Cisco Crosswork Workflow Manager Solutions 2.1 Installation Guide

First Published: 2026-01-30

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

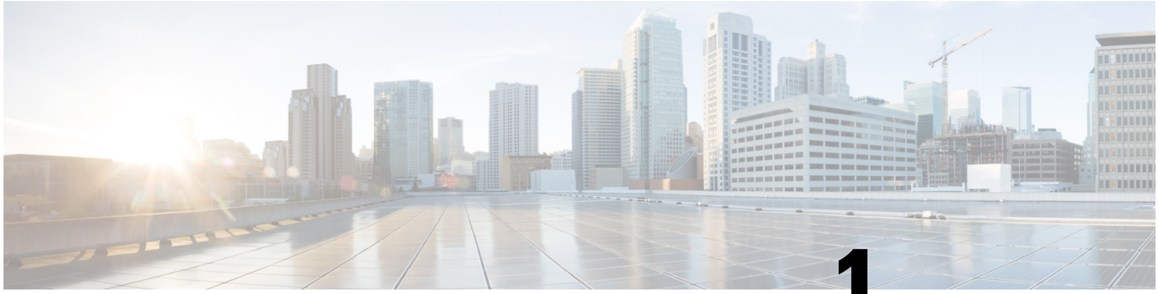
IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

CONTENTS



CHAPTER 1

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, on page 45.

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, on page 29.

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`

CHAPTER 2

VMware installation

This chapter covers the steps to install Crosswork Workflow Manager Solutions on VMware.

Install Crosswork on VMware using vSphere

Follow these steps to deploy Crosswork on a single VM using the VMware vSphere user interface.

Before you begin

Ensure that:

- You are familiar with the workflow and deployment decisions explained in Plan your installation, on page 1.
- The VMware host you have selected meets the requirements specified in Hardware requirements, on page 2 and VMware installation requirements, on page 3.
- The network is configured to meet all the requirements specified in Network requirements, on page 4
- The ports on the host and your devices are configured to meet the requirements specified in Management port requirements, on page 6 and Device port requirements, on page 7.
- You have assembled all of the installation values you will need, as specified in Gather installation parameter values, on page 9.

Attention The download file names given in this topic are subject to change. You can always find the latest versions by pointing your browser to https://software.cisco.com/download/home and searching for **Crosswork Network Controller** > **All Release**.

Procedure

Step 1 Install a supported version of VMware ESXi on the machine you plan to use as the Crosswork server.

Step 2 From Cisco Software Central, download the latest version of the Cisco Crosswork platform image file to a storage location on the same system: `cnc-workflowmanager-single-node-deployment-7.2.0-45.ova`.

Step 3 With VMware ESXi running, log into the VMware vSphere Web Client. On the left navigation pane, choose the ESXi host where you want to deploy the VM.

Step 4 In the vSphere UI, go to **Host** > **Configure** > **Networking** > **Virtual Switches** and select the virtual switch for the Management Network that will be used to access the UI of the VM. In the virtual switch, select **Edit** > **Security**, and configure the following DVS port group properties:

- Set **Promiscuous mode** as *Reject*
- Set **MAC address changes** as *Reject*

Confirm the settings and repeat the process for the virtual switch that will be used for the Data Network.

Step 5 Review and confirm that your network settings meet the requirements.

Ensure that the networks that you plan to use for Management Network and Data network are connected to the host. Contact your Cisco Experience team for assistance.

Step 6 Choose **Actions** > **Deploy OVF Template**.

Caution

The default VMware vCenter deployment timeout is 15 minutes. If vCenter times out during deployment, the resulting VM will not be bootable. To prevent this, we recommend that you document the choices (such as IP address, gateway, DNS server, etc.) so that you can enter the information quickly and avoid any issues with the VMware configuration.

Step 7 The VMware **Deploy OVF Template** window appears, with the first step, **1 - Select an OVF template**, highlighted. Click **Choose Files** to navigate to the location where you downloaded the OVA image file and select it. Once selected, the file name is displayed in the window.

Step 8 Click **Next**. The **Deploy OVF Template** window is refreshed, with **2 - Select a name and folder** now highlighted. Enter a name and select the respective data center for the Cisco Crosswork VM you are creating.

We recommend that you include the Cisco Crosswork version and build number in the name, for example: Cisco Crosswork 7.2 Build 48.

Step 9 Click **Next**. The **Deploy OVF Template** window is refreshed, with **3 - Select a compute resource** highlighted. Select the host for your Cisco Crosswork VM.

Step 10 Click **Next**. The VMware vCenter Server validates the OVA. Network speed will determine how long validation takes. After the validation is complete, the **Deploy OVF Template** window is refreshed, with **4 - Review details** highlighted.

Step 11 Review the OVF template that you are deploying. This information is gathered from the OVF, and cannot be modified.

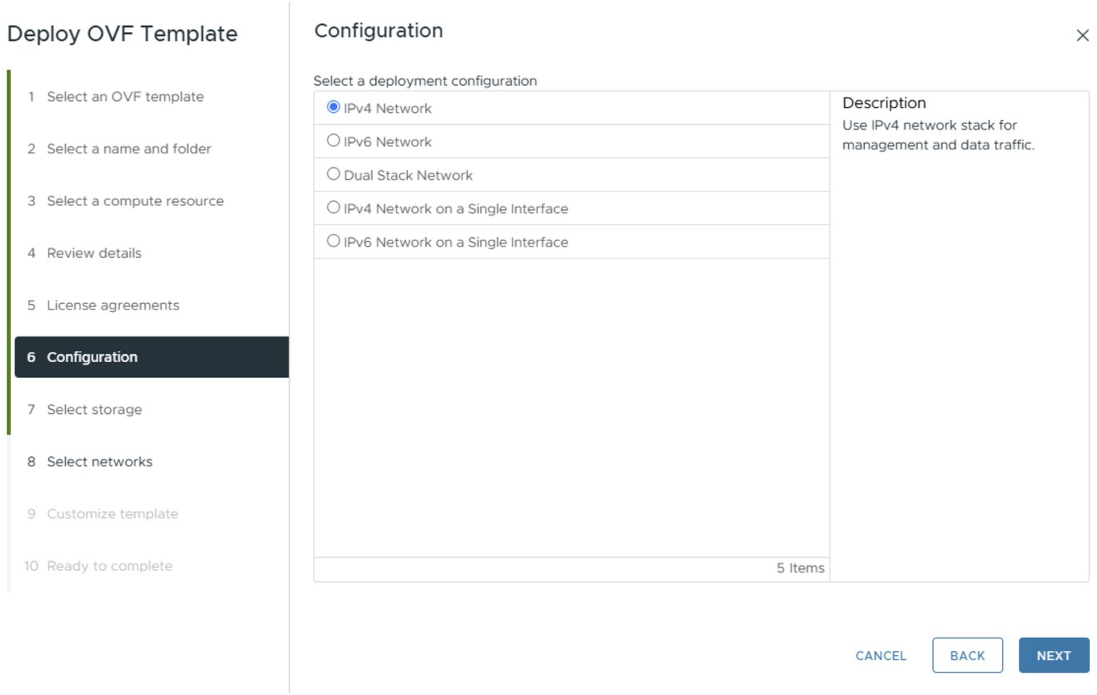
Note

You may see alerts regarding the OVF package containing advanced configuration options and/or about trusted certificates. These are common and you can safely select the "Ignore" option.

Step 12 Click **Next**. The **Deploy OVF Template** window is refreshed, with **5 - License agreements** highlighted. Review the End User License Agreement and if you agree, click the **I accept all license agreements** checkbox. Otherwise, contact your Cisco Experience team for assistance.

Step 13 Click **Next** The **Deploy OVF Template** window is refreshed, with **6 - Configuration** highlighted. Choose the desired deployment configuration.

Figure 1: Select a deployment configuration



Deploy OVF Template

Configuration

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Select a deployment configuration

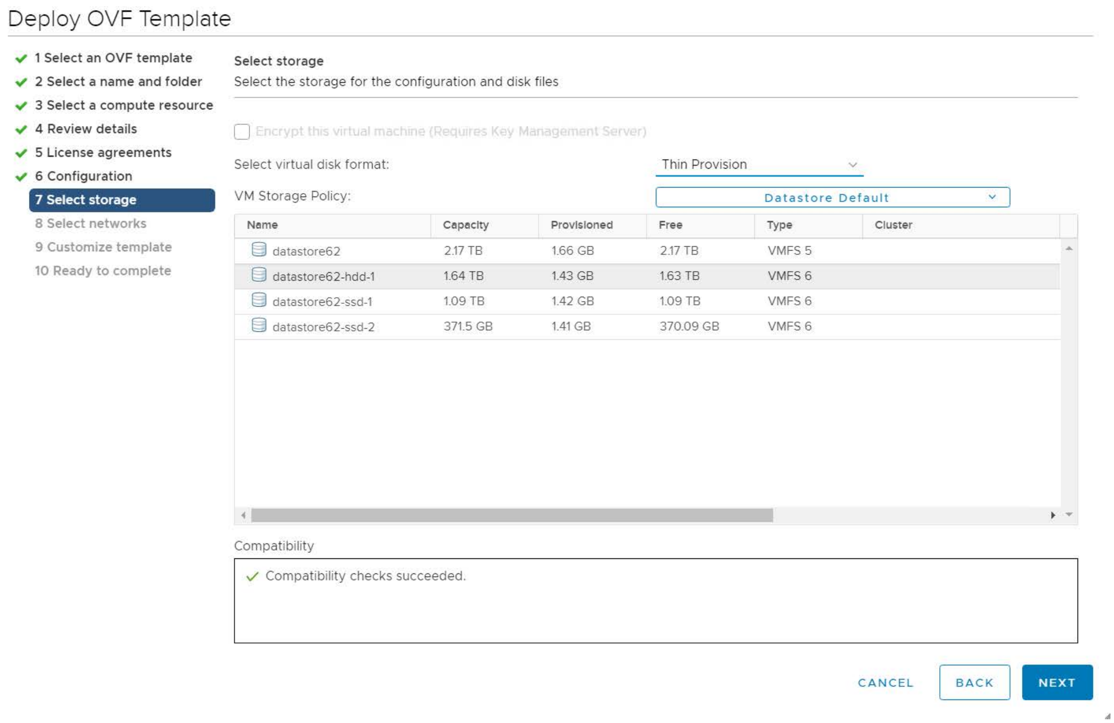
● IPv4 Network
○ IPv6 Network
○ Dual Stack Network
○ IPv4 Network on a Single Interface
○ IPv6 Network on a Single Interface

5 Items

Description
Use IPv4 network stack for management and data traffic.

Step 14 Click **Next**. The **Deploy OVF Template** window is refreshed, with **7 - Select Storage** highlighted. Choose the relevant option from the **Select virtual disk format** drop-down list. From the table, choose the datastore you want to use, and review its properties to ensure there is enough available storage.

Figure 2: Select Storage



Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select the storage for the configuration and disk files

□ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thin Provision

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
datastore62	2.17 TB	1.66 GB	2.17 TB	VMFS 5	
datastore62-hdd-1	1.64 TB	1.43 GB	1.63 TB	VMFS 6	
datastore62-ssd-1	1.09 TB	1.42 GB	1.09 TB	VMFS 6	
datastore62-ssd-2	371.5 GB	1.41 GB	370.09 GB	VMFS 6	

Compatibility

✓ Compatibility checks succeeded.

