskSize      = 0

```



```

# Pods that are marked as skip auto install will not be brought up until a dependent
application/pod explicitly asks for it
EnableSkipAutoInstallFeature = "False"

# DEMO/DEV USE ONLY - Enforce pod minimum resource reservations. Default and for production
use is True
EnforcePodReservations = "True"

# Optional: Provide a standard IANA time zone. Default value is Etc/UTC if not specified
Timezone = ""

/***** Crosswork VM Data Map *****/
# Configure named entries for each Cw VM.
# Number of Hybrid VMs minimum: 3; maximum: 3
# Number of Worker VMs minimum: 0; maximum: 3

CwVMs = {
  "0" = {
    VMName           = "cw-vm-0",
    ManagementIPAddress = "x.x.x.x",
    DataIPAddress     = "x.x.x.x",
    NodeType          = "Hybrid",
    #Op_Status = 2
  },
  "1" = {
    VMName           = "cw-vm-1",
    ManagementIPAddress = "x.x.x.x",
    DataIPAddress     = "x.x.x.x",
    NodeType          = "Hybrid",
    #Op_Status = 2
  },
  "2" = {
    VMName           = "cw-vm-2",
    ManagementIPAddress = "x.x.x.x",
    DataIPAddress     = "x.x.x.x",
    NodeType          = "Hybrid",
    #Op_Status = 2
  },
  "3" = {
    # This VM's name
    VMName           = "cw-worker-3",
    ManagementIPAddress = "x.x.x.x",
    DataIPAddress     = "x.x.x.x",
    NodeType          = "Worker",

    # The state for this VM; 2 = running. Only uncomment when doing a manual inventory
import
    #Op_Status = 2
  },
  "4" = {
    # This VM's name
    VMName           = "cw-worker-4",
    ManagementIPAddress = "x.x.x.x",
    DataIPAddress     = "x.x.x.x",
    NodeType          = "Worker",
    #Op_Status = 2
  }
}

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

```

```

VCenterDC = {
  VCenterAddress = "x.x.x.x",
  VCenterUser = "Cisco_User",
  VCenterPassword = "Test1234!",
  DCname = "Cisco-Crosswork",
  MgmtNetworkName = "Management Network",
  DataNetworkName = "Data Network",
  DCfolder = ""
  VMs = [{
    Host = "{path to resource Group}",

    Datastore = "iSCSI-DataStore",

    HSDatastore = "iSCSI-DataStore",

    HostedCwVMs = ["0", "1", "2", "3", "4"],

  }
]
}

```

Example 3: To deploy a cluster (3 hybrid nodes, 2 worker nodes) on dual stack configuration

The following example deploys a Crosswork cluster containing 3 Hybrid nodes (IDs 0,1, 2) and 2 worker nodes (IDs 3, 4) on a dual stack configuration.

```

#***** Crosswork Cluster Data *****#
Cw_VM_Image = ""
ClusterIPStack = "DUALSTACK"
ManagementVIPv4 = "x.x.x.x"
ManagementVIPv6 = "fded:1bc1:fc3e:96d0:192:168:5:450"
ManagementIPv4Netmask = "x.x.x.x"
ManagementIPv4Gateway = "x.x.x.x"
ManagementIPv6Netmask = "112"
ManagementIPv6Gateway = "fded:1bc1:fc3e:96d0:192:168:5:1"
DataVIPv6 = "fded:1bc1:fc3e:96d0:10:10:10:450"
DataVIPv4 = "x.x.x.x"
DataIPv6Netmask = "112"
DataIPv6Gateway = "fded:1bc1:fc3e:96d0:10:10:10:1"
DataIPv4Netmask = "x.x.x.x"
DataIPv4Gateway = "x.x.x.x"
DNSv6 = "fded:1bc1:fc3e:96d0:192:168:5:481"
DNSv4 = "x.x.x.x"
DomainName = "cisco.com"
CWPassword = "EFTPass123!"
VMSize = "Large"
NTP = "fded:1bc1:fc3e:96d0:192:168:5:481"
ThinProvisioned = false
EnableHardReservations = true
ManagementVIPName = "lhsmanagement"
DataVIPName = "lhsdata"

//#***** Crosswork VM Data Map *****#
CwVMs = {
  "0" = {
    VMName = "HYBRID-VM1",
    ManagementIPv4Address = "x.x.x.x",
    DataIPv4Address = "x.x.x.x",
    ManagementIPv6Address = "fded:1bc1:fc3e:96d0:192:168:5:451",
    DataIPv6Address = "fded:1bc1:fc3e:96d0:10:10:10:451",
    NodeType = "Hybrid"
  },
  "1" = {
    VMName = "HYBRID-VM2",

```

```

ManagementIPv4Address = "x.x.x.x",
DataIPv4Address = "x.x.x.x",
ManagementIPv6Address = "fded:1bc1:fc3e:96d0:192:168:5:452",
DataIPv6Address = "fded:1bc1:fc3e:96d0:10:10:10:452",
NodeType = "Hybrid"
},
"2" = {
VMName = "HYBRID-VM3",
ManagementIPv4Address = "x.x.x.x",
DataIPv4Address = "x.x.x.x",
ManagementIPv6Address = "fded:1bc1:fc3e:96d0:192:168:5:453",
DataIPv6Address = "fded:1bc1:fc3e:96d0:10:10:10:453",
NodeType = "Hybrid"
},
"3" = {
VMName = "WORKER-VM1",
ManagementIPv4Address = "x.x.x.x",
DataIPv4Address = "x.x.x.x",
ManagementIPv6Address = "fded:1bc1:fc3e:96d0:192:168:5:454",
DataIPv6Address = "fded:1bc1:fc3e:96d0:10:10:10:454",
NodeType = "Worker"
},
"4" = {
VMName = "WORKER-VM2",
ManagementIPv4Address = "x.x.x.x",
DataIPv4Address = "x.x.x.x",
ManagementIPv6Address = "fded:1bc1:fc3e:96d0:192:168:5:455",
DataIPv6Address = "fded:1bc1:fc3e:96d0:10:10:10:455",
NodeType = "Worker"
},
}
#***** vcenter Resource Data with Cw VM assignment *****
VCenterDC = {
VCenterAddress = "x.x.x.x",
VCenterUser = "Cisco_User",
VCenterPassword = "Test1234!",
DCName = "Cisco-Crosswork",
MgmtNetworkName = "port-100"
DataNetworkName = "port-103"
VMs = [
{
HostedCwVMs = ["0"]
Host = "x.x.x.x"
Datastore = "ds-ssd"
HSDatastore = "ds-ssd"
},
{
HostedCwVMs = ["1"]
Host = "x.x.x.x"
Datastore = "ds-ssd"
HSDatastore = "ds-ssd"
},
{
HostedCwVMs = ["2"]
Host = "x.x.x.x"
Datastore = "ds-ssd"
HSDatastore = "ds-ssd"
},
{
HostedCwVMs = ["3"]
Host = "x.x.x.x"
Datastore = "ds-ssd"
HSDatastore = "ds-ssd"
},
]
}

```

```
{
  HostedCwVMs = ["4"]
  Host = "x.x.x.x"
  Datastore = "ds-ssd"
  HSDatastore = "ds-ssd"
},
] }
```

Manual Installation of Cisco Crosswork using vCenter vSphere UI

This section explains how to build the cluster using the vCenter user interface. This same procedure can be used to add or replace nodes if necessary.

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

1. [Build the OVF template, on page 60](#)
2. [Deploy the template, on page 70](#)



Note If the cluster has already been installed (no matter the method used) the template file will already exist unless it was deleted. In this case, you can directly go to deploying the template (the second part of this procedure).

The manual installation is preferred if you face any of the following reasons:

- Owing to your data center configuration, you cannot deploy the cluster using the installer tool.
- You need to add nodes to the existing cluster.
- You need to replace a failed node.
- You want to migrate a node to a new host machine.



Important Anytime the configuration of the cluster is changed manually—whether to install the Crosswork cluster, add nodes, or move nodes to new hosts using the procedures detailed in this section—you must import the cluster inventory file (.tfvars file) to the Crosswork UI. You must set the parameter `OP_Status = 2` to enable manual import of the inventory. For more information, see [Import Cluster Inventory, on page 78](#).

Build the OVF template

Before you begin

- Make sure that your environment meets all the vCenter requirements specified under [Crosswork Cluster VM Requirements, on page 25](#) and [Installation Prerequisites for VMware vCenter, on page 19](#).

-
- Step 1** Download the latest available Cisco Crosswork platform 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 or cluster where 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.
- Ensure that the networks that you plan to use for Management network and Data network are connected to each host where VMs will be deployed.
- Step 5** Choose **Actions > Deploy OVF Template**.
- Caution** The default VMware vCenter deployment timeout is 15 minutes. If vCenter times out during deployment, the resulting VM will not be bootable. To prevent this, we recommend that you document the choices (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 data center 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 7.0 Build 152.
- Step 8** Click **Next**. The **Deploy OVF Template** window is refreshed, with **3 - Select a compute resource** highlighted. Select the host or cluster 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 if you agree, click the **I accept all license agreements** checkbox. Otherwise, contact your Cisco Experience team for assistance.
- Step 12** Click **Next**. The **Deploy OVF Template** window is refreshed, with **6 - Configuration** highlighted. Crosswork supports only the following deployment configurations: **IPv4 Network**, **IPv6 Network**, and **Dual Stack Network**. Please select your preferred deployment configuration.

Figure 3: 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

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

7 Items

CANCEL
BACK
NEXT

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.

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.

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

Figure 4: Select Storage

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration
- Select storage**
- Select networks
- Customize template
- 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 Eager Zeroed

VM Storage Policy: Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Cluster
<input type="radio"/>	datastore-005	--	2.17 TB	25.61 GB	2.15 TB	VMFS 5	
<input type="radio"/>	datastore-005-hdd-1	--	2.18 TB	983 MB	2.18 TB	VMFS 5	
<input type="radio"/>	datastore-005-hdd...	--	1.64 TB	1.43 GB	1.63 TB	VMFS 6	
<input checked="" type="radio"/>	datastore-005-ssd-1	--	1.09 TB	1.42 GB	1.09 TB	VMFS 6	
<input type="radio"/>	datastore-005-ssd-2	--	371.5 GB	99.79 GB	370.09 GB	VMFS 6	

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Step 14

Click **Next**. The **Deploy OVF Template** window is refreshed, with **8 - Select networks** highlighted. From the **Destination Network** drop-down list, select the proper networks for the Management Network and the Data Network.

Figure 5: Select a deployment configuration

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration
- Select storage
- Select networks**
- Customize template
- Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Management Network	MGMT-VLAN-21
Data Network	MGMT-VLAN-21
Admin Network	MGMT-VLAN-21
NBI Network	MGMT-VLAN-21

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Important Admin Network and NBI Network are not applicable for Crosswork Network Controller deployments. You should leave these fields with the default values.

Step 15

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

Note As you are creating a template now, enter the IP information for the first node.

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

Figure 6: 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	9
10 Ready to complete	10

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

CANCEL BACK NEXT

- 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 at least one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words. While they satisfy the criteria, such passwords are weak and will be rejected resulting in failure to setup the VM.

- d) Expand the **DNS and NTP Servers** settings. According to your deployment configuration (IPv4, IPv6 or dual stack), 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.
 - **Timezone:** Enter the timezone details. Default value is UTC.

Figure 7: Customize template - DNS and NTP Servers

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Configuration
- Select storage
- Select networks
- 9 Customize template**
- Ready to complete

Customize template

Customize the deployment properties of this software solution.

1 property has an invalid value

> Management Network	3 settings
> Data Network	3 settings
> Deployment Credentials	2 settings
▼ DNS and NTP Servers	4 settings
DNS IPv4 Address	Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated. 171.70.168.183 173.37.87.1
NTP Servers	Please enter NTP server hostname. Multiple NTP servers can be provided space separated. ntp.esl.cisco.com
DNS Search Domain	Please enter the DNS search domain. cisco.com
Timezone	Please enter the timezone. Input is a standard IANA time zone. Default value is UTC PST8PDT

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.

- 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.
- Expand **Crosswork Configuration** and enter your legal disclaimer text (users will see this text if they log into the CLI).
- Expand **Crosswork Cluster Configuration**. Provide relevant values for the following fields:

Figure 8: Customize template - Crosswork Cluster Configuration (part 1)

The screenshot shows the 'Customize template' dialog box with the following settings:

Setting	Value
VM Type	Type of CW Node Hybrid
Cluster seed node	True/False: Is this the Cw cluster seed node. There can be at most 1 in a cluster False
Crossworks Management Cluster Virtual IP	Please enter virtual IP on the management network 192.168.103.61
Crossworks Management Cluster Virtual IP Name	Please enter DNS hostname of virtual IP interface of the Management Network
Crossworks Data Cluster Virtual IP	Please enter virtual IP on the data network 10.10.10.61
Crossworks Data Cluster Virtual IP Name	Please enter DNS hostname of virtual IP interface of the Data Network

Buttons: CANCEL, BACK, NEXT

- **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.
- **Crosswork Management Cluster Virtual IP Name:** Enter the Management Virtual IP DNS name.
- **Crosswork Data Cluster Virtual IP:** Enter the Data Virtual IP address.
- **Crosswork Data Cluster Virtual IP Name:** Enter the Data Virtual IP DNS name.
- **Initial node count:** Set to the default value, which is 3.
- **Initial leader node count:** Set to the default value, which is 3.

Figure 9: Customize template - Crosswork Cluster Configuration (part 2)

The screenshot shows the 'Customize template' dialog box with the following fields and values:

Field	Value
Crossworks Data Cluster Virtual IP Name	10.10.10.61
Initial node count	3
Initial leader node count	3
For AWS Deployment - IP addresses list of "all" of the peer Manager/Hybrid nodes on the Management Network in the cluster, including this node	
For AWS Deployment - List IP addresses list of "all" of the peer Manager/Hybrid nodes on the Data Network in the cluster, including this node - Only needed when deploying with Data Network	
For AWS Deployment ONLY - AWS IAM Role name	

Buttons at the bottom: CANCEL, BACK, NEXT.

- **Location of VM:** Enter the location of VM.
- **K8 Orchestrator:** Enforces minimum resource reservations for the pod. If left blank, the default value ("True") is selected.
- **Kubernetes Service Network:** The network address for the kubernetes service network. By default, the CIDR range is fixed to '/16'.
- **Kubernetes Pod Network:** The network address for the kubernetes pod network. By default, the CIDR range is fixed to '/16'.

Figure 10: Customize template - Crosswork Cluster Configuration (part 3)

The screenshot shows the 'Customize template' dialog box with the following configuration:

Field	Value
Location of VM	A user configurable string San Jose
K8 Orchestrator	FOR EXPERIMENTAL USE ONLY - Enforce Pod resource reservations True
Kubernetes Service Network	The default network '10.96.0.0'. If you prefer to customize this, please enter the network address for the service network. Only Class A Private Blocks are allowed, 10.0.0.0 to 10.255.0.0. The CIDR range is fixed '/16'. Service and Pod network blocks must not be same. WARNING: This customization can't be changed once cluster is deployed. 10.75.0.0
Kubernetes Pod Network	The default network '10.244.0.0'. If you prefer to customize this, please enter the network address for the service network. Only Class A Private Blocks are allowed, 10.0.0.0 to 10.255.0.0. The CIDR range is fixed '/16'. Service and Pod network blocks must not be same. WARNING: This customization can't be changed once cluster is deployed. 10.225.0.0
Installation type	Was the VM installed by the Cw installer? <input type="checkbox"/>

Buttons: CANCEL, BACK, NEXT

- **Installation type:**

- *For new cluster installation:* Do not select the check box.
- *Replacing a failed VM:* Select the check box.
- *Adding a new worker node to an existing cluster:* Do not select the check box.

- **Enable Skip Auto Install Feature:** Any pods marked as skip auto install will not be brought up until a dependent application/pod explicitly asks for it. If left blank, the default value ("False") is selected.

- **Auto Action Manifest Definition:** Auto action functionality enables you to customize the installation of applications along with the cluster installation. For more information, see [Automate Application Installation Using Auto Action Functionality, on page 43](#).

- If you plan to use the auto action functionality, enter manifest definition details. You must compress or minimize the auto action JSON file and enclose it in CDATA format. The format is `<![CDATA[{auto action json compressed content}]]>`.

Sample auto action CDATA:

