Plan and Prepare

This chapter provides the prerequisites and planning details needed before starting the installation.

Plan your installation

This topic provides introductory information on how to plan your installation of the SVM (Single Virtual Machine) version of Cisco Crosswork Workflow Manager Solutions and its supporting software.

Installation workflow

To install Cisco Crosswork Workflow Manager Solutions, you must install or configure the following components, in this order:

1. **Install Crosswork SVM server**: Install a Crosswork SVM server to host the primary Cisco Crosswork platform infrastructure. The Crosswork SVM server hosts Crosswork Workflow Manager (CWM) and Crosswork Workflow Manager Solutions (CWM-S).
2. **Install NSO Server**: Install a second, **separate**, native Linux or Linux VM server hosting Cisco Network Services Orchestrator (NSO). NSO performs the direct manipulation of your network devices.
3. **Install CWM and CWM-S CAPPs**: Once the primary Crosswork SVM server is installed and configured, you can install on it the CWM and CWM-S CAPPs[1].
4. **Prepare NSO for package installation**: Before creating the NSO provider and installing the NSO packages from Crosswork, ensure the NSO server is configured properly.
5. **Configure Crosswork Credential Profiles and NSO Provider**: Configure a pair of credential profiles and a single NSO Provider profile. These profiles enable secure communications between Crosswork, your devices, and the NSO server. You create them on the Crosswork server, using the Crosswork server's administrative user interface.
6. **Install NSO Packages**: Install on NSO a set of update packages that allow NSO and Crosswork to share data. You install these on the NSO server from the Crosswork server, using the Crosswork server's administrative user interface.

[1] A CAPP is a **C**rosswork **APP**lication that has been specially packaged for easy installation on the Cisco Crosswork platform.

Choose your Crosswork SVM Server deployment method

You must install the Crosswork server on an SVM (Single Virtual Machine). You can do this using VM hypervisor software from VMware or KVM. If you choose VMware, you also have the option of creating the VM using either Docker or the native VMware vCenter vSphere installation tools. This gives you a choice of three possible deployment methods.

Before making your VM deployment decision, you will want to review the hardware, software, networking, port and other requirements described in Meet installation requirements, on page 2. You will also want to review the information you will need to provide for each deployment option, as detailed in Gather installation parameter values, on page 9. Finally, you will also want to consider whether VMware or KVM best fits your needs.

Meet installation requirements

This document explains the requirements you must meet in order to install Cisco Crosswork Workflow Manager Solutions successfully.

Hardware requirements

Server hardware resources for the virtual machines are as follows:

1. **Crosswork Server Requirements**: The VM hardware requirements for VMware and KVM deployments are similar:
   a. **VMware**: You can install the VMware hypervisor using either vCenter vSphere or Docker tools, on a hardware server other than the one on which NSO is installed. Cisco recommends a server with a minimum of 24 virtual CPUs, 128 GB RAM, and 1 Tb disk storage. Due to their high performance, Cisco recommends solid state drives (SSDs) over hard disk drives (HDDs). If you are using HDDs, their minimum speed should be over 15,000 RPM. The VM data store(s) must have disk-access latency less than 10 ms or greater than 5,000 IOPS.
   b. **KVM**: The server must be running an Intel Xeon CPU E5-2699 v4 at 2.20GHz or better, with a minimum of 24 virtual CPUs, 128 GB RAM, and 1 Tb disk storage, with 2 x 10 Gbps NICs. Install Red Hat Enterprise Linux (RHEL) 9.4 or later. Allocate a 20% buffer for CPU and memory, and a 30% buffer for storage to ensure smooth performance and prevent issues.
2. **NSO Server Requirements**: You can use native Linux or any container-based implementation of your choice. The Cisco NSO installed version must be 6.4.8.1. It must be a system install, ***not a local install*** (see the links to understand the difference and for help ensuring you have the correct installation type). For flexibility reasons, the NSO server must be separate from the Crosswork platform server. The installed

NSO server will also be running Crosswork Workflow Manager function packs, so Cisco recommends an NSO server with a minimum of 16 virtual CPUs, 256 GB RAM, and 1Tb disk storage (which is more than normally required for running basic NSO). Customers who do not already have a separate NSO deployment meeting these requirements may wish to install NSO *after* deploying Crosswork on VMware or KVM. It takes about an hour for the Crosswork platform infrastructure to come up on a VM, and this delay provides plenty of time to install NSO. In addition, before installing the CWM and CWM Solution CAPPs, you must install the pre-requisite NSO packages and perform the additional configurations detailed in NSO package pre-installation tasks.

