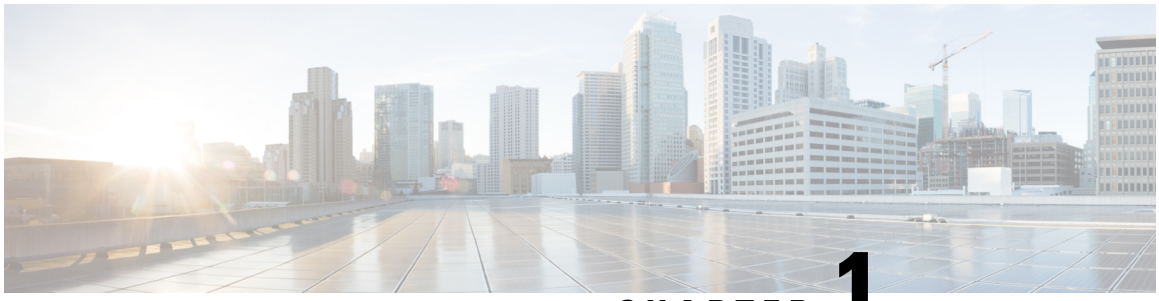
Cisco Crosswork Planning 7.2 Installation Guide

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

CONTENTS



CHAPTER 1

Getting started

This guide explains the requirements and processes to install and upgrade Cisco Crosswork Planning. For detailed information on how to use the Cisco Crosswork Planning Design and Cisco Crosswork Planning Collector applications, see the *Cisco Crosswork Planning Design 7.2 User Guide* and *Cisco Crosswork Planning 7.2 Collection Setup and Administration*.

This chapter contains these topics:

Audience

This guide is for experienced network users and operators who want to install Cisco Crosswork Planning in their network. This guide assumes that you are familiar with

- using a Docker container
- running scripts in Python
- deploying OVF templates using VMware vCenter, and
- deploying using OVF tool.

Core capabilities of Cisco Crosswork Planning

Cisco Crosswork Planning provides tools to create a model of the existing network by continuously monitoring the network and its traffic demands. At a given time, this network model contains all relevant information about a network, including topology, configuration, and traffic information. You can use this information as a basis for analyzing the impact on the network due to changes in traffic demands, paths, node and link failures, network optimizations, or other changes.

Key features

Some important features of Cisco Crosswork Planning include:

- Traffic engineering and network optimization: Compute TE LSP configuration to meet service level requirements, perform capacity management, and perform local or global optimization in order to maximize efficiency of deployed network resources.
- Demand engineering: Examine the impact on network traffic flow of adding, removing, or modifying traffic demands on the network.
- Topology and predictive analysis: Observe the impact to network performance of changes in the network topology, which is driven either by design or by network failures.
- TE tunnel programming: Examine the impact of modifying tunnel parameters, such as the tunnel path and reserved bandwidth.
- Class of service (CoS)-aware bandwidth on demand: Examine existing network traffic and demands, and admit a set of service-class-specific demands between routers.

Cisco Crosswork Planning applications

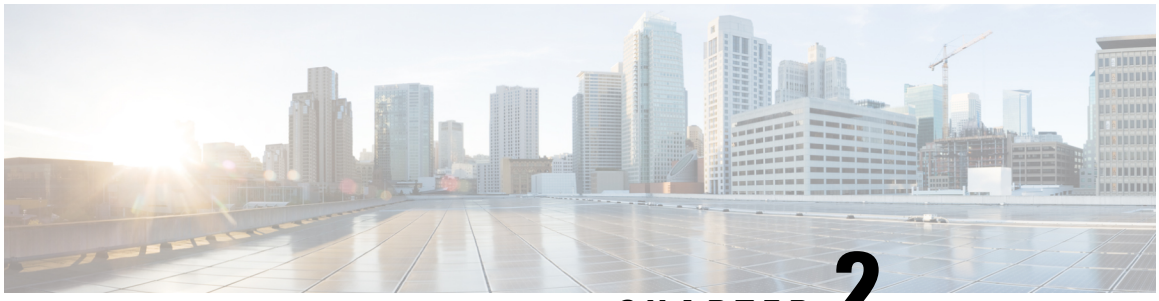
Cisco Crosswork Planning comprises two components. These components run independently. You can enable or disable them based on your requirements.