```
<![CDATA[{"auto_action":{"add_to_repository_requests":[{"file_location":{"uri":"file:///example.com/path/to/ovra-cdatastage-7.0.0-240831.tar.gz"}}, {"install_activate_requests":[{"package_identifier":{"id":"capp-coe","version":"7.0.0"}}]}}]]>
```

- If you do not plan to use this functionality, leave the field blank.

- **Default Application Resource Profile:** Use the default value (Empty).

- **Default Infra Resource Profile:** Use the default value (Empty).

Figure 11: Customize template - Crosswork Cluster Configuration (part 4)

The screenshot shows the 'Customize template' dialog box. On the left, a vertical progress bar lists 10 steps: 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 (highlighted), and 10. Ready to complete. The main area is titled 'Customize template' and contains the following configuration options:

Kubernetes Pod Network	The default network '10.244.0.0'. If you prefer to customize this, please enter the network address for the service network. Only Class A Private Blocks are allowed, 10.0.0.0 to 10.255.0.0. The CIDR range is fixed '/16'. Service and Pod network blocks must not be same. WARNING: This customization can't be changed once cluster is deployed. 10.225.0.0
Installation type	Was the VM installed by the Cw installer? <input type="checkbox"/>
Enable Skip Auto Install Feature	Enable feature where pods marked as skip auto install will not be brought up until a dependent app asks for it? False ▾
Auto Action Manifest Definition	Enter the auto action definition in json format enclosed within CDATA I
Default Application Resource Profile	Application Resource Profile ▾
Default Infra Resource Profile	Infra Resource Profile ▾

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT.

- **CA Private Key:** Use the default value (Empty).
- **CA Public Key:** Use the default value (Empty).
- **Use NonDefault Calico Bgp Port:** Leave the checkbox unchecked.
- **Ignore Diagnose Failure:** Use the default value (True).
- **Enable Diagnostics Script Check run:** Use the default value (True).

Figure 12: Customize template - Crosswork Cluster Configuration (part 5)

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 a VM, right-click on the template and select **New VM from This Template**.

Note If the template is no longer present, go back and create the template. For more information, see [Build the OVF template, on page 60](#).

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

Note If this is a new VM, the name must be unique and cannot be the same name as the template. If this VM is replacing an existing VM (for example, CW-VM-0) give the VM a unique temporary name (for example, CW-VM-0-New).

Step 3 Click **Next**. The **Deploy From Template** window will refresh, highlighting the **2 - Select a compute resource** section. Select the host for your Cisco Crosswork VM.

Step 4 Click **Next**. The **Deploy From Template** window will refresh, highlighting the **3 - Select Storage** section. Choose **Same format as source** option as the virtual disk format (recommended).

The recommended configuration for the nodes uses a combination of high-speed (typically SSD based) and normal (typical disks) storage. If you are following the recommended configuration follow the steps for two data stores. Otherwise, follow the steps for using a single data store.

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

- Enable **Configure per disk** option.
- Select same data store (regular) as the **Storage** setting for disks 1 through 5. This data store must have 916 GB of space.
- Select the host's high speed (ssd) data store as the **Storage** setting for disk 6. The high speed data store must have at least 50 GB of space.
- Click **Next**.

Figure 13: Select Storage - Configure per disk

cw-template - Deploy From Template

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

Select storage
Select the storage for the configuration and disk files

Configure per disk

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

Compatibility

Compatibility checks succeeded.

CANCEL BACK NEXT

- *If you are using a single data store:* Select the data store you wish to use, and click **Next**.
- *If your data center uses shared storage:* Configure all the drives to utilize the shared storage, and click **Next**.

Step 5

The **Deploy From Template** window will refresh, highlighting the **4 - Select clone options** section with the following checkboxes visible on the screen. Unless you have been given specific instructions to make modifications, select **Next**.

- **Customize the operating system:** Check this box if you want to customize the operating system to avoid conflicts when deploying the VM. This step is optional.
 - If you check this box, the **Deploy From Template** window will refresh, highlighting the **Customize guest OS** section. Make the necessary changes, and click **Next**.
- **Customize this virtual machine's hardware:** Check this box if you want to modify the IP settings or resource settings of this VM. This step is optional.
 - If you check this box, the **Deploy From Template** window will refresh, highlighting the **Customize hardware** section. Make the necessary changes, and click **Next**.
- **Power on virtual machine after creation:** Leave this checkbox unselected.

Step 6

Click **Next**. The **Deploy From Template** window will refresh, highlighting the **5 - Customize vApp properties** section. The vApp properties are prepopulated with the values entered during the template creation. Some of the values will need to be updated with the appropriate values for each node being deployed.

Tip

- It is recommended to change only the fields that are unique to each node. Leave all other fields at the default values.
 - If this VM is being deployed to replace a failed VM, or to migrate the VM to a new host, the IP and other settings must match the machine being replaced.
- Set the node type (Hybrid/Worker).
 - **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.
 - **Deployment Credentials:** Enter same deployment credentials for each VM in the cluster.
 - **DNS and NTP Servers:** Enter correct values for the DNS and NTP servers.
 - **Disk Configuration:** Leave at the default settings unless directed otherwise by the Cisco Customer Experience team.
 - **Crosswork Configuration:** Enter the disclaimer message.
 - **Crosswork Cluster Configuration:**
 - **VM Type:** Select Hybrid or Worker
 - **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 or moving the VM to a new host.
 - **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.

- Step 7** Click **Next**. The **Deploy From Template** window will refresh, highlighting the **6 - Ready to complete** section. Review your settings and then click **Finish** if you are ready to begin deployment.
- Step 8** For the newly created VM, confirm that the resource settings allocated for the VM match those specified in [Identify the Resource Footprint, on page 7](#).
- Step 9** Repeat from **Step 1** to **Step 8** to deploy the remaining VMs in the cluster.
- Important** When deploying the cluster for the first time, make sure the IP addresses and Seed node settings are correct. When replacing or migrating a node make sure the settings match the original VM.
- Step 10** Choose the relevant action:
- If you are deploying a new VM, power on the VM selected as the cluster seed node. After a delay of few minutes, power on the remaining nodes. To power on, expand the host's entry, click the Cisco Crosswork VM, and then choose **Actions > Power > Power On**.
 - If this VM is replacing an existing VM, perform the following:
 - Power down the existing VM.
 - Change the name of the original VM (for example, change to CW-VM-0-Old)
 - Change the name of the replacement VM (for example change to CW-VM-0-New) to match the name of the original VM (for example, CW-VM-0).
 - Power on the new VM. Monitor the health of the cluster using the Crosswork UI.
 - Once the cluster is healthy and stable, delete the original VM (now named as CW-VM-0-Old)
- Step 11** 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 Cluster Activation, on page 73](#) 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 the process to build a new Worker node, the node will automatically register itself 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 Network Controller 7.0 Administration Guide](#).

What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

Monitor Cluster Activation

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**, `cw-admin`, with the password that you provided in the manifest template. In case the installer is unable to apply the password, it creates the administrative ID with the default password `cw-admin`). The first time you log in using this administrative ID, you will be prompted to change the password.

The administrative username is reserved and cannot be changed. Data center administrators use this ID to log into and troubleshoot the Crosswork application VM.

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.

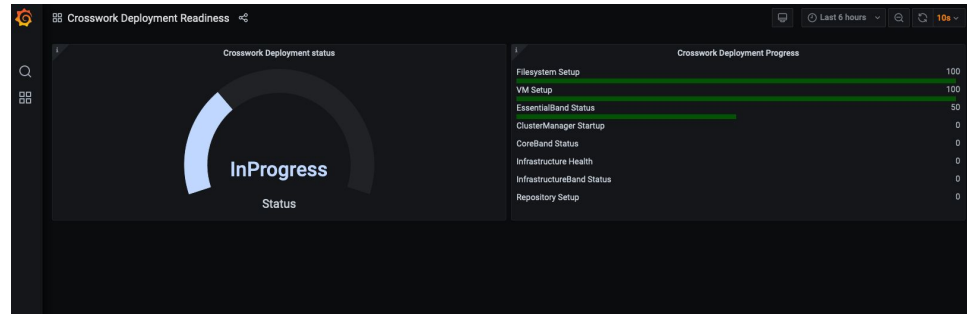
3. After each VM is created, it is powered on (either automatically when the installer completes, or after you power on the VMs during the manual installation). The parameters specified in the template are applied to the VM, and it is rebooted. The VMs are then registered by Kubernetes to form the cluster.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

1. While the cluster is being created, monitor the setup process from a browser accessible dashboard.
2. 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. This URL is temporary and will be available only for a limited time (around 30 minutes).
3. At the end of the deployment, the grafana dashboard will report a "Ready" status. If the URL is inaccessible, use the SSH console described in this section to monitor the installation process.

Figure 14: Crosswork Deployment Readiness



- **Using the console:**

1. Check the progress from the console of one of the hybrid VMs or by using SSH to the Virtual IP address.
2. In the latter case, login using the *cw-admin* user name and the password you assigned to that account in the install template.
3. Switch to super user using `sudo su -` command.
4. Run `kubectl get nodes` (to see if the nodes are ready) and `kubectl get pods` (to see the list of active running pods) commands.
5. Repeat the `kubectl get pods` command until you see `robot-ui` in the list of active pods.
6. 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 76](#).

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.

What to do next:

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

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.



Note For the supported browser versions, see the *Compatibility Information* section in the [Cisco Crosswork Network Controller 7.0 Release Notes](#).

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 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 restart the node(s). If you require assistance, please contact the Cisco Customer Experience team.

Step 1 Launch one of the supported browsers.

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 the Crosswork FQDN name.

The **Log In** window opens.

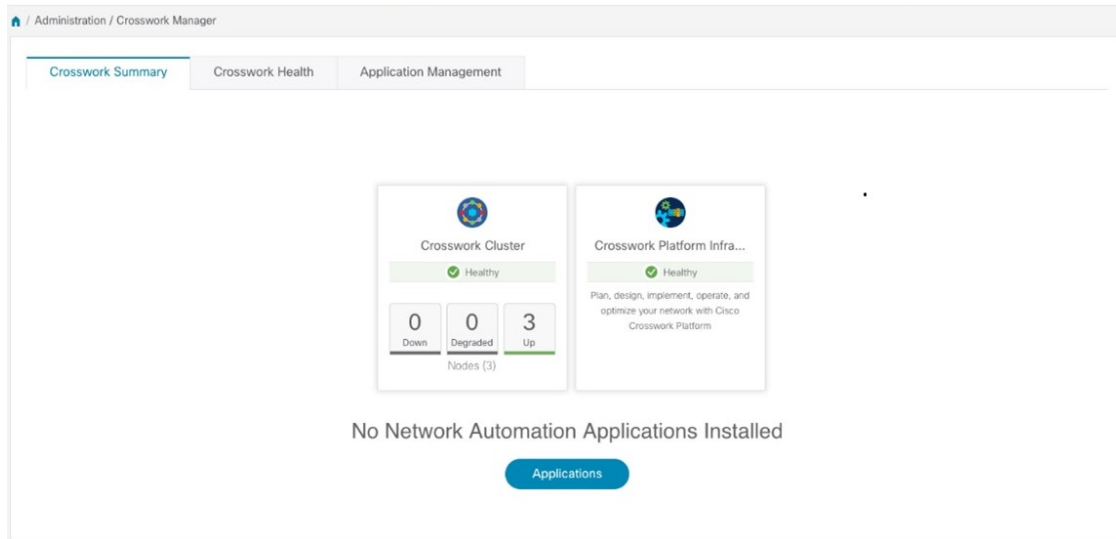
Note When you access the Cisco Crosswork for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from the Cisco Crosswork server. After you add a security exception, the browser accepts the server as a trusted site in all future login attempts. If you want to use a CA signed certificate, see the *Manage Certificates* topic in the *Cisco Crosswork Network Controller 7.0 Administration Guide*.

Step 3 Log into the Cisco Crosswork as follows:

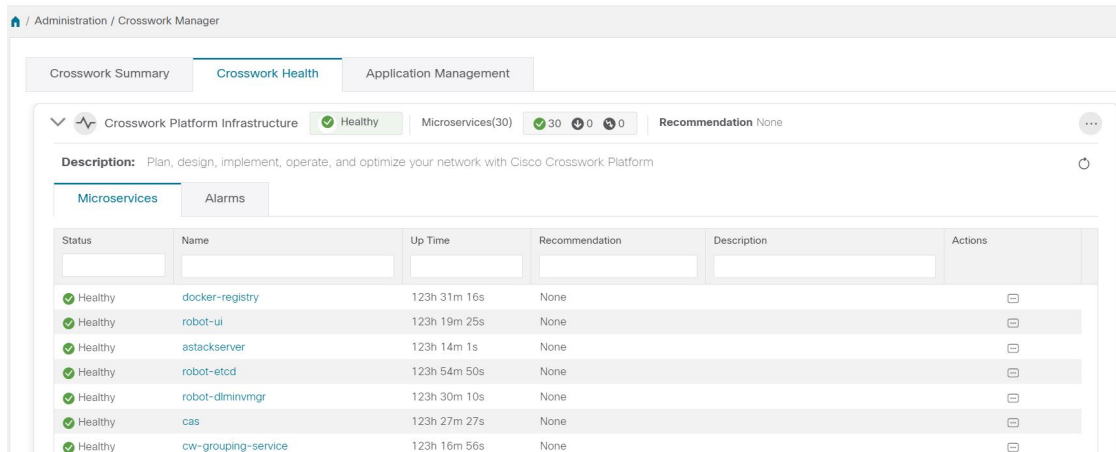
- a) Enter the Cisco Crosswork administrator username **admin** and the default password **admin**.
- b) Click **Log In**.
- c) When prompted to change the administrator's default password, enter the new password in the fields provided and then click **OK**.

Note Use a strong VM Password (minimum 8 characters long, including upper & lower case letters, numbers, and one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words.

The **Crosswork Manager** window is displayed.



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



Step 5 (Optional) Change the name assigned to the admin account (by default, it is "John Smith") to something more relevant.

Step 6 **In case of manual installation:** After logging into the Crosswork UI, ensure the cluster is healthy. Download the cluster inventory sample (.tfvars file) from the Crosswork UI and update it with information about the VMs in your cluster, along with the data center parameters. Then, import the file back into the Crosswork UI. For more information, see [Import Cluster Inventory, on page 78](#).

What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

Import Cluster Inventory

If you have installed your cluster manually using the vCenter UI, you must import an inventory file (.tfvars file) to Cisco Crosswork to reflect the details of your cluster. A sample inventory file can be downloaded from the Crosswork UI.



Note If the manual installation was performed to replace a failed VM, you must delete the original VM after importing the cluster inventory file.



Attention Crosswork cannot deploy or remove VM nodes in your cluster until you complete this operation.



Note Please uncomment the "OP_Status" parameter while importing the cluster inventory file manually. If you fail to do this, the status of the VM will incorrectly appear as "Initializing" even after the VM becomes functional.

-
- Step 1** From the main menu, choose **Administration > Crosswork Manager**.
 - Step 2** On the **Crosswork Summary** tab, click the **System Summary** tile to display the **Cluster Management** window. Ensure the cluster is healthy.
 - Step 3** Choose **Actions > Import Cluster Inventory** to display the **Import Cluster Inventory** dialog box.
 - Step 4** (Optional) Click **Download sample template file** to download the template. Update the file with information about the VMs in your cluster, along with the data center parameters. For more details on the installation parameters, see [Installation Parameters, on page 37](#).
 - Step 5** Click **Browse** and select the cluster inventory file.
 - Step 6** Click **Import** to complete the operation.
-

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.

Table 22: General scenarios

Scenario	Possible Resolution
Certificate Error	The ESXi hosts that will run the Crosswork application and the data gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors.

Scenario	Possible Resolution
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 Prerequisites for VMware vCenter, on page 19 .
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.
Crosswork VM is not allowing the admin user to log in OR The following error is displayed: <i>Error: Invalid value for variable on cluster_vars.tf line 113:</i> _____ <i>This was checked by the validation rule at cluster_vars.tf:115,3-13. Error: expected length of name to be in the range (1 - 80), got with data.vsphere_virtual_machine.template_from_ovf, on main.tf line 32, in data "vsphere_virtual_machine" "template_from_ovf": 32: name = var.Cw_VM_Image Mon Aug 21 18:52:47 UTC 2023: ERROR: Installation failed. Check installer and the VMs' log by accessing via console and viewing /var/log/firstBoot.log</i>	This happens when the password is not complex enough. Create a strong password, update the configuration manifest and redeploy. Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and at least one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words. While they satisfy the criteria, such passwords are weak and will be rejected resulting in failure to setup the VM.
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.

Scenario	Possible Resolution
<p>The VMs are deployed but the Crosswork cluster is not being formed.</p>	<p>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:</p> <pre>sudo kubectl get nodes</pre> <p>A healthy output for a 3-node cluster is:</p> <pre>NAME STATUS ROLES AGE VERSION 172-25-87-2-hybrid.cisco.com Ready master 41d v1.16.4 172-25-87-3-hybrid.cisco.com Ready master 41d v1.16.4 172-25-87-4-hybrid.cisco.com Ready master 41d v1.16.4</pre> <p>In case of a different output, collect the following logs: /var/log/firstBoot.log and /var/log/vm_setup.log</p> <p>In addition, for any cluster nodes not displaying the Ready state, collect:</p> <pre>sudo kubectl describe node <name of node></pre>
<p>The following error is displayed while uploading the image:</p> <p><i>govc: The provided network mapping between OVF networks and the system network is not supported by any host.</i></p>	<p>The Dswitch on the vCenter is misconfigured. Please check whether it is operational and mapped to the ESXi hosts.</p>
<p>VMs deploy but install fails with <i>Error: timeout waiting for an available IP address</i></p>	<p>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:</p> <pre>/var/log/firstBoot.log and /var/log/vm_setup.log</pre>
<p>When deploying on a vCenter, the following error is displayed towards the end of the VM bringup:</p> <p><i>Error processing disk changes post-clone: disk.0: ServerFaultCode: NoPermission: RESOURCE (vm-14501:2000), ACTION (queryAssociatedProfile): RESOURCE (vm-14501), ACTION (PolicyIDByVirtualDisk)</i></p>	<p>Enable Profile-driven storage. Query permissions for the vCenter user at the root level (i.e. for all resources) of the vCenter.</p>

Scenario	Possible Resolution
<p>On running or cleaning, installer reports <i>Error: cannot locate virtual machine with UUID "xxxxxxx": virtual machine with UUID "xxxxxxx" not found</i></p>	<p>The installer uses the <code>tfstate</code> file stored as <code>/data/crosswork-cluster.tfstate</code> 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.</p> <p>To resolve, remove the <code>/data/crosswork-cluster.tfstate</code> file.</p>

Scenario	Possible Resolution
----------	---------------------

Scenario	Possible Resolution
<p>Scenario</p> <p>In a cluster with five or more nodes, the databases move to hybrid nodes during a node reload scenario. Users will see the following alarm:</p> <p><i>"The robot-postgres/cw-timeseries-db pods are currently running on hybrid nodes. Please relocate them to worker nodes if they're available and health."</i></p> <p>Resolution</p> <p>To resolve the alarm, invoke the move API to move the databases to worker nodes.</p> <p>Use the following script to place services. It returns a job ID that can be queried to ensure the job is completed.</p> <p>[Place Services]</p> <p>Request</p> <pre>curl --request POST --location 'https://<Vip>:30603/crosswork/platform/v2/placement/move_services_to_nodes' \ --header 'Content-Type: application/json' \ --header 'Authorization: <your-jwt-token>' \ --data '{ "service_placements": [{ "service": { "name": "robot-postgres", "clean_data_folder": true }, "nodes": [{ "name": "fded-1bc1-fc3e-96d0-192-168-5-114-worker.cisco.com" }, { "name": "fded-1bc1-fc3e-96d0-192-168-5-115-worker.cisco.com" }] }, { "service": { "name": "cw-timeseries-db", "clean_data_folder": true }, "nodes": [{ "name": "fded-1bc1-fc3e-96d0-192-168-5-114-worker.cisco.com" }, { "name": "fded-1bc1-fc3e-96d0-192-168-5-115-worker.cisco.com" }] }] }'</pre> <p>Response</p> <pre>{ "job_id": "PJ5", "result": { "request_result": "ACCEPTED", "error": null } }</pre>	

Scenario	Possible Resolution
<pre> } } [GetJobs] Request curl --request POST --location 'https://<Vip>:30603/crosswork/platform/v2/placement/jobs/query' \ --header 'Content-Type: application/json' \ --header 'Authorization: <your-jwt-token>' \ --data '{"job_id":"PJ5"}' Response { "jobs": [{ "job_id": "PJ1", "job_user": "admin", "start_time": "1714651535675", "completion_time": "1714652020311", "progress": 100, "job_status": "JOB_COMPLETED", "job_context": {}, "job_type": "MOVE_SERVICES_TO_NODES", "error": { "message": "" }, "job_description": "Move Services to Nodes" }], "query_options": { "pagination": { "page_token": "1714650688679", "page_size": 200 } }, "result": { "request_result": "ACCEPTED", "error": null } } [GetEvents] </pre>	

Scenario	Possible Resolution
<pre>Request curl --request POST --location 'https://<Vip>:30603/crosswork/platform/v2/placement/events/query' \ --header 'Content-Type: application/json' \ --header 'Authorization: <your-jwt-token>' \ --data '{}'</pre> <pre>Response { "events": [{ "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Operation done", "event_time": "1714725461179" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Moving replica pod , to targetNodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com fded-1bc1-fc3e-96d0-192-168-6-116-worker.cisco.com]", "event_time": "1714725354163" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "robot-postgres - Cleaning up target nodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com fded-1bc1-fc3e-96d0-192-168-6-116-worker.cisco.com] for stale data folder", "event_time": "1714725346515" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Replica pod not found for service robot-postgres", "event_time": "1714725346507" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }] }] }</pre>	

Scenario	Possible Resolution
<pre> }], "message": "Started moving leader and replica pods for service robot-postgres", "event_time": "1714725346504" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": " robot-postgres - Source and target nodes are not subsets, source nodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com] , target nodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com fded-1bc1-fc3e-96d0-192-168-6-116-worker.cisco.com]", "event_time": "1714725346293" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Verified cw-timeseries-db location on target nodes", "event_time": "1714725345692" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Moved leader pod cw-timeseries-db-0, to targetNodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com fded-1bc1-fc3e-96d0-192-168-6-116-worker.cisco.com]", "event_time": "1714725345280" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "cw-timeseries-db-0 is ready", "event_time": "1714725345138" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "cw-timeseries-db-0 is ready", "event_time": "1714725241401" }, </pre>	

Scenario	Possible Resolution
	<pre> { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Checking for cw-timeseries-db-0 pod is ready", "event_time": "1714725211296" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Moving leader pod cw-timeseries-db-0, to targetNodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com fded-1bc1-fc3e-96d0-192-168-6-116-worker.cisco.com]", "event_time": "1714725211256" } { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "cw-timeseries-db-1 is ready", "event_time": "1714725132896" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Checking for cw-timeseries-db-1 pod is ready", "event_time": "1714725131684" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Moving replica pod cw-timeseries-db-1, to targetNodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com fded-1bc1-fc3e-96d0-192-168-6-116-worker.cisco.com]", "event_time": "1714725128203" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], } </pre>

Scenario	Possible Resolution
<pre> "message": "cw-timeseries-db - Cleaning up target nodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com fded-1bc1-fc3e-96d0-192-168-6-116-worker.cisco.com] for stale data folder", "event_time": "1714725119505" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "Started moving leader and replica pods for service cw-timeseries-db", "event_time": "1714725117684" }, { "event_tags": [{ "tag_type": "JOB_ID_EVENT", "tag_value": "PJ5" }], "message": "cw-timeseries-db - Source and target nodes are not subsets, source nodes [fded-1bc1-fc3e-96d0-192-168-6-111-hybrid.cisco.com fded-1bc1-fc3e-96d0-192-168-6-113-hybrid.cisco.com] , target nodes [fded-1bc1-fc3e-96d0-192-168-6-115-worker.cisco.com fded-1bc1-fc3e-96d0-192-168-6-116-worker.cisco.com]", "event_time": "1714725115883" }], "query_options": { "pagination": { "page_token": "1714725115883", "page_size": 200 } }, "result": { "request_result": "ACCEPTED", "error": null } } </pre>	

Table 23: Installer tool scenarios

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>

Scenario	Possible Resolution
<p>Error conditions such as:</p> <p><i>Error: Error locking state: Error acquiring the state lock: resource temporarily unavailable</i></p> <p><i>Error: error fetching virtual machine: vm not found</i></p> <p><i>Error: Invalid index</i></p>	<p>These errors are common when re-running the installer after an initial run is interrupted (Control C, or TCP timeout, etc). Remediation steps are:</p> <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>). 3. Retry the installation (<code>./cw-installer.sh clean -m <your manifest here></code>).
<p>The VMs take a long time to deploy</p>	<p>The time needed to clone the VMs during the installation will be determined by the workload on the disk drives used by the host machines. Running the install serially (without the [-p] flag) will lessen this load while increasing the time needed to deploy the VMs.</p>
<p>Installer reports plan to add more resources than the current number of VMs</p>	<p>Other than the Crosswork cluster VMs, the installer tracks 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.</p>
<p>On running or cleaning, installer reports</p> <p><i>Error: cannot locate virtual machine with UUID "xxxxxxx": virtual machine with UUID "xxxxxxx" not found</i></p>	<p>To resolve, remove the <code>/data/crosswork-cluster.tfstate</code> file.</p> <p>The installer uses the <code>tfstate</code> file stored as <code>/data/crosswork-cluster.tfstate</code> 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.</p>
<p>Encountered one of the following errors during execution:</p> <p>Error 1:</p> <p><i>% docker run --rm -it -v `pwd`:/data a45 docker: invalid reference format: repository name must be lowercase. See 'docker run --help'</i></p> <p>Error 2:</p> <p><i>docker: Error response from daemon: Mounts denied: approving /Users/Desktop: file does not exist ERRO[0000] error waiting for container: context canceled</i></p>	<p>Move the files to a directory where the path is in lowercase (all lowercase, no spaces or other special characters). Then navigate to that directory and rerun the installer.</p>

Table 24: Dual stack scenarios

Scenario	Possible Resolution
<p>During deployment, the following error message is displayed:</p> <p><i>ERROR: No valid IPv6 address detected for IPv6 deployment.</i></p>	<p>If you intend to use a dual stack configuration for your deployment, make sure that the host machine running the Docker installer meets the following requirements:</p> <ul style="list-style-type: none"> • It must have an IPv6 address from the same prefix as the Crosswork Management IPv6 network, or be able to route to that network. To verify this, try pinging the Gateway IP of the Management IPv6 network from the host. To utilize the host's IPv6 network, use the parameter <code>--network host</code> when running the Docker installer. • Confirm that the provided IPv6 network CIDR and gateway are valid and reachable.
<p>During deployment, the following error message is displayed:</p> <p><i>ERROR: seed v4 host empty</i></p>	<p>Ensure you use the approved version of Docker installer (19 or higher) to run the deployment.</p>
<p>During deployment, the following error message is displayed:</p> <p><i>ERROR: Installation failed. Check installer and the VMs' log by accessing via console and viewing /var/log/firstBoot.log</i></p>	<p>Common reasons for failed installation are:</p> <ul style="list-style-type: none"> • Incorrect IPv4 or IPv6 Gateway IP for either Management or Data interfaces. • Unreachable IPv4 or IPv6 Gateway IP for either Management or Data interfaces. • Errors in mapping the vCenter networks in <code>MgmtNetworkName</code> and <code>DataNetworkName</code> parameters in <code>.tfvars</code> file <p>Check the <code>firstBoot.log</code> file for more information, and contact Cisco Customer Experience team for any assistance.</p>

What to do next:

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)



CHAPTER 6

Install Crosswork Data Gateway on VMware vCenter

This chapter contains the following topics:

- [Crosswork Data Gateway Installation Workflow, on page 91](#)
- [Log in and Log out of the Data Gateway VM, on page 124](#)
- [Crosswork Data Gateway Authentication and Enrollment, on page 126](#)
- [Crosswork Data Gateway Post-installation Tasks, on page 127](#)
- [Troubleshoot Crosswork Data Gateway Installation and Enrollment, on page 128](#)

Crosswork Data Gateway Installation Workflow

Crosswork Data Gateway is installed as a base VM that contains only enough software to register itself with Cisco Crosswork.



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

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

1. Choose the deployment profile for the Data Gateway VM. See [Crosswork Data Gateway VM Requirements, on page 27](#).
2. Review the installation parameters at [Crosswork Data Gateway Parameters and Deployment Scenarios](#) and make sure that you have all the required information to install Data Gateway using the preferred deployment scenario.
3. Install Data Gateway using a preferred method:

Table 25: Crosswork Data Gateway installation options

VMware	Install Crosswork Data Gateway using vCenter vSphere Client, on page 105
	Install Crosswork Data Gateway via OVF Tool, on page 116



Note If you plan to install multiple Data Gateway VMs due to load or scale requirements or you wish to leverage Crosswork Data Gateway High Availability, we recommend that you install all the Data Gateway VMs first and then proceed with adding them to a Data Gateway pool.

- Complete the post-installation tasks mentioned in the section [Crosswork Data Gateway Post-installation Tasks, on page 127](#).
- Verify that the Data Gateway VM has enrolled successfully with Crosswork Network Controller. For information on how to verify the enrollment process, see [Crosswork Data Gateway Authentication and Enrollment, on page 126](#).

After verifying that the Data Gateway VM has enrolled successfully with Cisco Crosswork, set up the Data Gateway for collection by creating a Data Gateway pool. For more information, see the *Create a Crosswork Data Gateway Pool* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

Crosswork Data Gateway Parameters and Deployment Scenarios

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

During installation, Crosswork Data Gateway creates the following user accounts:

- 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 the data gateway.
- 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 the *Supported User Roles* topic in the [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

- Crosswork Data Gateway technical assistance center, with the username, `dg-tac`. The password for this user is set when one of the other users of the data gateways enables this account.

The **dg-admin**, **dg-oper**, and **dg-tac** user accounts are reserved user names and cannot be changed. You can change the password in the console for both the accounts. For more information, see the *Change Passphrase* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#). In case of lost or forgotten passwords, destroy the current VM, you have to create a new VM, and re-enroll the new VM with Cisco Crosswork.

The following table provides the label and key values of deployment parameters. Labels represent the parameters that can be configured in the VMware UI and Keys corresponds to field values in the OVF script that match your configuration.

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.



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 data gateway VM, create a new VM, and re-enroll the new VM with Cisco Crosswork.

Table 26: Crosswork Data Gateway Deployment Parameters and Scenarios

Label	Key	Description	Additional Information
DeploymentOption	DeploymentOption	Parameter conveys the VM resource profile. For an on-premise installation, choose either: <ul style="list-style-type: none"> • onpremise-standard • onpremise-extended 	This parameter is applicable only for the OVF tool.
Host Information			
Hostname*	Hostname	Name of the data gateway VM specified as a fully qualified domain name (FQDN). In larger systems, you are likely to have more than one data gateway VM. The host name must, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	Description	A detailed description of the data gateway.	
Crosswork Data Gateway Label	Label	Label used by Cisco Crosswork to categorize and group multiple data gateway VMs.	

Label	Key	Description	Additional Information
Allow Usable RFC 8190 Addresses*	AllowRFC8190	Choose how to validate interface addresses that fall in a usable RFC 8190 range. Options are: <i>Yes</i> , <i>No</i> , or <i>Ask</i> , where the initial configuration script prompts for confirmation. The default value is <i>Yes</i> .	The default value is <i>Yes</i> to automatically allow interface addresses in an RFC 8190 range.
Crosswork Data Gateway Private Key URI	DGCertKey	SCP URI to private key file for session key signing. You can retrieve this using SCP (user@host:path/to/file).	Cisco Crosswork uses self-signed certificates for handshake with Crosswork Data Gateway. These certificates are generated at installation.
Crosswork Data Gateway Certificate File and Key Passphrase	DGCertChainPwd	Passphrase of the SCP user to retrieve the Crosswork Data Gateway PEM formatted certificate file and private key.	However, if you want to use third party or your own certificate files, then enter these parameters. Certificate chains override any preset or generated certificates in the data gateway VM and are given as an SCP URI (user:host:/path/to/file). 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.
Data Disk Size	DGAppdataDisk	Indicates the size in GB of a second data disk. The default value of this parameter in each profile is: <ul style="list-style-type: none"> • 20 GB for Standard. • 520 GB for Extended. Do not change the default value without consulting a Cisco representative.	

Label	Key	Description	Additional Information
High Availability Network Mode *	HANetworkMode	Indicates the mode for the HA network. Options are: <ul style="list-style-type: none"> • L2 • L3 The default value is L2.	When deploying on VMware, set the network to L2.
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 data gateway pool creation as explained in the <i>Create a Crosswork Data Gateway Pool</i> section in Cisco Crosswork Network Controller 7.0 Administration Guide.</p> <p>Note Selecting None in both IPv4 Method and the IPv6 Method fields of the vNIC results in a nonfunctional deployment.</p>			
vNIC Role Assignment			
<p>Role assignment allows you to control the traffic that an interface must handle. If the preassigned roles don't meet the specific needs of your organization, you can explicitly assign roles to interfaces. For example, you can assign the role 'ADMINISTRATION' to an interface to route only the SSH traffic.</p> <p>Each parameter has a predefined role. The parameter accepts the interface value as eth0, eth1, or eth2.</p>			

Label	Key	Description	Additional Information
Default Gateway*	NicDefaultGateway	The interface used as the Default Gateway for processing the DNS and NTP traffic. Options are eth0, eth1, or eth2. The default value is eth0.	For information on the type of roles that you must assign to the vNICs, see Table 9: Crosswork Data Gateway default vNIC deployment modes , on page 23.
Administration*	NicAdministration	The interface used to access the VM through the SSH access. Options are eth0, eth1, or eth2. The default value is eth0.	
External Logging*	NicExternalLogging	The interface used to send logs to an external logging server. Options are eth0, eth1, or eth2. The default value is eth0.	
Management*	NicManagement	The interface used to send the enrollment and other management traffic. Options are eth0, eth1, or eth2. The default value is eth0.	
Control*	NicControl	The interface used to send the destination, device, and collection configuration. Options are eth0, eth1, or eth2. The default value is eth1.	
Northbound System Data*	NicNBSystemData		

Label	Key	Description	Additional Information
		<p>The interface used to send collection data to the system destination.</p> <p>As the system destinations share the same IP as interface that allows connection to the collection service, the northbound data for system destinations uses the Control role's interface.</p> <p>Options are <code>eth0</code>, <code>eth1</code>, <code>eth2</code> or <code>eth3</code>.</p>	
Northbound External Data*	<code>NicNBExternalData</code>	<p>The interface used to send the collection data to the external destinations configured by the user.</p> <p>Options are <code>eth0</code>, <code>eth1</code>, or <code>eth2</code>. The default value is <code>eth1</code>.</p>	
Southbound Data*	<code>NicSBData</code>	<p>The interface used to collect data from the devices.</p> <p>If the interface only has the <code>NicSBData</code> role, it doesn't need an IP during the deployment.</p> <p>Options are <code>eth0</code>, <code>eth1</code>, or <code>eth2</code>. The default value is <code>eth2</code>.</p>	
<p>vNIC IPv4 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)</p> <p>Important When using two or three NICs both vNIC0 and vNIC1 must be assigned static IPV4 or IPV6 addresses.</p> <p>All unused vNICs (IPv4 or IPV6) should be left set to Method "None" with the other fields left at the default.</p>			

Label	Key	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 - <i>None</i> or <i>Static</i> . The default value is <i>None</i> .	<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
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 <i>False</i> . Setting this to <i>True</i> skips configuring a gateway.	
vNIC IPv4 Gateway	Vnic0IPv4Gateway Vnic1IPv4Gateway Vnic2IPv4Gateway	IPv4 address of the vNIC gateway.	
vNIC IPv6 Address (vNIC0, vNIC1, and vNIC2 based on the number of interfaces you choose to use)			

Label	Key	Description	Additional Information
vNIC IPv6 Method*	Vnic0IPv6Method Vnic1IPv6Method Vnic2IPv6Method	Method in which the vNIC interface is assigned an IPv6 address - None, Static, or SLAAC. 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 IPv6 parameters. Enter information in the vNIC IPv4 Address parameters. • Static: Enter information in Address, Netmask, Skip Gateway, and Gateway fields <p>Do not change the VnicxIPv6Address default values.</p>
vNIC IPv6 Address	Vnic0IPv6Address Vnic1IPv6Address Vnic2IPv6Address	IPv6 address of the interface.	
vNIC IPv6 Netmask	Vnic0IPv6Netmask Vnic1IPv6Netmask Vnic2IPv6Netmask	IPv6 prefix of the interface.	
vNIC IPv6 Skip Gateway	Vnic0IPv6SkipGateway Vnic1IPv6SkipGateway Vnic2IPv6SkipGateway	Options are True or False. Selecting True skips configuring a gateway.	
vNIC IPv6 Gateway	Vnic0IPv6Gateway Vnic1IPv6Gateway Vnic2IPv6Gateway	IPv6 address of the vNIC gateway.	
DNS Servers			
DNS Address*	DNS	Space delimited list of IPv4 or IPv6 addresses of the DNS servers accessible from the management interface.	
DNS Search Domain*	Domain	DNS search domain. The default value is localdomain.	
DNS Security Extensions*	DNSSEC	Options are False, True, or Allow-Downgrade. The default value is False Select True to use DNS security extensions.	

Label	Key	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> .	If you choose <code>Resolve</code> , only resolution support is enabled. Responding is disabled. Select <code>True</code> to use link-local multicast name resolution.
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 the 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, data gateway fails to connect.

Label	Key	Description	Additional Information
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 Password	NTPKeyFilePwd	Password of SCP URI to the chrony key file.	
Remote Syslog Server			

Label	Key	Description	Additional Information
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 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
Syslog Server Addresses	SyslogAddress	Hostname, IPv4, or IPv6 address of a syslog server accessible in the management interface.	
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> , <code>REL</code> , or <code>TCP</code> to send the syslog. The default value is <code>UDP</code> .	
Syslog Multiserver Mode	SyslogMultiserverMode	Multiple servers in the failover or simultaneous mode. This parameter is applicable only when the protocol is set to a non-UDP value. UDP must use the simultaneous mode. Options are <code>Simultaneous</code> or <code>Failover</code> . The default value is <code>Simultaneous</code> .	
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 <code>SubjectAltName</code> or <code>subject common name</code> .	
Syslog Root Certificate File URI	SyslogCertChain		

Label	Key	Description	Additional Information
		<p>PEM formatted root cert of syslog server retrieved using SCP.</p> <p>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.</p>	
Syslog Certificate File Passphrase	SyslogCertChainPwd	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Server			
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.	<p>If desired, you can configure an external Auditd server. Crosswork Data Gateway sends audit notifications to the Auditd server when configured and present on the network.</p> <p>Specify these three settings to use an external Auditd server.</p>
Auditd Server Address	AuditdAddress	Hostname, IPv4, or IPv6 address of an optional Auditd server.	
Auditd Server Port	AuditdPort	<p>Port number of an optional Auditd server.</p> <p>The default port is 60.</p>	
Controller and Proxy Settings			
Crosswork Controller IP*	ControllerIP	<p>The Virtual IP address or the host name of Cisco Crosswork Cluster.</p> <p>Note If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).</p> <p>If geo redundancy is enabled, use the unified endpoint. For more information, see Unified Endpoint Requirements, on page 250.</p>	<p>This is required so that the data gateway can enroll with the Crosswork server during the installation and initial start up. Excluding this step will require you to manually ingest the certificate. For more information, see Import Controller Signing Certificate File, on page 132.</p>

Label	Key	Description	Additional Information
Crosswork Controller Port*	ControllerPort	Port of the Cisco Crosswork controller. The default port is 30607.	
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> <pre> cw-admin@<Crosswork_VM_Management_IP_Address> /usr/local/crosswork/ </pre> <p>Note If you are using an IPv6 address, it must be surrounded by square brackets ([:::1]).</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 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 132.</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.	

Label	Key	Description	Additional Information
Proxy Server URL	ProxyURL	URL of the HTTP proxy server.	<p>The proxy parameters apply to the Crosswork Data Gateway cloud deployment.</p> <p>The data gateway must connect to the Internet via TLS, and a proxy server may be required if it is not present in your environment.</p> <p>If you want to use a proxy server, specify these parameters.</p>
Proxy Server Bypass List	ProxyBypass	Comma-delimited list of addresses and hostnames that will not use the proxy server.	
Authenticated Proxy Username	ProxyUsername	Username for authenticated proxy servers.	
Authenticated Proxy Passphrase	ProxyPassphrase	Passphrase for authenticated proxy servers.	
HTTPS Proxy SSL/TLS Certificate File URI	ProxyCertChain	HTTPS proxy PEM formatted SSL/TLS certificate file retrieved using SCP.	
HTTPS Proxy SSL/TLS Certificate File Passphrase	ProxyCertChainPwd	Password of SCP user to retrieve proxy certificate chain.	
Geo Redundancy Settings			
Availability Zone ID	az_id	The physical location of Availability Zone 1 and 2.	
Region ID	region_id	The physical location of the data gateway VM.	
Site location*	site_location	<p>The location of the primary and second Crosswork sites.</p> <p>During enrollment, Crosswork sends this value to cdg-manager to preset the cluster affiliation of the instance.</p>	

Install Crosswork Data Gateway using vCenter vSphere Client

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

**Note**

- We have included sample images of Crosswork Data Gateway on-premise Standard deployment in the procedure.
- Depending on the vCenter version, the layout and order of fields on the vCenter vSphere screens can vary.
- Values that are not explicitly mentioned in this section but are required to align with your environment should be retained at their default values.

Before you begin**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 26: Crosswork Data Gateway Deployment Parameters and Scenarios, on page 93](#) for list of mandatory and optional parameters.

Step 1

Download the Crosswork Data Gateway UEFI OVA image file from [cisco.com](https://www.cisco.com) (*.ova). For the 7.0 release, download **signed-cw-na-dg-7.0.0-26-release-20240918.uefi.ova**.

Step 2

Connect to vCenter vSphere Client and 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.

Figure 15: Deploy OVF Template - Select an OVF Template Window

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

http | https://remoteserver-address/filetoinstall.ovf | .ova

Local file

signed-cw-na-dg-7.0.0-26-release-20240918.uefi.ova

Step 4

Click **Next** to go to **2 Select a name and folder**, as shown in the following figure.

- a) Enter a unique name for the VM that you are creating.
- b) In the **Select a location for the virtual machine** list, choose the data center under which the VM resides.

Figure 16: Deploy OVF Template - Name and Folder Selection Window

Deploy OVF Template

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

Select a name and folder
Specify a unique name and target location

Virtual machine name:

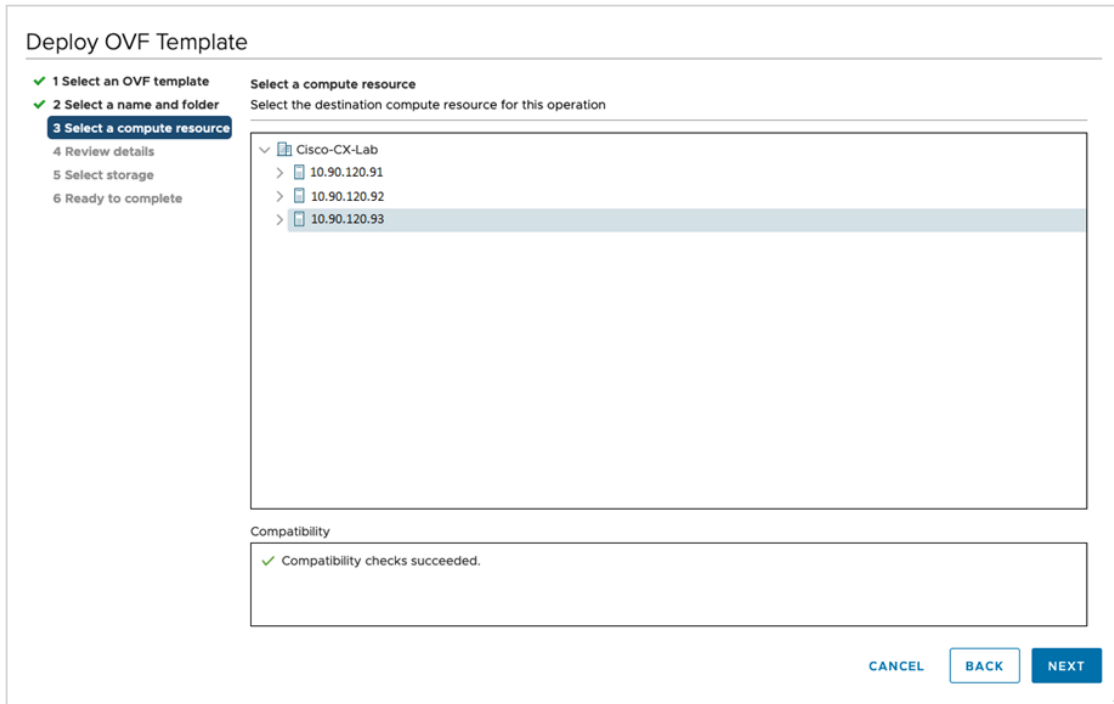
Select a location for the virtual machine.

- rcdn5-spm-vc-01.cisco.com
 - Cisco-CX-Lab
 - rcdn5-spm-dc-01
 - rcdn5-spm-dc-02
 - RTP

CANCEL BACK NEXT

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

Figure 17: Deploy OVF Template - Select a computer resource Window

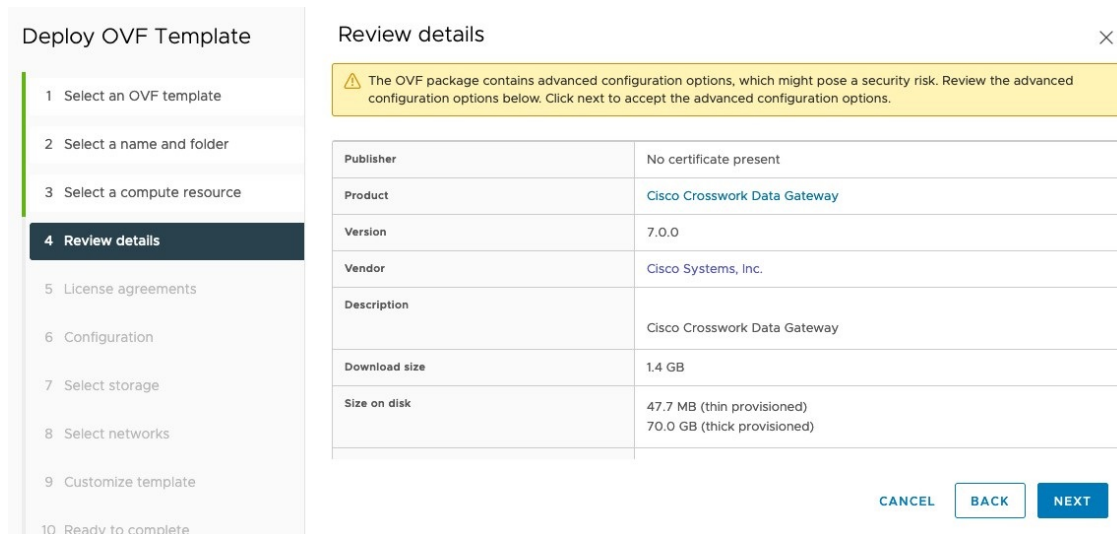
**Step 6**

Click **Next**. The VMware vCenter Server validates the OVA. Network speed determines how long validation takes. When the validation is complete, the wizard moves to **4 Review details**.

Take a moment to review the OVF template to make sure it matches the version you want to install and click **Next**.

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

Figure 18: Deploy OVF Template - Review details Window



Step 7 Click **Next** to go to **5 License agreements**. Review the end-user license agreement, and then click **Accept** if you agree with the conditions. Contact your Cisco representative, if you do not agree with the conditions.

Step 8 Click **Next** to go to **6 Configuration**, as shown in the following figure. Select **Crosswork On-Premise Standard** or **Crosswork On-Premise Extended**. See [Selecting the Crosswork Data Gateway Deployment Type, on page 27](#) for more information.

Figure 19: Deploy OVF Template - Configuration Window

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

Crosswork supports **Crosswork On-Premise Standard** and **Crosswork On-Premise Extended** deployment configuration for on-premises environment.

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. For Crosswork On-Premise Standard deployment, the storage requirement is 70 GB and for Crosswork On-Premise Extended, it is 570 GB.

Figure 20: Deploy OVF Template - Select storage Window

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. From the drop-down, select the network for each vNIC you plan to use. Unused vNIC may remain configured with the default value. For example,

- 2 NIC: Select the appropriate Destination Network for vNIC0 and vNIC1.
- 3 NIC: Select the appropriate Destination Network for vNIC0, vNIC1, and vNIC2.

Figure 21: Deploy OVF Template - Select networks Window

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 networks
Select a destination network for each source network.

Source Network	Destination Network
vNIC3	VM Network
vNIC2	VM Network
vNIC1	VM Network
vNIC0	VM Network

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

Crosswork does not support the **vNIC3** network. Cisco recommends that you do not change the default network settings.

Step 11

Click **Next** to go to **9 Customize template**, with the **Host information** already expanded. Enter the information for the parameters as explained in [Table 26: Crosswork Data Gateway Deployment Parameters and Scenarios, on page 93](#).

Note For larger systems, it is likely that you have more than one data gateway VMs. The data gateway hostname should, therefore, be unique and created in a way that makes identifying a specific VM easy.

Depending on the NIC deployment, note the following:

- For 2 NIC deployments, configure the IP, subnet, and gateway values for vNIC0 and vNIC1. After the data gateway pool is created, the VIP address is assigned as a secondary address on vNIC1.
- For the 3 NIC deployments, configure the IP, subnet, and gateway values for vNIC0 and vNIC1. After the data gateway pool is created, the VIP address is assigned to vNIC2 after data gateway is added to a pool.

Note Values that were not described in detail in [Crosswork Data Gateway Parameters and Deployment Scenarios, on page 92](#) which are not further explained in this section should be left at their default value.

Figure 22: Deploy OVF Template - Customize template > Host information Window

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 10 settings

a. Hostname * Please enter the server's hostname (dg.localdomain)
CDG01

b. Description *
Please enter a short, user friendly description for display in the Crosswork Controller
CDG 01

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

d. Allow Usable RFC 8190 Addresses
If an address for vNIC0, vNIC1, vNIC2, or vNIC3 falls into a usable range identified by RFC 8190 or its predecessors, reject, accept, or request confirmation during initial configuration
Yes

e. Crosswork Data Gateway Private Key URI
Please enter the optional Crosswork Data Gateway private key URI retrieved using SCP (user@host:/path/to/file)

f. Crosswork Data Gateway Certificate File URI

CANCEL BACK NEXT

For creating pools in the VMware environment, select L2 and specify IP addresses for creating the HA pool.

Figure 23: Deploy OVF Template - Customize template > Host information Window > High Availability Network Mode

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

Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted certificate file and private key

Password _____

Confirm Password _____

h. Data Disk Size Data disk size in GB mounted as /opt/dg/appdata
24

i. Amazon Web Services IAM Role Name
Please enter the AWS IAM role name to use for sending VIP updates. This is required when deploying on AWS EC2.

j. High Availability Network Mode
Select the network mode to use with external load balancers. This will determine whether all interfaces require an address.
✓ L2
L3

02. Passphrases 2 settings

a. dg-admin Passphrase *
Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
Password _____
Confirm Password _____

- a. Configure the vNIC Role Assignment based on the number of NICs that you have decided to use. Based on the number of NICs, refer to the following to use the customized template configuration:

Note The default configuration is for 3 NICs deployment.

- See [Deploy OVF Template - Customize Template for 2 vNICs deployment](#).
- See [Deploy OVF Template - Customize Template for 3 vNICs deployment](#).

Figure 24: Deploy OVF Template - Customize Template for 2 vNICs deployment

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: #0070C0; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<table border="1"> <thead> <tr> <th style="background-color: #D9E1F2;">03. vNIC Role Assignment</th> <th style="background-color: #D9E1F2;">7 settings</th> </tr> </thead> <tbody> <tr> <td>a. Default Gateway</td> <td>The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>b. Administration</td> <td>The interface used for SSH access to the VM <input type="text" value="eth0"/></td> </tr> <tr> <td>c. External Logging</td> <td>The interface used to send logs to an external logging server <input type="text" value="eth0"/></td> </tr> <tr> <td>d. Management</td> <td>The interface used for enrollment and other management traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>e. Control</td> <td>The interface used for destination, device, and collection configuration <input type="text" value="eth1"/></td> </tr> <tr> <td>g. Northbound External Data</td> <td>The interface used to send collection data to external destinations <input type="text" value="eth1"/></td> </tr> <tr> <td>h. Southbound Data</td> <td>The interface used collect data from all devices <input type="text" value="eth1"/></td> </tr> </tbody> </table>	03. vNIC Role Assignment	7 settings	a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>	b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>	c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>	d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>	e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>	g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>	h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth1"/>
03. vNIC Role Assignment	7 settings																
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>																
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>																
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>																
d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>																
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>																
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>																
h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth1"/>																

For 3 vNIC deployments, you can leave the settings with the default values.

Figure 25: Deploy OVF Template - Customize Template for 3 vNICs deployment

<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: #0070C0; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<table border="1"> <thead> <tr> <th style="background-color: #D9E1F2;">03. vNIC Role Assignment</th> <th style="background-color: #D9E1F2;">7 settings</th> </tr> </thead> <tbody> <tr> <td>a. Default Gateway</td> <td>The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>b. Administration</td> <td>The interface used for SSH access to the VM <input type="text" value="eth0"/></td> </tr> <tr> <td>c. External Logging</td> <td>The interface used to send logs to an external logging server <input type="text" value="eth0"/></td> </tr> <tr> <td>d. Management</td> <td>The interface used for enrollment and other management traffic <input type="text" value="eth0"/></td> </tr> <tr> <td>e. Control</td> <td>The interface used for destination, device, and collection configuration <input type="text" value="eth1"/></td> </tr> <tr> <td>g. Northbound External Data</td> <td>The interface used to send collection data to external destinations <input type="text" value="eth1"/></td> </tr> <tr> <td>h. Southbound Data</td> <td>The interface used collect data from all devices <input type="text" value="eth2"/></td> </tr> </tbody> </table>	03. vNIC Role Assignment	7 settings	a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>	b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>	c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>	d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>	e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>	g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>	h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth2"/>
03. vNIC Role Assignment	7 settings																
a. Default Gateway	The interface used as the Default Gateway and for DNS and NTP traffic <input type="text" value="eth0"/>																
b. Administration	The interface used for SSH access to the VM <input type="text" value="eth0"/>																
c. External Logging	The interface used to send logs to an external logging server <input type="text" value="eth0"/>																
d. Management	The interface used for enrollment and other management traffic <input type="text" value="eth0"/>																
e. Control	The interface used for destination, device, and collection configuration <input type="text" value="eth1"/>																
g. Northbound External Data	The interface used to send collection data to external destinations <input type="text" value="eth1"/>																
h. Southbound Data	The interface used collect data from all devices <input type="text" value="eth2"/>																

Figure 26: Deploy OVF Template - Customize Template > Controller Settings

Deploy OVF Template

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

16. Controller Settings 11 settings

a. Crosswork Controller IP *

Please enter the hostname, IPv4 address, or IPv6 address of the Crosswork Controller accessible from the Default Gateway role

b. Crosswork Controller Port *

Please enter the port number of the Crosswork Controller

30607

c. Controller Signing Certificate File URI

Please enter the optional Crosswork Controller PEM formatted signing certificate file URI retrieved using SCP (user@host:/path /to/file)

d. Controller SSL/TLS Certificate File URI

Please enter the optional Crosswork Controller PEM formatted SSL/TLS certificate file URI retrieved using SCP (user@host:/path /to/file)

e. Controller Certificate File Passphrase

Please enter the SCP user passphrase to retrieve the Crosswork Controller PEM formatted certificate file

Password

CANCEL BACK NEXT

Step 12 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish**.

Figure 27: Deploy OVF Template - Ready to Complete Window

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

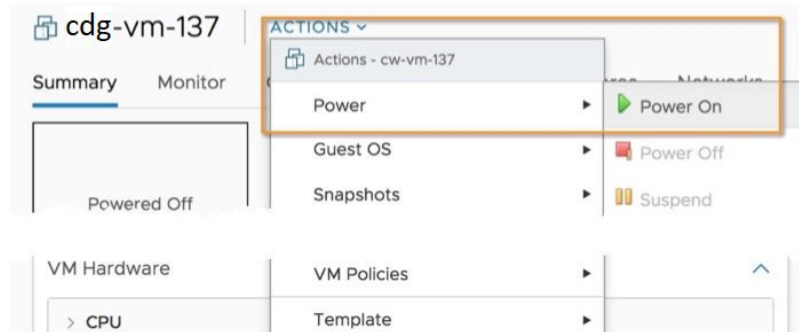
Ready to complete
Click Finish to start creation.

Provisioning type	Deploy from template
Name	CDG02
Template name	dg
Download size	1.4 GB
Size on disk	70.0 GB
Folder	Cisco-CX-Lab
Resource	10.90.147.99
Storage mapping	1
All disks	Datastore: Datastore2; Format: Thick provision lazy zeroed
Network mapping	4
vNIC3	Crosswork-Devices
vNIC2	Crosswork-Devices
vNIC1	Crosswork-Devices
vNIC0	VM Network

CANCEL BACK FINISH

Step 13 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:

Figure 28: Power On Action



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

After you log in, the data gateway should present you with the welcome screen and options menu indicating that the installation completed successfully. For information on how to log in, see [Log in and Log out of the Data Gateway VM, on page 124](#).

Log out and proceed with the post-installation tasks documented in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

Install Crosswork Data Gateway via OVF Tool

You must modify the list of mandatory and optional parameters in the script as per your requirements and run the OVF Tool. Refer to [Table 26: Crosswork Data Gateway Deployment Parameters and Scenarios, on page 93](#) for the list of installation parameters and their default values.



Note The file names mentioned in this topic are sample names and may differ from the actual file names on cisco.com.

Follow these steps to log in to the data gateway VM from SSH:

Before you begin

- In your vCenter data center, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch.

- In the virtual switch, select **Edit > Security**, and ensure that the following DVS port group properties are as shown:
 - Set **Promiscuous mode** as Reject
 - Set **MAC address changes** as Reject

Confirm the settings and repeat the process for each virtual switch used by Crosswork Data Gateway.

-
- Step 1** On the machine where you have the OVFtool installed, use the following command to confirm that you have OVFtool version 4.4:
- ```
ovftool --version
```
- Step 2** Download the OVA and the sample script files from [cisco.com](https://www.cisco.com). For these instructions, we use the file name as **signed-cw-na-dg-7.0.0-26-release-20240918.uefi.ova** and **signed-cw-na-dg-7.0.0-26-release-20240918.uefi.tar.gz**.
- Step 3** Use the following command to extract the files from the tar bundle:
- ```
tar -xvzf cw-na-dg-7.0.0-sample-install-scripts.tar.gz
```
- The file bundle is extracted. It includes the **DG-sample-install-scripts.tar** file and scripts for validating the samples install scripts.
- Step 4** Use the following command to extract the install scripts from the tar bundle:
- ```
tar -xvzf DG-sample-install-scripts.tar.gz
```
- Step 5** Review the contents of the README file to understand the components that are in the package and how they are validated.
- Step 6** Choose the sample script that corresponds to the deployment you plan to use. Cisco provides sample scripts for 1, 2, and 3 vNIC deployments, which you may optimize to meet your needs.
- Sample scripts for 3 vNIC deployments. Customize the script for the type of deployment you have planned. For more information, see the sample scripts:
- [Sample Script for the Crosswork Data Gateway IPv4 Deployment, on page 118](#)
  - [Sample Script for the Crosswork Data Gateway IPv6 Deployment, on page 120](#)
  - [Sample Script for Crosswork Data Gateway Dual-Stack Deployment, on page 121](#)
  - [Sample Script for Crosswork Data Gateway Dual-Stack Deployment with Geo-Redundancy](#)
- Step 7** Use the following command to make the script executable:
- ```
chmod +x {filename}
```
- Step 8** Use the following command to execute the script from the directory where the OVA and script files are stored:
- ```
./{script name} {path and ova file name}
```
- For example:
- ```
./<script name> <Absolute path to signed-cw-na-dg-7.0.0-26-release-20240918.uefi.ova>
```
- Step 9** If the values provided in the script are valid, provide the vCenter user's password when you are prompted.
- If the script fails due to invalid values, a message like the following is displayed:
- ```
admin@nso-576-tsdn-410-aio:~/CDG_Install$./three-nic
/home/admin/CDG_Install/signed-cw-na-dg-7.0.0-26-release-20240918.uefi.ova
```

## Sample Script for the Crosswork Data Gateway IPv4 Deployment

```
Opening OVA source: /home/admin/CDG_Install/signed-cw-na-dg-7.0.0-26-release-20240918.uefi.ova
The manifest does not validate
Warning:
- Line -1: Unsupported value 'firmware' for attribute 'key' on element 'ExtraConfig'.
- Line -1: Unsupported value 'uefi.secureBoot.enabled' for attribute 'key' on element 'ExtraConfig'.
Enter login information for target vi://rcdn5-spm-vc-01.cisco.com/
Username: johndoe
Password: *****
```

After entering the password, monitor the screen or the vCenter console to review the installation progress. For example,

```
Opening VI target: vi://johndoe@rcdn5-spm-vc-01.cisco.com:443/Cisco-sample-sample/host/10.10.100.10
Warning:
- Line 146: Unable to parse 'enableMPTSupport' for attribute 'key' on element 'Config'.
- Line 229: Unable to parse 'vmxnet3.noOprom' for attribute 'key' on element 'Config'.
Deploying to VI: vi://johndoe@rcdn5-spm-vc-01.cisco.com:443/Cisco-sample-sample/host/10.10.100.10
Disk progress: 65%
```

When the installation is complete, the data gateway VM is powered on, is automatically configured based on the settings that you have provided in the script, and registers with the Crosswork cluster.

### What to do next

Log in to the VM. For more information, see [Log in and Log out of the Data Gateway VM, on page 124](#). After you log in, the data gateway should present you with the welcome screen, and options menu indicating that the installation is complete. Log out and proceed with the postinstallation tasks explained in [Crosswork Data Gateway Post-installation Tasks, on page 127](#).

## Sample Script for the Crosswork Data Gateway IPv4 Deployment

Using this example you can deploy Crosswork Data Gateway with the IPv4 address.

Before running the script, ensure that you are using OVFtool version 4.4.x.

```
#!/usr/bin/env bash
DM=""
Disclaimer=""
DNSv4=""
NTP=""
Domain=""
Hostname=""

VM_NAME=""
DeploymentOption=""
DS=""
Host=""
ManagementNetwork=""
DataNetwork=""
DeviceNetwork=""
ManagementIPv4Address=""
ManagementIPv4Netmask=""
ManagementIPv4Gateway=""
DataIPv4Address=""
DataIPv4Netmask=""
DataIPv4Gateway=""
dgadminpwd=""
dgoperpwd=""
ControllerIP=""
ControllerPassword=""
ControllerPort="30607"
```

```

CDG_OVA_PATH=$1

VCENTER_LOGIN="Administrator%40vsphere.local@<vCenter-IP>"
VCENTER_PATH="<vCenter-DC-NAME>/host"

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name=$VM_NAME \
--deploymentOption=${DeploymentOption} \
--net:"vNIC0=${ManagementNetwork}" \
--prop:"ControllerIP=${ControllerIP}" \
--prop:"ControllerPort=${ControllerPort}" \
--prop:"ControllerSignCertChain=cw-admin@${ControllerIP}:/home/cw-admin/controller.pem" \
--prop:"ControllerCertChainPwd=${ControllerPassword}" \
--prop:"Hostname=${Hostname}" \
--prop:"Description=${Disclaimer}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:"Vnic0IPv4Method=Static" \
--prop:"Vnic0IPv4Address=${ManagementIPv4Address}" \
--prop:"Vnic0IPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"Vnic0IPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"NicDefaultGateway=eth0" \
--prop:"NicAdministration=eth0" \
--prop:"NicExternalLogging=eth0" \
--prop:"NicManagement=eth0" \
--prop:"NicControl=eth0" \
--prop:"NicNBExternalData=eth0" \
--prop:"NicSBData=eth0" \
--prop:"dg-adminPassword=${dgadminpwd}" \
--prop:"dg-operPassword=${dgoperpwd}" \
$CDG_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

#####
Append section below for Two NIC deployment
#####
#--net:"vNIC1=${DataNetwork}" \
#--prop:"Vnic1IPv4Method=Static" \
#--prop:"Vnic1IPv4Address=${DataIPv4Address}" \
#--prop:"Vnic1IPv4Gateway=${DataIPv4Gateway}" \
#--prop:"Vnic1IPv4Netmask=${DataIPv4Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth1" \

#####
Append section below for three NIC deployment
#####
#--net:"vNIC1=${DataNetwork}" \
#--net:"vNIC2=${DeviceNetwork}" \
#--prop:"Vnic1IPv4Method=Static" \
#--prop:"Vnic2IPv4Method=Static" \
#--prop:"Vnic1IPv4Address=${DataIPv4Address}" \
#--prop:"Vnic1IPv4Gateway=${DataIPv4Gateway}" \
#--prop:"Vnic1IPv4Netmask=${DataIPv4Netmask}" \

```

```

#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth2" \

```

## Sample Script for the Crosswork Data Gateway IPv6 Deployment

Using this example you can deploy Crosswork Data Gateway with the IPv6 address.

Before running the script, ensure that you are using OVFtool version 4.4.x.

```

#!/usr/bin/env bash
DM=""
Disclaimer=""
DNSv4=""
NTP=""
Domain=""
Hostname=""

VM_NAME=""
DeploymentOption=""
DS=""
Host=""
ManagementNetwork=""
DataNetwork=""
DeviceNetwork=""
ManagementIPv6Address=""
ManagementIPv6Netmask=""
ManagementIPv6Gateway=""
DataIPv6Address=""
DataIPv6Netmask=""
DataIPv6Gateway=""
dgadminpwd=""
dgoperpwd=""
ControllerIP=""
ControllerPassword=""
ControllerPort="30607"

CDG_OVA_PATH=$1

VCENTER_LOGIN="Administrator%40vsphere.local@<vCenter-IP>"
VCENTER_PATH="/host"

ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS --diskMode=$DM
--overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--name=$VM_NAME \
--deploymentOption=${DeploymentOption} \
--net:"vNIC0=${ManagementNetwork}" \
--prop:"ControllerIP=${ControllerIP}" \
--prop:"ControllerPort=${ControllerPort}" \
--prop:"ControllerSignCertChain=cw-admin@${ControllerIP}:/home/cw-admin/controller.pem" \
--prop:"ControllerCertChainPwd=${ControllerPassword}" \
--prop:"Hostname=${Hostname}" \
--prop:"Description=${Disclaimer}" \
--prop:"DNS=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
--prop:"Vnic0IPv6Method=Static" \
--prop:"Vnic0IPv6Address=${ManagementIPv6Address}" \
--prop:"Vnic0IPv6Gateway=${ManagementIPv6Gateway}" \

```



```

--prop:"Vnic0IPv6Netmask=${ManagementIPv6Netmask}" \
--prop:"NicDefaultGateway=eth0" \
--prop:"NicAdministration=eth0" \
--prop:"NicExternalLogging=eth0" \
--prop:"NicManagement=eth0" \
--prop:"NicControl=eth0" \
--prop:"NicNBExternalData=eth0" \
--prop:"NicSBData=eth0" \
--prop:"dg-adminPassword=${dgadminpwd}" \
--prop:"dg-operPassword=${dgoperpwd}" \
$CDG_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

#####
Append section below for Two NIC deployment
#####
#--net:"vNIC1=${DataNetwork}" \
#--prop:"Vnic1IPv6Method=Static" \
#--prop:"Vnic1IPv6Address=${DataIPv6Address}" \
#--prop:"Vnic1IPv6Gateway=${DataIPv6Gateway}" \
#--prop:"Vnic1IPv6Netmask=${DataIPv6Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth1" \

#####
Append section below for three NIC deployment
#####
#--net:"vNIC1=${DataNetwork}" \
#--net:"vNIC2=${DeviceNetwork}" \
#--prop:"Vnic1IPv6Method=Static" \
#--prop:"Vnic1IPv6Address=${DataIPv6Address}" \
#--prop:"Vnic1IPv6Gateway=${DataIPv6Gateway}" \
#--prop:"Vnic1IPv6Netmask=${DataIPv6Netmask}" \
#--prop:"NicDefaultGateway=eth0" \
#--prop:"NicAdministration=eth0" \
#--prop:"NicExternalLogging=eth0" \
#--prop:"NicManagement=eth0" \
#--prop:"NicControl=eth1" \
#--prop:"NicNBExternalData=eth1" \
#--prop:"NicSBData=eth2" \

```

## Sample Script for Crosswork Data Gateway Dual-Stack Deployment

Using this example you can deploy Crosswork Data Gateway with a dual-stack configuration.



**Note** The controller IP address parameter can be a controller VIP or FQDN of controller VIP.

Before running the script, ensure that you are using OVFtool version 4.4.x.

```

#!/usr/bin/env bash
VM_NAME=""
DM=""
DS=""
Vcenter=""
Host=""
DC=""

```

```

CDGIPv4MgmtIpv4="<CDG management IPv4>"
ManagementIPv4Netmask="<Management network IPv4 mask>"
ManagementIPv4Gateway="<Management IPv4 gateway>"
NorthDataIPv4Address="<Northbound data IPv4>"
NorthDataIPv4Netmask="<Northbound data IPv4 mask>"
NorthDataIPv4Gateway="<Northbound data IPv4 gateway>"
SouthDataIPv4Address="<Southbound data IPv4>"
SouthDataIPv4Netmask="<Southbound data IPv4 mask>"
SouthDataIPv4Gateway="<Southbound data IPv4 gateway>"
CDGIPv6MgmtIpv6="<CDG management IPv6>"
ManagementIPv6Netmask="<Management network IPv6 mask>"
ManagementIPv6Gateway="<Management network IPv6 gateway>"
NorthDataIPv6Address="<Northbound data network IPv6 address>"
NorthDataIPv6Netmask="<Northbound data network IPv6 mask>"
NorthDataIPv6Gateway="<Northbound data network IPv6 gateway>"
SouthDataIPv6Address="<Southbound data network IPv6 address>"
SouthDataIPv6Netmask="<Southbound data network IPv6 mask>"
SouthDataIPv6Gateway="<Southbound data network IPv6 gateway>"
PrivateKey="<Private key>"
Disclaimer="Cisco CDG VM for Crosswork Deployment"
DNsv6="<DNS address>"
NTP="<NTP address>"
Domain="<Domain>"
CtrlrCertChainPwd="<Controller certificate password>"
ClientCertChainPwd="<Client certificate password>"
DgAdminPwd="<Data gateway admin password>"
DgOperPwd="<Data gateway operator password>"
ControllerIP="<Controller VIP or FQDN of the controller VIP>"
ControllerPassword="<CNC Password>"
ControllerPort="30607"
cdgDomain="<Data gateway domain>"
SouthDataNetwork="<South data network>"
NorthDataNetwork="<North data network>"

ovftool --version
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv --overwrite --powerOffTarget
 --powerOn --noSSLVerify --allowExtraConfig \
 -ds=${DS} \
 --deploymentOption="onpremise-standard" \
 --diskMode=${DM} \
 --prop:"ControllerIP=${ControllerIP}" \
 --prop:"ControllerPort=${ControllerPort}" \
 --prop:"ControllerSignCertChain=cw-admin@${CwIpv6Mgmt}:/home/cw-admin/controller.pem"
 \
 --prop:"ControllerCertChainPwd=${ControllerPassword}" \
 --name="${VM_NAME}" \
 --prop:"Hostname=${cdgDomain}" \
 --prop:"Description=CDG Base VM for Automation" \
 --prop:"Vnic0IPv6Method=Static" \
 --prop:"Vnic0IPv6Address=${CDGIPv6MgmtIpv6}" \
 --prop:"Vnic0IPv6Netmask=${ManagementIPv6Netmask}" \
 --prop:"Vnic0IPv6Gateway=${ManagementIPv6Gateway}" \
 --prop:"Vnic1IPv6Method=Static" \
 --prop:"Vnic1IPv6Address=${NorthDataIPv6Address}" \
 --prop:"Vnic1IPv6Netmask=${NorthDataIPv6Netmask}" \
 --prop:"Vnic1IPv6Gateway=${NorthDataIPv6Gateway}" \
 --prop:"Vnic0IPv4Method=Static" \
 --prop:"Vnic0IPv4Address=${CDGIPv4MgmtIpv4}" \
 --prop:"Vnic0IPv4Netmask=${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=${DNSv6}" \
--net:"vNIC0=DPortGMgmt12" \
--net:"vNIC1=${NorthDataNetwork}" \
--net:"vNIC2=${SouthDataNetwork}" \
--prop:"NTP=${NTP}" \
--prop:"Domain=${Domain}" \
$CDG_OVA_PATH \
vi://Administrator%40vsphere%2Elocal:Crosswork123%21@$Vcenter/$DC/host/$Host

```

## Sample Script for Crosswork Data Gateway Dual-Stack Deployment with Geo-Redundancy

Using this example you can deploy Crosswork Data Gateway with a dual-stack configuration.

Before running the script, ensure that you are using OVFTool version 4.4.x.