VMware installation requirements

In addition to meeting the hardware requirements discussed above, Crosswork server installations performed using VMware must meet the following installation requirements (this includes both vSphere and Docker):

- Fleet Upgrade supports the following VMware hypervisor and vCenter versions:
  - VMware vCenter Server 8.0 (U2c or later) and ESXi 8.0 (U2b or later)
  - VMware vCenter Server 7.0 (U3p or later) and ESXi 7.0 (U3p or later)
- Cisco Crosswork SVM must be hosted on hardware with Hyper Threading disabled.
- Ensure that profile-driven storage is enabled by the vCenter admin user. Query permissions for the vCenter user at the root level (for all resources) of the vCenter.
- Cisco recommends that you enable vCenter storage control.
- The networks required for the Crosswork Management and Data networks need to be built and configured in the data centers, and must allow low-latency L2 communication (latency with RTT <= 10 ms).
- Ensure the user account you use for accessing vCenter has the following privileges:
  - VM (Provisioning): Clone VM on the VM you are cloning.
  - VM (Provisioning): Customize on the VM or VM folder if you are customizing the guest operating system.
  - VM (Inventory): Create from the existing VM on the data center or VM folder.
  - VM (Configuration): Add a new disk on the data center or VM folder.
  - Resource: Assign a VM to a resource pool on the destination host or resource pool.
  - Datastore: Allocate space on the destination datastore or datastore folder.
  - Network: Assign the network to which the VM will be assigned.
  - Profile-driven storage (Query): This permission setting needs to be allowed at the root of the data center tree level.

KVM installation requirements

In addition to meeting the hardware requirements discussed above, you will need to perform these steps to set up a Crosswork server deployment using KVM on RHEL:

1. Ensure that your RHEL server supports virtualization. This is typically enabled in the BIOS. To check, use these commands:

- For Intel CPUs: `grep -wo 'vmx' /proc/cpuinfo`
- For AMD CPUs: `grep -wo 'svm' /proc/cpuinfo`

2. Update all the packages on your system to their latest versions using the following command: `sudo dnf update -y`.
3. Reboot the system after all the updates are installed successfully: `sudo reboot`.
4. Install the virtualization tools:
   a. Install the virt-install and virt-viewer tools for creating and interacting with virtual machines: `sudo dnf install virt-install virt-viewer -y`.
   b. Install the libvirt virtualization daemon needed to manage VMs: `sudo dnf install -y libvirt`.
   c. Install virt-manager, a graphical interface for managing VMs: `sudo dnf install virt-manager -y`
   d. Install additional virtualization tools for managing VMs: `sudo dnf install -y virt-top libguestfs-tools`.
5. Run the libvirtd virtualization daemon:
   a. Start the libvirtd daemon: `sudo systemctl start libvirtd`
   b. Enable the libvertd daemon: `sudo systemctl enable libvirtd`
   c. Verify that the daemon is running: `sudo systemctl status libvirtd`
6. Add users to the required groups, for example, libvert and qemu. In the following commands, replace *your_username* with the actual username:

   ```
   sudo usermod --append --groups libvirt your_username
   sudo usermod --append --groups qemu your_username
   ```

7. Ensure that IOMMU is enabled. If it is not enabled, run this command to enable it:

   ```
   grubby --update-kernel=ALL --args=intel_iommu=on
   dmesg | grep -I IOMMU
   ```

8. Check IOMMU and validate the setup. Ensure that all checks show as `PASS`.

   ```
   virt-host-validate
   ```

   If the IOMMU check is not `PASS`, use the following commands to enable it.

   ```
    sudo grubby --update-kernel=ALL --args=intel_iommu=on
   sudo reboot
   ```

9. Ensure that the KVM modules are loaded using this command: `lsmod | grep kvm`

Also see Configure network bridges or SRIOV.

Network requirements

The following table details the network requirements for all VM deployments.

Table 1: Network requirements

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. If using KVM on RHEL: Ensure that the same network name is used and configured on the RHEL bare metal host machine that is hosting the Crosswork VM.
IP Addresses	**IPv4 and/or IPv6 addresses**: Crosswork SVM supports dual stack (simultaneous deployment using IPv4 and IPv6 protocols). The number and type of IP addresses you reserve for Crosswork SVM depends on these factors: • Whether you are deploying using single or dual stack. • Your plans for future growth, flexibility, and implementation of geo redundancy. This is especially important because, at this time, your Crosswork IP allocation is permanent and cannot be changed without re-deployment. Bare-minimum IP address reservations for Crosswork SVM deployments are as follows: • **Single VM single stack** - 4 total: 2 Management, 2 Data (all 4 either IPv4 or IPv6) • **Single VM dual stack** - 8 total: 2 IPv4 Management, 2 IPv4 Data, 2 IPv6 Management, 2 IPv6 Data **Note** • The IP addresses must be able to reach the gateway address for the network, or the installation will fail. • When deploying with IPv6 or dual stack, the installation needs to run on an IPv6 enabled container/VM. • For more information, contact the Cisco Customer Experience team.

