Installation Prerequisites for AWS EC2

This chapter contains the following topics:

Overview

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

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

Amazon EC2 Settings

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

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

Crosswork is deployed in Amazon EC2 using CloudFormation (CF) templates. The CloudFormation process is faster and less error-prone than the manual procedure to build the cluster, however you must have the necessary skills to prepare a CloudFormation template with details of the cluster deployment.

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

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

Table 1: AWS Prerequisites and Settings

Requirement	Description
VPC and Subnets	Virtual Private Cloud (VPC) is created and configured with dedicated subnets for Crosswork interfaces (Management and Data) and Crosswork Data Gateway (Management, Data, and Device) interfaces. Direct IP connectivity is required between all subnets.
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 are using different management subnets for the Crosswork VM and the Crosswork Data Gateway VM, ensure that you specify both the management subnets so that the endpoint has access to both the subnets. **Important** The interface subnet should not conflict with the Network Load Balancer (NLB). For information on how to configure the endpoints, refer to the AWS documentation.
IAM role	A role is created in Identity and Access Management (IAM) with relevant permission policies. An IAM role is an identity that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust. **Note** • The minimum permissions required for a Crosswork role are **ec2:DescribeNetworkInterfaces**, **ec2:AssignPrivateIpAddresses** and **ec2:UnassignPrivateIpAddresses**. • The trust policy for your role must have the **"Action": "sts:AssumeRole"** condition.
Key pairs	Key pairs (private keys used to log into the VMs) are created and configured.
Placement Groups	A placement group of *Cluster* strategy is created. In a *cluster* placement group, instances are logically grouped in a single availability zone that benefit from low network latency and high network throughput. This requirement is required only for launching the Crosswork cluster instances.

Requirement	Description
IP addresses	**Crosswork cluster**: When using single NIC, you require one IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and one additional IP address to be used as the Virtual IP (VIP) address. When using dual NICs (one for the Management network and one for the Data network), you require a management and data IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and two additional IP addresses to be used as the management and data Virtual IP (VIP) address. For example, in the case of a 3 VM cluster with a single NIC, you need 4 IP addresses, and in the case of a 3 VM cluster with dual NIC, you need 8 IP addresses (4 for management network and 4 for data network). **Crosswork Data Gateway**: IP addresses for Management Traffic and Data Traffic only. IP address for Device Access Traffic is assigned during Crosswork Data Gateway pool creation as explained in the Section: *Create a Crosswork Data Gateway Pool* in the *Cisco Crosswork Network Controller 6.0 Administration Guide*. • The IP addresses must be able to reach the gateway address for the network where Cisco Crosswork Data Gateway will be installed, or the installation fails. • At this time, your IP allocation is permanent and cannot be changed without redeployment. For more information, contact the Cisco Customer Experience team.
Security group	A security group must be created and configured to specify which ports or traffic are allowed.

Instance type	The resource profile for your instance deployment. The AWS Instance type should be selected to conform with the VM resource and network requirements listed in Plan Your Deployment.
	
	• **Crosswork Cluster**:
	  • Select **m5.4xlarge** for demos or lab deployments.
	  • Select **m5.8xlarge** for production deployments.
	
	• **Crosswork Data Gateway** (production and lab deployments):
	  • **Standard** - Select **m5.4xlarge**
	  • **Extended** - Select **m5.8xlarge**

CloudFormation (CF) template	The CF template (.yaml) files for the Crosswork components that must be uploaded during the installation. For more information, see Extract CF Template Image.
Route53DomainName	Domain name configured for Route53 DNS hosted zone.
User data	The VM-specific parameters script that must be specified during the manual installation procedure.

Requirement	Description
Hosted Zone ID	The Hosted Zone ID must be provided with the domain name (Route53DomainName). The Network Load Balancer (NLB) deployments require a predefined Route53 hosted zone.

Host VM Requirements

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

- Crosswork Cluster VM Requirements
- Crosswork Data Gateway VM Requirements

Crosswork Cluster VM Requirements

The Crosswork cluster consists of three VMs or nodes operating in a hybrid configuration. This is the minimum configuration necessary to support the applications in a standard network. Additional VMs or nodes (maximum up to 2 worker nodes) in a worker configuration can be added later to scale your deployment, as needed, to match the requirements of your network, or as other applications are introduced (see Table 1 for more information on VM count for each Crosswork Network Controller package). Please consult with the Cisco Customer Experience team for guidance on your deployment to best meet your needs.

The table below explains the network requirements per VM host:

Table 2: Network Requirements (per VM)

Requirement	Description
Network Connections	For production deployments, we recommend that you use dual interfaces, one for the Management network and one for the Data network. For optimal performance, the Management and Data networks should use links configured at a minimum of 10 Gbps.
NTP Servers	The IPv4 or IPv6 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize the Crosswork application VM clock, devices, clients, and servers across your network. Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.
DNS Servers	The IPv4 or IPv6 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network. Ensure that the DNS servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.
DNS Search Domain	The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.

Requirement	Description
Backup Server	Cisco Crosswork will back up the configuration of the system to an external server using SCP. The SCP server storage requirements will vary slightly but you must have at least 50 GB of storage.