```

#!/usr/bin/env bash
VM_NAME=""
DM=""
DS=""
Vcenter=""
Host=""
DC=""
CDGIPv4MgmtIPv4=""
ManagementIPv4Netmask=""
ManagementIPv4Gateway=""
NorthDataIPv4Address=""
NorthDataIPv4Netmask=""
NorthDataIPv4Gateway=""
SouthDataIPv4Address=""
SouthDataIPv4Netmask=""
SouthDataIPv4Gateway=""
CDGIPv6MgmtIPv6=""
ManagementIPv6Netmask=""
ManagementIPv6Gateway=""
NorthDataIPv6Address=""
NorthDataIPv6Netmask=""
NorthDataIPv6Gateway=""
SouthDataIPv6Address=""
SouthDataIPv6Netmask=""
SouthDataIPv6Gateway=""
PrivateKey=""
Disclaimer="Cisco CDG VM for Crosswork Deployment"
DNSv6=""
NTP=""
Domain=""
CtrlrCertChainPwd=""
ClientCertChainPwd=""
DgAdminPwd=""
DgOperPwd=""
ControllerIP=""
ControllerPassword=""
ControllerPort="30607"
cdgDomain=""
SouthDataNetwork=""
NorthDataNetwork=""

ovftool --version
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv --overwrite --powerOffTarget
--powerOn --noSSLVerify --allowExtraConfig \
--ds=$DS \
--deploymentOption="onpremise-standard" \
--diskMode=$DM \

```

```

--prop:"ControllerIP=${ControllerIP}" \
--prop:"ControllerPort=${ControllerPort}" \
 --prop:"ControllerSignCertChain=cw-admin@${CwIpv6Mgmt}:/home/cw-admin/controller.pem"
\
 --prop:"ControllerCertChainPwd=${ControllerPassword}" \
 --name="${VM_NAME}" \
 --prop:"Hostname=${cdgDomain}" \
 --prop:"Description=CDG Base VM for Automation" \
 --prop:"Vnic0IPv6Method=Static" \
 --prop:"Vnic0IPv6Address=${CDGIPv6MgmtIpv6}" \
 --prop:"Vnic0IPv6Netmask=${ManagementIPv6Netmask}" \
 --prop:"Vnic0IPv6Gateway=${ManagementIPv6Gateway}" \
 --prop:"Vnic1IPv6Method=Static" \
 --prop:"Vnic1IPv6Address=${NorthDataIPv6Address}" \
 --prop:"Vnic1IPv6Netmask=${NorthDataIPv6Netmask}" \
 --prop:"Vnic1IPv6Gateway=${NorthDataIPv6Gateway}" \
 --prop:"Vnic0IPv4Method=Static" \
 --prop:"Vnic0IPv4Address=${CDGIPv4MgmtIpv4}" \
 --prop:"Vnic0IPv4Netmask=${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=${DNSv6}" \
 --net:"vNIC0=DPortGMgmt12" \
 --net:"vNIC1=${NorthDataNetwork}" \
 --net:"vNIC2=${SouthDataNetwork}" \
 --prop:"NTP=${NTP}" \
 --prop:"Domain=${Domain}" \
 $CDG_OVA_PATH \
 vi://Administrator%40vsphere%2Elocal:Crosswork123%21@$Vcenter/$DC/host/$Host

```

## Log in and Log out of the Data Gateway VM

You can log in to the data gateway VM in one of the following ways:

- [Access Crosswork Data Gateway VM from SSH, on page 124](#)
- [Access Crosswork Data Gateway through vCenter, on page 125](#)

To log out from the data gateway VM, see [Log Out of Crosswork Data Gateway VM, on page 126](#).

## 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 causes the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures cause the blocked time to be increased. Each client IP is tracked separately.

Follow these steps to log in 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,

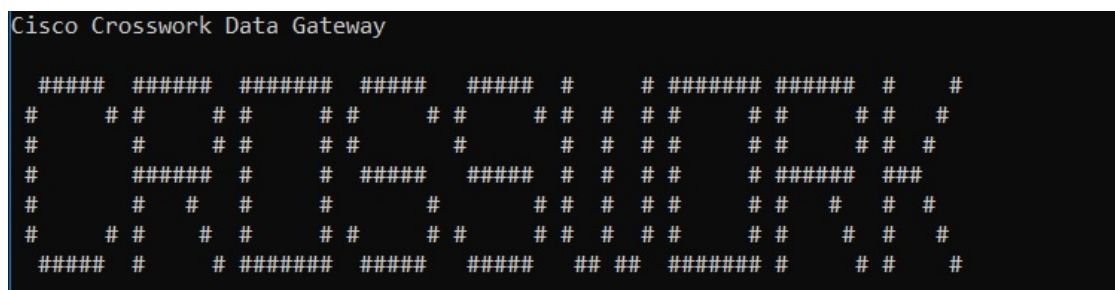
To login as administrator user: `ssh dg-admin@<ManagementNetworkIP>`

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

**Step 2** Provide the corresponding password, which was created during installation process, and press **Enter**.

The Crosswork Data Gateway flash screen opens prompting for password.

*Figure 29: Crosswork screen*



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 reinstall 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 the installation process) and press **Enter**.

The Crosswork Data Gateway flash screen opens prompting for password.

Figure 30: Crosswork screen

```

Cisco Crosswork Data Gateway

#
#
#
###
#
#
#

```

## Log Out of Crosswork Data Gateway VM

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

## 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 data gateway instance in its database and waits for a "first-sign-of-life" from the data gateway VM.

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

To verify if the data gateway VM has enrolled successfully with Cisco Crosswork:

1. Log in to the Cisco Crosswork UI. See [Log into the Cisco Crosswork UI, on page 76](#).
2. Navigate to **Administration > Data Gateway Management**.
3. Click on the **Data Gateway Instances** tab.

All the data gateway VMs that have successfully enrolled with Cisco Crosswork are displayed here.

The initial **Operational State** of data gateway VMs is **Unknown**. During the handshake and image download, the status is **Degraded**. After the handshake is complete, the status is **Not Ready**. While it depends on the bandwidth between the data gateway VMs and Cisco Crosswork, this operation typically takes between 5 to 10 minutes. If it takes longer than the stipulated duration, contact Cisco Customer Experience team for assistance.

For information about the different operational states of the VMs, see the *Overview of Cisco Crosswork Data Gateway* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).



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

**What to do next:**

Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

## Crosswork Data Gateway Post-installation Tasks

After installing Crosswork Data Gateway, configure the timezone of the data gateway VM.

- [Configure Timezone of the Data Gateway VM, on page 127](#)

**What to do next:**

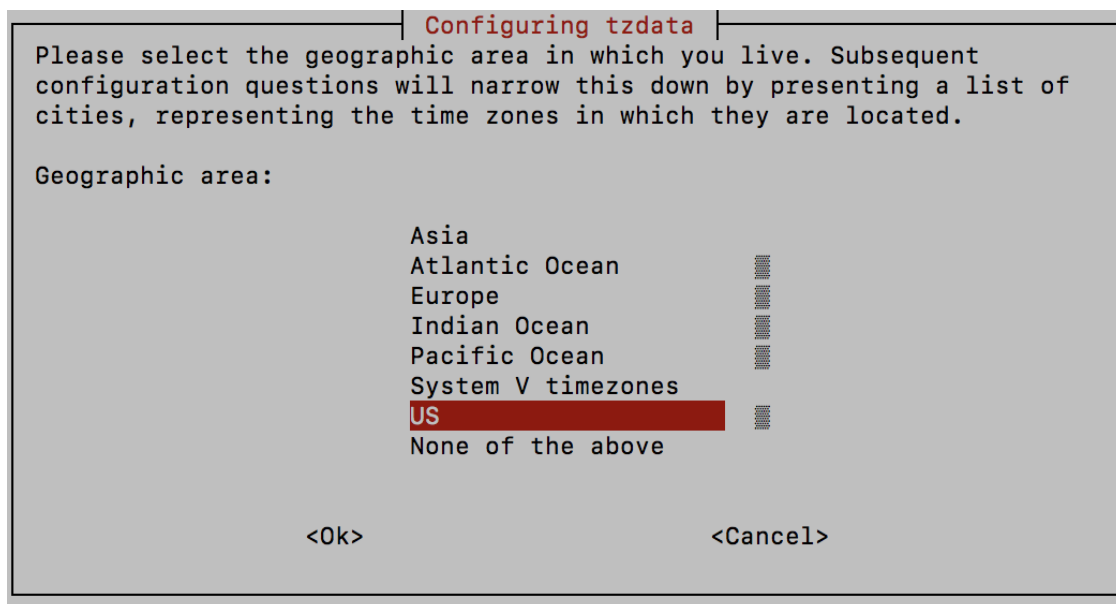
Return to the installation workflow: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)

## Configure Timezone of the Data Gateway VM

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

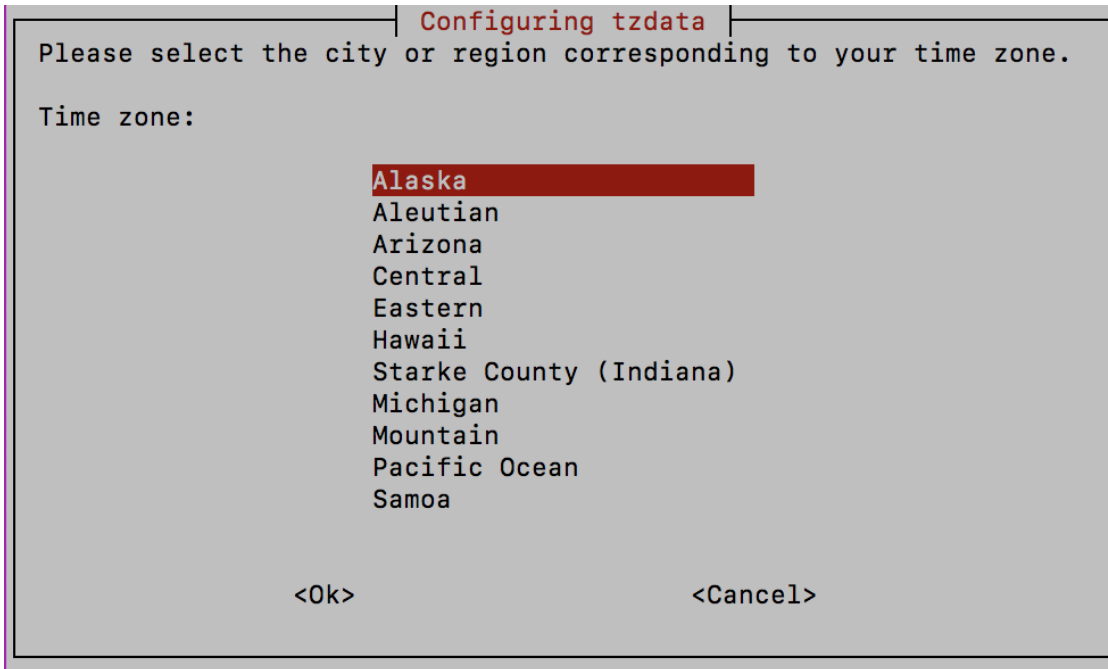
- 
- Step 1** Log in to the data gateway VM.
- Step 2** In the data gateway VM interactive menu, select **3 Change Current System Settings**.
- Step 3** From the menu, select **9 Timezone**.
- Step 4** Select the geographic area in which you live.

*Figure 31: Timezone Settings - Geographic Area Selection*



**Step 5** Select the city or region corresponding to your timezone.

Figure 32: Timezone Settings - Region Selection



**Step 6** Select **OK** to save the settings.

**Step 7** Reboot the data gateway VM so that all processes pick up the new timezone.

**Step 8** Log out of the data gateway VM.

## Troubleshoot Crosswork Data Gateway Installation and Enrollment

If Crosswork Data Gateway fails to autoenroll with Crosswork Network Controller, 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 the *Collect show-tech logs from the Interactive Console* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#). If there are session establishment or certificate-related issues, ensure that the `controller.pem` certificate is uploaded using the Interactive Console.



**Important** When using an IPv6 address, it must be surrounded by square brackets ([1::1]).

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



Table 27: Troubleshooting the Installation or Enrollment

| Issue                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Crosswork Data Gateway cannot be enrolled with Crosswork Network Controller due to an NTP issue, that is, there is a clock-drift between the two.</b></p> <p><b>The clock-drift might be with either Crosswork Data Gateway or Crosswork Network Controller.</b></p> <p><b>Also, on the NTP servers for Crosswork Network Controller and Crosswork Data Gateway, the initial time is set to the ESXi server. For this reason, the ESXi server must also have NTP configured.</b></p> <p><b>Sync the clock time on the host and retry.</b></p> | <ol style="list-style-type: none"> <li>1. Log in to the data gateway VM.</li> <li>2. From the main menu, select <b>5 Troubleshooting &gt; 2 Run show-tech</b>.<br/>Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>.<br/>The show-tech is now encrypted with a file extension ending with .tar.xz.</li> <li>3. Run the following command to decrypt the show-tech file.<br/><pre>openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in &lt;showtech file&gt; -out &lt;decrypted filename&gt; -pass pass:&lt;encrypt string&gt;</pre><br/>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 Crosswork Network Controller.</li> </ol> <ol style="list-style-type: none"> <li>3. From the main menu, go to <b>3 Change Current System Settings &gt; 1 Configure NTP</b>.<br/>Configure NTP to sync with the clock time on the Crosswork Network Controller server and try reenrolling Crosswork Data Gateway.</li> </ol> |

| Issue                                                                                                                                                                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals" due to certificate errors.</b></p>              | <ol style="list-style-type: none"> <li>1. Log in to the data gateway VM.</li> <li>2. From the main menu, select <b>5 Troubleshooting &gt; 2 Run show-tech</b>.<br/><br/>Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>.<br/><br/>The show-tech is now encrypted with a file extension ending with .tar.xz.</li> <li>3. Run the following command to decrypt the show-tech file.<br/><br/> <pre>openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in &lt;showtech file&gt; -out &lt;decrypted filename&gt; -pass pass:&lt;encrypt string&gt;</pre> </li> </ol> <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 reupload the Controller Signing Certificate, as explained in the following steps:</p> <ol style="list-style-type: none"> <li>1. From the main menu, select <b>3 Change Current System Settings &gt; 7 Import Certificate</b>.</li> <li>2. From the <b>Import Certificates</b> menu, select <b>1 Controller Signing Certificate File</b> and click <b>OK</b>.</li> <li>3. Enter the SCP URI for the certificate file and click <b>OK</b>.</li> </ol> |
| <p><b>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.</b></p> | <ol style="list-style-type: none"> <li>1. Reupload the certificate file using the following steps: <ol style="list-style-type: none"> <li>a. From the main menu, select <b>3 Change Current System Settings &gt; 7 Import Certificate</b>.</li> <li>b. From the <b>Import Certificates</b> menu, select <b>1 Controller Signing Certificate File</b> and click <b>OK</b>.</li> <li>c. Enter the SCP URI for the certificate file and click <b>OK</b>.</li> </ol> </li> <li>2. Reboot the data gateway VM: <ol style="list-style-type: none"> <li>a. From the main menu, select <b>5 Troubleshooting</b> and click <b>OK</b>.</li> <li>b. From the Troubleshooting menu, select <b>4 Reboot VM</b> and click <b>OK</b>.</li> <li>c. When the reboot is complete, check if the data gateway's operational status is <b>Up</b>.</li> </ol> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                                         |

| Issue                                                                                                                                                                                                                                                   | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Crosswork Data Gateway goes into Error state</b></p>                                                                                                                                                                                              | <p>For vCenter deployment, check the vNIC values in the OVF template and correct them if required.</p> <p>If you are redeploying the Data Gateway instance, you must first delete the existing instance that is currently in an error state.</p> <p>For more information about</p> <ul style="list-style-type: none"> <li>• deleting the instance and its impact on the collection jobs, see <a href="#">Delete Crosswork Data Gateway Instance from Crosswork Network Controller</a></li> <li>• understanding the impact of redeployment on enrollment, see <a href="#">Redeploy a Crosswork Data Gateway Instance</a>.</li> </ul> |
| <p><b>Crosswork Data Gateway deploys Standard profile instead of Extended profile</b></p>                                                                                                                                                               | <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>                                                                                                                                                                                                                                                                                                                                                                          |
| <p><b>During a Crosswork upgrade, some of the Crosswork Data Gateways may not get upgraded or reenrolled leading to logging multiple error messages in the dg-manager logs.</b></p>                                                                     | <p>Reenroll or redeploy the Crosswork Data Gateways. For more information, see the <a href="#">Redeploy a Crosswork Data Gateway Instance</a> and <a href="#">Re-enroll Crosswork Data Gateway</a> sections in <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a>.</p>                                                                                                                                                                                                                                                                                                                                     |
| <p><b>If a Crosswork Data Gateway instance that was previously attached to Crosswork is now reattached to a different Crosswork version 4.x or 5.0, the operational state of the instance may be Degraded with the robot-astack-influxdb error.</b></p> | <ol style="list-style-type: none"> <li>1. Log in to the Crosswork UI from the SSH.</li> <li>2. Run the Docker executive commands to access the <b>robot-astack-influxdb</b> pod.</li> <li>3. In the pod, navigate to the following directory and delete it:<br/><br/><code>/mnt/datafs/influxdb</code></li> <li>4. Restart the service using the following command:<br/><br/><code>supervisorctl restart all</code></li> </ol>                                                                                                                                                                                                      |
| <p><b>If a data gateway is redeployed without moving the gateway to the Maintenance mode, Crosswork enrollment will be unsuccessful and errors will be logged in the dg-manager and controller-gateway logs.</b></p>                                    | <p>Move the data gateway to the <b>Maintenance</b> mode or manually reenroll the gateway. For more information, see the <a href="#">Re-enroll Crosswork Data Gateway</a> section in <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a>.</p>                                                                                                                                                                                                                                                                                                                                                                |

| Issue                                                                                                                                                             | Action                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Crosswork Data Gateway fails to enroll with Cisco Crosswork when the data gateway is deployed on a single stack while Crosswork is deployed on dual stack.</b> | <p>Redeploy the data gateway on dual stack.</p> <p>For more information, see the <i>Redeploy a Crosswork Data Gateway Instance</i> and <i>Re-enroll Crosswork Data Gateway</i> sections in <i>Cisco Crosswork Network Controller 7.0 Administration Guide</i>.</p> |

## Import Controller Signing Certificate File

The Controller Certificate file is automatically imported after the VM boots. If there is an import failure, the data gateway VM makes several attempts to import the certificate while giving you the option to manually import it.

- You have not specified the **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.
- Cisco Crosswork configuration is in-progress when Crosswork Data Gateway tries to import the Controller Certificate file.
- The Cisco Crosswork Controller IP address is unreachable or incorrect.
- The Cisco Crosswork username or password is incorrect.

Follow these steps to import the controller signing certificate file:

- 
- Step 1** From the 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 the **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 132](#).
- 

## View the Controller Signing Certificate File

Follow these steps to view the signing certificate:

---

**Step 1** From the 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



## PART **III**

# **Install Cisco Crosswork Network Controller on AWS EC2**

- [Installation Prerequisites for AWS EC2, on page 137](#)
- [Install Cisco Crosswork Network Controller on AWS EC2, on page 149](#)







## CHAPTER

# 7

# Installation Prerequisites for AWS EC2

---

This chapter contains the following topics:

- [Overview, on page 137](#)
- [Amazon EC2 Settings, on page 137](#)
- [Host VM Requirements, on page 140](#)
- [Crosswork TCP/UDP Port Requirements, on page 143](#)
- [IP Address Restrictions, on page 147](#)

## Overview

This chapter explains the general (such as VM requirements, port requirements, application requirements, etc.) and platform-specific prerequisites to install each Crosswork component.

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

## Amazon EC2 Settings

This section describes the settings that must be configured to install Crosswork Network Controller on Amazon EC2.

Crosswork can be deployed in Amazon Elastic Compute Cloud (EC2). Amazon EC2 is a web service that provides compute resources in the cloud to host your Crosswork applications.

Crosswork is deployed in Amazon EC2 using CloudFormation (CF) templates. 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.

Installing Crosswork and its components in the AWS environment requires you to review and meet the following prerequisites:



---

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

---

Table 28: AWS Prerequisites and Settings

| Requirement      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VPC and Subnets  | <p>Virtual Private Cloud (VPC) is created and configured with dedicated subnets for Crosswork interfaces (Management and Data) and Crosswork Data Gateway (Management, Data, and Device) interfaces.</p> <p>Direct IP connectivity is required between all subnets.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Endpoints        | <p>An endpoint is created in your VPC with the following parameters:</p> <ul style="list-style-type: none"> <li>• <b>Service name:</b> EC2 service for the region (availability zone) where you are deploying.</li> <li>• <b>Private DNS names:</b> Enabled</li> <li>• <b>Endpoint type:</b> Interface</li> <li>• Under <b>Subnets</b>, specify the management subnet that you intend to use for the installation. If you are using different management subnets for the Crosswork VM and the data gateway VM, ensure that you specify both the management subnets so that the endpoint has access to both the subnets.</li> </ul> <p><b>Important</b> The interface subnet should not conflict with the Network Load Balancer (NLB).</p> <p>For information on how to configure the endpoints, refer to the AWS documentation.</p> |
| IAM role         | <p>A role is created in Identity and Access Management (IAM) with relevant permission policies. An IAM role is an identity that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.</p> <p><b>Note</b></p> <ul style="list-style-type: none"> <li>• The minimum permissions required for a Crosswork role are <b>ec2:DescribeNetworkInterfaces</b>, <b>ec2:AssignPrivateIpAddresses</b> and <b>ec2:UnassignPrivateIpAddresses</b>.</li> <li>• The trust policy for your role must have the "<b>Action</b>": "<b>sts:AssumeRole</b>" condition.</li> </ul>                                                                                                                                                                                                |
| 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 that benefit from low network latency and high network throughput.</p> <p>This requirement is required only for launching the Crosswork cluster instances.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

| Requirement                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP addresses                 | <p><b>Crosswork cluster:</b> When using dual NICs (one for the Management network and one for the Data network), you require 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 management and data Virtual IP (VIP) address.</p> <p>For example, 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><b>Crosswork Data Gateway:</b> IP addresses for Management Traffic and Data Traffic only. IP address for Device Access Traffic is assigned during the data gateway pool creation as explained in the <i>Create a Crosswork Data Gateway Pool</i> section in the <i>Cisco Crosswork Network Controller 7.0 Administration Guide</i>.</p> <ul style="list-style-type: none"> <li>• The IP addresses must be able to reach the gateway address for the network where Crosswork Data Gateway will be installed, or the installation fails.</li> <li>• At this time, your IP allocation is permanent and cannot be changed without redeployment. For more information, contact the Cisco Customer Experience team.</li> </ul> |
| Security group               | A security group must be created and configured to specify which ports or traffic are allowed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Instance type                | <p>The resource profile for your instance deployment. The AWS Instance type should be selected to conform with the VM resource and network requirements listed in <a href="#">Plan Your Deployment, on page 5</a>.</p> <ul style="list-style-type: none"> <li>• <b>Crosswork Cluster:</b> <ul style="list-style-type: none"> <li>• Select <b>m5.4xlarge</b> for demos or lab deployments.</li> <li>• Select <b>m5.8xlarge</b> for production deployments.</li> </ul> </li> <li>• <b>Crosswork Data Gateway</b> (production and lab deployments): <ul style="list-style-type: none"> <li>• <b>Standard</b> - Select <b>m5.4xlarge</b></li> <li>• <b>Extended</b> - Select <b>m5.8xlarge</b></li> </ul> </li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| CloudFormation (CF) template | The CF template (.yaml) files for the Crosswork components that must be uploaded during the installation. For more information, see <a href="#">Extract CF Template Image, on page 149</a> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Route53DomainName            | Domain name configured for Route53 DNS hosted zone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| User data                    | The VM-specific parameters script that must be specified during the manual installation procedure.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Hosted Zone ID               | <p>The Hosted Zone ID must be provided with the domain name (Route53DomainName).</p> <p>The Network Load Balancer (NLB) deployments require a predefined Route53 hosted zone.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

# 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 25](#)
- [Crosswork Data Gateway VM Requirements, on page 27](#)

## Crosswork Cluster VM Requirements

The Crosswork cluster consists of three VMs or nodes operating in a hybrid configuration. This is the minimum configuration necessary to support the applications in a standard network. Additional VMs or nodes in a worker configuration can be added later to scale your deployment, as needed, to match the requirements of your network, or as other applications are introduced (see [Table 1: Crosswork Network Controller packages, on page 6](#) for more information on VM count for each Crosswork Network Controller package). Please consult with the Cisco Customer Experience team for guidance on your deployment to best meet your needs.

The table below explains the network requirements per VM host:

**Table 29: Network Requirements (per VM)**

| Requirement         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Connections | For production deployments, we recommend that you use dual interfaces, one for the Management network and one for the Data network.<br><br>For optimal performance, the Management and Data networks should use links configured at a minimum of 10 Gbps.                                                                                                                                                                                                          |
| 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.<br><br>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.<br><br>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, <a href="http://cisco.com">cisco.com</a> . 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 50 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.

## Crosswork Data Gateway VM Requirements

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

- [Selecting the Crosswork Data Gateway Deployment Type, on page 141](#)
- [Crosswork Data Gateway VM Requirements, on page 141](#)

### Selecting the Crosswork Data Gateway Deployment Type

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

**Table 30: Crosswork Data Gateway deployment types**

| 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                                                                                | On-Premise Extended               |

The VM resource requirements for Crosswork Data Gateway differ based on the deployment type and cannot be modified. If your resource needs change, you must redeploy the data gateway to transition from one type to another.

For information on redeployment, see the *Redeploy a Crosswork Data Gateway VM* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

### Crosswork Data Gateway VM Requirements

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

**Table 31: Crosswork Data Gateway Requirements for on-premise applications**

| Requirement | Description                                                                             |
|-------------|-----------------------------------------------------------------------------------------|
| Data Center | VMware. See <a href="#">Installation Prerequisites for VMware vCenter, on page 19</a> . |

| Requirement  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                    |                                                                                                       |                       |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------|-----------------------|
| Interfaces   | Minimum: 2<br>Maximum: 3<br>Crosswork Data Gateway can be deployed with 2 or 3 interfaces as per the combinations below:<br><b>Note</b> If you use two interfaces on your Crosswork Cluster, then you can use two, or three interfaces on the data gateway as per your network requirements.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                    |                                                                                                       |                       |
|              | <b>No. of NICs</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | <b>vNIC0</b>       | <b>vNIC1</b>                                                                                          | <b>vNIC2</b>          |
|              | 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Management Traffic | <ul style="list-style-type: none"> <li>Control/Data Traffic</li> <li>Device Access Traffic</li> </ul> | —                     |
|              | 3                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Management Traffic | Control/Data Traffic                                                                                  | Device Access Traffic |
|              | <ul style="list-style-type: none"> <li>Management traffic: for accessing the Interactive Console and passing the Control/Data information between servers (for example, a Crosswork application to Crosswork Data Gateway).</li> <li>Control/Data traffic: for data and configuration transfer between Crosswork Data Gateway and Crosswork applications and other external data destinations.</li> <li>Device access traffic: for device access and data collection.</li> </ul> <b>Note</b> Due to security policies, traffic from subnets of a vNIC received on other vNICs is dropped. For example, in a 3 vNIC model setup, all device traffic (incoming and outgoing) must be routed through default vNIC2. Crosswork Data Gateway drops device traffic received over vNIC0 and vNIC1.                                        |                    |                                                                                                       |                       |
| IP Addresses | 1 or 2 IPv4 or IPv6 addresses based on the number of interfaces you choose to use.<br>An additional IP address to be used as the Virtual IP (VIP) address. For each active data gateway, a unique VIP is required.<br>For more information, refer to the <i>Interfaces</i> section in the <a href="#">Table 26: Crosswork Data Gateway Deployment Parameters and Scenarios, on page 93</a> .<br><b>Note</b> In a 3-NIC deployment, you need to provide an IP address for Management interface (vNIC0) and Control/Data interface (vNIC1) during installation. A virtual IP address for Device Access Traffic (vNIC2) is assigned when you create a data gateway to a pool as explained in the <i>Create a Crosswork Data Gateway Pool</i> section in <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a> . |                    |                                                                                                       |                       |

| 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 devices, clients, and servers across your network. Verify that the NTP IP address or host name is reachable on the network else the installation fails.<br><br>Also, the ESXi hosts that run the Crosswork application and Crosswork Data Gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors. |
| DNS Servers                              | The IPv4 or IPv6 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network. Confirm that the DNS servers are reachable on the network before attempting installation. The installation fails if the servers cannot be reached.                                                                                                                                                                                                                                                            |
| DNS Search Domain                        | The search domain you want to use with the DNS servers, for example, <a href="http://cisco.com">cisco.com</a> . You can have only one search domain.                                                                                                                                                                                                                                                                                                                                                                                                                 |
| FQDN                                     | The FQDN addresses are configured for Amazon EC2 deployments.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Internet Control Message Protocol (ICMP) | The Crosswork uses ICMP in the communications with Crosswork Data Gateway. Ensure that the firewall between Crosswork and Crosswork Data Gateway passes this traffic.                                                                                                                                                                                                                                                                                                                                                                                                |

## Crosswork TCP/UDP Port Requirements

### Crosswork Cluster Port Requirements

The following TCP/UDP port numbers need to be allowed through any external firewall or access-list rules deployed by the data center administrator. Depending on the NIC deployment, these ports may be applicable to only one or both NICs.



**Note** Crosswork cluster ports allow bidirectional flow of information.

**Table 32: External Ports used by Crosswork Cluster**

| Port      | Protocol | Used for                                      |
|-----------|----------|-----------------------------------------------|
| 22        | TCP      | Remote SSH traffic                            |
| 179       | TCP      | Calico BGP (Kubernetes)                       |
| 80, 443   | TCP      | Outgoing communication to access the EC2 API. |
| 500, 4500 | UDP      | IPSec                                         |
| 2379/2380 | TCP      | Kubernetes etcd                               |

| Port        | Protocol | Used for                                                                                                                                                                                                                                                                   |
|-------------|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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).<br><br>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)<br><br>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 33: Ports used by other Crosswork components

| Port  | Protocol | Used for                                                                    |
|-------|----------|-----------------------------------------------------------------------------|
| 30602 | TCP      | to monitor the installation (Crosswork Network Controller)                  |
| 30604 | TCP      | Used for Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server. |
| 30607 | TCP      | Crosswork Data Gateway vitals collection                                    |
| 30608 | TCP      | Crosswork Data Gateway gRPC channel with the data gateway VMs               |
| 30609 | TCP      | Used by the Expression Orchestrator (Crosswork Service Health)              |
| 30610 | TCP      | Used by the Metric Scheduler (Crosswork Service Health)                     |
| 30611 | TCP      | Used by the Expression Tracker component (Crosswork Service Health)         |
| 30617 | TCP      | Used for Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server.     |



| Port                | Protocol | Used for                                                                          |
|---------------------|----------|-----------------------------------------------------------------------------------|
| 30620               | TCP      | Used to receive plug-and-play HTTP traffic on the ZTP server.                     |
| 30649               | TCP      | To set up and monitor 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 34: 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 35: Ports to be Opened for Management Traffic**

| Port | Protocol | Used for   | Direction |
|------|----------|------------|-----------|
| 22   | TCP      | SSH server | Inbound   |
| 22   | TCP      | SCP client | Outbound  |

| Port  | Protocol | Used for             | Direction |
|-------|----------|----------------------|-----------|
| 123   | UDP      | NTP Client           | Outbound  |
| 53    | UDP      | DNS Client           | Outbound  |
| 30607 | TCP      | Crosswork Controller | Outbound  |



**Note** SCP port can be tuned.

**Table 36: Ports to be Opened for Device Access Traffic**

| Port                                                                                                | Protocol | Used for                                                                                                                                                                                                                             | Direction |
|-----------------------------------------------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| 161                                                                                                 | UDP      | SNMP Collector                                                                                                                                                                                                                       | Outbound  |
| 1062                                                                                                | UDP      | SNMP Trap Collector<br><b>Note</b> This is the default value. You can change this value after installation from the Cisco Crosswork UI. See <a href="#">Configure Crosswork Data Gateway Global Parameters</a> for more information. | Inbound   |
| 9010                                                                                                | TCP      | MDT Collector                                                                                                                                                                                                                        | Inbound   |
| 22                                                                                                  | TCP      | CLI Collector                                                                                                                                                                                                                        | Outbound  |
| 6514                                                                                                | TLS      | Syslog Collector<br><br>This is the default value. You can change this value after installation from the Cisco Crosswork UI. See <a href="#">Configure Crosswork Data Gateway Global Parameters</a> for more information.            | Inbound   |
| 9898                                                                                                | TCP      |                                                                                                                                                                                                                                      |           |
| 9514                                                                                                | UDP      |                                                                                                                                                                                                                                      |           |
| Site Specific<br>Default ports differ from XR, XE to vendor. Check platform-specific documentation. | TCP      | gNMI Collector                                                                                                                                                                                                                       | Outbound  |

Table 37: Ports to be Opened for Control/Data Traffic

| Port                    | Protocol      | Used for                   | Direction |
|-------------------------|---------------|----------------------------|-----------|
| 30649                   | TCP           | Crosswork Controller       | Outbound  |
| 30993<br>30994<br>30995 | TCP           | Crosswork Kafka            | Outbound  |
| Site Specific           | Site Specific | Kafka and gRPC Destination | Outbound  |

## IP Address Restrictions

Crosswork cluster uses specific IP ranges for internal communications by default, which cannot be used for other devices or purposes within your network. It is recommended to isolate your Crosswork cluster to ensure all communications remain internal and that there are no address space overlaps with external integration points (e.g., connections to devices, external servers, or the NSO server).

If these default IP ranges conflict with your network, collaborate with the Cisco Customer Experience team for assistance in modifying the settings before deployment.



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



**Note** The default values for the `K8sServiceNetwork` (10.96.0.0) and `K8sPodNetwork` (10.244.0.0) parameters can be changed.

Table 38: 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, 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         |

| IP Type | Subnet               | Remarks                                                                                        |
|---------|----------------------|------------------------------------------------------------------------------------------------|
| 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, 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                                                                      |

**What to do next:**

- For installation instructions on VMware, see [Install Crosswork Cluster on VMware vCenter, on page 37](#).
- For installation instructions on AWS EC2, see [Install Cisco Crosswork Network Controller on AWS EC2, on page 149](#).
- For installation instructions for Single VM deployment, see [Install Cisco Crosswork Network Controller on a Single VM, on page 291](#).



## CHAPTER 8

# Install Cisco Crosswork Network Controller on AWS EC2

---

This chapter contains the following topics:

- [Installation Overview, on page 149](#)
- [Extract CF Template Image, on page 149](#)
- [Roles and Policy Permissions, on page 151](#)
- [Configure the CloudFormation \(CF\) Template Parameters, on page 151](#)
- [Install Using Module Deployment Method, on page 164](#)
- [Manage CF Template Deployment, on page 171](#)
- [Accessing the Crosswork UI, on page 173](#)
- [Crosswork Data Gateway Post-installation Tasks, on page 174](#)

## Installation Overview

This section provides an overview of how Cisco Crosswork is installed on Amazon EC2.

Cisco Crosswork uses the CloudFormation (CF) templates to deploy the cluster stacks. The CF 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 CF template with details of the cluster deployment.



---

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

---



---

**Important** The CF templates (.yaml file) provided are samples that must be customized according to your production preferences and executed as per the steps mentioned in this chapter.

---

## Extract CF Template Image

This section explains the procedure to extract and validate the Cisco Crosswork CF template image.




---

**Attention** The file names mentioned in this topic are sample names and may differ from the actual file names in release version.

---

**Step 1** Download the Crosswork CF template package (**signed-CFT-7.0.0\_release700\_47.tar.gz**) from [cisco.com](https://www.cisco.com).

**Step 2** Use the following command to unzip the package:

```
tar -xzvf signed-CFT-7.0.0_release700_47.tar.gz
```

The contents of the package is unzipped to a new directory. This new directory contains the CF template image and files necessary to validate the image.

For example:

```
tar -xzvf signed-CFT-7.0.0_release700_47.tar.gz
x CFT-7.0.0_release700_47.tar.gz
x CFT-7.0.0_release700_47.tar.gz.signature
x README
x CW-CCO_RELEASE.cer
x cisco_x509_verify_release.py3
x cisco_x509_verify_release.py
```

**Step 3** 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 4** Navigate to the directory created in the previous step and use the following command to verify the signature of the installer image:

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

If you are using Python 2.x, use the following command 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
```

For example:

```
python cisco_x509_verify_release.py3 -e CW-CCO_RELEASE.cer -i CFT-7.0.0_release700_47.tar.gz -s
CFT-7.0.0_release700_47.tar.gz.signature -v dgst -sha512
Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of CFT-7.0.0_release700_47.tar.gz using CW-CCO_RELEASE.cer
```

The contents of the package is extracted and validated successfully.

**Step 5** In the directory, locate the `install-cnc-templates` file and follow the instructions provided within its **Description** section. Customize the CF templates in the directory to install Cisco Crosswork on Amazon EC2.

---

**What to do next**

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

## Roles and Policy Permissions

This section describes the roles and the policy permissions that you must have when deploying the CF template on Amazon. For information on how to create and manage the roles, refer to the Amazon documentation.

**Table 39: Amazon EC2 Roles and Actions Assigned to the Roles**

| Role   | Actions                                                                                                                                                                                                                                                                                                                              |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2    | DescribeInternetGateways, DescribeNetworkInterfaces, DescribeImages, DeleteLaunchTemplate, DescribeSubnets, DescribeAccountAttributes, DescribeSecurityGroups, RunInstances, DescribeVpcs, DescribeInstances, CreateNetworkInterface, CreateTags, DescribeKeyPairs, CreateLaunchTemplate, DeleteNetworkInterface, TerminateInstances |
| ELB    | DescribeLoadBalancers, CreateLoadBalancer, ModifyLoadBalancerAttributes, AddTags, DeleteLoadBalancer                                                                                                                                                                                                                                 |
| ELB v2 | DescribeLoadBalancers, CreateLoadBalancer, AddTags, DeleteLoadBalancer, CreateTargetGroup, CreateListener, DeleteListener, DescribeTargetGroups, ModifyLoadBalancerAttributes, DescribeListeners, RegisterTargets, DeleteTargetGroup, ModifyTargetGroupAttributes, DescribeTargetHealth                                              |
| IAM    | CreateNodegroup, DescribeNodegroup, DeleteNodegroup                                                                                                                                                                                                                                                                                  |

## Configure the CloudFormation (CF) Template Parameters

This section explains the important parameters that must be specified for module deployments.

- [CF Template Parameters for Installing Cisco Crosswork Cluster VMs, on page 152](#)
- [CF Template Parameters for Installing Crosswork Data Gateway, on page 158](#)
- [CF Template Parameters for Installing NSO, on page 161](#)
- [CF Template Parameters for Installing Single Hybrid Cluster or Worker Node, on page 162](#)

**Important**

- The parameters that are mandatory for creating the templates are indicated explicitly. Parameters without this indication are optional and are populated with the default values, which you can alter based on your deployment requirement.
- All IP addresses you enter as parameters should be available.

## CF Template Parameters for Installing Cisco Crosswork Cluster VMs

This section describes the parameters that are required for deploying Cisco Crosswork Cluster VMs with 3 hybrid VMs on Amazon EC2. It also describes the Management and Data NLB parameters.

Once you have determined the subnet for your cluster nodes and any other virtual machines you are going to deploy, confirm that there are enough available IP addresses to support the number of VMs (and virtual IP addresses) needed.