Requirement	Description
Interfaces	Crosswork is deployed on a single VM with **2 interfaces**. • **No. of NICs**: 2 • **vNIC0**: Management Traffic (for accessing the interactive console and passing the Control/Data information between servers). • **vNIC1**: Device Access Traffic (for device access and data collection). **Note** Due to security policies, traffic from subnets of a vNIC received on other vNICs is dropped. For example, in a setup with two vNICs, all device traffic (incoming and outgoing) must be routed through the default vNIC1.
NTP Server	The IPv4 and/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.
DNS Servers	The IPv4 and/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 an FQDN (Fully Qualified Domain Name) to access the VM. If you choose to use the FQDN, you will need one for the Management and one for the Data network. **Note** If you choose to supply the FQDNs during the initial installation, the DNS server must be populated with them before the VM is powered on; otherwise, the installation script will fail to complete the environment setup.

Management port requirements

The following table details the management-network port requirements for all installations.

Table 2: Ports used by Crosswork single VM deployment on the management network

Port	Protocol	Used for	Direction
30602	TCP	Monitoring the installation (Crosswork Network Controller)	Inbound
30603	TCP	Crosswork Network Controller Web user interface (NGINX server listens for secure connections on port 443)	Inbound
30604	TCP	Classic Zero Touch Provisioning (Classic ZTP) on the NGINX server	Inbound
30653	TCP	Raft peer cluster communication port	Inbound
30617	TCP	Secure Zero Touch Provisioning (Secure ZTP) on the ZTP server	Inbound
30620	TCP	Receiving plug-and-play HTTP traffic on the ZTP server	Inbound
7	TCP/UDP	Discovering endpoints using ICMP	Outbound
22	TCP	Initiating SSH connections with managed devices	Outbound
22	TCP	Remote SSH connection	Inbound
53	TCP/UDP	Connecting to DNS	Outbound
123	UDP	Network Time Protocol (NTP)	Outbound
830	TCP	Initiating NETCONF	Outbound

Device port requirements

The following table details the device-network port requirements for both server installations.

When configuring the ports for Embedded Collectors, ensure that the ports mentioned in the following table are configured on the device. For example, in case the port used for sending traps was previously set to 1062, change it to a port that is within the acceptable range for deploying a single virtual machine. The acceptable range is provided with the port number in the following table.

Table 3: Ports used by Crosswork single VM deployment on the Device Network

Port	Protocol	Used for	Direction
161	UDP	SNMP Collector	Outbound
31062 Accepted range of ports is 30160–31560	UDP		Inbound
22	TCP	CLI Collector	Outbound
30614 Accepted range of ports is 30160–31560	TLS	Syslog Collector This is the default value. You can change this value after installation from the Cisco Crosswork UI.	Inbound
30898 Accepted range of ports is 30160–31560	TCP		
30514 Accepted range of ports is 30160–31560	UDP		
30621	TCP	An active FTP server is required. FTP (available on data interface only). The additional ports used for file transfer are 31121 (TCP), 31122 (TCP), and 31123 (TCP). This port is available only when the supported application is installed on Cisco Crosswork and the FTP settings are enabled.	Inbound
30622	TCP	An active SFTP server is required. SFTP (available on data interface only) This port is available only when the supported application is installed on Cisco Crosswork and the SFTP settings are enabled.	Inbound
Site Specific[2]	TCP	gNMI collector	Outbound
Site Specific[3]	Site Specific	Kafka and gRPC destination	Outbound

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

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

Additional requirements

Supported browsers: Google Chrome (Version 131.0.x) and Mozilla Firefox (134.0.1). For full functionality, browsers must have JavaScript and cookies enabled.

Site preparation: The user network environment must include the following:

- All network devices need access to the data network. The data network is the portion of the network dedicated to the transmission of user data, as opposed to the management network, which is optimized for IT management and control traffic.
- The Cisco Software Download feature requires access to the Internet from the server, and a Cisco customer username and password with authorization to download images from software.cisco.com.

Gather installation parameter values

The tables below describe important parameter values you will need to specify either in GUI or in installation templates while installing Crosswork in VMware or KVM deployments. Before installation, be sure that you have the relevant values to supply for each of the parameters mentioned in the tables.