Cisco Crosswork Planning Collector

Cisco Crosswork Planning Collector consists of a set of services that create, maintain, and archive a model of the current network. It achieves this through continual monitoring and analysis of the network and the traffic demands placed on it. For more information, see *Cisco Crosswork Planning 7.2 Collection Setup and Administration*.

Cisco Crosswork Planning Design

Cisco Crosswork Planning Design is a network design and planning tool. It helps network engineers and operators predict growth in their network, simulate failures, and optimize design to meet performance objectives while minimizing cost. For more information, see *Cisco Crosswork Planning Design 7.2 User Guide*.



CHAPTER 2

Installation Requirements

Profile specifications

This table provides an overview of the scale support for various features and the hardware specifications for each profile in Cisco Crosswork Planning.

Table 1: Profile specifications

Parameters	Profile 1	Profile 2	Profile 3
Scale support			
Total number of network devices	1000	3000	6000
Total number of interfaces (including virtual interfaces)	40000	100000	200000
Total number of demands	50000	100000	500000
Total number of policies (SR and RSVP)	2000	5000	10000
Total number of VPNs	4 Endpoints per VPN service: 30	4 Endpoints per VPN service: 60	8 Endpoints per VPN service: 80
Hardware requirements			

Parameters	Profile 1	Profile 2	Profile 3
Number of VMs	1	2	2
CPU	16 vCPU	16 vCPU	24 vCPU
Memory	125 GB	125 GB	256 GB
Disk space	1 TB	1 TB	2 TB

Note

- For Profile 2 and Profile 3, two VMs are necessary: one operates exclusively as the Collector application, and the other functions as the Design application.
- There is no provision to tune the resource usage settings for individual services.

VMware settings

If your vCenter data center does not meet these requirements, you must deploy the Virtual Machine (VM) individually. For more information on manual installation, see Install Cisco Crosswork Planning using the vCenter vSphere UI.

- Supported 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)
- The machine where you run the installer must have high-speed network connectivity to the vCenter data center where you plan to install Cisco Crosswork Planning.
- Host the Cisco Crosswork Planning VM on hardware with Hyper Threading disabled.
- Ensure that the vCenter admin user has enabled profile-driven storage. Verify that the vCenter user has the necessary query permissions at the root level for all resources in vCenter.
- Build and configure the networks required for Crosswork Management and Data in the data centers. These networks must allow low-latency L2 communication (latency with RTT ≤10 ms).
- Ensure that the user account used to access vCenter has these privileges:
  - VM (Provisioning): Clone the VM on the VM you are cloning.
  - VM (Provisioning): Customize the VM or VM folder if you are customizing the guest operating system.
  - VM (Inventory): Create a new VM from an existing VM in the data center or VM folder.
  - VM (Configuration): Add new disk on the data center or VM folder.
  - Resource: Assign a VM to resource pool on the destination host or resource pool.
  - Datastore: Allocate space in 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.

- We also recommend that you enable vCenter storage control.

Cisco Crosswork Planning VM requirements

This table describes the resource requirements per VM to deploy Cisco Crosswork Planning.

Table 2: 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.