**Table 40: Cisco Crosswork Cluster VMs Deployment Parameters**

| Parameter            | Description                                                                                                                                                                                    |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VpcId                | The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.                                                                                                   |
| SecGroup             | Precreated security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to ports 22, 30160:31560.                                  |
| CwSSHPassword        | The SSH password of the Crosswork Network Controller.<br><b>Important</b> We recommend using an external secret store for the password.                                                        |
| CwAmiId              | The Crosswork AMI ID.<br>This is a mandatory parameter.                                                                                                                                        |
| CwMgmtSubnet1Id      | Management subnet for Crosswork VM 1.<br>This is a mandatory parameter.                                                                                                                        |
| CwMgmtSubnet2Id      | Management subnet for Crosswork VM 2.<br>This is a mandatory parameter.                                                                                                                        |
| CwMgmtSubnet3Id      | Management subnet for Crosswork VM 3.<br>This is a mandatory parameter.                                                                                                                        |
| CwMgmtSubnet1Netmask | The first management subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when deploying on a single interface.<br>This is a mandatory parameter.  |
| CwMgmtSubnet2Netmask | The second management subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when deploying on a single interface.<br>This is a mandatory parameter. |
| CwMgmtSubnet3Netmask | The third management subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when deploying on a single interface.<br>This is a mandatory parameter.  |



| Parameter                  | Description                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CwMgmtSubnet1Gateway       | The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode.<br><br>This is a mandatory parameter.                               |
| CwMgmtSubnet2Gateway       | The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode.<br><br>This is a mandatory parameter.                               |
| CwMgmtSubnet3Gateway       | The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode.<br><br>This is a mandatory parameter.                               |
| ManagementVIPName          | Crosswork Management VIP name. For example, dev1-cwmgnt.<br><br>This will be the host name to access the Crosswork cluster.                                                                                                                   |
| DataVIPName                | Crosswork Data VIP name. For example, dev1-cwdata.                                                                                                                                                                                            |
| Route53DomainName          | Domain name used for all Route53 objects.<br><br>This is the DNS domain name for the Crosswork cluster.<br><br>This is a mandatory parameter.                                                                                                 |
| HostedZoneId               | The Hosted Zone ID provided with the domain name (Route53DomainName). The Network Load Balancer (NLB) deployments require a predefined Route53 hosted zone.<br><br>This is a mandatory parameter.                                             |
| UseExternalNLB             | Determines whether to use an external NLB for the Crosswork cluster (multi-AZ or subnet) or a Crosswork VIP (only single AZ or subnet). Options are <code>True</code> or <code>False</code> .<br><br>This is a mandatory parameter.           |
| CwClusterPlacementStrategy | The EC2 instance placement strategy that is valid for single availability zone. Default 'cluster' ensures maximum throughput. Options are: <ul style="list-style-type: none"> <li>• cluster</li> <li>• partition</li> <li>• spread</li> </ul> |

| Parameter               | Description                                                                                                                                                                                                                                                                                     |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CwNodeType              | <p>The Crosswork Node Type for deployment. Options are <code>Hybrid</code> or <code>Worker</code>.</p> <p>A replacement Hybrid node must reuse the same IP addresses as the Hybrid node it is replacing.</p> <p>Default value is <code>Worker</code>.</p> <p>This is a mandatory parameter.</p> |
| InterfaceDeploymentMode | <p>The deployment mode.</p> <p>Options are <code>1</code> to deploy the Management interface or <code>2</code> to deploy the Management and Data interface.</p>                                                                                                                                 |
| CwDataSubnet1Id         | <p>Data subnet of Crosswork VM 1.</p> <p>In a single interface, the deployments happen on the subnet where the Management interface is deployed.</p> <p>This is a mandatory parameter.</p>                                                                                                      |
| CwDataSubnet2Id         | <p>Data subnet of Crosswork VM 2.</p> <p>In a single interface, the deployments happen on the subnet where the Management interface is deployed.</p> <p>This is a mandatory parameter.</p>                                                                                                      |
| CwDataSubnet3Id         | <p>Data subnet of Crosswork VM 3.</p> <p>In a single interface, the deployments happen on the subnet where the Management interface is deployed.</p> <p>This is a mandatory parameter.</p>                                                                                                      |
| CwDataSubnet1Netmask    | <p>The first data subnet netmask in the dotted-decimal form. For example, <code>255.255.255.0</code>. This parameter is ignored when deploying in a single interface mode.</p> <p>This is a mandatory parameter.</p>                                                                            |
| CwDataSubnet1Gateway    | <p>The first default data gateway on the selected data subnet. Typically, the value is the first address on the subnet. This parameter is ignored when deploying in a single interface mode.</p> <p>This is a mandatory parameter.</p>                                                          |
| CwDataSubnet2Netmask    | <p>The second data subnet netmask in the dotted-decimal form. For example, <code>255.255.255.0</code>. This parameter is ignored when deploying in a single interface mode.</p> <p>This is a mandatory parameter.</p>                                                                           |
| CwDataSubnet2Gateway    | <p>The second data subnet netmask in the dotted-decimal form. This parameter is ignored when deploying in a single interface mode.</p> <p>This is a mandatory parameter.</p>                                                                                                                    |

| Parameter            | Description                                                                                                                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CwDataSubnet3Netmask | The third data subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when deploying in a single interface mode.<br><br>This is a mandatory parameter. |
| CwDataSubnet3Gateway | The third data subnet netmask in the dotted-decimal form. This parameter is ignored when deploying in a single interface mode.<br><br>This is a mandatory parameter.                             |
| CwMgmtVIP            | The current Crosswork Management VIP address.                                                                                                                                                    |
| CwDataVIP            | The current Crosswork Data VIP address. When using an external NLB, you can leave this parameter empty.                                                                                          |
| Cw1MgmtIP            | A free address on the management subnet. If not specified, an address is automatically assigned.                                                                                                 |
| Cw1DataIP            | A free address on the data subnet. If not specified, an address is automatically assigned.                                                                                                       |
| Cw2MgmtIP            | A free address on the management subnet. If not specified, an address is automatically assigned .                                                                                                |
| Cw2DataIP            | A free address on the data subnet. If not specified, an address is automatically assigned.                                                                                                       |
| Cw3MgmtIP            | A free address on the management subnet. If not specified, an address is automatically assigned.                                                                                                 |
| Cw3DataIP            | A free address on the data subnet. If not specified, an address is automatically assigned .                                                                                                      |
| OtherCwMgmtIP1       | The Management IP address \#1 of the existing Crosswork node. This is used when the deployment happens with an external load balancer.                                                           |
| OtherCwMgmtIP2       | The Management IP address \#2 of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.                                                 |
| OtherCwDataIP1       | The Data IP address \#1 of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.                                                       |
| OtherCwDataIP2       | The Data IP address \#2 of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.                                                       |

Table 41: Crosswork VM Customization

| Parameter         | Description                                                                                                                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| InstanceType      | The EC2 instance type for the node instances.<br>This is a mandatory parameter.                                                                                                                                                           |
| RunAsSpotInstance | A spot instance.<br>Options are: <ul style="list-style-type: none"> <li>• True: to enable the feature</li> <li>• False: to disable the feature</li> </ul> Default value is False.<br>This is a mandatory parameter.                       |
| DataDiskSize      | Crosswork data disk size. The default is 450 GB and should be fine for most deployments. Enter the default unless otherwise directed by Cisco Customer Experience team.<br>This is a mandatory parameter.                                 |
| K8sServiceNetwork | The network address for the Kubernetes service network. The CIDR range is fixed to '/16'. If not provided, the default will be taken, that is, 10.96.0.0.<br>This is a mandatory parameter.                                               |
| K8sPodNetwork     | The network address for the Kubernetes pod network. The CIDR range is fixed to '/16'.<br>This is a mandatory parameter.                                                                                                                   |
| SkipAutoInstall   | Configures the Skip Auto Install feature. Options are: <ul style="list-style-type: none"> <li>• True: to enable the feature</li> <li>• False: to disable the feature</li> </ul> Default value is False.<br>This is a mandatory parameter. |

Table 42: Cisco Crosswork Cluster Management NLB Deployment Parameters

| Parameter            | Description                                                                                  |
|----------------------|----------------------------------------------------------------------------------------------|
| VpcId                | The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3. |
| CwTargetSubnetIdList | This is a list of the Crosswork management subnets.<br>This is a mandatory parameter.        |
| CwTargetIP1          | This is a Crosswork VM management IP. In this template, this is a mandatory parameter.       |

| Parameter         | Description                                                                            |
|-------------------|----------------------------------------------------------------------------------------|
| CwTargetIP2       | This is a Crosswork VM management IP. In this template, this is a mandatory parameter. |
| CwTargetIP3       | This is a Crosswork VM management IP. In this template, this is a mandatory parameter. |
| Route53DomainName | Domain name used for all Route53 objects.<br>This is a mandatory parameter.            |
| HostName          | The domain name used for all Route53 objects.<br>This is a mandatory parameter.        |
| HostedZoneId      | The hosted zone ID.<br>This is a mandatory parameter.                                  |

**Table 43: Data NLB Deployment Parameters**

| Parameter            | Description                                                                                      |
|----------------------|--------------------------------------------------------------------------------------------------|
| VpcId                | The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.     |
| CwTargetSubnetIdList | The first management subnet for the Crosswork VMs.<br>This is a mandatory parameter.             |
| CwTargetIP1          | A free address on the management subnet. If not specified, an address is automatically assigned. |
| CwTargetIP2          | A free address on the management subnet. If not specified, an address is automatically assigned. |
| CwTargetIP3          | A free address on the management subnet. If not specified, an address is automatically assigned. |
| Route53DomainName    | Domain name used for all Route53 objects.<br>This is a mandatory parameter.                      |
| HostName             | The domain name used for all Route53 objects.<br>This is a mandatory parameter.                  |
| HostedZoneId         | The hosted zone ID.<br>This is a mandatory parameter.                                            |

## CF Template Parameters for Installing Crosswork Data Gateway

This section describes the parameters that are required when creating the data gateway control plane, node, pool, and other important containers. It also has parameters that are required for creating EC2 Crosswork Data Gateway NLB stack.

**Table 44: Crosswork Data Gateway Deployment Parameters**

| Parameter               | Description                                                                                                                                                                                                                                                                        |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| AwsIamRole              | The Amazon Web Services IAM role name for the EC2 VIP update.                                                                                                                                                                                                                      |
| VpcId                   | The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.                                                                                                                                                                                       |
| SecGroup                | A pre-created security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to all ports that Crosswork, NSO, Crosswork Data Gateway, and IOS-XR uses.                                                                  |
| CDGSSHPassword          | The SSH password to be configured on the data gateway node.                                                                                                                                                                                                                        |
| CDGOperPassword         | The password to be configured on data gateway for Dg-Oper user.                                                                                                                                                                                                                    |
| CDGAmiId                | The Crosswork Data Gateway AMI ID.                                                                                                                                                                                                                                                 |
| InstanceType            | The EC2 instance type for the node instances.<br>This is a mandatory parameter.                                                                                                                                                                                                    |
| CNCControllerIP         | Host address or name of the data gateway controller. In a multi-AZ deployment, this value must be the name.<br>This is a mandatory parameter.                                                                                                                                      |
| CNCControllerPassword   | The cw-admin user password used to access Crosswork or CNC Controller.                                                                                                                                                                                                             |
| InterfaceDeploymentMode | Crosswork Data Gateway deployment mode.<br>The options are: <ul style="list-style-type: none"> <li>• 1: to deploy all the interfaces.</li> <li>• 2: to deploy the Management and Data interfaces.</li> <li>• 3: to deploy the Management, Data, and Control interfaces.</li> </ul> |
| CDGInterface0IPAddress  | A free IP address on the subnet. If set to 0.0.0.0, the IP address is automatically allocated.<br>This is a mandatory parameter.                                                                                                                                                   |
| CDGInterface0SubnetId   | The first interface subnet for the data gateway VM.                                                                                                                                                                                                                                |
| CDGInterface0Gateway    | The default gateway on the selected subnet. Typically, the first address on the subnet.                                                                                                                                                                                            |

| Parameter                  | Description                                                                                                                                                                                        |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CDGInterface0SubnetNetmask | The first interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0.<br><br>This is a mandatory parameter.                                                                   |
| CDGInterface1IPAddress     | A free IP address on the first subnet. If set to 0.0.0.0, the IP address is automatically allocated.<br><br>This is a mandatory parameter.                                                         |
| CDGInterface1SubnetId      | The second interface subnet for the data gateway. The subnet must be in the same availability zone as the <code>CDGInterface0SubnetId</code> .                                                     |
| CDGInterface1Gateway       | The second interface default gateway on the selected subnet. Typically, the first address on the subnet.<br><br>This is a mandatory parameter.                                                     |
| CDGInterface1SubnetNetmask | The second interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when dual interface mode is not used.<br><br>This is a mandatory parameter.  |
| CDGInterface2IPAddress     | A free IP address on the second subnet. If set to 0.0.0.0, the IP address is automatically allocated.<br><br>This is a mandatory parameter.                                                        |
| CDGInterface2SubnetId      | The third interface subnet for the data gateway VM. The subnet must be in the same availability zone as the <code>CDGInterface0SubnetId</code> .                                                   |
| CDGInterface2Gateway       | The third interface default gateway on the selected subnet. Typically, the first address on the subnet.<br><br>This is a mandatory parameter.                                                      |
| CDGInterface2SubnetNetmask | The third interface subnet netmask in the dotted-decimal form. For example, 255.255.255.0. This parameter is ignored when triple interface mode is not used.<br><br>This is a mandatory parameter. |
| CNCControllerIP            | Host address of the data gateway controller.                                                                                                                                                       |

| Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| HANetworkMode       | <p>The data gateway HA mode.</p> <p>The pool mode options are:</p> <ul style="list-style-type: none"> <li>• L2: Use this option when you specify IP addresses for creating the HA pool.</li> <li>• L3: Use this option when you specify FQDN for creating the HA pool and for multi-subnet deployment.</li> </ul> <p>For information on the pool types, refer to the <i>Create a Cisco Crosswork Data Gateway Pool</i> section in <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a>.</p> <p>This is a mandatory parameter.</p> |
| DataDiskSize        | <p>Size of the Crosswork data disk. The minimum size is 20. Default size is 50.</p> <p>This is a mandatory parameter.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| CDGProfile          | <p>The deployment profile of data gateway.</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• Extended</li> </ul> <p>This is a mandatory parameter.</p>                                                                                                                                                                                                                                                                                                                                                                                    |
| CdgInstanceHostname | The data gateway instance name, for example CDG-01.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| az_id               | The physical location of Availability Zone 1 and 2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| region_id           | The physical location of the data gateway VM.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| site_location       | <p>The location of the primary and second Crosswork sites.</p> <p>During enrollment, Crosswork sends this value to cdg-manager to preset the cluster affiliation of the instance.</p>                                                                                                                                                                                                                                                                                                                                                                    |

**Table 45: Crosswork Data Gateway and Network Load Balancer (NLB) Stack Parameters**

| Parameter | Description                                                                      |
|-----------|----------------------------------------------------------------------------------|
| VpcId     | <p>The VPC ID of the worker instances.</p> <p>This is a mandatory parameter.</p> |
| SubnetId1 | <p>The management ID of subnet 1.</p> <p>This is a mandatory parameter.</p>      |
| SubnetId2 | <p>The management ID of subnet 2.</p> <p>This is a mandatory parameter.</p>      |



| Parameter       | Description                                                                                                          |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| DomainName      | The domain name.<br>This is a mandatory parameter.                                                                   |
| HostedZoneId    | The hosted zone ID.<br>This is a mandatory parameter.                                                                |
| CdgPoolHostname | Name of the Route53 record.<br>This is a mandatory parameter.                                                        |
| CdgTargetIP1    | The IP address 1 of the Management node.<br>In the event of a single data gateway, one target IP must be configured. |
| CdgTargetIP2    | The IP address 2 of the Management node.                                                                             |
| LBIPAddress1    | The first LB IP address on subnet.<br>This is a mandatory parameter.                                                 |
| LBIPAddress2    | The second LB IP address on subnet.<br>This is a mandatory parameter.                                                |

## CF Template Parameters for Installing NSO

This section describes the parameters that are required for deploying NSO on Amazon EC2.

**Table 46: NSO Deployment Parameters**

| Parameter              | Description                                                                                                                                                      |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VpcId                  | The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.                                                                     |
| SecGroup               | A pre-created security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to ports 22, 30160:31560. |
| NSOSubnetId            | The subnet for the NSO VM.                                                                                                                                       |
| KeyName                | Name of an existing EC2 Key Pair to enable SSH access to the instance.                                                                                           |
| NSOAmiId               | The NSO AMI ID.<br>This is a mandatory parameter.                                                                                                                |
| NSOInterface0IPAddress | A free IP address on the second subnet. If set to 0.0.0.0, the IP address is automatically allocated.<br>This is a mandatory parameter.                          |

| Parameter    | Description                                                                     |
|--------------|---------------------------------------------------------------------------------|
| InstanceType | The EC2 instance type for the node instances.<br>This is a mandatory parameter. |

## CF Template Parameters for Installing Single Hybrid Cluster or Worker Node

This section describes the parameters that are required for deploying a single cluster node (Hybrid or Worker).



### Attention

- A replacement hybrid node must reuse the same IP addresses as the hybrid VM it is replacing.
- As you will be adding another node (worker or hybrid) to the existing cluster determine the subnet that is being used and find an additional available IP on that subnet.

**Table 47: Single Hybrid Cluster or Worker Cisco Crosswork Nodes Deployment Parameters**

| Parameter         | Description                                                                                                                                                      |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| VpcId             | The virtual private cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.                                                                     |
| SecGroup          | A pre-created security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to ports 22, 30160:31560. |
| EC2ENIRole        | Existing role name for the Crosswork cluster. The role must permit EC2 access.                                                                                   |
| CwAmiId           | The Crosswork AMI ID.<br>This is a mandatory parameter.                                                                                                          |
| CwSSHPassword     | The SSH password of the Crosswork Network Controller.<br><b>Important</b> We recommend using an external secret store for the password.                          |
| InstanceType      | The EC2 instance type for the node instances.<br>This is a mandatory parameter.                                                                                  |
| ManagementVIPName | Crosswork Management VIP name. For example, dev1-cwmgmt.                                                                                                         |
| DataVIPName       | Crosswork Data VIP name. For example, dev1-cwdata.                                                                                                               |
| Route53DomainName | Domain name used for all Route53 objects.<br>This is a mandatory parameter.                                                                                      |

| Parameter           | Description                                                                                                                                                                                                                                  |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| UseExternalNLB      | Determines whether to use an external NLB for the Crosswork cluster (multi-AZ or subnet) or a Crosswork VIP (only single AZ or subnet). Options are <code>True</code> or <code>False</code> .<br><br>This is a mandatory parameter.          |
| CwMgmtSubnetId      | The management subnet for the Crosswork VMs.                                                                                                                                                                                                 |
| CwMgmtSubnetNetmask | The management subnet netmask in dotted decimal form. For example, 255.255.255.0. This parameter is ignored when deploying in a single interface mode.<br><br>This is a mandatory parameter.                                                 |
| CwDataSubnetGateway | The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode.<br><br>This is a mandatory parameter.                              |
| CwDataSubnetId      | The data subnet for the Crosswork VMs.                                                                                                                                                                                                       |
| CwDataSubnetNetmask | The data subnet netmask in dotted decimal form. For example, 255.255.255.0. This parameter is ignored when deploying in a single interface mode.<br><br>This is a mandatory parameter.                                                       |
| CwDataSubnetGateway | The data default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed on single interface mode.<br><br>This is a mandatory parameter.                                    |
| CwNodeType          | The Crosswork Node Type for deployment. Options are <code>Hybrid</code> or <code>Worker</code> .<br><br>A replacement Hybrid node must reuse the same IP addresses as the Hybrid node it is replacing.<br><br>This is a mandatory parameter. |
| DataDiskSize        | Crosswork data disk size. The default is 450 (in GB) and should be fine for most deployments. Enter the default unless otherwise directed by Cisco Customer Experience team.<br><br>This is a mandatory parameter.                           |
| K8sServiceNetwork   | The network address for the Kubernetes service network. The CIDR range is fixed to '/16'. If not provided, the default (10.96.0.0) is taken.                                                                                                 |
| K8sPodNetwork       | The network address for the Kubernetes pod network. The CIDR range is fixed to '/16'. If not provided, the default (10.244.0.0) is taken.                                                                                                    |

Table 48: Optional VM parameters

| Parameters     | Description                                                                                                                                         |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| CwMgmtVIP      | The current Crosswork Management VIP address.                                                                                                       |
| CwDataVIP      | The current Crosswork Data VIP address. When using an external NLB, you can leave this parameter empty.                                             |
| CwlMgmtIP      | A free address on the management subnet. If not specified, an address is automatically assigned.                                                    |
| CwlDataIP      | A free address on the data subnet. If not specified, an address is automatically assigned.                                                          |
| OtherCwMgmtIP1 | The first Management IP address of the existing Crosswork node. This is used when the deployment happens with an external load balancer.            |
| OtherCwMgmtIP2 | The second Management IP address of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer. |
| OtherCwDataIP1 | The first Data IP address of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.        |
| OtherCwDataIP2 | The second Data IP address of the existing Crosswork node. This parameter is used when the deployment happens with an external load balancer.       |

## Install Using Module Deployment Method

The module-based deployment procedures involve deploying each resource separately. Each resource has its own template file, which can be used to deploy them individually. For more information, see the following topics:

- [Install Cisco Crosswork Cluster on Amazon EC2, on page 164](#)
- [Install Crosswork Data Gateway on Amazon EC2, on page 165](#)
- [Install Cisco NSO on Amazon EC2, on page 170](#)
- [Deploy an Additional Crosswork Cluster Node, on page 171](#)

## Install Cisco Crosswork Cluster on Amazon EC2

This section provides an overview of how Cisco Crosswork cluster is installed on Amazon EC2.

Cisco Crosswork uses a set of CF templates to deploy Crosswork cluster.

### Crosswork Cluster Deployment Workflow

The Crosswork cluster deployment procedure involves deploying various Crosswork resources using the corresponding YAML files.

**Table 49: Resources Deployed During Crosswork Cluster Deployment**

| Resource       | Description                                                                                                                             |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| EC2 Cluster    | The main stack ( <b>cw-cluster.yaml</b> ) which will deploy other nested stacks for creating EC2 CW NLBs.                               |
| Management NLB | The <b>cw-mgmt-nlb.yaml</b> file creates Network Load Balancer, Target Groups, Listeners and Route53Record for EC2 CW Management Nodes. |
| Data NLB       | The <b>cw-data-nlb.yaml</b> file creates Network Load Balancer, Target Groups, Listeners and Route53Record for EC2 CW Data Nodes        |

### Installation Parameters

For list of important parameters that you must specify in the CF templates that are used to deploy Crosswork cluster, see [CF Template Parameters for Installing Cisco Crosswork Cluster VMs, on page 152](#). Crosswork cluster is deployed on Amazon EC2 based on the parameters specified in the templates.



**Note** Once you have determined the subnet for your cluster nodes and any other virtual machines you are going to deploy, confirm that there are enough available IP addresses to support the number of VMs (and virtual IP addresses) needed.

### Deploy the CF Templates

You can install the Crosswork cluster on Amazon EC2 by customizing the CF templates. For the list of CF templates that are used for Crosswork cluster deployment, see [Crosswork Cluster Deployment Workflow, on page 164](#).

For instructions on how to deploy the CF templates on Amazon EC2, see [Deploy a CF Template, on page 172](#).

### Verify the Installation

Verify that the Crosswork cluster installation is successful by following the steps in [Monitor the Installation, on page 173](#).

### Deploy an Additional Crosswork Cluster Node

For instructions on how to deploy an additional worker/hybrid node on the Crosswork cluster, see [Deploy an Additional Crosswork Cluster Node, on page 171](#).

### What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

## Install Crosswork Data Gateway on Amazon EC2

This section provides an overview of how Crosswork Data Gateway is installed on Amazon EC2.

## Crosswork Data Gateway Deployment Workflow

Crosswork Data Gateway deployment procedure involves deploying various Crosswork resources using the corresponding YAML files.

The main file **cdg-stack-ec2.yaml** deploys the stacks for a single data gateway NLB (**cdg-nlb.yaml**) and two data gateways (**cdg.yaml**).

- An additional data gateway VM to the data gateway high availability pool is deployed using the **cdg.yaml** file. For each additional VM deployment, you must repeat the deployment procedure.
- An additional NLB and data gateway high availability pool is deployed using the **cdg-nlb.yaml** file.

The following table provides information about the components are installed:

**Table 50: Resources Deployed During Crosswork Data Gateway Deployment**

| Resource                                     | Description                                                                                                                                                   |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2 Crosswork Data Gateway                   | The resources related to EC2 node are created by deploying the <b>cdg.yaml</b> file.                                                                          |
| Crosswork Data Gateway Network Load Balancer | The EC2 NLB components (target groups, network load balancer, data listeners, and NLB route 53 record) are created by deploying the <b>cdg-nlb.yaml</b> file. |

### Installation Parameters

For list of important parameters in the Crosswork Data Gateway CF templates, see [CF Template Parameters for Installing Crosswork Data Gateway, on page 158](#).

The data gateway is deployed on Amazon EC2 based on the parameters specified in the CF templates. For list of CF templates that are used for data gateway deployment, see [#unique\\_100 unique\\_100\\_Connect\\_42\\_section\\_rpb\\_cpy\\_pxb](#).

### Deploy the CF Templates

For instructions on how to deploy the CF templates on Amazon EC2, see [Deploy a CF Template, on page 172](#).




---

**Note** Amazon EC2 mandates entering an IP address for the vNIC2 interface when data gateway is deployed using 3 NICs. This is an AWS EC2 requirement and not imposed by Crosswork.

---

### Verify the Installation

Verify that the Crosswork Data Gateway installation is successful by following the steps in [Monitor the Installation, on page 173](#).

### What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

## Auto-Configuration for Deploying Crosswork Data Gateway

The auto-configuration procedure discovers the configuration parameters that are missing, and it automatically defines the mandatory parameters to install Base VM. The configuration parameters are passed using the Dynamic Host Configuration Protocol (DHCP) framework. In the Day 0 configuration, the auto-configuration mechanism defines only the essential parameters with the default values.

A default password is provided during the auto-configuration to comply with the security policies. On the initial log in, the dg-admin and dg-oper users must change the default password. The Crosswork Data Gateway services are inactive until the default password is changed.

The auto-configuration process supports the default 3 NIC deployment. In particular, only eth0 is configured for the Management network.

The DHCP interaction takes place over the eth0 interface. The auto-configuration procedure uses the default values stored on the DHCP server. After Base VM is deployed, you can configure or modify the default values using the Interactive Console. For more information about the console, see [Cisco Crosswork Network Controller 7.0 Administration Guide](#).




---

**Important** The auto-configuration mechanism is not supported for deploying data gateway on the VMware platform.

---

### How does Auto-configuration Work

1. Install the Base VM.
2. Crosswork Data Gateway searches for the Day 0 `config.txt` file.
3. If the `config.txt` file is not found, the Crosswork Data Gateway starts the auto-configuration process, and the required parameters are set with the default values. In the background, the Crosswork Data Gateway sends a request to the DHCP server to obtain the default parameter values. Once the response is received, the parameters are configured accordingly.

### Parameters used during Auto-Configuration

The auto-configuration utility configures the following parameters with the default values. For more information about these parameters, see [Crosswork Data Gateway Parameters and Deployment Scenarios](#), on page 92.

**Table 51: Cisco Crosswork Data Gateway Mandatory Deployment Parameters**

| Name                      | Parameter      | Default Value                            |
|---------------------------|----------------|------------------------------------------|
| AllowRFC8190              | AllowRFC8190   | The default value is Yes.                |
| Auditd Server Port        | AuditdPort     | The default port is 60.                  |
| Crosswork Controller Port | ControllerPort | The default port is 30607.               |
| Description               | Description    | The default value is CDG auto configure. |

| Name                                 | Parameter          | Default Value                                                                                                                                                                 |
|--------------------------------------|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dg-admin Passphrase                  | dg-adminPassword   | The default password is <code>changeme</code> .<br>Reset the default value with the password that you have chosen for the dg-admin user.<br>Password must be 8-64 characters. |
| dg-oper Passphrase                   | dg-operPassword    | The default password is <code>changeme</code> .<br>Reset the default value with the password you have chosen for the dg-oper user.<br>Password must be 8-64 characters.       |
| Data Disk Size                       | DGAppdataDisk      | The default value of this parameter is 5.                                                                                                                                     |
| DNS Address                          | DNS                | The default values of this parameter are<br><code>208.67.222.222</code><br><code>208.67.220.220</code>                                                                        |
| DNS Security Extensions              | DNSSEC             | The default value of this parameter is <code>False</code> .                                                                                                                   |
| DNS over TLS                         | DNSTLS             | The default value of this parameter is <code>False</code> .                                                                                                                   |
| DNS Search Domain                    | Domain             | The default value of this parameter is <code>localdomain</code> .                                                                                                             |
| Crosswork Data Gateway HA mode       | HANetworkMode      | The default value of this parameter is <code>L2</code> .                                                                                                                      |
| Hostname                             | Hostname           | The default value of this parameter is <code>dg-&lt;eth0 address&gt;</code> .<br>Where <code>&lt;eth0-address&gt;</code> is the address of vNIC0.                             |
| Link-Local Multicast Name Resolution | LLMNR              | The default value of this parameter is <code>False</code> .                                                                                                                   |
| Multicast DNS                        | mDNS               | The default value of this parameter is <code>False</code> .                                                                                                                   |
| NicAdministration                    | NicAdministration  | The default value of this parameter is <code>eth0</code> .                                                                                                                    |
| NicControl                           | NicControl         | The default value of this parameter is <code>eth1</code> .                                                                                                                    |
| NicDefaultGateway                    | NicDefaultGateway  | The default value of this parameter is <code>eth0</code> .                                                                                                                    |
| NicExternalLogging                   | NicExternalLogging | The default value of this parameter is <code>eth0</code> .                                                                                                                    |
| NicManagement                        | NicManagement      | The default value of this parameter is <code>eth0</code> .                                                                                                                    |
| NicNBExternalData                    | NicNBExternalData  | The default value of this parameter is <code>eth1</code> .                                                                                                                    |
| NicNBSystemData                      | NicNBSystemData    | The default value of this parameter is <code>eth1</code> .                                                                                                                    |



| Name                     | Parameter             | Default Value                                                                                                       |
|--------------------------|-----------------------|---------------------------------------------------------------------------------------------------------------------|
| NicSBData                | NicSBData             | The default value of this parameter is the last active interface such as eth0 for 1-NIC deployment, eth1 for 2-NIC. |
| NTPv4 Servers            | NTP                   | The default values of this parameter are<br>162.159.200.1<br>65.100.46.164<br>40.76.132.147<br>104.131.139.195      |
| Use NTPv4 Authentication | NTPAuth               | The default value of this parameter is <code>False</code> .                                                         |
| Profile                  | Profile               | The default value of this parameter is <code>Standard</code> .                                                      |
| Syslog Multiserver Mode  | SyslogMultiserverMode | The default value of this parameter is <code>Simultaneous</code> .                                                  |
| Syslog Server Port       | SyslogPort            | The default value of this parameter is <code>514</code> .                                                           |
| Syslog Server Protocol   | SyslogProtocol        | The default value of this parameter is <code>UDP</code> .                                                           |
| Use Syslog over TLS      | SyslogTLS             | The default value of this parameter is <code>False</code> .                                                         |
| Use Remote Auditd Server | UseRemoteAuditd       | The default value of this parameter is <code>False</code> .                                                         |
| Use Remote Syslog Server | UseRemoteSyslog       | The default value of this parameter is <code>False</code> .                                                         |
| vNIC IPv4 Method         | Vnic0IPv4Method       | The default value of this parameter is <code>DHCP</code> .                                                          |
| vNIC IPv4 Skip Gateway   | Vnic0IPv4SkipGateway  | The default value of this parameter is <code>False</code> .                                                         |
| vNIC IPv6 Method         | Vnic0IPv6Method       | The default value is <code>None</code> .                                                                            |
| vNIC IPv6 Skip Gateway   | Vnic0IPv6SkipGateway  | The default value is <code>False</code> .                                                                           |
| vNIC IPv4 Method         | Vnic1IPv4Method       | The default value is <code>DHCP</code> .                                                                            |
| vNIC IPv4 Skip Gateway   | Vnic1IPv4SkipGateway  | The default value is <code>False</code> .                                                                           |
| vNIC IPv6 Method         | Vnic1IPv6Method       | The default value is <code>None</code> .                                                                            |
| vNIC IPv6 Skip Gateway   | Vnic1IPv6SkipGateway  | The default value is <code>False</code> .                                                                           |
| vNIC IPv4 Method         | Vnic2IPv4Method       | The default value is <code>DHCP</code> .                                                                            |
| vNIC IPv4 Skip Gateway   | Vnic2IPv4SkipGateway  | The default value is <code>False</code> .                                                                           |
| vNIC IPv6 Method         | Vnic2IPv6Method       | The default value is <code>None</code> .                                                                            |
| vNIC IPv6 Skip Gateway   | Vnic2IPv6SkipGateway  | The default vale is <code>False</code> .                                                                            |

## Install Cisco NSO on Amazon EC2

This section provides an overview of how Cisco NSO is installed on Amazon EC2.

Cisco Crosswork uses a set of CF templates to deploy NSO.

### NSO Deployment Workflow

The NSO deployment procedure involves deploying various Crosswork resources using the corresponding YAML files.

The **nso-stack-ec2.yaml** file deploys stacks for one NSO NLB (**nso-nlb-ec2.yaml**) and two NSOs (**nso.yaml**). See below table for more information.

**Table 52: Resources Deployed During NSO Deployment**

| Resource | Description                                                                                                                                                                |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EC2 NSO  | The <b>nso.yaml</b> file is deployed to create the EC2 node resources (network interface and an instance) in the stack.                                                    |
| NSO NLB  | The <b>nso-nlb-ec2.yaml</b> file is deployed to create the EC2 NLB resources (target groups, network load balancer, data listeners, and NLB route 53 record) in the stack. |

### Installation Parameters

For list of important parameters that you must specify in the CF templates that are used to deploy NSO, see [CF Template Parameters for Installing NSO, on page 161](#). NSO is deployed on Amazon EC2 based on the parameters specified in the templates.




---

**Note** While deleting the NSO setup, delete the NSO Route53 Record (NsoRoute53RecordName) manually.

---

### Deploy the CF Templates

You can install NSO on Amazon EC2 by customizing the CF templates. For list of CF templates that are used for NSO deployment, see [NSO Deployment Workflow, on page 170](#).

For instructions on how to deploy the CF templates on Amazon EC2, see [Deploy a CF Template, on page 172](#).

### Verify the Installation

Verify that the NSO installation is successful by following the steps in [Monitor the Installation, on page 173](#).

### What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

## Deploy an Additional Crosswork Cluster Node

This section explains how to deploy an additional worker/hybrid node on the Crosswork cluster.

Deploying an additional node on the Crosswork cluster involves deploying the Crosswork network configuration and VM customization resources using the `cw-add-vm.yaml` file.



---

**Important** Before deploying an additional worker node, ensure that the Crosswork cluster and Crosswork application have been created.

---



---

**Note** A new hybrid node **MUST** reuse the same IP addresses as the hybrid VM it is replacing, and a maximum of 3 hybrid nodes are allowed.

---

### Installation Parameters

For list of important parameters that you must specify in the CF template that is used to deploy an additional node on the Crosswork cluster, see [CF Template Parameters for Installing Single Hybrid Cluster or Worker Node, on page 162](#). Additional nodes are deployed on the Crosswork cluster based on the parameters specified in the templates.

### Deploy the CF Templates

You can install an additional worker/hybrid node on the Crosswork cluster by customizing the CF template.

For instructions on how to deploy the CF templates on Amazon EC2, see [Deploy a CF Template, on page 172](#).

### Verify the Installation

Verify that the nodes are attached to the Crosswork cluster. On the EC2 console, select the Crosswork cluster and make sure that the nodes that you added appear under the **Compute** section. For more information, see [Monitor the Installation, on page 173](#).

### What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

## Manage CF Template Deployment

The following sections explain how to deploy a CF template on Amazon EC2 and verify its installation:

- [Deploy a CF Template, on page 172](#)
- [Monitor the Installation, on page 173](#)

## Deploy a CF Template

You can install Crosswork on Amazon EC2 with custom resources. Depending on the configured parameters, the needed components with the capabilities are also installed.

### Before you begin

- Make sure that you have met the [Table 28: AWS Prerequisites and Settings](#) and [Amazon EC2 Settings](#) prescribed for installing Crosswork on Amazon EC2.
- Ensure that you have access to the CloudFormation templates that are stored in the S3 bucket or on your local machine. If the template is in Amazon S3, keep the URL of the template file copied.

---

**Step 1** Log in to the AWS account and navigate to the S3 bucket. If the CF template is on your local computer, you can upload the template.

**Step 2** In the AWS CloudFormation console, navigate to the **Stacks** page and choose **Create stack > With new resources (standard)**. The **Create stack** page opens.

**Step 3** Enter the following details:

- a. Under **Prerequisite - Prepare template**, select **Template is ready**.
- b. Under **Specify template > Template source**, select one of the following options:
  - If you have the YAML or JSON file URL directing to the S3 bucket where the CF template is located, select **Amazon S3 URL**. In the **Amazon S3 URL** field, enter the URL and click **Next**.
  - If the CF template is saved on your local computer, select **Upload a template file** and click **Choose File** to select the file that you want to upload. After you have selected the template, Amazon uploads the file and displays the S3 URL. Click **Next**.

**Note** (Optional) Click **View in Designer** to view a visual representation of the execution flow in your CF template.

**Step 4** In the **Specify stack details** page, enter the relevant values for the stack name and parameter values. Click **Next**.

**Note** The parameter field names visible in this window are defined by the parameters in the CF template.

**Step 5** Review the parameter values that you have configured.

**Step 6** Under the **Capabilities**, select the check boxes next to:

- **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**
- **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY\_AUTO\_EXPAND.**

**Step 7** Click **Submit**.

---

### 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 173](#) to know how you can check the status of the installation.

## Monitor the Installation

This section describes how to verify if the deployment is complete without errors.

- 
- Step 1** In the CloudFormation console, from the left-hand side **Stacks** pane, select the stack that you have deployed.
- Step 2** The stack details are displayed on the right. Click on each tab in this window to view details of the stack. If the stack creation is in progress, the status of the stack in the **Events** tab is `CREATE_IN_PROGRESS`.
- Step 3** After the stack is 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 **Outputs** tab has details of the VM's interface IP addresses.
- 

### What to do next

After the stack creation is complete, you can access the Crosswork UI and monitor the health of your cluster. For more information on how to log in to the Crosswork UI, see [Accessing the Crosswork UI, on page 173](#).

## Accessing the Crosswork UI

After the stacks are created, you can check if all the nodes are up and running in the cluster from the Cisco Crosswork UI.

### Before you begin

- Ensure that you have a spare Network Load Balancer (NLB). To access Crosswork UI, use an external NLB that routes requests to its targets using the protocol DNS and port number that you specify.
- Verify that the Crosswork cluster and pods are in the running state. For information on how to view the status of the cluster, see [Monitor the Installation, on page 173](#).
- Make sure to keep the IP address of the Management node copied. This IP address is used to access the Crosswork UI. You can copy the IP address from the **Outputs** tab of the CloudFormation console. For information on accessing the **Outputs** tab, see [Monitor the Installation, on page 173](#).

- 
- Step 1** Log in to the AWS console and navigate to **Target Groups** to register the targets.
- Step 2** Under **Targets**, click **Register targets**. The **Register targets** page opens.

- Step 3** In the **IPv4 address**, specify the Management IP address that you copied from the CloudFormation console.
- Step 4** Specify the port as 30603. Click **Include as pending below**
- Step 5** Click **Register pending targets**.
- To deregister the targets that are no longer in use, select the target and click **Deregister**.
- Step 6** After the target is in the healthy state, click on the load balancer name under **Details**. The **Load balancer** page opens.
- Step 7** Copy the DNS name from the **DNS name** column.
- Step 8** Launch a supported browser and enter the following in the address bar: `https://<DNS_name>:30603/`
- Note** When you access 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 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 *Crosswork Network Controller 7.0 Administration Guide*.
- Step 9** Log in to 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.
- Step 10** (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.

---

### What to do next

Return to the installation workflow: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

## Crosswork Data Gateway Post-installation Tasks

This section lists the steps that you can complete after you have deployed Crosswork Data Gateway.

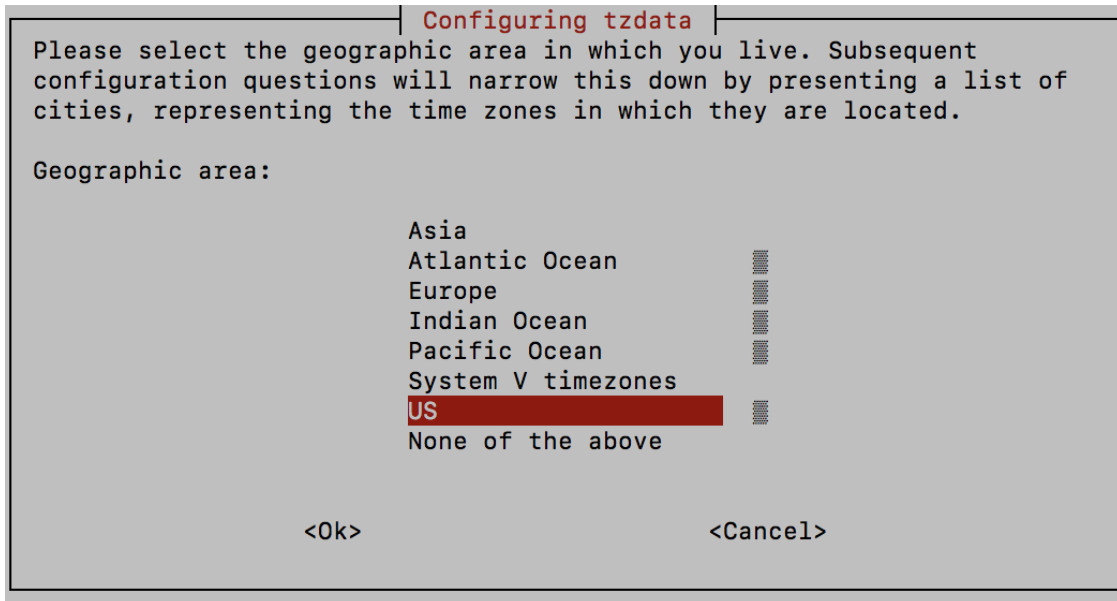
### Configure Timezone of the Data Gateway VM

In general, the data gateway VM launches with the default timezone as UTC. Cisco recommends that you configure the timezone to match your geographical area. With this configuration, all the Crosswork Data Gateway processes including the Showtech logs use the same configured timezone.

- 
- Step 1** In the data gateway VM interactive menu, select **Change Current System Settings**.
- Step 2** Select **9 Timezone**.

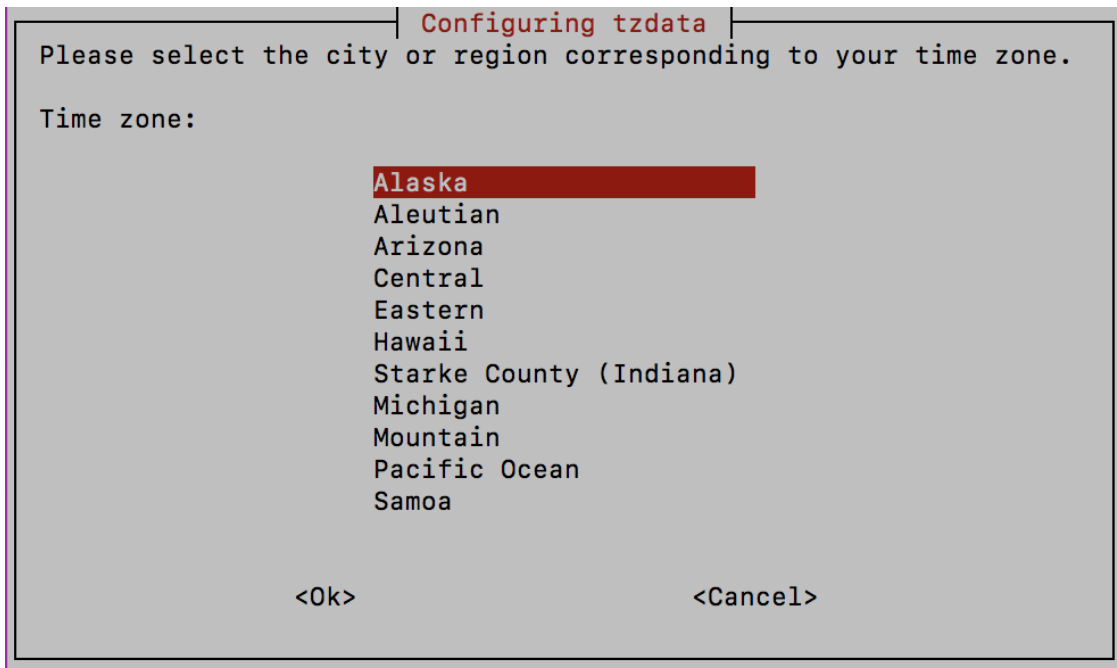
**Step 3** Select the geographic area in which you live.

*Figure 33: Timezone Settings - Geographic Area Selection*



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

*Figure 34: Timezone Settings - Region Selection*



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

**Step 6** Reboot the data gateway VM so that all processes pick up the new timezone.

**Step 7** Log out of the data gateway VM.

---

## Log in and Log out of the Data Gateway VM

This section describes how to log in and out to the data gateway VM.

Follow these steps to access and log out of the data gateway VM:

- [Access Crosswork Data Gateway VM from SSH, on page 176](#)
- [Log out of Crosswork Data Gateway VM, on page 176](#)

### Access Crosswork Data Gateway VM from SSH

Secure Shell (SSH) offers a protection from brute force attacks by blocking the client IP after several 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 causes the client IP to be blocked for at least 7 minutes. Continuing to accumulate failures cause the blocked time to be increased. Each client IP is tracked separately.

Follow these steps to log in to the data gateway VM from SSH.

---

**Step 1** From your work station with network access to the 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 log in 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 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 data gateway VM and reinstall with the correct network settings.

### Log out of Crosswork Data Gateway VM

To log out of the data gateway VM, from the **Main Menu**, select **l Logout** and press **Enter** or click **OK**.

## Troubleshoot Crosswork Data Gateway Installation and Enrollment

If Crosswork Data Gateway fails to autoenroll with Crosswork Network Controller, 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 the *Collect show-tech*



logs from the *Interactive Console* section in *Cisco Crosswork Network Controller 7.0 Administration Guide*. If there are session establishment or certificate-related issues, ensure that the `controller.pem` certificate is uploaded using the Interactive Console.



**Important** When using an IPv6 address, it must be surrounded by square brackets ([1::1]).

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 53: Troubleshooting the Installation/Enrollment**

| Issue                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Crosswork Data Gateway cannot be enrolled with Crosswork Network Controller due to an NTP issue, that is, there is a clock-drift between the two.</b></p> <p><b>The clock-drift might be with either Crosswork Data Gateway or Crosswork Network Controller.</b></p> <p><b>Also, on the NTP servers for Crosswork Network Controller and Crosswork Data Gateway, the initial time is set to the ESXi server. For this reason, the ESXi server must also have NTP configured.</b></p> <p><b>Sync the clock time on the host and retry.</b></p> | <ol style="list-style-type: none"> <li>1. Log in to the data gateway VM.</li> <li>2. From the main menu, select <b>5 Troubleshooting &gt; 2 Run show-tech</b>.<br/>Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>.<br/>The show-tech is now encrypted with a file extension ending with <code>.tar.xz</code>.</li> <li>3. Run the following command to decrypt the show-tech file.<br/><pre>openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in &lt;showtech file&gt; -out &lt;decrypted filename&gt; -pass pass:&lt;encrypt string&gt;</pre></li> </ol> <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 Crosswork Network Controller.</p> <ol style="list-style-type: none"> <li>3. From the main menu, go to <b>3 Change Current System Settings &gt; 1 Configure NTP</b>.<br/>Configure NTP to sync with the clock time on the Crosswork Network Controller server and try reenrolling Crosswork Data Gateway.</li> </ol> |

| Issue                                                                                                                                                                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>Crosswork Data Gateway remains in degraded state for more than 10 minutes with reason stated as "Could not collect vitals" due to certificate errors.</b></p>              | <ol style="list-style-type: none"> <li>Log in to the data gateway VM.</li> <li>From the main menu, select <b>5 Troubleshooting &gt; 2 Run show-tech</b>.<br/><br/>Enter the destination to save the tarball containing logs and vitals and click <b>OK</b>.<br/><br/>The show-tech is now encrypted with a file extension ending with .tar.xz.</li> <li>Run the following command to decrypt the show-tech file.<br/><br/> <pre>openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in &lt;showtech file&gt; -out &lt;decrypted filename&gt; -pass pass:&lt;encrypt string&gt;</pre> </li> </ol> <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 reupload the Controller Signing Certificate, as explained in the steps below:</p> <ol style="list-style-type: none"> <li>From the main menu, select <b>3 Change Current System Settings &gt; 7 Import Certificate</b>.</li> <li>From the <b>Import Certificates</b> menu, select <b>1 Controller Signing Certificate File</b> and click <b>OK</b>.</li> <li>Enter the SCP URI for the certificate file and click <b>OK</b>.</li> </ol> |
| <p><b>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.</b></p> | <ol style="list-style-type: none"> <li>Reupload the certificate file using the following steps: <ol style="list-style-type: none"> <li>From the main menu, select <b>3 Change Current System Settings &gt; 7 Import Certificate</b>.</li> <li>From the <b>Import Certificates</b> menu, select <b>1 Controller Signing Certificate File</b> and click <b>OK</b>.</li> <li>Enter the SCP URI for the certificate file and click <b>OK</b>.</li> </ol> </li> <li>Reboot the data gateway VM following the steps below: <ol style="list-style-type: none"> <li>From the main menu, select <b>5 Troubleshooting</b> and click <b>OK</b>.</li> <li>From the Troubleshooting menu, select <b>4 Reboot VM</b> and click <b>OK</b>.</li> <li>Once the reboot is complete, check if the data gateway's operational status is <b>Up</b>.</li> </ol> </li> </ol>                                                                                                                                                                                                                                                                                                                                                                 |

| Issue                                                                                                                                                                                                                                            | Action                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>During a Crosswork upgrade, some of the Crosswork Data Gateways may not get upgraded or reenrolled leading to logging multiple error messages in the dg-manager logs.</b>                                                                     | Reenroll or redeploy the data gateways. For more information, see the <i>Redeploy a Crosswork Data Gateway Instance</i> and <i>Reenroll Crosswork Data Gateway</i> sections in <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a> .                                                                                                                                                                    |
| <b>If a Crosswork Data Gateway instance that was previously attached to Crosswork is now reattached to a different Crosswork version 4.x or 5.0, the operational state of the instance may be Degraded with the robot-astack-influxdb error.</b> | <ol style="list-style-type: none"> <li>1. Log in to the Crosswork UI from the SSH.</li> <li>2. Run the Docker executive commands to access the <b>robot-astack-influxdb</b> pod.</li> <li>3. In the pod, navigate to the following directory and delete it:<br/><br/><code>/mnt/dataafs/influxdb</code></li> <li>4. Restart the service using the following command:<br/><br/><code>supervisorctl restart all</code></li> </ol> |
| <b>If Data Gateway is redeployed without moving the gateway to the Maintenance mode, Crosswork enrollment will be unsuccessful and errors will be logged in the dg-manager and controller-gateway logs.</b>                                      | Move the Data Gateway to the <b>Maintenance</b> mode or manually reenroll the gateway. For more information, see the <i>Reenroll Crosswork Data Gateway</i> section in <a href="#">Cisco Crosswork Network Controller 7.0 Administration Guide</a> .                                                                                                                                                                            |

## Import Controller Signing Certificate File

The Controller Certificate file is automatically imported after the VM boots. If there is an import failure, the data gateway VM makes several attempts to import the certificate while giving you the option to manually import it.

