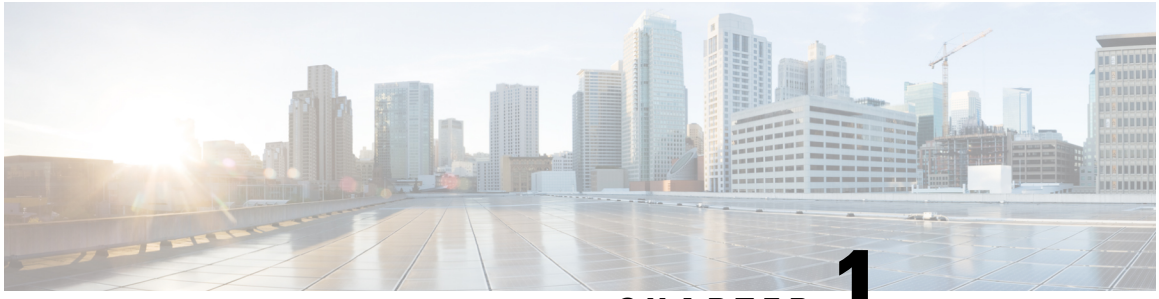
Cisco Crosswork Data Gateway 4.5 Installation and Configuration Guide for Cloud Applications

First Published: 2023-01-27

Last Modified: 2023-02-06

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

CONTENTS



CHAPTER 1

Overview

This section contains the following topics:

Audience

This guide is for experienced network administrators who want to deploy Cisco Crosswork Data Gateway for Crosswork Cloud in their network. Users of this guide should have a valid login for the Cisco Crosswork Cloud environment. This guide assumes that you are familiar with the following topics:

- Deploying OVF templates using VMware vCenter or OVF Tool.
- Working knowledge of the OpenStack platform.
- Deploying Cisco Crosswork Data Gateway using the CloudFormation template in Amazon Elastic Compute Cloud (EC2).
- Network monitoring and troubleshooting.
- Different operating systems used on devices that form your network, such as Cisco IOS-XR, IOS-XE, and NX-OS.
- Proxy settings necessary to connect from your company's internal network to the Crosswork Cloud.

Overview of Cisco Crosswork Data Gateway

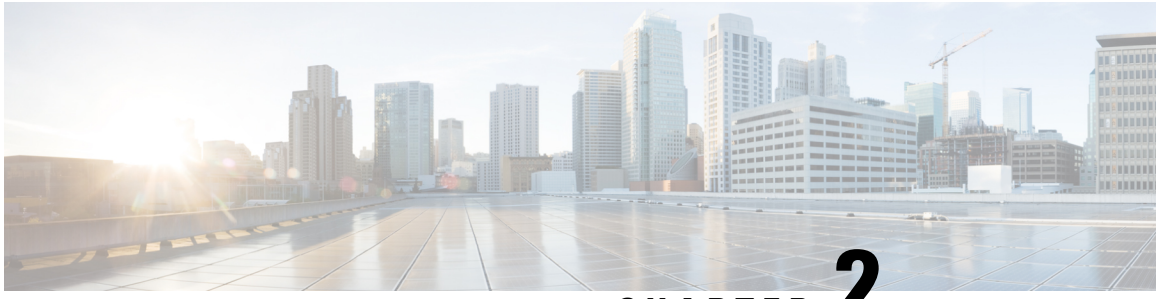
Cisco Crosswork Data Gateway enables collection of data from the monitored devices and forwards the collected data to the Cisco Crosswork Cloud applications. These applications can use the data for further analysis and if required, alert an administrator for further action.

Attention This guide explains how to install and configure Cisco Crosswork Data Gateway for Cloud applications.

For details on deploying Crosswork Data Gateway with on-premise applications, refer to the *Cisco Crosswork Infrastructure 4.5 and Applications Installation Guide*.

Crosswork Data Gateway has been validated for use with the following Crosswork Cloud applications:

- Cisco Crosswork Trust Insights is a cloud-based SaaS solution that reports on the integrity of devices and provides forensics for assured inventory.
- Cisco Crosswork Cloud Traffic Analysis service is a hosted application that provides rich analysis, visualization, and optimization recommendations for network traffic flows.



CHAPTER 2

Installation Requirements

This chapter provides information about the general guidelines and minimum requirements for installing Crosswork Data Gateway on the following platforms:

- VMware
- OpenStack Platform
- Amazon EC2

Crosswork Data Gateway Pre-installation Checklist

The pre-installation checklist helps you:

- Verify that all system requirements are met, all required ports are enabled.
- Gather the information required to complete the installation.

Before installing Crosswork Data Gateway, complete the pre-installation checklist.

1. Ensure that the host server meets the resource requirements. See VM Requirements, on page 3
2. Enable ports that are required for the Crosswork Data Gateway to operate. See Ports Used, on page 7.
3. Understand if a proxy server may be required in your environment. See Proxy Server Requirements, on page 7.

VM Requirements

The table shows software requirements for the supported virtualization platforms along with the physical and network resource requirements needed to support the Crosswork Data Gateway.

The resource requirements to install Crosswork Data Gateway are the same for all the data centers.

Table 1: Cisco Crosswork Data Gateway VM Requirements for Cloud applications

Requirement	Description
Data Center	**VMware** • VMware vCenter server 6.7, ESXi 6.5 • VMware vCenter Server 7.0, ESXi 6.5 and 6.7 **Attention** In VMware vCenter 6.5 (Flash and HTML5 interfaces) and 6.7 releases (6.7U1), the GUI installer does not process the OVF parameter list correctly. To prevent this issue, ensure that the following parameters in the **vCenter vSphere Client > Deploy OVF Template > Customize template > 03. vNIC Role Assignment** are specified as: • The interface for **03. vNIC Role Assignment > e. Control** must be `eth0` • The interface for **03. vNIC Role Assignment > g. Northbound External Data** must be `eth0` • The interface for **03. vNIC Role Assignment h. Southbound Data** must be `eth0` • The **16. Controller Setting > a. Crosswork Controller IP** should be crosswork.cisco.com • The **16 Controller Setting > b. Crosswork Controller Port** should be 443 **OpenStack** • OpenStack OSP16 **Amazon** • Amazon Elastic Cloud Compute
Memory	32 GB
Total Disk space (Boot disk + Data disk)	74 GB (50 GB + 24 GB) **Note** Data disk space is an optional requirement.
vCPU	8

Requirement	Description				
Interfaces	Minimum: 1 Maximum: 4 Crosswork Data Gateway can be deployed with either 1, 2, 3, or 4 interfaces as per the following combinations:				
	No. of NICs	**vNIC0**	**vNIC1**	**vNIC2**	**vNIC3**
	1	• Management Traffic • Control/Data Traffic • Device Access Traffic	—	—	—
	2	• Management Traffic	• Control/Data Traffic • Device Access Traffic	—	—
	3	• Management Traffic	• Control/Data Traffic	• Device Access Traffic	—
	4	—	—	—	Custom traffic

Requirement	Description
	• Management traffic: for accessing the Interactive Console and troubleshooting the Crosswork Data Gateway VM. • Control or Data traffic: to receive configuration of collection jobs from the Crosswork Cloud and to forward collected data to the Crosswork Cloud. **Important** Crosswork Data Gateway can connect to the Cloud only when the Control or Data interface has access to the Internet. • Device access traffic: for device management and telemetry data. • Custom traffic: for routing the custom traffic such as SSH traffic. For deployment using multiple vNICs, you can assign traffic types across different vNICs based on the network design. For example, in a 2 vNIC deployment, you can select either vNIC0 or vNIC1 for processing the following traffic: • Management traffic • Control or Data traffic • Device access traffic
IP Addresses	One, two, three, or four IPv4 or IPv6 addresses based on the number of interfaces you choose to use. **Note** Crosswork does not support dual stack configurations. Therefore, ALL addresses for the environment must be either IPv4 or IPv6.
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. **Note** Confirm that the NTP IP address or host name is reachable on the network or installation fails. The Crosswork Data Gateway host and virtual machine must be synchronized to an NTP server or the enrollment with Crosswork Cloud may not go through.
DNS Servers	The IPv4 or IPv6 addresses of the DNS servers you plan to use. If you want to enter multiple DNS servers, separate them with spaces. These should be the same DNS servers you use to resolve host names across your network.
DNS Search Domain	The search domain you want to use with the DNS servers (for example, cisco.com). You can only have one search domain.
(optional) Proxy Server	URL of an optional management network proxy server. If your environment requires an HTTP or HTTPS proxy in order to access URLs on the public Internet, you must configure a proxy server for the Cisco Crosswork Data Gateway to successfully connect to the Crosswork Cloud service.
(optional) Syslog Server	Hostname, IPv4, or IPv6 address of an optional Syslog server.

Requirement	Description
(optional) Auditd Server	Hostname, IPv4, or IPv6 address of an optional Auditd server.

Ports Used

The following table shows the minimum set of ports needed for Crosswork Data Gateway to operate correctly.

Note This is only to enable the base Crosswork Data Gateway functionality. Additional ports may be enabled depending on the application that is running the Crosswork Data Gateway.

Table 2: Ports to be opened for Management Traffic

Port	Protocol	Used for...	Direction
22	TCP	SSH server	Inbound
22	TCP	SCP client **Note** The SCP port can be configured.	Outbound
123	UDP	NTP Client	Outbound
53	UDP	DNS Client	Outbound
443	TCP	Crosswork Cloud Controller	Outbound

Table 3: Ports to be opened for Control/Data Traffic

Port	Protocol	Used for...	Direction
179	TCP	BGP	Outbound
179	TCP	BGP	Inbound
161	UDP	SNMP	Outbound
2055	UDP	Netflow	Inbound

Proxy Server Requirements

Many production environments do not allow direct connectivity to public Internet sites. If your environment requires an HTTP or HTTPS proxy in order to access URLs on the public Internet, you must configure a proxy

server in order for the Cisco Crosswork Data Gateway to successfully connect to the Crosswork Cloud service. Consult with your network administrator to understand if a proxy server may be required.

If a proxy server is required, the details of the proxy server on the Crosswork Data Gateway are configured in one of the following ways:

- (recommended) By entering the proxy server credentials during installation. See **Controller and Proxy Settings** in Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12.
- From the Interactive Console of the Crosswork Data Gateway after installation. See Configure Control Proxy, on page 93

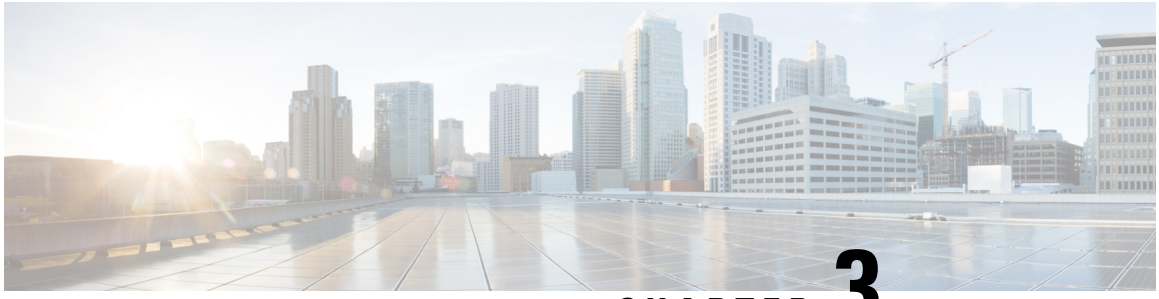
Amazon EC2 Settings

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

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

Requirement	Description
VPC & Subnets	Virtual Private Cloud (VPC) is created and configured with dedicated subnets for Crosswork interfac Crosswork Data Gateway (Management, Data, and Device) interfaces. Ensure that you do not use any
Endpoints	An endpoint is created in your VPC with the following parameters: • **Service name:** EC2 service for the region (availability zone) where you are deploying. • **Private DNS names:** Enabled • **Endpoint type:** Interface • Under **Subnets**, specify the management subnet that you intend to use for the installation. If you subnets for the Crosswork VM and the Crosswork Data Gateway VM, ensure that you specify bo that the endpoint has access to the subnets.
IAM role	A role is created in Identity and Access Management (IAM) with relevant permission policies. An IA permissions with credentials that are valid for short durations. Roles can be assumed by entities that y **Note** • The minimum permissions required for a Crosswork role are **ec2:AssignPrivateIpA ec2:UnassignPrivateIpAddresses**. • The trust policy for your role must have the **"Action": "sts:AssumeRole"** conditio
Key pairs	Key pairs (private keys used to log into the VMs) are created and configured.

Requirement	Description
IP addresses	**Crosswork Data Gateway**: IP addresses for Management Traffic and Data Traffic only: • The IP addresses must be able to reach the gateway address for the network where Cisco Cro or the installation fails. • Now, your IP allocation is permanent and cannot be changed without redeployment. For more Experience team.
Security group	A security group must be created and configured to specify which ports or traffic are allowed.
Instance type	The **t2.2xlarge** instance type is supported for Crosswork Data Gateway (production and lab deplo
CloudFormation (CF) template	The CF template (.yaml) files for Crosswork Data Gateway VMs that must be uploaded during th templates procedure. For more information, see Install Crosswork Data Gateway on Amazon EC2 page 72.
User data	The VM-specific parameters script that must be specified during the manual installation procedur • Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template, on page • Install Crosswork Data Gateway on Amazon EC2 Manually, on page 73



CHAPTER 3

Installation Tasks

This section contains the following topics:

Install Cisco Crosswork Data Gateway

Cisco Crosswork Data Gateway is initially deployed as a VM called Base VM (containing only enough software to enroll itself with Crosswork Cloud). Once the Crosswork Data Gateway is registered with Crosswork Cloud, Crosswork Cloud pushes the collection job configuration down to the Crosswork Data Gateway, enabling it to gather the data it needs from the network devices.

Based on the size and geography of your network, you can deploy more than one Cisco Crosswork Data Gateway.

Cisco Crosswork Data Gateway Deployment and Set Up Workflow

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

1. Plan your installation. Refer to the topic Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 for information on deployment parameters and possible deployment scenarios.

2. Ensure that you have the software image required to deploy Cisco Crosswork Data Gateway on your preferred platform:

VMware	Install Crosswork Data Gateway Using vCenter vSphere Client, on page 25
	Install Crosswork Data Gateway Via OVF Tool, on page 31

OpenStack	Install Crosswork Data Gateway on OpenStack from OpenStack CLI, on page 34 Install Crosswork Data Gateway on OpenStack from the OpenStack UI, on page 48
Amazon EC2	Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template, on page 72 Install Crosswork Data Gateway on Amazon EC2 Manually, on page 73

3. Generate and export Enrollment package.
   - Generate Enrollment Package, on page 80
   - Obtain the Enrollment Package, on page 82
4. Enroll Cisco Crosswork Data Gateway with Crosswork Cloud applications. See Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 84.

Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

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

Interface addresses

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

User Accounts

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

- Cisco Crosswork Data Gateway administrator, with the username, **dg-admin**, and the password set during installation. The administrator uses this ID to log in and troubleshoot Cisco Crosswork Data Gateway.
- Cisco Crosswork Data Gateway operator, with the username, **dg-oper**, and the password set during installation. This is a read-only user and has permissions to perform all ‘read’ operations and limited ‘action’ commands.
- A **dg-tac** user account that is used to enable Cisco to assist you in troubleshooting issues with the Crosswork Data Gateway. (Enable TAC Shell Access, on page 107). The temporary password for this account is created when you enable troubleshooting access.

To know what operations an admin and operator can perform, see Section Supported User Roles, on page 87.

The **dg-admin** and **dg-oper** user accounts are reserved usernames and cannot be changed. You can change the password in the console for both the accounts. See Change Password, on page 89. In case of lost or forgotten passwords, you have to create a new VM, destroy the current VM, and reenroll the new VM on Crosswork Cloud.

Installation Parameters and Scenarios

In the following table:

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

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

Note When entering the parameters for deployment, ensure that you add the correct parameters. If the parameter values are incorrect, you have to destroy the current Crosswork Data Gateway VM, create a new VM, and reenroll the new VM with Cisco Crosswork.

Table 4: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios

Name	Parameter	Description	Additional Information
Host Information			
Hostname*	`Hostname`	Name of the Cisco Crosswork Data Gateway VM specified as a fully qualified domain name (FQDN). **Note** In larger systems, you are likely to have more than one Cisco Crosswork Data Gateway VM. The hostname must, therefore, be unique and created in a way that makes identifying a specific VM easy.	
Description*	`Description`	A detailed description of the Cisco Crosswork Data Gateway.	

Name	Parameter	Description	Additional Information
Label	`Label`	Label used by Cisco Crosswork Cloud to categorize and group multiple Cisco Crosswork Data Gateways.	
Deployment	`Deployment`	Parameter that conveys the controller type. Specify the value as `Crosswork Cloud` for Cloud deployment.	You must specify this parameter for VMware or OVF tool installation.
AllowRFC8190	`AllowRFC8190`	Automatically allow addresses in an RFC 8190 range. Options are `True`, `False`, or `Ask`, where the initial configuration script prompts for confirmation. The default value is `True`.	

Name	Parameter	Description	Additional Information
Private Key URI	`DGCertKey`	URI to private key file for session key signing. You can retrieve this using SCP (`user@host:path/to/file`).	Crosswork Cloud uses self-signed certificates for handshake with Cisco Crosswork Data Gateway. These certificates are generated at installation. However, if you want to use third party or your own certificate files enter these parameters. Certificate chains override any preset or generated certificates in the Cisco Crosswork Data Gateway VM and are given as an SCP URI (user:host:/path/to/file). **Note** The host with the URI files must be reachable on the network (in the vNIC0 interface via SCP) and files must be present at the time of install.
Certificate File and Key Passphrase	`DGCertChainPwd`	SCP user passphrase to retrieve the Cisco Crosswork Data Gateway PEM formatted certificate file and private key.	
Data Disk Size	`DGAppdataDisk`	Size in GB of a second data disk. The minimum size is 20GB. The default size is 24GB.	

Name	Parameter	Description	Additional Information
AwsIamRole	`AwsIamRole`	AWS IAM role name for EC2 installation.	A role created in Identity and Access Management (IAM) in the AWS environment with relevant permissions.
Passphrases			
dg-admin Passphrase*	`dg-adminPassword`	The password you have chosen for the dg-admin user. Password must be 8–64 characters.	
dg-oper Passphrase*	`dg-operPassword`	The password you have chosen for the dg-oper user. Password must be 8-64 characters.	
Interfaces **Note** You must select either an IPv4 or IPv6 address. Selecting **None** in both IPv4 Method and IPv6 Method fields results in a nonfunctional deployment.			
vNIC Role Assignment 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. Each parameter has a predefined role. The parameter accepts the interface value as eth0, eth1, or eth2. The fourth interface, eth3, allows you to separate SSH, management, control (Crosswork Cloud service), and north data, and south data traffic.			

Name	Parameter	Description	Additional Information
NicDefaultGateway	`NicDefaultGateway`	Interface used as the Default Gateway for processing the DNS and NTP traffic. Traffic that is not assigned to any other interface is defaulted to this interface. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	You can configure the number of interfaces based on the vNIC model that you chose to deploy Crosswork Data Gateway. For example, if you deployed Crosswork Data Gateway on 2 active vNICs, the roles must be configured to use the eth0 and eth1 interfaces. • The NicControl, NicNBExternalData, and NicSBData roles map to eth1. • The NicControl, NicNBExternalData, NicSBData roles map to `eth1`. • The NicSBData role maps to `eth2`. • The NicControl, and NicNBExternalData roles map to `eth1`.
NicAdministration	`NicAdministration`	Interface used to route the traffic associated with the administration of the Crosswork Data Gateway. The interface uses SSH protocol through the configured port. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicExternalLogging	`NicExternalLogging`	Interface used to send logs to Crosswork Cloud. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicManagement	`NicManagement`	Interface used to send the enrollment and other management traffic. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicControl	`NicControl`	Interface used for sending the destination, device, and collection configuration. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
NicNBExternalData	`NicNBExternalData`	Interface used to send collection data to Crosswork Cloud. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	

Name	Parameter	Description	Additional Information
NicSBData	`NicSBData`	Interface used to collect data from all devices. Options are `eth0`, `eth1`, `eth2`, or `eth3`. The default value is `eth0`.	
vNIC IPv4 Address (vNIC0, vNIC1, vNIC2, and vNIC3 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information

vNIC IPv4 Method*	`Vnic0IPv4Method`
	`Vnic1IPv4Method`
	`Vnic2IPv4Method`
	`Vnic3IPv4Method`
		Options are `None`, `Static`, or `DHCP`.
		Note DHCP support is enabled only for deployments performed using the QCOW2 images.
		To use IPv4 address, select Method as `Static` or `DHCP`, and select the vNICxIPv6 Method as `None`.
		The default value for Method is `None`.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for IPv4 address. Enter information in the vNIC IPv6 Address parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			• **DHCP**: Values for the vNIC IPv4 Address parameters are assigned automatically.
			Do not change the default values.

vNIC IPv4 Address*	`Vnic0IPv4Address`
	`Vnic1IPv4Address`
	`Vnic2IPv4Address`
	`Vnic3IPv4Address`
		IPv4 address of the interface.	

vNIC IPv4 Netmask*	`Vnic0IPv4Netmask`
	`Vnic1IPv4Netmask`
	`Vnic2IPv4Netmask`
	`Vnic3IPv4Netmask`
		IPv4 netmask of the interface in dotted quad format.	

vNIC IPv4 Skip Gateway*	`Vnic0IPv4SkipGateway`
	`Vnic1IPv4SkipGateway`
	`Vnic2IPv4SkipGateway`
	`Vnic3IPv4SkipGateway`
		Options are `True` or `False`.
		Selecting `True` skips configuring a gateway.
		The default value is `False`.	

vNIC IPv4 Gateway*	`Vnic0IPv4Gateway`
	`Vnic1IPv4Gateway`
	`Vnic2IPv4Gateway`
	`Vnic3IPv4Gateway`
		IPv4 address of the vNIC gateway.	

vNIC IPv6 Address (vNIC0, vNIC1, vNIC2, and vNIC3 based on the number of interfaces you choose to use)			

Name	Parameter	Description	Additional Information

vNIC IPv6 Method*	`Vnic0IPv6Method`
	`Vnic1IPv6Method`
	`Vnic2IPv6Method`
	`Vnic3IPv6Method`
		Options are `None`, `Static`, `DHCP` or `SLAAC (QCOW2 only)`.
		The default value for **Method** is `None`.
		Note DHCP support is enabled only for deployments performed using the QCOW2 images.
			If you have selected **Method** as:
			• **None**: Skip the rest of the fields for IPv6 address. Enter information in the **vNIC*x* IPv4 Address** parameters.
			• **Static**: Enter information in **Address**, **Netmask**, **Skip Gateway**, and **Gateway** fields
			• **DHCP**: Values for the vNIC IPv6 Address parameters are assigned automatically.
			Do not change the VnicxIPv6Address default values.

vNIC IPv6 Address*	`Vnic0IPv6Address`
	`Vnic1IPv6Address`
	`Vnic2IPv6Address`
	`Vnic3IPv6Address`
		IPv6 address of the interface.	

vNIC IPv6 Netmask*	`Vnic0IPv6Netmask`
	`Vnic1IPv6Netmask`
	`Vnic2IPv6Netmask`
	`Vnic3IPv6Netmask`
		IPv6 prefix of the interface.	

vNIC IPv6 Skip Gateway*	`Vnic0IPv6SkipGateway`
	`Vnic1IPv6SkipGateway`
	`Vnic2IPv6SkipGateway`
	`Vnic3IPv6SkipGateway`
		Options are `True` or `False`.
		Selecting `True` skips configuring a gateway.
		The default value is `False`.	

vNIC IPv6 Gateway*	`Vnic0IPv6Gateway`
	`Vnic1IPv6Gateway`
	`Vnic2IPv6Gateway`
	`Vnic3IPv6Gateway`
		IPv6 address of the vNIC gateway.	

