Installation Prerequisites for VMware vCenter

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.

Supported Network Topology Models

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

Routed and Device Networks

The following table describes the types of traffic that comes from the Crosswork Network Controller. This traffic can use a single NIC (typically in lab installs) or dual NICs.

Table 1: Types of Crosswork Network Traffic

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

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

Connectivity between the various components should be accomplished via an external routing entity. The Network Topology figures in this section show various line styles suggesting possible routing domains within the routed network.

- Solid - Management routing domain.
- Dotted - Data/Control routing domain (information transferred between Cisco Crosswork and Cisco Crosswork Data Gateway, and other data destinations (external Kafka or gRPC)).
- Dashes - Device access routing domain (from Cisco Crosswork Data Gateway and NSO).
- Blue dotted/dashed line - Alternate SR-PCE configuration path

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

Routing between domains is needed for Crosswork and NSO to reach the devices. However, proper firewall rules need to be in place to allow only select sources (for example, Crosswork and NSO) to reach the devices.

Important

- It is vital to have secure firewalls between Crosswork Network Controller and the network devices. However, the firewalls are not provided by Crosswork Network Controller and must be set up separately by the user. This topic highlights what application flows need to be allowed through the user-provided firewall system.
- On the device network, devices can be reached in-band or using out-of-band management interfaces, depending on the local security policies of each deployment.

The three supported configurations are:

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

Figure 1: Cisco Crosswork - 1 NIC Network Topology

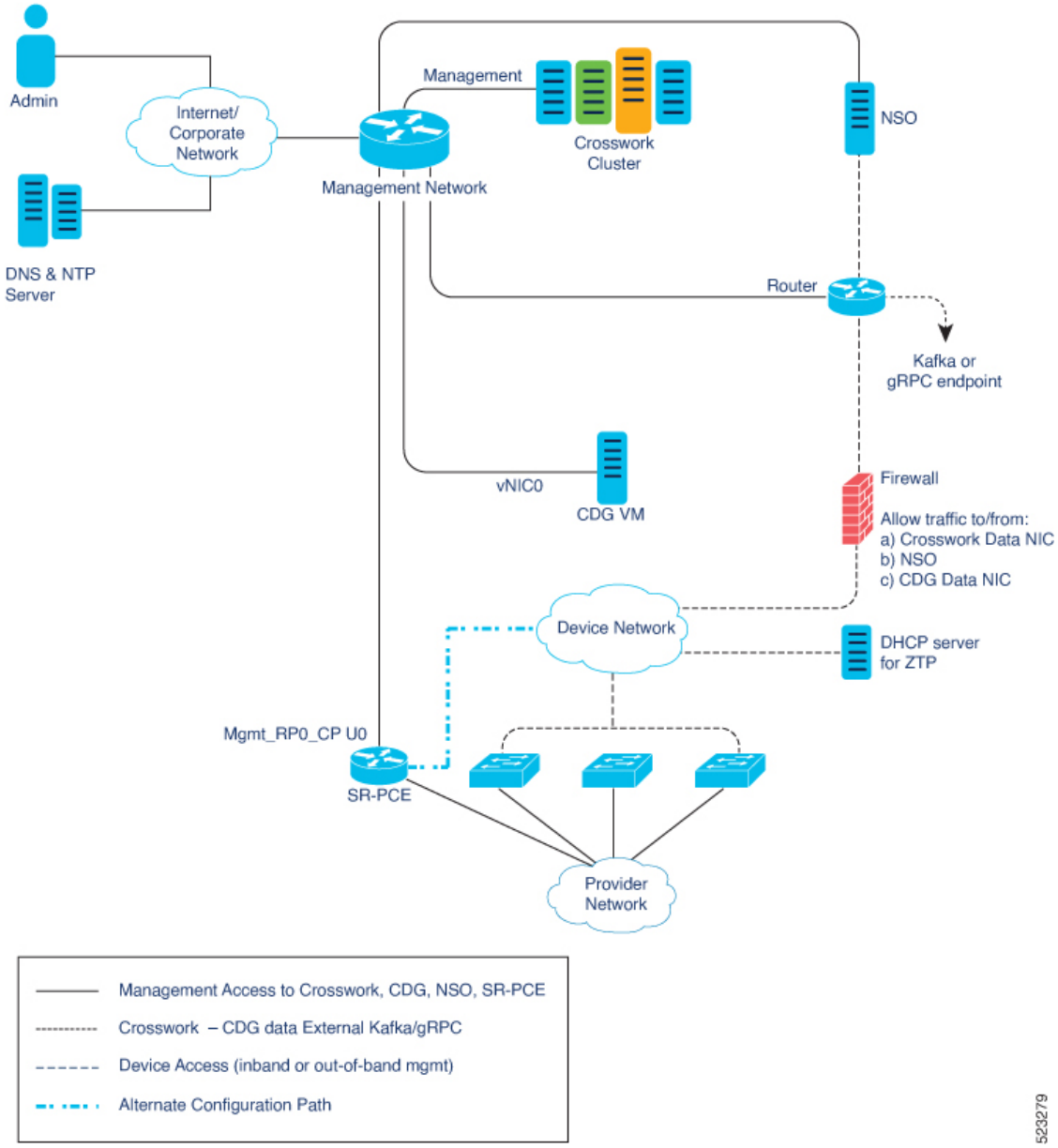