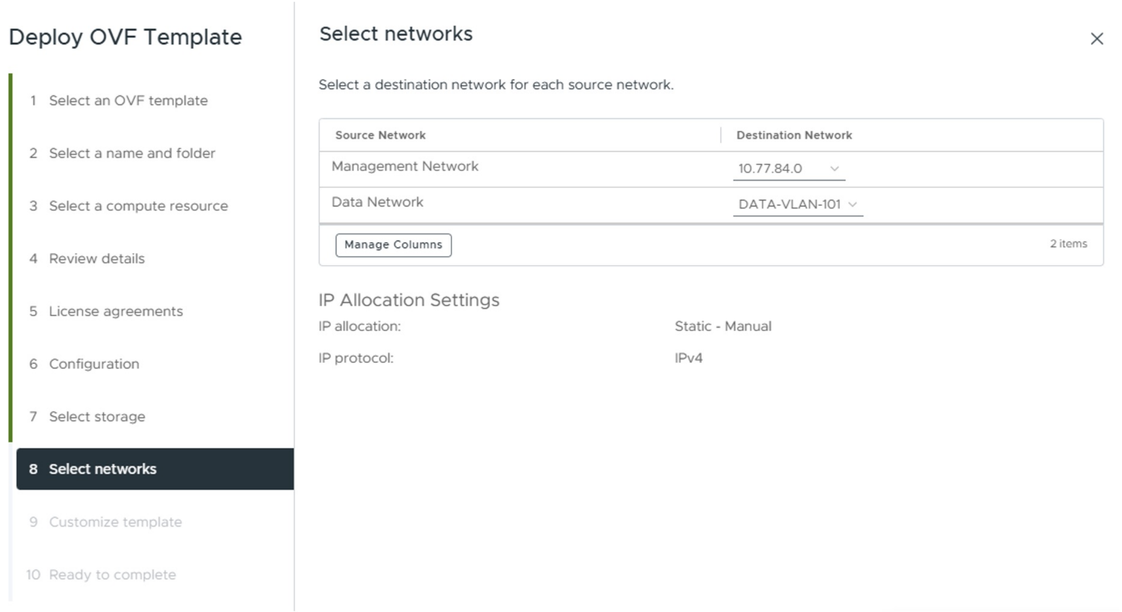
Note

For production deployment, choose the **Thick Provision Eager Zeroed** option because this will preallocate disk space and provide the best performance. For lab purposes, we recommend the **Thin Provision** option because it saves disk space.

Crosswork does not support the 2TB option for single VM installations.

Step 15 Click **Next**. The **Deploy OVF Template** window is refreshed, with **8 - Select networks** highlighted. From the **Destination Network** drop-down list, select the proper networks for the Management Network and the Data Network.

Figure 3: Select networks



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Configuration
7 Select storage
8 Select networks
9 Customize template
10 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Management Network	10.77.84.0
Data Network	DATA-VLAN-101

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

Step 16 Click **Next**. The **Deploy OVF Template** window is refreshed, with **9 - Customize template** highlighted.

a) Expand the **Management Network** settings. Provide information for the IPv4 and/or IPv6 deployment (as per your selection) such as IP address, IP netmask, IP gateway, virtual IP address, and virtual IP DNS name.

b) Expand the **Data Network** settings. Provide information for the IPv4 and/or IPv6 deployment (as per your selection) such as IP address, IP netmask, IP gateway, virtual IP address, and virtual IP DNS name.

c) Expand the **Deployment Credentials** settings. Enter relevant values for the VM Username and Password.

Note
Avoid using passwords that resemble dictionary words (for example, 'Pa55w0rd!') or easily guessable patterns. While such passwords might meet the initial criteria, they are considered weak and could cause the VM setup to fail without a clear explanation. To ensure a successful installation, use a complex password with a minimum of 8 characters that combines uppercase and lowercase letters, numbers, and special characters in a non-predictable sequence.

d) Expand the **DNS and NTP Servers** settings. According to your deployment configuration (IPv4 and/or IPv6), the fields that are displayed are different. Provide information in the following three fields:

- **DNS IP Address**: The IP addresses of the DNS servers you want the Cisco Crosswork server to use. Separate multiple IP addresses with spaces.
- **NTP Servers**: The IP addresses or host names of the NTP servers you want to use. Separate multiple IPs or host names with spaces.
- **DNS Search Domain**: The name of the DNS search domain.
- **Timezone**: Enter the timezone details. Default value is UTC.

Note
The DNS and NTP servers must be reachable using the network interfaces you have mapped on the host. Otherwise, the configuration of the VM will fail.

e) Expand the **Disk Configuration** settings. Provide relevant values for these fields:

- **Logfs Disk Size**
- **Datafs Disk Size**
- **Corefs Partition Size**
- **High Speed Disk Size**
- **Minimum backup partition size**

The default disk configuration settings should work for most environments. Change the settings only if you are instructed to by the Cisco Customer Experience team.

f) Expand **Crosswork Configuration** and enter your legal disclaimer text (users will see this text if they log into the CLI).

g) Expand **Crosswork Cluster Configuration**. Provide relevant values for these fields:

- **VM Type**: Choose **Hybrid**.
- **Cluster Seed node**: Choose **True**.
- **Crosswork Management Cluster Virtual IP**: Enter virtual IP of the management network.
- **Crosswork Management Cluster Virtual IP Name**: Enter DNS hostname of virtual IP interface of the management network.
- **Crosswork Data Cluster Virtual IP**: Enter virtual IP of the data network.
- **Crosswork Data Cluster Virtual IP Name**: Enter DNS hostname of virtual IP interface of the data network.
- **Initial hybrid node count**: Set to 1.
- **Initial total node count**: Set to 1.
- **Location of VM**: Enter the geographical location of VM.
- **Disclaimer**: Enter your legal disclaimer text (users will see this text if they log into the CLI).
- **Installation type**: Not applicable to single VM deployment. Do not select any checkbox.
- **Enable Skip Auto Install Feature**: Set to **True**.
- **Auto Action Manifest Definition**: Use the default value (Empty).
- **Product specific definition**: Enter the product specific definition.
- **Ignore Diagnostic Failure?**: Use the default value (**False**).

Step 17 Click **Next**. The **Deploy OVF Template** window is refreshed, with **10 - Ready to Complete** highlighted.

Step 18 Review your settings and then click **Finish** if you are ready to begin deployment. Wait for the deployment to finish before continuing. To check the deployment status:

a) Open a VMware vCenter client.

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

Step 19 Once the deployment is completed, right-click on the VM and select **Edit Settings**. The **Edit Settings** dialog box is displayed. Under the **Virtual Hardware** tab, update these attributes:

- **VM profile**: `XLarge`
- **CPU**: `24`
- **Memory**: `128 GB`

Click **OK** to save the changes.

Step 20 Power on the Crosswork VM. To power on, expand the host's entry, click the Cisco Crosswork VM, and then choose **Actions** > **Power** > **Power On**.

The time taken to create the VM can vary based on the size of your deployment profile and the performance characteristics of your hardware. To track creation of the VM and success of the installation, follow the steps in Monitor Crosswork Server Activation, on page 37.

Install Crosswork on VMware using Docker

Follow these steps to deploy Crosswork on a single VM using the Docker installer tool.

Before you begin

Ensure that:

- Python is installed on the machine where you are downloading software. If you do not have Python installed, go to python.org and download the version of Python that is appropriate for your work station before beginning the installation.
- You are familiar with the workflow and deployment decisions explained in Plan your installation, on page 1.
- The VMware host you have selected meets the requirements specified in Hardware requirements, on page 2 and .
- The network is configured to meet all the requirements specified in Network requirements, on page 4
- The ports on the host and your devices are configured to meet the requirements specified in Management port requirements, on page 6 and .
- You have assembled all of the installation values you will need, as specified in Gather installation parameter values, on page 9.

During and after the install, note that:

- The edited template in the `/data` directory contains sensitive information (VM passwords and the vCenter password). It will be your responsibility to manage access to this content. Cisco recommends that you store the templates used for your install in a secure environment or edit them to remove the passwords.
- During the install, the files `install.log`, `install_tf.log`, and `.tfstate` will be created and stored in the `/data` directory. If you encounter trouble with the installation and must open a case with the Cisco Customer Experience team, please remember to provide these files to the team.

- The install script is safe to run multiple times. Upon error, input parameters can be corrected and re-run. You must remove the `install.log`, `install_tf.log`, and `tfstate` files before each re-run. Running the Docker installer tool multiple times may result in the deletion and re-creation of VMs.
- In order to change install parameters or to correct parameters following installation errors, it is important to distinguish whether the installation has managed to deploy the VM successfully or not. You can detect that a VM was deployed successfully if the installer provides output similar to the following:

```
vsphere_virtual_machine.crosswork-IPv4-vm["1"]: Creation complete after 2m50s
[id=4214a520-c53f-f29c-80b3-25916e6c297f]
```

- If you use the same installer tool for multiple Crosswork installations, it is important to run the tool from different local directories, allowing for the deployment-state files to be independent. The simplest way to do this is to create a local directory on the host for each deployment, and map each new local directory to the container accordingly.

Be aware that:

- Docker version 19 or higher is required while using the installer tool. For more information on Docker, see https://docs.docker.com/get-docker/.
- Crosswork installed on a single VM does not currently support VMware vCenter storage folders or datastores organized under a virtual folder structure. Ensure that the datastores referenced are not grouped under a folder.

Attention The download file names given in this topic are subject to change. You can always find the latest versions by pointing your browser to https://software.cisco.com/download/home and searching for **Crosswork Network Controller** > **All Release**.

Procedure

Step 1 In your Docker-capable machine, create a directory where you will store everything you will use during this installation.

Note
If you are using a Mac, ensure that the directory name is in lower case.

Step 2 From https://software.cisco.com/download/home, download the Crosswork platform installer bundle (.tar.gz) and OVA image file to the directory you created previously: `CW-CWM-Solutions-Advantage-2.1.0-14-SVM-7.2.0-45-ova.signed.bin`.

Step 3 Use the following command to extract the installer bundle:

```
tar -xvf cnc-workflowmanager-single-node-docker-deployment-7.2.0-45.tar.gz
```

The contents of the installer bundle are unzipped to a new directory (e.g. `cnc-workflowmanager-single-node-docker-deployment-7.2.0-45`). The extracted files will contain the installer image (`cw-na-cnc-workflowmanager-svm-installer-7.2.0-45.tar.gz`) and files necessary to validate the image.

Step 4 Review the contents of the README file to understand everything that is in the package and how it will be validated in the following steps.

Step 5 If you don't already know the version of python installed on your workstation, use the following command to detect it:

```
python --version
```

Step 6 Use the following command to verify the signature of the installer image:

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

```
python cisco_x509_verify_release.py -e filename.cer -i filename.tar.gz -s Signaturefilename.tar.gz
-v dgst -sha512
```

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

```
python3 cisco_x509_verify_release.py3 -e filename.cer -i filename.tar.gz -s Signaturefilename.tar.gz
-v dgst -sha512
```

Step 7 Use the following command to load the installer image file into your Docker environment.

```
docker load -i filename.tar.gz
```

For example:

```
docker load -i cw-na-cnc-workflowmanager-svm-installer-7.2.0-45.tar.gz
```

Step 8 Run the Docker image list or Docker images command to get the "image ID" (which is needed in the next step).

For example:

```
docker images
```

The result will be similar to the following: (the output section we will need is underlined for clarity)

```
My Machine% docker images
REPOSITORY                       TAG                                                      IMAGE ID
       CREATED        SIZE
dockerhub.cisco.com/cw-installer  cnc-workflowmanager-svm-7.2.0-45   a4570324fad30  7 days ago
 276MB
```

Note
Pay attention to the "CREATED" time stamp in the table presented when you run `docker images`, as you may have other images present from the installation of prior releases. If you want to remove these, use the `docker image rm {image id}` command.

Step 9 Launch the Docker container using the following command:

```
docker run --rm -it -v `pwd`:/data image id of the installer container
```

To run the image loaded in our example, you would use the following command:

```
docker run --rm -it -v `pwd`:/data a4570324fad30
```

Note

- You do not have to enter the full image ID value. Docker requires only enough of the image ID to uniquely identify the image you want to use for the installation. In our example, a command like ``docker run --rm -it -v `pwd`:/data a45`` would also be adequate.
- In the above command, we are using the backtick (`). Do not use the single quote or apostrophe ('), as this means something very different to the shell. By using the backtick, the template and OVA files will be stored in the current directory where you are located on your local disk when you run the commands, instead of inside the container.
- When deploying an IPv6 setup, the installer needs to run on an IPv6-enabled container/VM. This requires additionally configuring the Docker daemon before running the installer, using the following method:

  - **Linux hosts *only***: Run the Docker container in host networking mode by adding the `-network host` flag to the `docker run` command:

    ```
    docker run --network host remainder of docker run options
    ```

- **Centos/RHEL hosts**: These hosts, by default, enforce a strict SELinux policy which does not allow the installer container to read from or write to the mounted data volume. On such hosts, run the Docker volume command with the `Z` option, as shown below:

  ```
  docker run --rm -it -v `pwd`:/data:Z remainder of docker run options
  ```

Note

The Docker command provided will use the current directory to read the template and the OVA files, and to write the log files used during the install. If you encounter either of the following two errors, you should move the files to a directory where the path is in lowercase (all lowercase, no spaces or other special characters). Then navigate to that directory and rerun the installer.