DNS Servers			
DNS Address*	`DNS`	Space-delimited list of IPv4 or IPv6 addresses of the DNS server accessible in the management interface.	

Name	Parameter	Description	Additional Information
DNS Search Domain	`Domain`	DNS search domain. The default value is `localdomain`.	
DNS Security Extensions	`DNSSEC`	Options are `False`, `True`, or `Allow-Downgrade`. Select `True` to use DNS security extensions. The default value is `False`.	
DNS over TLS	`DNSTLS`	Options are `False`, `True`, or `Opportunistic`. Select `True` to use DNS over TLS. The default value is `False`.	
Multicast DNS	`mDNS`	Options are `False`, `True`, or `Resolve`. Select `True` to use multicast DNS. The default value is `False`.	
Link-Local Multicast Name Resolution	`LLMNR`	Options are `False`, `True`, `Opportunistic`, or `Resolve`. Select `True` to use link-local multicast name resolution. The default value is `False`.	
NTP Servers			
NTPv4 Servers*	`NTP`	NTPv4 server list. Enter 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 <sample>.ntp.org. NTP server is critical for time synchronization between Cisco Crosswork Data Gateway, Crosswork Cloud, and devices. Using a nonfunctional or dummy address may cause issues when Crosswork Cloud and Cisco Crosswork Data Gateway try to communicate with each other.

Name	Parameter	Description	Additional Information
Use NTPv4 Authentication	`NTPAuth`	Select `True` to use NTPv4 authentication. The default value is `False`.	The `NTPKey`, `NTPKeyFile`, and `NTPKeyFilePwd` can be configured only when the `NTPAuth` is set to `True`.
NTPv4 Keys	`NTPKey`	Key IDs to map to the server list. Enter space-delimited list of Key IDs.	
NTPv4 Key File URI	`NTPKeyFile`	SCP URI to the chrony key file.	
NTPv4 Key File Passphrase	`NTPKeyFilePwd`	Password of SCP URI to the chrony key file.	
Remote Syslog Server			

Name	Parameter	Description	Additional Information
Use Remote Syslog Server	`UseRemoteSyslog`	Select `True` to send syslog messages to a remote host. The default value is `False`.	Configuring an external syslog server sends service events to the external syslog server. Otherwise, they are logged only to the Cisco Crosswork Data Gateway VM. If you want to use an external syslog server, you must specify these seven settings. **Note** The host with the URI files must be reachable on the network (from vNIC0 interface via SCP) and files must be present at the time of install.
Syslog Server Address	`SyslogAddress`	IPv4 or IPv6 address of a syslog server accessible in the management interface. **Note** If you are using an IPv6 address, surround it with square brackets ([1::1]).	
Syslog Server Port	`SyslogPort`	Port number of the optional syslog server. The port value can range 1–65535. By default, this value is set to 514.	
Syslog Server Protocol	`SyslogProtocol`	Options are `UDP`, `TCP`, or `RELP` to send the syslog. The default value is `UDP`.	
Use Syslog over TLS	`SyslogTLS`	Select `True` to use TLS to encrypt syslog traffic. By default, this parameter is set to `False`.	
Syslog TLS Peer Name	`SyslogPeerName`	The syslog server hostname exactly as entered in the server certificate SubjectAltName or subject common name.	
Syslog Root Certificate File URI	`SyslogCertChain`	URI to the PEM formatted root cert of syslog server retrieved using SCP.	
Syslog Certificate File Passphrase	`SyslogCertChainPwd`	Password of SCP user to retrieve Syslog certificate chain.	
Remote Auditd Server			

Name	Parameter	Description	Additional Information
Use Remote Auditd Server	`UseRemoteAuditd`	Select `True` to send Auditd message to a remote host. The default value is `False`.	Configure the Crosswork Data Gateway VM to send auditd messages to a remote server. Specify these three settings to forward auditd messages to an external Auditd server.
Auditd Server Address	`AuditdAddress`	Hostname, IPv4, or IPv6 address of an optional Auditd server.	
Auditd Server Port	`AuditdPort`	Port number of an optional Auditd server. The default port number is 60.	
Controller and Proxy Settings			
Proxy Server URL	`ProxyURL`	URL of an optional HTTP proxy server.	In Cloud deployment, Cisco Crosswork Data Gateway must connect to the Internet via TLS. If you use a proxy server, specify these parameters.
Proxy Server Bypass List	`ProxyBypass`	Comma-separated list of addresses and hostnames that will not use the proxy.	
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.	
Auto Enrollment Package Transfer			

Name	Parameter	Description	Additional Information
Enrollment Destination Host and Path**	`EnrollmentURI`	SCP host and path to transfer the enrollment package using SCP (`user@host:/path/to/file`).	Cisco Crosswork Data Gateway requires the Enrollment package to enroll with Crosswork Cloud. If you specify these parameters during the installation, the enrollment package is automatically transferred to the local host once Cisco Crosswork Data Gateway boots up for the first time. If you do not specify these parameters during installation, then export enrollment package manually by following the procedure Obtain the Enrollment Package, on page 82.
Enrollment Passphrase**	`EnrollmentPassphrase`	SCP user passphrase to transfer enrollment package.	

What do next: Proceed to installing the Cisco Crosswork Data Gateway VM.

Install Crosswork Data Gateway on VMware

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

- Install Crosswork Data Gateway Using vCenter vSphere Client, on page 25
- Install Crosswork Data Gateway Via OVF Tool, on page 31

Install Crosswork Data Gateway Using vCenter vSphere Client

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

Step 1 Refer to Cisco Crosswork Data Gateway 4.5 Release Notes for Cloud Application and download the Crosswork Data Gateway image (*.ova) file.

Note When using the latest Mozilla Firefox version to download the .ova image, if the downloaded file has the extension as .dms, change the extension back to .ova before installation.

Step 2 Connect to vCenter and login with your credentials.

Step 3 Select the data center where you want to deploy the Crosswork Data Gateway VM.

Step 4 Connect to vCenter vSphere Client. Then select **Actions** > **Deploy OVF Template**.

Warning The default VMware vCenter deployment timeout is 15 minutes. If the time taken to complete the OVF template deployment exceeds 15 minutes, vCenter times out and you have to start over again. To prevent this, we recommend that you plan what you enter by reviewing the template before you start the deployment.

Connect to vCenter and login with your credentials.

Step 5 The VMware **Deploy OVF Template** wizard appears and highlights the first step, **1 Select template**.

a) Select **Local File** and then click **Browse** to navigate to the location where you downloaded the OVA image file and select it.

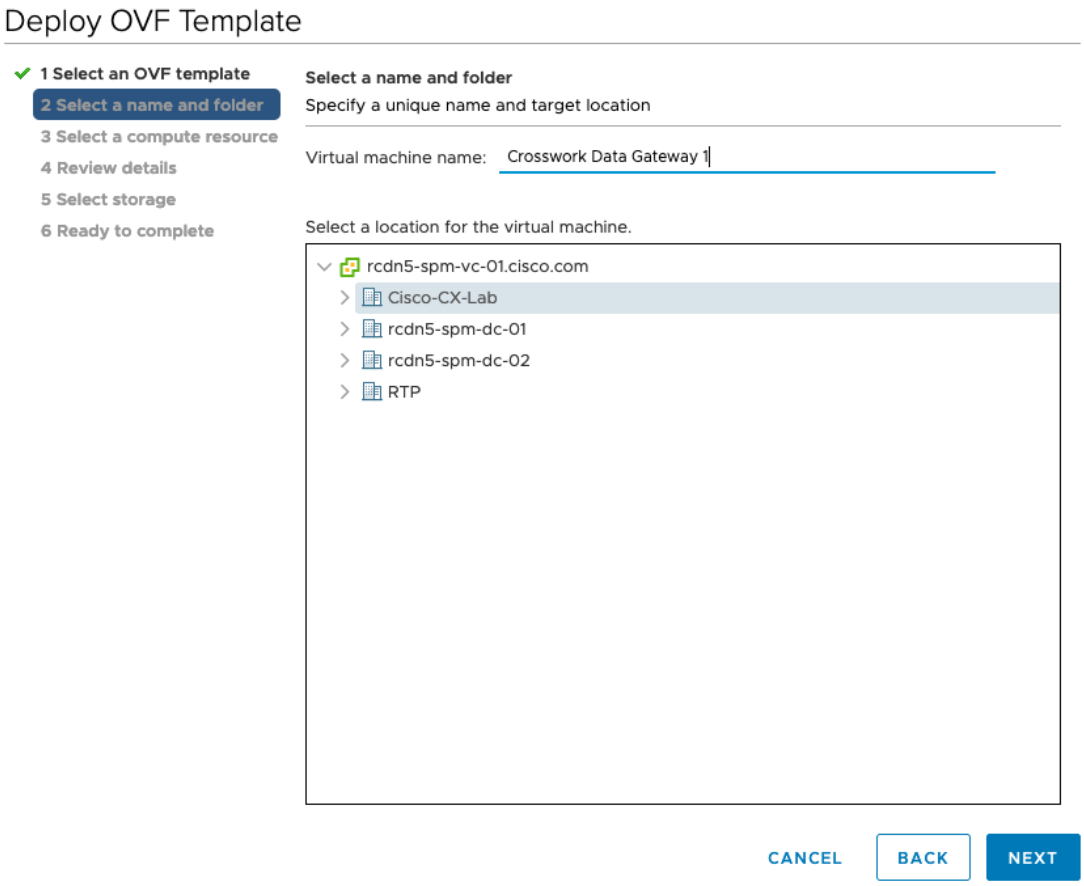
The filename is displayed in the window.

Step 6 Click **Next** to go to **2 Select name and folder**, as shown in the following figure.

a) Enter a name for the Cisco Crosswork Data Gateway VM you are creating.

For larger systems it is likely that you will have more than one Cisco Crosswork Data Gateway VM. The Cisco Crosswork Data Gateway name should, therefore, be unique and created in a way that makes identifying a specific VM easy.

b) In the **Select a location for the virtual machine** list, choose the datacenter under which the Cisco Crosswork Data Gateway VM resides.



Step 7 Click **Next** to go to **3 Select a compute resource**. Choose the VM's host.

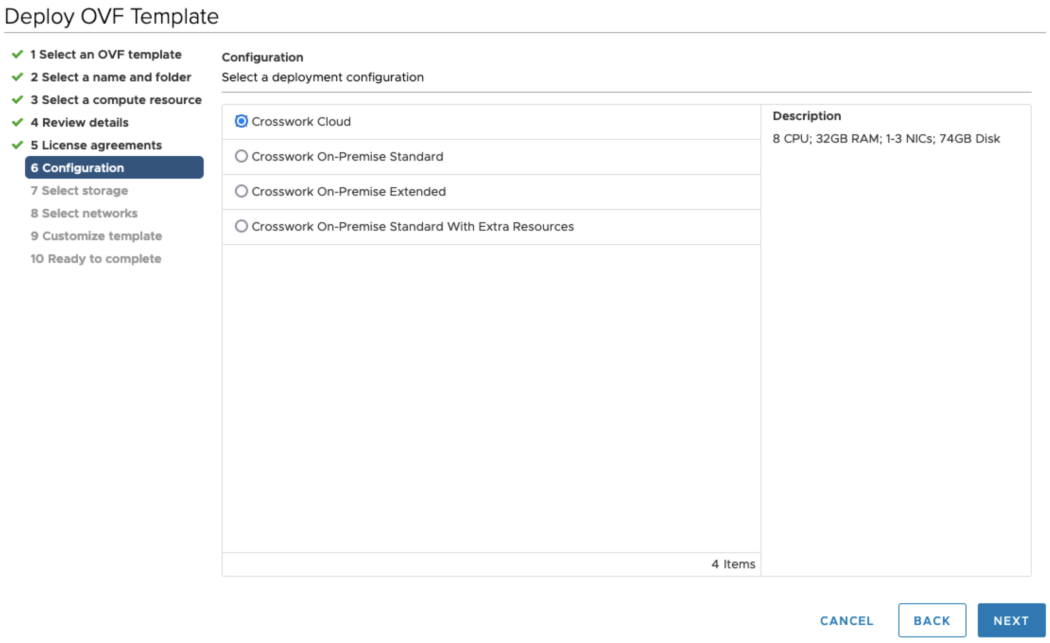
Step 8 Click **Next**. The VMware vCenter Server validates the OVA. The network speed determines how long the validation takes. When the validation is complete, the wizard moves to **4 Review details**. Review the OVA's information and then click **Next**.

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

Note This information is gathered from the OVF and cannot be modified. The template reports disk requirements for an on-premise deployment. This can be ignored as you will select the correct disk configuration in the next step.

Step 9 Click **Next** to go to **5 License agreements**. Review the End User License Agreement and click **Accept**.

Step 10 Click **Next** to go to **6 Configuration**, as shown in the following figure. Select **Crosswork Cloud**.

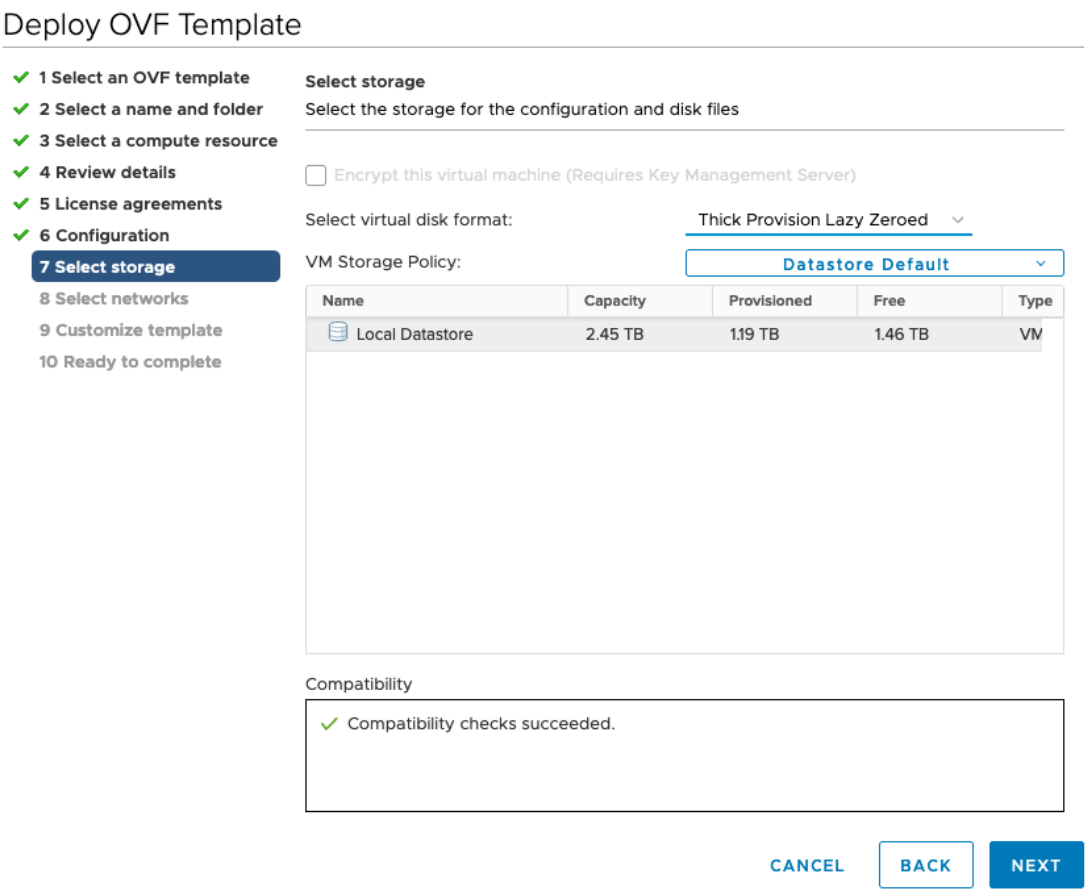


Step 11 Click **Next** to go to **7 Select storage**, as shown in the following figure.

a) In the **Select virtual disk format** field,

- For production environment, choose **Thick Provision Lazy Zeroed**.
- For development environment, choose **Thin Provision**.

b) From the **Datastores** table, choose the datastore you want to use.

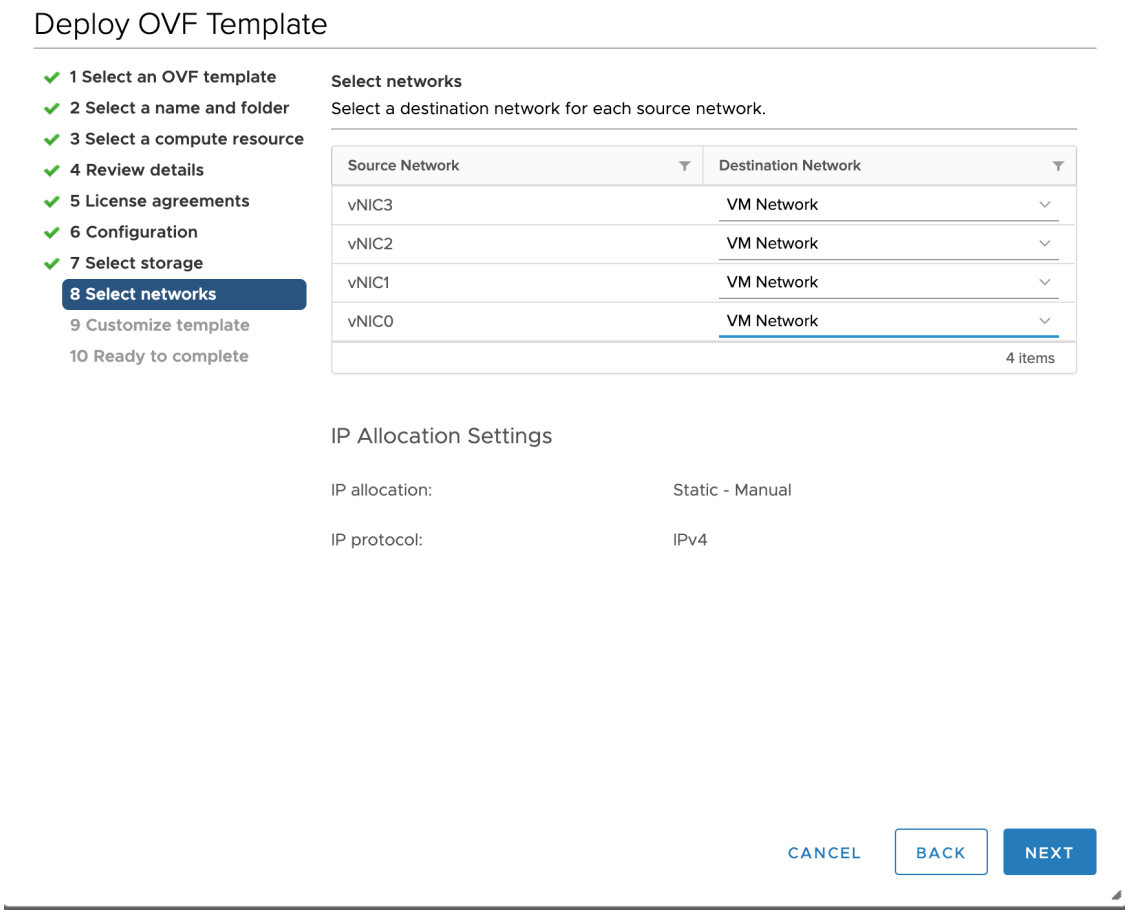


Step 12 Click **Next** to go to **8 Select networks**, as shown in the following figure. In the drop-down table at the top of the page, choose the appropriate destination network for each source network based on the number of vNICs you plan to use.

Start with **vNIC0** and select a destination network that will be used. Leave unused **vNICs** set to the default value.

Note In the following image,

- **VM Network** is the management network for accessing the Interactive Console and troubleshooting the Crosswork Data Gateway VM.
- **Crosswork-Cloud** is the controller network where the Crosswork Data Gateway connects to Crosswork Cloud.
- **Crosswork-Devices** is the network for device access traffic.



Step 13 Click **Next** to go to **9 Customize template**, with the **Host Information Settings** already expanded.

Note

- The VMware vCenter Server 6.7, 6.5, ESXi version 5.5 or 6.0 has issue with expanding the correct parameters. To override this issue, ensure that in the **Customize template > 03. vNIC Role Assignment** section, the following parameters are set as:
  - All the roles are set to eth0.
  - **16. Controller Setting > a. Crosswork Controller IP**: crosswork.cisco.com
  - **16. Controller Setting > b. Crosswork Controller Port**: 443
- For larger systems it is likely that you will have more than one Cisco Crosswork Data Gateway VM. The Cisco Crosswork Data Gateway hostname should, therefore, be unique and created in a way that makes identifying a specific VM easy.