Figure 2: Cisco Crosswork - 2 NIC Network Topology

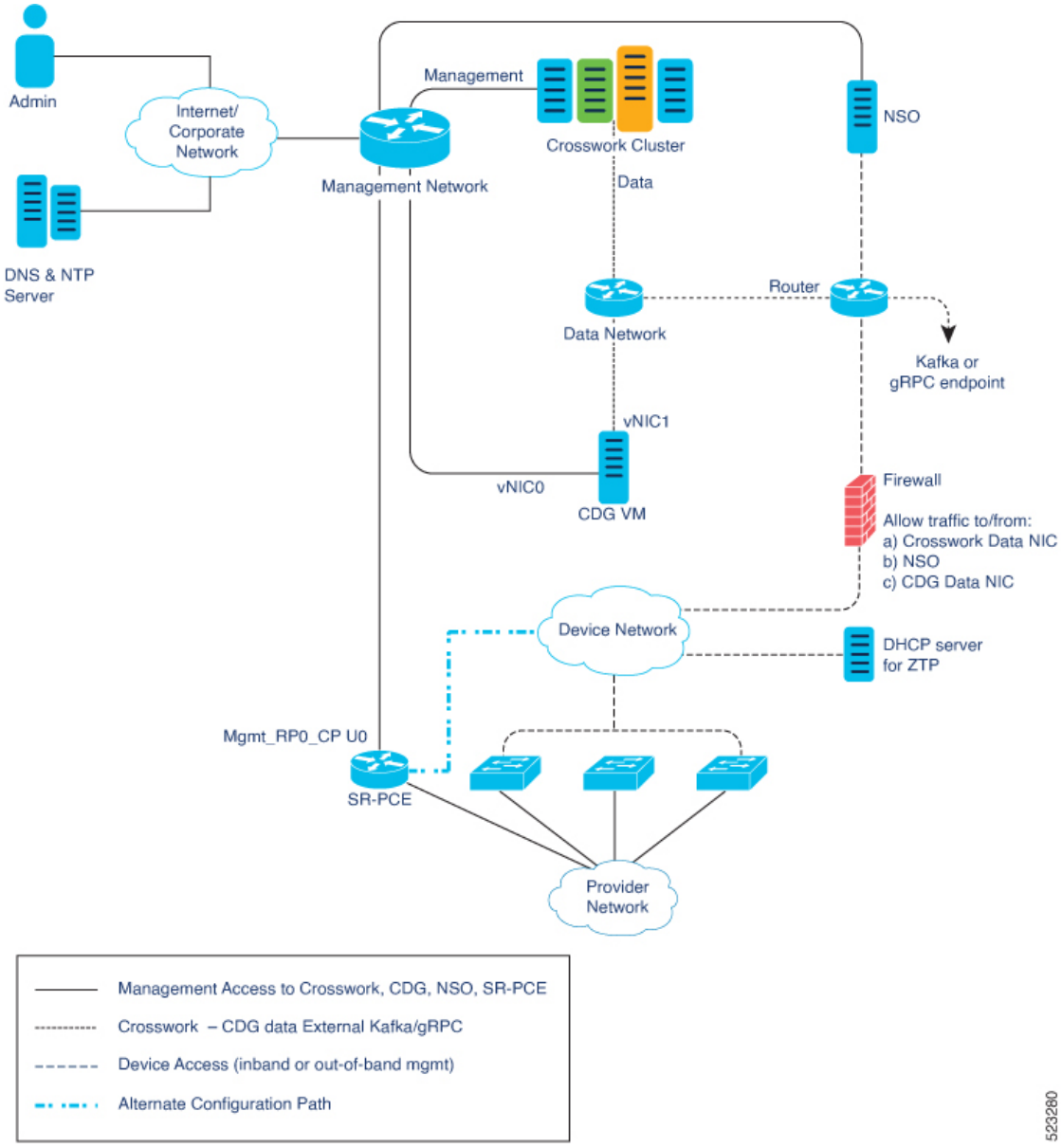
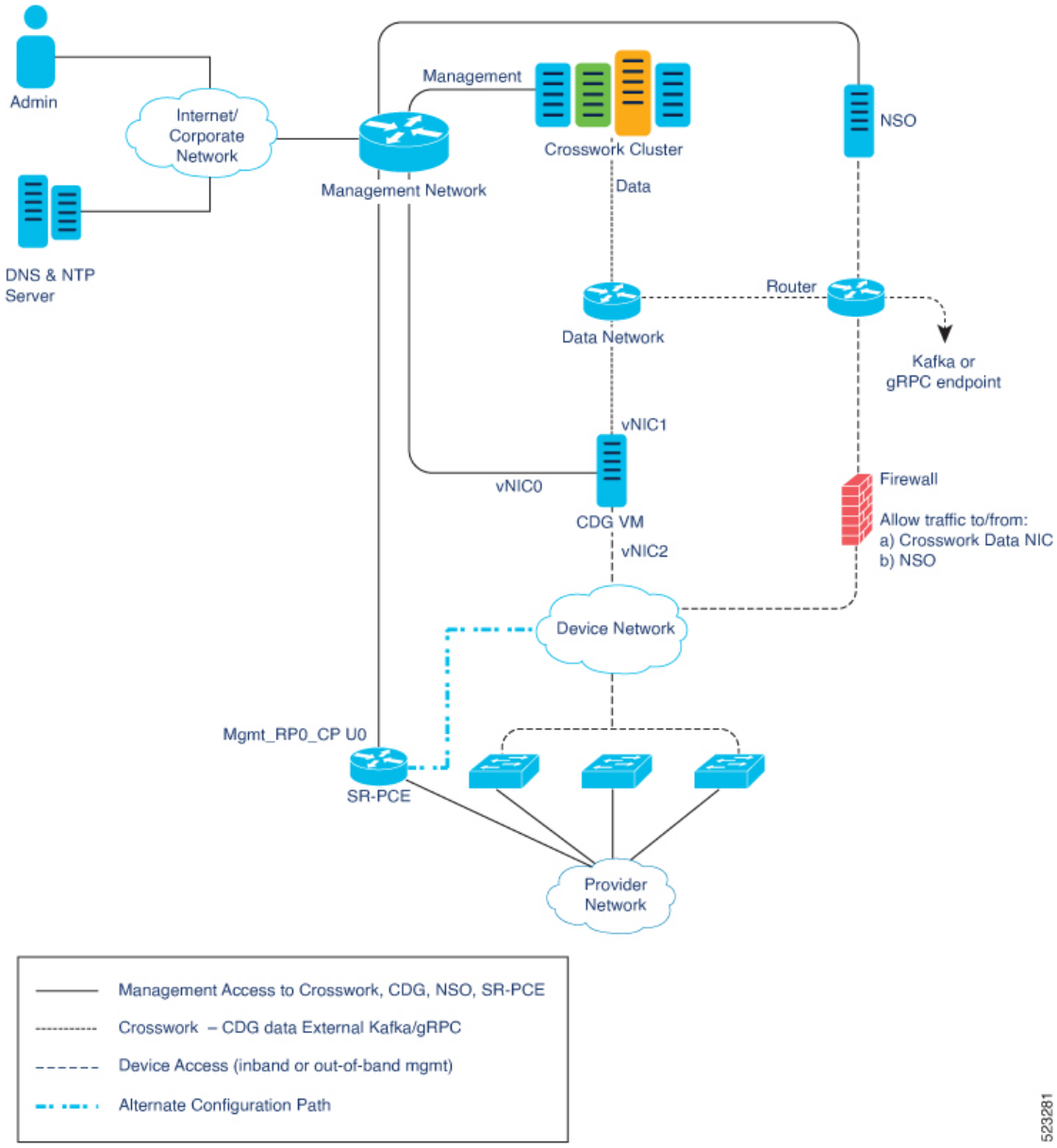