General parameters

These parameters are used in both VMware and KVM installations.

Table 4: General parameters

Parameter Name	Description
`ClusterIPStack`	The IP stack protocol: `IPv4`, `IPv6` or `dualstack`.
`ManagementIPAddress`	The Management IP address of the VM (IPv4 and/or IPv6).
`ManagementIPNetmask`	The Management IP subnet in dotted decimal format (IPv4 and/or IPv6).
`ManagementIPGateway`	The Gateway IP on the Management Network (IPv4 and/or IPv6). The address must be reachable, otherwise the installation will fail.
`ManagementVIP`	The Management Virtual IP for the Crosswork VM.
`DataIPAddress`	The Data IP address of the VM (IPv4 and/or IPv6).
`DataIPNetmask`	The Data IP subnet in dotted decimal format (IPv4 and/or IPv6).
`DataIPGateway`	The Gateway IP on the Data Network (IPv4 and/or IPv6). The address must be reachable, otherwise the installation will fail.

Parameter Name	Description
`DataVIP`	The Data Virtual IP for the Crosswork VM.
`DNS`	The IP address of the DNS server (IPv4 and/or IPv6). The address must be reachable, otherwise the installation will fail.
`NTP`	NTP server address or name. The address must be reachable, otherwise the installation will fail.
`DomainName`	The domain name used for the VM.
`CWPassword`	Password to log into Cisco Crosswork. When setting up a VM, ensure the password is strong and meets the following criteria: • It must be at least 8 characters long and include uppercase and lowercase letters, numbers, and at least one special character. • The following special characters are not allowed: backslash (\), single quote ('), or double quote ("). • Avoid using passwords that resemble dictionary words (such as "Pa55w0rd!"). While such passwords may meet the specified criteria, they are considered weak and will be rejected, resulting in a failure to set up the VM.
`VMSize`	Size of the VM. For Crosswork Workflow Manager Solutions deployments, specify the `"XLarge"` profile.
`VMName`	Name of the VM.
`NodeType`	Indicates the type of VM. Choose **Hybrid**.
`IsSeed`	Set to `"True"`.
`InitNodeCount`	Set value to **1**.
`InitMasterCount`	Set value to **1**.
`BackupMinPercent`	Minimum percentage of the data disk space to be used for the size of the backup partition. The default value is 35 (valid range is from 1 to 80). Please use the default value unless recommended otherwise. **Note** The final backup partition size will be calculated dynamically. This parameter defines the minimum.
`ThinProvisioned`	Set to **false** for production deployments.

Parameter Name	Description
`SchemaVersion`	The configuration Manifest schema version. This indicates the version of the installer to use with this template. Schema version should map to the version packaged with the sample template in the installer tool on cisco.com. You should always build a new template from the default template provided with the release you are deploying, as template requirements may change from one release to the next.
`LogFsSize`	Log partition size (in gigabytes). Minimum value is 20 GB and Maximum value is 1000 GB. If left blank, the default value (20 GB) is selected.
`EnableSkipAutoInstallFeature`	Pods marked as "skip auto install" will not be brought up unless explicitly requested by a dependent application or pod. By default, the value is set as `"False"`. For Crosswork Workflow Manager Solutions deployment, you must set the value as `"True"`. **Note** • If left blank, the default value (`"False"`) is automatically selected. • This parameter accepts a string value, so be sure to enclose the value in double quotes.
`EnforcePodReservations`	Enforces minimum resource reservations for the pod. If left blank, the default value (`"True"`) is selected. This parameter accepts a string value, so be sure to enclose the value in double quotes.
`K8sServiceNetwork`	The network address for the kubernetes service network. By default, the CIDR range is fixed to '/16'.
`K8sPodNetwork`	The network address for the kubernetes pod network. By default, the CIDR range is fixed to '/16'.