Enter the information for the parameters as described in Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12.

Note When this menu is first displayed, there is an error "7 properties have invalid values". This is normal and clear as you enter appropriate values.

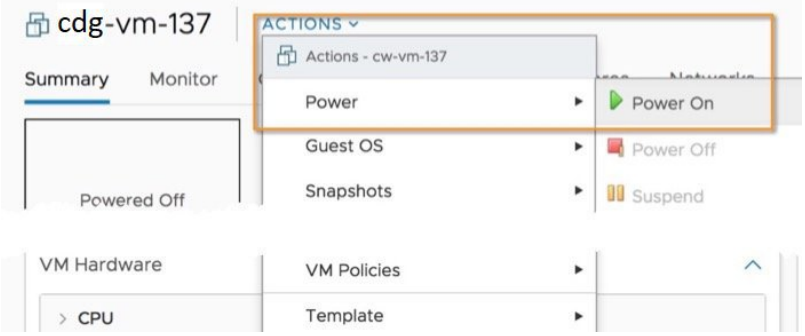
Step 14 Click **Next** to go to **10 Ready to complete**. Review your settings and then click **Finish** if you are ready to begin deployment.

Step 15 Check deployment status.

a) Open the vCenter vSphere client.

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

Step 16 After the deployment status becomes 100%, power on the VM to complete the deployment process. Expand the host's entry so you can click the VM and then choose **Actions** > **Power** > **Power On**, as shown in the following figure:



Wait for at least five minutes for the VM to come up and then log in through vCenter or SSH.

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. Make any changes to these settings at your own risk. If you wish to change the IP address, destroy the current VM, create a new VM, and reenroll the new one on the Crosswork Cloud.

Verify that the installation was successful.

1. Log in to Crosswork Data Gateway VM Via vCenter:

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

2. Access Crosswork Data Gateway VM Via SSH:

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 in an IPv4 or IPv6 address format.

   For example,

   To log in as an administrator user: **ssh dg-admin@<ManagementNetworkIP>**

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

Note The SSH process is protected 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.

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

If you are unable to access the Cisco Crosswork Data Gateway VM, there is an issue with your network configuration settings. From the VMware 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.

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud by generating and exporting the enrollment package. See Obtain the Enrollment Package, on page 82.

Install Crosswork Data Gateway Via OVF Tool

You can modify mandatory or optional parameters in the command or script as per your requirement and run the OVF Tool (ovftool). See Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12.

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

Below is a sample script if you are planning to run the OVF Tool with a script. The sample that follows creates a Crosswork Data Gateway VM with the hostname of "dg-141" using two network interfaces.

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

# robot.ova path

DG_OVA_PATH="<mention the orchestrator path>"

VM_NAME="dg-141"
DM="thin"
Deployment="Crosswork-Cloud"

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

DNS="<DNS_ip_address>"
NTP="<NTP Server>"
Domain="cisco.com"
```

```
Description="Description for Cisco Crosswork Data Gatewayi : "dg-141""
Label="Label for Cisco Crosswork Data Gateway dg-141"

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

EnrollmentURI="<enrollment_package_URI>"
EnrollmentPassphrase="<password>"

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

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

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

ovftool --acceptAllEulas --X:injectOvfEnv --skipManifestCheck --overwrite --noSSLVerify
--powerOffTarget --powerOn \
--datastore="$DS" --diskMode="$DM" \
--name=$VM_NAME \
--net:"vNIC0=VM Network" \
--net:"vNIC1=DPortGroupVC-1" \
--deploymentOption=$Deployment \
--prop:"EnrollmentURI=$EnrollmentURI" \
--prop:"EnrollmentPassphrase=$EnrollmentPassphrase" \
--prop:"Hostname=$Hostname" \
--prop:"Description=$Description" \
--prop:"Label=$Label" \
--prop:"ActiveVnics=$ActiveVnics" \
--prop:"Vnic0IPv4Address=$Vnic0IPv4Address" \
--prop:"Vnic0IPv4Gateway=$Vnic0IPv4Gateway" \
--prop:"Vnic0IPv4Netmask=$Vnic0IPv4Netmask" \
--prop:"Vnic0IPv4Method=$Vnic0IPv4Method" \
--prop:"Vnic1IPv4Address=$Vnic1IPv4Address" \
--prop:"Vnic1IPv4Gateway=$Vnic1IPv4Gateway" \
--prop:"Vnic1IPv4Netmask=$Vnic1IPv4Netmask" \
--prop:"Vnic1IPv4Method=$Vnic1IPv4Method" \
--prop:"DNS=$DNS" \
--prop:"NTP=$NTP" \
--prop:"dg-adminPassword=$dg_adminPassword" \
--prop:"dg-operPassword=$dg_operPassword" \
--prop:"Domain=$Domain" $DG_OVA_PATH "vi://$VCENTER_LOGIN/$VCENTER_PATH"
```

Step 1 Open a command prompt on the machine where you want to install Crosswork Data Gateway.

Step 2 Open the template file and edit it to match the settings you chose for Crosswork Data Gateway.

Note The sample shell script includes only the mandatory options. If you want to customize the optional parameters in the OVF Tool command, see the Table 4: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 13 for information about these parameters.

Step 3 Navigate to the location where you installed the OVF Tool.

Step 4 Run the OVF Tool using the script.

```
root@cxcloudctrl:/opt# ./<script_file>
```

For example,

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

Verify that the installation was successful.

1. Log in to Crosswork Data Gateway VM Via vCenter:

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

2. Access Crosswork Data Gateway VM Via SSH:

1. From your workstation 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 in an IPv4 or IPv6 address format.

   For example,

   To log in as an administrator user: **ssh dg-admin@<ManagementNetworkIP>**

   To log in as operator user: **ssh dg-oper@<ManagementNetworkIP>**
2. Input the corresponding password (the one that you created during installation process) and press **Enter**.

Note 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.

If you are unable to access the Cisco Crosswork Data Gateway VM, there is an issue with your network configuration settings. From the VMware 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.

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud. See Obtain the Enrollment Package, on page 82.

Install Crosswork Data Gateway on OpenStack Platform

You can install the Crosswork Data Gateway on OpenStack Platform in one of the following ways:

Install Crosswork Data Gateway on OpenStack from OpenStack CLI

This section provides details of the procedure to install Crosswork Data Gateway on the OpenStack platform.

Note

1. This procedure lists commands to create networks, ports, and volumes in the OpenStack environment. Please note that there are multiple ways to do this.
2. All IP addresses mentioned here are sample IP addresses mentioned for the purpose of documentation.

Before you begin

Ensure you have the following information ready:

- Number of Crosswork Data Gateway VM instances to install.
- Plan your installation. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12.
- Decide the addressing method that you will use (DHCP or Static) for one or more VMs.
- Have network information such as IP addresses, subnets, and ports ready for each VM if you are using Static addressing.
- Understand security group rules and policies before you create and use them.

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

a) Download the latest available Cisco Crosswork Data Gateway image (*.bios.signed.bin) from cisco.com to your local machine or a location on your local network that is accessible to your OpenStack. For the purpose of these instructions, we use the package name **"cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin"**.

b) Extract the content of the bin file to the current directory by running the following command.

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
```

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

```
CDG-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
README
cisco_x509_verify_release.py
cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz.signature
```

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

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

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

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

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

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

d) Unzip the QCOW2 file (**cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz**) with the following command:

```
tar -xvf cw-na-dg-4.0.1-65-release-20221130.uefi.tar.gz
```

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

Step 2 Complete the steps in Step 3 **OR** Step 4 based on the type of addressing you will be using for the Crosswork Data Gateway VM.

Step 3 **Update the `config.txt` for a Crosswork Data Gateway VM with Static addressing.**

a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.

b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 for more information.

This is a sample `config.txt` file for a 1 NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
```

```
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
 role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from the
 Default Gateway role
NTP=changeme

#### Optional Parameters
```

```
### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple DG
 instances
Label=

## 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
# Default value: Yes
AllowRFC8190=Yes

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

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
```

```
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from the
 Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted cetificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from the
 Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60
```

```
### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved using
 SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS certificate
 file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package using
 SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters  - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
```

```
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.

d) **(Important)** Make a note of the IP address that you enter here for the vNIC IP addresses in the `config.text`. You will need to specifiy the same IP addresses when creating the ports for the VM in Step 9.

e) Repeat **Step 3 (b)** and **Step 3 (d)** to update and save a unique config.txt file for each VM using static addressing.

f) Proceed to **Step 5**.

Step 4 **Update the `config.txt` for Crosswork Data Gateway VMs using DHCP.**

a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.

b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 for more information.

This is a sample `config.txt` file for a 1 NIC deployment with the host name as `cdg1-nodhcp` when using DHCP. Mandatory parameters in this list have been highlighted.

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme
```

```
## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers
```

```
## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
 role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from the
 Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple DG
 instances
Label=

## 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
# Default value: Yes
AllowRFC8190=Yes

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

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False
```

```
## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from the
 Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted cetificate file
```

```
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from the
 Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved using
 SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS certificate
 file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package using
 SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters  - Do not change this section

### Deployment Settings

## Deployment Type
```

```
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.

d) Repeat **Step 4 (b)** and **Step 4 (c)** to update and save a unique config.txt file for each VM using DHCP addressing.

e) Proceed to **Step 5**.

Step 5 Log in to the OpenStack VM from CLI.

Step 6 **Create the resource profile or flavor for the VMs.**

```
openstack flavor create --public --id auto --vcpus 8 --ram 32768 --disk 74 cdg-cloud
```

Step 7 **Create image for OpenStack install.**

```
openstack image create --public --disk-format qcow2 --container-format bare --file
<bios_release_image_file> <image_name>
```

For example:

```
openstack image create --public --disk-format qcow2 --container-format bare --file
cw-na-dg-4.0.1-65-release-20221130.bios.qcow2 cdg-cloud-bios
```

Step 8 **Create the VM-specific parameters for each Crosswork Data Gateway VM.**

Create the following parameters for each Crosswork Data Gateway VM instance that you want to install.

a) **(Optional) Create a 24 GB second data disk.**

```
openstack volume create --size
```

Sample commands:

```
openstack volume create --size 24 cdg-vol1
```

b) **Create a security policy to allow incoming TCP/UDP/ICMP connections.**

OpenStack does not allow incoming TCP/UDP/ICMP connections by default. Create a security policy to allow incoming connections from TCP/UDP/ICMP protocols.

```
openstack security group create open
openstack security group rule create open --protocol tcp --dst-port <port_number> --remote-ip
<IP_address>
openstack security group rule create open --protocol udp --dst-port <port_number> --remote-ip
<IP_address>
openstack security group rule create --protocol icmp open
```

c) **Create ports with specified IP address ONLY for Crosswork Data VMs using Static addressing.**

Important This step is required only if you are using Static addressing. If you are using DHCP addressing, the IP addresses for the ports are automatically assigned from the IP addresses allocation pool for the subnet.

```
openstack port create --network network_name --fixed-ip
subnet=subnet_name,ip-address=port_ip_address port_name
```

Sample commands to create ports for CDG VMs with 1 NICs using static addressing:

```
openstack port create --network network1 --fixed-ip subnet=subnet1,ip-address=10.10.11.101
mgmt-port1
```

In the previous command, `network1` is the management network in your environment, `subnet1` is the subnet on the management network, `mgmt-port1` is the port that we are creating with the IP address as `10.10.11.101` for vNIC0 as specified in the `config.txt` file for the VM.

d) **Apply the security policy to the ports.**

```
openstack port set <port_name> --security-group open
```

For example,

```
openstack port set mgmt-port1 --security-group open
```

e) Repeat Step **9** for all the VMs you will be installing.

Step 9 **Install the Crosswork Data Gateway VM(s).**

Commands to install Crosswork Data Gateway VM with 1 NIC that uses static addressing

```
openstack server create --flavor <flavor_name> --image <image_name> --port <mgmt-port>
--config-drive True --user-data <config.txt> --block-device-mapping
vdb=<volume_name>:::true <CDG_hostname>
```

For example:

```
openstack server create --flavor cdg-cloud --image cdg-cloud-bios --port mgmt-port1
--config-drive True --user-data config-nodhcp-cdg1.txt --block-device-mapping
vdb=cdg1:::true cdg1-nodhcp
```

OR

```
openstack server create --config-drive true --flavor cdg --image <image_name> --key-name default
--nic net-id=<network id>,v4-fixed-ip=<CDG static IP> --security-group <security group name> --user-data
<config.txt> <CDG_hostname>
```

Commands to install Crosswork Data Gateway VM with 1 NIC with DHCP

```
openstack server create --flavor <flavor_name> --image <image_name> --network <network1> --network
<network2> --network <network3> --config-drive True --user-data <config.txt> --host <boot_drive>
--block-device-mapping vdb=<volume_name>:::true <CDG_hostname>
```

For example:

```
openstack server create --flavor <flavor_name> --image <image_name> --network <network1>
--config-drive True --user-data <config.txt> --host <boot_drive>
--block-device-mapping vdb=<volume_name>:::true <CDG_hostname>
```

OR

```
openstack server create --config-drive true --flavor cdg --image --key-name default --network
--security-group --user-data
```

Note The number of networks in the command to install the VMs depends on the number of NICs in the deployment.

For example, the command to install a VM with 2 NICs is:

```
openstack server create --flavor cdg-cloud --image cdg-cloud-bios --port mgmt-port2 --port
south-port2 --config-drive True --user-data config-nodhcp_2nic.txt --block-device-mapping
vdb=cdg-vol:::true cdg-bios-nodhcp_2NIC
```

Verify that the Crosswork Data Gateway VMs were installed successfully.

Run the following command to view the status of the installation of the VMs.

```
openstack server list
```

```
(osp16VTS) [stack@ospd16-director cdg-image]$ openstack server list
+--------------------------------------+----------------------+--------+-----------------------------------------------------------------------------------------+----------------------+-----------+
| ID                                   | Name                 | Status | Networks                                                                                | Image                | Flavor    |
+--------------------------------------+----------------------+--------+-----------------------------------------------------------------------------------------+----------------------+-----------+
| 8b039d3c-1bb9-4ce2-9b24-1654216c4dd6 | cdg-bios-nodhcp_2NIC | ACTIVE | network1-nodhcp=[redacted]; network3-nodhcp=[redacted]                                  | cdg-cloud-bios-345 | cdg-cloud |
| 9c6d913f-c24b-43a3-9816-f865e58e7e95 | cdg-bios-nodhcp      | ACTIVE | network1-nodhcp=[redacted]; network2-nodhcp=[redacted]; network3-nodhcp=[redacted]      | cdg-cloud-bios-345 | cdg-cloud |
+--------------------------------------+----------------------+--------+-----------------------------------------------------------------------------------------+----------------------+-----------+
```

After the status of the VMs is displayed as **Active**, wait for about 10 minutes, and check if the VM was deployed properly and running as expected either from the CLI or the OpenStack UI.

From OpenStack CLI

1. Run the following command in the OpenStack CLI to fetch the URL of the VM instance.

   ```
   openstack console url show <CDG hostname>
   ```

   For example:

   ```
   openstack console url show cdg-dhcp
   ```

2. Log in as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the `config.txt` file of the VM. The Crosswork Data Gateway Interactive console is displayed after you log in successfully.

From OpenStack UI

1. Log in to the OpenStack UI.
2. Navigate to **Compute** > **Instances**.
3. Click the Crosswork Data Gateway VM name. The link to the VM console opens in a new tab.
4. Log in as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the `config.txt` file of the VM. The Crosswork Data Gateway interactive console is displayed after you log in successfully.

What to do next

Proceed to adding the Crosswork Data Gateway with Crosswork Cloud. See Obtain the Enrollment Package, on page 82.

Install Crosswork Data Gateway on OpenStack from the OpenStack UI

This section provides details of the procedure to install Crosswork Data Gateway on the OpenStack platform.

Note All IP addresses mentioned here are sample IP addresses mentioned for the purpose of documentation.

Before you begin

Ensure you have the following information ready:

- Number of Crosswork Data Gateway VM instances to install.
- Plan your installation. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12.
- Decide the addressing method that you will use (DHCP or Static) for one or more VMs.
- Have network information such as IP addresses, subnets, and ports ready for each VM if you are using Static addressing.
- Understand security group rules and security policies before you create security groups to apply to the VM.

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

a) Download the latest available Cisco Crosswork Data Gateway image (*.bios.signed.bin) from cisco.com to your local machine or a location on your local network that is accessible to your OpenStack. In these instructions, we use the package name **"cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin"**.

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

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
```

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

```
CDG-CCO_RELEASE.cer
cisco_x509_verify_release.py3
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
README
cisco_x509_verify_release.py
cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin
cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz.signature
```

If you encounter any network connectivity issues, skip this verification and perform a manual verification as explained in the next step.

```
sh cw-na-dg-4.0.1-65-release-20221130.bios.signed.bin --skip-verification
```

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

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

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

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

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

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

d) Unzip the QCOW2 file (**cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz**) with the following command:

```
tar -xvf cw-na-dg-4.0.1-65-release-20221130.bios.tar.gz
```

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

Step 2 Complete the steps in Step 3 **OR** Step 4 based on the type of addressing you will be using for the Crosswork Data Gateway VM.

Step 3 **Update the `config.txt` for a Crosswork Data Gateway VM with Static addressing.**

a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.

b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 for more information.

Important Make a note of the IP address that you are using to create the ports for the VM. You will need to specify the same IP addresses that you enter here for the vNIC IP addresses in the `config.text` file for each of the VMs.

This is a sample `config.txt` file for a 1 NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud
```

```
### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False
```

```
## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
 role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from
the Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple
 DG instances
Label=

## 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
# Default value: Yes
AllowRFC8190=Yes

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

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
 using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False
```

```
## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
 list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from
the Default Gateway role
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
```

```
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted cetificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from
the Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
 the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved
using SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File
 URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS
certificate file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package
using SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
```

```
EnrollmentPassphrase=

#### Static Parameters  - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.

d) **(Important)** Make a note of the IP address that you enter here for the vNIC IP addresses in the `config.txt`. You will need to specify the same IP addresses when creating the ports for the VM in Step 9.

e) Repeat **Step 3 (b)** and **Step 3 (d)** to update and save a unique `config.txt` file for each VM using static addressing.
f) Proceed to **Step 5**.

Step 4 **Update the `config.txt` for a Crosswork Data Gateway VM with DHCP.**

a) Navigate to the directory where you have downloaded the Crosswork Data Gateway release image.
b) Open the `config.txt` file and modify the parameters as per your installation requirements. Refer to the section Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 for more information.

This is a sample `config.txt` file for a 1 NIC deployment with the host name as `cdg1-nodhcp` when using static addressing. Mandatory parameters in this list have been highlighted.

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False

## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
```

```
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
 role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from
the Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple
 DG instances
Label=

## 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
# Default value: Yes
AllowRFC8190=Yes

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

```
## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
 using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
 list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from
the Default Gateway role
SyslogAddress=
```

```
## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted cetificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from
the Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
 the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=
```

```
## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved
using SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File
 URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS
certificate file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package
using SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters  - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
NicControl=eth0
```

```
## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

c) Save the `config.txt` file with the hostname of the VM or a name that makes it easy for you to identify the VM for which you have updated it.

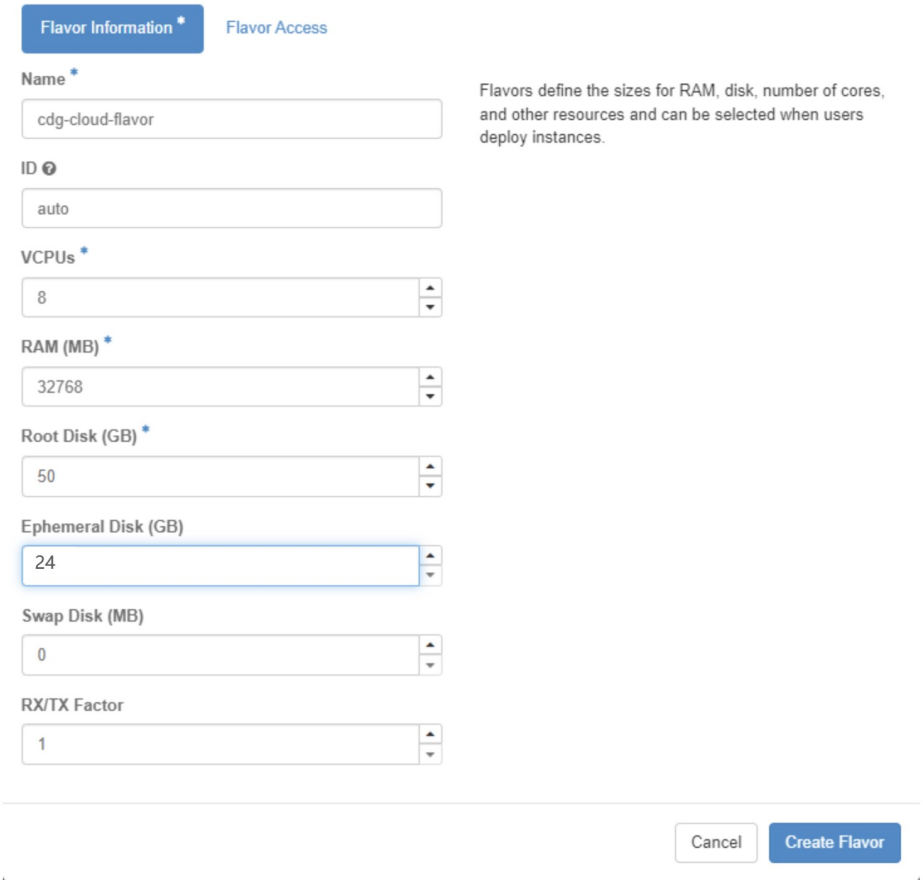
d) Repeat **Step 4 (b)** and **Step 4 (c)** to update and save a unique `config.txt` file for each VM using static addressing.

e) Proceed to **Step 5**.

Step 5 Log in to the OpenStack VM from the OpenStack UI.

Step 6 Navigate to **Compute** > **Flavors** to create the resource profile or flavor.