Error 1:

```
% docker run --rm -it -v `pwd`:/data a45
docker: invalid reference format: repository name must be lowercase.
See 'docker run --help'
```

Error 2:

```
docker: Error response from daemon: Mounts denied: approving /Users/Desktop: file does not exist
ERRO[0000] error waiting for container: context canceled
```

Step 10 Navigate to the directory with the VMware template:

```
cd /opt/installer/deployments/7.2.0/vcentre
```

Step 11 Copy the template file found under `/opt/installer/deployments/7.2.0/vcentre/deployment_template_tfvars` to the `/data` folder using a different name.

For example: `cp deployment_template_tfvars /data/deployment.tfvars`

For the rest of this procedure, we will use the file name `deployment.tfvars` in all the examples.

Step 12 Using a text editor of your choice, open the template file you copied to the `/data` directory and edit it to match the properties for your planned deployment.

For reference, here is an example `deployment.tfvars`, edited using sample parameter values. You must use the values you gathered for your deployment, as specified in Gather installation parameter values, on page 9

```
Cw_VM_Image = ""    # Line added automatically by installer.
ClusterIPStack        = "IPv4"
DNS                   = "171.70.168.183"
DomainName            = "cisco.com"
CWPassword            = "*********"
NTP                   = "ntp.esl.cisco.com"
VMSize                = "XLarge"
ThinProvisioned = "true"
IgnoreDiagnosticsCheckFailure = "True"
Timezone           = "America/Los_Angeles"
EnableSkipAutoInstallFeature = "True"
ManagementVIP     = "172.22.140.180"
ManagementIPNetmask = "255.255.255.0"
ManagementIPGateway = "172.22.140.1"
DataVIP           = "14.14.14.12"
```

```
DataIPNetmask     = "255.255.255.0"
DataIPGateway     = "14.14.14.1"
CwVMs = {
  "0" = {
    VMName                = "svm-180",
    ManagementIPAddress = "172.22.140.182",
    DataIPAddress       = "14.14.14.13",
    NodeType               = "Hybrid"
  }
}
VCenterDC = {
  VCenterAddress = "<VCenterIPAddress>",
  VCenterUser = "administrator@vsphere.local",
  VCenterPassword = "<VCenterPassword>",
  DCname = "SVM-Datacenter",
  MgmtNetworkName = "VM Network",
  DataNetworkName = "Network2"
  VMs = [{
    HostedCwVMs = ["0"],
    Host = "172.22.140.210",
    Datastore = "datastore1",
    HSDatastore = "datastore1"
  }
]
}
SchemaVersion = "7.2.0"
```

Step 13 From the `/opt/installer` directory, run the installer.

```
./cw-installer.sh install -m /data/template file name -o /data/filename.ova
```

For example:

```
./cw-installer.sh install -m /data/deployment.tfvars -o
/data/cnc-workflowmanager-single-node-deployment-7.2.0-45.ova
```

Step 14 The installer will display the End User License Agreement (EULA). Read, and then enter "yes" if you accept the EULA. Otherwise, exit the installer and contact your Cisco representative.

Step 15 When prompted, enter "yes" to begin the installation operation.

Step 16 To track creation of the VM and success of the installation, follow the steps in Monitor Crosswork Server Activation, on page 37.

Step 17 When the installation operation exits, confirm the successful installation or re-run a failed installation, as follows:

It is not uncommon to see warnings like the following during the install:

```
Warning: Line 119: No space left for device '8' on parent controller '3'.
Warning: Line 114: Unable to parse 'enableMPTSupport' for attribute 'key' on element 'Config'.
```

You can ignore warnings like this if the install process proceeds to a successful conclusion, as indicated by the sample output below:

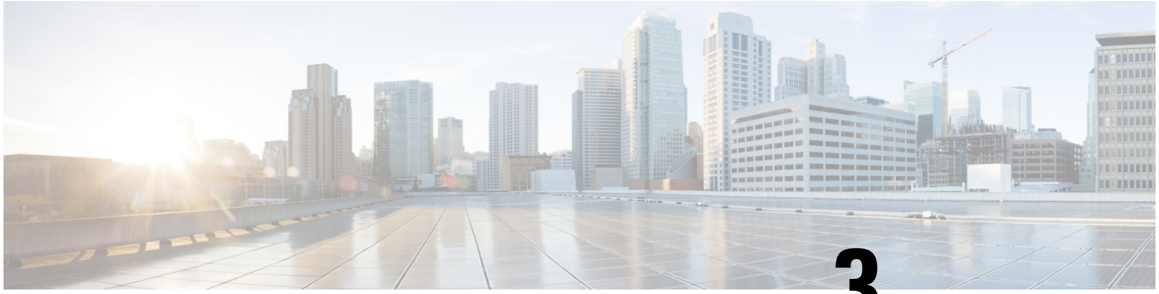
Sample output for successful installation:

```
cw_vms = .......
INFO: Copying day 0 state inventory to CW
INFO: Waiting for deployment status server to startup on ip address. Elapsed time 0s, retrying in
30s
Crosswork deployment status available at
http://ipaddress:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark
Once deployment is complete login to Crosswork via: https://ipaddress:30603/#/logincontroller
INFO: Cw Installer operation complete.
```

If the installation fails:

a. Open a support case with Cisco. Include with the case copies of the error messages reported during the installation. Remember to include copies of the following `log` files created in the `/data` directory (and the local directory where you launched the installer Docker container) with the case: `install.log`, `install_tf.log`, and `.tfstate`

b. The two most common reasons for the install to fail are a password that is not adequately complex, and errors in the template file, such as a mistyped IP address. If the installer fails due to errors like this, correct the error and rerun the install script. Remember to delete the `log` files before re-running the installation.



CHAPTER 3

KVM Installation

This chapter explains the required network configuration and the steps to install Crosswork Workflow Manager Solutions in a KVM environment.

Configure network bridges or SRIOV

Crosswork requires a 10G interface for all the data layer communications to operate at a scale. You can choose any networking configuration that provides 10G throughput.

Note For KVM deployment, configure **either** network bridges **or** SRIOV, **but not both**.

For detailed instructions, see these topics:

- Configure network bridges, on page 29
- Configure SRIOV, on page 31

Configure network bridges

A network bridge, such as Linux bridge and Open vSwitch (OVS), acts like a virtual network switch, allowing multiple network interfaces to communicate as if they are on the same physical network.

Follow these steps to configure network bridges.

Procedure

Step 1 Create a new network connection of type "bridge" with the interface name `intMgmt` and assign it the connection name `intMgmt`.

```
nmcli connection add type bridge ifname intMgmt con-name intMgmt
```

Step 2 Add a new `bridge-slave` connection, associating the physical network interface `<interface1>` with the previously created bridge `intMgmt`.

```
nmcli connection add type bridge-slave ifname <interface1> controller intMgmt
```

Example:

```
nmcli con add type bridge-slave ifname <hostmgmtIntf> master intMgmt con-name
intMgmt-slave-<hostmgmtIntf>
```

Step 3 Assign IP address to the bridge.

```
nmcli connection modify intMgmt ipv4.addresses <IPv4-address>/<subnet-mask>
```

Example:

```
nmcli con modify intMgmt ipv4.addresses <hostmgmtIp/mask> ipv4.gateway
<mgmtgw> ipv4.dns <dnsIp> ipv4.method manual ipv4.route-metric 50
```

Step 4 Bring up the `intMgmt` network connection.

```
nmcli connection up intMgmt
```

Example:

```
nmcli con up intMgmt
nmcli con up intMgmt-slave-<hostmgmtIntf>
```

Step 5 Create another network bridge connection with the interface name `intData` and assign it the connection name `intData`.

```
nmcli connection add type bridge ifname intData con-name intData
```

Example:

```
nmcli con add type bridge ifname intData con-name intData
```

Step 6 Add a bridge-slave connection, associating the physical network interface `<interface2>` with the previously created bridge `intData`.

```
nmcli connection add type bridge-slave ifname <interface2> controller intData
```

Example:

```
nmcli con add type bridge-slave ifname <hostdataIntf> master intData con-name
intData-slave-<hostdataIntf>
```

Step 7 Assign IP address to `intData`.

```
nmcli connection modify intData ipv4.addresses <IPv4-address>/<subnet-mask>
```

Example:

```
nmcli con modify intData ipv4.addresses <hostdataIp/mask> ipv4.method manual ipv4.gateway <datagw>
ipv4.route-metric 90
```

Step 8 Bring up the `intData` network connection.

```
nmcli connection up intData
```

Example:

```
nmcli con up intData
nmcli con up intData-slave-<hostdataIntf>
```

Both network bridges, intMgmt and intData, are configured and active, enabling communication across associated network interfaces as if connected to the same physical network.

Configure SRIOV

SRIOV allows you to share a single physical network interface among multiple VMs by creating multiple Virtual Functions (VFs).

Follow these steps to configure SRIOV.

Procedure

Step 1 Open the `rc.local` file in the vi editor.

```
vi /etc/rc.d/rc.local
```

Step 2 Set the number of VFs for the network interfaces according to your requirement. In a Cisco Crosswork Planning single VM installation, you need a minimum of two network interfaces: one for management and one for data. By default, two VFs are configured for each interface. You can configure additional VFs for future scalability needs.

For example, to set the number of VFs to 2 for each `<interface1>` and `<interface2>`, use these commands. In this example, `<interface1>` refers to the management interface and `<interface2>` refers to the data interface.

```
echo 2 > /sys/class/net/<interface1>/device/sriov_numvfs
echo 2 > /sys/class/net/<interface2>/device/sriov_numvfs
```

Step 3 Change the permissions of the `rc.local` file to make it executable.

```
chmod +x /etc/rc.d/rc.local
```

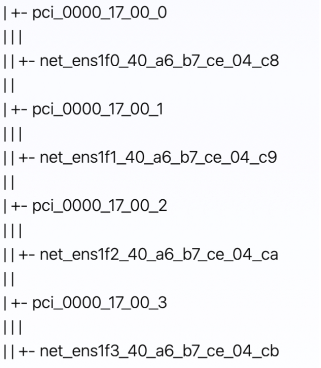
Step 4 If any of the interfaces are configured for VLAN, assign VLAN IDs to the interfaces.

```
ip link set <interface1> vf 0 vlan <vlanid>
ip link set <interface2> vf 1 vlan <vlanid>
```

Step 5 Save the changes and reboot the system.

Step 6 List all the PCI devices for all the virtual functions in a tree format. This is useful for verifying the setup and ensuring that the VFs are correctly recognized by the KVM hypervisor.

```
virsh nodedev-list --tree
```



```
| +- pci_0000_17_00_0
| | |
| | +- net_ens1f0_40_a6_b7_ce_04_c8
| |
| +- pci_0000_17_00_1
| | |
| | +- net_ens1f1_40_a6_b7_ce_04_c9
| |
| +- pci_0000_17_00_2
| | |
| | +- net_ens1f2_40_a6_b7_ce_04_ca
| |
| +- pci_0000_17_00_3
| | |
| | +- net_ens1f3_40_a6_b7_ce_04_cb
```

In this procedure, since we set the number of VFs as 2 in Step 2, two VFs for each management interface and data interface are created. As a result, a total of four PCI devices are generated: two for management and two for data.

This PCI device information is used during the installation process with SRIOV (Step 4 of).

Install Crosswork on KVM

Follow these steps to deploy Crosswork on a single VM on KVM RHEL.

Note The time taken to create the VM can vary based on the size of your deployment profile and the performance characteristics of your hardware.

Before you begin

Ensure that:

- You are familiar with the workflow and deployment decisions explained in Plan your installation, on page 1.
- Your KVM host meets all the requirements for a KVM host specified in Hardware requirements, on page 2.
- Your KVM RHEL environment is set up and verified as explained in KVM installation requirements, on page 3.
- You have set up either network bridges or SRIOV as specified in Configure network bridges or SRIOV, on page 29.
- The network is configured to meet all the requirements specified in Network requirements, on page 4.
- The ports on the host and your devices are configured to meet the requirements specified in Management port requirements, on page 6 and Device port requirements, on page 7.
- You have assembled all of the installation values you will need, as specified in Gather installation parameter values, on page 9.

Attention The download file names given in this topic are subject to change. You can always find the latest versions by pointing your browser to https://software.cisco.com/download/home and searching for **Crosswork Network Controller** > **All Release**.

Procedure

Step 1 Prepare a config IOS file `ovf-env.xml`) to use when installing the Crosswork VM.