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

Crosswork Data Gateway VM Requirements

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

- Selecting the Crosswork Data Gateway Deployment Type, on page 5
- Crosswork Data Gateway VM Requirements, on page 6

Selecting the Crosswork Data Gateway Deployment Type

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

Note The VM resource requirements for Crosswork Data Gateway are different for each type and cannot be modified. Therefore, if your requirements change, you must re-deploy the Crosswork Data Gateway to move from one type to another. For more information, see the *Redeploy a Crosswork Data Gateway VM* section in *Cisco Crosswork Network Controller 6.0 Administration Guide*.

Table 3: Crosswork Data Gateway deployment types

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

Crosswork Data Gateway VM Requirements

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

Table 4: Crosswork Data Gateway Requirements for on-premise applications

<table>
<tr><th>Requirement</th><th colspan="4">Description</th></tr>
<tr><td>Data Center</td><td colspan="4">VMware. See Installation Prerequisites for VMware vCenter.</td></tr>
<tr><td>Interfaces</td><td colspan="4">Minimum: 1
Maximum: 3
Cisco Crosswork Data Gateway can be deployed with either 1, 2, and 3 interfaces as per the combinations below:
Note If you use one interface on your Crosswork cluster, you must use only one interface on the Crosswork Data Gateway. If you use two interfaces on your Crosswork Cluster, then you can use two, or three interfaces on the Crosswork Data Gateway as per your network requirements.</td></tr>
<tr><td></td><td>No. of NICs</td><td>vNIC0</td><td>vNIC1</td><td>vNIC2</td></tr>
<tr><td></td><td>1</td><td>• Management Traffic
• Control/Data Traffic
• Device Access Traffic</td><td>—</td><td>—</td></tr>
<tr><td></td><td>2</td><td>Management Traffic</td><td>• Control/Data Traffic
• Device Access Traffic</td><td>—</td></tr>
<tr><td></td><td>3</td><td>Management Traffic</td><td>Control/Data Traffic</td><td>Device Access Traffic</td></tr>
<tr><td></td><td colspan="4">• Management traffic: for accessing the Interactive Console and passing the Control/Data information between servers (for example, a Crosswork application to Crosswork Data Gateway).
• Control/Data traffic: for data and configuration transfer between Cisco Crosswork Data Gateway and Crosswork applications and other external data destinations.
• Device access traffic: for device access and data collection.
Note Due to security policies, traffic from subnets of a vNIC received on other vNICs is dropped. For example, in a 3 vNIC model setup, all device traffic (incoming and outgoing) must be routed through default vNIC2. Crosswork Data Gateway drops device traffic received over vNIC0 and vNIC1.</td></tr>
</table>

Requirement	Description
IP Addresses	1 or 2 IPv4 or IPv6 addresses based on the number of interfaces you choose to use. An additional IP address to be used as the Virtual IP (VIP) address. For each active data gateway, a unique VIP is required. For more information, refer to the *Interfaces* section in the Table 1. **Note** Crosswork does not support dual stack configurations. Therefore, all addresses for the environment must be either IPv4 or IPv6. In a 3-NIC deployment, you need to provide an IP address for Management interface (vNIC0) and Control/Data interface (vNIC1) during installation. A virtual IP address for Device Access Traffic (vNIC2) is assigned when you create a Crosswork Data Gateway to a pool as explained in the *Create a Crosswork Data Gateway Pool* section in *Cisco Crosswork Network Controller 6.0 Administration Guide*.
NTP Servers	The IPv4 or IPv6 addresses or host names of the NTP servers you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize devices, clients, and servers across your network. Verify that the NTP IP address or host name is reachable on the network else the installation fails. Also, the ESXi hosts that run the Crosswork application and Cisco Crosswork Data Gateway VM must have NTP configured, or the initial handshake may fail with "certificate not valid" errors.
DNS Servers	The IPv4 or IPv6 addresses of the DNS servers you plan to use. These should be the same DNS servers you use to resolve host names across your network. Confirm that the DNS servers are reachable on the network before attempting installation. The installation fails if the servers cannot be reached.
DNS Search Domain	The search domain you want to use with the DNS servers, for example, cisco.com. You can have only one search domain.
FQDN	Crosswork does not support dual stack configurations. Therefore, all FQDN addresses configured for the deployment environment must be either IPv4 or IPv6. The FQDN addresses are configured for Amazon EC2 deployments.
Internet Control Message Protocol (ICMP)	The Crosswork uses ICMP in the communications with Crosswork Data Gateway. Ensure that the firewall between Crosswork and the Crosswork Data Gateway passes this traffic.

Crosswork TCP/UDP Port requirements

Crosswork Cluster Port Requirements

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

Note Crosswork cluster ports allow bidirectional flow of information.