Figure 3: Cisco Crosswork - 3 NIC Network Topology



Cisco Crosswork Virtual Machine (VM)

The Cisco Crosswork VM has the following vNIC deployment options:

Table 2: Cisco Crosswork vNIC deployment modes

No. of vNICs	vNIC	Description
1	Management	Management, Data, and Device access passing through a single NIC (For lab use only)

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

Cisco Crosswork Data Gateway VM

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

Note If you use one interface on your Crosswork cluster, you must use only one interface on the Crosswork Data Gateway. If you use two interfaces on your Crosswork Cluster, then you can use two or three interfaces on the Crosswork Data Gateway as per your network requirements.

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

Table 3: Cisco Crosswork Data Gateway default vNIC deployment modes

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

SR-PCE Configuration

The Segment Routing Path Computation Element (SR-PCE) is both a device and a Software-Defined Networking (SDN) controller. Some deployments may want to treat an SR-PCE instance as a device, in which case they would need access via the device network. Some deployments may want to treat an SR-PCE instance as an SDN controller and access it on the Management routing domain. Crosswork supports both models. By default, Crosswork will use **`eth0`** (Management) to access SR-PCE as an SDN controller on the Management domain (shown in the figures). For more information on enabling Crosswork access to an SR-PCE instance as a device on the device network (shown as alternate path in the figures), please refer to Add Cisco SR-PCE Providers.

ZTP Requirements

If you plan to use Zero Touch Provisioning, the device network needs to be equipped with a DHCP server (not provided as part of Cisco Crosswork). Some forms of ZTP also require a TFTP server (not provided as part of Cisco Crosswork). Additionally, all devices that use ZTP must have network connectivity to the Crosswork cluster as they will pull files (software and/or configuration) directly from the Crosswork cluster. For more information on Zero Touch Provisioning concepts and features, please refer to the *Zero Touch Provisioning* chapter in the *Cisco Crosswork Network Controller 6.0 Administration Guide*.

Cisco Network Services Orchestrator (NSO) VM

The NSO VM has the following vNICs:

- Management: Used for Crosswork applications to reach NSO.
- Device Access: Used for NSO to reach devices or NSO Resource Facing Services (RFS).

VMware Settings

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

- Hypervisor and vCenter supported:
  - VMware vCenter Server 7.0 and ESXi 7.0.
  - VMware vCenter Server 6.7 (Update 3g or later) and ESXi 6.7 (Update 1).
- If you plan to use the Crosswork installer tool, the machine where you run the installer must have network connectivity to the vCenter data center where you plan to install the cluster. If this mandatory requirement cannot be met, you must manually install the cluster. For more information on manual installation, see Manual Installation of Cisco Crosswork using vCenter vSphere UI.
- Cisco Crosswork cluster VMs (Hybrid nodes and Worker nodes) must be hosted on hardware with Hyper Threading disabled.
- As Cisco Crosswork cluster nodes place high demands on the VMs, ensure that you have not oversubscribed CPU or memory resources on the machines hosting the nodes.
- All the physical host machines must be organized within the same VMware Data Center, and while it is possible to deploy all the cluster nodes on a single physical host (provided it meets the requirements), it is recommended that the nodes be distributed across multiple physical hosts. This prevents the host from being a single point of failure and improves solution resilience.
- Ensure that profile-driven storage is enabled by the vCenter admin user. Query permissions for the vCenter user at the root level (for all resources) of the vCenter.
- The networks required for the Crosswork Management and Data networks need to be built and configured in the data centers, and must allow low latency L2 communication (latency with RTT <= 10 ms).