Use the following example template to prepare the `ovf-env.xml` file:

```
<Environment
     xmlns="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xmlns:oe="http://schemas.dmtf.org/ovf/environment/1"
     xmlns:ve="http://www.vmware.com/schema/ovfenv"
     oe:id=""
   <PlatformSection>
```

```
      <Kind>KVM</Kind>
      <Version>7.2.0</Version>
      <Vendor>KVM</Vendor>
      <Locale>en</Locale>
   </PlatformSection>
    <PropertySection>
         <Property oe:key="CWPassword" oe:value="**********"/>
         <Property oe:key="CWUsername" oe:value="cw-admin"/>
         <Property oe:key="ClusterCaKey" oe:value=""/>
         <Property oe:key="ClusterCaPubKey" oe:value=""/>
         <Property oe:key="CwInstaller" oe:value="False"/>
         <Property oe:key="DNSv4" oe:value="171.70.168.183"/>
         <Property oe:key="DNSv6" oe:value="::0"/>
         <Property oe:key="DataIPv4Address" oe:value="192.168.5.48"/>
         <Property oe:key="DataIPv4Gateway" oe:value="192.168.5.1"/>
         <Property oe:key="DataIPv4Netmask" oe:value="255.255.255.0"/>
         <Property oe:key="DataIPv6Address" oe:value="::0"/>
         <Property oe:key="DataIPv6Gateway" oe:value="::1"/>
         <Property oe:key="DataIPv6Netmask" oe:value="64"/>
         <Property oe:key="DataPeerIPs" oe:value=""/>
         <Property oe:key="DataVIP" oe:value="192.168.5.51"/>
         <Property oe:key="DataVIPName" oe:value=""/>
         <Property oe:key="Deployment" oe:value="cw_ipv4"/>
         <Property oe:key="Disclaimer" oe:value="Cisco Crosswork"/>
         <Property oe:key="Domain" oe:value="cisco.com"/>
         <Property oe:key="EnableSkipAutoInstallFeature" oe:value="True"/>
         <Property oe:key="EnforcePodReservations" oe:value="True"/>
         <Property oe:key="IgnoreDiagnosticsCheckFailure" oe:value="True"/>
         <Property oe:key="InitMasterCount" oe:value="1"/>
         <Property oe:key="InitNodeCount" oe:value="1"/>
         <Property oe:key="IsSeed" oe:value="True"/>
         <Property oe:key="K8Orch" oe:value=""/>
         <Property oe:key="K8sPodNetworkV4" oe:value="10.244.0.0"/>
         <Property oe:key="K8sServiceNetworkV4" oe:value="10.96.0.0"/>
         <Property oe:key="ManagementIPv4Address" oe:value="10.19.70.148"/>
         <Property oe:key="ManagementIPv4Gateway" oe:value="10.19.70.1"/>
         <Property oe:key="ManagementIPv4Netmask" oe:value="255.255.255.0"/>
         <Property oe:key="ManagementIPv6Address" oe:value="::0"/>
         <Property oe:key="ManagementIPv6Gateway" oe:value="::1"/>
         <Property oe:key="ManagementIPv6Netmask" oe:value="112"/>
         <Property oe:key="ManagementVIP" oe:value="10.19.70.151"/>
         <Property oe:key="ManagementVIPName" oe:value=""/>
         <Property oe:key="ManagerPeerIPs" oe:value=""/>
         <Property oe:key="NTP" oe:value="ntp.esl.cisco.com"/>
         <Property oe:key="Timezone" oe:value="US/Pacific"/>
         <Property oe:key="VMLocation" oe:value="default"/>
         <Property oe:key="VMType" oe:value="Hybrid"/>
         <Property oe:key="bckup_min_percent" oe:value="35"/>
         <Property oe:key="corefs" oe:value="18"/>
         <Property oe:key="ddatafs" oe:value="485"/>
         <Property oe:key="logfs" oe:value="20"/>
         <Property oe:key="ramdisk" oe:value="0"/>
         <Property oe:key="ssd" oe:value="15"/>
         <Property oe:key="VMSize" oe:value="XLarge"/>
         <Property oe:key="ThinProvisioned" oe:value="False"/>
         <Property oe:key="UseNonDefaultCalicoBgpPort" oe:value="False"/>
         <Property oe:key="bootOptions.efiSecureBootEnabled" oe:value="True"/>
   </PropertySection>
</Environment>
```

Step 2 Update the `ovf-env.xml` file you created using the parameter values you gathered for your KVM deployment (see General parameters, on page 9).

```
$ cat ovf-env.xml
```

Step 3 Generate the ISO file.

```
$ mkisofs -R -relaxed-filenames -joliet-long -iso-level 3 -l -o cnc1.iso ovf-env.xml
```

Note
In the above command, `cnc1` is the host name of the Cisco Crosswork VM.

Step 4 From https://software.cisco.com/download/home, download the latest version of the Cisco Crosswork platform `qcow2.tar.gz` file to a storage location on your KVM host: `CW-CWM-Solutions-workflowmanager-2.1.0-14-SVM-7.2.0-45-qcow2.signed.bin`.

Step 5 Extract the tar.gz file using the following command:

```
tar -xvf cnc-workflowmanager-single-node-deployment-7.2.0-45-qcow2.tar.gz
```

This command creates three `qcow2` files:

- `cnc-workflowmanager-single-node-deployment-7.2.0-45_dockerfs.qcow2`
- `cnc-workflowmanager-single-node-deployment-7.2.0-45_extrafs.qcow2`
- `cnc-workflowmanager-single-node-deployment-7.2.0-45_rootfs.qcow2`

Step 6 Navigate to the required installation folder and create three disks.

```
cd cnc1/
qemu-img create -f qcow2 disk3 20G
qemu-img create -f qcow2 disk4 485G
qemu-img create -f qcow2 disk6 15G
```

```
ls -1
cw_dockerfs.qcow2
cw_extrafs.qcow2
cw_rootfs.qcow2
disk3
disk4
disk6
```

Step 7 Install the Crosswork VM using either network bridge or SRIOV.

In these examples, `cnc1` is the host name of the Crosswork VM.

- Using network bridge:

```
virt-install --boot uefi --boot hd,cdrom --connect qemu:///system --virt-type kvm --name cnc1
--ram 98304 --vcpus 12 --os-type linux --disk
path=cnc-workflowmanager-single-node-deployment-7.2.0-45_rootfs.qcow2,format=qcow2,bus=scsi --disk
 path=cnc-workflowmanager-single-node-deployment-7.2.0-45_dockerfs.qcow2,format=qcow2,bus=scsi
--disk path=disk3,format=qcow2,bus=scsi --disk path=disk4,format=qcow2,bus=scsi --disk
path=cnc-workflowmanager-single-node-deployment-7.2.0-45_extrafs.qcow2,format=qcow2,bus=scsi
--disk path=disk6,format=qcow2,bus=scsi --disk=cnckvm.iso,device=cdrom,bus=scsi --import --network
 bridge=intMgmt,model=virtio --network bridge=intData,model=virtio --noautoconsole --os-variant
 ubuntu22.04 --graphics vnc,listen=0.0.0.0
```

- Using SRIOV:

```
virt-install --boot uefi --boot hd,cdrom --connect qemu:///system --virt-type kvm --name cnc1
--ram 98304 --vcpus 12 --cpu host-passthrough --disk path=cw_rootfs.qcow2,format=qcow2,bus=scsi
 --disk path=cw_dockerfs.qcow2,format=qcow2,bus=scsi --disk path=disk3,format=qcow2,bus=scsi
--disk path=disk4,format=qcow2,bus=scsi --disk path=cw_extrafs.qcow2,format=qcow2,bus=scsi --disk
 path=disk6,format=qcow2,bus=scsi --disk=cnc1.iso,device=cdrom,bus=scsi --import --network none
 --host-device=pci_0000_01_10_0 --host-device=pci_0000_01_10_0 --os-variant ubuntu-lts-latest &
```

Step 8 To track creation of the VM and success of the installation, follow the steps in Monitor Crosswork Server Activation, on page 37.

CHAPTER 4

Verify Installation Status

This chapter outlines the actions needed to verify and monitor the system after installation.

Monitor Crosswork Server Activation

This topic explains how to monitor and verify that the Crosswork server installation has completed successfully.

As the installer builds and configures the VM, it will report progress. The installer will prompt you to accept the license agreement and then ask if you want to continue the installation. After you confirm that you want to continue, the installation will progress and any errors will be logged in the `installer.log` or `installer_tf.log` files. If the VM is built and is able to boot, any errors in applying the operator-specified configuration will be logged on the VM in the `/var/log/firstboot.log` file.

About the administrative user ID

During installation, Crosswork will create a special administrative user ID (with the username *cw-admin* and the description **virtual machine (VM) administrator**). The *cw-admin* username, when created, will use the password that you provided in the installation manifest template. In cases where the installer is unable to apply the password, it creates the administrative user ID using the default password *cw-admin*. The first time you log in using the administrative username with the default password, you will be prompted to change the password.

The administrative user ID username *cw-admin* is reserved and cannot be changed. Data center administrators use this ID to log into and troubleshoot the Crosswork application VM.

Deployment progress stages

Successful deployment of Cisco Crosswork and its VM host normally progress through these stages:

1. The installer scripts upload the Crosswork image file to the server.
2. The installer creates the VM and then displays a success message, such as "Creation Complete".
3. The installer powers on the VM. It applies to the VM the parameters specified in the template, reboots the VM, and then registers it with Kubernetes.
4. Once the VM becomes accessible, the installer script displays a success message, such as "Crosswork Installer operation complete". The installer script then exits and returns you to a CLI prompt.

You can monitor most of these deployment stages as they occur, using the methods in the following section, Monitor deployment progress during installation, on page 38.

Once the Crosswork installer operation completes successfully, the Cisco Crosswork UI becomes accessible and you can monitor Crosswork status by logging into the UI, as explained in the topic Log into the Cisco Crosswork UI in the *Cisco Crosswork Network Controller Installation Guide*. The login and heath-check process is the same for single VM installations and cluster installations.

Monitor deployment progress during installation

You can monitor VM startup and Crosswork installation progress using these methods.

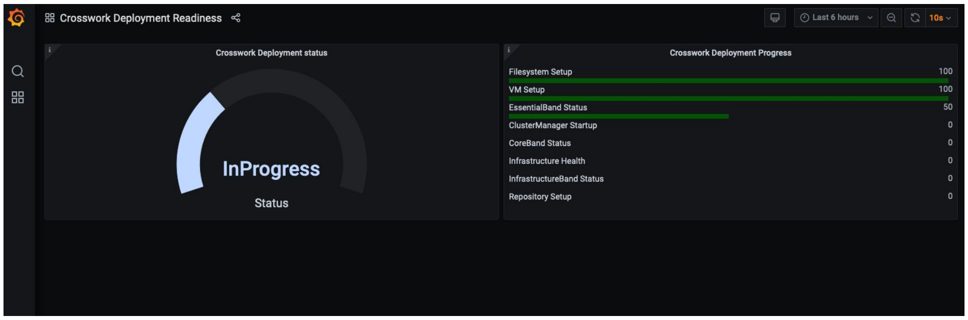
Using the browser-accessible dashboard:

1. Once the VM has been created (stage 2, after the "Creation Complete" message), you can monitor Crosswork Deployment Readiness from the browser-accessible grafana dashboard, using this URL:

   ```
   http://{VIP}:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark
   ```

   Where *{VIP}* is the Virtual IP address of the VM.

   Figure 4: Crosswork Deployment Readiness

   Crosswork Deployment status

   InProgress

   Status

   Crosswork Deployment Progress

Filesystem Setup	100
VM Setup	100
EssentialBand Status	50
ClusterManager Startup	0
CoreBand Status	0
Infrastructure Health	0
InfrastructureBand Status	0
Repository Setup	0

> **Note** The dashboard is available only:
>
> - Once the installer completes creating the VM.
> - For around 30 minutes total.

2. At the end of the deployment, the dashboard will report a "Ready" status.

   If the dashboard URL is inaccessible, use the SSH console described below to monitor the installation process.

Using the SSH console:

1. Check the progress from the console of the VM or use SSH to access the Virtual IP address of the VM.
2. In the latter case, login using the *cw-admin* user name and the password you assigned to that account in the install template.
3. Switch to super user mode using `sudo su -` command.

4. Run `kubectl get nodes` (to see if the nodes are ready) and `kubectl get pods` (to see the list of active running pods) commands.