Table 5: External Ports used by Crosswork Cluster

Port	Protocol	Used for
22	TCP	Remote SSH traffic
111	TCP/UDP	GlusterFS (port mapper)
179	TCP	Calico BGP (Kubernetes)
80, 443	TCP	Accessing the EC2 API.
500	UDP	IPSec
2379/2380	TCP	Kubernetes etcd
4500	UDP	IPSec
6443	TCP	kube-apiserver (Kubernetes)
9100	TCP	Kubernetes metamonitoring
10250	TCP	kubelet (Kubernetes)
24007	TCP	GlusterFS
30603	TCP	User interface (NGINX server listens for secure connections on port 443)
30606	TCP	Docker Registry
30621	TCP	For FTP (available on data interface only). The additional ports used for file transfer are 31121 (TCP), 31122 (TCP), and 31123 (TCP). This port is available only when the supported application is installed on Cisco Crosswork and the FTP settings are enabled.
30622	TCP	For SFTP (available on data interface only) This port is available only when the supported application is installed on Cisco Crosswork and the SFTP settings are enabled.
49152:49370	TCP	GlusterFS

Table 6: Ports used by other Crosswork components

Port	Protocol	Used for
30602	TCP	to monitor the installation (Crosswork Network Controller)
30603	TCP	Crosswork Network Controller Web User interface (NGINX server listens for secure connections on port 443)
30604	TCP	Used for Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server.
30607	TCP	Crosswork Data Gateway vitals collection
30608	TCP	Data Gateway gRPC channel with Data Gateway VMs
30609	TCP	Used by the Expression Orchestrator (Crosswork Service Health)
30610	TCP	Used by the Metric Scheduler (Crosswork Service Health)
30611	TCP	Used by the Expression Tracker component (Crosswork Service Health)
30617	TCP	Used for Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server.
30620	TCP	Used to receive plug-and-play HTTP traffic on the ZTP server.
30649	TCP	To set up and monitor Crosswork Data Gateway collection status.
30650	TCP	astack gRPC channel with astack-client running on Data Gateway VMs
30993, 30994, 30995	TCP	Crosswork Data Gateway sending the collected data to Crosswork Kafka destination.

Table 7: Destination Ports used by Crosswork Cluster

Port	Protocol	Used for
7	TCP/UDP	Discover endpoints using ICMP
22	TCP	Initiate SSH connections with managed devices
53	TCP/UDP	Connect to DNS
123	UDP	Network Time Protocol (NTP)
830	TCP	Initiate NETCONF
2022	TCP	Used for communication between Crosswork and Cisco NSO (for NETCONF).

Port	Protocol	Used for
8080	TCP	REST API to SR-PCE
8888	TCP	Used for communication between Crosswork and Cisco NSO (for HTTPS).
20243	TCP	Used by the DLM Function Pack for communication between DLM and Cisco NSO
20244	TCP	Used to internally manage the DLM Function Pack listener during a Reload Packages scenario on Cisco NSO

Crosswork Data Gateway Port Requirements

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

Inbound: Crosswork Data Gateway listens on the specified ports.

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

Table 8: Ports to be Opened for Management Traffic

Port	Protocol	Used for	Direction
22	TCP	SSH server	Inbound
22	TCP	SCP client	Outbound
123	UDP	NTP Client	Outbound
53	UDP	DNS Client	Outbound
30607	TCP	Crosswork Controller	Outbound

Note SCP port can be tuned.

Table 9: Ports to be Opened for Device Access Traffic

Port	Protocol	Used for	Direction
161	UDP	SNMP Collector	Outbound

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

Table 10: Ports to be Opened for Control/Data Traffic

Port	Protocol	Used for	Direction
30649	TCP	Crosswork Controller	Outbound

Port	Protocol	Used for	Direction
30993 30994 30995	TCP	Crosswork Kafka	Outbound
Site Specific	Site Specific	Kafka and gRPC Destination	Outbound

IP Address Restrictions

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

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

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

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

Table 11: Protected IP Subnets

IP Type [1]	Subnet	Remarks
IPv4	172.17.0.0/16	Docker Subnet (Infrastructure)
	169.254.0.0/16	Link local address block
	127.0.0.0/8	Loopback address
	192.88.99.0/24	Reserved, previously used for relay servers to do IPv6 over IPv4
	240.0.0.0/4	Reserved for future use (previously class E block)
	224.0.0.0/4	MCAST-TEST-NET
	0.0.0.0/8	Current network, valid as source address only

IP Type [1]	Subnet	Remarks
IPv6	2001:db8:1::/64	Docker Subnet (Infrastructure)
	fdfb:85ef:26ff::/48	Pod Subnet (Infrastructure)
	fd08:2eef:c2ee::/110	Service Subnet (Infrastructure)
	::1/128	Loopback address
	fe80::/10	Link local
	ff00::/8	IPv6 Multicast
	2002::/16	Reserved, previously used for relay servers to do IPv6 over IPv4
	2001:0000::/32	Terredo tunnel and relay
	2001:20::/28	Used by ORCHID and not IPv6 routable
	100::/64	Discard prefix, used in specific use-cases not applicable to Crosswork Zero Touch Provisioning
	::/128	Unspecified address, cannot be assigned to hosts
	::ffff:0:0/96	IPv4 mapped addresses
	::ffff:0:0:0/96	IPv4 translated addresses

[1] Dual stack configuration is not supported in Crosswork Platform Infrastructure. Therefore, **all** addresses for the environment must be either IPv4 or IPv6.