- You have not specified the **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.
- Cisco Crosswork configuration is in-progress when Crosswork Data Gateway tries to import the Controller Certificate file.
- The Cisco Crosswork Controller IP address is unreachable or incorrect.
- The Cisco Crosswork username or password is incorrect.

Follow these steps to import the controller signing certificate file:

---

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

**View the 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 132](#).

---

## View the Controller Signing Certificate File

Follow these steps to view the signing certificate:

---

**Step 1** From the 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.

---



## PART **IV**

# Install Crosswork Applications

- [Install Crosswork Applications, on page 183](#)





## CHAPTER 9

# Install Crosswork Applications

This chapter contains the following topics:

- [Install Crosswork Applications, on page 183](#)

## Install Crosswork Applications

This section explains how to install Crosswork applications on the Cisco Crosswork UI.

The Crosswork Network Controller applications are offered as **Essentials**, **Advantage**, and **Add-on** packages. Every package contains crosswork applications in a particular format unique to Crosswork known as CAPP (Crosswork APPLication). As a first step, you must download the relevant Crosswork Network Controller package from [cisco.com](http://cisco.com) and then proceed to install the applications which are part of the package.

### Before you begin

Ensure that all requirements of your application are met.

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

- Navigate to [cisco.com](http://cisco.com) and download the signed Crosswork Network Controller package that you require to a directory in your machine. For the purpose of these instructions, we will use the file name **signed-cw-na-cncessential-7.0.0-85-release700-240823.tar.gz**.
- Decompress the signed Crosswork Network Controller package.

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

Example:

```
cd <folder where tar was download>
tar -xvf signed-cw-na-cncessential-7.0.0-85-release700-240823.tar.gz
README
cw-na-cncessential-7.0.0-85-release700-240823.tar.gz
cw-na-cncessential-7.0.0-85-release700-240823.tar.gz.signature
CW-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cisco_x509_verify_release.py
```

- 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:**

```
python cisco_x509_verify_release.py3 -s
cw-na-cncessential-7.0.0-85-release700-240823.tar.gz.signature -i
cw-na-cncessential-7.0.0-85-release700-240823.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/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of cw-na-cncessential-7.0.0-85-release700-240823.tar.gz using
CW-CCO_RELEASE.cer
```

**Note** If you do not have python installed, go to [python.org](http://python.org) and download the version of python that is appropriate for your work station.

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

- 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.

- Click on **Application Management** and select the **Applications** tab.
- Click on the **Add File (.tar.gz)** option to add the package that contains the CAPP files.

**Note** When installing a Crosswork Network Controller package, there is no need to untar the package. You can add the package tarball as-is to the Crosswork UI and the applications within are automatically added. You can then install the individual applications as needed.


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

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 a Crosswork Network Controller package, the loading process may stop at 50% for a while depending on the resources your host platform has available.

The newly added application files are displayed as tiles 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.



**Important** After you install Crosswork Cluster and Crosswork Data Gateway, the applications in the Crosswork Network Controller package (Essential or Advantage) need to be installed in the following sequence:

1. Element Management Functions (available in Essentials and Advantage packages)
2. Crosswork Optimization Engine (available in Advantage package)
3. Crosswork Active Topology (available in Advantage package)
4. Crosswork Service Health (available in Advantage package)


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 to launch and for the applications to report as healthy. If a newly installed application is not healthy after an hour, contact the Cisco Customer Experience team.

---

### What to do next

Return to the installation workflow:

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)





## PART **V**

# **Integrate Cisco NSO and SR-PCE with Cisco Crosswork Network Controller**

- [Integrate Cisco NSO, on page 189](#)
- [Integrate SR-PCE, on page 203](#)





# CHAPTER 10

## Integrate Cisco NSO

---

This chapter contains the following topics:

- [NSO Integration Workflow](#), on page 189
- [Add Cisco NSO Providers](#), on page 190
- [Install Cisco NSO Function Pack Bundles from Crosswork UI](#), on page 193
- [Install NSO Function Packs Manually](#), on page 202

### NSO Integration Workflow

This section explains the steps in integrating Cisco NSO with Crosswork Network Controller.

The compatible version of NSO is 6.1.11.2.

#### 1. Install the compatible version of Cisco NSO

Ensure that you have installed the compatible version of Cisco NSO:

- If you are a VMware user, follow the instructions in [NSO documentation](#).
- If you are a AWS EC2 user, follow the instructions in [Install Cisco NSO on Amazon EC2](#), on page 170.

Additionally, for Cisco NSO LSA setup, see [\(Optional\) Set up Cisco NSO Layered Service Architecture](#), on page 193.

See the *Compatibility Information* section in the [Crosswork Network Controller 7.0 Release Notes](#) for information on the compatible versions of NSO/NED.

#### 2. Add the NSO provider and verify connectivity

Follow the instructions in [Add Cisco NSO Providers](#), on page 190.

#### 3. Install the mandatory NSO core function packs

Depending on the Cisco Crosswork application or solution that you are using, there are mandatory function packs that must be installed on Cisco NSO to make the products compatible.

The NSO core function packs are bundled in [cisco.com](http://cisco.com) as follows:

Table 54: NSO Core Function Packs

| Package Name                                                                                                         | Contents                                                                                                                                                                                                                                                                                         |
|----------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco Crosswork Network Controller Function Pack<br><b>File name:</b> <i>signed-cw-na-functionpacks-7.0.0.tar.gz</i> | <ul style="list-style-type: none"> <li>• <i>Cisco NSO Transport SDN Function Pack Bundle</i></li> <li>• <i>Cisco NSO DLM Service Pack</i></li> <li>• <i>Cisco NSO Telemetry Traffic Collector Function Pack</i></li> <li>• <i>Cisco Crosswork Change Automation NSO Function Pack</i></li> </ul> |

You can install the function packs using either of the following methods:

- [Install Cisco NSO Function Pack Bundles from Crosswork UI, on page 193](#) (Recommended)
- [Install NSO Function Packs Manually, on page 202](#)



**Note** The Cisco Crosswork Network Controller Function Pack SDK Application (*cw-na-platform-7.0.0-signed-tdn-sdk.tar.gz*) is also available for download on [cisco.com](http://cisco.com). The SDK provides tools and source-code examples you can use to develop, build, package and deploy the TSDN function pack on Crosswork Network Controller.

## Add Cisco NSO Providers

The Cisco Network Services Orchestrator (Cisco NSO) provider supplies the following functionality:

- Network services and device configuration services to Cisco Crosswork applications.
- Device management and configuration maintenance services.



**Note** Crosswork supports Cisco NSO Layered Service Architecture (LSA) deployment. The LSA deployment is constructed from multiple NSO providers, that function as the customer-facing service (CFS) NSO containing all the services, and the resource-facing service (RFS), which contains the devices. Crosswork automatically identifies the NSO provider as CFS or RFS. Only one CFS is allowed. On the **Manager Provider Access** page, the **Type** column identifies the NSO provider as CFS.

Follow the steps below to add a Cisco NSO provider through the UI. Note that you can import several providers at the same time by preparing a CSV file with the details of all the providers and importing it into Crosswork.

### Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider.

- Know the name you want to assign to the Cisco NSO provider.
- Know the Cisco NSO NED device models and driver versions used in your topology. You can find the Cisco NSO version using the `version` command.

```
admin@ncs# show ncs-state version
ncs-state version 6.1.11.2
```

- Know the Cisco NSO server IP address or FQDN (Domain name and host name). When NSO is configured with HA, the IP address would be management VIP address.
- Confirm Cisco NSO device configurations.
- The NSO cross launch feature is not available for user roles with read-only permissions.

**Step 1** From the main menu, choose **Administration > Manage Provider Access**.

**Step 2** Click .

**Step 3** Enter the following values for the Cisco NSO provider fields:

a) Required fields:

- **Provider Name:** Enter a name for the provider.
- **Credential Profile:** Select the previously created Cisco NSO credential profile.
- **Family:** Select **NSO**.
- **Protocol:** Select **HTTPS** and/or **SSH**.
  - Note** To use the **Backup NSO** option during backup, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail.
- **Server Details:** Enter either the IP address (IPv4 or IPv6) or FQDN (Domain name and Host name) of the server.
- **Port:** For HTTPS, enter the port that corresponds with what is configured on the NSO VM in `etc/ncs/ncs.conf` to access NSO using HTTPS. NSO uses **8888** as default port.
- **Model:** Select the model (Cisco-IOS-XR, Cisco-NX-OS, or Cisco-IOS-XE). Add a model for each type of device that will be used in the topology. If you have more than one, add another supported model.
- **Version:** Enter the NED software version installed for the device model in NSO.

**Note** The site name can be configured for NSO from the NCS backend, and it will be displayed as a read-only value on the NSO provider in the Crosswork UI. To configure the NSO site name:

1. Login into `ncs_cli` in config mode.
2. Set `hcc dns member master ip-address ns01-mgmt-IP location site1-location`
3. Set `hcc dns member standby ip-address ns02-mgmt-IP location site2-location`
4. Commit


**Note** If you set the **Site location** parameter in NSO, you can determine if geo-fencing is violated during testing when Crosswork and the active NSO are not in the same site location. Crosswork will also raise and clear alarms if a geo-fence violation is detected.

**Important** When you modify or update the NSO provider IP address or FQDN, you need to detach devices from corresponding virtual data gateway, and reattach them. If you fail to do this, the provider changes will not be reflected in MDT collection jobs.

b) Optional values:

- **Timeout:** The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.

c) **Provider Properties:** Enter one of the following key/value pairs in the first set of fields:

| Property Key                                                                                      | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>forward</b>                                                                                    | <p><b>true</b></p> <p>This property is necessary when using the Cisco Crosswork Network Controller solution to allow provisioning operations within the UI and to enable the northbound interface to NSO via the Crosswork API gateway.</p> <p><b>Note</b> The default value of <b>forward</b> is "false". If this is not changed, the devices added to Crosswork will not be added to NSO. This setting is used in conjunction with the <b>Edit Policy</b> option (step 5).</p>                                                                                                              |
| <b>nso_crosslaunch_url</b><br><b>Note</b> This property is used only for NSO standalone provider. | <p>Enter the URL for cross-launching NSO in the format: <b>https://&lt;NSO IP address/FQDN&gt;: port number</b></p> <p>To enable cross-launch of the NSO application from the Crosswork UI. Requires a valid protocol (<b>HTTP</b> or <b>HTTPS</b>), and the provider must be reachable.</p> <p>The cross launch icon (  ) is displayed in the <b>Provider Name</b> column. Alternately, you can cross launch the NSO application using the launch icon located at the top right corner of the window.</p> |
| <b>input_url_prefix</b><br><b>Note</b> This property is used only for NSO LSA provider.           | <p>Enter the RFS ID in the format: <b>/rfc-x</b>, where <b>x</b> refers to the number of the RFS node.</p> <p>Example (for RFS node 1):<br/>input_url_prefix: /rfc-1</p>                                                                                                                                                                                                                                                                                                                                                                                                                      |

**Step 4** When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

**Step 5** **To edit a NSO policy:**

a) On an NSO provider, click **Actions > Edit policy details**.

The **Edit policy details** window for the selected NSO provider is displayed.

b) Edit the configuration fields to match the requirements of your environment.

**Note** Set **Onboard from** to **TRUE**) to trigger Crosswork to rescan NSO.

c) Click **Save** to save your changes.



**What to do next**

- Add NSO Function Packs: [Manage NSO Function Pack Bundles, on page 195](#)

## (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 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](#).

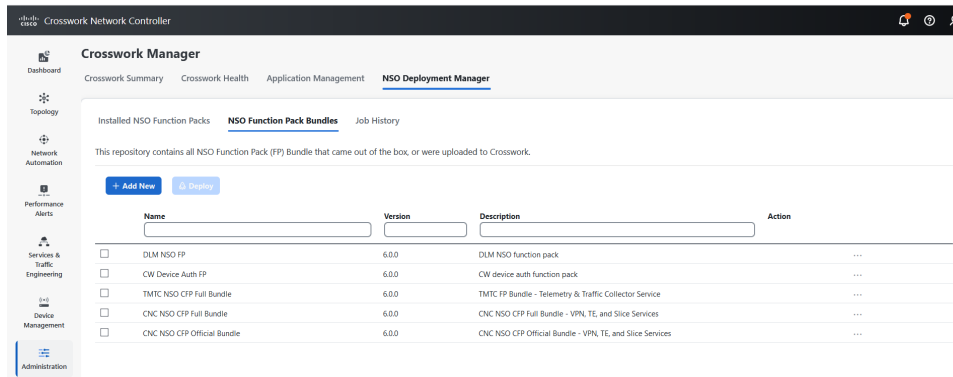
## Install Cisco NSO Function Pack Bundles from Crosswork UI

In the Cisco NSO function pack bundles, the NSO function pack files are bundled as tar.gz files. To ensure interoperability with Crosswork, Cisco NSO requires the installation of the essential function packs.

In the Crosswork UI, the **NSO Deployment Manager** tab lets you manage the function pack bundles using the following tabs:

- **Installed NSO Function Packs:** Provides the list of NSO function packs deployed on the configured NSO server. See [View NSO Function Pack Bundles, on page 194](#) for more information.
- **NSO Function Pack Bundles:** Allows you to add and deploy the function pack bundles. Use this tab, to view the artifacts in the function pack bundle, download, and delete the function pack bundles. See [Manage NSO Function Pack Bundles, on page 195](#) for more information.
- **Job History:** The **Job History** tab displays a summary of the jobs, job ID, time when the job is started and completed, job description, and target. See [View NSO Function Pack Job History, on page 201](#) for more information.

Figure 35: NSO Deployment Manager Window



## View NSO Function Pack Bundles

Operators can retrieve a list of all of the function pack bundles installed on each available NSO server via the Crosswork UI or using the API.

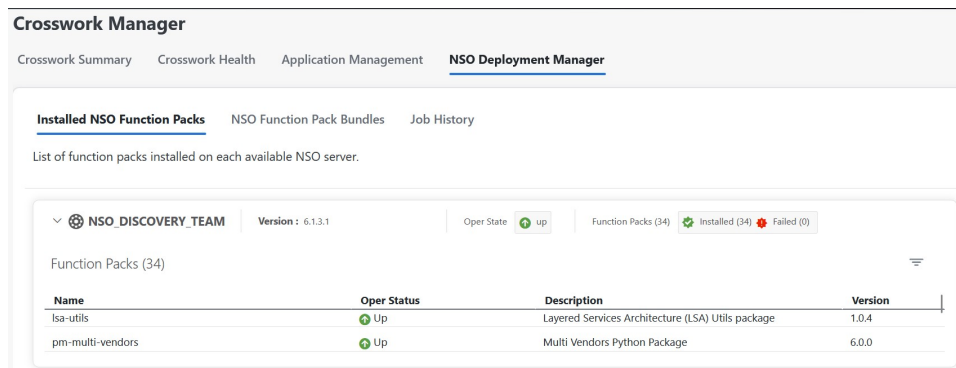


**Attention** If any of the NSO service providers is unreachable, you cannot view the installed NSO function packs. An error "Server is temporarily unavailable, try to relogin" is displayed.

Follow the steps below to view the installed NSO function pack bundles through the UI.

- Step 1** From the main menu, choose **Administration > Crosswork Manager**, click the **NSO Deployment Manager** tab.
- Step 2** Click the **Installed NSO Function Packs** tab.
- Step 3** Select the NSO provider and expand the NSO server entry to view the list of function packs and their details (function pack name, operational state as **Up** or **Down**, description, and version).

Figure 36: Installed NSO Function Packs Window



## Manage NSO Function Pack Bundles

You can add and deploy custom NSO function packs in addition to the function packs that are added by default to the Crosswork UI. The preinstalled bundles include the following packs:

**Table 55: Default NSO Core Function Packs Bundles**

| Package Name                | Contents                                                                                                                     |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------|
| DLM NSO FP                  | Cisco NSO DLM Service Pack                                                                                                   |
| Device Auth NSO FP          | Cisco Crosswork Change Automation NSO Function Pack                                                                          |
| TMTC NSO FP                 | Cisco NSO Telemetry Traffic Collector Function Pack                                                                          |
| CNC NSO FPs Plus Sample FPs | Crosswork Network Controller NSO Function Packs for VPN, TE, and Slice services. It also contains the sample function packs. |
| CNC NSO FPs                 | Crosswork Network Controller NSO function packs for VPN, TE, and Slice services.                                             |

### Before you begin

Each function pack bundle includes a metadata.yaml file detailing the prerequisites for installing the bundle on NSO. The following is a comprehensive list of the prerequisites for the supplied function packs:

- Java version 17.0.0 or higher
- Python version 3.8.0
- NSO configured to allow 64,000 openFileDescriptors

Follow the steps below to manage the function pack bundles.

**Step 1** Ensure that your NSO setup meets all of the prerequisites.

Check the python and java versions using the `--version` command.

```
python --version
```

```
Python 3.8.10
```

```
java --version
```

```
openjdk 17.0.9 2023-10-17
```

```
OpenJDK Runtime Environment (build 17.0.9+9-Ubuntu-120.04)
```

```
OpenJDK 64-Bit Server VM (build 17.0.9+9-Ubuntu-120.04, mixed mode, sharing)
```

**Step 2** From the main menu, choose **Administration > Crosswork Manager**, click the **NSO Deployment Manager** tab.

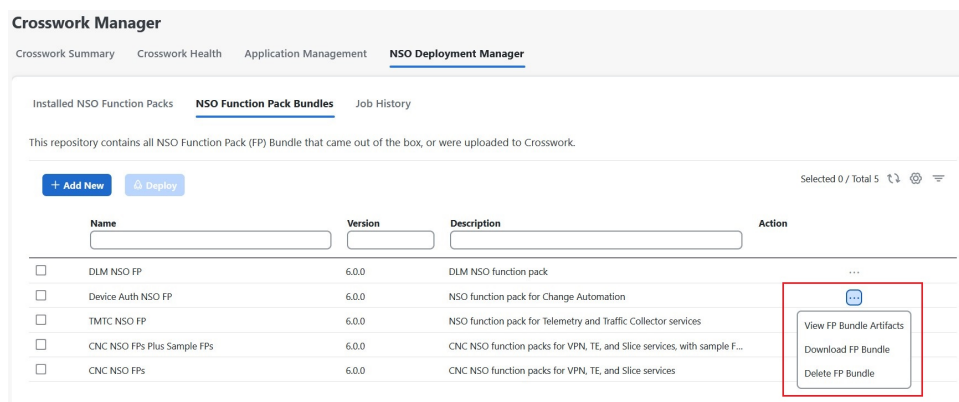
**Step 3** Click the **NSO Function Pack Bundles** tab.

All the installed NSO function pack bundles get displayed with the bundle name, version, and description information.

To manage the bundles, select one or more bundles and click the **Action** menu to perform the following:

- **View FP Bundle Artifacts:** View the hierarchy of the artifacts that are bundled in the selected package.
- **Download FP Bundle:** Download the function pack bundle.
- **Delete FP Bundle:** Delete the function pack bundle.

Figure 37: Action Menu



**Step 4** Click **Add New** to install the new function pack bundle. The **Add New NSO Function Pack Bundle** page is displayed.

**Note** The **Add New** button is disabled when Crosswork is in maintenance mode.

**Step 5** In the **Add New NSO Function Pack Bundle** page, enter the following:

- **Host Name/IP address:** Enter the IP address and subnet mask of the Cisco NSO server.
- **Port:** For HTTPS, enter the port that corresponds with what is configured on the NSO VM in `etc/ncs/ncs.conf` to access NSO using HTTPS. NSO uses 8888 as the default port.
- **User Name:** The username used to log in to the NSO server.
- **Password:** The password credentials to authenticate into the NSO server.
- **Server Path/Location:** The server path of the NSO server.

Figure 38: Add New NSO Function Packs Bundle Window

Crosswork Manager

### Add New Nso Function Pack Bundle

**Upload NSO Function Pack Bundle**  
Use the Secure Copy(SCP) protocol to upload the file(.tar.gz).

Host Name / Ip Address\*

Port\*

User Name\*

Password\*  [Show](#) [Test SSH Connectivity](#)

Server Path/Location\*

[+ Add Another](#)

[Add](#) [Cancel](#)

- Step 6** Click **Test SSH Connectivity** again to validate SSH-based connectivity. If the connection is successful, a confirmation message indicating that the NSO bundle upload is in-progress appears. Click **View Progress in Job History** to view the upload status.
- Step 7** Click **Add**.
- Step 8** Check the **Job History** to monitor the addition of the package to Crosswork. Once the package has been added, the next step is to deploy the function pack.

#### What to do next

After the function pack is added, deploy the function pack on NSO. See [Deploy NSO Function Pack Bundles, on page 197](#).

## Deploy NSO Function Pack Bundles

This topic explains the process to deploy the NSO function pack bundles.

The Cisco NSO sample function packs are provided as a starting point for VPN service provisioning functionality in Cisco Crosswork Network Controller. While the samples can be used “as is” in some limited network configurations, they are intended to demonstrate the extensible design of Cisco Crosswork Network Controller. Answers to common questions can be found on Cisco Devnet and Cisco Customer Experience representatives can provide answers to general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team.



**Attention** NSO function packs cannot be deployed when Crosswork is in maintenance mode.

### Before you begin

- Ensure that the NSO function pack bundle is uploaded to the Crosswork UI. See [Manage NSO Function Pack Bundles, on page 195](#) for more information.
- If you plan to deploy the function pack bundle in an HA environment, you must have the primary and secondary server details readily available.
- If your primary and secondary NSO servers and Crosswork servers are in different subnets, you must configure either an IP static route (**Administration > Settings > Static Routes**) or an IP rule policy (run `ip rule add from all to 10.19.0.4 lookup cw_data` on the Crosswork server) to enable connectivity between the servers.

**Step 1** From the main menu, choose **Administration > Crosswork Manager**, click the **NSO Deployment Manager** tab.

**Step 2** Click the **NSO Function Pack Bundles** tab.

**Step 3** Select the NSO function pack bundle and click **Deploy**.

**Note** You can only select up to 3 Function Packs to be installed at a time. To install more, install the 3 function packs first and then repeat this process until you have installed all the Function Packs you will use.

**Figure 39: NSO Function Pack Bundles Window**

| Name                                                 | Version | Description                                                                      | Action |
|------------------------------------------------------|---------|----------------------------------------------------------------------------------|--------|
| <input checked="" type="checkbox"/> DLM NSO FP       | 6.0.0   | DLM NSO function pack                                                            | ...    |
| <input type="checkbox"/> Device Auth NSO FP          | 6.0.0   | NSO function pack for Change Automation                                          | ...    |
| <input type="checkbox"/> TMTC NSO FP                 | 6.0.0   | NSO function pack for Telemetry and Traffic Collector services                   | ...    |
| <input type="checkbox"/> CNC NSO FPs Plus Sample FPs | 6.0.0   | CNC NSO function packs for VPN, TE, and Slice services, with sample FPs included | ...    |
| <input type="checkbox"/> CNC NSO FPs                 | 6.0.0   | CNC NSO function packs for VPN, TE, and Slice services                           | ...    |

**Step 4** In the **Deploy Crosswork NSO FP Bundle** page, enter the following SSH connection details:

- **User Name:** The SSH username for server access.
- **Password:** The SSH password for server access.
- **Sudo Password:** The SSH sudo password.

Figure 40: SSH Connection Details Page

**Step 5** Click **Next**.

**Step 6** In the **Deployment Target** section, review the target details:

- **Provider Name:** Displays the name of the provider.
- **Reachability:** Displays the reachability status of the provider.
- **CFS Role Selection:** This column appears when a role is not assigned to a provider. Select the check box that corresponds to the provider row to assign the customer-facing service (CFS) role. The resource-facing service (RFS) role is automatically assigned to the other providers. For more information about CFS, RFS, and Cisco NSO Layered Service Architecture (LSA) deployment concepts, see the *Prepare Infrastructure for Device Management* chapter in the [Cisco Crosswork Network Controller 7.0 Administration Guide](#).
- **High Availability:** Depending on your deployment preferences for the function packs bundle on an NSO node, select either non-HA or HA. If you have selected HA, enter the server details in the **Primary Server** and **Secondary Server** fields.

Figure 41: Deployment Target Page

| Provider Name                                              | Reachability | CFS Role Selection                  | High Availability                                                | Primary Server | Secondary Server |
|------------------------------------------------------------|--------------|-------------------------------------|------------------------------------------------------------------|----------------|------------------|
| <input checked="" type="checkbox"/> NSO_DISCOVERY_TEAM_CFS | Reachable    | <input checked="" type="checkbox"/> | <input checked="" type="radio"/> Non HA <input type="radio"/> HA |                |                  |
| <input type="checkbox"/> NSO_DISCOVERY_TEAM_RFS1           | Reachable    | <input type="checkbox"/>            | <input type="radio"/> Non HA <input type="radio"/> HA            |                |                  |
| <input type="checkbox"/> NSO_DISCOVERY_TEAM_RFS2           | Reachable    | <input type="checkbox"/>            | <input type="radio"/> Non HA <input type="radio"/> HA            |                |                  |

**Step 7** Click **Next**.

**Step 8** In the **Review & Deploy** page, review the NSO bundle and deployment target details that you have configured. If you want to modify your selection, click **Previous** to view the earlier pages and modify it as required.

**Note** If the provider is deployed on a standalone NSO node, the role is displayed as STANDALONE.

Figure 42: Review Selection Page

Crosswork Manager  
Deploy Crosswork NSO FP Bundle

Provider Credentials    Deployment Target    Review & Deploy

Review your selection  
Before deploying the FP bundle, please review your choice.

NSO Function Pack Bundle  
DLM\_NS0\_FP

Deployment Target & HA

| Provider Name      | Role       | High Availability | Primary Server | Secondary Server |
|--------------------|------------|-------------------|----------------|------------------|
| NSO_DISCOVERY_TEAM | STANDALONE | NON HA            | -              | -                |

Cancel    Previous    Deploy


- Step 9** Click **Deploy**.
- Step 10** Check the **Job History** to monitor the installation.
- Step 11** Repeat the process for any additional Function Packs that you need to install.

## Troubleshoot the NSO Function Pack Installation

The following table lists common problems that might be experienced while installing or deploying a Cisco NSO function pack.



Table 56: Troubleshooting the Function Pack Installation Issues

| Issue                                                                                                                                       | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|---------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>The function pack deployment failed with the following error:</p> <pre>Failed to open SSH connection to host coffee-ns01.cisco.com</pre> | <p>In an HA configuration, the NSO engine assumes that the NSO primary and secondary servers, and the Crosswork server reside in the same subnet.</p> <p>If the servers have different subnets, you must configure an IP route or an IP rule policy to ensure connectivity between the servers. When the routes are not configured, the engine cannot locate the subnet, and the function pack deployment fails.</p> <p><b>Note</b> Static routes can only be configured when ZTP application is installed.</p> <p>Use one of the following steps to resolve the issue:</p> <ul style="list-style-type: none"> <li>To configure the static routes, from the main menu, select <b>Administration &gt; Settings &gt; Static Routes</b>. Click the  icon, enter the destination subnet IP address and mask (in slash notation), then click <b>Add</b>.</li> <li>To configure the IP rule, log in to the Crosswork server and use the following command: <pre>ip rule add from all to 10.19.0.4 lookup cw_data</pre> </li> </ul> |

## View NSO Function Pack Job History

The **Job History** tab shows detailed information of when jobs were started and ended, job ID, status, and other vital information.


Follow the steps below to view the details of the jobs.

**Step 1** From the main menu, choose **Administration > Crosswork Manager**, click the **NSO Deployment Manager** tab.

**Step 2** Click the **Job History** tab.

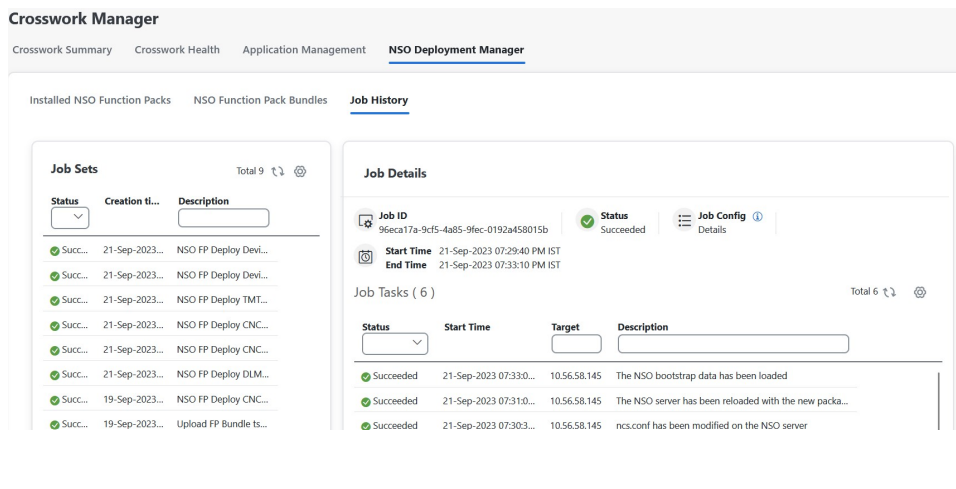
In the **Job History** tab, the **Job Sets** pane displays the state of the job, job ID, and the job description. You can show or hide the columns based on the job creation time, status, and description.

**Step 3** In the **Job Sets** pane, select the job sets to view the associated job information in the **Job Details** pane. You can view the summary of the job tasks based on job task ID, task status, the task start and end time, and description.

To view the job configuration information in JSON format, click the  icon next to **Job Config**. A config window opens that lets you view the configuration in the following modes:

- View Mode
- Text Mode

Figure 43: Job History Window



## Install NSO Function Packs Manually

If you need to install individual function packs manually, follow the relevant procedure from the below table:

Table 57: NSO Function Packs

| Crosswork Product                                                                       | Required Function Pack documentation                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Crosswork Network Controller Essentials<br>OR<br>Crosswork Network Controller Advantage | <ul style="list-style-type: none"> <li><a href="#">Cisco NSO Transport SDN Function Pack Bundle 7.0.0 User Guide</a></li> <li><a href="#">Cisco NSO Transport SDN Function Pack Bundle 7.0.0 Installation Guide</a></li> <li><a href="#">Cisco Network Services Orchestrator DLM Service Pack 7.0.0 Installation Guide</a></li> <li><a href="#">Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 7.0.0 Installation Guide</a></li> <li><a href="#">Cisco Crosswork Change Automation NSO Function Pack 7.0.0 Installation Guide</a></li> </ul> |
| Crosswork Optimization Engine (Standalone)                                              | <ul style="list-style-type: none"> <li><a href="#">Cisco Network Services Orchestrator DLM Service Pack 7.0.0 Installation Guide</a></li> <li><a href="#">Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 7.0.0 Installation Guide</a></li> </ul>                                                                                                                                                                                                                                                                                             |



# CHAPTER 11

## Integrate SR-PCE

---

This chapter contains the following topics:

- [SR-PCE Integration Workflow, on page 203](#)
- [Configure SR-PCE, on page 203](#)
- [Add Cisco SR-PCE Providers, on page 206](#)

### SR-PCE Integration Workflow

This section explains the steps in integrating Cisco SR-PCE with Crosswork Network Controller.

The compatible version of SR-PCE is Cisco IOS XR 24.2.1.

#### 1. Install the compatible version of Cisco SR-PCE

Select the type of SR-PCE (for VMware ESXi or AWS) and follow the relevant install instructions in the [Cisco IOS XRv 9000 Router Installation Guide](#).

#### 2. Configure SR-PCE

Follow the instructions in [Configure SR-PCE, on page 203](#).

#### 3. Add SR-PCE provider and verify connectivity

Follow the instructions in [Add Cisco SR-PCE Providers, on page 206](#).

### Configure SR-PCE

This section explains how to configure SR-PCE after you have installed it.



---

**Note** The Cisco IOS XRv 9000 is the recommended platform to act as the SR-PCE.

---

Table 58: Configure SR-PCE

| Step | Command or Action                                                                                                                        | Description                                                                                                                                                                                                                                                                                                    |
|------|------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1    | <code>configure</code><br>Example:<br>RP/0/RP0/CPU0:router# <code>configure</code>                                                       | Enters mode.                                                                                                                                                                                                                                                                                                   |
| 2    | <code>pce</code><br>Example:<br>RP/0/RP0/CPU0:router(config)# <code>pce</code>                                                           | Enables PCE and enters PCE configuration mode.                                                                                                                                                                                                                                                                 |
| 3    | <code>address ipv4 address</code><br>Example:<br>RP/0/RP0/CPU0:router(config-pce)# <code>address ipv4 192.168.0.1</code>                 | Configures a PCE IPv4 address.                                                                                                                                                                                                                                                                                 |
| 4    | <code>state-sync ipv4 address</code><br>Example:<br>RP/0/RP0/CPU0:router(config-pce)# <code>state-sync ipv4 192.168.0.3</code>           | Configures the remote peer for state synchronization.                                                                                                                                                                                                                                                          |
| 5    | <code>tcp-buffer size size</code><br>Example:<br>RP/0/RP0/CPU0:router(config-pce)# <code>tcp-buffer size 1024000</code>                  | Configures the transmit and receive TCP buffer size for each PCEP session, in bytes. The default buffer size is 256000. The valid range is from 204800 to 1024000.                                                                                                                                             |
| 6    | <code>password {clear   encrypted} password</code><br>Example:<br>RP/0/RP0/CPU0:router(config-pce)# <code>password encrypted pwd1</code> | Enables TCP MD5 authentication for all PCEP peers. Any TCP segment coming from the PCC that does not contain a MAC matching the configured password will be rejected. Specify if the password is encrypted or clear text.<br><br><b>Note</b> TCP-AO and TCP MD5 are never permitted to be used simultaneously. |

| Step | Command or Action                                                                                                                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7    | <pre>tcp-ao key-chain [include-tcp-options] [accept-ao-mismatch-connection]  Example: RP/0/RP0/CPU0:router(config-pce)# tcp-ao pce_tcp_ao include-tcp-options</pre> | <p>Enables TCP Authentication Option (TCP-AO) authentication for all PCEP peers. Any TCP segment coming from the PCC that does not contain a MAC matching the configured key chain will be rejected.</p> <ul style="list-style-type: none"> <li>• <b>include-tcp-options</b>—Includes other TCP options in the header for MAC calculation.</li> <li>• <b>accept-ao-mismatch-connection</b>—Accepts connection even if there is a mismatch of AO options between peers.</li> </ul> <p><b>Note</b> TCP-AO and TCP MD5 are never permitted to be used simultaneously.</p> |
| 8    | <pre>segment-routing {strict-sid-only   te-latency}  Example: RP/0/RP0/CPU0:router(config-pce)# segment-routing strict-sid-only</pre>                               | <p>Configures the segment routing algorithm to use strict SID or TE latency.</p> <p><b>Note</b> This setting is global and applies to all LSPs that request a path from this controller.</p>                                                                                                                                                                                                                                                                                                                                                                           |
| 9    | <pre>timers  Example: RP/0/RP0/CPU0:router(config-pce)# timers</pre>                                                                                                | <p>Enters timer configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| 10   | <pre>keepalive time  Example: RP/0/RP0/CPU0:router(config-pce-timers)# keepalive 60</pre>                                                                           | <p>Configures the timer value for locally generated keep-alive messages. The default time is 30 seconds.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 11   | <pre>minimum-peer-keepalive time  Example: RP/0/RP0/CPU0:router(config-pce-timers)# minimum-peer-keepalive 30</pre>                                                 | <p>Configures the minimum acceptable keep-alive timer that the remote peer may propose in the PCEP OPEN message during session establishment. The default time is 20 seconds.</p>                                                                                                                                                                                                                                                                                                                                                                                      |
| 12   | <pre>reoptimization time  Example: RP/0/RP0/CPU0:router(config-pce-timers)# reoptimization 600</pre>                                                                | <p>Configures the re-optimization timer. The default timer is 1800 seconds.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| 13   | <pre>exit  Example: RP/0/RP0/CPU0:router(config-pce-timers)# exit</pre>                                                                                             | <p>Exits timer configuration mode and returns to PCE configuration mode.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**What to do next:**

Return to the installation workflow:

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)

## Sample SR-PCE config

This is a sample SR-PCE configuration:

```
pce
address ipv4 1.1.1.98
api
 user cisco {This is the username and password that the
 credential profile used for the PCE will need to have for HTTP}
 password encrypted 032752180500701E1D48
!
```

## Add Cisco SR-PCE Providers

Cisco Segment Routing Path Computation Elements (Cisco SR-PCE) providers supply device discovery, management, configuration-maintenance and route-calculation services to the Cisco Crosswork applications. At least one SR-PCE provider is required in order to learn and discover SR policies, Layer 3 links, and devices. You have the option to configure a second SR-PCE as a backup. Both SR-PCE devices must be connected to the same network as Crosswork Network Controller does not support managing more than one domain.




---

**Note** To enable Cisco Crosswork application access to an SR-PCE as an SDN controller on the management domain, SR-PCE needs to be added as a provider.

---

Follow the steps below to add (through the UI) one or more instances of Cisco SR-PCE as providers.

**Before you begin**

You will need to:

- Configure a device to act as the SR-PCE. See SR configuration documentation for your specific device platform to enable SR (for IS-IS or OSPF protocols) and configure an SR-PCE (for example: [Segment Routing Configuration Guide for Cisco NCS 540 Series Routers](#)).
- Create a credential profile for the Cisco SR-PCE provider. This should be a basic HTTP text-authentication credential (currently, MD5 authentication is not supported). If the Cisco SR-PCE server you are adding does not require authentication, you must still supply a credential profile for the provider, but it can be any profile that does not use the HTTP protocol.
- Know the name you want to assign to the Cisco SR-PCE provider. This is usually the DNS hostname of the Cisco SR-PCE server.
- Know the Cisco SR-PCE server IP address.

- Know the interface you want to use to communicate between Cisco SR-PCE and the Cisco Crosswork application server.
  - Determine whether you want to auto-onboard the devices that Cisco SR-PCE discovers and, if so, whether you want the new devices to have their management status set to **off**, **managed** or **unmanaged** when added.
  - If you plan to auto-onboard devices that the Cisco SR-PCE provider discovers, and set them to a managed state when they are added to the database:
    - Assign an existing credential profile for communication with the new managed devices.
    - The credential profile must be configured with an SNMP protocol.
  - For high availability, ensure that you set up two separate Cisco SR-PCE providers with unique names and IP addresses, but with matching configurations.
- 

**Step 1** From the main menu, choose **Administration > Manage Provider Access**.

**Step 2** Click .

**Step 3** Enter the following values for the SR-PCE provider fields:

a) Required fields:

- **Provider Name:** Name of the SR-PCE provider.
- **Credential Profile:** Select the previously created Cisco SR-PCE credential profile.
- **Family:** Select **SR\_PCE**. All other options should be ignored.
- **Protocol:** Select **HTTP**.
- **IP Address/ Subnet Mask:** Enter the IP address (IPv4 or IPv6) and subnet mask of the server.
- **Port:** Enter **8080** for the port number.
- **Provider Properties:** Enter one of the following key/value pairs in the first set of fields:

| Property Key              | Value                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>auto-onboard</b>       | <p><b>off</b></p> <p><b>Note</b> Use this option if you plan to manually (via UI or CSV import) enter all of your network devices.</p> <p>When devices are discovered, the device data is recorded in the Cisco SR-PCE database, but is not registered in Crosswork Network Controller Inventory Management database.</p>                                                                                                                                                                                                                                                                                                                                                                     |
|                           | <p><b>unmanaged</b></p> <p>If this option is enabled, all devices that Crosswork Network Controller discovers will be registered in the Crosswork Network Controller Inventory Management database, with their configured state set to <b>unmanaged</b>. SNMP polling will be disabled for these devices, and no management IP information will be included. To get these devices into the <b>managed</b> state later, you will need to either edit them via the UI or export them to a CSV make modifications and then import the updated CSV. You can also assign credential profiles by adding them to the device CSV file before import (the credential profiles must already exist).</p> |
|                           | <p><b>managed</b></p> <p>If this option is enabled, all devices that Cisco SR-PCE discovers will be registered in the Crosswork Network Controller Inventory Management database, with their configured state set to <b>managed</b>. SNMP polling will be enabled for these devices, and Cisco SR-PCE will also report the management IP address (TE Router ID for IPv4, or IPv6 Router ID for IPv6 deployment). The devices will be added with the credential profile associated with the device-profile key in the SR-PCE provider configuration.</p>                                                                                                                                       |
| <b>device-profile</b>     | <p>The name of a credential profile that contains SNMP credentials for all the new devices.</p> <p><b>Note</b> This field is necessary only if <b>auto-onboard</b> is set to <b>managed</b> or <b>unmanaged</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>outgoing-interface</b> | <p><b>eth1</b></p> <p><b>Note</b> You have to set this only if you want to enable Cisco Crosswork application access to SR-PCE via the data network interface when using the two NIC configuration.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>preferred-stack</b>    | <p><b>ipv4</b> or <b>ipv6</b> or <b>NOT SET</b>.</p> <p>This property is applicable only for dual stack deployments.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>topology</b>           | <p><b>off</b> or <b>on</b>.</p> <p>This is an optional property. If not specified, the default value is <b>on</b>.</p> <p>If value is specified as <b>off</b>, it means that L3 topology is not accessible for the SR-PCE provider.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



| Property Key     | Value                                                                                                                                                                                                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>pce</code> | <p><code>off</code> or <code>on</code>.</p> <p>This is an optional property. If not specified, the default value is <code>on</code>.</p> <p>If value is specified as <code>off</code>, it means that LSPs and policies are not accessible for the SR-PCE provider.</p> |

**Note** If **managed** or **unmanaged** options are set and you want to delete a device later, you must do one of the following:

- Reconfigure and remove the devices from the network before deleting the device from Crosswork Network Controller. This avoids Crosswork Network Controller from rediscovering and adding the device back.
- Set auto-onboard to **off**, and then delete the device from Crosswork Network Controller. However, doing so will not allow Crosswork Network Controller to detect or auto-onboard any new devices in the network.

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the SR-PCE server. The default is 30 seconds.

**Step 4** When you have completed entries in all of the required fields, click **Save** to add the SR-PCE provider.

**Step 5** Confirm that the SR-PCE provider shows a green Reachability status without any errors. You can also view the Events window (**Administration > Events**) to see if the provider has been configured correctly.