Enter details in the **Name**, **VCPUs**, **RAM**, **Root Disk** and **Ephemeral Disk** fields as shown in the following image and click **Create Flavor**.

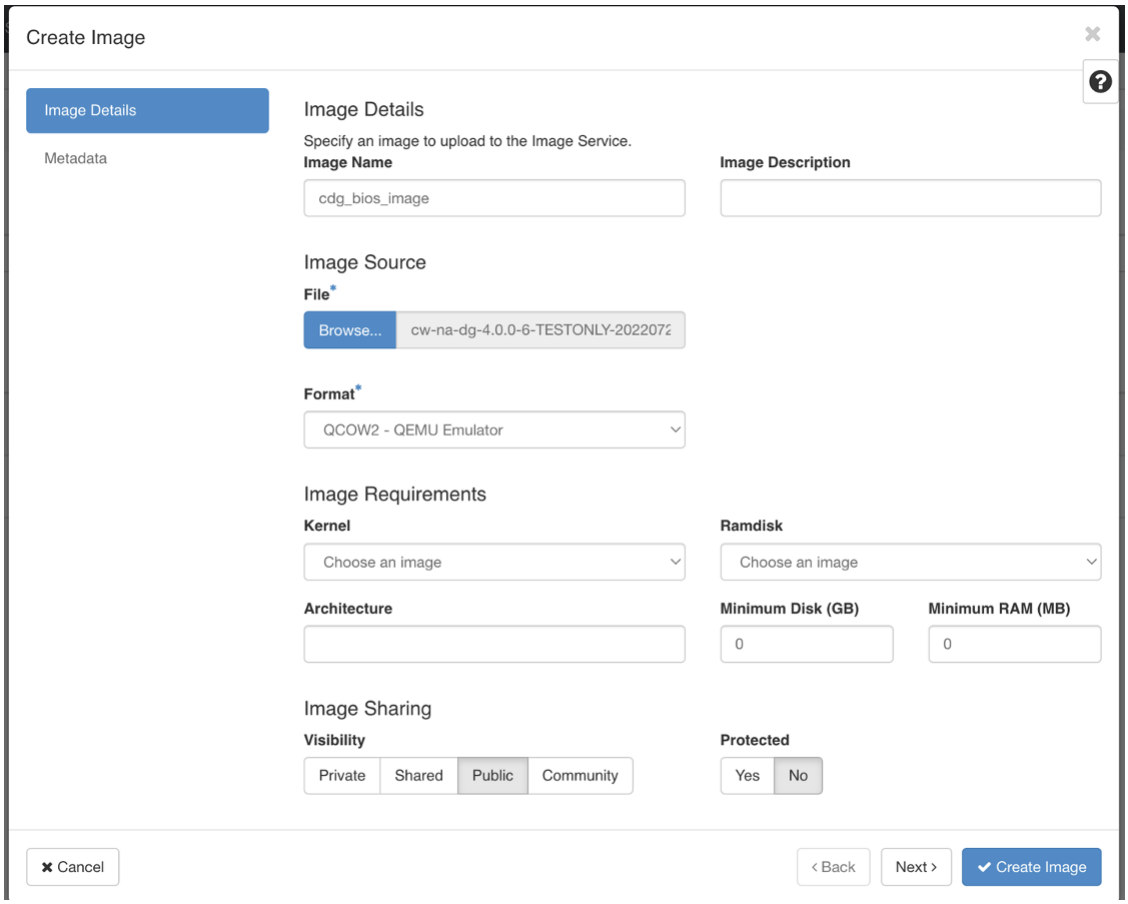


Step 7 **Create an image for OpenStack install.**

a) Enter details in the following fields:

1. **Image Name** - Specify a name for the image you are creating.
2. **File** - Navigate to the directory where you have downloaded the Crosswork Data Gateway release image and select the image.
3. **Format** - Select **QCOW2 - QEMU Emulator** from the drop-down list.
4. Leave the other settings to the values as shown in the image.

b) Click **Create Image**.



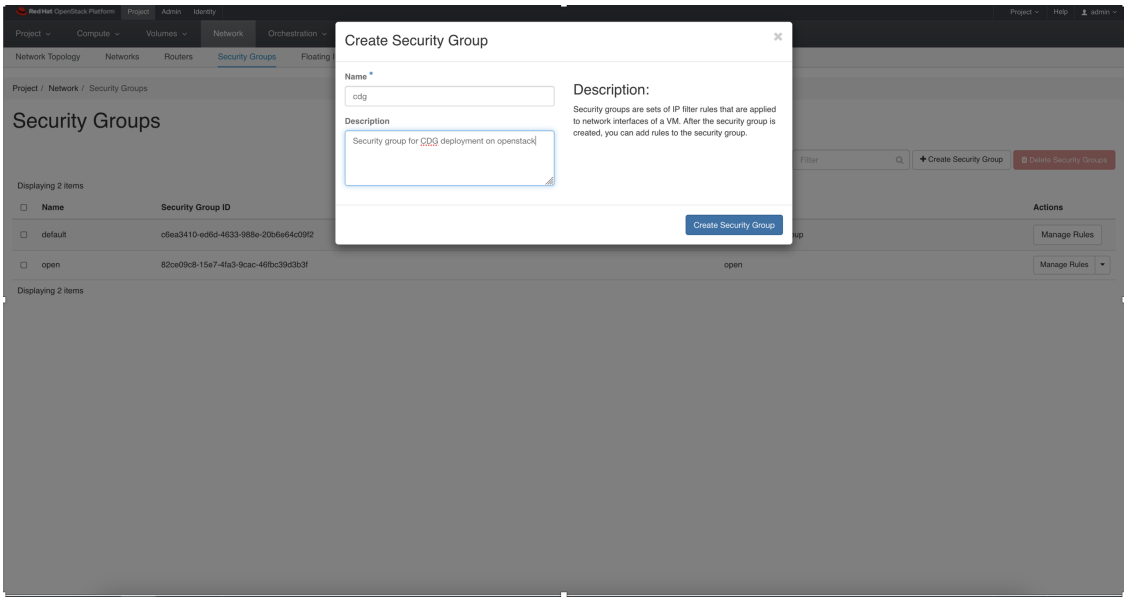
Step 8 **Create a security group policy to allow incoming TCP/UDP/ICMP connections.**

OpenStack does not allow incoming TCP/UDP/ICMP connections by default. Create a security policy to allow incoming connections from TCP/UDP/ICMP protocols.

Note You can create security groups and apply them to the VM even after the Crosswork Data Gateway is deployed.

a) In the OpenStack UI, navigate to **Networks** > **Security Groups.**.

b) Click **+ Create Security Group**.



c) Specify the **Name** and **Description** of the security group. Click **Create Security Group**.

d) In the new window that appears to create security rules, click **Add Rule** to create a security policy for each protocol by specifying the direction, port range and the IP addresses range.

The security group contains two rules by default. Use the **Delete Rule** option to delete these rules.

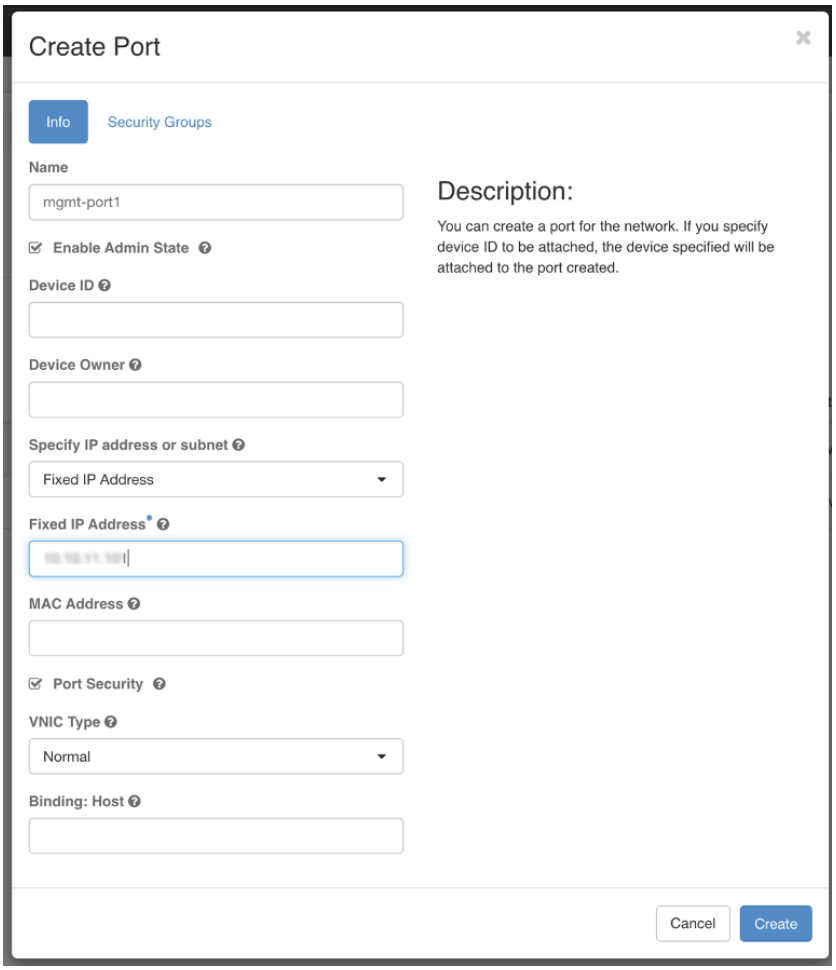
Step 9 **Create ports with specified IP address ONLY if you are using Static addressing.**

Important This step is required only if you are using Static addressing. If you are using DHCP addressing, the IP addresses for the ports are automatically assigned from the IP addresses allocation pool for the subnet.

a) In the OpenStack UI, navigate to **Network** > **Networks**.

b) Depending on the number of NICs in your deployment, (starting with the management network), select a network and click **+ Create Ports**.

c) Enter details in the **Name** and **Fixed IP Address** fields. Select the **Enable Admin State** and **Port Security** check box.

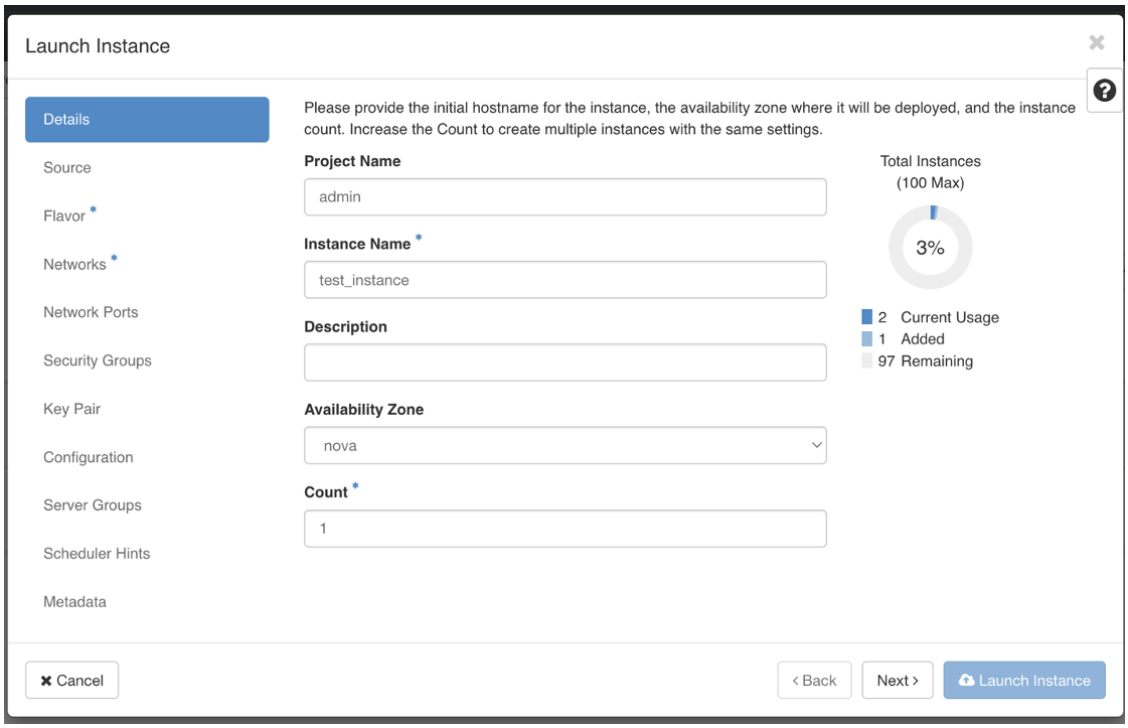


Step 10 Navigate to **Compute** > **Instances**. Click **Launch Instance** in this page.

A **Launch Instance** window appears to start the VM installation.

Step 11 In the **Details** tab, specify the VM name in the **Instance Name** field and the **Count** as 1. Click **Next**.

Note For larger systems it is likely that you will have more than one Cisco Crosswork Data Gateway VM. The Cisco Crosswork Data Gateway name should, therefore, be unique and created in a way that makes identifying a specific VM easy. We recommend that you enter the same name you had specified in the `Hostname` parameter in the `config.txt` file for the VM.



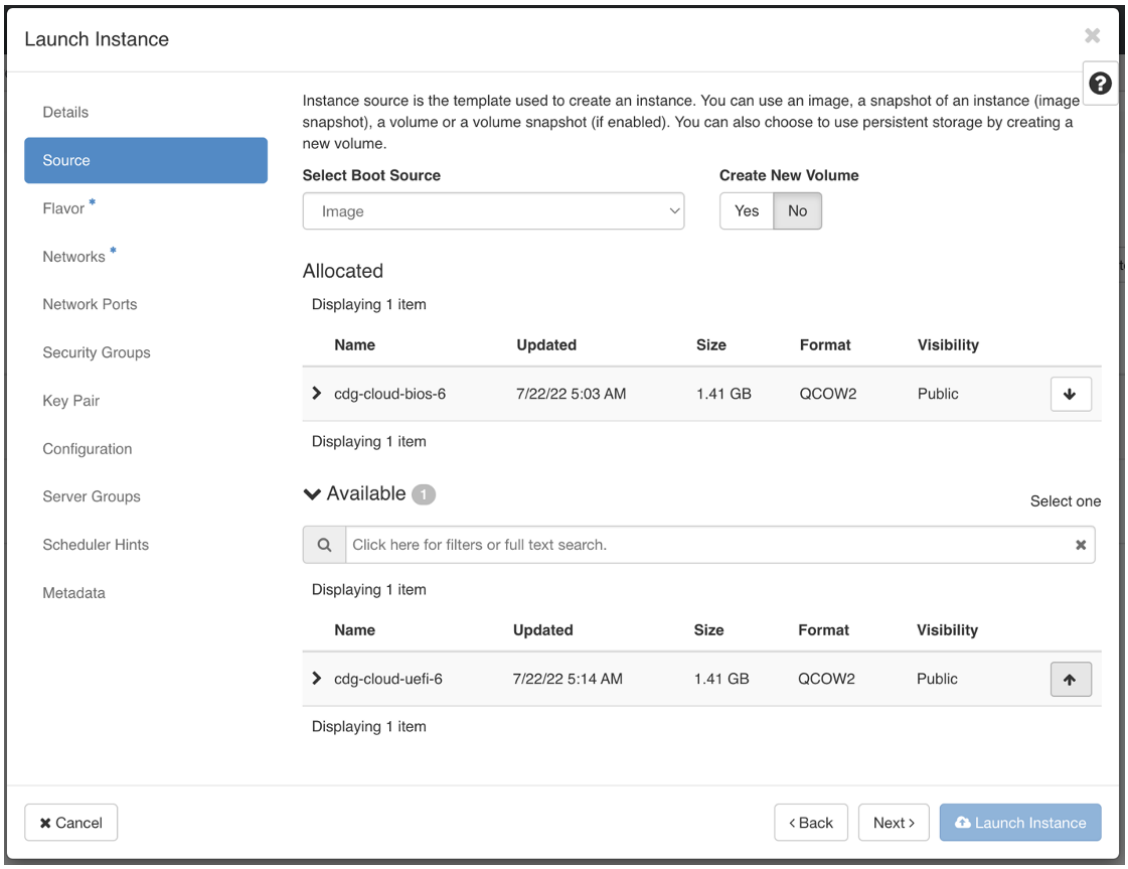
Step 12 In the **Source** tab:

a. **Select Boot Source** - Select **Image** from the drop-down list.

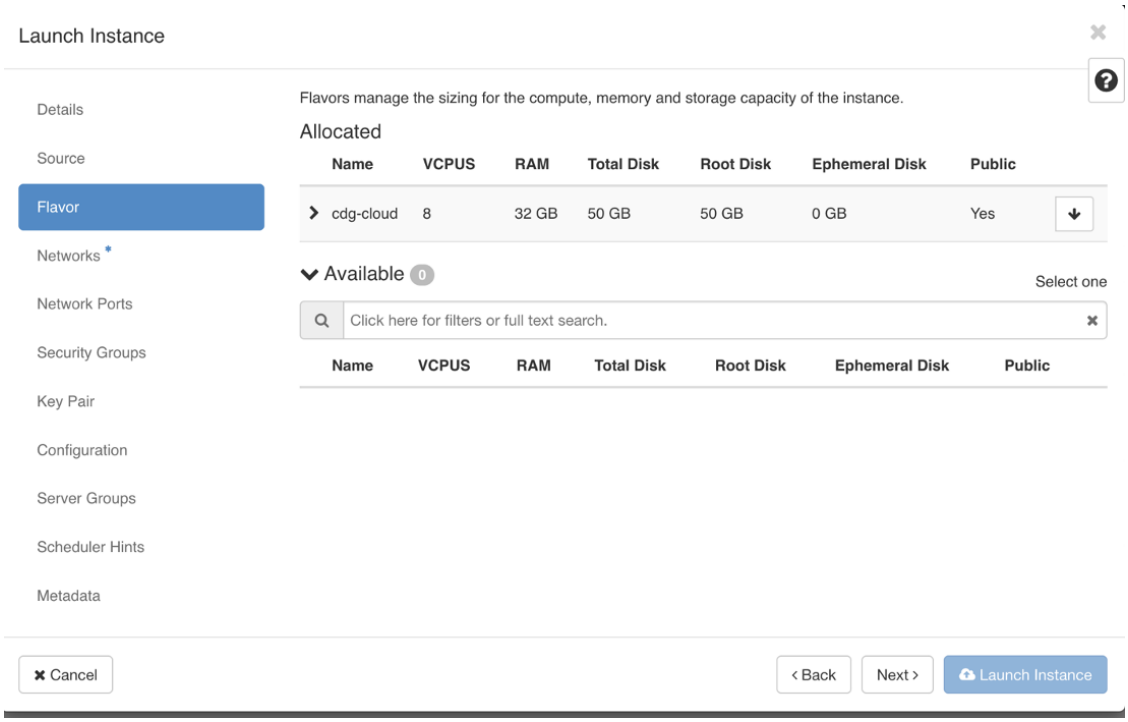
b. **Create New Volume** - Select **No**.

c. All images available in the OpenStack environment are listed under the **Available** pane. Click  to select the image. Doing this will now move the image to the **Allocated** pane indicating that you have selected the image.

d. Click **Next**.

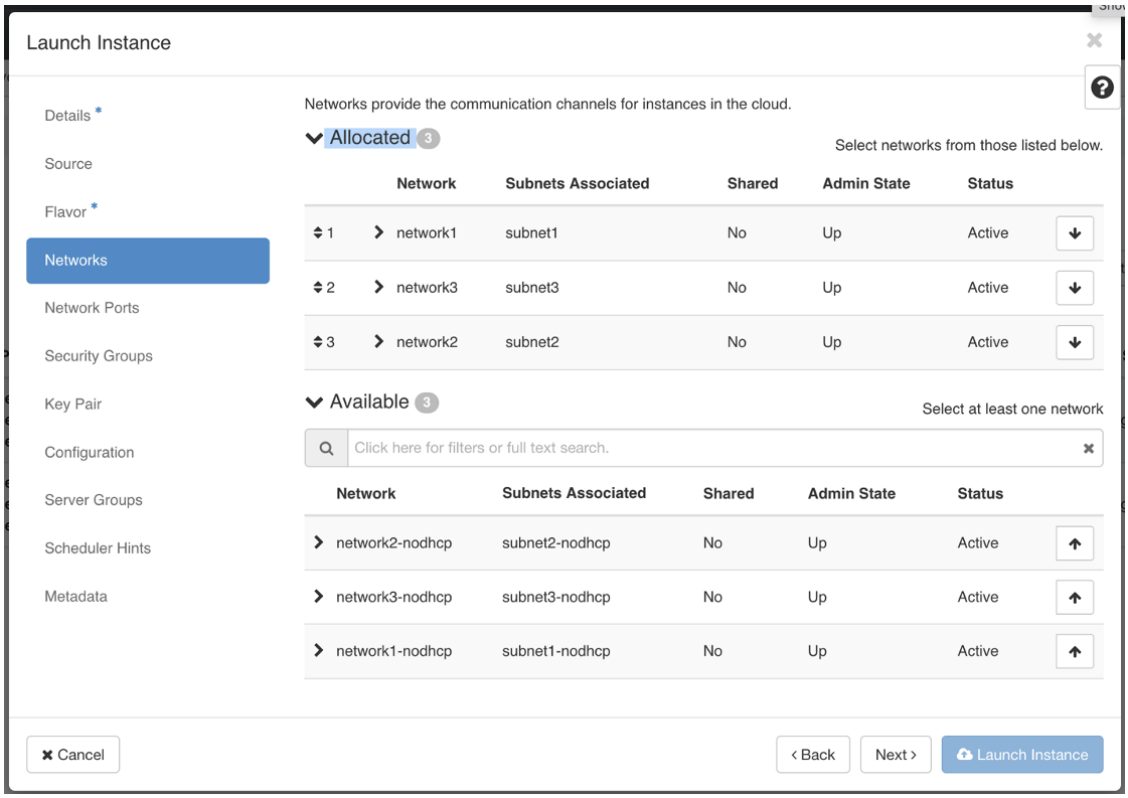


Step 13 In the **Flavor** tab, in the **Available** pane, for the flavor you want to select for the VM, click  to move it from the **Available** pane to the **Allocated** pane. Click **Next**.