5. Repeat the `kubectl get pods` command until you see `robot-ui` in the list of active pods.

6. At this point, you can try to access the Cisco Crosswork UI as explained in the topic in the *Cisco Crosswork Network Controller Installation Guide*.

Diagnostic assessment

During deployment, the system verifies VM datastore resource values, including disk latency, IOPS, and network bandwidth. If any value falls below the recommended threshold, the diagnostic assessment reports a failure, requiring user action to proceed with the installation. See the topic Log into the Cisco Crosswork UI in the *Cisco Crosswork Network Controller Installation Guide*.

Deployment failure

In the event of one of the failure scenarios listed below, contact the Cisco Customer Experience team and provide the `installer.log`, `installer_tf.log`, and `firstBoot.log` files for review:

- Installation is incomplete.
- Installation is completed, but the VMs are not functional.
- Installation is completed, but you are directed to check `/var/log/firstBoot.log` or `/opt/robot/bin/firstBoot.log` file.

CHAPTER 5

Install Applications

This chapter details the installation steps for the Crosswork Workflow Manager and CWM Solutions CAPPs.

Install the Crosswork Workflow Manager CAPP

Once you have deployed Crosswork on a VMware or KVM virtual machine, you can install the Crosswork Workflow Manager (CWM) application, which is distributed as a Crosswork CAPP.

Before you begin

Ensure that you have deployed Crosswork successfully on your VMware or KVM host. To verify that Crosswork is installed and functional, log in to Crosswork using an administrative ID at `https://`*`CrossworkIP`*`:30603/`, where *`CrossworkIP`* is the IP address on the virtual machine where Crosswork was installed.

Attention The download file names given in this topic are subject to change. You can always find the latest versions by pointing your browser to https://software.cisco.com/download/home and searching for **Crosswork Workflow Manager 2**.

Procedure

Step 1 On a remote host accessible by HTTP, HTTPS or SCP from your Crosswork VM host, create a storage directory to contain the download you will use in this procedure.

Step 2 From https://software.cisco.com/download/home, download to the remote host the Crosswork Workflow Manager file appropriate for the VM deployment you chose:

- For a VMware deployment: `cw-na-cwm-2.1.0-20-releasecwm210-260124-ova.signed.bin`
- For a KVM deployment: `cw-na-cwm-2.1.0-20-releasecwm210-260124-qcow2.signed.bin`

Step 3 Use the following command to extract the `tar.gz` installer bundle from the appropriate `signed.bin` file:

```
sh cw-na-cwm-2.1.0-20-releasecwm210-260124-ova.signed.bin
```

or

```
sh cw-na-cwm-2.1.0-20-releasecwm210-260124-qcow2.signed.bin
```

The contents of the installer bundle and files necessary to validate the image are extracted to the same directory on the remote host.

Step 4 Use the following command to extract the `tar.gz` installer bundle:

```
tar -vxf cw-na-cwm-2.1.0-20-releasecwm210-260124-ova.tar.gz
```

or

```
tar -vxf cw-na-cwm-2.1.0-20-releasecwm210-260124-qcow2.tar.gz
```

The contents of the installer bundle and files necessary to validate the image are extracted to the same directory on the remote host.

Step 5 Log in to Crosswork using an admin ID and select **Administration** > **Crosswork Manager** > **Application Management**.

Step 6 Click **Add new file** and select **Upload CAPP file (.tar.gz)**.

Step 7 Using the **Add File (.Tar.Gz)** page, first select the **Protocol** you want to use to add the CWM CAPP file to the system. Then:

a) If you selected **URL**: Enter the **URL** for the remote host where the CAPP file is stored (including the path to the `tar.gz` file).

b) If the **Basic Auth** checkbox is selected, enter the **Username** and **Password** needed to access the remote host.

c) If you selected **SCP**: Enter the file's **Server path/Location** on the remote host, the remote host server's **Host name/IP address**, the **Port**, and the login **Username** and **Password**.

Step 8 Click **Add**. You can select the **Job History** option to monitor the progress of the CAPP file upload.

Step 9 When the upload completes, the **Workflow Manager** tile appears on the **Applications** page, indicating that the application is ready to install.

Step 10 Click the **More** icon (three dots) on the **Workflow Manager** tile to display the **Workflow Manager** installation pop up, then click **Install**. When installation is complete, the **Applications Management** > **Job History** tab should display an "Activation Successful" message.

Step 11 Verify successful installation by choosing **Administration** > **Crosswork Manager** > **Crosswork Health** > **Workflow Manager**. The **Microservices** tab displays the microservices, all with **Healthy** showing in the **Status** column.

Install the CWM Solutions CAPP

Once you have installed CWM, you can install CWM-S.

Before you begin

Ensure that you have already installed Crosswork Workflow Manager (CWM), as explained in Install the Crosswork Workflow Manager CAPP, on page 41. If you have done this, you will find the Crosswork Workflow Manager Solutions (CWM-S) installer bundle extracted to the same directory on the remote host where you extracted the Crosswork Workflow Manager (CWM) CAPP installer bundle.

Procedure

Step 1 From https://software.cisco.com/download/home, download to the remote host the Crosswork Workflow Manager file appropriate for the VM deployment you chose:

- For a VMware deployment: `cw-na-cwm-sol-2.1.0-21-releasecwms210-260124-ova.signed.bin`
- For a KVM deployment: `cw-na-cwm-sol-2.1.0-21-releasecwms210-260124-qcow2.signed.bin`

Step 2 Use the following command to extract the `tar.gz` installer bundle from the appropriate `signed.bin` file:

```
sh cw-na-cwm-sol-2.1.0-21-releasecwms210-260124-ova.signed.bin
```

or

```
sh cw-na-cwm-sol-2.1.0-21-releasecwms210-260124-qcow2.signed.bin
```

The contents of the installer bundle and files necessary to validate the image are extracted to the same directory on the remote host.

Step 3 Use the following command to extract the `tar.gz` installer bundle:

```
tar -vxf cw-na-cwm-sol-2.1.0-21-releasecwms210-260124-ova.tar.gz
```

or

```
tar -vxf cw-na-cwm-sol-2.1.0-21-releasecwms210-260124-qcow2.tar.gz
```

The contents of the installer bundle and files necessary to validate the image are extracted to the same directory on the remote host.

Step 4 Log in to Crosswork using an admin ID and select **Administration** > **Crosswork Manager** > **Application Management**.

Step 5 Click **Add new file** and select **Upload CAPP file (.tar.gz)**.

Step 6 Using the **Add File (.Tar.Gz)** page, first select the **Protocol** you want to use to add the CWM Solutions CAPP file to the system. Then:

a) If you selected **URL**: Enter the **URL** for the remote host where the CAPP file is stored (including the path to the `tar.gz` file).

b) If the **Basic Auth** checkbox is selected, enter the **Username** and **Password** needed to access the remote host.

c) If you selected **SCP**: Enter the file's **Server path/Location**, the server's **Host name/IP address**, **Port**, and the login **Username** and **Password**.

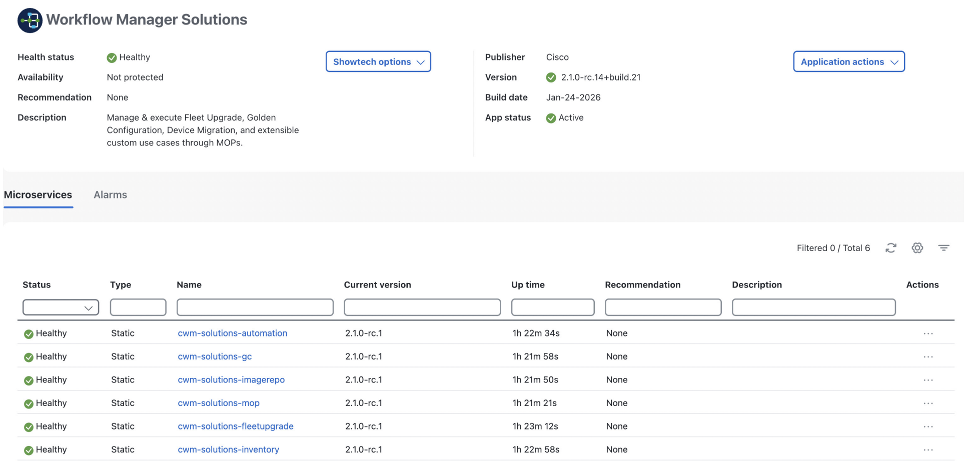
Step 7 Click **Add**. You can select the **Job History** option to monitor the upload while it proceeds.

Step 8 When the addition completes, the **Workflow Manager Solutions** tile appears on the **Applications** page at the far right, next to the **Workflow Manager**tile, indicating that the **Workflow Manager Solutions** application is ready to install.

Step 9 Click the **More** icon (three dots) on the **Workflow Manager Solutions** tile to display the installation pop up menu, then click **Install**.

Step 10 When installation is completed, the **Application Management** > **Job History** tab should display an "Activation of application Workflow Manager Solutions Successful" message.

Step 11 Choose **Administration** > **Crosswork Manager** > **Crosswork Health** > **Workflow Manager Solutions**. The **Microservices** tab should display that the CWM Solutions microservices are in a **Healthy** state.



Workflow Manager Solutions

Health status	Healthy	Showtech options	Publisher	Cisco
Availability	Not protected		Version	2.1.0-rc.14+build.21
Recommendation	None		Build date	Jan-24-2026
Description	Manage & execute Fleet Upgrade, Golden Configuration, Device Migration, and extensible custom use cases through MOPs.		App status	Active

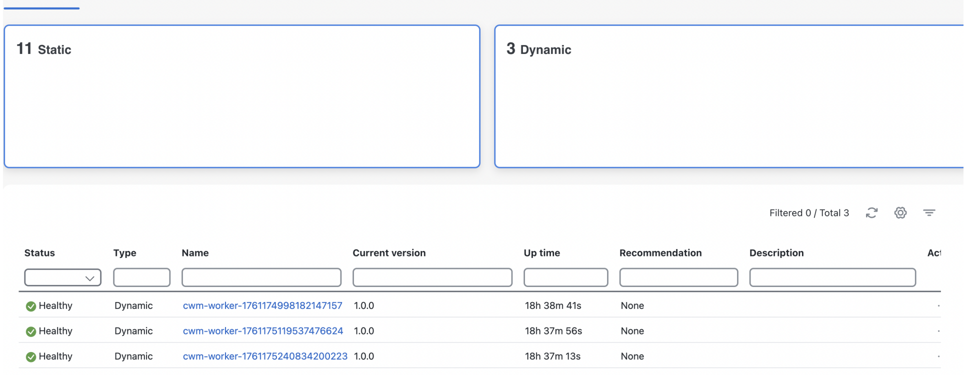
Application actions

Microservices | Alarms

Filtered 0 / Total 6

Status	Type	Name	Current version	Up time	Recommendation	Description	Actions
Healthy	Static	cwm-solutions-automation	2.1.0-rc.1	1h 22m 34s	None		···
Healthy	Static	cwm-solutions-gc	2.1.0-rc.1	1h 21m 58s	None		···
Healthy	Static	cwm-solutions-imagerepo	2.1.0-rc.1	1h 21m 50s	None		···
Healthy	Static	cwm-solutions-mop	2.1.0-rc.1	1h 21m 21s	None		···
Healthy	Static	cwm-solutions-fleetupgrade	2.1.0-rc.1	1h 23m 12s	None		···
Healthy	Static	cwm-solutions-inventory	2.1.0-rc.1	1h 22m 58s	None		···

Step 12 Finally, CWM Solutions will add three dynamic service pods to CWM. These are worker pods for the three CWM adapters that CWM Solutions installed automatically. You will find them under **Administration** > **Crosswork Manager** > **Crosswork Health** > **Workflow Manager** (not under Workflow Manager Solutions).



11 Static

3 Dynamic

Filtered 0 / Total 3

Status	Type	Name	Current version	Up time	Recommendation	Description	Act
Healthy	Dynamic	cwm-worker-1761174998182147157	1.0.0	18h 38m 41s	None		·
Healthy	Dynamic	cwm-worker-1761175119537476624	1.0.0	18h 37m 56s	None		·
Healthy	Dynamic	cwm-worker-1761175240834200223	1.0.0	18h 37m 13s	None		·

CHAPTER 6

NSO Configuration

This chapter lists the configuration tasks required to prepare NSO for integration.

NSO package pre-installation tasks

Before installing the CWM Solutions packages for NSO, you must ensure that `ulimit` values are set properly, additional Python packages are installed and that NSO supports REST. CWM Solutions can use both SSL and HTTPS, so you can choose to enable both in the REST configuration if needed. You will need to install SSL certificate files and specify their location in the RESTCONF configuration if you want to enable SSL.