**Step 6** Repeat this process for each SR-PCE provider.



**Note** It is not recommended to modify auto-onboard options once set. If you need to modify them, do the following:

1. Delete the provider and wait until deletion confirmation is displayed in the Events window.
2. Re-add the provider with the updated auto-onboard option.
3. Confirm the provider has been added with the correct auto-onboard option in the Events window.

#### What to do next

- If you entered the **auto-onboard/off** pair, navigate to **Device Management > Network Devices** to add a devices.
- If you opted to automatically onboard devices, navigate to **Device Management > Network Devices** to view the device list. To add more node information such as geographical location details, export the device list (.csv), update it, and import it back. If geographical location data is missing, you will only be able to see device topology using the logical map.

**Return to the installation workflow:**

- VMware: [Install Cisco Crosswork Network Controller on VMware vCenter, on page 11](#)
- AWS EC2: [Install Cisco Crosswork Network Controller on AWS EC2, on page 13](#)



## PART VI

# Upgrade Cisco Crosswork Network Controller

- [Upgrade Cisco Crosswork, on page 213](#)





## CHAPTER 12

# Upgrade Cisco Crosswork

---

This chapter contains the following topics:

- [Upgrade Overview, on page 213](#)
- [Upgrade Requirements, on page 214](#)
- [Upgrade Using Existing Hardware, on page 216](#)
- [Upgrade Using Parallel Hardware, on page 227](#)
- [Update Crosswork Network Controller applications \(standalone activity\) , on page 234](#)

## Upgrade Overview

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



---

**Note** Supported migration scenarios in Crosswork 7.0 (non-geo HA deployments):

- Crosswork 6.0 (IPv4 stack) to Crosswork 7.0 (IPv4 stack)
  - Crosswork 6.0 (IPv6 stack) to Crosswork 7.0 (IPv6 stack)
  - Crosswork 6.0 (IPv4 stack) to Crosswork 7.0 (dual stack)
  - Crosswork 6.0 (IPv6 stack) to Crosswork 7.0 (dual stack)
- 

You can upgrade Cisco Crosswork in the following methods:

1. [Upgrade Using Existing Hardware, on page 216](#)
2. [Upgrade Using Parallel Hardware, on page 227](#)

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.
- For the upgrade from Crosswork 6.0 to 7.0, the Health Insights alert checkbox will be disabled, and an alarm will be raised for the KPI profile having custom KPI.
- Before attempting to load a KPI, ensure that it complies with the requirements of the current release. If you try to load a KPI that was created for a previous release and is not compatible, you will receive an error message.
- 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 Crosswork Network Controller applications \(standalone activity\)](#), on page 234.

## Upgrade Requirements

This section explains the requirements for upgrading the Cisco Crosswork.

### AWS EC2

Record the configuration parameters used in the previous Crosswork cluster and Crosswork Data Gateway deployments. These parameters include:

- VM Node IP addresses
- Elastic Network Interface (ENI) ID mapped to the respective nodes (found under **Networking** tab > **ENI ID**)
- Subnet ID
- Security Group
- Availability Zone (AZ)

If you are using the Crosswork Optimization Engine, and have enabled feature packs (Local Congestion Mitigation, SR Circuit Style Manager, or Bandwidth on Demand) in an earlier version of Crosswork and want to upgrade to the latest version, you must perform the following tasks prior to upgrading:

## LCM

- From the LCM **Configuration** page:
  1. Set the **Delete Tactical SR Policies when Disabled** option to **False**. This task must be done prior to disabling LCM so that tactical policies deployed by LCM remain in the network after the upgrade.
  2. Set the **Enable** option to **False**. If LCM 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 **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 (**Traffic Engineering > Local Congestion Mitigation > Export** icon). Confirm the interfaces are valid by reimporting the CSV file without errors. For more information, see .
- After the upgrade, wait until the **Traffic Engineering** page shows all the nodes and links before enabling LCM

### 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.

## CSM

- Set the **Enable** option to **False**.
- Note all options (Basic and Advanced) in the CSM **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 CSM.
- Circuit Style SR-TE policies will go to operation down (Oper Down) state if CSM is not enabled within 8 hours after disabling.

### 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 Existing Hardware

This section explains how to migrate to the latest version of Crosswork Network Controller 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 the Data Gateway VMs, on page 217](#)
2. [Create Backup and Shut Down Cisco Crosswork, on page 217](#)
3. [Install the latest version of the Crosswork Network Controller Cluster, on page 220](#)



### Important

While the cluster installation is in progress, you must upgrade NSO to version 6.1.11.2. The process to upgrade NSO is not covered in this document. For more information, see the relevant [Cisco NSO documentation](#). You must also upgrade your SR-PCE to version 24.2.1. For install instructions, see the [Cisco IOS XRv 9000 Router Installation Guide](#).

4. [Install the Crosswork Network Controller Applications, on page 221](#)



### Note

You are recommended to download and validate the application CAPP files 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 Crosswork Network Controller Backup, on page 221](#)
6. [Upgrade Crosswork Data Gateway, on page 223](#)
7. [Post-upgrade Checklist, on page 226](#)



After you complete the upgrade steps, you must install the NSO function packs. For the installation instructions, you can either refer to [Install Cisco NSO Function Pack Bundles from Crosswork UI, on page 193](#) or [Install NSO Function Packs Manually, on page 202](#), depending on your preference.

## Shut Down the Data Gateway VMs

This is the first stage of the upgrade workflow.



---

**Note** When the 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 all the tabs in the **Data Gateway Management** page to keep a record of the list of 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 Crosswork Data Gateway, on page 223](#).

---

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

**Step 2** Shut down the data gateway VMs.

a) Log in to the data gateway VM. See [Access Crosswork Data Gateway VM from SSH, on page 124](#).

Crosswork Data Gateway launches an Interactive Console after you log in successfully.

b) Choose **5 Troubleshooting**.

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

**Step 3** **For cloud-based deployment:**

a. Terminate the Crosswork Data Gateway instances for all the previous Crosswork nodes. Do not delete the associated cluster stack.

b. Manually delete the associated ENI IDs.

**Note** Since you are terminating the EC2 instances and not the stack, you must manually delete the associated ENI IDs.

---

## 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 Crosswork Network Controller to a new version.



---

**Note** We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Crosswork Network Controller 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 Crosswork Network Controller cluster and the SCP server must be in the same IP environment. For example: If Crosswork Network Controller 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 new version of Cisco Crosswork. See [Post-upgrade Checklist, on page 226](#) 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 the new version of Cisco Crosswork. 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 Local Congestion Mitigation (LCM), SR Circuit Style Manager (CSM), and Bandwidth on Demand (BWod) are enabled, you must disable them before proceeding. You must also, if available, export the current list of interfaces managed by LCM (**Traffic Engineering > Local Congestion Mitigation > Domain Identifier <domain\_id> > Interface Thresholds > Export**). Follow the steps documented in [Upgrade Requirements, on page 214](#).

---

**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 Crosswork Network Controller 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 Crosswork Network Controller main menu, choose **Administration > Backup and Restore**.
- b) Click **Actions > Data Backup** to display the **Data 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.

**Note** To use the **Backup NSO** option during backup, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail. Follow the instructions given in *Backup Cisco Crosswork with Cisco NSO* section in the *Cisco Crosswork Network Controller 7.0 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 prefilled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

- g) (Optional) Click **Verify Backup Readiness** to verify that Crosswork Network Controller has enough free resources to complete the backup. If the verifications are successful, Crosswork Network Controller 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. Crosswork Network Controller 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 Crosswork Network Controller cluster by powering down the VMs hosting each node (start with the Hybrid VMs):

- **For on-premise deployment:**

- 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 the above steps (a to d) for each of the remaining VMs.
- **For cloud-based deployment:**
    - a. Terminate the EC2 instance for all the previous Crosswork nodes. Do not delete the associated cluster stack.
    - b. Manually delete the associated ENI IDs.
      - Note** Since you are terminating the EC2 instances and not the stack, you will need to manually delete the associated ENI IDs.

**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
```

## Install the latest version of the Crosswork Network Controller Cluster

After the successful backup of the old version of Crosswork Network Controller, proceed to install the latest version of the Crosswork Network Controller cluster.



**Note** The number of VMs installed in the new version of Crosswork Network Controller must be equal or more than the number of VMs in the old version of Crosswork Network Controller.

### Before you begin

- Make sure that your environment meets all the installation prerequisites (see [Installation Prerequisites for VMware vCenter, on page 19](#) for VMware and [Installation Prerequisites for AWS EC2, on page 137](#) for AWS).
- 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 1** **For on-premise deployments:** Install Crosswork Network Controller cluster using the instructions in [Install Crosswork Cluster on VMware vCenter, on page 37](#).

**Step 2** **For cloud-based deployments:** Install Crosswork Network Controller cluster using the template for a single VM (the sample template file (.yaml) can be downloaded from [cisco.com](#)). Deploy the template sequentially for each VM in your cluster, ensuring a minimum interval of 10 minutes between each deployment.

- Important**
- Ensure that you update the parameters (such as VM Node IP addresses, ENI ID, Subnet ID, Security Group, AZ, etc.) in the sample template to match the values used in the previous cluster deployment.
  - The first VM deployed must be configured as the seed node (by setting `IsSeed` as `True`).
  - Each script run should have a unique stack name. Do not use the stack name of the previous cluster. Ensure that you use a unique stack name when deploying each VM.

After the installation is completed for all nodes, verify that the Load Balancer value (**Load balancer > Choose any one Listener > Registered Target groups**) matches the value in the previous cluster stack.

### Step 3

After the installation is completed, log into the Crosswork Network Controller UI. From the Crosswork Network Controller 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.

Ensure all the nodes are up and running in the cluster. Check the health status to confirm everything is functioning correctly.

---

## Install the Crosswork Network Controller Applications

After successfully installing the new version of the Crosswork Network Controller cluster, proceed to install the latest version of the Crosswork Network Controller applications.



---

**Note** The Crosswork Network Controller applications that you install must be the same ones that were backed up during [Create Backup and Shut Down Cisco Crosswork, on page 217](#).

---

**Step 1** Install the Crosswork Network Controller applications using the steps described in [Install Crosswork Applications, on page 183](#).

**Step 2** After the applications are successfully installed, check the health of the new Crosswork Network Controller cluster.

- a) From the Crosswork Network Controller main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
- b) Click **Crosswork Cluster** tile to view the health details of the cluster.

---

## Migrate Crosswork Network Controller Backup

After successfully installing the new versions of the Crosswork Network Controller applications, proceed to migrate the Crosswork Network Controller backup taken earlier to the new Crosswork Network Controller 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 217](#).
- The name and path of the backup file created in [Create Backup and Shut Down Cisco Crosswork, on page 217](#).
- 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:**

- From the main menu, choose **Administration > Backup and Restore**.
- Click **Destination** to display the **Edit Destination** dialog box.
- 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 217](#).

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

**Step 3** **Migrate the previous Crosswork Network Controller backup on the new Crosswork Network Controller cluster:**

- From the Crosswork Network Controller main menu, choose **Administration > Backup and Restore**.
- Click **Actions > Data Migration** to display the **Data Migration** dialog box with the destination server details prefilled.
- Provide the name of the data migration backup (created in [Create Backup and Shut Down Cisco Crosswork, on page 217](#)) in the **Backup File Name** field.
- If you want to perform the data migration backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
- Click **Start Migration** to start the data migration operation. Crosswork Network Controller 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.

- 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.

- 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 new Crosswork Network Controller cluster.

- From the Crosswork Network Controller main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
- Click **Crosswork Cluster** tile to view the health details of the cluster.

## Upgrade Crosswork Data Gateway

This is the final stage of the upgrade workflow. Ensure that the migration is complete and the new Cisco Crosswork UI is available before you proceed with installing the latest version of Crosswork Data Gateway.



**Note** The upgrade procedure is required only for 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 Data Gateway upgrade process consists of the following steps replacing all the old Data Gateway VMs with the Data Gateway VMs in the network.



**Important** Step 8 in this procedure requires you to log out of Cisco Crosswork and log in again after verifying the deployment and enrollment of the latest data gateway VMs with Cisco Crosswork. 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.

### Before you begin

The administrators must assign the Crosscluster API to the user roles. This permission is required for a user to access the Data Gateway Management page.

To assign the API permissions, from the Crosswork UI, go to **Administration > Users and Roles > Roles > Global API permissions > Crosscluster Infra**. For more information on Roles, see the *User Roles, Functional Categories, and Permissions* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

**Step 1** Log out of Cisco Crosswork 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 data gateway VMs with the same number and the same information (management interface importantly) as the old data gateway VMs.

The installation procedure for the new data gateway VMs may vary depending on your data center.

- **For on-premise deployment:**

Follow the steps in the [Crosswork Data Gateway Installation Workflow, on page 91](#).

- **For cloud-based deployment:**

- a. Install the data gateway VM nodes using the sample Crosswork Data Gateway templates (.yaml) which you can download from [cisco.com](https://www.cisco.com). Deploy the templates sequentially for each data gateway VM, ensuring a minimum interval of 10 minutes between each deployment.

- Important**
- Ensure that you update the parameters (such as VM Node IP addresses, ENI ID, Subnet ID, Security Group, AZ, etc.) in the sample template to match the values used in the previous cluster deployment.
  - Each script run should have a unique stack name. Do not use the stack name of the previous cluster. Ensure that you use a unique stack name when deploying each VM.

- b. After a few minutes, verify if the data gateway is operational.

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

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

Figure 44: Data Gateway Instances Window

| Data gateway instance ... | Operational state | Administr... | Data gateway inst... | Pool name | Outage history | Data gatewa... | PDG identifier      | High availability s... | Actions |
|---------------------------|-------------------|--------------|----------------------|-----------|----------------|----------------|---------------------|------------------------|---------|
| cdg-181.cisco.c...        | Error             | Up           | Unassigned           |           |                |                | 95664c0-5a3f-47b... | Not protected          | ...     |
| cdg-186.cisco.c...        | Error             | Up           | Assigned             | test      |                | test-1         | dc9c6c6a-5d54-46... | None planned           | ...     |

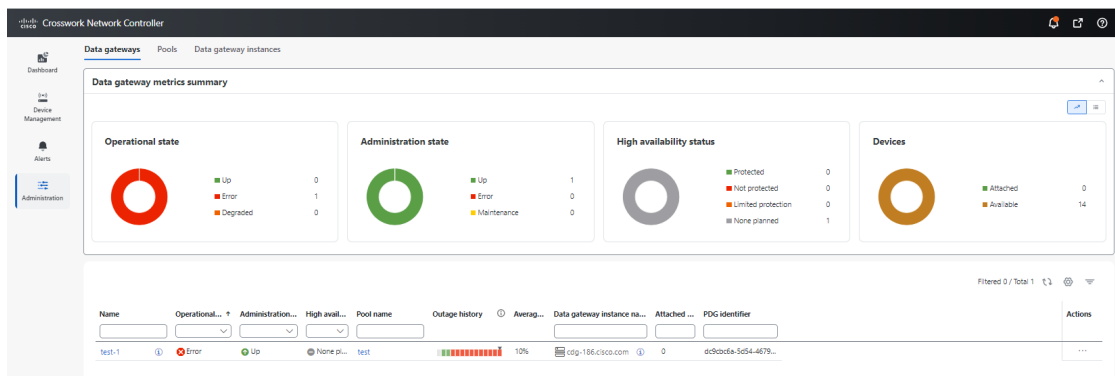
**Step 6** After the **Operational State** of the VMs changes to **Ready**, navigate to the **Pools** tab and verify that all the data gateway pools from the previous version of Cisco Crosswork, are listed here. Edit each data gateway pool to verify that the active data gateway is the same as one that you noted in the previous version of Cisco Crosswork. To view the pool details, click the pool name.

**Important** If you are upgrading the Crosswork Data Gateway from a single stack deployment to a dual stack deployment, edit the pool and specify the VIP IP address of the additional stack. For example, if the pool was created with an IPv4 address, you must provide the IPv6 address. For information on editing a pool, see the *Edit or Delete a Crosswork Data Gateway Pool* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

**Step 7** Verify that devices are attached to the data gateways in the Cisco Crosswork UI.

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

Figure 45: Data Gateway Window



**Step 8** Log out of Cisco Crosswork.

After the upgrade is complete:



- The data gateway VMs are enrolled with Cisco Crosswork.
- All destinations, data gateway pools, device-mapping information can be viewed on the Cisco Crosswork UI with the upgraded data gateway VMs.
- Collection jobs start again automatically with the new data gateway VMs.
- After upgrading the data gateway VM, you must reconfigure the collector resources and the disabled containers. Global Parameter resources that were configured before the upgrade are not retained. To configure the resource parameters, on the Crosswork UI, navigate to **Administration > Data Gateway Global Settings > Data Gateway > Resource**. For more information on the resources, see [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

### What to do next

1. After you log in to the Crosswork Network Collection UI, a window appears prompting for confirmation is displayed. In the pop-up that appears, click **Acknowledge**.



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

2. To move Cisco NSO out of maintenance or read-only mode, use:

```
ncs_cmd -c maapi_read_write
```

## Troubleshoot Crosswork Data Gateway Upgrade Issues

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

| Issue                                                                                                                                                                                                                                                              | Recommended Action                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Some of the data gateway VMs are in <b>Error</b> or <b>Degraded</b> state because you clicked <b>Acknowledge</b> before the VMs came to the <b>Up/Not Ready</b> state                                                                                              | <ol style="list-style-type: none"> <li>1. Wait for the data gateway VMs to have the state as <b>Up</b> or <b>Not Ready</b> state.</li> <li>2. Once the VMs have the state as <b>Up</b> or <b>Not Ready</b>, delete all data gateway pools and create them again.</li> </ol>                                                                                                       |
| Some of the data gateway VMs are in <b>Error</b> or <b>Degraded</b> state because you clicked <b>Acknowledge</b> before the VMs came to the <b>Up/Not Ready</b> state. The state of the VMs did not change to <b>Up/Ready</b> and they are still in <b>Error</b> . | <ol style="list-style-type: none"> <li>1. Delete all data gateway pools.</li> <li>2. Check if the VMs now have the state as <b>Up</b> or <b>Not Ready</b>.</li> <li>3. If the VMs are still in a state of <b>Error</b>, manually re-enroll the VMs with the new version of Cisco Crosswork. See <a href="#">Re-enroll Crosswork Data Gateway</a> for more information.</li> </ol> |

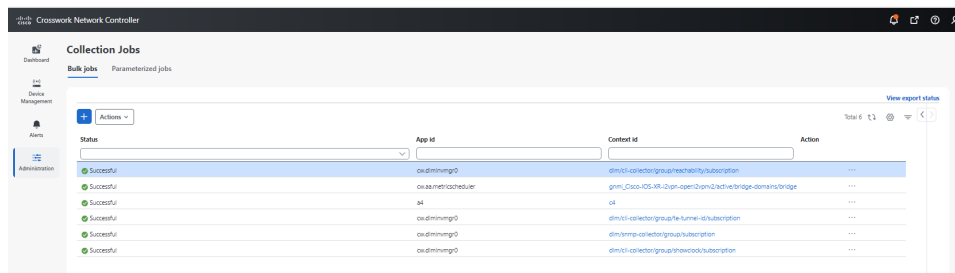
| Issue                                                                                                                                                                                                              | Recommended Action                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| The data gateways VMs are stuck in the <b>Degraded</b> state with Image manager being in exited state. The list of components for the data gateway either do not show Image manager or show it in an exited state. | <ol style="list-style-type: none"> <li>1. In the Cisco Crosswork UI, navigate to <b>Data Gateway Management &gt; Virtual Machines</b>.</li> <li>2. Click the data gateway that is degraded.</li> <li>3. Click <b>Actions</b> and click <b>Reboot</b>.</li> </ol> |

## Post-upgrade Checklist

After you upgrade Cisco Crosswork to the latest version, 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 UI and delete the duplicate system jobs.

**Figure 46: Collection Jobs Window**



- Verify that the collection jobs are running on the data gateway 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 the upgraded Cisco Crosswork.
- (Optional) Based on your network requirements, download the relevant map files from cisco.com and re-upload them to the upgraded Cisco Crosswork.
- (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 the new version of Cisco Crosswork.
- (Optional) If you have saved views in your topology, you may need to re-apply certain settings (such as map configuration, table filters, etc.) as this data might not be fully migrated.
- 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 collection to the external destination is working. Also, check if the alert dashboard is displaying the correct data.

- For Traffic Engineering, perform the following actions:
  - Upgrade the software versions in your devices as per the supported Cisco IOS XE/XR versions documented in the [Traffic Engineering Compatibility Information](#).
  - Verify feature packs (Local Congestion Mitigation (LCM), Bandwidth Optimization (BWOpt), and Bandwidth on Demand (BWoD)) using the instructions in [Upgrade Requirements, on page 214](#).

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 the latest version of Crosswork Network Controller using new hardware. This method relies on installing the new Cisco Crosswork 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.



---

**Attention** Upgrade using parallel hardware is only supported for on-premise deployments. For cloud-based deployments, please follow the instructions in [Upgrade Using Existing Hardware, on page 216](#).

---

The stages of the parallel upgrade workflow are:

1. [Deploy a new Crosswork Network Controller Cluster, on page 227](#)



---

**Important** While the cluster installation is in progress, you must upgrade NSO to version 6.1.11.2. The process to upgrade NSO is not covered in this document. For more information, see the relevant [Cisco NSO documentation](#). You must also upgrade your SR-PCE to version 24.2.1. For install instructions, see the [Cisco IOS XRv 9000 Router Installation Guide](#).

---

2. [Backup Cisco Crosswork Cluster, on page 228](#)
3. [Update DNS Server and Run Migration , on page 230](#)
4. [Add Crosswork Data Gateway to Cisco Crosswork, on page 231](#)
5. [Shut Down the old Cisco Crosswork Cluster, on page 233](#)

After you complete the upgrade steps, you must install the NSO function packs. For the installation instructions, you can either refer to [Install Cisco NSO Function Pack Bundles from Crosswork UI, on page 193](#) or [Install NSO Function Packs Manually, on page 202](#), depending on your preference.

## Deploy a new Crosswork Network Controller Cluster

Install the latest version of Crosswork Network Controller cluster and applications on a new set of VMs in parallel.




---

**Note** The new Crosswork Network Controller cluster must be installed with the same FQDN and same number of nodes as in the old version of Crosswork Network Controller.

---

### Before you begin

- Make sure that your environment meets all the installation prerequisites (see [Installation Prerequisites for VMware vCenter](#), on page 19)

---

**Step 1** Install the new Crosswork Network Controller cluster (see [Install Crosswork Cluster on VMware vCenter](#), on page 37).

**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 Crosswork Network Controller UI by navigating to [https://<NEW\\_VIP>:30603](https://<NEW_VIP>:30603).

**Step 3** Check if all the nodes are up and running in the cluster.

- From the Crosswork Network Controller 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 Crosswork Network Controller. For more information, see [Install Crosswork Applications](#), on page 183.

**Step 5** After the applications are successfully installed, check the health of the new Crosswork Network Controller 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 Crosswork Network Controller cluster and the SCP server must be in the same IP environment. For example: If Crosswork Network Controller 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 upgrading Cisco Crosswork. See [Post-upgrade Checklist, on page 226](#) 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 the upgraded Cisco Crosswork. 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 214](#).




---

**Note** We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Crosswork Network Controller 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 Crosswork Network Controller 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 Crosswork Network Controller 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** check box if you don't want to include Cisco NSO data in the backup.

**Note** To use the **Backup NSO** option during backup, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail. Follow the instructions given in *Backup Cisco Crosswork with Cisco NSO* section in the *Cisco Crosswork Network Controller 7.0 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 prefilled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

- g) (Optional) Click **Verify Backup Readiness** to verify that Crosswork Network Controller has enough free resources to complete the backup. Crosswork Network Controller will also confirm that none of the applications are being updated, if the remote destination is correctly defined and if the applications are healthy. If the verifications are successful, Crosswork Network Controller 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. Crosswork Network Controller 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 Crosswork Network Controller cluster to the <VIP> of the new Crosswork Network Controller cluster.

**Step 2** Navigate to the upgraded Cisco Crosswork UI 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 228](#).

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

**Step 4** **Migrate the old Crosswork Network Controller backup:**

- a) From the Crosswork Network Controller 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 228](#)) in the **Backup File Name** field.
- d) If you want to perform the data migration backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
- e) Click **Start Migration** to start the data migration operation. Crosswork Network Controller 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 new Crosswork Network Controller cluster.

- a) From the Crosswork Network Controller 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 to Cisco Crosswork

Ensure that the migration is complete and the new Cisco Crosswork UI is available before you proceed with installing the new version of Crosswork Data Gateway.



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

Crosswork Data Gateway functions because a passive device in the network. The Crosswork Data Gateway upgrade process consists of replacing all old data gateway VMs with the new data gateway VMs (latest version) in the network.



**Important** Step 6 in this procedure requires you to log out of Cisco Crosswork and log in again after verifying the deployment and enrollment of the new data gateway VMs with Cisco Crosswork. 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 that are mentioned in Step 3, Step 4 and Step 5 in the procedure.

- Step 1** Log out of the upgraded Cisco Crosswork 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 data gateway VMs (latest version) with the same number and the same information (management interface importantly) as the old data gateway VMs. Follow the steps in the [Crosswork Data Gateway Installation Workflow, on page 91](#).
- Step 4** Wait for about 5 minutes and navigate to **Administration > Data Gateway Management**.
- Step 5** Check the **Data Gateway Instances** tab to verify that the new data gateway VMs are enrolled with the new Cisco Crosswork, and have the **Admin State** as **Up** and **Operational State** as **Not Ready**.

*Figure 47: Data Gateway Instances Window*

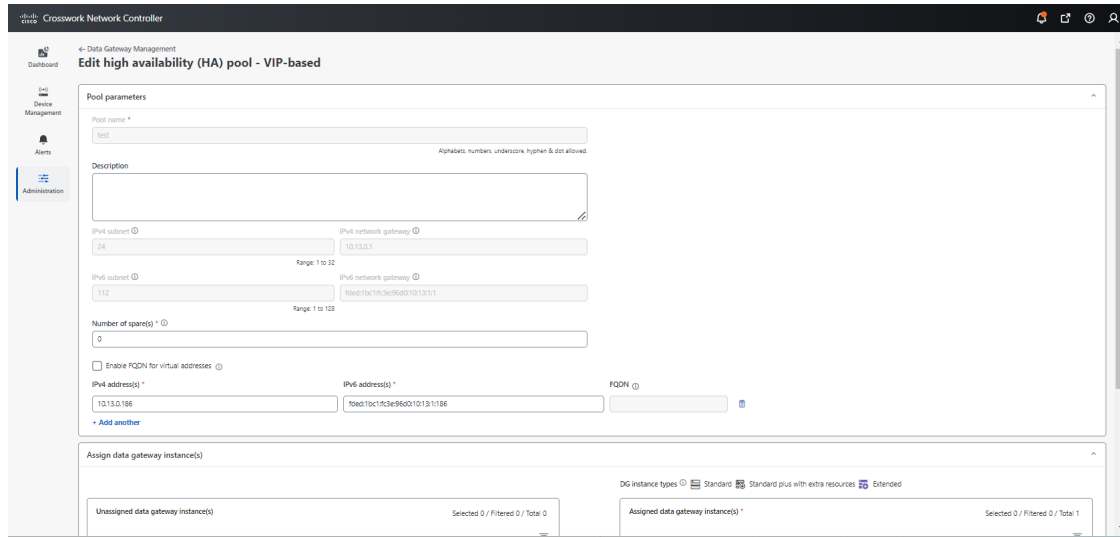
| Data gateway instance ... | Operational state | Administr... | Data gateway inst... | Pool name | Outage history | Data gatewa... | PDG identifier       | High availability s... | Actions |
|---------------------------|-------------------|--------------|----------------------|-----------|----------------|----------------|----------------------|------------------------|---------|
| cdg-181.cisco.c...        | Error             | Up           | Unassigned           |           |                |                | 956864c0-5a3f-47b... | Not protected          | ...     |
| cdg-186.cisco.c...        | Error             | Up           | Assigned             | test      |                | test-1         | dc9c6a-5d54-46...    | None planned           | ...     |

- 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 old 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 older version of Cisco Crosswork.

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



Figure 48: Edit HA Pool Window



**Step 7** Verify that devices are attached to the new data gateways in the upgraded Cisco Crosswork UI.

- a) Navigate to the **Administration > Data Gateway Management** page.
- b) Check the **Attached Device Count** of the data gateway.

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

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

**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** To move Cisco NSO out of maintenance or read-only mode, use:

```
ncs_cmd -c maapi_read_write
```

After the upgrade is complete:

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

## Shut Down the old Cisco Crosswork Cluster

### Before you begin

Gather the following information before shutting down the older 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 Crosswork Network Controller 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 data gateway VMs.
- Log in to the previous version of the data gateway VM. See [Access Crosswork Data Gateway VM from SSH, on page 124](#).  
Crosswork Data Gateway launches an Interactive Console after you login successfully.
  - Choose **5 Troubleshooting**.
  - 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 relevant [Cisco NSO documentation](#).
-

Update Crosswork Network Controller applications (standalone activity)

This section explains how to independently update Crosswork Network Controller applications 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.

The Crosswork Network Controller applications are offered as **Essentials**, **Advantage**, and **Add-on** packages. Every package contains crosswork applications in a particular format unique to Crosswork known as CAPP (Crosswork APPLication).

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 Network Controller package 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. 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](https://www.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 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 signed-cw-na-coe-7.0.0-78-release700-240816.tar.gz
```

```
ff47a72ed7dc4fc4be388db3a43fa13f
```

Verify that the result value matches with the posted value on [cisco.com](https://www.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**.**Step 5** To upgrade, click the Upgrade prompt and the new version of the application is installed. Alternately, click  on the tile, and select the **Upgrade** option from the drop down list.

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

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

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

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



PART **VII**

Uninstall Cisco Crosswork Network Controller

- [Uninstall Cisco Crosswork, on page 239](#)



CHAPTER 13

Uninstall Cisco Crosswork

This chapter contains the following topics:

- [Uninstall the Crosswork Cluster, on page 239](#)
- [Uninstall Crosswork Data Gateway, on page 240](#)
- [Uninstall Crosswork Applications, on page 242](#)

Uninstall the Crosswork Cluster

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

- [Delete the VM using the Cluster Installer Tool, on page 239](#)
- [Delete the VM using the vSphere UI, on page 240](#)

Delete the VM using the Cluster Installer Tool

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 Crosswork Network Controller 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* topic in the [Cisco Crosswork Network Controller 7.0 Administration Guide](#).
 - Delete the Crosswork Data Gateway VM from Crosswork Network Controller 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 Crosswork Data Gateway.

- [Delete the Data Gateway VM from Cisco Crosswork, on page 241](#)
- [Delete Crosswork Data Gateway from the Crosswork Cluster, on page 241](#)

Delete the Data Gateway VM from Cisco Crosswork

Before you begin

The data gateway VM you want to delete:

- Must be in the maintenance mode.
- Must not be a part of a pool or attached to a device.


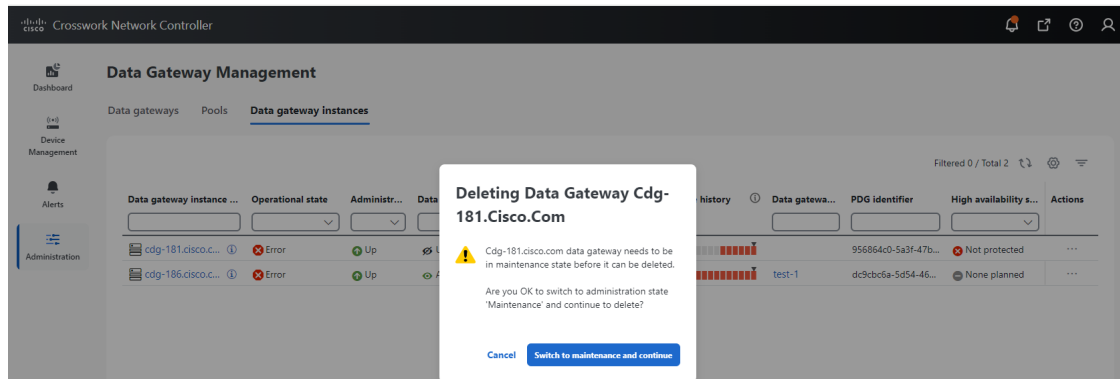
-
- Step 1** Log into Crosswork Network Controller UI.
- Step 2** From the navigation panel, select **Administration > Data Gateway Management**.
Click the **Data Gateway Instances** tab.
- Step 3** In the **Data Gateway Instances** list, find the data gateway instance you want to delete and click  under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

Figure 49: Switch to Maintenance and Continue Pop-up Window



The data gateway instance is deleted.

Delete Crosswork Data Gateway from the Crosswork Cluster

To remove a data gateway from the Crosswork cluster, follow the below steps:

-
- Step 1** Remove the data gateway instance from the Crosswork UI. Note down the **Data Gateway Instance Name** and **PDG Identifier** from the Crosswork UI.
- Step 2** Execute the following commands to remove the pods from the Crosswork cluster:
- `kubectl edit cdgoperator cdgoperator-cr -n cdg`

- If there is only one data gateway in the cluster, remove the CDG array **including** `cdg_dep_plan` under the **spec** section.
 - If there are more than one data gateway in the cluster, remove only the data gateway array entry **under** `cdg_dep_plan` which has to be deleted and save it.
- `kubectl delete infraservices <Data Gateway Instance Name> -n cdg`
For example, `kubectl delete infraservices op-cdg -n cdg`
 - `kubectl delete collectors collector-<PDG Identifier> -n cdg`
For example, `kubectl delete collectors collector-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg`
 - `kubectl delete icon icon-<PDG Identifier> -n cdg`
For example, `kubectl delete icon icon-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg`
 - If offload pods are present, `kubectl delete offload offload-<PDG Identifier> -n cdg`
For example, `kubectl delete offload offload-26b0053f-5132-4379-a107-f924dfde77f4 -n cdg`

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.

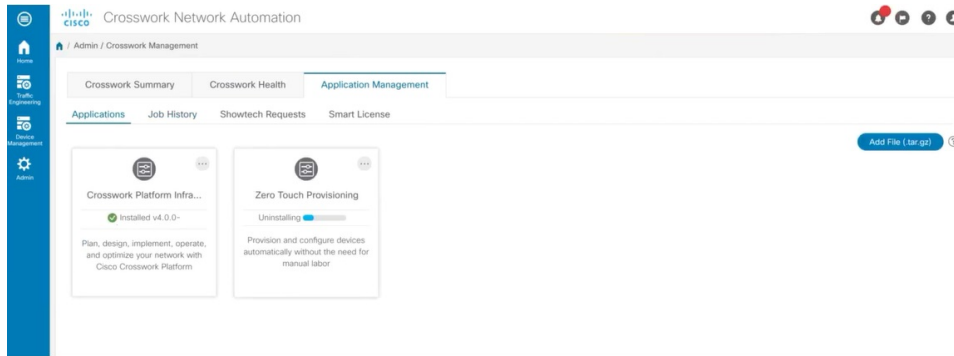
Step 1 Click on **Admin > Crosswork Manager**, and select the **Application Management** tab.

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.

Step 3 Click **Uninstall** to confirm when prompted.

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

Figure 50: Application Management Window

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.



PART **VIII**

Enable Geo Redundancy

- [Geo Redundancy Overview, on page 247](#)
- [Geo Redundancy Requirements, on page 249](#)
- [Enable Geo Redundancy Solution, on page 253](#)
- [Geo Redundancy Switchover, on page 271](#)
- [Upgrade to Geo Redundancy Solution, on page 277](#)



CHAPTER 14

Geo Redundancy Overview

This chapter contains the following topics:

- [Introduction, on page 247](#)

Introduction

The chapters in this part explain the requirements and processes to install or upgrade Geo Redundancy in the Crosswork Network Controller solution.



Attention Geo Redundancy is an optional functionality offered by Crosswork Network Controller solution. For any assistance, please contact the Cisco Customer Experience team.

The geo redundancy solution ensures business continuity in case of a region or data center failure for on-premise deployment. It adds another layer of protection in the high availability stack for Crosswork through geographical or site redundancy. Geo redundancy protects against entire site failure, reduces disruption during system upgrades, and reduces overall data loss.

Geo redundancy involves placing physical servers in geographically diverse availability zones (AZ) or data centers (DC) to safeguard against catastrophic events and natural disasters.

Some of the key factors that ensure geo redundancy are:

- *VM Node availability*: Ensure that both the active and standby clusters are configured with the same number of virtual machines (cluster nodes, NSO, Crosswork Data Gateway, etc.) and maintain same level of network accessibility between the clusters and the network nodes.
- *Geo availability of Nodes*: Physical data centers must not share any common infrastructure, such as power and network connectivity. It is recommended to place them in different availability zones (AZ) or regions to avoid a single point of failure that could impact all the VM nodes.
- *Network Availability*: To keep the clusters synchronized, the network link between the data centers must meet the availability and latency requirements detailed later in this chapter.



CHAPTER 15

Geo Redundancy Requirements

This chapter contains the following topics:

- [Crosswork Cluster Requirements](#), on page 249
- [Crosswork Data Gateway Requirements](#), on page 250
- [Unified Endpoint Requirements](#), on page 250
- [Data Store Roles](#), on page 250

Crosswork Cluster Requirements

Geo redundancy solution requires double the number of VMs required for a regular Crosswork Cluster installation. For more information, see [Installation Prerequisites for VMware vCenter](#), on page 19.

Ports Requirements

The additional ports, 30180 and 30190, are outside the normal Crosswork cluster deployment. Both ports are used for database replication (PQ binary protocol) and are secured by SSL.

Important Notes

- To ensure synchronization between the clusters, the network connection between the data centers should be set up with a minimum bandwidth of 5 Gbps and a latency of less than 100 milliseconds.
- While preparing inventory file, you must include details of cluster constituents along with connectivity information.
- Setup the DNS server for your setup. The DNS server should resolve the unified multi-cluster FQDN domain (for example, *.cw.cisco) you want to use and be reachable from both the clusters, Crosswork Data Gateway, NSO, and SR-PCE. For more information on DNS setup procedure, see the [Cisco Prime Network Registrar Caching and Authoritative DNS User Guide](#).
- The DNS server should forward any outside domains to the external DNS servers.
- Crosswork cluster and Crosswork Data Gateway deployments should be configured in dual stack mode, with the geo FQDN pointing to the dual stack IP addresses.
- You should sequentially bring up the active and standby clusters using the existing installer mechanism. Ensure you use the previously identified DNS server during the installation of the Crosswork cluster, Crosswork Data Gateway, and NSO. It is recommended to have multiple DNS servers, with one in each data center.

- Applications should be installed only after enabling geo redundancy and completing the initial on-demand synchronization. Begin by installing applications on the active cluster, followed by the standby cluster.
- Other configuration information (such as devices, providers, or destinations) must be onboarded only on the active cluster and will be synchronized between the clusters as part of the activation process.
- Before enabling geo redundancy mode, you are recommended to make a backup of the active and standby cluster.


Warning

Once the geo redundancy mode is set up, it cannot be undone because the certificates are regenerated using common root CA. To revert to non-geo redundancy mode, you must restore the backup made prior to enabling the geo redundancy mode.

Crosswork Data Gateway Requirements

Confirm that you have met the minimum requirements outlined for Crosswork Data Gateway installation. For more information, see [Installation Prerequisites for VMware vCenter](#).

Unified Endpoint Requirements

- Unified endpoint hides multiple instances in high availability for various components.
- DNS allows endpoints to be referred via Fully Qualified Domain Name (FQDN), which should point to the active instance IP.
- Domain zone provisioning is needed where Crosswork components have IP addresses mapped to FQDN.
- The DNS authoritative server must have an A or AAAA entry for the IP address from you for the domain zone dedicated to Crosswork components.

Data Store Roles

Following roles are applicable for both Geo HA or non-Geo HA deployments when Postgres or Timeseries data stores are operational:

- **Leader:** should be in `running` status.
- **Replica:** indicates a regular standby.
- **Sync Standby:** similar to standby replica, but applicable when synchronous mode is ON in `postgresql.conf`.

For *robot-postgres*, when synchronous mode is ON, the replica is assigned the Sync Standby role. For *cw-timeseries-db*, when synchronous mode is OFF, the replica retains the Replica role. The state will be `streaming` on the respective replica to indicate that local replication is occurring correctly within the PG cluster.

Additionally, in Geo HA deployments, when Cross Cluster replication is enabled and the standby cluster is streaming from a remote active cluster, its leader will assume the **Standby Leader** role, and the status will be `streaming`.

Sync operation

One of the initial steps in a synchronization operation cycle involves setting up asynchronous data replication for local Postgres and Timescale data stores. The system first verifies the health status of the data store. It then aligns the Cross Cluster state and data store state to ensure consistency (for example, if the service `cw-timeseries-db-0` is already active for Timescale DB, the system will assign the `ACTIVE_REPLICATION_ROLE` to the Timescale data store). After setting the role for the active side, the system will replicate this process for the standby side. Once asynchronous replication is complete, the system initiates backup and restore operations (e.g., for the Neo4J data store). These operations can also be monitored in the **Backup and restore jobs** window.

During a sync, the data stores in active and standby clusters have some expected roles. After the sync, the data store roles are verified to confirm a successful sync. The active cluster should contain one Leader with `running` status. See the example below of the Postgres and Timescale data stores on an active cluster.

Figure 51: Roles in an active cluster during sync

```

root@192-168-133-179-hybrid:/home/cw-admin# rpg
robot-postgres-0:/# patronictl list
+ Cluster: robot-postgres (7308802285703659589) -----+-----+-----+
| Member          | Host       | Role      | State   | TL | Lag in MB |
+-----+-----+-----+-----+-----+-----+
| robot-postgres-0 | 10.244.68.8 | Leader    | running | 2  |           |
| robot-postgres-1 | 10.244.21.12 | Sync Standby | streaming | 2  | 0         |
+-----+-----+-----+-----+-----+-----+
robot-postgres-0:/# exit
exit
root@192-168-133-179-hybrid:/home/cw-admin# kubectl exec -it cw-timeseries-db-0 -- bash
cw-timeseries-db-0:/# patronictl list
+ Cluster: cw-timeseries-db (7308804407218782284) -----+-----+-----+
| Member          | Host       | Role      | State   | TL | Lag in MB |
+-----+-----+-----+-----+-----+-----+
| cw-timeseries-db-0 | 10.244.251.13 | Leader    | running | 3  |           |
| cw-timeseries-db-1 | 10.244.21.14 | Replica   | streaming | 3  | 0         |
+-----+-----+-----+-----+-----+-----+

```

Similarly, the standby cluster should contain one Standby Leader with `streaming` status. See the example below of the Postgres and Timescale data stores on a standby cluster.

Figure 52: Roles in a standby cluster during sync

```

cw-admin@192-168-133-165-hybrid:~$ sudo su
[sudo] password for cw-admin:
root@192-168-133-165-hybrid:/home/cw-admin# rpg
robot-postgres-1:/# patronictl list
+ Cluster: robot-postgres (7308802285703659589) ----+-----+-----+-----+
| Member          | Host          | Role          | State    | TL | Lag in MB |
+-----+-----+-----+-----+
| robot-postgres-0 | 10.244.131.12 | Sync Standby | streaming | 2 | 0 |
| robot-postgres-1 | 10.244.27.8   | Standby Leader | streaming | 2 |  |
+-----+-----+-----+-----+
robot-postgres-1:/# exit
exit
root@192-168-133-165-hybrid:/home/cw-admin# kubectl exec -it cw-timeseries-db-0 -- bash
cw-timeseries-db-0:/# patronictl list
+ Cluster: cw-timeseries-db (7308804407218782284) ---+-----+-----+-----+
| Member          | Host          | Role          | State    | TL | Lag in MB |
+-----+-----+-----+-----+
| cw-timeseries-db-0 | 10.244.76.12 | Replica       | streaming | 3 | 0 |
| cw-timeseries-db-1 | 10.244.27.10 | Standby Leader | streaming | 3 |  |
+-----+-----+-----+-----+
cw-timeseries-db-0:/#

```



CHAPTER 16

Enable Geo Redundancy Solution

This chapter contains the following topics:

- [Geo Redundancy Workflow \(Day 0\)](#), on page 253
- [Geo Redundancy Scenarios](#), on page 266
- [Install Geo High Availability Crosswork Data Gateway](#), on page 268
- [Geo Redundancy Workflow \(Day N\)](#), on page 268

Geo Redundancy Workflow (Day 0)

This topic explains the workflow to enable geo redundancy on day 0. The workflow provides a high-level description of the tasks required to install and enable geo redundancy in Crosswork Network Controller.



Note The recommended day 0 setup for enabling geo redundancy is an empty Crosswork cluster (without any applications, devices or data gateways onboarded).