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

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

Property	Value
Promiscuous mode	Reject
MAC address changes	Reject

- The VRRP protocol requires unique router_id advertisements to be present on the network segment. The IDs can vary based on the deployment. For example, Crosswork usually uses the ID 169 on the management and ID 170 on the data network segments when multicast is used in discovery. In case of a symptom of conflict such as the VIP address not being reachable, check if any of the router IDs is duplicated and remove the conflicting VRRP router machines or use a different network.
- Ensure the user account you use for accessing vCenter has the following privileges:
  - VM (Provisioning): Clone VM on the VM you are cloning.
  - VM (Provisioning): Customize on the VM or VM folder if you are customizing the guest operating system.
  - VM (Inventory): Create from the existing VM on the data center or VM folder.
  - VM (Configuration): Add new disk on the data center or VM folder.
  - Resource: Assign VM to resource pool on the destination host, cluster, or resource pool.
  - Datastore: Allocate space on the destination datastore or datastore folder.
  - Network: Assign network to which the VM will be assigned.
  - Profile-driven storage (Query): This permission setting needs to be allowed at the root of the data center tree level.
- We also recommend you to enable vCenter storage control.

Host VM Requirements

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

- Crosswork Cluster VM Requirements, on page 9
- Crosswork Data Gateway VM Requirements, on page 10

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 4: 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 with a latency of less than 10 milliseconds.
IP Addresses	**When using dual NICs** (one for the Management network and one for the Data network): A management and data IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and two additional IP addresses to be used as the Virtual IP (VIP) address (one for the Management network and one for the Data network). **When using single NIC:** One IP address (IPv4 or IPv6) for each node being deployed (Hybrid or Worker) and one additional IP address to be used as the Virtual IP (VIP) address. For example, in the case of a cluster with 3 hybrid VMs and 1 worker VM with a single NIC, you need 5 IP addresses, and in the case of the same configuration with dual NIC, you need 10 IP addresses (5 for management network and 5 for data network). **Note** • The IP addresses must be able to reach the gateway address for the network where Cisco Crosswork Data Gateway will be installed, or the installation will fail. • When deploying a IPv6 cluster, the installer needs to run on an IPv6 enabled container/VM. • At this time, your IP allocation is permanent and cannot be changed without re-deployment. For more information, contact the Cisco Customer Experience team.
NTP Server	The IPv4 or IPv6 addresses or host names of the NTP server you plan to use. If you want to enter multiple NTP servers, separate them with spaces. These should be the same NTP servers you use to synchronize the Crosswork application VM clock, devices, clients, and servers across your network. Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.

Requirement	Description
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.
Backup Server	Cisco Crosswork will back up the configuration of the system to an external server using SCP. The SCP server storage requirements will vary slightly but you must have at least 25 GB of storage.
FQDN (Optional)	The installation process supports using either a VIP (Virtual IP address) or a FQDN (Fully Qualified Domain Name) to access the cluster. If you choose to use the FQDN, you will need one for the Management and one for the Data network. In case of lab installation using single NIC, the FQDN is only required for the Management network. **Note** Secure ZTP and Secure Syslog require the Crosswork cluster to be deployed with FQDN.

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

Crosswork Data Gateway VM Requirements

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

- Selecting the Crosswork Data Gateway Deployment Type, on page 10
- Crosswork Data Gateway VM Requirements, on page 11

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 5: 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 6: Crosswork Data Gateway Requirements for on-premise applications

Requirement	Description
Data Center	VMware. See Installation Prerequisites for VMware vCenter, on page 1.

<table>
<tr><th>Requirement</th><th>Description</th></tr>
<tr><td>Interfaces</td><td>
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.
<table>
<tr><th>No. of NICs</th><th>vNIC0</th><th>vNIC1</th><th>vNIC2</th></tr>
<tr><td>1</td><td>• Management Traffic
• Control/Data Traffic
• Device Access Traffic</td><td>—</td><td>—</td></tr>
<tr><td>2</td><td>Management Traffic</td><td>• Control/Data Traffic
• Device Access Traffic</td><td>—</td></tr>
<tr><td>3</td><td>Management Traffic</td><td>Control/Data Traffic</td><td>Device Access Traffic</td></tr>
</table>
• 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

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

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

Crosswork Cluster Port Requirements

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

Note Crosswork cluster ports allow bidirectional flow of information.