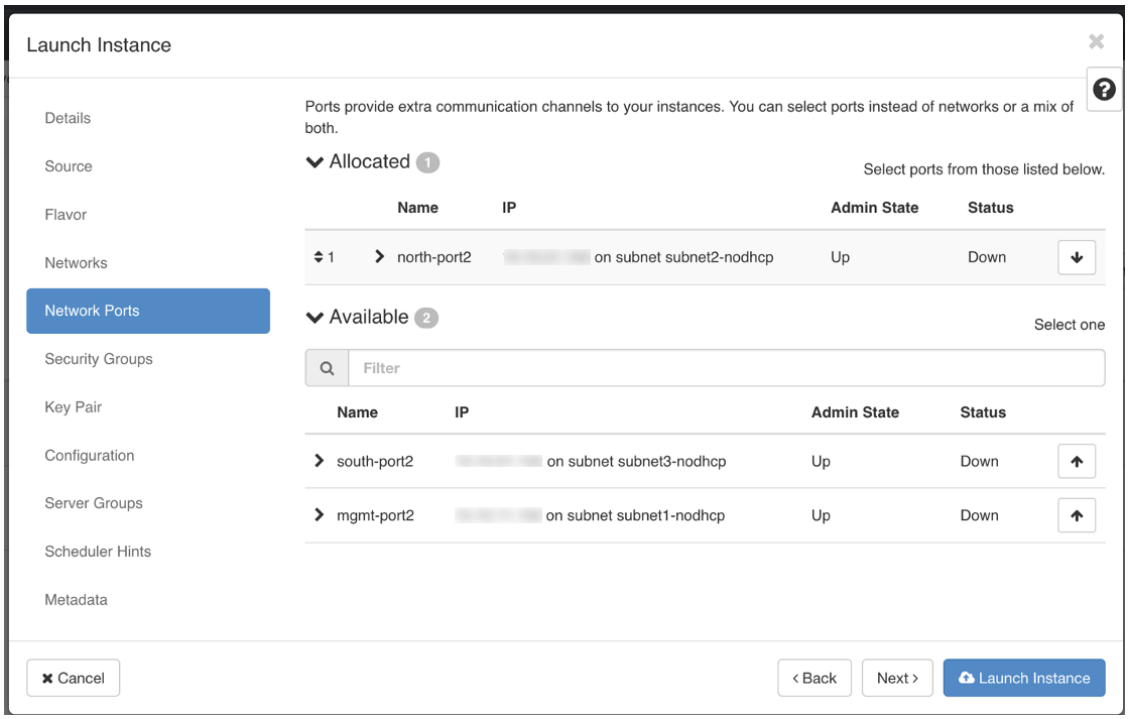
Step 14 Assign networks to the VM. Depending on the number of vNICs in your deployment, select up to 3 networks for the VM by clicking  for each network from the list of networks in the **Available** pane. Doing this moves the selected networks to the **Allocated** pane. Click **Next**.

Important The order in which you select the networks is important. In a 3-NIC deployment, the first network you select will be assigned to the vNIC0 interface, the second to the vNIC1 interface and the third to the vNIC2 interface.



Step 15 Assign ports to the VM.

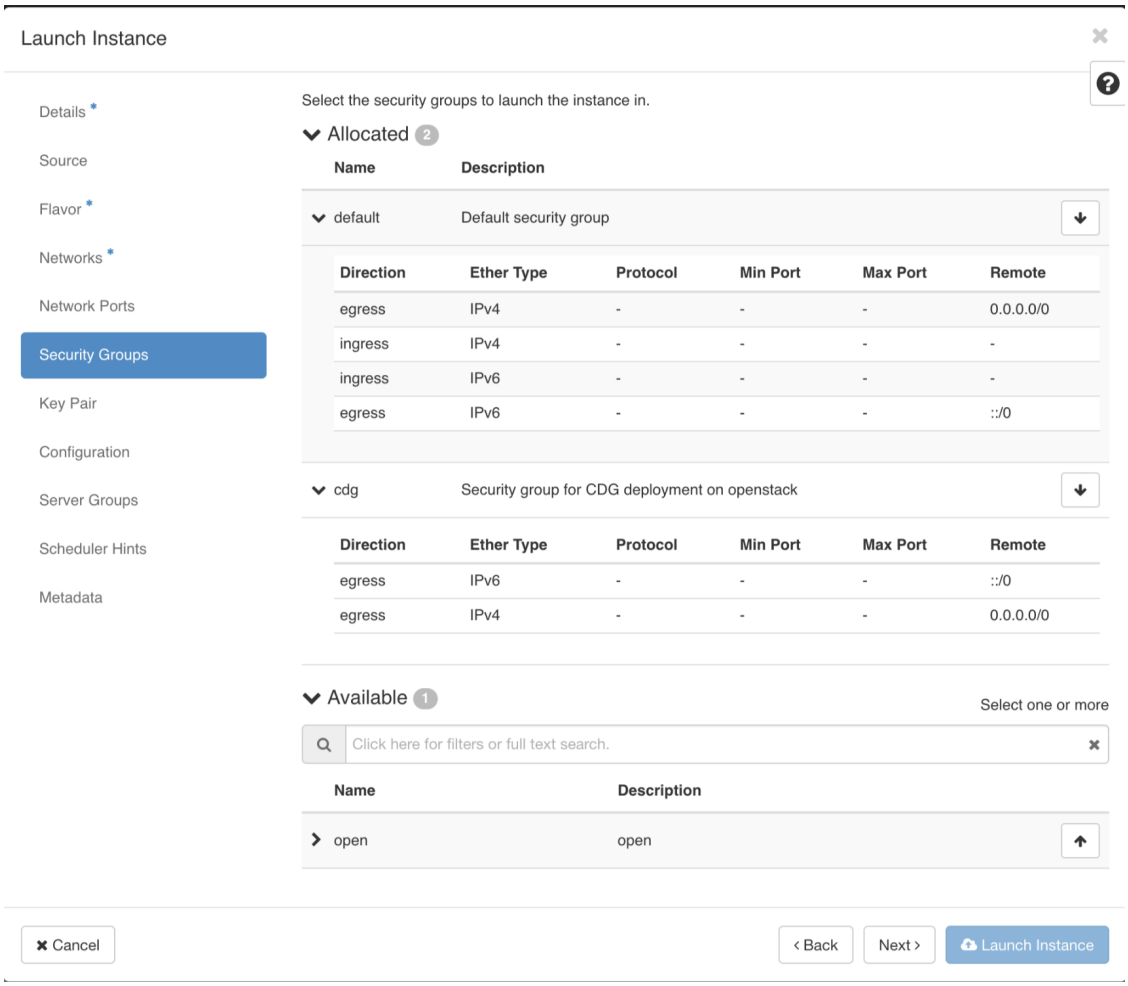
From the list of ports that are displayed in the **Available** pane, click  to move the port to the **Allocated** pane. .



Click **Next**.

Step 16 Assign **Security Groups** to the VM by moving the security groups you wish to apply to the VM from the **Available** pane to the **Allocated** pane. .

In the following image, 2 security groups - default and cdg, are applied to the VM.

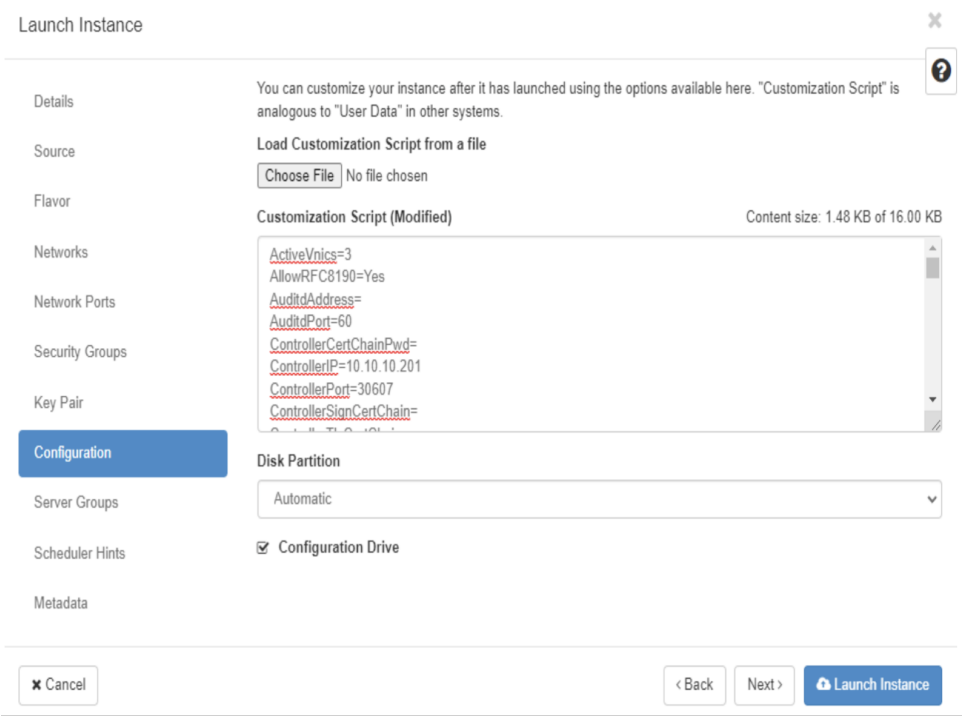


Click **Next**.

Step 17 In the **Key Pair** tab, click **Next**.

Step 18 In the **Configuration** tab:

- Click **Choose File** to select and upload the `config.txt` file you had modified and saved for the VM.
- Select the **Configuration Drive** check box.



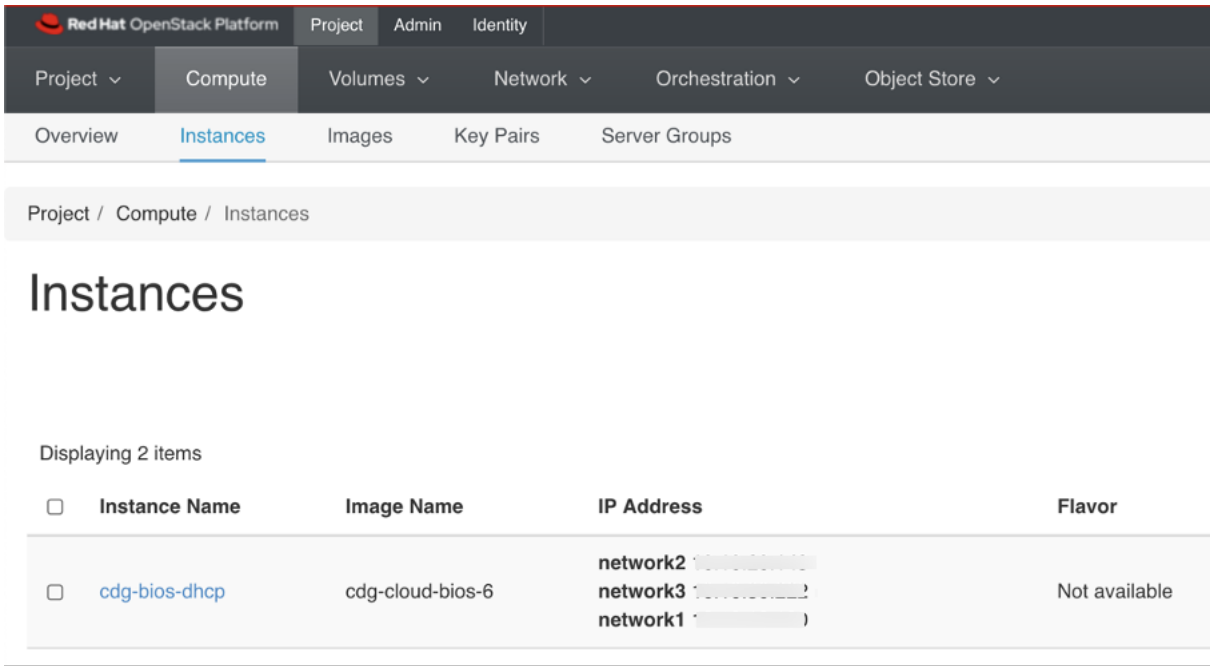
Step 19 Click **Launch Instance**.

OpenStack begins installation of the VM.

Step 20 Repeat **Step 9** to **Step 20** of the procedure to install all Crosswork Data Gateway VMs.

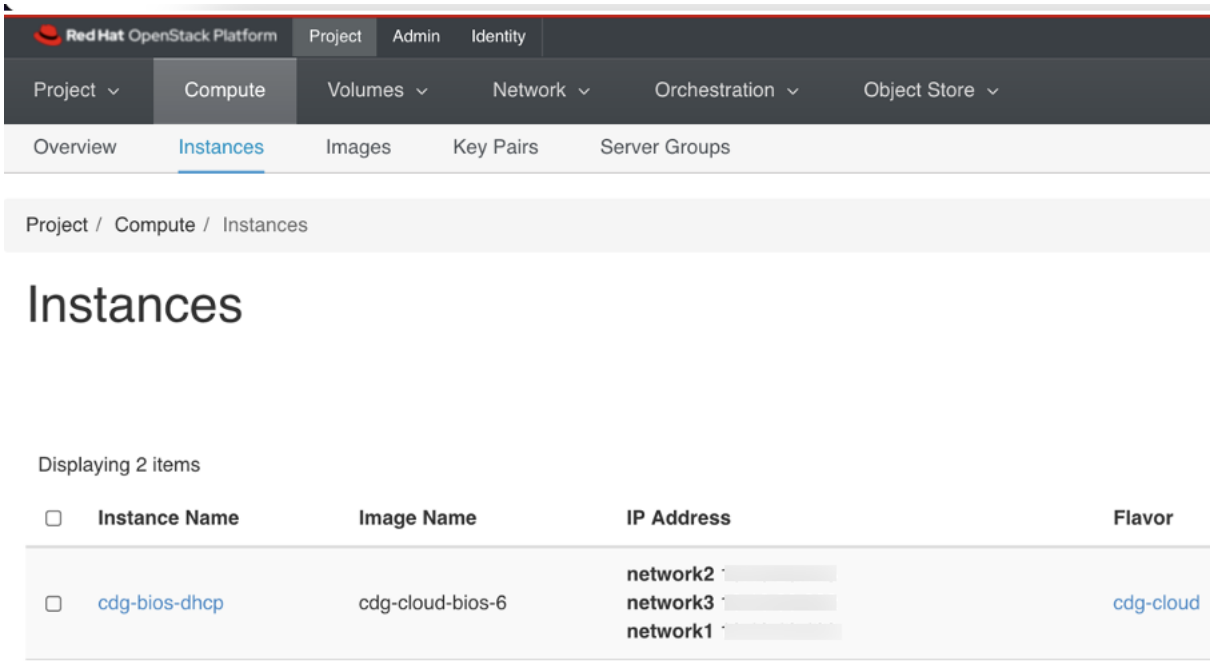
Verify that the Crosswork Data Gateway VMs were installed successfully.

1. In the OpenStack UI, navigate to **Compute** > **Instances**.
2. The list of Crosswork Data Gateway VMs that are installed and being installed is displayed here.



A Crosswork Data Gateway VM that is being installed will have the **Status** as **Build**, **Task** as **Spawning** and **Power State** as **No State**.

3. Once the VM is successfully installed, the **Status** changes to **Active**, **Task** is **None** and **Power State** as **Running**.



4. After the Status changes to **Active**, wait for about 10 minutes.

   Click the Crosswork Data Gateway VM name. The link to the VM console opens.

5. Log in as the dg-admin or dg-oper user (as per the role assigned to you) and the corresponding password you had entered in the `config.txt` file of the VM. The Interactive console of the Crosswork Data Gateway is displayed after you login successfully.

What to do next

Proceed to enrolling the Crosswork Data Gateway with Crosswork Cloud by generating and exporting the enrollment package. See Export Enrollment Package, on page 82.

Install Crosswork Data Gateway on Amazon EC2

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

- Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template, on page 72
- Install Crosswork Data Gateway on Amazon EC2 Manually, on page 73

Install Crosswork Data Gateway on Amazon EC2 using CloudFormation Template

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

Before you begin

- Ensure that you have met the requirements specified in the section Amazon EC2 Settings, on page 8.
- All the Cisco Crosswork VMs have been installed.

Step 1 Log in to AWS and search for the CloudFormation service. The CloudFormation dashboard opens.

Step 2 Click **Stacks** from the side menu.

All existing stacks in the environment are displayed here.

Step 3 In **Step 1 - Specify template**, select the following settings:

a) Under **Prepare template**, select **Template is ready**.
b) Under **Template source**, select **Upload a template file**.
c) Click **Choose file**, and select your CF template (.yaml file).
d) Click **Next**.

Step 4 In **Step 2 - Specify stack details**, enter relevant values for the stack name and each parameter field, and click **Next**.

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

Step 5 In **Step 3 - Configure stack options**, enter the relevant values for the settings based on your production preferences. Click **Next** to continue.

Step 6 In **Step 4 - Review**, review the settings you have configured.

Step 7 Select the acknowledgment checkbox, and click **Create stack** to start the VM installation.

Verify that the VMs were installed successfully

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

   The status of the stack in the **Events** tab will be **CREATE_IN_PROGRESS**
3. After the stack has been created:
   - The status of the stack changes to **CREATE_COMPLETE** and the **Logical ID** displays the stack name.
   - The **Resources** tab displays details of the all the resources that the CF template has created, including the physical IDs.
   - The **Output** tab has details of the VM's interface IP addresses.
4. Click the **Physical ID** of the VM instance in your stack.

   Doing this will open the Instances window in the EC2 dashboard with details of the selected VM instance.
5. Click **Connect** (top right corner).
6. In the **Connect to instance** window that appears, click the **EC2 Serial Control** tab and click **Connect**.
7. Click on the **EC2 serial console** tab. Click **Connect** to connect to the console of the VM.
8. Log in to the VM as a `dg-admin` or `dg-oper` user using the password you configured.

   The Interactive Console of the VM is displayed on successful login.

Install Crosswork Data Gateway on Amazon EC2 Manually

Follow these steps to install Crosswork Data Gateway on EC2.

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

Before you begin

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

- Ensure that you have met the requirements specified in Amazon EC2 Settings, on page 8.
- All the Cisco Crosswork VMs are installed.
- Decide the number of Crosswork Data Gateway VM instances to install.

- Have the Crosswork Data Gateway AMI image saved in a location accessible to your AWS.

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

a) Prepare the user data for Crosswork Data Gateway VMs. See Cisco Crosswork Data Gateway Deployment Parameters and Scenarios, on page 12 for more information about the parameters. Sample user data for a VM is attached here for your reference. Important parameters have been highlighted.

For Amazon EC2 deployment, this document assumes that a user of this procedure is familiar with AWS and the CloudFormation concepts, and as such, the CF template creation is out of the scope of this document. In the example, AwsIamRole is an optional parameter for the Amazon EC2 deployment.

```
#### Required Parameters

### Deployment Settings

## Resource Profile
# How much memory and disk should be allocated?
# Default value: Crosswork-Cloud
Profile=Crosswork-Cloud

### Host Information

## Hostname
# Please enter the server's hostname (dg.localdomain)
Hostname=changeme

## Description
# Please enter a short, user friendly description for display in the Crosswork Controller
Description=changeme

### Passphrases

## dg-admin Passphrase
# Please enter a passphrase for the dg-admin user. It must be at least 8 characters.
dg-adminPassword=changeme

## dg-oper Passphrase
# Please enter a passphrase for the dg-oper user. It must be at least 8 characters.
dg-operPassword=changeme

### vNIC0 IPv4 Address

## vNIC0 IPv4 Method
# Skip or statically assign the vNIC0 IPv4 address
# Default value: DHCP
Vnic0IPv4Method=None

## vNIC0 IPv4 Address
# Please enter the server's IPv4 vNIC0 address if statically assigned
Vnic0IPv4Address=0.0.0.0

## vNIC0 IPv4 Netmask
# Please enter the server's IPv4 vNIC0 netmask if statically assigned
Vnic0IPv4Netmask=0.0.0.0

## vNIC0 IPv4 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv4SkipGateway=False
```

```
## vNIC0 IPv4 Gateway
# Please enter the server's IPv4 vNIC0 gateway if statically assigned
Vnic0IPv4Gateway=0.0.0.1

### vNIC0 IPv6 Address

## vNIC0 IPv6 Method
# Skip or statically assign the vNIC0 IPv6 address
# Default value: None
Vnic0IPv6Method=None

## vNIC0 IPv6 Address
# Please enter the server's IPv6 vNIC0 address if statically assigned
Vnic0IPv6Address=::0

## vNIC0 IPv6 Netmask
# Please enter the server's IPv6 vNIC0 netmask if statically assigned
Vnic0IPv6Netmask=64

## vNIC0 IPv6 Skip Gateway
# Skip statically assigning a gateway address to communicate with other devices, VMs, or services
# Default value: False
Vnic0IPv6SkipGateway=False

## vNIC0 IPv6 Gateway
# Please enter the server's IPv6 vNIC0 gateway if statically assigned
Vnic0IPv6Gateway=::1

### DNS Servers

## DNS Address
# Please enter a space delimited list of DNS server addresses accessible from the Default Gateway
 role
DNS=changeme

## DNS Search Domain
# Please enter the DNS search domain
Domain=changeme

### NTPv4 Servers

## NTPv4 Servers
# Please enter a space delimited list of NTPv4 server hostnames or addresses accessible from the
 Default Gateway role
NTP=changeme

#### Optional Parameters

### Host Information

## Label
# An optional freeform label used by the Crosswork Controller to categorize and group multiple DG
 instances
Label=

## 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
# Default value: Yes
AllowRFC8190=Yes

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

```
DGCertKey=

## Crosswork Data Gateway Certificate File URI
# Please enter the optional Crosswork Data Gateway PEM formatted certificate file URI retrieved
using SCP (user@host:/path/to/file)
DGCertChain=

## Crosswork Data Gateway Certificate File and Key Passphrase
# Please enter the SCP user passphrase to retrieve the Crosswork Data Gateway PEM formatted
certificate file and private key
DGCertChainPwd=