The following table describes the stages to install and enable the geo redundancy mode on Crosswork Network Controller.

Table 59: Geo Redundancy Workflow (Day 0)

Step	Action
1. Install the Active Crosswork cluster.	Install using your preferred method: <ul style="list-style-type: none">• <i>Using cluster installer tool:</i> Install Cisco Crosswork on VMware vCenter using the Cluster Installer Tool, on page 47• <i>Manual Installation:</i> Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 60 Verify if the installation was successful, and log into the Cisco Crosswork UI. <ul style="list-style-type: none">• Monitor Cluster Activation, on page 73• Log into the Cisco Crosswork UI, on page 76
2. Install the Standby Crosswork cluster.	

Step	Action
3. Validate the Crosswork Inventory.	In case of manual installation of Crosswork Cluster, you must import a cluster inventory file (.yaml file) to the Crosswork UI. For more information, see the Import Cluster Inventory, on page 78 topic. Important If you fail to ensure this step, the geo redundancy enablement will fail.
4. Create a backup of your Crosswork cluster.	Follow the instructions in <i>Manage Backups</i> chapter in <i>Cisco Crosswork Network Controller 7.0 Administration Guide</i> .
5. Perform the connectivity checks.	Follow the instructions in Connectivity Checks, on page 255 topic.
6. Prepare and upload the cross cluster inventory template in the Active and Standby clusters to enable geo redundancy.	Follow the instructions in Enable Geo Redundancy, on page 256 topic.
7. Verify that the geo redundancy was successfully enabled on the active and standby clusters.	Follow the instructions in View Cross Cluster Status, on page 260 topic. Check the following: <ul style="list-style-type: none"> • In the Cross Cluster Health Status, ensure the operational state is Connected. • In the Cross Cluster Health Status, ensure that Active cluster state is Healthy. • In the Cross Cluster Health Status, ensure that Standby cluster state is Healthy. • In the Cross Cluster Health Status, ensure the High Availability state is AVAILABLE. • Verify if the heartbeat count between the clusters is incrementing and no failures are observed for over a 30-minute period. • Confirm the completion of one successful sync between the clusters.
8. Configure the cross cluster settings	Follow the instructions in topics below: <ul style="list-style-type: none"> • Cross Cluster settings: Configure Cross Cluster Settings, on page 262 • (Optional) Notification settings: Configure Cross Cluster Notification Settings, on page 265
9. Complete an on-demand sync operation successfully.	On the Cross Cluster window, select Actions > Synchronize to initiate the sync operation.

Step	Action
10. Install the Crosswork Applications on the active cluster	Follow the instructions in Install Crosswork Applications, on page 183 topic.
11. Install the Crosswork Applications on the standby cluster	<p>Once geo redundancy is enabled, a Geo Redundancy tile is added to the Application management window. This tile is built-in and cannot be upgraded, uninstalled, or deactivated.</p> <p>Warning</p> <ul style="list-style-type: none"> • Parallel installation of applications on the active and standby clusters should be avoided. Complete the installation on the active cluster before proceeding with the installation on the standby cluster. • Applications should not be installed during a periodic or on-demand sync operation. Ensure there is sufficient time for the installation to complete before initiating a sync, and verify that no sync operation is in progress before installing an application. It is recommended to temporarily disable periodic sync when installing applications.
12. Install and enroll Crosswork Data Gateway, and onboard devices.	Follow the instructions in Install Geo High Availability Crosswork Data Gateway, on page 268 topic.

Connectivity Checks

Perform the following connectivity checks before enabling geo redundancy:

- Copy (using SCP) a file from Availability Zone 1 (AZ1) to Availability Zone 2 (AZ2), and from AZ2 to AZ1 in corresponding Crosswork VMs and Crosswork Orchestrator pods to ensure connectivity between both clusters.

```
# Perform the below steps from AZ1 to AZ2, and from AZ2 to AZ1:
```

```

cw-admin@192-168-6-101-hybrid:~$ sudo su
[sudo] password for cw-admin:
root@192-168-6-101-hybrid:/home/cw-admin # kubectl exec -it -n=kube-system
robot-orch-76856487-562w6 -- bash
robot-orch-76856487-562w6:~ # touch t.txt
robot-orch-76856487-562w6:~ # scp t.txt
cw-admin@YOUR_PEER_CLUSTER_MGMT_VIP:/home/cw-admin/
(cw-admin@192.168.5.100) Password:
t.txt

robot-orch-76856487-562w6:~# scp t.txt cw-admin@YOUR_PEER_CLUSTER_DATA_VIP:/home/cw-admin/
(cw-admin@192.168.5.100) Password:
t.txt

```

- Mesh connectivity is required between Crosswork Network Controller, Crosswork Data Gateway, NSO, and data interface components across the AZs.
- L2/L3 connectivity is supported.
- Test the DNS resolution on system wide DNS server.

```

### Internal Authoritative resolution

dig @your_dns_server_ip your_name.cw.cisco

; <<>> DiG 9.10.6 <<>> @172.28.122.84 geomanagement.cw.cisco
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8167
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; QUESTION SECTION:
;your_name.cw.cisco.          IN A

; ANSWER SECTION:
your_name.cw.cisco. 5     IN A   192.168.6.100

; Query time: 126 msec
; SERVER: 172.28.122.84#53(172.28.122.84)
; WHEN: Fri Jun 30 23:47:51 PDT 2023
; MSG SIZE rcvd: 67

### External forwarding and resolution

dig @your_dns_server_ip ntp.esl.cisco.com

; <<>> DiG 9.10.6 <<>> @172.28.122.84 ntp.esl.cisco.com
; (1 server found)
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43986
; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; QUESTION SECTION:
;ntp.esl.cisco.com.          IN A

; ANSWER SECTION:
ntp.esl.cisco.com. 1     IN A   171.68.38.66

; Query time: 311 msec
; SERVER: 172.28.122.84#53(172.28.122.84)
; WHEN: Fri Jun 30 23:46:37 PDT 2023
; MSG SIZE rcvd: 62

```

- Verify if the DNS TTL in your VM is less than 60 seconds (< 60s).

```

# DNS TTL with 5s for FQDN entry

cw-user@admin-M-C2EM ~ % dig +nocmd +noall +answer @your_dns_server_ip your_fqdn
geomanagement.cw.cisco. 60 IN A   192.168.6.100

```

Enable Geo Redundancy

This topic explains the procedure to enable geo redundancy from Crosswork UI. Geo redundancy can be configured at any time after the active cluster is built. The process does vary slightly if the standby cluster is not built and activated within 6 hours of the active cluster. These variations are clearly noted in this procedure.



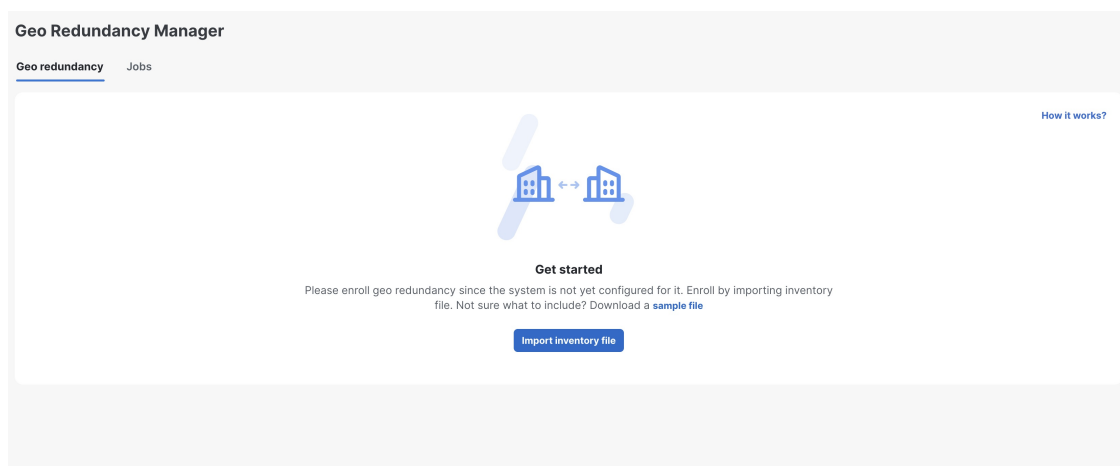
Tip Click on **How it works?** link to view a visual representation of how geo redundancy is enabled.

Before you begin

Ensure you have met all the requirements specified in [Geo Redundancy Requirements, on page 249](#).

- Step 1** Log in to the Crosswork cluster that will function as the active cluster.
- Step 2** From the main menu, choose **Administration > Geo Redundancy Manager**. The **Geo Redundancy Manager** window is displayed.

Figure 53: Geo Redundancy Manager



- Step 3** Click on **sample file** to download the sample template (.yaml file) for the cross cluster inventory (for more details, see [Sample Cross Cluster Inventory Template](#)). Fill the template file with the relevant information for active and standby clusters and the unified cross cluster.

Note In a dual stack configuration, only IPv6 addresses are supported for cross-cluster inventory, even if both IPv4 and IPv6 addresses are present. IPv4 addresses are supported in a single stack configuration.

- Step 4** Click **Import inventory file**, and the **Import Inventory File** dialog box is displayed. Click **Browse** and select the cross cluster inventory file that you prepared. Verify the contents of the template file.
- Step 5** In this step you will be configuring the server to be used with Geo Redundancy. **This step cannot be undone**. You should have already made a backup of you cluster before proceeding with this action. To activate Geo Redundancy on the server, click **Enroll**. A service interruption alert is displayed. Click **Proceed** to continue.

The progress can be viewed from the **Jobs** window, or by clicking the  icon.

- Step 6** After inventory upload is completed in the first cluster, the same process must be repeated in the second cluster. Log in to the Crosswork cluster that will function as the standby cluster, and repeat the actions in steps 4 and 5.

Important Please enable **Pairing mode** if the standby cluster is activated more than 6 hours after the active cluster.

After the standby cluster is configured, the **Job status** will be displayed as **Completed** on both clusters.

Figure 54: Geo Redundancy Jobs

Geo Redundancy Manager

Geo redundancy Jobs

Job sets

Status	Job ID	Description	User
Completed	GJ1	Activate geo mode	admin

Job details

Job ID: GJ1 | Job status: Completed | User: admin | Completion time: 10 mins 27 secs

Time stamp	Description
16-Jul-2024 04:33:47 PM IST	Published geo mode setup done notifications. Job execution duration :10m27.584653714s
16-Jul-2024 04:33:42 PM IST	Ready for peer cluster enrollment
16-Jul-2024 04:33:42 PM IST	Geo Mode setup done
16-Jul-2024 04:33:35 PM IST	Dumping encrypted certificates
16-Jul-2024 04:33:35 PM IST	Encrypting certificates
16-Jul-2024 04:33:35 PM IST	Getting generated certificates
16-Jul-2024 04:33:35 PM IST	Getting regenerated common certificates
16-Jul-2024 04:33:35 PM IST	Preparing system for pairing
16-Jul-2024 04:33:35 PM IST	Activated Geo capp
16-Jul-2024 04:31:14 PM IST	Installing And Activating Geo capp
16-Jul-2024 04:31:14 PM IST	All tyk/cas pods are running
16-Jul-2024 04:31:04 PM IST	Waiting for all tyk/cas pods to be ready
16-Jul-2024 04:30:57 PM IST	Recreating controller.pem

Once the inventory upload is successfully completed on both clusters, the status will be updated in the **Geo Redundancy Manager** window.

Figure 55: Geo Redundancy Status Update

Geo Redundancy Manager

Geo redundancy status

cluster-sjc

Setup done

16.17.0.21 (Logged in)

San Jose

cluster-nyc

Setup done

160.170.0.21

New York

Cross cluster inventory

View, re-import inventory

[View inventory](#) [Re-import](#)

Pairing mode

Disabled

Pairing mode is disabled

The next section contains a sample for your reference. To continue with the activation, see .

Step 7

The next section contains a sample cross cluster inventory template for your reference. To continue with the activation, see [View Cross Cluster Status, on page 260](#).

Sample Cross Cluster Inventory Template

Here is an example of the cross cluster inventory file (.yaml) that you need to prepare to enable geo redundancy:



- Note**
- Cross Cluster inventory supports only IPv6 addresses. If both IPv4 and IPv6 addresses are present, only the IPv6 addresses will be used. If the Cross Cluster inventory is provided with only IPv4 addresses, the system will generate an error.
 - For details on each parameter, see the **sample file** downloaded from the **Geo Redundancy Manager** window.

```
---
meta_version: 1.0.0
crosscluster_name: mycnc-lhs-geo-cluster-ipv6
crosscluster_unified_connectivity:
  unified_end_point:
    unified_endpoint_type:
      fqdn_type: {}
    unified_endpoint_implementation: DNS
  management_fqdn:
    domain_name: cw.cisco
    host_name: geomangement
  data_fqdn:
    domain_name: cw.cisco
    host_name: geodata
clusters:
- cluster_name: geo-lhs-cluster-ipv6
  initial_preferred_leadership_state: ACTIVE
  connectivity:
    unified_end_point:
      unified_endpoint_type:
        ip_type: {}
      unified_endpoint_implementation: VRRP
    data_vip: fded:1bc1:fc3e:96d0:10:10:10:50
    data_vip_mask: 112
    management_vip_mask: 112
    management_vip: fded:1bc1:fc3e:96d0:192:168:5:50
  site_location:
    location: San Jose
  cluster_credential:
    https_credential:
      username: admin
      password: "*****"
    ssh_credential:
      username: cw-admin
      password: "*****"
- cluster_name: mycnc-geo-rhs-cluster-ipv6
  initial_preferred_leadership_state: STANDBY
  connectivity:
    unified_end_point:
      unified_endpoint_type:
        ip_type: {}
      unified_endpoint_implementation: VRRP
    data_vip: fded:1bc1:fc3e:96d0:10:10:11:50
    data_vip_mask: 112
    management_vip_mask: 112
    management_vip: fded:1bc1:fc3e:96d0:192:168:6:150
  site_location:
    location: New York
```

```
cluster_credential:
  https_credential:
    username: admin
    password: "*****"
  ssh_credential:
    username: cw-admin
    password: "*****"
secret: Your-secret1
is_post_migration_activation: false
is_skip_peer_check_enabled: false
```

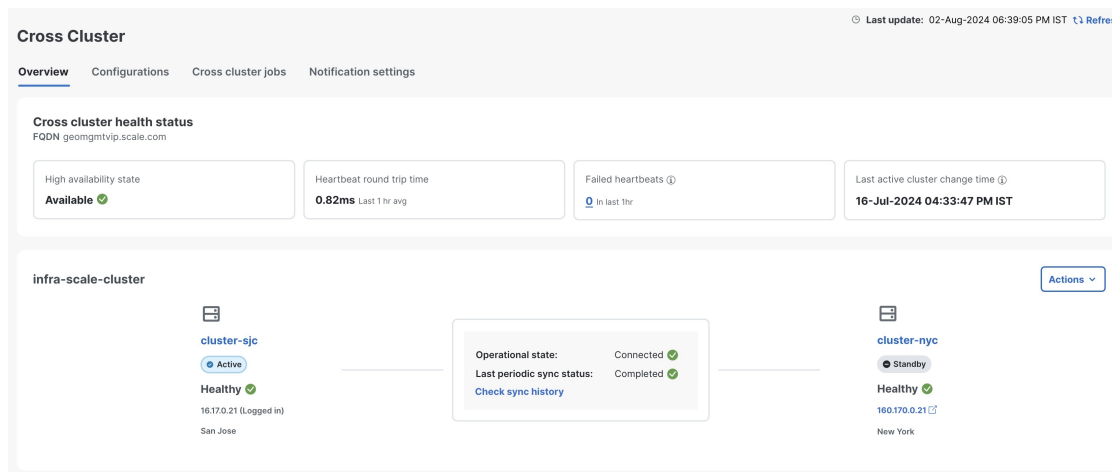
View Cross Cluster Status

This topic explains how to view the cross cluster status after successfully enabling geo redundancy.

Step 1 From the main menu, choose **Administration > Cross Cluster**. The **Cross Cluster** window is displayed.

The cross cluster health status is displayed along with the high availability state, heartbeats round trip time, failed heartbeats, and last active cluster change time. You can also view the status of the active and standby clusters along with the operational state and last sync status.

Figure 56: Cross Cluster window



Scroll further down to see the data store replication states. The **Data stores** table will show all the different data stores that have been replicated along with the lag info for them.

- Each **Data store type** has a corresponding **Sync type**. Postgres and Timescale data stores support live synchronization, while Neo4J and gluster are updated via periodic sync.

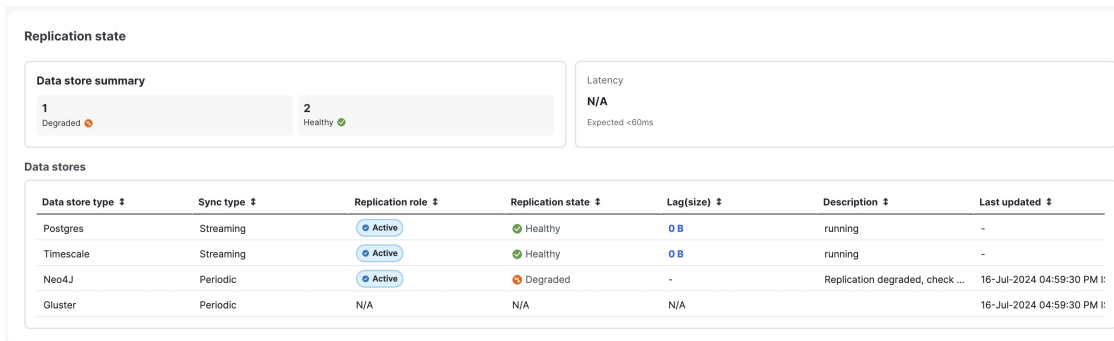
Table 60: Data store types

Data store type	Sync type
Postgres	Streaming
Timescale	Streaming
Neo4J	Periodic

Data store type	Sync type
Gluster	Periodic

- The **Replication role** displays the role of the cluster. For example, the value for an active cluster will be *Active*.
- The **Replication state** displays the status of the data store.
- The **Lag(size)** value indicates the lag between the active and standby clusters.

Figure 57: Cross Cluster window - Replication state

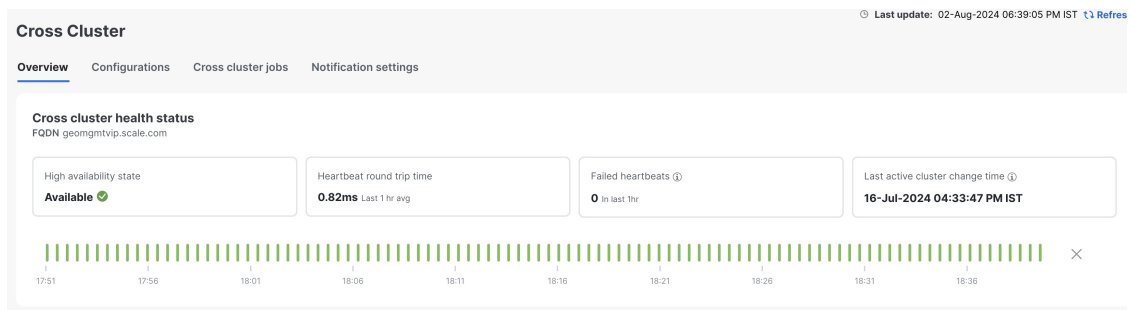


Step 2

You can perform the following operations on the **Cross Cluster** window.

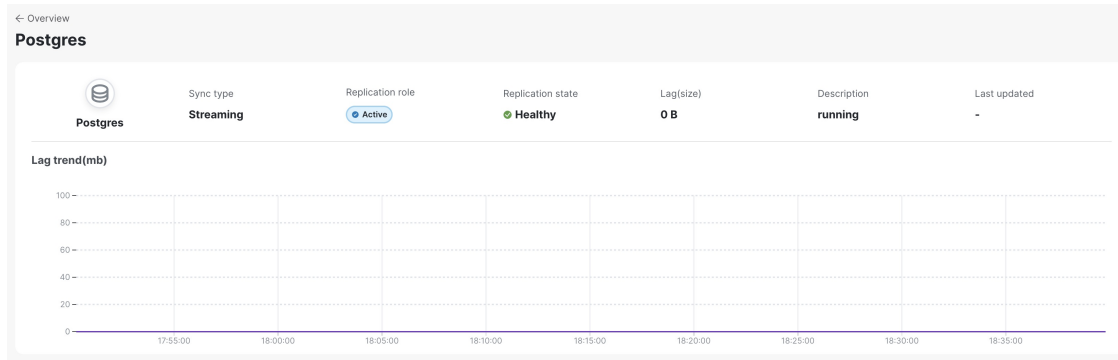
- Click next to failed heartbeats to see a visual representation of the heartbeat count.

Figure 58: Cross Cluster window - Failed Heartbeats



- Click on the name of the active and standby clusters to view the cluster details.
- Click on **Lag(size)** for a data store to view a detailed graph of the replication summary.

Figure 59: Data store Lag trend



Step 3 You can select and perform the following optional operations from the **Actions** drop-down menu.

- Click **Actions** > **Switch cluster role** to initiate the cluster switchover. For more information, see [Geo Redundancy Switchover, on page 271](#).
- Click **Actions** > **Showtech request**, and the **Showtech Request** pop-up window is displayed. Enter the relevant SCP host details and click **Export** to download the showtech logs.
- Click **Actions** > **Synchronize** to initiate an on-demand sync operation.

Important Do not perform the **Synchronize** operation before completing the other configurations (such as storage, DNS, and sync settings). Once a sync is initiated, it cannot be stopped midway.

- Click **Actions** > **Repair system** to address any sync issues that require the system to kickstart the replication or bootstrap the standby cluster from the active side. This operation will attempt to automatically repair the applications and database.

Configure Cross Cluster Settings

Configuring cross cluster settings is important to ensure secure data transfer between clusters, to facilitate reliable backups and recovery, and data compliance.

This topic explains how to configure the cross cluster settings.



Note The default values shown in the Cross Cluster Configuration UI are the recommended settings.

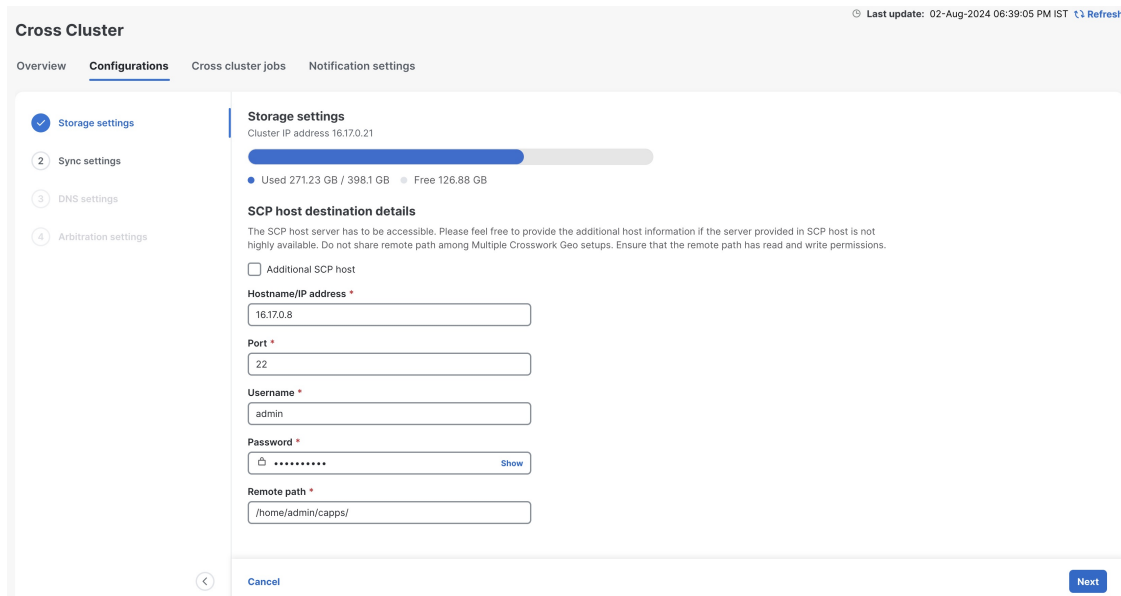
Step 1 From the main menu, choose **Administration** > **Cross Cluster**. The **Cross Cluster** window is displayed. Click on the **Configurations** tab.

Step 2 The **Configurations** window is displayed, with the first step, **1 - Storage settings**, highlighted. Fill all the fields provided for the SCP Host server.

To add additional SCP host, select the **Additional SCP host** checkbox. Additional SCP host is needed only when the current SCP host is not highly available across both AZs.

Note After a SCP host is configured, you can view the used and free space available in the server.

Figure 60: Storage settings

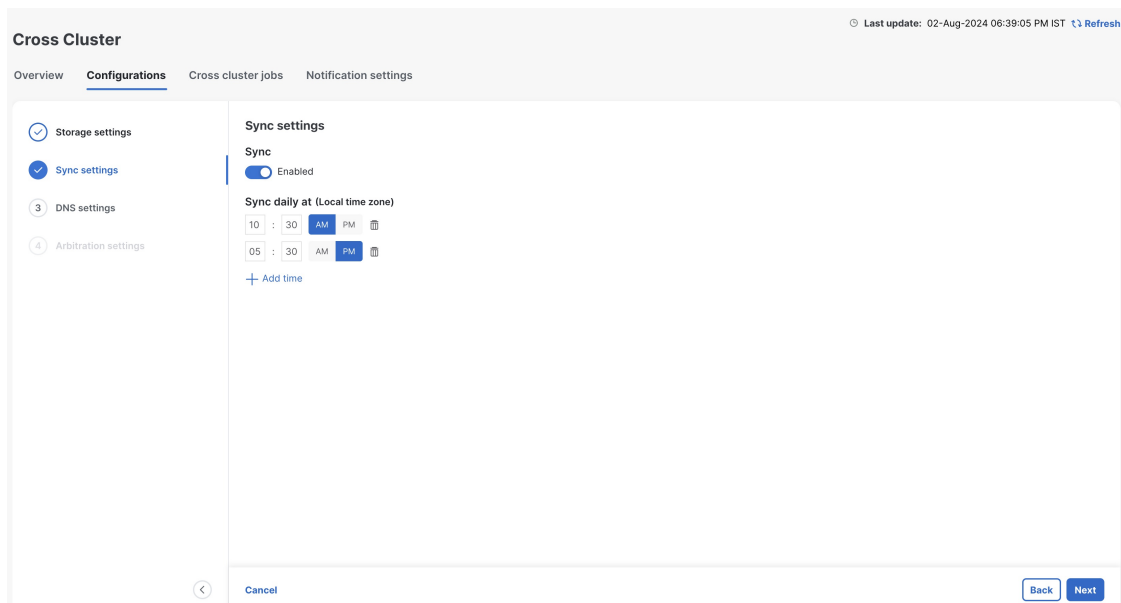


Step 3 Click **Next**. The **Configurations** window is displayed, with the next step, **2 - Sync settings**, highlighted. Data synchronization ensures high availability, consistency, load balancing, and data compliance between geo redundant clusters.

Enable the **Sync** slider button to set an auto-sync schedule, and set the sync times.

Note It is recommended to sync at least once every 8 hours.

Figure 61: Sync settings



Step 4 Click **Next**. The **Configurations** window is displayed, with the next step, **3 - DNS settings**, highlighted. Add the details for the **Authoritative DNS server** and **Port**.

- Note**
- The DNS server should be configured with the same management FQDN and data FQDN displayed on the UI.
 - The DNS record TTL for FQDN must be lesser than 60 seconds (< 60s).

Figure 62: DNS settings

Cross Cluster Last update: 02-Aug-2024 06:39:05 PM IST Refresh

Overview **Configurations** Cross cluster jobs Notification settings

Storage settings
Sync settings
DNS settings
Arbitration settings

DNS settings

Management FQDN
geomgmtvip.scale.com

Data FQDN
geodatavip.scale.com

Authoritative DNS server * Port

Cancel Back Next

Step 5 Click **Next**. The **Configurations** window is displayed, with the final step, **4 - Arbitration settings**, highlighted. Set relevant values for the **Heartbeat time interval** and **Failure detection wait period** fields.

Note

Figure 63: Arbitration settings

The screenshot shows the 'Cross Cluster' configuration interface. At the top right, it indicates 'Last update: 02-Aug-2024 06:39:05 PM IST' and a 'Refresh' button. Below this are tabs for 'Overview', 'Configurations', 'Cross cluster jobs', and 'Notification settings'. The 'Configurations' tab is active, showing a list of settings on the left: 'Storage settings', 'Sync settings', 'DNS settings', and 'Arbitration settings' (which is selected). The main area displays 'Arbitration settings' with two dropdown menus: 'Heartbeat time interval' set to '30s' and 'Failure detection wait period' set to '800s'. Below these is a 'Peer cluster settings' section with a checked checkbox labeled 'Apply the same configurations to peer cluster'. At the bottom, there are 'Cancel', 'Back', and 'Save' buttons.

Step 6 (Optional) Select the checkbox to apply the same configuration to the other cluster.

Step 7 Click **Save** to save the changes.

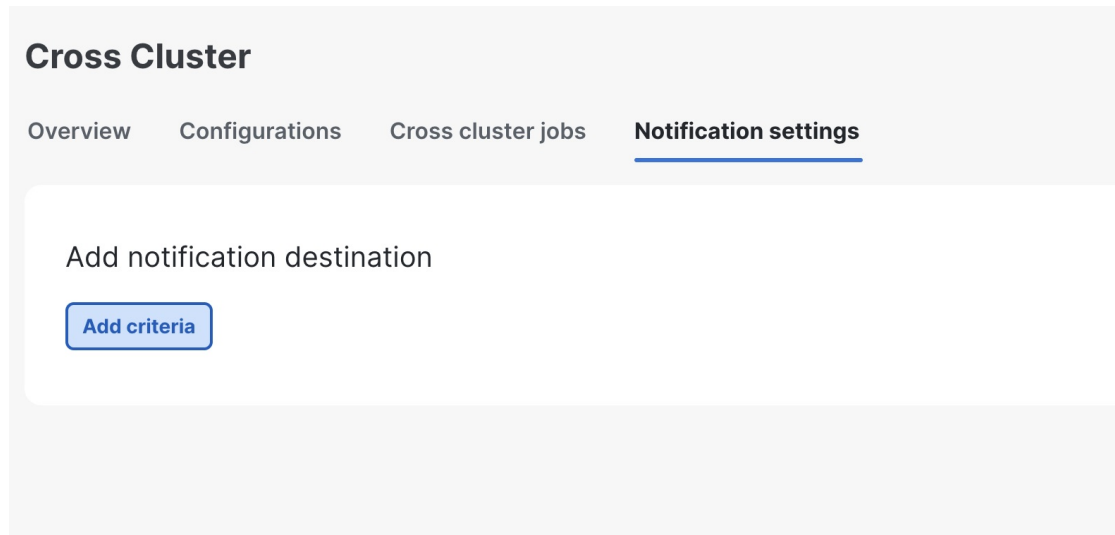
Configure Cross Cluster Notification Settings

This topic explains how to configure the cross cluster notification settings.

Step 1 From the main menu, choose **Administration > Cross Cluster**. The **Cross Cluster** window is displayed.

Step 2 Click on the **Notification settings** tab, and **Add notification destination** window is displayed.

Figure 64: Notification Settings



Step 3 Click **Add Criteria**, and you will be navigated to the **Create Notification Policies** window.

Enter relevant values for the following fields, and save the policy.

- Policy name
- Criteria
- Notification destination

For more information, see *Create Notification Policy for System Events* in the [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

Geo Redundancy Scenarios

There are many scenarios with expected system behaviors that you should be aware of when geo redundancy is enabled.

Application Installation

Table 61: Application Installation Scenarios

Scenario	Expected System Behavior
Application or version mismatch between active and standby clusters prior to enabling geo redundancy.	An equivalency check done prior to the geo redundancy enablement will identify any mismatch between the active and standby clusters (in terms of applications or versions), and prevent enablement. To proceed, please ensure that applications and versions match on both clusters.

Scenario	Expected System Behavior
Application or version mismatch between active and standby cluster after enabling geo redundancy.	Any configured sync operation will fail until the mismatch is corrected.
Installing an application or patch while a sync is in progress.	A sync operation can be configured as a periodic event or initiated on demand. While a sync operation is in progress, application installation will not be allowed.
Installing an application or patch when sync is not happening.	When sync is not happening, application installation is allowed.

Backup and Restore

Table 62: Backup and Restore Scenarios

Scenario	Expected System Behavior
Taking a backup on the active crosswork cluster.	This operation is allowed. You are recommended to take backup of the active cluster to have a point-in-time backup to roll back to in case the data sync is corrupted.
Taking a data only backup on the standby crosswork cluster.	This operation is not permitted.
Disaster recovery from a corrupted data sync between the clusters.	This operation is allowed. In case the data sync is corrupted between clusters, you can restore the data only backup made on the active cluster and allow the normal sync flow to sync the standby cluster.
Disaster recovery where both clusters need to be recovered	In the rare case that the active and standby clusters are unrecoverable or unusable, please redeploy the active and standby clusters and apply the data only backup on the active cluster. The standby will sync in the normal sync flow.
Perform restore operation on the standby cluster.	This operation is not permitted.
Perform restore operation on the active cluster.	This operation is allowed. If you want to restore a previous backup, perform the restore on the active cluster. The standby cluster will sync on the next sync cadence.

Password Update

Follow the below sequence while updating password on a geo redundant cluster:

1. Update the password on the active cluster.
2. Wait for the sync operation to complete, and the password update is pushed to the standby cluster.
3. Update the inventory file on the active cluster.

Install Geo High Availability Crosswork Data Gateway

Crosswork Data Gateway is installed as a base VM that contains only enough software to register itself with Crosswork Network Controller.



Note If you are redeploying the same data gateway with Crosswork Network Controller, delete the previous data gateway entry from the Virtual Machine table under Data Gateway Management. For information on how to delete a data gateway VM, see [Delete Crosswork Data Gateway from the Crosswork Cluster, on page 241](#).

To install a data gateway VM for use with Crosswork Network Controller, follow these steps:

1. Choose the deployment profile for the data gateway VM.
For the VM requirements, see [Crosswork Cluster VM Requirements, on page 25](#).
2. Review the installation parameters and make sure that you have all the required information to install the data gateway using the preferred deployment scenario. For the parameter information, see [Crosswork Data Gateway Parameters and Deployment Scenarios, on page 92](#).
3. Install the data gateway using your preferred method:

Table 63: Data gateway installation options

VMware	Install Crosswork Data Gateway using vCenter vSphere Client, on page 105
	Install Crosswork Data Gateway via OVF Tool, on page 116

4. Complete the postinstallation tasks mentioned in the section [Crosswork Data Gateway Post-installation Tasks, on page 127](#).
5. Verify that the data gateway VM has enrolled successfully with Crosswork Network Controller. For information on how to verify the enrollment process, see [Crosswork Data Gateway Authentication and Enrollment, on page 126](#).

After verifying that the data gateway VM has enrolled successfully with Crosswork Network Controller, set up the data gateway for collection by creating a data gateway pool. For more information, see the *Create a Crosswork Data Gateway Pool* section in [Cisco Crosswork Network Controller 7.0 Administration Guide](#).

Geo Redundancy Workflow (Day N)

This topic outlines the high-level workflow for the tasks required to enable geo redundancy on day N when Crosswork Network Controller (version 7.0) is operating in a standalone cluster.

A Crosswork cluster is considered as a "day N" scenario if it has configured the below options:

- Application are installed.
- Devices are configured.

- Crosswork Data Gateway is enrolled.
- Providers are added.
- Collection jobs are running.

A backend check is conducted to verify the cluster's eligibility for enabling geo redundancy. If any checks fail, geo redundancy cannot be enabled, and alarms will be generated to notify you.



Note Once geo redundancy is enabled on day N, please perform a sync from the Active to the Standby cluster before installing any applications.

Table 64: Geo-Redundancy Workflow (Day N) for Standalone Crosswork Cluster

Step	Action
1. Convert single instance NSO to NSO HA	Follow the instructions in Convert Single Instance NSO to NSO HA, on page 279 topic. Note Crosswork Network Controller 7.0 supports NSO version 6.1.11.2. The process to upgrade NSO is not covered in this document. For more information, see the relevant Cisco NSO documentation .
2. Deploy SR-PCE	Deploy SR-PCE in a Point of Presence (PoP) site closer to the Crosswork's Availability Zone. For more information, refer to the relevant install instructions in the Cisco IOS XRv 9000 Router Installation Guide . Note Crosswork Network Controller 7.0 supports IOS XR 24.2.1.
3. Install the standby cluster and enable geo redundancy solution.	Follow the instructions in Install the Standby Cluster and Enable Geo Redundancy, on page 283 topic.
4. Configure the Controller IP for Crosswork Data Gateway	Follow the instructions in Configure Controller IP for Crosswork Data Gateway, on page 285 topic.
5. Update the providers.	Follow the instructions in Update Providers, on page 286 topic.
6. Complete the geo redundancy enablement operation.	Follow the instructions in Complete Geo Redundancy Enablement, on page 286 topic.
7. Perform Sync	After geo redundancy is enabled on both the active and standby clusters, update the sync settings and perform the first sync either manually or allow it to occur at the scheduled time. Any further application files should be installed only after the first sync is completed.



CHAPTER 17

Geo Redundancy Switchover

This chapter contains the following topics:

- [Perform Switchover, on page 271](#)
- [Crosswork Optimization Engine License Count After a Switchover, on page 275](#)
- [Geo Redundant Cluster Disaster Recovery, on page 275](#)

Perform Switchover

Switchover is the process of interchanging the roles of the active cluster and standby cluster in the event of a failure.

In case of a failure, the system performs many preliminary checks (heartbeat count, connectivity checks, HTTP and SSH login checks, etc.) and raises alarms if they fail. If you notice an alarm, you are expected to check both clusters to verify the authenticity of the alarms before you initiate the switchover.



Note

- If a switchover operation is completed on a standby VM (before the sync operation), there are no rows or entries displayed on the **Publish Details** for tech-support jobs. This happens because the tech-support history is written to ETCD which is not synced across geo redundancy setups. This is an expected system behavior.
 - All services provisioned on AZ1 are continuously synced to AZ2 through live asynchronous replication.
 - If you use the Service Health application, you must trigger an additional periodic or on-demand sync after a switchover to reconcile the replication data in the Neo4j data stores between the clusters.
 - After a switchover, the topology is discovered more quickly on AZ2 because it is built via resync rather than from scratch.
-

Before you begin

Before the switchover, it is important that both clusters have the same application versions and resource footprints used.

Step 1 Log in to the standby cluster.

Step 2 From the main menu, choose **Administration > Cross Cluster**. The **Cross Cluster** window is displayed.

Step 3 Click **Actions > Switch cluster role**

The **Switch Cluster Role** dialog box is displayed with the initial state of the clusters. For the purpose of this topic, SJC cluster (cluster-sjc) is in *Active* state and NYC cluster (cluster-nyc) is in *Standby* state.

Figure 65: Switch Cluster Role

Switch Cluster Role

Please set the role of current cluster to ACTIVE/STANDBY.

To ensure you don't lose any data, it's important to sync between clusters if there have been any configuration changes since the last time you synced.

To switch over, follow these three steps:

1. Switch the role of the current ACTIVE to STANDBY cluster.
2. Make sure that the DNS Resource records are manually updated to point to the new active cluster endpoint (virtual IP) within 5 minutes after switching.
3. In peer cluster, switch the role from STANDBY to ACTIVE.

The screenshot shows a dialog box with two cluster cards. The left card is for 'cluster-nyc' (New York) and has a 'Standby' button with a minus sign. The right card is for 'cluster-sjc' (San Jose) and has an 'Active' button with a checkmark. At the bottom right of the dialog are 'Cancel' and 'Save' buttons.

Step 4 Click on the NYC cluster to change it to *Active* state. Click **Save** to confirm change.

Figure 66: Switch standby cluster to active

Switch Cluster Role

Please set the role of current cluster to ACTIVE/STANDBY.

To ensure you don't lose any data, it's important to sync between clusters if there have been any configuration changes since the last time you synced.

To switch over, follow these three steps:

1. Switch the role of the current ACTIVE to STANDBY cluster.
2. Make sure that the DNS Resource records are manually updated to point to the new active cluster endpoint (virtual IP) within 5 minutes after switching.
3. In peer cluster, switch the role from STANDBY to ACTIVE.

The screenshot shows a dialog box titled "Switch Cluster Role". It contains two cluster cards. The first card, "cluster-nyc", is highlighted with a blue border and shows "New York" and a blue "Active" button with a checkmark. The second card, "cluster-sjc", shows "San Jose" and a blue "Active" button with a checkmark. At the bottom right of the dialog, there are "Cancel" and "Save" buttons.

Step 5 Update the DNS server records of Management FQDN and Data FQDN to point to the new active cluster.

Step 6 Now log in to the SJC cluster (already active). In the **Cross Cluster** window, click **Actions** > **Switch cluster role**.

Note At this point, till the time you change the cluster state, both clusters will be in *Active* state.

Step 7 In the **Switch Cluster Role** dialog box, click on the cluster to change it to *Standby* state.

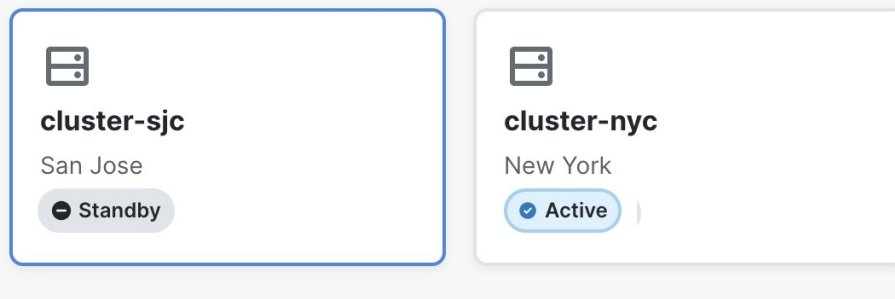
Figure 67: Switch active cluster to standby

Switch Cluster Role

Please set the role of current cluster to ACTIVE/STANDBY.
To ensure you don't lose any data, it's important to sync between clusters if there have been any configuration changes since the last time you synced.

To switch over, follow these three steps:

1. Switch the role of the current ACTIVE to STANDBY cluster.
2. Make sure that the DNS Resource records are manually updated to point to the new active cluster endpoint (virtual IP) within 5 minutes after switching.
3. In peer cluster, switch the role from STANDBY to ACTIVE.



Click **Save** to confirm the change.

Note Wait for the device reachability to converge before moving to resume operations on the standby cluster.

Step 8 After few minutes, log in to the first cluster. The switchover will be completed.

Step 9 Post-switchover, verify the following:

- a) Verify the cluster health and device status to ensure the system is functioning properly.
- b) Check the health status of the Crosswork Data Gateway to ensure it is functioning properly.
- c) Check the status of the HA pool.
- d) Check the Collection status and confirm that traffic is flowing smoothly to the newly active cluster.

Crosswork Optimization Engine License Count After a Switchover

For Crosswork Optimization Engine, the Smart Licenses page reflects the correct license count only after 24 hours or by 1:00 am after a switchover.

If you cannot wait 24 hours or until 1:00 am, there are two methods to force a license update:

- You can disable or enable feature packs (Bandwidth on Demand, Circuit Style Manager, or Local Congestion Manager).
- You can detach and add devices back again.

Geo Redundant Cluster Disaster Recovery

At some time during normal operations of your Cisco Crosswork cluster, you may find that you need to recover the entire system. This can be the result of one or more malfunctioning nodes, one or more malfunctioning services or applications, or a disaster that destroys the hosts for the entire cluster.

This section explains the steps needed to perform to recover your geo redundant clusters.

Destruction of Standby Cluster

This topic explains the recovery steps that must be executed when the standby cluster is destroyed.

-
- Step 1** Deploy the new standby cluster with the same IP and Virtual IP (VIP) addresses.
 - Step 2** Install the same version of applications as the active cluster.
 - Step 3** Enable pairing mode in the active cluster. For more information, see [Enable Geo Redundancy, on page 256](#)
 - Step 4** Enable geo redundancy on the standby cluster. For more information, see [Enable Geo Redundancy, on page 256](#)
 - Step 5** Enter the Cross Cluster settings on the new standby cluster as per the settings on the active cluster. Alternatively, you can enable the **Apply the same configuration to peer cluster** checkbox for the Cross Cluster settings on the active cluster, and save the settings.
 - Step 6** On the Cross Cluster window, use the **Initiate Sync** option to ensure the standby cluster pulls data from the active cluster.
-

Destruction of Active Cluster

This topic explains the recovery steps that must be executed when the active cluster is destroyed.

