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 1
2. Enable ports that are required for the Crosswork Data Gateway to operate. See Ports Used, on page 5.
3. Understand if a proxy server may be required in your environment. See Proxy Server Requirements, on page 5.

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

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

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.
- From the Interactive Console of the Crosswork Data Gateway after installation. See Configure Control Proxy

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
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 • Install Crosswork Data Gateway on Amazon EC2 Manually