### DNS Servers

## DNS Security Extensions
# Use DNS security extensions
# Default value: False
DNSSEC=False

## DNS over TLS
# Use DNS over TLS
# Default value: False
DNSTLS=False

## Multicast DNS
# Use multicast DNS
# Default value: False
mDNS=False

## Link-Local Multicast Name Resolution
# Use link-local multicast name resolution
# Default value: False
LLMNR=False

### NTPv4 Servers

## NTPv4 Authentication
# Use authentication for all NTPv4 servers
# Default value: False
NTPAuth=False

## NTPv4 Keys
# Please enter a space delimited list of IDs present in the key file. The number of IDs in the
list must match the number of servers, even if some or all are the same ID.
NTPKey=

## NTPv4 Key File URI
# Please enter the optional Chrony key file retrieved using SCP (user@host:/path/to/file)
NTPKeyFile=

## NTPv4 Key File Passphrase
# Please enter the SCP user passphrase to retrieve the Chrony key file
NTPKeyFilePwd=

### Remote Syslog Servers

## Remote Syslog Server
# Send Syslog messages to a remote host
# Default value: False
UseRemoteSyslog=False

## Syslog Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the Syslog server accessible from the
 Default Gateway role
```

```
SyslogAddress=

## Syslog Server Port
# Please enter a Syslog port
# Default value: 514
SyslogPort=514

## Syslog Server Protocol
# Please enter the Syslog protocol
# Default value: UDP
SyslogProtocol=UDP

## Syslog over TLS
# Use Syslog over TLS (must use TCP or RELP as the protocol)
# Default value: False
SyslogTLS=False

## Syslog TLS Peer Name
# Please enter the Syslog server's hostname exactly as entered in the server certificate
subjectAltName or subject common name
SyslogPeerName=

## Syslog Root Certificate File URI
# Please enter the optional Syslog root PEM formatted certificate file retrieved using SCP
(user@host:/path/to/file)
SyslogCertChain=

## Syslog Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the Syslog PEM formatted cetificate file
SyslogCertChainPwd=

### Remote Auditd Servers

## Remote auditd Server
# Send auditd messages to a remote host
# Default value: False
UseRemoteAuditd=False

## Auditd Server Address
# Please enter a hostname, IPv4 address, or IPv6 address of the auditd server accessible from the
 Default Gateway role
AuditdAddress=

## Auditd Server Port
# Please enter na auditd port
# Default value: 60
AuditdPort=60

### Controller Settings

## Proxy Server URL
# Please enter the optional HTTP/HTTPS proxy URL
ProxyURL=

## Proxy Server Bypass List
# Please enter an optional space delimited list of subnets and domains that will not be sent to
the proxy server
ProxyBypass=

## Authenticated Proxy Username
# Please enter an optional username for an authenticated proxy servers
ProxyUsername=

## Authenticated Proxy Passphrase
```

```
# Please enter an optional passphrase for an authenticated proxy server
ProxyPassphrase=

## HTTPS Proxy SSL/TLS Certificate File URI
# Please enter the optional HTTPS Proxy PEM formatted SSL/TLS certificate file URI retrieved using
 SCP (user@host:/path/to/file). This will override the Controller SSL/TLS Certificate File URI.
ProxyCertChain=

## HTTPS Proxy SSL/TLS Certificate File Passphrase
# Please enter the SCP user passphrase to retrieve the HTTPS Proxy PEM formatted SSL/TLS certificate
 file
ProxyCertChainPwd=

### Auto Enrollment Package Transfer

## Enrollment Destination Host and Path
# Please enter the optional SCP destination host and path to transfer the enrollment package using
 SCP (user@host:/path/to/file)
EnrollmentURI=

## Enrollment Passphrase
# Please enter the optional SCP user passphrase to transfer the enrollment package
EnrollmentPassphrase=

#### Static Parameters  - Do not change this section

### Deployment Settings

## Deployment Type
# What type of deployment is this?
# Default value: Crosswork Cloud
Deployment=Crosswork Cloud

### Host Information

## Data Disk Size
# Data disk size in GB mounted as /opt/dg/appdata
DGAppdataDisk=24

### vNIC Role Assignment

## Default Gateway
# The interface used as the Default Gateway and for DNS and NTP traffic
# Default value: eth0
NicDefaultGateway=eth0

## Administration
# The interface used for SSH access to the VM
# Default value: eth0
NicAdministration=eth0

## External Logging
# The interface used to send logs to an external logging server
# Default value: eth0
NicExternalLogging=eth0

## Management
# The interface used for enrollment and other management traffic
# Default value: eth0
NicManagement=eth0

## Control
# The interface used for destination, device, and collection configuration
# Default value: eth0
```

```
NicControl=eth0

## Northbound System Data
# The interface used to send collection data to the system destination
# Default value: eth0
NicNBSystemData=eth0

## Northbound External Data
# The interface used to send collection data to external destinations
# Default value: eth0
NicNBExternalData=eth0

## Southbound Data
# The interface used collect data from all devices
# Default value: eth0
NicSBData=eth0
```

b) Repeat the previous step to create the user data for each Crosswork Data VM that you plan to install.

Step 2 **Install the Crosswork Data Gateway VM.**

a) Log in to AWS and search for the EC2 service. The EC2 dashboard opens.

b) Navigate to **Launch Instance** pane on the dashboard and click **Launch Instance** > **Launch Instance**.

A **Launch an Instance** window appears.

c) In the **Name and tags** section, enter the name of the Crosswork Data Gateway VM.

d) In the **Application and OS Images (Amazon Machine Image)** section, click **My AMIs** > **Owned by me** and select the Crosswork Data Gateway AMI image in the **Amazon Machine Image (AMI)** field.

e) In the **Instance type** section, select the **t2.2xlarge** instance type (both production and lab environment) for the Crosswork Data VM you are deploying.

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

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

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

1. Enter values in the following fields:

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

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

2. Update the **Description**, **Primary IP** (vNIC0 IP address from the user data), **Subnet**, **Security groups**.

h) In the **Configure Storage** section, click **Advanced** and click **Add new volume** to add an additional partition for your VM. Update the following fields for the newly created volume.

- **Device name**: /device/sdb
- **Size (GIB)**: 20 GB or 520 GB. If you do not specify a size, the default size of 50 GB is considered.

When extra disk space is required for processing additional dossier collection, you can add node disk.

- **Volume type**: We recommend using gp2 or gp3.

i) In the **Advanced Settings** section, update the following fields.

- **IAM instance profile**: Select the AWS IAM role that you had specified in the user data or create a new role.
- **Metadata accessible**: Enabled.
- **Metadata version**: V1 and V2 (token optional)
- **Metadata response hop limit**: 2
- **User data**: Copy the user data that you had prepared in Step 1 and paste it within the window here. If you are providing the parameters in a base64 encoded format, select the check box.

Note Ensure that there are no leading white spaces when you paste the user data otherwise the deployment fails.

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

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

Verify that the VMs were installed successfully.

1. In the EC2 dashboard, click **Instances** from the menu on the left to view the VMs that were deployed. You can search for the VMs using the name, attributes, or tags.

   Wait for about 20 minutes for the VMs to be deployed.
2. After the VMs are launched successfully, they have the **Instance State** as **Running**.
3. To verify that the VMs were installed successfully, select a VM and click **Connect** (top-right corner).
4. In the **Connect to instance** window that appears, click the **EC2 Serial Control** tab and click **Connect**.
5. Log in to the VM as a `dg-admin` or `dg-oper` user using the password you configured in the user data.

   The Interactive Console of the VM is displayed on successful login.

Generate Enrollment Package

Every Crosswork Data Gateway must be identified by an immutable identifier. This requires generation of an enrollment package. The enrollment package can be generated using any of the following methods:

- By supplying **Auto Enrollment Package** parameters during installation process (see Auto Enrollment Package under Table 4: Cisco Crosswork Data Gateway Deployment Parameters and Scenarios.).
- By using the **Export Enrollment Package** option from the Interactive Console (see Export Enrollment Package, on page 82).
- By using the **Display base64 Encoded Enrollment Package** option from the Interactive Console (see Create an Encoded Enrollment Package, on page 83)

The enrollment package is a JSON document created from the information obtained through the OVF template populated by the user during installation. It includes all the necessary information about Crosswork Data Gateway required for registering, such as Certificate, UUID of the Crosswork Data Gateway, and metadata like Crosswork Data Gateway name, creation time, version information, and so on.

If you opted not to export the enrollment package during install, then you must export or copy it before you can enroll the Crosswork Data Gateway with Crosswork Cloud. The steps to do so are described in Obtain the Enrollment Package, on page 82.

Note The enrollment package is unique to each Crosswork Data Gateway.

Sample enrollment packages in JSON format is shown below:


```
{
  "name": "cdg450-test01",
  "description": "cdg450-test01",
  "profile": {
    "cpu": 8,
    "memory": 31,
    "nics": 1,
    "base_vm": "true"
  },
  "interfaces": [
    {
      "name": "eth0",
      "mac": "xx:xx:xx:xx:xx:xx",
      "ipv4Address": "x.x.x.x/24",
      "roles":
"ADMINISTRATION,CONTROL,DEFAULT_GATEWAY,EXTERNAL_LOGGING,MANAGEMENT,NB_EXTERNAL_DATA,NB_SYSTEM_DATA,SB_DATA"

    }
  ],
  "certChain": [

"MIIJcjCCBVqgAwIBAgIUVBf8hVppCcDBA+yZG6tzIEvq/mEwDQYJKoZIhvcNAQENBQAwLDELMAkGA1UECgwCREcxHTAbBgNVBAMMFGlhbmFzLWNkZzQ1MC
10ZXN0MDExMB4XDTIzMDIwMTE3MTQ0OVoXDTQzMDIwMjE3MTQ0OVowLDELMAkGA1UECgwCREcxHTAbBgNVBAMMFGlhbmFzLWNkZzQ1MC10ZXN0MDExMIIEIjANB
gkqhkiG9w0BAQEFAAOCBA8AMIIECgKCBAEAuvgIWyIDi6FOlecovhbUoGagARPQ32QBkz3s07QgpkatyJalHUYTeseGi0rAPKfzDKoeTZioK5JphDKLRnSze6XJBM
kNpaNyhRIEXWcR/Dds5lRzMQ9qwY3NpWuYlJLKgmbxypabttakLGs0FjXNuqBm4RL3XrhMMooRDkwf7YF5WSMQnszfTGRfDtEVMPMC3xeIul9FLkULSl8FaPgt2cJN
ylK9Z019KeRxpQHP0M5G+d3Nt0ytEFkCdIyjKlwhJRmdpXUcoqaXJLHyg129XouKMTA58ByurbWhR/0th7VAzFFSM5/mncVrvoG0NH8pxpX16ZMPKDyLeHRkyX6EOBb
kwPD3ysEmT/Hw+XsVbOpt8alLQeaQK8MaOsbManZ0ksR8DZk/g8QUXwFWoRsNnq8+GfpvBdzVkoyT1irp43QFrsXxdpIX8pATlwNxoZOkD21jDK7sYTQoNHxKlA1KRu
YIMHDQZt30C5oHRvZfA9V95MWxt+oRaUhdq7JXG8UYyDc/FhVmoqlbEE8ossdBiGwncz/xQ4jaEmAu3UAWFWRISFZuSLdoPD/PsgfblPpYFhnuq/5Um49HB2PYXZuI
yJaKbhX6FAzD49dE6Zm5VuaZPrfPm8v4mu/2l+PPhTfY17nYyXRwEMCX7ZwXtfyZ+bH3xSgi7rG3Vqkte4XqNL/lVkHod2SXKWQ4M/l/cV0FDNX9ifVwPtlmUQgRlen
KvzXWSxCqKCK3olqjz1TELPUPvvkKoZk3x6AqD5IZoriWX5CGHv1ikqHQCDlV9DatnbmIHPVtVQyM30TycVw8uOHJLDqU130LqDCl26kORCT26muJRi35DN4NpIszh2
oBAaYH6hy7rZaIMIC/Uw6BZ4AJ4k4Bpobvlyr Dxf0xeg5Nvf47/GP+LLsn9JeaRhUOdFF8xcNINHjXvH8IfJ72H1lHlsrRB73+V4w3rCC92lsDK8sxN8YAssQm+IRa
Ze6Pw4lvddlfulVYs7PqYwI9LSbeCePzPbKZ4zgl7/A2Ijh8XsV52HZ7shOPgUyaNbjvBi/+/0pI3wILFTbawVAmlEOTOekYm+N1pWWcwH9sB6SEXjG7mLl1jGWFHqV
nduZtjABjWhPE2ZHluZWlA2aLU25Ihd4do+DeDwtsMiMOgvIkSm5c5YS2xjDvZmJF2pf85AY0brVUjRep0z46p3D+zFtuW9DPYn65M+Bypf+OZIms7TfhUXxZlwKCLEM
xvcUc0gc6eOeMhF2lDC26cIBbE2eY5Y99mu8RtQFOLeCC9tcaYifhOB2f9pEGFOuX3DnSc0oXFzhBo9IZhCNUyPjvp1H/bERuFAiENGo0QPy3+vf+LMQK3JKX0BLpMF2Hc
0KhwIDAQABo4GIMIGIMB0GA1UdDgQWBBRBoccosvgUjVkqagHBuZ2UHslsiTzAfBgNVHSMEGDAWgBRBoccosvgUjVkqagHBuZ2UHslsiTzAPBgNVHRMBAf8EBTADAQH/MDUG
A1UdEQQuMCyCFGlhbmFzLWNkZzQ1MC10ZXN0MDExghRtYW5hcy1jZGc0NIAtdGVzdDAxMIANBgkqhkiG9w0BAQ0FAAOCBAFAoLczUuKA4Z8RC5QMVIyx9xeFMslPx7XEF2z
DOhesdIs1SVUDoolplKaQa5hyYtyD5fwzipSgY4H1ylTkyrB+LMbVrGAE6K5A1//rMaft7KWbhJqx57O6FY0JghefGpVyAZ/gW/HI9uxPbDaWHG/SNXPH3zRb/mEIX2vksG
1rpYF1UDap2rDoGNahMC7ueNeDcPYMU9F5hIQeI/gocgg31BE6uUI6mY9gfcMZ94EFcs/RlkI1XR/YwzoCibRWtiJqiZRIuZHX3rYa2vYX8QWIV9BXcVx561r342dIy5/1w9F
ZZHL0SQiWjXozOHFEHBwcMCLo4SbQRuWj8qFg4+dGGuBZvpZkGiaB7bwghBx/JzQpEC0Kv5IZ9YGvnDeX7O9idNkAIRZsbE88U+VZu6DlXstrrRlPmbC/cgEbo3iXIHJZkXa9
4734TSBYI1siluJzAzJXfAYLYR0yoYYoxx7xS4/up0U0amess/HaQcuElOBiYS+/cEnF5r4QT9rQQTIK43G2Gi40vIX6kFYjmKD9Ik7A++TbEWt+BfNIlYjoNHbR8vyrMCFI
J4AlzLYu5/229Vog62LTdpupXJxC7s8sBzfU6TrdCJx0A2FhiHQFS3ElrZAnBpYPkzAGLQBeArlslwOH5cMAgxyOG2wFgca5Oe8PEJRFeB3M+oi3AOv8nJoseXfaPHyuhemDQ
o9XkBEg4w/PSq5rrM8vfWn6Plajo2PbDJq8y8zP0yNjyEP8Dc6IL2bvHn4Jmzz/OQZ4m5a003UmbDK+sQwUmNVfd7MOqrMVvJrhOXc4lUi3srhwoPf5gK82m8S0/QhsWSoz
wGgKxPGTQNR46rRXBxXcuzYyAxSwrsPntMONYRepCUrITFW4a7Ra9srSMO6QcREmX7FlS3h4HetxB/4M/Kmx4XtNRQ+T4HnR9HKJnZ+KXaBkHIy8Lt55JrdlvNrGXcFU/uV9di
F08uwiO+ChhaZC8yfFG855f/dKdHanVBqp5fS47B3IYTC9AxF37q/6Hv1udZDzSkEbWqUbAONGpkOn4poCfePcAXKQ7iDcPr1Jyu3XIUBpkzADKBqRa28G3Y1lriD0k7pb7HII
11YOdGl0C53OnboLrhmnM6BFHYUGI0sMWWWmsiiDrQpbly63khoBzzzA++9tnJtpOeFBOHo5GoJbSqfY+XnpZ5zr2Nt9mF61e8Cv8G4LFXkpCgkKJr5v/VshrFcFlPOudU8Cy
PhpqONBGD0+YHOxhFGDcUCyM3rE7gGAAch4rJDlwkqZWacVSF7fwmMbGlAsb+IbBiDmaelQ6y17LeiWqA3xeSZLXQ7xyXHjYa3hWbjwbAM17vI/9RvnHZSGYEjyNrEmWZuew=="
```

```
  ],
  "version": "4.5.0 (branch dg45x - build number 19)",
  "duuid": "a3bf6411-1ad0-418c-9957-eb199e9395e0",
  "profileType": "VM_PROFILE_STANDARD"
}
```


Obtain the Enrollment Package

You can obtain the enrollment package by exporting or copying and pasting the encoded contents of the package to create an enrollment file.

Step 1 Log in to Cisco Crosswork Data Gateway.

Step 2 From the Main Menu, select **Get Enrollment Package**.

Step 3 Select **Export Enrollment Package** or **Display base64 Encoded Enrollment Package**.

Step 4 Click **OK**.

What to do next

Depending on the option that you have selected, obtain the enrollment package referring to Export Enrollment Package, on page 82 or Create an Encoded Enrollment Package, on page 83

Export Enrollment Package

To enroll the Cisco Crosswork Data Gateway with Crosswork Cloud, you must have a copy of the enrollment package on your local computer.

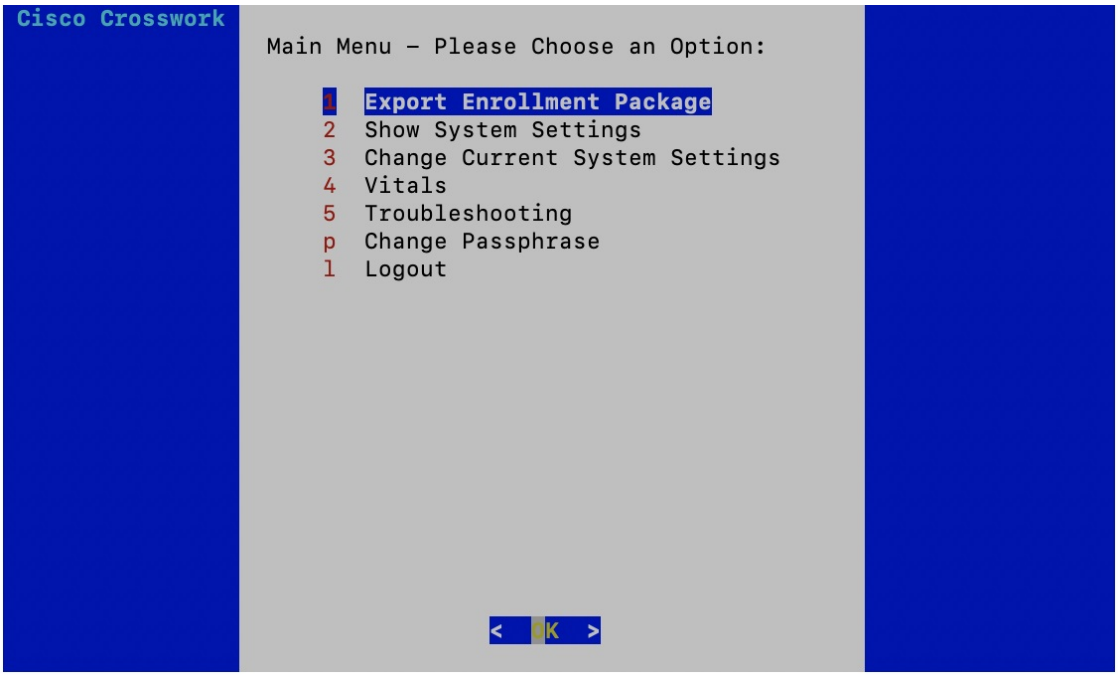
Note This is needed only if you have not specified **Auto Enrollment Package Transfer** settings during installation. Otherwise, the file will be copied to the SCP URI destination you selected after the VM boots. Proceed to Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 84 if you had already specified the **Auto Enrollment Package Transfer** settings during installation.

Step 1 Log in to the Cisco Crosswork Data Gateway.

Step 2 From the Main Menu, select **1 Get Enrollment Package**.

Step 3 Select **Export Enrollment Package**.

Step 4 Click **OK**.



Step 5 Enter the SCP URI for exporting the enrollment package and click **OK**.

Note

- The host must run an SCP server. Ideally, you should export the enrollment package to the local computer you'll use to access the Crosswork server.
- If you are not using the default port 22, you can specify the port as a part of the SCP command. For example, For example, to export the enrollment package as an admin user, placing the file in that user's home directory with port 4000, you can give the following command:

  ```
  scp -P4000 admin@<ip_address>:/home/admin
  ```

- The enrollment file is created with a unique name. For example: 9208b9bc-b941-4ae9-b1a2-765429766f27.json

Step 6 Enter the SCP passphrase (the SCP user password) and click **OK**.

Step 7 If you could not copy the enrollment package directly to your local computer, manually copy the enrollment package from the SCP server to your local computer.

What to do next

Proceed with enrolling the Cisco Crosswork Data Gateway with Crosswork Cloud as explained in Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 84.

Create an Encoded Enrollment Package

You can create an enrollment package file on your local machine by copying and pasting the package contents from the interactive console. The content is secured in the JSON format and encoded using the Base64 schemes.

Step 1 Log in to Cisco Crosswork Data Gateway.

Step 2 From the Main Menu, select **Get Enrollment Package > Display base64 Encoded Enrollment Package**. The enrollment package content is displayed on the console.


ewogICJuYW1lIjogImNk2y0xNzAuY2lzY2BuY29tIiwKICAiZGVzY3JpcHRpb24iOiAiRGV2X1ZN
IiwKICAicHJvZmlsZSI6IHsKICAgICJjcHUiOiAxMiwKICAgICJtZW1vcnkiOiA0NyuKICAgICJu
aWNzIjogMyuKICAgICJiYXN1X3ZtIjogInRydWUiCiAgfSwKICAiaW50ZXJmYWN1cyI6IFsKICAg
IHsKICAgICAgIm5hbWUiOiAiZXRoMCIsCiAgICAgICJtYWMiOiAiMDA6NTA6NTY6YWU6OWU6Y2Ui
LAogICAgICAiaXB2MEFkZHJlc3MiOiAiMTkyLjE2OC41LjE3MC8yNCIsCiAgICAgICJyb2xlcyI6
ICJBRE1JTk1TVFJBVE1PTixERUZBUUxUX0dBUEVXQUksRVhURVJQQUxfTE9HR0IORyxNQU5BR0VM
RU5UIgogICAgfSwKICAgIHsKICAgICAgIm5hbWUiOiAiZXRoMSIsCiAgICAgICJtYWMiOiAiMDA6
NTA6NTY6YWU6ZTA6MzUiLAogICAgICAiaXB2MEFkZHJlc3MiOiAiMTAwMTQuMC4xNzAvMTYiLAog
ICAgICAicm9sZXMiOiAiQ09OVFJPTCxOQ19FWFRFUk5BTF9EQVRBLE5CX1NZU1RFTV9EQVRBIgog
ICAgfSwKICAgIHsKICAgICAgIm5hbWUiOiAiZXRoMiIsCiAgICAgICJtYWMiOiAiMDA6NTA6NTY6
YWU6MZQ6OTciLAogICAgICAicm9sZXMiOiAiU0JfREFUQSIKICAgIH0KICBdLAogICJzZXJ0Q2hh
aW4iOiBbCiAgICAiTUlJS1dqQ0NCVUtnQXdJQkFnSVVSWU94VzlXcjZEdDBTdFMwUE95ZnpJckJm
dlF3RFF2SktvWklodmNOQVFTkJRQXdLUEVMTUFrR0ExVUUD23dDUkVjeEdqQV1C205WQkFNTUUX
TmtaeTB4TnpBdVkybHpZMjh1WTI5dE1CNFhEUE16TURFeE1URTRNRGt4TlZoWERUUXpNREU4TWpF
NE1Ea3hOVm93S1RFTE1Ba0dBMVVFQ2d3Q1JFY3hWakFZQmdOVkJBTU1FV05rWnkweE56QXVZMmx6
WTI4dVkyOXRNSU1FSWpBTkJna3Foa2lHOXcuQkFRRUZBQU9DQkE4QU1JSUVDZ0tDQkFFQXFKRmVz
U1FJcElqZUVyLyt5bUhsZVVySFA0ZUN3a2IxSklyckguVnFFSkJHbmRFdXlXQUx1OWR2YXRjYVFN
QU1US3lpU1k3MzFNVy9vV3l4TXpqM09SVXBiT1VqQTY0ZWtrbEpmWE9uQklHWjR6MmZtbVZLcEU1
bkVYdERKVjMNW1NQT0pTalZpZ3ZRS0tkUXM4MnVPanpwdjJYVzJMV1BLZU9yK1d4MDZ2TTRnNzZz
K0s0SXhPcUR2aTNQYkJydDB0U3BUeksv2GZPdTAzRWk2aDRrdEdmVnhESnB4YzB5ZU1PWXo4SXMm
dFY4djFBSEVBVEhhcVMVZV2Xa295d0hHYU1SLzd0bkh5TUMyODBoSnRDcW9mMG5Zc3Y0d0k0eU1E
UkdOW1lSVDhRcTFFWFhCblhuTHBqTGFQY2psMEJwR3AwZWZKTGxCbE5uQVR1UkRHZnNQU2hJQVhT
S1dqVUZzUnV5cnlQZDRFYlVHNnZ2M12NS0pOMkE4Nktz23UwR0drTW9LUDZFdEM5WWR6Y1VMbU85
aEJxTVJmc1p6Ylk3RFlTdWt jd3V1MXNjUXJkdk1lM0RnSk1QZXcvQZlzQUViLzNPZ31EaVpLZUs4
NHVvMUVEZjVmMVp3YUY4Yn25ejBjSWdtUUVEQTlMMys0eWx5UjJ4L0lkYXZud12weENSMEN2bHpV
NStINFQwUEt4THlCMzlGTXNO2mhScnB0elVHQzNEMGFlZVJZU1pXWGFiRkw1MVZTKzlDQmN0cHQ0
QWRpdVZMMm1zLOg1blJOSk9mUENpUURy2TlgZWhlL0FyVVB6eDJxb1Bman5TQjYvdktMRjMsNZ5y
MEZOT1duQ0YrTkEzUFFKSUtMZkx1aEFJNnIxZHRnSTEydWdXM1VwVHNmS1lCRDNMa jZyMnVqMS9x
VEtXdzkZblddknFEbFdiQ3FUem1BUGppRkJMbk10VjJNYUhWbXdRYTBiRUczRXh4eG9jcU1KZktP
bXNpV0VhS09LNUZpNTR4MZdrOGkvNX1VVV1mdk4rbzhVa0xEdF1RaHFiMVR2TFBLRkszV1pt WEpD
UHU4MmU1Y1JrVVNhMXRt2nBOSEx5dVI3UmF3aWdCSGJJZzgvWW95YZJoNitvZG9Z209MSzRrVWZ4
RzFYdG9ZcHdGUi90UjJd5VEtSWjl4bTg4MnRpd1GRDdOcGUxbytEcjhEU1dYcGg3eXErZklkZEgz
WXhRUFF4QzIrRStEdzJoRmdtVjlhR2g1TE1IK2pQVTJWdWEwcWZ5eXFKblpUMVk5QURYREp2dE9J
N21vMHlaWTBveVlaZ2tIRZB2ZU1JaE5QR3VOQzYzNGg5dkpBQlEwWXpO21c5ei83d0MyOEpvVEhM
Y3lXVTVKVDRiMThyYTBtMXBKRzBzMTgxWFpkcDFuS1lQMHZCVmhvUkNjSE85eWxDTXZGbUt2VkRG
aitZbZxWQ3NvWmY0SHJzTzJWdUMmSVQyWmZXb0xBb2JuQStsMytZWGhTNSsxeDJkMHYzMnRjNWVm
WnpBNWlKZGpITEszODdURzdpU2x4UnJ5bW1OMXdzdkhXaVF1Lz I4TX1xVnRiOG90VTE2dDdYMGgz
RDBSYmNmVmFCRW1NaORQdUpVK2poVkhOM1V5NE96N1UrbUFpcXJmM0xBUitkb2UrdkNUclAvait3
aGdvUU9YWXBtT1UwVE1RMnNvbjdxSE1GOXNrZFhDQ3ppN31MOXcrMFh4ZH1aTzxVRzA1dFFFS2Ex
L0g3TWtaVm1NcH1xTWNvUU1NWVErU1ZFMS9SYXBzdUxmNmtXSjh3eUNrUmJvUVp0THdJREFRQUJv
M29ZURBZEJnTlZIUTRFRmdRVTJIWlo2ZGMyaHJ2RmNtZG5JcFpCazR3WHRNY3dId11EVlIwakJC
Z3dGb0FUMkhaWjZkY3Jocn2GY21kbklwWkJrNHdYdE1jd0R3WURWUjBUQVFIL0JBUXdBd0UCL3pB
bEJnT1ZIUkVFSGpBY2doRmpaR2N0TVRjd0xtTnBjMk5TG1OdmJZSUhZM1JuTFRFM01EQU5CZ2tx
aGtpRzl3MEJBUTBGQUFPQ0JBRUFqMXZEWGlRdkE2T0FZbE9SVWZZa3Z pVkuuV2OzV1JNTlBOWFK
L3lKeVVibAuanZXS0VjR2ZCRUJsM2Fielp2Rl1EUjNkQkU1eEJHTZtBMjhPZXZIb3MyTnlwMk1L
MEZxalFEQ3ZTdmVoeGh3eXpmdlQuMmdUd3FrbzJKL1g1YXYrVnF0MjB5S2dHNm1Ta0JmbzNTYzQy
WlpYM2NEQXRSa0FmN21LZUxncVNEKzUyTURmdXQ0SHhqQkFybFIQL0NCV1MqQ3hCeHhqM3N1SDZ1
--More--

Step 3 Copy the package contents and paste it to a .json file. Save this file.

What to do next

Proceed with enrolling the Cisco Crosswork Data Gateway with Crosswork Cloud as explained in Register Crosswork Data Gateway with Crosswork Cloud Applications, on page 84.

Register Crosswork Data Gateway with Crosswork Cloud Applications

The .json registration file of the Crosswork Data Gateway contains unique digital certificates that are used to enroll Crosswork Data Gateway into Crosswork Cloud. Add that information in Crosswork Cloud as explained below.

Note If you use a firewall on your Crosswork Data Gateway egress traffic, ensure that your firewall configuration allows cdg.crosswork.cisco.com and crosswork.cisco.com.

Step 1 Log in to Crosswork Cloud.

Step 2 From the main window, click **Configure** > **Data Gateways**, then click **Add**.

Step 3 Click **Registration File** to upload the enrollment data file you downloaded from Crosswork Data Gateway, navigate to the location of the .json file, then click **Next**.

Step 4 Enter a name for the Crosswork Data Gateway.

Step 5 In the **Application** field, select the Crosswork Cloud application for which you're using this Crosswork Data Gateway instance. Each Crosswork Data Gateway can be applied to one Crosswork Cloud application only.

Step 6 Complete the rest of the required fields, then click **Next**.

Step 7 (Optional) Enter a tag name, which allows you to group Crosswork Data Gateways with the same tag, then click **Next**.

Step 8 Review the Crosswork Data Gateway information that you entered, then click **Next**.

Step 9 Click **Accept** to accept the security certificate.

A message appears to indicate the Crosswork Data Gateway was successfully added.

What to do next

Repeat this procedure to enroll all the Crosswork Data Gateways in your network with Crosswork Cloud.

To verify that the Crosswork Data Gateway is successfully connected, click **Data Gateways**, click on the name of the Crosswork Data Gateway, and verify the following values for the Crosswork Data Gateway you added:

- **Session Up**: Active
- **Connectivity**: Session Up

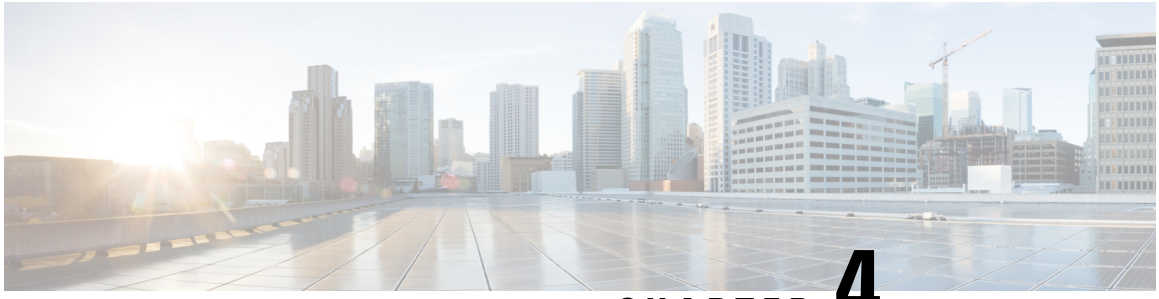
If the Crosswork Data Gateway has not successfully connected to the Crosswork Cloud service, refer to the Troubleshoot the Crosswork Data Gateway Connectivity, on page 85 section.

Troubleshoot the Crosswork Data Gateway Connectivity

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

Table 5: Troubleshooting Crosswork Data Gateway Connectivity

Issue	Action
Crosswork Data Gateway cannot be enrolled with Cisco Crosswork Cloud due to an NTP issue, i.e., there is a clock-drift between the two.	1. Log into the Crosswork Data Gateway VM. 2. From the main menu, go to **5 Troubleshooting** > **Run show-tech**. Enter the destination to save the tarball containing logs and vitals and click **OK**. In the show-tech logs (in file `session.log` at location `/cdg/logs/components/controller-gateway/session.log`), if you see the error `UNAUTHENTICATED:invalid certificate. reason: x509: certificate has expired or is not yet valid` , then there is a clock-drift between Crosswork Data Gateway and Cisco Crosswork Cloud. 3. From the main menu, go to **3 Change Current System Settings** > **1 Configure NTP**. Configure NTP to sync with the clock time on the Cisco Crosswork Cloud server and try enrolling the Crosswork Data Gateway with Crosswork Cloud again.
Crosswork Data Gateway does not have direct connectivity to external web services.	**1.** Configure a proxy server if a proxy server is missing in your environment. **2.** If a proxy server is already present in your enviroment, check if the proxy URL is correct. **3.** Check if the credentials of the proxy (certificate, proxy name etc) are correct. To update the proxy server details on the Crosswork Data Gateway, see Configure Control Proxy, on page 93.



CHAPTER 4

Configure Crosswork Data Gateway Instance

A Cisco Crosswork Data Gateway instance is created as a standalone instance and can be geographically separate from the controller application (Crosswork Cloud). This instance is capable of connecting to the controller application which will enable data collection from the network.

This chapter contains the following topics:

Manage Crosswork Data Gateway Users

This section contains the following topics:

Supported User Roles

Cisco Crosswork Data Gateway supports only two users with the following user roles:

- **Administrator**: One default **dg-admin** user with administrator role is created when Cisco Crosswork Data Gateway is brought up for the first time. This user cannot be deleted and has both read and write privileges such as starting and shutting down the Cisco Crosswork Data Gateway VM, registering an application, applying authentication certificates, configuring server settings, and performing a kernel upgrade.
- **Operator**: The **dg-oper** user is also created by default during the initial VM bring up. This user can review the health of the Cisco Crosswork Data Gateway, retrieve error logs, receive error notifications and run connectivity tests between Cisco Crosswork Data Gateway instance and the output destination.

Note

- User credentials are configured for both the user accounts during Cisco Crosswork Data Gateway installation.
- Users are locally authenticated.

The following table shows the permissions available to each role:

Table 6: Permissions Per Role

Permissions	Administrator	Operator
Get Enrollment Package	✓	✓
Show system settings		
vNIC Addresses NTP DNS Proxy UUID Syslog Certificates First Boot Provisioning Log Timezone	✓	✓
Change Current System Settings		
Configure NTP Configure DNS Configure Control Proxy Configure Static Routes Configure Syslog Create new SSH keys Import Certificate Configure vNIC MTU Configure Timezone Configure Password Requirements Configure Simultaneous Login Limits Configure Idle Timeout	✓	×
Vitals		

Permissions	Administrator	Operator
Docker Containers Docker Images Controller Reachability NTP Reachability Route Table ARP Table Network Connections Disk Space Usage Linux services NTP Status System Uptime	✓	✓
Troubleshooting		
Run Diagnostic Commands	✓	✓
Run show-tech	✓	✓
Export auditd logs	✓	✓
Enable TAC Shell Access	✓	×
Change Passphrase	✓	✓

Change Password

Both adminstrator and operator users can change their own passphrases but not each others'.

Follow these steps to change your passphrase:

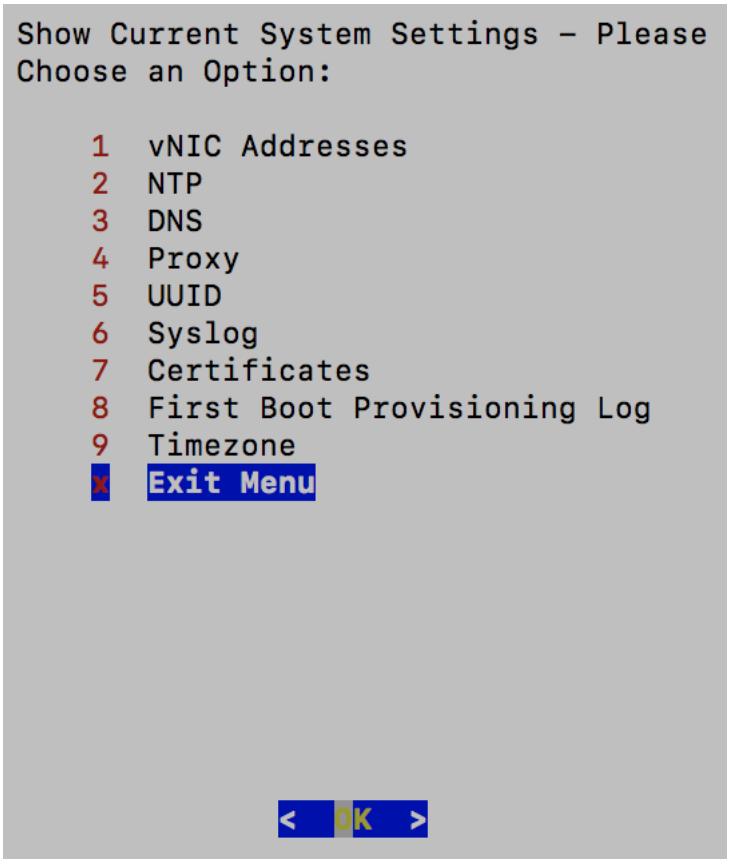
Step 1 From the Main Menu, select **p Change Passphrase** and click **OK**.

Step 2 Input your current password and press Enter.

Step 3 Enter new password and press Enter. Re-type the new password and press Enter.

View Current System Settings

Crosswork Data Gateway allows you to view the following settings:



Follow these steps to view the current system settings:

Step 1 From the Main Menu, select **2 Show System Settings**, as shown in the following figure:

Step 2 Click **OK**. The **Show Current System Settings** menu opens.

Step 3 Select the setting you want to view.

Setting Option	Description
1 vNIC Addresses	Displays the vNIC configuration, including address information.
2 NTP	Displays currently configured NTP server details.
3 DNS	Displays DNS server details.
4 Proxy	Displays proxy server details (if any configured).
5 UUID	Displays the system UUID.
6 Syslog	Displays the Syslog forwarding configuration. If no Syslog forwarding is configured, this will display only "# Forwarding configuration follows" on screen.

Setting Option	Description
7 Certificates	Provides options to view the following certificate files: • Crosswork Data Gateway signing certificate file • Controller signing certificate file • Controller SSL/TLS certificate file • Syslog certificate file • Collector certificate file
8 First Boot Provisioning Log	Displays the content of the first boot log file.
9 Timezone	Displays the current timezone setting.

Change Current System Settings

Crosswork Data Gateway allows you to configure the following settings:

- NTP
- DNS
- Control proxy
- Static routes
- Syslog
- SSH keys
- Certificate
- vNIC MTU
- Timezone
- Password requirements
- Simultaneous login limits
- Idle timeout
- Configure auditd

Note

- Crosswork Data Gateway system settings can only be configured by the administrator.
- If you are using an IPv6 address, it must be surrounded by square brackets ([1::1]).
- In the settings options where you must use SCP, if you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,

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

  Where 55 is a custom port.

Configure NTP

It is important that NTP time be synchronized with the controller application and its Crosswork Data Gateway instances. If not, then session handshake doesn't happen and functional images are not downloaded. In such cases, error message clock time not matched and sync failed is logged in controller-gateway.log. To access log files, see Run show-tech, on page 105. You can use Controller Reachability and NTP Reachability options from **Main Menu** > **Vitals** to check NTP reachability for the controller application as well as the Crosswork Data Gateway. See View Crosswork Data Gateway Vitals, on page 99. If NTP has been set incorrectly,you will see error Session not established.

When configuring Crosswork Data Gateway to use authentication via a keys file, the chrony.keys file must be formatted in a specific way as documented at https://chrony.tuxfamily.org/doc/3.5/chrony.conf.html#keyfile. For sites that use ntpd and are configured to use a ntp.keys file, it is possible to convert from ntp.keys to chrony.keys using the tool https://github.com/mlichvar/ntp2chrony/blob/master/ntp2chrony/ntp2chrony.py. The tool converts ntpd configuration into a chrony compatible format, but only the keys file is required to be imported into Crosswork Data Gateway.

Follow the steps to configure NTP settings:

Step 1 From the **Change Current System Settings** Menu, select **1 Configure NTP**.

Step 2 Enter the following details for the new NTP server:

- Server list, space delimited
- Use NTP authentication?
- Key list, space delimited and must match in number with server list
- Key file URI to SCP to the VM
- Key file passphrase to SCP to the VM

Step 3 Click **OK** to save the settings.

Configure DNS

Step 1 From the **Change Current System Settings** menu, select **2 Configure DNS** and click **OK**.

Step 2 Enter the new DNS server address(es) and domain.

Step 3 Click **OK** to save the settings.

Configure Control Proxy

If you have not configured a proxy server during installation, avail this option to set up a proxy sever:

Step 1 From the **Change Current System Settings** menu, select **3 Configure Control Proxy** and click **OK**.

Step 2 Click **Yes** for the following dialog if you wish to proceed. Click **cancel** otherwise.

Step 3 Enter the new Proxy server details:

- Server URL
- Bypass addresses
- Proxy username
- Proxy passphrase

Step 4 Click **OK** to save the settings.

Configure Static Routes

The static routes are configured when Crosswork Data Gateway receives add/delete requests from the collectors. The **Configure Static Routes** option from the main menu can be used for troubleshooting purpose.

Note Static routes configured using this option are lost when the Crosswork Data Gateway reboots.

Add Static Routes

Follow the steps to add static routes:

Step 1 From the **Change Current System Settings** menu, select **4 Configure Static Routes**.

Step 2 To add a static route, select **a Add**.

Step 3 Select the interface for which you want to add a static route.

Step 4 Select the IP version.

Step 5 Enter IPv4 or IPv6 subnet in CIDR format when prompted.

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

Delete Static Routes

Follow the steps to delete a static route:

Step 1 From the **Change Current System Settings** Menu, select **4 Configure Static Routes**.

Step 2 To delete a static route, select **d Delete**.

Step 3 Select the interface for which you want to delete a static route.

Step 4 Select the IP version.

Step 5 Enter IPv4 or IPv6 subnet in CIDR format.

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

Configure Syslog

Note For any Syslog server configuration with IPv4 or IPv6 support for different Linux distributions, please refer your system administrator and configuration guides.

Follow the steps to configure Syslog:

Step 1 From the **Change Current System Settings** Menu, select **5 Configure Syslog**.

Step 2 Enter the new values for the following syslog attributes:.

- Server address: IPv4 or IPv6 address of a syslog server accessible from the management interface.
- Port: Port number of the syslog server
- Protocol: Use UDP, TCP, or RELP when sending syslog.
- Use Syslog over TLS?: Use TLS to encrypt syslog traffic.
- TLS Peer Name: Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.
- Syslog Root Certificate File URI: PEM formatted root cert of syslog server retrieved using SCP.
- Syslog Certificate File Passphrase: Password of SCP user to retrieve Syslog certificate chain.

Step 3 Click **OK** to save the settings.

Create New SSH Keys

Creating new SSH keys will remove the current keys.

Follow the steps to create new SSH keys:

Step 1 From the **Change Current System Settings** Menu, select **6 Create new SSH keys**.

Step 2 Click **OK**. Crosswork Data Gateway launches an auto-configuration process that generates new SSH keys.

Import Certificate

Updating any certificate other than Controller Signing Certificate causes a collector restart.

Crosswork Data Gateway allows you to import the following certificates:

- Controller signing certificate file
- Controller SSL/TLS certificate file
- Syslog certficate file
- Proxy certificate file

Step 1 From the **Change Current System Settings** Menu, select **7 Import Certificate**.

Step 2 Select the certificate you want to import.

Step 3 Enter SCP URI for the selected certificate file.

Step 4 Enter passphrase for the SCP URI and click **OK**.

Configure vNIC2 MTU

You can change vNIC2 MTU only if you are using 3 NICs.

If your interface supports jumbo frames, the MTU value lies in the range of 60-9000, inclusive. For interfaces that do not support jumbo frames, the valid range is 60-1500, inclusive. Setting an invalid MTU causes Crosswork Data Gateway to revert the change back to the currently configured value. Please verify with your hardware documentation to confirm what the valid range is. An error will be logged into kern.log for MTU change errors which can be viewed after running showtech.

Step 1 From the **Change Current System Settings** menu, select **8 Configure vNIC1 MTU**.

Step 2 Enter vNIC2 MTU value.

Step 3 Click **OK** to save the settings.

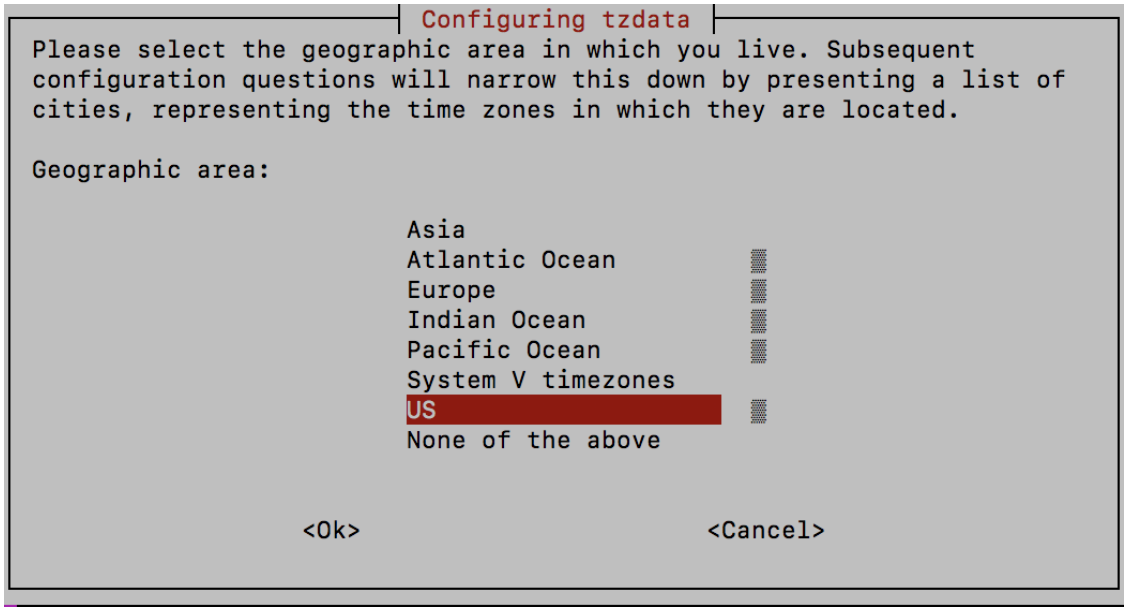
Configure Timezone of the Crosswork Data Gateway VM

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

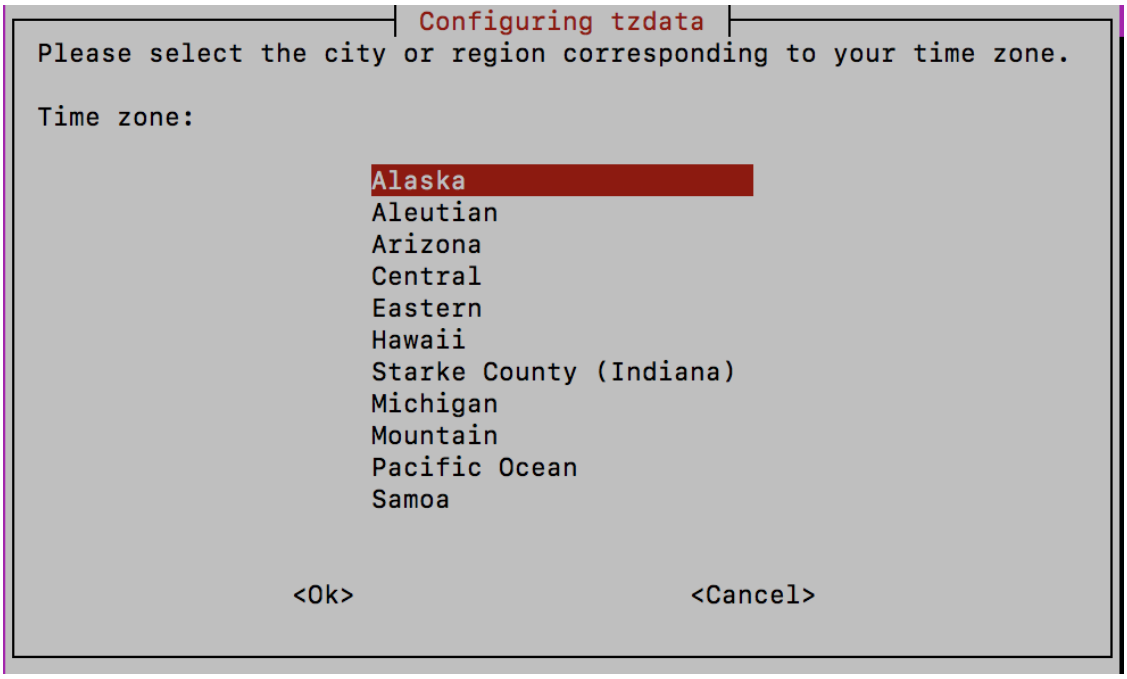
Step 1 In Crosswork Data Gateway VM interactive menu, select **Change Current System Settings**.

Step 2 Select **9 Timezone**.

Step 3 Select the geographic area in which you live.



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



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

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

Step 7 Log out of the Crosswork Data Gateway VM.

Configure Password Requirements

You can configure the following password requirements:

- Password Strength
- Password History
- Password expiration
- Login Failures

Step 1 From **Change Current System Settings** menu, select **0 Configure Password Requirements**.

Step 2 Select the password requirement you want to change.

Set the options you want to change:

- **Password Strength**
  - Min Number of Classes
  - Min Length
  - Min Changed Characters

  - Max Digit Credit
  - Max Upper Case Letter Credit
  - Max Lower Case Letter Credit
  - Max Other Character Credit
  - Max Monotonic Sequence
  - Max Same Consecutive Characters
  - Max Same Class Consecutive Characters
- **Password History**
  - Change Retries
  - History Depth
- **Password expiration**
  - Min Days
  - Max Days
  - Warn Days
- **Login Failures**
  - Login Failures
  - Initial Block Time (sec)
  - Address Cache Time (sec)

Step 3 Click **OK** to save the settings.

Configure Simultaneous Login Limits

By default, Crosswork Data Gateway supports 10 simultaneous sessions for the **dg-admin** and **dg-oper** user on each VM. To change this:

Step 1 From the **Change Current System Settings** menu, select **a Configure Simultaneous Login Limits**.

Step 2 In the window that appears, enter the number of simultaneous sessions for the **dg-admin** and **dg-oper** user.

Step 3 Select **Ok** to save your changes.

Configure Idle Timeout

Step 1 From the **Change Current System Settings** menu, select **b Configure Idle Timeout**.

Step 2 Enter the new value of idle timeout in the window that appears.

Step 3 Enter **Ok** to save your changes.

Configure Remote Auditd Server

Use this procedure to configure the auditd daemon export to a remote server.

Step 1 From the **Change Current System Settings** menu, select **c Configure auditd**.

Step 2 Enter the following details:

- Remote auditd server address.
- Remote auditd server port.

Step 3 Select **OK** to save your changes.

View Crosswork Data Gateway Vitals

Follow these steps to view Cisco Crosswork Data Gateway vitals:

Step 1 From the Main Menu, select **4 Vitals**.

Step 2 From the **Show VM Vitals** menu, select the vital you want to view.