Before you begin

Ensure that you have met the basic requirements for the NSO installation, as explained in Meet installation requirements, on page 2. If you plan to enable HTTPS/SSL as part of the REST configuration, Cisco recommends that you create and install SSL certificate and key files in the NCS configuration directory before completing this task.

Please see https://developer.cisco.com/docs/nso/guides/installation/#installation for related NSO installation requirements, such as required Python and Java versions, and so on.

Procedure

Step 1 Set **ulimit** values, as follows:

a) Edit the `/etc/security/limits.conf` file to add the following lines:

Switch to super user: `sudo su`

Edit `/etc/security/limits.conf` and add these lines:

```
*       soft nproc 65535
*       hard nproc 65535
*       soft nofile 65535
*       hard nofile 65535
*      hard memlock 65535
*      soft memlock 65535
```

b) Because Ubuntu distributions may require an explicit root username `ulimit` specification, add the following lines to the file:

```
root    -       nofile  65535
root    -       nproc   65535
root    soft    memlock unlimited
root    hard    memlock unlimited
```

c) When you have finished the edit, run the `sysctl -p` script to set the parameters.

d) Log out and log in again to apply the new values.

e) Run **ulimit -a** to verify that the **ulimit** values have been applied correctly. You should see output like the following.

```
$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 95697
max locked memory       (kbytes, -l) 65536
max memory size         (kbytes, -m) unlimited
open files                      (-n) 65535
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) unlimited
max user processes              (-u) 65535
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

Step 2 Open port 20243 and associate the the host name with the host IP address, as follows:

a) Open port 20243 so that the NSO host VM can communicate with Crosswork Device Lifecycle Manager. For example:

```
sudo firewall-cmd --zone=public --add-port=20243/tcp --permanent
sudo firewall-cmd --reload
```

b) Check `/etc/hosts` and verify that the NSO host IP is associated with the NSO host name (if they are not associated, port 20243 might not start automatically). For example:

```
sudo vi /etc/hosts
127.0.0.1   localhost localhost.localdomain localhost4 localhost4.localdomain4
172.22.143.219 <hostname>
::1         localhost localhost.localdomain localhost6 localhost6.localdomain6
```

Step 3 Install the following Python packages on the NSO server using these commands:

```
~$ sudo pip install textfsm
~$ sudo pip install jinja2
~$ sudo pip instapp pyyaml
~$ sudo pip install pycryptodome
```

Step 4 Enable support for REST, CGI, SSL/HTTPS `webui`, `tcp`, and `stream`, as follows.

a) Edit the NSO `ncs.conf` file:

```
sudo vi /etc/ncs/ncs.conf

 <webui>
    <enabled>true</enabled>
    <transport>
<tcp>
```

```
  <enabled>true</enabled>
  <ip>0.0.0.0</ip>
  <port>8080</port>
  <extra-listen>
    <ip>::</ip>
    <port>8080</port>
  </extra-listen>
</tcp>
<ssl>
  <enabled>true</enabled>
  <ip>0.0.0.0</ip>
  <port>8888</port>
  <key-file>${NCS_CONFIG_DIR}/ssl/cert/host.key</key-file>
  <cert-file>${NCS_CONFIG_DIR}/ssl/cert/host.cert</cert-file>
  <extra-listen>
    <ip>::</ip>
    <port>8888</port>
  </extra-listen>
      </ssl>
    </transport>

    <cgi>
      <enabled>true</enabled>
      <php>
        <enabled>false</enabled>
      </php>
    </cgi>
  </webui>

  <restconf>
    <enabled>true</enabled>
  </restconf>


**Add the below stream under the below section
  <notifications>
    <event-streams>**

<stream>
  <name>service-aa-changes</name>
  <description>Notifications relating to the service aa configuration change</description>
  <replay-support>true</replay-support>
  <builtin-replay-store>
    <enabled>true</enabled>
    <dir>${NCS_RUN_DIR}/state</dir>
    <max-size>S10M</max-size>
    <max-files>50</max-files>
  </builtin-replay-store>
</stream>
```

b) When you have finished the edit, save the `ncs.conf` file and restart NSO. For example:

```
sudo systemctl restart ncs
```

c) Once NSO restarts, using an admin user ID, verify that REST is working correctly on your NSO installation. For example:

```
admin@ncs% run show ncs-state rest
ncs-state rest listen tcp
 ip   ::
 port 8080
ncs-state rest listen tcp
 ip   0.0.0.0
 port 8080
```

```
ncs-state rest listen ssl
 ip   ::
 port 8888
ncs-state rest listen ssl
 ip   0.0.0.0
 port 8888
```

Step 5 Ensure that the NETCONF Access Control Model (NACM) rule list grants the ncsadmin and Linux users permissions to perform functions on NSO. For example:

```
admin@ncs% set nacm groups group ncsadmin user-name admin
admin@ncs% commit


admin@ncs% show nacm
read-default     deny;
write-default    deny;
exec-default     deny;
groups {
    group ncsadmin {
        user-name [ admin private ];
    }
    group ncsoper {
        user-name [ public ];
    }
}
```

For help adding more users, including adding them to auth groups, see the *NSO Administration Guide* topic Adding a User.

Step 6 Determine the devices you will be supporting using CWM Solutions, then install the NSO Network Element Drivers (NEDs) appropriate for those devices, as follows:

a) Using the URLs on the NED license certificates supplied by your account team, download the NEDs for your devices from Cisco Software Download to a resource on your NSO host. The NEDs are `signed.bin` files that you must run to validate and extract the NED code.

b) Verify, extract and install the downloaded NEDs as explained in the he *NSO Administration Guide* topic Install New NEDs.

c) When you have finished installing the new NEDs, restart NSO. For example:

```
sudo systemctl restart ncs
```

Create Crosswork credential profiles

Crosswork credential profiles store login user names and passwords in a secure fashion. Crosswork uses them to authenticate with its providers, such as Cisco NSO, which are helper applications that perform specialized services for Crosswork. Crosswork and its providers also use credential profiles to authenticate with your network devices when accessing them.

In this procedure, we’ll create two credential profiles. Crosswork Workflow Manager Solutions will use the first profile to log in to NSO and request that NSO access your network devices or perform changes on them. NSO will use the second profile to log into your network devices.

The credentials you provide in credential profiles are protocol-specific. That is, in each credential profile, you specify a "communication type" (also known as a protocol) and for each protocol, one set of credentials (typically, a user name and password) that works with that protocol on your device or application. You then **+ add another** protocol, and a corresponding set of credentials, until all the protocols and credentials you want the profile to work with are added to the collection.

You can't have a credential profile with two different sets of credentials for the same protocol. If you want to specify a different set of credentials for protocols you already specified in one credential profile, you will need to create another credential profile.

For more about credential profiles and providers, see Credential Profiles in the Cisco Crosswork Network Controller Administration Guide.

Before you begin

Ensure that you've already installed CWM Solutions per the instructions in Install the CWM Solutions CAPP, on page 42.

Procedure

Step 1 Log in to Crosswork and select **Device Management** > **Credential Profiles**. Crosswork displays the **Credential Profiles** list.

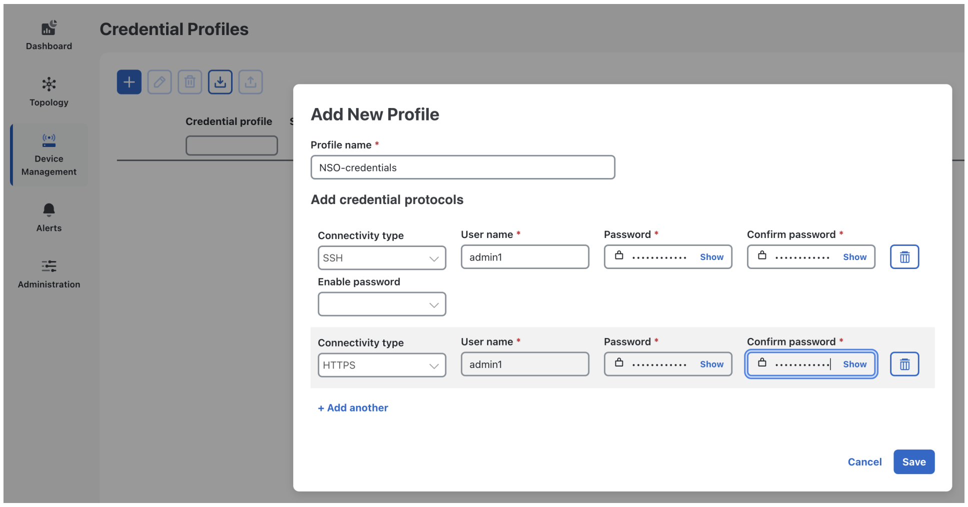
Step 2 **Create the NSO provider credential profile as follows:**

a) Click **+** to add a credential profile for the NSO provider.

b) Complete the fields on the **Add New Profile** window as follows:

In this field...	Enter or select:
Profile name	**`NSO-Credentials`** (or any unique name you find meaningful)
Connectivity type	**`SSH`**
User name	The username for an SSH admin user on the NSO server. This user name can be a dedicated CWM Solutions user name with admin privileges that you create on the NSO server. In any case, this admin user name *must* be one that is in the `ncsadmin` group on the NSO server.
Password	The password for this user name.
Confirm password	The same password you entered in **Password**.
Enable password	Leave this field blank.

c) Click **+ Add another** to display another set of connectivity protocols to add to the same NSO credential profile. This time, select **`HTTPS`** as the **Connectivity type**, and enter the same NSO user and password information for this protocol, just as you did for Step 2b. For example:



Profile name *: NSO-credentials

Add credential protocols

Connectivity type: SSH | User name *: admin1 | Password *: ············ | Confirm password *: ············

Enable password:

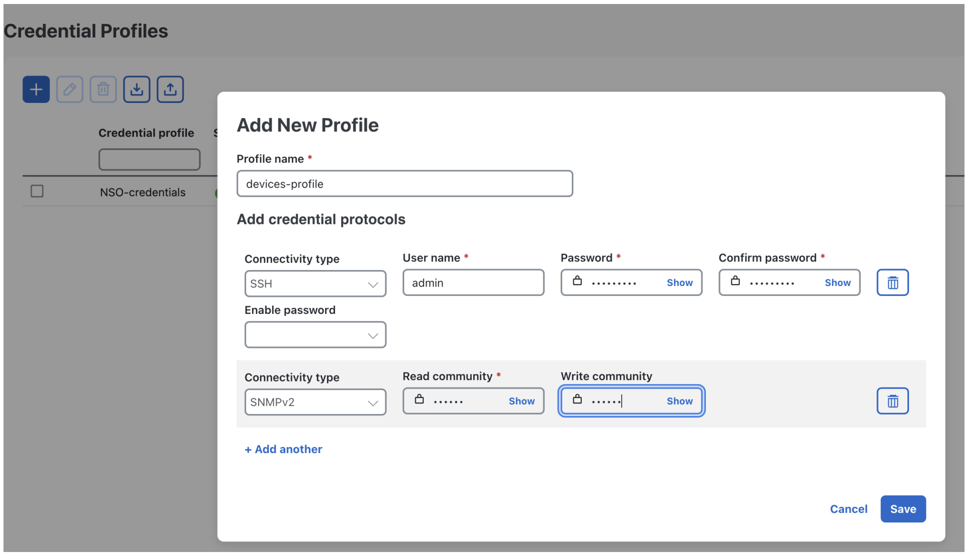
Connectivity type: HTTPS | User name *: admin1 | Password *: ············ | Confirm password *: ············

d) When you are finished, click **Save** to save the NSO credential profile. You should see the **Profile name** you specified appear on the **Credential Profiles** list.

Step 3 **(Optional) Repeat Step 2 to create another credential profile for your devices**. You will want to add as many device login credentials and protocols as are appropriate for the devices you intend to manage using Crosswork Workflow Manager Solutions. Don't add protocols to a credential profile if the devices you are managing are not using those protocols. The following table provides a survey of all the protocols you can add to a Crosswork credential profile and the kinds of device functions they support.

Protocol	Used For
SSH	Devices providing IoT device control and secure file transfer. Common used protocol for device management.
NETCONF	Remote configuration and RPC exchange, typically used with SSH.
HTTP	Hosts providing insecure web resource access.
HTTPS	Hosts providing secure, encrypted web resource exchange.
SCP	Devices providing secure, encrypted file exchange relying on SSH.
TELNET	A common protocol for console access, used for most Cisco XR, Cisco XE, and Juniper Junos devices.
SNMPv2	Standard protocol for device management, used with many devices.
gRPC	Devices participating in high-performance distributed systems. It allows client applications to directly invoke remote procedure calls on server applications as if they were local. An alternative to REST.
SNMPv3	Latest version of the standard protocol for device management, used with some newer devices.
gNMI	Devices providing real-time network monitoring, telemetry and device management in secure streaming format. Often used in place of SNMP by data centers and service providers.

The following figure shows how you might create a single device credential profile that for two of the most commonly used protocols. You might create multiple credential profiles like this if you have groups of devices using the same two protocols but with different credentials.



Add New Profile

Profile name *: devices-profile

Add credential protocols

Connectivity type: SSH
User name *: admin
Password *: ·········
Confirm password *: ·········
Enable password:

Connectivity type: SNMPv2
Read community *: ······
Write community: ······

Create an NSO provider profile

A Crosswork provider is a helper application that lets Crosswork perform special functions. In this task, we will use the NSO credential profile to create an NSO provider and give it the information it needs to authenticate with Crosswork. NSO will then be able to access the device authentication information stored in the device credential profile we created.

Before you begin

Ensure that you've already created the credential profiles explained in Create Crosswork credential profiles, on page 48. You will need the name of the NSO credential profile you created during that task to complete the following task.

Procedure

Step 1 Log in to Crosswork and select **Administration** > **Manage Provider Access**.

Step 2 Click + to add an NSO provider.

Step 3 Complete the first set of fields on the **Add New Profile** window as follows:

In this field...	Enter or select:
Provider name	The name of the provider, such as `NSO`.

In this field...	Enter or select:
Credential profile	The name of the NSO credential profile you created in Create Crosswork credential profiles, on page 48.
Family	`NSO`

Step 4 Complete the fields on the **Connection type(s)** section as follows:

In this field...	Enter or select:
Protocol	Select the principal protocol that the Cisco Crosswork application will use to connect to the provider. Select `HTTPS`. To add more connectivity protocols for this provider, click the ⊕ icon at the end of the first row. To delete a protocol you have entered, click the ⊗ icon shown next to that row. You can enter as many sets of connectivity details as you want, including multiple sets for the same protocol.
Server details	Select one of these options: • **IP Address**, then enter the NSO host's **IP Address** (IPv4 or IPv6, with subnet mask). • **FQDN**, then enter the NSO host's **Domain Name** and **Host Name**.
Port	The port number to use to connect to the NSO host. This is the port corresponding to the protocol being configured. For example, if the protocol used to communicate with the NSO host is SSH, the port number is usually 22.
Timeout (sec)	The amount of time (in seconds) to wait before the connection times out. The default is 30 seconds.

Step 5 Entries in the **Provider Properties** section are optional. If needed, enter one or more of the following key/value pairs:

Property Key	Value
`forward`	`true` This property is necessary when using Crosswork to allow provisioning operations within the UI and to enable the northbound interface to NSO via the Crosswork API gateway. **Note** The default value of `forward` is "false". If this is not changed, the devices added to Crosswork will not be added to NSO. This setting is used in conjunction with the **Edit Policy** option.

Property Key	Value
nso_crosslaunch_url **Note** This property is used for NSO providers only.	Enter the URL for cross-launching NSO in the format: **https://<NSO IP address/FQDN>: port number** To enable cross-launch of the NSO application from the Crosswork UI. Requires a valid protocol (**HTTP** or **HTTPS**), and the provider must be reachable. A cross-launch icon is displayed in the **Provider Name** column. Alternately, you can cross launch the NSO application using a launch icon located at the top right corner of the window.

input_url_prefix
Note
This property is used only for NSO LSA providers.
	Enter the RFS ID in the format: **/rfc-x**, where **x** refers to the number of the RFS node.
	`Example (for RFS node 1):`
	`input_url_prefix: /rfc-1`

Step 6 Complete the fields in the **Model Prefix Info** section as follows:

In this field...	Enter or select:
Model	Select the model prefix that matches the NED CLI used by Cisco NSO. Valid values are: **Cisco-IOS-XR** **Cisco-IOS-XE** **Cisco-NX-OS** For telemetry, only **Cisco-IOS-XR** is supported. To add more model prefix information for this NSO provider, click the ⊕ icon at the end of any row in the **Model Prefix Info** section. To delete a model prefix you have entered, click the ⊗ icon shown next to that row.
Version	Enter the Cisco NSO NED driver version used on the NSO server.

Step 7 When you are finished, click **Save** to save the NSO Provider profile. After a delay while Crosswork attempts to reach NSO, you should see the profile appear on the **Manage Provider Access** list.

Deploy the NSO Function Packs

Use Crosswork's NSO Deployment Manager to deploy the NSO function packs on NSO. These function packs will provide the basic inventory management and other NSO capabilities needed to use Crosswork Workflow Manager Solutions. You will also need to log in to NSO directly, to ensure that NACM is enabled on NSO and that other NSO settings are properly configured.

Before you begin

Ensure you have added NSO as a provider as explained in Create an NSO provider profile, on page 51.

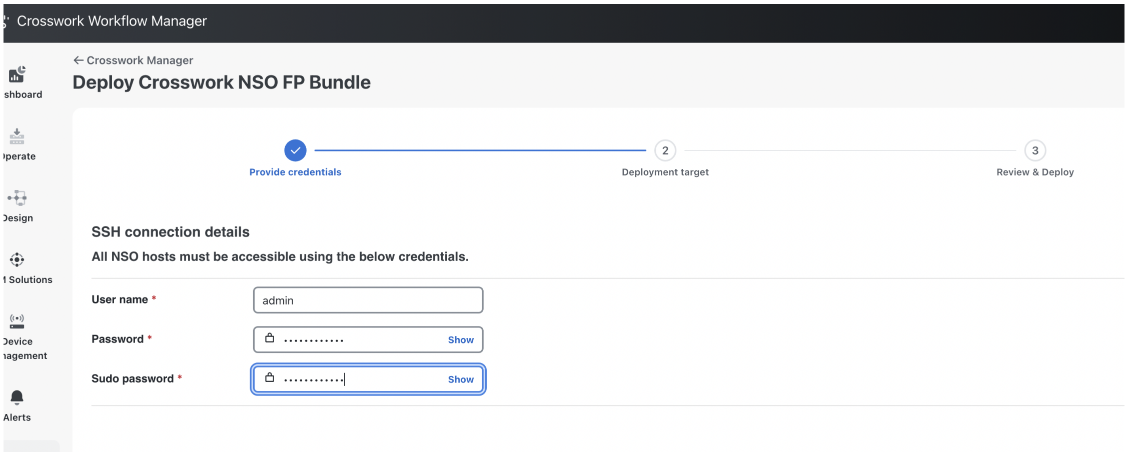
Procedure

Step 1 If you have not already done so: Contact your Cisco Sales team to identify and download the Cisco NSO Network Element Drivers (NEDs) required for your network environment. Before proceeding, install these NEDs on your NSO server, as explained in Install New NEDs.

Step 2 Once the NEDs are installed: Log in to Crosswork Workflow Manager and choose **Administration** > **Crosswork Manager** > **NSO Deployment Manager**.

Step 3 Under **NSO Deployment Manager**, choose the **NSO function pack bundles** tab and click the check box next to **CWM SOLUTIONS FPS**. Then click the **Deploy** button to start the deployment process.

Step 4 When prompted on the first **Provide credentials** page, provide the SSH **User name**, **password** and **Sudo password** credentials.



Deploy Crosswork NSO FP Bundle

SSH connection details

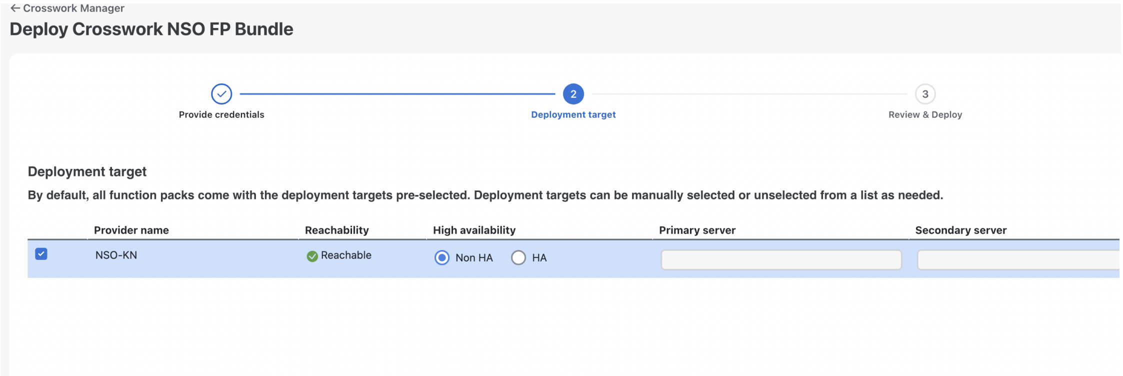
All NSO hosts must be accessible using the below credentials.

User name * admin

Password * ············

Sudo password * ············

Step 5 On the **Deployment target** page, select **Non-HA** in the **High Availability** column, as shown below.



Deploy Crosswork NSO FP Bundle

Deployment target

By default, all function packs come with the deployment targets pre-selected. Deployment targets can be manually selected or unselected from a list as needed.

	Provider name	Reachability	High availability	Primary server	Secondary server
☑	NSO-KN	✓ Reachable	● Non HA ○ HA		

Step 6 When prompted on the **Review & Deploy** page, click **Deploy**.

Step 7 Click the **Job History** tab to monitor the NSO deployment as it proceeds. You will see the packages listed in the **Job Details** window for the running job.

Step 8 When the job is listed as **Succeeded**, click the **Installed NSO function packs** tab and expand the NSO provider to verify that the packages are all installed.

The package list should look like the illustration below.

You can also verify that all the packages are installed correctly by running the `show packages` command on NSO with the options shown below and then comparing your command output with the results in the following figure. The figure represents a minimum list of packages. You may have more, and some packages may have later versions.

```
admin1@ncs% run show packages package oper-status | tab

                           PROGRAM
                           CODE     JAVA           PYTHON
NAME                   UP  ERROR    UNINITIALIZED  UNINITIALIZED
-----------------------------------------------------------------
cisco-ios-cli-6.107    X   -        -              -
cisco-iosxr-7.70       X   -        -              -
cisco-ztp              X   -        -              -
dlm-svc                X   -        -              -
fleet-upgrade          X   -        -              -
goldenconfig           X   -        -              -
inventory              X   -        -              -
inventory-junos        X   -        -              -
juniper-junos-nc-4.17  X   -        -              -
resource-manager       X   -        -              -

admin1@ncs% run show packages package package-version  | tab
                       PACKAGE
NAME                   VERSION
--------------------------------
cisco-ios-cli-6.107    6.107.2
cisco-iosxr-7.70       7.70
cisco-ztp              2.1.0
dlm-svc                7.2.0
fleet-upgrade          2.1.0
goldenconfig           2.1.0
inventory              2.1.0
inventory-junos        2.1.0
juniper-junos-nc-4.17  4.17.14
resource-manager       4.2.9
```

Step 9 If you haven't already done so, log in to NSO and set the following device global settings in configuration mode. These NSO settings are required for Crosswork Workflow Manager Solutions.

```
admin@ncs% set devices global-settings connect-timeout 600
admin@ncs% set devices global-settings read-timeout 600
admin@ncs% set devices global-settings write-timeout 600
admin@ncs% set devices global-settings ssh-algorithms public-key ssh-rsa
admin@ncs% set devices global-settings trace pretty
admin@ncs% set devices global-settings ned-settings
                           cisco-iosxr read admin-show-running-config false
admin@ncs% commit

admin@ncs% show devices global-settings
connect-timeout 600;
read-timeout    600;
write-timeout   600;
ssh-algorithms {
    public-key [ ssh-rsa ];
}
trace           pretty;
ned-settings {
    cisco-iosxr {
        read {
            admin-show-running-config false;
        }
    }
}
```

Step 10 Note that NETCONF Access Control Model (NACM) is required for NSO. Ensure that the NACM rule list grants ncsadmin and the Linux user rights to perform functions on NSO. For example:

```
admin@ncs% set nacm groups group ncsadmin user-name admin
admin@ncs% commit


admin@ncs% show nacm
read-default     deny;
write-default    deny;
exec-default     deny;
groups {
    group ncsadmin {
        user-name [ admin private ];
    }
    group ncsoper {
        user-name [ public ];
    }
}
```

Step 11 Copy the `ncs_backup.sh`, `ncs_restore.sh` and `get_technical_support_data.sh` scripts from the provided bundle to the `scripts` directory under the `NCS_RUN_DIR`, and update the permissions of the copied scripts to make them executable.