Table 7: External Ports used by Crosswork Cluster

Port	Protocol	Used for	Location (in 2 NIC deployment)
22	TCP	Remote SSH traffic	Management Network / vNIC0
111	TCP/UDP	GlusterFS (port mapper)	Management Network / vNIC0
179	TCP	Calico BGP (Kubernetes)	Management Network / vNIC0
80, 443	TCP	Accessing the EC2 API	Management Network / vNIC0
500	UDP	IPSec	Management Network / vNIC0
2379/2380	TCP	Kubernetes etcd	Management Network / vNIC0
4500	UDP	IPSec	Management Network / vNIC0
6443	TCP	kube-apiserver (Kubernetes)	Management Network / vNIC0
9100	TCP	Kubernetes metamonitoring	Management Network / vNIC0
10250	TCP	kubelet (Kubernetes)	Management Network / vNIC0
24007	TCP	GlusterFS	Management Network / vNIC0
30603	TCP	User interface (NGINX server listens for secure connections on port 443)	Management Network / vNIC0
30606	TCP	Docker Registry	Management Network / vNIC0
30621	TCP	For FTP (available on data interface only). The additional ports used for file transfer are 31121 (TCP), 31122 (TCP), and 31123 (TCP). This port is available only when the supported application is installed on Cisco Crosswork and the FTP settings are enabled.	Management Network / vNIC0

Port	Protocol	Used for	Location (in 2 NIC deployment)
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.	Management Network / vNIC0
49152:49370	TCP	GlusterFS	Management Network / vNIC0

Table 8: Ports used by other Crosswork components

Port	Protocol	Used for	Location (in 2 NIC deployment)
30602	TCP	To monitor the installation (Crosswork Network Controller)	Management Network / vNIC0
30603	TCP	Crosswork Network Controller Web User interface (NGINX server listens for secure connections on port 443)	Management Network / vNIC0
30604	TCP	Used for Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server	Management Network / vNIC0
30607	TCP	Crosswork Data Gateway vitals collection	Data Network / vNIC1
30608	TCP	Data Gateway gRPC channel with Data Gateway VMs	Data Network / vNIC1
30609	TCP	Used by the Expression Orchestrator (Crosswork Service Health)	Management Network / vNIC0
30610	TCP	Used by the Metric Scheduler (Crosswork Service Health)	Management Network / vNIC0
30611	TCP	Used by the Expression Tracker component (Crosswork Service Health)	Management Network / vNIC0
30617	TCP	Used for Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server	Management Network / vNIC0
30620	TCP	Used to receive plug-and-play HTTP traffic on the ZTP server	Management Network / vNIC0
30649	TCP	To set up and monitor Crosswork Data Gateway collection status	Data Network / vNIC1
30650	TCP	The astack gRPC channel with astack-client running on Data Gateway VMs	Data Network / vNIC1
30993, 30994, 30995	TCP	Crosswork Data Gateway sending the collected data to Crosswork Kafka destination	Data Network / vNIC1

Table 9: Destination Ports used by Crosswork Cluster

Port	Protocol	Used for	Location (in 2 NIC deployment)
7	TCP/UDP	Discover endpoints using ICMP	Management Network / vNIC0
22	TCP	Initiate SSH connections with managed devices	Management Network / vNIC0
53	TCP/UDP	Connect to DNS	Management Network / vNIC0
123	UDP	Network Time Protocol (NTP)	Management Network / vNIC0
830	TCP	Initiate NETCONF	Management Network / vNIC0
2022	TCP	Used for communication between Crosswork and Cisco NSO (for NETCONF)	Management Network / vNIC0
8080	TCP	REST API to SR-PCE	Management Network / vNIC0
8888	TCP	Used for communication between Crosswork and Cisco NSO (for HTTPS)	Management Network / vNIC0
20243	TCP	Used by the DLM Function Pack for communication between DLM and Cisco NSO	Management Network / vNIC0
20244	TCP	Used to internally manage the DLM Function Pack listener during a Reload Packages scenario on Cisco NSO	Management Network / vNIC0

Crosswork Data Gateway Port Requirements

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

Inbound: Crosswork Data Gateway listens on the specified ports.

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

Table 10: Ports to be Opened for Management Traffic

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

Note SCP port can be tuned.

Table 11: Ports to be Opened for Device Access Traffic

Port	Protocol	Used for	Direction
161	UDP	SNMP Collector	Outbound
1062	UDP	SNMP Trap Collector 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 Check the platform-specific documentation.	TCP	gNMI Collector	Outbound

Table 12: Ports to be Opened for Control/Data Traffic

Port	Protocol	Used for	Direction
30649	TCP	Crosswork Controller	Outbound
30993 30994 30995	TCP	Crosswork Kafka	Outbound
Site Specific	Site Specific	Kafka and gRPC Destination	Outbound

IP Address Restrictions

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

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

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

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

Table 13: 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.