-
- Step 1** Switch the standby cluster to become the new active cluster. For more information, see [Geo Redundancy Switchover, on page 271](#).
 - Step 2** Re-deploy the destroyed cluster (currently, the standby cluster) with the same IP and Virtual IP (VIP) addresses.
 - Step 3** Install the same version of applications as the active cluster.

- Step 4** Enable pairing mode in the active cluster. For more information, see [Enable Geo Redundancy, on page 256](#)
- Step 5** Edit the Cross Cluster inventory file (.yaml) to reflect the current state of the Cross Cluster after the switchover in step 1.
- Step 6** On the Geo Redundancy window of the active cluster, click **Browse** and upload the edited inventory file (.yaml file).
- Step 7** Enable geo redundancy on the standby cluster. For more information, see [Enable Geo Redundancy, on page 256](#)
- Step 8** Enter the Cross Cluster settings on the new standby cluster as per the settings on the active cluster. Alternatively, you can enable the **Apply the same configuration to peer cluster** checkbox for the Cross Cluster settings on the active cluster, and save the settings.
- Step 9** On the Cross Cluster window, synchronize data to ensure the standby cluster pulls data from the active cluster.
- Step 10** (Optional) Switch the standby cluster to become the new active cluster.
-



CHAPTER 18

Upgrade to Geo Redundancy Solution

This chapter contains the following topics:

- [Upgrade from Crosswork Network Controller 6.0 to 7.0 \(Geo Redundant\), on page 277](#)

Upgrade from Crosswork Network Controller 6.0 to 7.0 (Geo Redundant)

This topic provides a high-level description of the tasks required to upgrade from Crosswork Network Controller version 6.0 to version 7.0 (geo redundant).

Supported migration scenarios:

- Crosswork 6.0 (non-Geo, IPv4 stack) to Crosswork 7.0 (Geo, IPv4 stack)
- Crosswork 6.0 (non-Geo, IPv4 stack) to Crosswork 7.0 (Geo, dual stack)



Note Any day N activity will yield the system ineligible to migrate to a geo redundant solution. You will need to re-install the Crosswork cluster to enable geo redundancy.

Table 65: Upgrade from Crosswork 6.0 to 7.0 Geo Redundancy (Day 0)

Step	Action
1. Convert single instance NSO to NSO HA	Follow the instructions in Convert Single Instance NSO to NSO HA, on page 279 topic. Note Crosswork Network Controller 7.0 supports NSO version 6.1.11.2. The process to upgrade NSO is not covered in this document. For more information, see the relevant Cisco NSO documentation .

Step	Action
2. Deploy SR-PCE	<p>Deploy SR-PCE in a Point of Presence (PoP) site closer to the Crosswork's Availability Zone. For more information, refer to the relevant install instructions in the Cisco IOS XRv 9000 Router Installation Guide.</p> <p>Note Crosswork Network Controller 7.0 supports IOS XR 24.2.1.</p>
3. Create backup of the Crosswork 6.0 cluster.	Follow the instructions in Create Backup of the Cisco Crosswork Cluster, on page 279 topic.
4. Shut down the Crosswork 6.0 cluster	<p>Shut down the Crosswork Network Controller 6.0 cluster by powering down the VMs hosting each node (start with the Hybrid VMs).</p> <ol style="list-style-type: none"> Gather following information before shutting down the cluster. <ul style="list-style-type: none"> All IP addresses of the cluster. All IP addresses of the Crosswork Data Gateways Shut down the VMs of the Crosswork cluster. For vcenter shutdown all the VMs using vcenter UI 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 the steps for each of the remaining VMs. (Optional) Put NSO in read-only mode using <code>ncs_cmd -c maapi_read_only</code> command.
4. Install the Crosswork Network Controller 7.0 cluster and applications.	Follow the instructions in Install the Crosswork Network Controller Cluster and Applications, on page 281 topic.
5. Perform the migration.	Follow the instructions in Run Migration, on page 282 topic.
6. Install the standby cluster and enable geo redundancy solution.	Follow the instructions in Install the Standby Cluster and Enable Geo Redundancy, on page 283 topic.
7. Upgrade Crosswork Data Gateway 6.0 to 7.0 with Geo Redundancy	Follow the instructions in Upgrade Crosswork Data Gateway 6.0 to 7.0 Geo Redundancy, on page 284 topic.
8. Configure the Controller IP for Crosswork Data Gateway	Follow the instructions in Configure Controller IP for Crosswork Data Gateway, on page 285 topic.
9. Update the providers.	Follow the instructions in Update Providers, on page 286 topic.

Step	Action
10. Complete the geo enablement operation.	Follow the instructions in Complete Geo Redundancy Enablement, on page 286 topic.

Convert Single Instance NSO to NSO HA

This topic explains the procedure to convert a single instance NSO to NSO HA (High Availability). For detailed instructions, please refer to the [NSO Administration Guide on HA](#).



Attention Make a backup and upgrade your NSO setup to the compatible version before executing the below steps.

Follow the below guidelines to create a HA setup from a standalone NSO.

-
- Step 1** Determine the High Availability topology to follow: L2 or L3
 - Step 2** Make a backup of the original NSO system.
 - Step 3** Clone the original NSO to a new instance.
 - Step 4** Install the hcc package on both nodes.
 - Step 5** Configure the high availability and hcc as per the selected network topology.
 - Step 6** Request to enable high availability on both nodes.
 - Step 7** Verify the changes made.
-

Create Backup of the Cisco Crosswork Cluster

Creating a backup is a prerequisite when upgrading your current version of Crosswork Network Controller to a new version.



Note We recommend that you create a backup only during a scheduled upgrade window. Users should not attempt to access Crosswork Network Controller 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 Crosswork Network Controller cluster and the SCP server must be in the same IP environment. For example: If Crosswork Network Controller 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 new version of Cisco Crosswork.
- 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 the new version of Cisco Crosswork. 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).

Step 1 Login to the Crosswork UI by navigating to `https://<VIP>:30603`.

The VIP refers to the Management Virtual IP of the cluster.

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 Crosswork Network Controller 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 Crosswork Network Controller 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.

Note To use the **Backup NSO** option during backup, you must configure the SSH connectivity protocol in the NSO provider; otherwise, the backup will fail. Follow the instructions given in *Backup Cisco Crosswork with Cisco NSO* section in the *Cisco Crosswork Network Controller 7.0 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 prefilled **Host Name**, **Port**, **Username**, **Password** and **Remote Path** fields to specify a different destination.

- g) (Optional) Click **Verify Backup Readiness** to verify that Crosswork Network Controller has enough free resources to complete the backup. If the verifications are successful, Crosswork Network Controller 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. Crosswork Network Controller 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.

Note You can also perform a data backup (backup using rest-api). The data backup is faster as it does not include application binaries. To perform, do the following:

- Get JWT (using sso apis)
- API to take the data backup (<https://<VIP>:30603/crosswork/platform/v1/platform/backup/dataonly>)
- Payload for the api {"jobName": "jobname", "force": false}

- 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**.

Install the Crosswork Network Controller Cluster and Applications

This install the latest version of the Crosswork Network Controller cluster and applications.



Important While the cluster installation is in progress, you must upgrade your NSO setup to the compatible version. Please monitor actively to ensure that the NSO leader is in the same site as Crosswork.

Before you begin

- Make sure that your environment meets all the installation prerequisites (see [Installation Prerequisites for VMware vCenter, on page 19](#)).

Step 1 Install the new version of the Crosswork Network Controller cluster (see [Install Crosswork Cluster on VMware vCenter, on page 37](#)) using the same IP addresses and same number of nodes as in old cluster.

Step 2 After the installation is completed, log into the Crosswork Network Controller UI (using `https://<VIP>:30603`) and check if all the nodes are up and running in the cluster.

Step 3 Install the Crosswork Network Controller applications which were installed in the old cluster. Ensure that you install the latest versions that are compatible with the new version of the cluster. For installation instructions, please refer to the [Install Crosswork Applications, on page 183](#) chapter.

Note The applications binaries and versions are not updated in the migration job.

Step 4 After the applications are successfully installed, check the health of the new Crosswork Network Controller cluster.

- a) From the Crosswork Network Controller main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
 - b) Click **Crosswork Cluster** tile to view the health details of the cluster.
-

Run Migration

After successfully installing the new versions of the Crosswork Network Controller applications, proceed to migrate the Crosswork Network Controller backup taken earlier to the new Crosswork Network Controller 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 of the Cisco Crosswork Cluster, on page 279](#).
 - The name and path of the backup file created in [Create Backup of the Cisco Crosswork Cluster, on page 279](#).
 - 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 of the Cisco Crosswork Cluster, on page 279](#).

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

Step 3 Migrate the previous Crosswork Network Controller backup on the new Crosswork Network Controller cluster:

- a) From the Crosswork Network Controller 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 of the Cisco Crosswork Cluster, on page 279](#)) in the **Backup File Name** field.
- d) If you want to perform the data migration backup despite any Crosswork Network Controller application or microservice issues, check the **Force** check box.
- e) Click **Start Migration** to start the data migration operation. Crosswork Network Controller 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 new Crosswork Network Controller cluster.

- a) From the Crosswork Network Controller main menu, choose **Administration > Crosswork Manager > Crosswork Summary**.
- b) Click **Crosswork Cluster** tile to view the health details of the cluster.

Install the Standby Cluster and Enable Geo Redundancy

After completing the migration on the active cluster, install the standby cluster and enable geo redundancy.



Note When you are enabling geo redundancy after the 5.0 to 6.0 migration, you must set the following flag in the inventory file:

```
## install
is_post_migration_activation: true
```

-
- Step 1** In the second site, install the standby cluster. For more information, refer to the installation instructions in [Install Cisco Crosswork on VMware vCenter using the Cluster Installer Tool, on page 47](#) or [Manual Installation of Cisco Crosswork using vCenter vSphere UI, on page 60](#).
- Step 2** Install the applications (that were installed on the active cluster) on the standby cluster.
- Note** Migration is not required in the standby cluster, as the changes would be taken from the active cluster during the periodic sync operation.
- Step 3** Ensure DNS connectivity on both sites. Perform DNS server update on both sites if needed to ensure that Crosswork cluster is using the right DNS server.
- Step 4** Ensure unified cross cluster endpoint is resolved on *site 1* (active site).
- Step 5** Create and upload the inventory file on *site 1* to create the active cluster, and verify the operation. For more information, refer to the instructions in [Enable Geo Redundancy, on page 256](#).
-

Upgrade Crosswork Data Gateway 6.0 to 7.0 Geo Redundancy

This topic explains the procedure to upgrade from Crosswork Data Gateway version 6.0 to version 7.0 (geo redundancy-enabled).

For the 76.0 Crosswork Network Controller release, it is mandatory to deploy data gateway using the FQDN. When Crosswork undergoes an upgrade, the existing data gateways transition to the ERROR state because of their enrollment using the VIP address, resulting in a discrepancy in the enrollment information.

To install data gateway after an upgrade:

Before you begin

Ensure that you are aware of the following:

- After Crosswork is upgraded, the data gateways, virtual data gateways, HA pool, and device-mapping configuration are restored.
- The Data Gateway Manager automatically assigns the active Crosswork site as the default site for all existing data gateways.

-
- Step 1** Redeploy the data gateway instance by removing the old instance and replacing it with a new installation. During the redeployment, use the unified management FQDN for ControllerIP in the OVF deployment script.
- For information on removing a data gateway instance, see [Delete Crosswork Data Gateway from the Crosswork Cluster, on page 241](#) and installing a new instance, see [Install Geo High Availability Crosswork Data Gateway, on page 268](#).
- If the data gateways are redeployed using the same name and hostname attribute provided in the OVF script, the Data Gateway Manager considers them as existing gateways and automatically enrolls them with the upgraded Crosswork during the migration process.
- Important** We recommend that you initiate a sync operation to enhance the accuracy of the data after the addition of a new device or the deployment of a new gateway. See [View Cross Cluster Status, on page 260](#) for information on how to perform a sync operation.

- Step 2** Modify the high availability data gateway pools:
- If a new data gateway instance is added to a high availability pool from the Standby site, which is currently the Active site, and a switchover occurs. The data gateway's role changed from Spare to Assigned.
 - By default, the existing pools will be tagged as imbalanced, as there are no data gateways connected to the standby site. For preserving the data gateway balance, deploy new data gateways on the standby site.
 - The SBConfig is configured to the Shared option. You must configure it to be Site-specific.
 - Configure the VIP or FQDNs for the standby site.
- Step 3** Migrate data gateway from a single stack that is IPv4 or IPv6 to a dual stack:
- Update the pool information by including the dual stack configuration's VIP IPs and gateway details. For instance, if you have configured IPv4 address when creating a pool, you must add the IPv6 information.
- Step 4** Accept an upgrade acknowledgment message that appears on the Crosswork UI when all the data gateways with the Assigned role are in the UP state and the Spare gateways in the NOT_READY state.

Data gateways with the Assigned role start the data collection.

What to do next

If the data gateways cannot connect with the Active cluster, reenroll the gateway from the interactive menu. See the *Reenroll Crosswork Data Gateway* section in the [Cisco Crosswork Network Controller 7.0 Administration Guide](#) for more information.

Configure Controller IP for Crosswork Data Gateway

This topic explains the procedure for configuring the controller IP or FQDN for the data gateway after enabling the geo redundancy feature.

When a data gateway is deployed with an invalid controller IP, it may get stuck in the enrollment process. To address this, reconfigure the controller IP. Also, if a data gateway is enrolled to a Crosswork and there is a change in controller virtual IP or the IP is changed to FQDN due to the enabled geo redundancy feature, it must be reconfigured.

To configure the controller IP for a new enrollment or change the controller IP of an existing Crosswork that the data gateway is enrolled with:

Navigate to the data gateway on the active cluster before the geo redundancy feature is enabled.

-
- Step 1** Log in to the data gateway VM on the active cluster before the geo redundancy feature is enabled.
- Step 2** In the data gateway VM interactive menu, select **3 Change Current System Settings**.
- Step 3** Select **Configure Controller IP/FQDN**.
- Step 4** Enter the SCP URI for the controller signing certificate file.
- Step 5** Enter the SCP passphrase or the SCP user password for the controller signing certificate file.
- Step 6** Enter the controller IP.

A message appears to confirm that Crosswork has updated the controller's IP or FQDN, and the VM is rebooted.

The data gateway connects to Crosswork and progresses to the UP state. If the data gateways are in the Assigned state with devices attached, they resume data collection.

Update Providers

After enabling geo redundancy on the active cluster, update the providers.



Note Skip this step if you are not planning to enable geo redundancy.

- Step 1** Add the RBAC JWT token on the Cisco NSO VMs.
 - Step 2** Upload and update the JWT package on the Cisco NSO High Availability VMs.
 - Step 3** Reload the NCS packages on both VMs.
 - Step 4** Update the **JWT auth file** with *geo-CW FQDN cnc-host* value on both VMs.
 - Step 5** Update the *cert.pem* on both VMs.
 - Step 6** Update NSO with unified cluster endpoint in the **Manage Providers** window.
 - Step 7** (Optional) Update SR-PCE IP address in the **Manage Providers** window.
 - Step 8** (Optional) While upgrading from a non-HA setup to geo redundant mode, Crosswork Data Gateway will end with multiple VIPs for southbound devices. These devices need to be set up for syslogs, traps and MDT. In case of MDT, you can use admin DOWN/UP to push the configuration changes to the devices.
- Note** Any other external destination needs to be in HA mode with its own unified endpoint in the form of VIP or FQDN.
-

Complete Geo Redundancy Enablement

After updating the providers, activate geo redundancy on the standby cluster.



Note Skip this step if you are not planning to enable geo redundancy.

- Step 1** Create and upload the cluster inventory file on site 2, to create the standby cluster. Verify the operation. For more information, refer to the instructions in [Enable Geo Redundancy, on page 256](#).
- Step 2** Configure the cross cluster settings. For more information, see step 7 in the [Geo Redundancy Workflow \(Day 0\), on page 253](#) topic.
- Step 3** Perform a on-demand sync to sync the data from active to standby cluster.

Once geo redundancy is enabled, a **Geo Redundancy** tile is added to the **Application management** window. This tile is built-in and cannot be upgraded, uninstalled, or deactivated.



PART **IX**

Install Cisco Crosswork Network Controller on a Single VM

- [Install Cisco Crosswork Network Controller on a Single VM, on page 291](#)



CHAPTER 19

Install Cisco Crosswork Network Controller on a Single VM

This chapter contains the following topics:

- [Introduction, on page 291](#)
- [Installation Parameters, on page 291](#)
- [Installation Requirements, on page 295](#)
- [Install Crosswork Network Controller using the vCenter vSphere UI, on page 300](#)
- [Install Cisco Crosswork via the OVF Tool, on page 306](#)
- [Install Crosswork Network Controller using the Docker Installer Tool, on page 309](#)

Introduction

This chapter explains the requirements and processes to install Crosswork Network Controller on a single VM or node. Cisco Crosswork Network Controller enables you to proactively manage your end-to-end networks, by providing automation solutions to ensure faster innovation, optimal user experience, and operational excellence.

For the single VM deployment, Crosswork Network Controller consists of the Cisco Crosswork Infrastructure, Embedded Collectors, and the Element Management Functions application bundled together in a package. Here is a brief overview of each component:

- The Cisco Crosswork Infrastructure is a microservices-based platform and is the foundation required for running Crosswork applications.
- On the single VM installation, as opposed to the cluster based installation, the Embedded Collector that gathers information from managed devices runs on the same VM as a Crosswork application.
- Element Management Functions is a library of functions that provides deep inventory collection, zero touch provisioning, performance management, alarm management and image management on the managed devices.

Installation Parameters

This section explains the important parameters that must be specified while installing the Crosswork VM. Kindly ensure that you have relevant information to provide for each of the parameters mentioned in the table.



Attention Please use the latest template file that comes with the Crosswork build file.

Table 66: General parameters

Parameter Name	Description
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.
ManagementVIP	The Management Virtual IP for the Crosswork VM.
ManagementVIPName	Name of the Management Virtual IP for the Crosswork VM. This is an optional parameter used to reach Crosswork Management VIP via DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server.
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 Crosswork VM.
DataVIPName	Name of the Data Virtual IP for the Crosswork VM. This is an optional parameter used to reach Crosswork Data VIP via DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server.
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 VM.
CWusername	Username to log into Cisco Crosswork.
CWPassword	<p>Password to log into Cisco Crosswork.</p> <p>Use a strong VM Password (8 characters long, including upper & lower case letters, numbers, and at least one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words. While they satisfy the criteria, such passwords are weak and will be rejected resulting in failure to setup the VM.</p>

Parameter Name	Description
VMSize	VM size. Value is <code>xLarge</code> . This parameter is required only for deploying via the docker installer tool.
VMName	Name of the VM.
NodeType	Indicates the type of VM. Choose "Hybrid".
IsSeed	Set to "True".
InitNodeCount	Set value to 1.
InitLeaderCount	Set value to 1.
BackupMinPercent	<p>Minimum percentage of the data disk space to be used for the size of the backup partition. The default value is 35 (valid range is from 1 to 80).</p> <p>Please use the default value unless recommended otherwise.</p> <p>Note The final backup partition size will be calculated dynamically. This parameter defines the minimum.</p>
ManagerDataFsSize	<p>Refers to the data disk size for the Crosswork node (in Giga Bytes). This is an optional parameter and the default value is 485 (valid range is from 485 to 8000), if not explicitly specified.</p> <p>Please use the default value unless recommended otherwise.</p>
ThinProvisioned	Set to "false" for production deployments.
EnableHardReservations	<p>Determines the enforcement of VM CPU and Memory profile reservations. This is an optional parameter and the default value is <code>true</code>, if not explicitly specified.</p> <p>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.</p> <p>If set as <code>false</code> (only set for lab installations), the VM's resources are provided on best efforts. In this state, insufficient CPU cores can impact performance or cause installation failure.</p>
RamDiskSize	<p>Size of the Ram disk.</p> <p>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>HSDatstore</code> value is not used.</p>
SchemaVersion	<p>The configuration Manifest schema version. This indicates the version of the installer to use with this template.</p> <p>Schema version should map to the version packaged with the sample template in the installer tool on cisco.com. You should always build a new template from the default template provided with the release you are deploying, as template requirements may change from one release to the next.</p>

Parameter Name	Description
LogFsSize	Log partition size (in Giga Bytes). Minimum value is 20 GB and Maximum value is 1000 GB. If left blank, the default value (20 GB) is selected.
Timezone	Enter the timezone. Input is a standard IANA time zone (for example, "America/Chicago"). If left blank, the default value (UTC) is selected. This is an optional parameter.
EnableSkipAutoInstallFeature	Any pods marked as skip auto install will not be brought up until a dependent application/pod explicitly asks for it. Set to "True".
EnforcePodReservations	Enforces minimum resource reservations for the pod. If left blank, the default value ("True") is selected.
K8sServiceNetwork	The network address for the kubernetes service network. By default, the CIDR range is fixed to '/16'.
K8sPodNetwork	The network address for the kubernetes pod network. By default, the CIDR range is fixed to '/16'.
DefaultApplicationResourceProfile	Resource profile for application pods. If left blank, resource profile defaults to the deployment's VM profile (recommended option).
DefaultInfraResourceProfile	Resource profile for infra pods. If left blank, resource profile defaults to the deployment's VM profile (recommended option).
IsRunDiagnosticsScriptForCheck	Used to enable/disable execution of the diagnostic script. The values are "true" (default value) and "false". You are recommended to select the default value.
IgnoreDiagnosticsCheckFailure	Used to set the system response in case of a diagnostic check failure. If set to "true" (default value), the diagnostic check is ignored and installation will continue. If set to "false", the installation is terminated. You are recommended to select the default value.

Table 67: 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.

Parameter Name	Description
DCname	The name of the Data Center resource to use. Example: DCname = "WW-DCN-Solutions"
MgmtNetworkName	The name of the vCenter network to attach to the VM's Management interface. This network must already exist in VMware or the installation will fail.
DataNetworkName	The name of the vCenter network to attach to the VM's Data interface. This network must already exist in VMware or the installation will fail.
Host	The ESXi host, or ONLY the vcenter VM/resource group name where the VM is to be deployed. The primary option is to use the host IP or name (all the hosts should be under the data center). If the hosts are under a VM in the data center, only provide the VM name (all hosts within the VM will be picked up). The subsequent option is to use a resource group. In this case, a full path should be provided. Example: Host = "Main infrastructure/Resources/00_trial"
Datastore	The datastore name available to be used by this host or resource group. The primary option is to use host IP or name. The subsequent option is to use a resource group. Example: Datastore = "SDRS-DCNSOL-prodexsi/bru-netapp-01_FC_Prodesx_ds_15"
HSDatastore	The high speed datastore available for this host or resource group. When not using a highspeed data store, set to same value as Datastore.
Cw_VM_Image	The name of Crosswork VM image in vCenter. This value is set as an option when running the installer tool and does not need to be set in the template file.
HostedCwVMs	The ID of the VM to be hosted by the ESXi host or resource.

Installation Requirements

Resource Requirements

The following table lists the recommended resources for the Crosswork VM:

Table 68: Recommended Resources for Crosswork VM

vCPU	Memory (RAM)	Storage	Latency
24	128 GB	2 TB	< 10 ms

VMware Requirements

- Hypervisor and vCenter supported:
 - VMware vCenter Server 8.0 (U2c or later) and ESXi 8.0 (U2b or later)
 - VMware vCenter Server 7.0 (U3p or later) and ESXi 7.0 (U3p or later)
- Cisco Crosswork VM (Hybrid node) must be hosted on hardware with Hyper Threading disabled.
- Ensure that profile-driven storage is enabled by the vCenter admin user. Query permissions for the vCenter user at the root level (for all resources) of the vCenter.
- We also recommend you to enable vCenter storage control.
- 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 (latency with RTT \leq 10 ms).
- 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 a new disk on the data center or VM folder.
 - Resource: Assign a VM to a resource pool on the destination host or resource pool.
 - Datastore: Allocate space on the destination datastore or datastore folder.
 - Network: Assign the 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.

Crosswork VM Requirements

Table 69: Network Requirements

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 with a latency of less than 10 milliseconds.</p>

Requirement	Description
IP Addresses	<p>4 IPv4 or IPv6 addresses: A management and data IP address for the Hybrid node being deployed, and two additional IP addresses to be used as the Virtual IP (VIP) address (one for the Management network and one for the Device network).</p> <p>Note</p> <ul style="list-style-type: none"> • Crosswork does not support dual-stack configurations for single VM deployment. Therefore, all addresses for the environment must be either IPv4 or IPv6. • The IP addresses must be able to reach the gateway address for the network, or the installation will fail. • When deploying with IPv6, the installation 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.
Interfaces	<p>Crosswork is deployed on a single VM with 2 interfaces.</p> <ul style="list-style-type: none"> • No. of NICs: 2 • vNIC0: Management Traffic (for accessing the interactive console and passing the Control/Data information between servers). • vNIC1: 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 setup with two vNICs, all device traffic (incoming and outgoing) must be routed through the default vNIC1.</p>
NTP Server	<p>The IPv4 or IPv6 addresses or host names of the NTP server 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.</p> <p>Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.</p>
DNS Servers	<p>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.</p> <p>Ensure that the DNS servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.</p>
DNS Search Domain	<p>The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.</p>
Backup Server	<p>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.</p>

Requirement	Description
FQDN (Optional)	<p>The installation process supports using either a VIP (Virtual IP address) or an FQDN (Fully Qualified Domain Name) to access the VM.</p> <p>If you choose to use the FQDN, you will need one for the Management and one for the Data network.</p> <p>Crosswork deployed on a single VM does not support dual-stack configurations. Therefore, all FQDN addresses configured for the deployment environment must be either IPv4 or IPv6.</p> <p>Note If you choose to supply the FQDNs during the initial installation, the DNS server must be populated with them before the VM is powered on; otherwise, the installation script will fail to complete the environment setup.</p>

Port Requirements

Table 70: Ports used by Crosswork Single VM deployment on the Management Network

Port	Protocol	Used for	Direction
30602	TCP	Monitoring the installation (Crosswork Network Controller)	Inbound
30603	TCP	Crosswork Network Controller Web user interface (NGINX server listens for secure connections on port 443)	Inbound
30604	TCP	Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server	Inbound
30617	TCP	Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server	Inbound
30620	TCP	Receiving plug-and-play HTTP traffic on the ZTP server	Inbound
7	TCP/UDP	Discovering endpoints using ICMP	Outbound
22	TCP	Initiating SSH connections with managed devices	Outbound
22	TCP	Remote SSH connection	Inbound

Port	Protocol	Used for	Direction
53	TCP/UDP	Connecting to DNS	Outbound
123	UDP	Network Time Protocol (NTP)	Outbound
830	TCP	Initiating NETCONF	Outbound

When configuring the ports for Embedded Collectors, ensure that the ports mentioned in the following tables are configured on the device. For example, in case the port used for sending traps was previously set to 1062, change it to a port that is within the acceptable range for deploying a single virtual machine. The acceptable range is provided with the port number in [Table 71: Ports used by Crosswork Single VM deployment on the Device Network](#).

Table 71: Ports used by Crosswork Single VM deployment on the Device Network

Port	Protocol	Used for	Direction
31062 Accepted range of ports is 30160–31560	UDP	SNMP Collector	Outbound
22	TCP	CLI Collector	Outbound
30614 Accepted range of ports is 30160–31560	TLS	Syslog Collector This is the default value. You can change this value after installation from the Cisco Crosswork UI.	Inbound
30898 Accepted range of ports is 30160–31560	TCP		
30514 Accepted range of ports is 30160–31560	UDP		
30621	TCP	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.	Inbound

Port	Protocol	Used for	Direction
30622	TCP	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.	Inbound
Site Specific 6	TCP	gNMI collector	Outbound
Site Specific 7	Site Specific	Kafka and gRPC destination	Outbound

⁶ For default port information of a device, see the platform-specific documentation.

Ensure that port number on the device is the same as that configured on **Device Management > Network Devices > Edit Device**.

⁷ You cannot modify the port numbers of system-created destinations as they are created with predefined ports.

To modify the user-defined destination ports, edit the port number from **Administration > Data Collector(s) Global Settings > Data destinations > Edit destination**.

Install Crosswork Network Controller using the vCenter vSphere UI

This topic explains how to deploy Crosswork Network Controller on a single VM using the vCenter user interface.

This is the recommended method for installing Crosswork Network Controller on a single VM.

-
- Step 1** Download the latest available Cisco Crosswork platform 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 where you want to deploy the VM.
- Step 3** In the vSphere UI, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch for the Management Network that will be used to access the UI of the VM. 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 the virtual switch that will be used for the Data Network.
- Step 4** Review and confirm that your network settings meet the requirements.

Ensure that the networks that you plan to use for Management Network and Data network are connected to the host. Contact your Cisco Experience team for assistance.

Step 5 Choose **Actions > Deploy OVF Template**.

Caution The default VMware vCenter deployment timeout is 15 minutes. If vCenter times out during deployment, the resulting VM will not be bootable. To prevent this, we recommend that you document the choices (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 data center 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 7.0 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. This information is gathered from the OVF, and cannot be modified.

Note You may see alerts regarding the OVF package containing advanced configuration options and/or about trusted certificates. These are common and you can safely select the "Ignore" option.

Step 11 Click **Next**. The **Deploy OVF Template** window is refreshed, with **5 - License agreements** highlighted. Review the End User License Agreement and if you agree, click the **I accept all license agreements** checkbox. Otherwise, contact your Cisco Experience team for assistance.

Step 12 Click **Next**. The **Deploy OVF Template** window is refreshed, with **6 - Configuration** highlighted. Choose the desired deployment configuration.

Important For single VM deployment, the supported configurations are **IPv4 Network** and **IPv6 Network** using two NICs.

Figure 68: Select a deployment configuration

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 69: Select Storage

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	

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 **Destination Network** drop-down list, select the proper networks for the Management Network and the Data Network.

Figure 70: Select networks

8. Select networks

Select a destination network for each source network.

Source Network	Destination Network
Management Network	VM Network
Data Network	DPortGroup10
Admin Network	VM Network
NBI Network	VM Network

4 items

IP Allocation Settings

CANCEL BACK NEXT

Important Keep Admin Network and NBI Network at default values.

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 71: 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

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

- 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 at least one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words. While they satisfy the criteria, such passwords are weak and will be rejected resulting in failure to setup the VM.

- 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: #0070C0; color: white; padding: 2px;">9 Customize template 10 Ready to complete 	<table border="1"> <tr> <td colspan="2">Deployment Credentials</td> <td>2 settings</td> </tr> <tr> <td>Original VM Username</td> <td colspan="2">Default system administrator username: cw-admin</td> </tr> <tr> <td></td> <td colspan="2">cw-admin</td> </tr> <tr> <td>VM Password</td> <td colspan="2">Password for the default system administrator account</td> </tr> <tr> <td></td> <td>Password</td> <td>.....</td> </tr> <tr> <td></td> <td>Confirm Password</td> <td>.....</td> </tr> <tr> <td colspan="2">DNS and NTP Servers</td> <td>3 settings</td> </tr> <tr> <td colspan="3">DNS IPv4 Address</td> </tr> <tr> <td colspan="3">Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated.</td> </tr> <tr> <td colspan="3">8.8.8.8.8.4.4</td> </tr> <tr> <td colspan="3">NTP Servers</td> </tr> <tr> <td colspan="3">Please enter NTP server hostname. Multiple NTP servers can be provided space separated.</td> </tr> <tr> <td colspan="3">ntp.crosswork.com</td> </tr> <tr> <td colspan="2">DNS Search Domain</td> <td>Please enter the DNS search domain.</td> </tr> <tr> <td colspan="2"></td> <td>crosswork.com</td> </tr> <tr> <td colspan="2">Disk Configuration</td> <td>5 settings</td> </tr> <tr> <td colspan="2">Logfs Disk Size</td> <td>Please enter the size of the logfs disk in GB.</td> </tr> </table>	Deployment Credentials		2 settings	Original VM Username	Default system administrator username: cw-admin			cw-admin		VM Password	Password for the default system administrator account			Password		Confirm Password	DNS and NTP Servers		3 settings	DNS IPv4 Address			Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated.			8.8.8.8.8.4.4			NTP Servers			Please enter NTP server hostname. Multiple NTP servers can be provided space separated.			ntp.crosswork.com			DNS Search Domain		Please enter the DNS search domain.			crosswork.com	Disk Configuration		5 settings	Logfs Disk Size		Please enter the size of the logfs disk in GB.
Deployment Credentials		2 settings																																																		
Original VM Username	Default system administrator username: cw-admin																																																			
	cw-admin																																																			
VM Password	Password for the default system administrator account																																																			
	Password																																																		
	Confirm Password																																																		
DNS and NTP Servers		3 settings																																																		
DNS IPv4 Address																																																				
Please enter the DNS server's IPv4 address. Multiple DNS server IPs can be provided space separated.																																																				
8.8.8.8.8.4.4																																																				
NTP Servers																																																				
Please enter NTP server hostname. Multiple NTP servers can be provided space separated.																																																				
ntp.crosswork.com																																																				
DNS Search Domain		Please enter the DNS search domain.																																																		
		crosswork.com																																																		
Disk Configuration		5 settings																																																		
Logfs Disk Size		Please enter the size of the logfs disk in GB.																																																		

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**.
 - **Cluster Seed node**: Choose **True**.
 - **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**: Set to 1.
 - **Initial leader node count**: Set to 1.
 - **Location of VM**: Enter the location of VM.
 - **Installation type**: Not applicable to single VM deployment. Do not select any checkbox.
 - **Enable Skip Auto Install Feature**: Set to **True**.
 - **Ignore Diagnose Failure?**: Use the default value (True).
 - **Enable Diagnostics Script Check Run?**: Use the default value (True).

- **Default Application Resource Profile:** Use the default value (Empty).
- **Default Infra Resource Profile:** Use the default value (Empty).
- **Auto Action Manifest Definition:** Use the default value (Empty).

- 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:
- Open a VMware vCenter client.
 - In the **Recent Tasks** tab of the host VM, view the status of the **Deploy OVF template** and **Import OVF package** jobs.
- Step 18** Once the deployment is completed, right-click on the VM and select **Edit Settings**. The **Edit Settings** dialog box is displayed. Under the **Virtual Hardware** tab, update the following attributes:
- **CPU:** change to **24**
 - **Memory:** change to **128 GB**
- Click **OK** to save the changes.
- Step 19** Power on the Crosswork VM. 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 VM can vary based on the size of your deployment profile and the performance characteristics of your hardware.

Install Cisco Crosswork via the OVF Tool

This topic explains how to deploy Crosswork Network Controller on a single VM using the OVF tool. You must modify the list of mandatory and optional parameters in the script as per your requirements and run the OVF tool.



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

Follow these steps to log in to the Cisco Crosswork VM from SSH:

Before you begin

- In your vCenter data center, go to **Host > Configure > Networking > Virtual Switches** and select the virtual switch. In the virtual switch, select **Edit > Security**, and ensure that the following DVS port group properties are as shown:
 - Set **Promiscuous mode** as **Reject**
 - Set **MAC address changes** as **Reject**

Confirm the settings and repeat the process for each virtual switch used by Crosswork.

- Ensure you are using the OVF tool version 4.4 or higher.

Step 1 On the machine where you have the OVF tool installed, use the following command to confirm that you have OVF tool version 4.4:

```
ovftool --version
```

Step 2 Create the script file (see example below) and provide relevant information as per your target environment (such as IP addresses, gateway, netmask, password, and VCENTER_PATH, etc.).

```
cat svm_install.sh
#!/usr/bin/env bash
Host="X.X.X.X"
DM="thick"
DS="DS36"
Deployment="cw_ipv4"
DNSv4="10.10.0.99"
NTP="ntp.cisco.com"
Timezone="US/Pacific"
EnforcePodReservations="True"
EnableSkipAutoInstallFeature="True"
Domain="cisco.com"
Disclaimer="ACCESS IS MONITORED"
VM_NAME="svmEMS"
DataNetwork="DataNet"
ManagementNetwork="MgmtNet"
DataIPv4Address="x.x.x.x"
DataIPv4Gateway="x.x.x.x"
DataIPv4Netmask="x.x.x.x"
ManagementIPv4Address="x.x.x.x"
ManagementIPv4Gateway="x.x.x.x"
ManagementIPv4Netmask="x.x.x.x"
K8sServiceNetworkV4="10.75.0.0"
K8sPodNetworkV4="10.225.0.0"
Password="CLI Password"
Username="cw-admin"
ManagementVIP="x.x.x.x"
DataVIP="x.x.x.x"
VMType="Hybrid"
IsSeed="True"
InitNodeCount="1"
InitMasterCount="1"

SVM_OVA_PATH=$1

VCENTER_LOGIN="Administrator%40vsphere%2Elocal:Password%40123%21@x.x.x.x"
VCENTER_PATH="DC1/host"

ovftool --version
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS \
--numberOfCpus:"*" =24 --viCpuResource=:50000: \
--memorySize:"*" =131072 --viMemoryResource=:131072: \
--diskMode=$DM --overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--deploymentOption=$Deployment \
--prop:"DNSv4=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Timezone=${Timezone}" \
--prop:"EnforcePodReservations=${EnforcePodReservations}" \
--prop:"EnableSkipAutoInstallFeature=${EnableSkipAutoInstallFeature}" \
--prop:"Domain=${Domain}" \
--prop:"Disclaimer=${Disclaimer}" \
```

```

--name=$VM_NAME \
--net:"Data Network=${DataNetwork}" \
--net:"Management Network=${ManagementNetwork}" \
--prop:"DataIPv4Address=${DataIPv4Address}" \
--prop:"DataIPv4Gateway=${DataIPv4Gateway}" \
--prop:"DataIPv4Netmask=${DataIPv4Netmask}" \
--prop:"ManagementIPv4Address=${ManagementIPv4Address}" \
--prop:"ManagementIPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"ManagementIPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"K8sServiceNetworkV4=${K8sServiceNetworkV4}" \
--prop:"K8sPodNetworkV4=${K8sPodNetworkV4}" \
--prop:"CWPassword=${Password}" \
--prop:"CWUsername=${Username}" \
--prop:"ManagementVIP=${ManagementVIP}" \
--prop:"DataVIP=${DataVIP}" \
--prop:"VMType=${VMType}" \
--prop:"IsSeed=${IsSeed}" \
--prop:"InitNodeCount=${InitNodeCount}" \
--prop:"InitMasterCount=${InitMasterCount}" \
$SVM_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host

```

Step 3 Download the OVA and install scripts from [cisco.com](https://www.cisco.com). For the purpose of these instructions, we use the file name as **signed-cw-na-unifiedems-7.0.0-85-release700-240823.ova**.

Use the following command to extract the files from the tar bundle:

```
tar -xvzf signed-cw-na-unifiedems-7.0.0-85-release700-240823.ova
```

The OVA is extracted:

```

svm]# ls -al
-rw-r--r-- 1 root root 15416145920 Mar 28 11:12 cw-na-unifiedems-7.0.0-85-release700-240823.ova
-rwxr-xr-x 1 root root          2324 Apr  2 14:06 svm_install.sh

```

Step 4 Use the following command to make the scripts executable:

```
chmod +x {filename}
```

For example:

```
chmod +x svm_install.sh
```

Step 5 Execute the script with the OVA file name as parameter:

```

svm]# ./svm_install.sh cw-na-unifiedems-7.0.0-85-release700-240823.ova
VMware ovftool 4.4.0 (build-16360108)
Opening OVA source: cw-na-unifiedems-7.0.0-85-release700-240823.ova
<Removed some output >
Completed successfully

```

The time taken to create the VM can vary based on the size of your deployment profile and the performance characteristics of your hardware.

Install Crosswork Network Controller using the Docker Installer Tool

This section explains the procedure to install Crosswork Network Controller on a single VM using the docker installer tool. This method is less recommended compared to using the vCenter UI or the OVF tool for installation.

Before you begin

- Make sure that your environment meets all the vCenter requirements specified in [Installation Requirements, on page 295](#).
- The edited template in the `/data` directory contains sensitive information (VM passwords and the vCenter password). The operator needs to manage access to this content. Store the templates used for your install in a secure environment or edit them to remove the passwords.
- The `install.log`, `install_tf.log`, and `.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.
- The install script is safe to run multiple times. Upon error, input parameters can be corrected and re-run. You must remove the `install.log`, `install_tf.log`, and `tfstate` files before each re-run. Running the installer tool multiple times may result in the deletion and re-creation of VMs.
- In case you are using the same installer tool for multiple Crosswork 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 installer tool. 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 VM or not. Deployed VM is 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]
```

Known limitations:

- The vCenter host VMs defined must use the same network name (vSwitch) across all hosts in the data center.
- The vCenter storage folders or datastores organized under a virtual folder structure, are not currently supported. Ensure that the datastores referenced are not grouped under a folder.

Step 1

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, ensure that the directory name is in lower case.

Step 2 Download the installer bundle (.tar.gz file) and the OVA file from cisco.com to the directory you created previously. For the purpose of these instructions, we will use the file name as **signed-cw-na-unifiedems-installer-7.0.0-85-release700-240823.tar.gz** and **signed-cw-na-unifiedems-7.0.0-85-release700-240823.ova**.

Attention The file names mentioned in this topic are sample names and may differ from the actual file names in cisco.com.

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

```
tar -xvf signed-cw-na-unifiedems-installer-7.0.0-85-release700-240823.tar.gz
```

The contents of the installer bundle is extracted (e.g. `signed-cw-na-unifiedems-installer-7.0.0-85-release700-240823-release`). The extracted files will contain the installer image (**signed-cw-na-unifiedems-installer-7.0.0-85-release700-240823.tar.gz**) and files necessary to validate the image.

Step 4 Review the contents of the README file to understand everything that is in the package and how it will be validated in the following steps.

Step 5 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:

```
python3 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 have Python installed, go to python.org and download the version of Python that is appropriate for your work station.

Step 6 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-unifiedems-installer-7.0.0-85-release700-240823.tar.gz
```

Step 7 Run the 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-unifiedems-7.0.0-85-release700-240823  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 image rm {image id}` command can be used.

Step 8 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, use the following command:

```
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 setup, 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). Then navigate to that directory and rerun the installer.

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 9 Navigate to the directory with the VMware template.

```
cd /opt/installer/deployments/7.0.0/vcentre
```

Step 10 Copy the template file found under

/opt/installer/deployments/7.0.0/vcentre/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 11 Edit the template file located in the /data directory in a text editor, to match your planned deployment (for reference, see [Sample Manifest Template, on page 312](#)). The <sample manifest template> includes an example that you can reference for proper formatting. The example is more compact due to the removal of descriptive comments:

Step 12 From the /opt/installer directory, run the installer.

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

For example:

```
./cw-installer.sh install -m /data/deployment.tfvars -o
/data/signed-cw-na-unifiedems-7.0.0-85-release700-240823.ova
```

Step 13 Read, and then enter "yes" if you accept the End User License Agreement (EULA). Otherwise, exit the installer and contact your Cisco representative.

Step 14 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_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, open a case with Cisco and provide the .log files that were created in the /data directory (and the local directory where you launched the installer Docker container), to Cisco for review. The two most common reasons for the install to fail are: (a) password that is not adequately complex, and (b) errors in the template file. If the installer fails for any errors in the template (for example, mistyped IP address), correct the error and rerun the install script.

Sample Manifest Template

This topic presents the manifest template example for deploying Crosswork on a single VM:

```
Cw_VM_Image = ""      # Line added automatically by installer.
ClusterIPStack      = "IPv4"
ManagementVIP       = "10.78.103.198"
ManagementIPNetmask = "255.255.255.0"
ManagementIPGateway = "10.78.103.1"
DataVIP             = "192.168.100.198"
DataIPNetmask       = "255.255.255.0"
DataIPGateway       = "0.0.0.0"
DNS                 = "72.163.128.140"
DomainName          = "cisco.com"
CWPassword          = "*****!"
VMSize              = "XLarge"
```



```
NTP                                = "ntp.esl.cisco.com"
Timezone                           = "Asia/Calcutta"
EnableSkipAutoInstallFeature = "True"
CwVMs = {
  "0" = {
    VMName           = "SVM198",
    ManagementIPAddress = "10.78.103.197",
    DataIPAddress    = "192.168.100.197",
    NodeType         = "Hybrid"
  }
}
VCentreDC = {
  VCentreAddress = "10.64.80.220",
  VCentreUser = "<your-username>",
  VCentrePassword = "*****",
  DCname = "Crosswork-Single-VM",
  MgmtNetworkName = "VM Network",
  DataNetworkName = "CW-7.0-VLAN21",
  VMs = [
    {
      HostedCwVMs = ["0"],
      Host = "10.78.103.62",
      Datastore = "5.2TB-SSD-62-2",
      HSDatastore="5.2TB-SSD-62-2"
    }
  ]
}
SchemaVersion = "7.0.0"
```