```
# Locate the NCS_RUN_DIR using the following command
cat /etc/systemd/system/ncs.service | grep NCS_RUN_DIR=

# Update the permissions
chmod +x ncs_backup.sh ncs_restore.sh get_technical_support_data.sh
```

CHAPTER 7

Upgrade CWM Solutions

This chapter lists the configuration tasks required to migrate CWM Solutions to the latest version.

CWM Solutions upgrade workflow

This section describes the steps to migrate data from CWM Solutions version 2.0 to version 2.1.

1. Before you migrate, on page 57
2. Back up the CWM Solutions data, on page 57
3. Upgrade NSO, on page 58
4. Restore the CWM Solutions data backup, on page 62
5. Post-migration checks, on page 62

Before you migrate

- Confirm that all applications and pods are in a healthy, non-degraded, and fully functional state.
- Ensure that all NSO providers are reachable and healthy.
- Verify that every device has an administrative state of `UP` and an NSO state of **synced**.

Back up the CWM Solutions data

Before moving to the new version, you must create a secure backup of your current data.

Note This procedure applies only if you are already using CWM Solutions version 2.0 on Crosswork platform version 7.1.

Procedure

Step 1 **Configure destination for backup**:

a) Go to **Administration** > **Backup and Restore**.

b) Click **Destination** and provide relevant details in the **Add Destination** drawer window.

- Host name (FQDN) or IP address
- Access port
- Username and password
- Server path or location

Click **Save** to confirm your changes.

Step 2 **Create a data backup file**:

a) Go to **Administration** > **Backup and Restore**.

b) Click **Actions** > **Data Backup**.

c) In the **Data Backup** dialog box, Provide a relevant name in the **Job Name** field.

d) Check the **Backup NSO** checkbox .

e) Verify that the destination information matches the details entered in the previous step.

f) Click **Verify backup readiness** to confirm sufficient resources for the backup. If successful, click **OK** to acknowledge the warning about the operation's duration.

g) Click **Backup** to execute the backup.

The system creates a backup job set and adds it to the job list. The **Job details** panel reports the status of each backup step.

Note
Applications will enter maintenance mode and be inaccessible for approximately five minutes during the backup process.

Step 3 **Verify backup completion**:

a) Monitor the backup progress in the **Job details** panel.

b) Select the job entry and confirm that the status is **Completed successfully** and all sub-tasks are finished.

c) Once the backup is confirmed, shut down the Crosswork platform 7.1 instance.

Upgrade NSO

This section provides a detailed procedure for upgrading Cisco NSO from version **6.4.1.1** to **6.4.8.1**. This upgrade is a critical component of the migration from CWM Solutions 2.0 to version 2.1.0.

The upgrade process involves moving the NSO and the associated packages to newer versions to support migration of CWM Solutions. This procedure ensures that the NSO instance, core packages, function packs, and Network Element Drivers (NEDs) are correctly aligned with the new system requirements.

1. NSO upgrade prerequisites, on page 59

2. Install new NSO version and update configuration, on page 59
3. Manage CWM Solution packages, on page 60
4. NSO startup and validation, on page 60
5. Verification and device migration, on page 61

NSO upgrade prerequisites

- Ensure that the NSO instance and its packages are fully operational and in a **healthy** condition on Crosswork Manager before starting.
- Perform a full backup of NSO. For detailed instructions, see the NSO documentation. Store the backup tar file outside of `/var/opt/ncs` to prevent data loss.
- Ensure you have downloaded the required NSO 6.4.8.1 installer and CWM Solutions 2.1.0 packages from the Cisco software portal.

Install new NSO version and update configuration

Follow these steps to stop the current NSO instance and install the new version in **system install** mode.

Procedure

Step 1 Run the following command to stop the NSO service:

```
$ sudo systemctl stop ncs
```

Step 2 Run the installer with the system install flag to install the new NSO version:

```
$ sudo sh nso-6.4.8.1.linux.x86_64.installer.bin --system-install
```

Step 3 Switch to the NSO directory and update the "current" symbolic link to point to the new version:

```
$ sudo -s
# cd /opt/ncs
# rm -f current
# ln -s ncs-6.4.8.1 current
# exit
```

Step 4 Update `ncs.conf`.

a) Back up the current `/etc/ncs/ncs.conf`.

b) Locate the new template at `/opt/ncs/ncs-6.4.8.1/etc/ncs/ncs.conf.install`.

c) Modify the template to include custom configurations from your original `ncs.conf`.

Important
Ensure you carry over all <encrypted-strings> values to maintain device connectivity.

Step 5 Replace `/etc/ncs/ncs.conf` with the modified version.

Manage CWM Solution packages

Follow this procedure to uninstall old package links and install the CWM Solution 2.1.0 core and supporting packages.

Procedure

Step 1 Remove old symbolic links by deleting the links for the 6.4.1.1 packages in the runtime directory.

Caution
Do not remove existing NED packages at this stage.

```
$ sudo rm /var/opt/ncs/packages/ncs-6.4.1.1-cisco-ztp-2.0.0.tar.gz
$ sudo rm /var/opt/ncs/packages/ncs-6.4.1.1-dlm-svc-7.1.0-74.tar.gz
$ sudo rm /var/opt/ncs/packages/ncs-6.4.1.1-fleet-upgrade-2.0.0.tar.gz
$ sudo rm /var/opt/ncs/packages/ncs-6.4.1.1-goldenconfig-2.0.0.tar.gz
$ sudo rm /var/opt/ncs/packages/ncs-6.4.1.1-inventory-2.0.0.tar.gz
$ sudo rm /var/opt/ncs/packages/ncs-6.4.1.1-inventory-junos-2.0.0.tar.gz
$ sudo rm /var/opt/ncs/packages/ncs-6.4.1-resource-manager-4.2.9.tar.gz
```

Step 2 Install CWM Solutions 2.1.0 core packages.

a) Unpack the CWM Solutions 2.1.0 tarball.
b) Copy the packages to `/opt/ncs/packages/`.
c) Create symbolic links to `/var/opt/ncs/packages/`.

For example, to link the Zero Touch Provisioning package:

```
$ sudo cp ncs-6.4.8.1-cisco-ztp-2.1.0.tar.gz /opt/ncs/packages
$ sudo ln -s /opt/ncs/packages/ncs-6.4.8.1-cisco-ztp-2.1.0.tar.gz /var/opt/ncs/packages
```

d) Repeat these steps for the Fleet Upgrade, Golden Config, Inventory, and Resource Manager packages.

Step 3 Install DLM function pack and NEDs.

a) Install the DLM CFP package (`ncs-6.4.7-dlm-svc-7.2.0-85.tar.gz`).
b) Install the required NEDs (for example, `Cisco IOS-XR 7.70`, `IOS-XE 6.107`, and `Juniper JunOS 4.18.26`).

Step 4 Install the Backup Restore scripts.

Copy these scripts from the CWM Solutions 2.1.0 package to the NSO scripts folder to support Crosswork Infrastructure functions:

```
$ sudo cp ncs_backup.sh /var/opt/ncs/scripts/
$ sudo cp ncs_migrate.sh /var/opt/ncs/scripts/
$ sudo cp ncs_restore.sh /var/opt/ncs/scripts/
```

NSO startup and validation

Perform a controlled restart of NSO to force package reloading and ignore initial validation errors during the transition.

Procedure

Step 1 Modify the `ncs.service` file by adding the `--ignore-initial-validation` flag to the `ExecStart` line in `/etc/systemd/system/ncs.service`:

```
ExecStart=/bin/sh -ac '. ${NCSDIR}/ncsrc; exec ${NCSDIR}/bin/ncs --cd ${NCS_RUN_DIR} --heart
--ignore-initial-validation -c ${NCS_CONFIG_DIR}/ncs.conf'
```

Reload systemd: `$ sudo systemctl daemon-reload`

Step 2 Force a package reload by editing `/etc/ncs/ncs.systemd.conf` and setting `NCS_RELOAD_PACKAGES=force`. Then, restart NSO:

```
$ sudo systemctl restart ncs
```

Step 3 Once NSO is running, revert `NCS_RELOAD_PACKAGES` to `false` in `ncs.systemd.conf` and remove the `--ignore-initial-validation` flag from `ncs.service`. Reload systemd again.

Verification and device migration

Verify the upgrade and migrate devices to the new NED versions.

Procedure

Step 1 Verify the NSO version.

Run the following command and confirm the output:

```
$ ncs --version
# Expected Output: 6.4.8.1
```

Step 2 Check package status.

Log in to the NSO CLI and verify that all packages show `UP` in the operational status:

```
user@ncs> show packages package oper-status up
```

Step 3 Migrate devices to the new NED versions (`NED_ID`). Always perform a dry-run first to check for schema changes:

```
user@ncs% request devices device <DEVICE_NAME> migrate new-ned-id <NEW_NED_ID> dry-run verbose
user@ncs% request devices device <DEVICE_NAME> migrate new-ned-id <NEW_NED_ID> no-networking
```

Step 4 Perform a **sync-from** to pull new capabilities and verify backpointers:

```
user@ncs% request devices device <DEVICE_NAME> sync-from
user@ncs% show devices device <DEVICE_NAME> config | display service-meta-data
```

Step 5 (Optional) After successful migration, remove the old NED packages and their symbolic links from `/opt/ncs/packages/` and `/var/opt/ncs/packages/`.

Restore the CWM Solutions data backup

After deploying Crosswork platform infrastructure version 7.2, follow these steps to restore the CWM Solutions data backup.

Procedure

Step 1 **Verify instance readiness**:

a) Go to **Administration** > **Crosswork Manager** > **Crosswork health**.
b) Confirm all applications and microservices/pods are in **healthy** status.
c) Ensure the NSO provider is reachable.

Step 2 **Configure destination for restore**:

a) Go to **Administration** > **Backup and Restore**.
b) Click **Destination** and provide information on the host or server where the Crosswork platform 7.1 backup is stored (use the same details as in Back up the CWM Solutions data, on page 57.

Step 3 **Restore the data backup file**:

a) Go to **Administration** > **Backup and Restore**.
b) Select **Actions** > **Data migration** and enter the name of the backup file created in Back up the CWM Solutions data, on page 57.
c) Click **Start migration**. The system creates a migration job set and adds it to the job list. The **Job details** panel reports the status of each migration step.

Step 4 **Verify migration completion**:

a) Monitor the job progress in the **Job details** panel.
b) Select the job entry and confirm that the status is **Completed successfully** and all sub-tasks are finished.

Post-migration checks

Perform these checks to ensure data integrity and functionality in CWM Solutions version 2.1.

Table 6: Post-migration checks

Feature	Navigation path	Verification criteria
Workers	**Administration > Workflow Administration > Workers**	Confirm that all workers display • **Admin state** as **UP** • **Operational Status** as **running**
Adapters	**Administration > Workflow Administration > Adapters**	Ensure both old and new adapters are present; verify the current version is **Set as default**, and **In Use** is set to **True**.
NSO providers	**Administration > Manage Provider Access**	Verify that the provider is present and in **Reachable** status.

Feature	Navigation path	Verification criteria
CWM Solutions resources	**Administration** > **Workflow Administration** > **Resources**	Confirm that resources are present and accessible.
Network devices	**Device Management** > **Network Devices**	Ensure all previously onboarded devices show • **Admin state** as **UP** • **NSO state** as **Synced**
MOP list	**CWM Solutions** > **MOPs**	Confirm that previously created MOPs are imported and accessible.
Image policy	**CWM Solutions** > **Fleet Upgrade** > **Software conformance** > **Image policies**	Verify that existing image policies are present.
Conformance reports	**CWM Solutions** > **Fleet Upgrade** > **Software conformance** > **Conformance reports**	Confirm that previous reports are carried over and can be re-run.
Image repository	**CWM Solutions** > **Fleet Upgrade** > **Image repository** > **Local repository**	Validate that uploaded image artifacts are intact.
Fleet upgrade	**CWM Solutions** > **Fleet Upgrade**	Select images and initiate a "New Software Update" job to test operational soundness.