```
Show VM Vitals - Please Choose an
Option:

    1  Docker Containers
    2  Docker Images
    3  Controller Reachability
    4  NTP Reachability
    5  Route Table
    6  ARP Table
    7  Network Connections
    8  Disk Space Usage
    9  Linux Services
    0  NTP Status
    a  System Uptime
    x  Exit Menu

                 <  OK  >
```

Vital	Description
Docker Containers	Displays the following vitals for the Docker containers currently instantiated in the system: • Container ID • Image • Name • Command • Created Time • Status • Port

Vital	Description
Docker Images	Displays the following details for the Docker images currently saved in the system: • Repository • Image ID • Created Time • Size • Tag
Controller Reachability	Displays the results of controller reachability test run: • Default IPv4 gateway • Default IPv6 gateway • DNS server • Controller • Controller session status
NTP Reachability	Displays the result of NTP reachability tests: • NTP server resolution • Ping • NTP Status • Current system time
Route Table	Displays IPv4 and IPv6 routing tables.
ARP Table	Displays ARP tables.
Network Connections	Displays the current network connections and listening ports.
Disk Space Usage	Displays the current disk space usage for all partitions.
Linux Services	Displays the status of the following Linux services: • NTP • SSH • Syslog • Docker • Cisco Crosswork Data Gateway Infrastructure containers.
Check NTP Status	Displays the NTP server status.

Vital	Description
Check System Uptime	Displays the system uptime.

Troubleshooting Crosswork Data Gateway VM

To access **Troubleshooting** menu, select **5 Troubleshooting** from the Main Menu.

Note The image shows the Troubleshooting menu corresponding to **dg-admin** user. Few of these options are not available to **dg-oper** user. See Table Table 6: Permissions Per Role, on page 88.

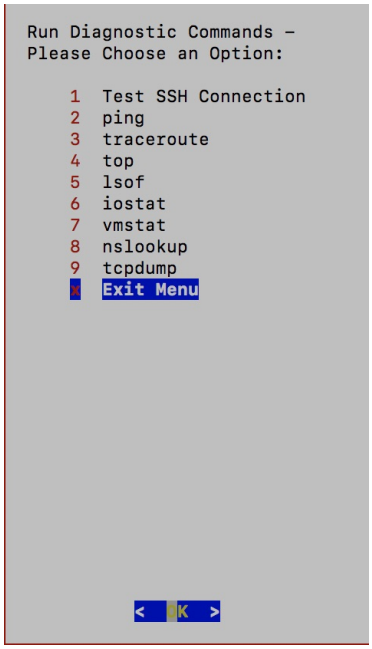
The **Troubleshooting** menu that provides the following options:

Note Crosswork Cloud does not support the **Troubleshooting > Remove All Non-Infra Containers and Reboot** option.

Run Diagnostic Commands

The **Run Diagnostics** menu provides you the following options in the console:

Figure 1: Run Diagnostics Menu



Ping a Host

Crosswork Data Gateway provides you ping utility that can be used to check reachability to any IP address.

Step 1 From **Run Diagnostics** menu, select **2 ping**.

Step 2 Enter the following information:

- Number of pings
- Destination hostname or IP
- Source port (UDP, TCP, TCP Connect)
- Destination port (UDP, TCP, TCP Connect)

Step 3 Click **OK**.

Traceroute to a Host

Crosswork Data Gateway provides **traceroute** option to help troubleshoot latency issues. Using this option provides you a rough time estimate for the Crosswork Data Gateway to reach the destination.

Step 1 From **Run Diagnostics** menu, select **3 traceroute**.

Step 2 Enter the traceroute destination.

Step 3 Click **OK**.

Command Options to Troubleshoot

Crosswork Data Gateway provides several commands for troubleshooting.

Step 1 Navigate to **5 Troubleshooting** > **1 Run Diagnostics**.

Step 2 Select the command and other option or filters for each of the commands:

- **4 top**
- **5 lsof**
- **6 iostat**
- **7 vmstat**
- **8 nsolookup**

Step 3 Click **Ok**.

Once you have selected all the options, Crosswork Data Gateway clears the screen and runs the command with the specified options.

Download tcpdump

Crosswork Data Gateway provides the tcpdump option that allows you to capture and analyze network traffic.

Note This task can only be performed by a **dg-admin** user.

Step 1 Go to **5 Troubleshooting** > **Run Diagnostics** > **9 tcpdump**.

Step 2 Select an interface to run the tcpdump utility. Select the **All** option to run it for all interfaces.

Step 3 Select the appropriate checkbox to view the packet information on the screen or save the captured packets to a file.

Step 4 Enter the following details and click **Ok**.

- Packet count limit
- Collection time limit
- File size limit
- Filter expression

Depending on the option you choose, Crosswork Data Gateway displays the packet capture information on the screen or saves it to a file. Once the tcpdump utility reaches the specified limit, Crosswork Data Gateway

compresses the file and prompts for the SCP credentials to transfer the file to a remote host. The compressesd file is deleted once the transfer is complete or if you've decided to cancel the file transfer before completion.

Run a Controller Session Test

After Crosswork Data Gateway is installed, you can validate if the instance is able to establish a connection with Crosswork Cloud by using the controller session test option. In addition to the connection tests, the utility validates and analyzes the discrepancies between the resources (CPU and memory) assigned to the VM and the resources prescribed by the deployment profile.

From **Run Diagnostics** menu, select **Run Controller Session Tests**. If the connection is completed, the console displays a message indicating that the instance was able to establish a connection. When the connection fails, additional validation tests are performed, and the following information is displayed:

- DNS server IP address
- DNS domain
- NTP server address
- NTP status
- Proxy URL
- Proxy reachability status
- Controller URL
- Controller reachability status
- The date when the tests were last performed.

What to do next

If the controller session was not established, review the information displayed on the console to determine the probable cause of the failure and perform the corrective actions proposed on the console.

Run show-tech

Crosswork Data Gateway provides the option **show_tech** to export its log files to a user-defined SCP destination.

The collected data includes the following:

- Logs of all the Data Gateway components running on Docker containers
- VM Vitals

It creates a tarball in the directory where it is executed. The output is a tarball named `DG-<CDG version>-<CDG host name>-year-month-day--hour-minute-second.tar.xz.enc`.

The execution of this command may take several minutes depending on the state of Crosswork Data Gateway.

Step 1 From **Troubleshooting** menu, select **5 Show-tech** and click **OK**.

Step 2 Enter the destination to save the tarball containing logs and vitals.

Step 3 Enter your SCP passphrase and click **OK**.

The showtech file downloads in an encrypted format.

Note Depending on how long the system was in use, it may take several minutes to download the showtech file.

Step 4 After the download is complete run the following command to decrypt it:

Note In order to decrpyt the file, you must use OpenSSL version 1.1.1i. Use the command `openssl version` to check the openssl version on your system.

To decrypt the file on a MAC, you must install OpenSSL 1.1.1+. This is because LibreSSL's `openssl` command does not support all the switches supported by OpenSSL's `openssl` command.

```
openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Shutdown the Crosswork Data Gateway VM

From the **Troubleshooting** Menu, select **5 Shutdown VM** to power off the Crosswork Data Gateway VM.

Export auditd Logs

Follow the steps to export auditd logs:

Step 1 From **Troubleshooting**, select **9 Export audit Logs**.

Step 2 Enter a passphrase for auditd log tarball encryption.

Step 3 Click **OK**.

Remove Rotated Log Files

Use this procedure to removes all rotated log files (*.gz or *.xz) in the `/var/log` and `/opt/dg/log` folders.

Step 1 From **Troubleshooting** menu, select **8 Remove Rotated Log files**.

Step 2 Select **Yes** in the dialog that appears to save your changes.

Enable TAC Shell Access

The TAC Shell Access function allows a Cisco engineer to directly log in to the Ubuntu shell via multifactor authentication, using a reserved user named **dg-tac**.

Initially, the **dg-tac** user account is locked and password is expired to prevent the user from getting a shell prompt. Once enabled, the dg-tac user is active until the next calendar day, 12:00 a.m UTC (midnight UTC), which is less than 24 hours.

The steps to enable the **dg-tac** user are as follows:

Note Enabling this access requires you to communicate actively with the Cisco engineer.

Before you begin

Ensure that the Cisco engineer who is working with you has access to the SWIMS Aberto tool.

Step 1 Log in to the Data Gateway VM as the **dg-admin** user.

Step 2 From the main menu, select **5 Troubleshooting**.

Step 3 From the **Troubleshooting** menu, select **t Enable TAC Shell Access**.

A dialog appears, warning that the **dg-tac** user login requires a password that you set and a response to a challenge token from TAC. At this point, you may answer **No** to stop the enable process or **Yes** to continue.

Step 4 If you continue, the system prompts for a new password to use and shows the day when the account disables itself.

Step 5 Enter a password to unlock the account in the console menu.

Step 6 Log out of the Crosswork Data Gateway.

Step 7 Follow these steps if the Crosswork Data Gateway VM can be accessed by the Cisco engineer directly. Move to **Step 8** otherwise.

a) Share the password that you had set in Step 5 for the **dg-tac** user with the Cisco engineer who is working with you.

b) The Cisco engineer logs in as the **dg-tac** user Via SSH with the password you had set.

After entering the password, the system presents the challenge token. The Cisco engineer signs the challenge token using the SWIMS Aberto tool and pastes the signed response to the challenge token back at the Crosswork Data Gateway VM.

c) The Cisco engineer logs in successfully as the **dg-tac** user and completes the troubleshooting.

There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

d) After troubleshooting is complete, the Cisco engineer logs out of the TAC shell.

Step 8 If Crosswork Data Gateway VM cannot be accessed directly by the Cisco engineer, start a meeting with the Cisco engineer with desktop sharing enabled.

a) Log in as the **dg-tac** user Via SSH using the following command:

```
ssh dg-tac@<DG hostname or IP>
```

b) Enter the password that you set for the **dg-tac** user.

After entering the password, the system presents the challenge token. Share this token with the Cisco engineer who will then sign the token using the SWIMS Aberto tool and share the response with you.

c) Paste the signed response to the challenge token back to the Crosswork Data Gateway VM and press enter to get the shell prompt.

d) Share your desktop or follow the Cisco engineer's instructions for troubleshooting.

   There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

e) Log out of the TAC shell after troubleshooting is complete.

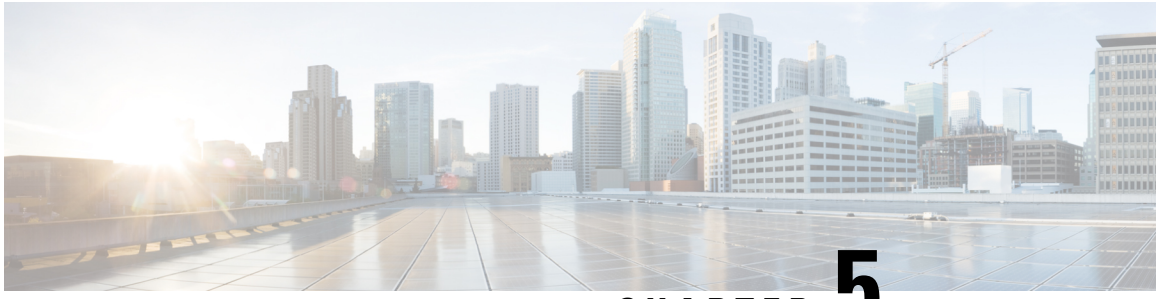
Audit TAC Shell Events

Timestamp information of the following list of TAC shell events is logged to the **tac_shell.log** file. The Tac shell events are also sent to the Crosswork Cloud controller.

- TAC shell enabled
- TAC shell disabled
- dg-tac login
- dg-tac log out

If the Data Gateway is unable to connect to the Crosswork Cloud controller, the TAC shell events are logged in the `/opt/dg/data/controller-gateway/audit/pending` folder. Once the Crosswork Cloud controller is reachable, these events are sent within 5 minutes.

The **tac_shell.log** file is available in the showtech bundle of the Crosswork Data Gateway VM.



CHAPTER 5

Delete the Virtual Machine

This section contains the following topics:

Delete VM using vSphere UI

This section explains the procedure to delete a Crosswork Data Gateway VM from vCenter.

Note Be aware that this procedure deletes all your Crosswork Data Gateway data.

Before you begin

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

Step 1 Log in to 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.

Delete VM from OpenStack

Follow the steps to delete the Crosswork Data Gateway Service from OpenStack using the OpenStack UI:

Note This procedure deletes the Crosswork Data Gateway VM data. The Crosswork Data Gateway VM cannot be recovered once it has been deleted.

Before you begin

Ensure that you have deleted the Crosswork Data Gateway from Crosswork Cloud as described in the Section: *Delete Crosswork Data Gateways* in the *Cisco Crosswork Cloud User Guide*.

Step 1 **From the OpenStack UI:**

a) Log in to the OpenStack UI.
b) Navigate to **Compute** > **Instances**.
c) From the list of VM displayed in this page, select the VM you want to delete.
d) Click **Delete Instances**.
e) Click **Delete Instances** in the confirmation window that appears to delete the VM.

OR

Step 2 **From the OpenStack CLI:**

a) Log in to the OpenStack VM from CLI.
b) Run the following command:

```
openstack server delete CDG_VM_name
```

For example,

```
openstack server delete cdg-ospd1
```

c) (Optional) Confirm that the VM has been deleted by viewing the list of all VMs.

```
openstack server list
```