Parameter Name	Description
`IgnoreDiagnosticsCheckFailure`	Used to set the system response in case of a diagnostic-check failure. If set to `"False"`, the installation will terminate if the diagnostic check reports an error. If set to `"True"`, the diagnostic check will be ignored, and the installation will continue. The default value is `"False"`. Cisco recommends that you leave the value set to `"False"` whenever you are installing in a production environment. If the installation is failing with this setting, contact Cisco Customer Experience. This parameter accepts a string value, so be sure to enclose the value in double quotes. **Note** • The log files (`diagnostic_stdout.log` and `diagnostic_stderr.log`) can be found at **/var/log**. The result from each diagnostic execution is kept in a file at **/home/cw-admin/diagnosis_report.txt**. • Use **diagnostic all** command to invoke the diagnostic manually on day N. • Use **diagnostic history** command to view previous test report.
`ManagementVIPName`	Name of the Management Virtual IP for the Crosswork VM. This is an optional parameter used to reach the Crosswork Management VIP via a DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server.
`DataVIPName`	Name of the Data Virtual IP for the Crosswork VM. This is an optional parameter used to reach the Crosswork Data VIP via a DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server.
`EnableHardReservations`	Determines the enforcement of VM CPU and Memory profile reservations. This is an optional parameter and the default value is `"True"`, if not explicitly specified. This parameter accepts a string value, so be sure to enclose the value in double quotes. If set as `"True"`, the VM's resources are provided exclusively. In this state, the installation will fail if there are insufficient CPU cores, memory or CPU cycles. If set as `"False"` (only set for lab installations), the VM's resources are provided on best efforts. In this state, insufficient CPU cores can impact performance or cause installation failure.

Parameter Name	Description
`ManagerDataFsSize`	This parameter is applicable only when installing with the Docker installer tool. Refers to the data disk size for the Crosswork node (in gigabytes). This is an optional parameter and the default value is 485 (valid range is from 485 to 8000), if not explicitly specified. Please use the default value unless recommended otherwise.
`RamDiskSize`	Size of the RAM disk. This parameter is only used for lab installations (value must be at least 2). When a non-zero value is provided for `RamDiskSize`, the `HSDatastore` value is not used.

`Timezone`	Enter the timezone name. The name must be a standard IANA "TZ" timezone name in English (for example, "America/Chicago"). The name is a string value, so be sure to enclose it in double quotes.
	
	You can find the authoritative list of IANA TZ timezone names at https://data.iana.org/time-zones/tzdb-2021a/zone1970.tab. You can also see the list by entering the following at any Ubuntu command line:
	
	`timedatectl list-timezones`
	
	Setting the TZ timezone in this manner is optional. If you leave this field blank, the VM will set the system clock when it boots and connects to your local NTP server. The system clock will then use the NTP server's UTC protocol. UTC ensures proper server time synchronization across the network but does not provide local timezone or DST adjustments, which can complicate global network management unless your organization has a defined policy for implementing the NTP protocol. For help with this, see Use Best Practices for Network Time Protocol.
	
	If you later decide you want to use an IANA "TZ" timezone name, you can set one using the CNC server VM's command line, as follows:
	
	1. Access the command line of the CNC server VM:
	
	`ssh cw-admin@VMIPaddress`
	
	2. Switch to the administrative user (you may be prompted for the administrative password):
	
	`sudo su`
	
	3. Set the timezone, using the IANA TZ name you have selected:
	
	`timedatectl set-timezone TZName`
	
	4. Confirm that the setting was accepted:
	
	`timedatectl status`

VMware parameters

If you plan to specify a VMware deployment, you will need to configure the following parameters in your VMware GUI options or VMware template.

Table 5: VMware GUI or template parameters

Parameter Name	Description
`VCenterAddress`	The vCenter IP or host name.
`VCenterUser`	The username needed to log into vCenter.
`VCenterPassword`	The password needed to log into vCenter.
`DCname`	The name of the Data Center resource to use. Example: `DCname = "WW-DCN-Solutions"`
`MgmtNetworkName`	The name of the vCenter network to attach to the VM's Management interface. This network must already exist in VMware or the installation will fail.
`DataNetworkName`	The name of the vCenter network to attach to the VM's Data interface. This network must already exist in VMware or the installation will fail.
`Host`	The ESXi host, or ONLY the vCenter VM/resource group name where the VM is to be deployed. The primary option is to use the host IP or name (all the hosts should be under the data center). If the hosts are under a VM in the data center, only provide the VM name (all hosts within the VM will be picked up). The subsequent option is to use a resource group. In this case, a full path should be provided. Example: `Host = "Main infrastructure/Resources/00_trial"`
`Datastore`	The datastore name available to be used by this host or resource group. The primary option is to use host IP or name. The subsequent option is to use a resource group. Example: `Datastore = "SDRS-DCNSOL-prodexsi/bru-netapp-01_FC_Prodesx_ds_15"`
`HSDatastore`	The high speed datastore available for this host or resource group. When not using a high speed data store, set to same value as Datastore.
`Cw_VM_Image`	The name of Crosswork VM image in vCenter. This value is set as an option when running the installer tool and does not need to be set in the template file.
`HostedCwVMs`	The ID of the VM to be hosted by the ESXi host or resource.

Dual-Stack Parameters

If you plan to specify a dual-stack deployment, you will need to configure the following IPv4 and IPv6 versions of values for the following Management, Data, and DNS parameters.

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