Requirement	Description
IP addresses	Four IPv4 addresses: One management and one data IP address for the Cisco Crosswork Planning node being deployed, and two additional IP addresses to be used as the Virtual IP (VIP) address (one for the Management network and one for the Data network). **Note** The assignment of VIP addresses follows the standard configuration approach used in clustered environments. In a Cisco Crosswork Planning (single node) deployment, these addresses are included for consistency; they are allocated but are not used for high availability functions. • **Management IP address:** Used for user access and node management. • **Data IP address:** Used for communication with external devices and for data collection. • **Management VIP address:** An additional IP address for the management network. It is typically used in clustered environments to provide high availability and seamless management access. In a Cisco Crosswork Planning (single node) deployment, this serves as a placeholder. • **Data VIP Address:** An additional IP address for the data network. It is generally used in clusters to ensure data network availability. In a Cisco Crosswork Planning (single node) deployment, this serves as a placeholder. **Note** • Cisco Crosswork Planning does not support dual-stack and IPv6 configurations. Therefore, all addresses for the environment must be IPv4. • The IP addresses must be able to reach the gateway address for the network, or the installation will fail. • At this time, your IP allocation is permanent. If you want to change your IP allocation, you must redeploy. For more information, contact the Cisco Customer Experience team.
Interfaces	Cisco Crosswork Planning is deployed on a single VM with two interfaces. • Number 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).
NTP server	The IPv4 addresses or host names of the NTP server you plan to use. To specify multiple NTP servers, separate each entry with a space. These should be the same NTP servers you use to synchronize the Cisco Crosswork Planning VM clock, devices, clients, and servers across your network. Ensure that the NTP servers are reachable on the network before attempting installation. The installation will fail if the servers cannot be reached.

Requirement	Description
DNS servers	The IPv4 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. Verify that the DNS servers are reachable on the network you start 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 Planning will back up the configuration of the system to an external server using SCP. The SCP server storage requirements may 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. Cisco Crosswork Planning deployed on a single VM does not support dual-stack and IPv6 configurations. Therefore, all FQDN addresses configured for the deployment environment must be IPv4. **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.

KVM host bare metal requirements

This table describes the host bare metal requirements for deploying Cisco Crosswork Planning on KVM.

Table 3: Host bare metal requirements

Component	Minimum requirement per host
Processor	Intel(R) Xeon(R) CPU E5-2699 v4 @ 2.20GHz or latest
NIC	2 x 10 Gbps NICs.
OS	Red Hat Enterprise Linux 8.10

Resource requirements

This table describes the resource requirements per host.

Table 4: Host resource requirements

Component	Minimum requirement per host	
	Large VM profile	**XLarge VM profile**
RAM	You can calculate the total RAM needed using this formula: Buffer (for example, 20%): RAM per VM * 0.20 Estimated total RAM needed (GB) = Total RAM + Buffer **Example:** RAM per VM (GB): 125 GB Buffer (20%): 125 * 0.20 = 25 GB Estimated total RAM needed (GB): 125 + 25 = 150 GB	You can calculate the total RAM needed using this formula: Buffer (for example, 20%): RAM per VM * 0.20 Estimated total RAM needed (GB) = Total RAM + Buffer **Example:** RAM per VM (GB): 256 GB Buffer (20%): 256 * 0.20 = 51.2 GB Estimated total RAM needed (GB): 256 + 51.2 = 307.2 GB
CPU	You can calculate the number of vCPUs needed using this formula: Buffer (for example, 20%): Total vCPUs * 0.20 Estimated total vCPUs needed = vCPUs per VM + Buffer **Example:** vCPUs per VM: 16 Buffer (20%): 16 * 0.2 = 3.2 Estimated total vCPUs needed: 16 + 3.2 = 19.2	You can calculate the number of vCPUs needed using this formula: Buffer (for example, 20%): Total vCPUs * 0.20 Estimated total vCPUs needed = vCPUs per VM + Buffer **Example:** vCPUs per VM: 24 Buffer (20%): 24 * 0.2 = 4.8 Estimated total vCPUs needed: 24 + 4.8 = 28.8
Storage	You can calculate the storage required using this formula: Buffer: additional 100 GB per VM Estimated total storage needed (GB) = Storage per VM + Buffer **Example:** Storage per VM (GB): 1000 GB Buffer: 100 GB Estimated total storage needed (GB): 1000 + 100 = 1100 GB	You can calculate the storage required using this formula: Buffer: additional 100 GB per VM Estimated total storage needed (GB) = Storage per VM + Buffer **Example:** Storage per VM (GB): 2000 GB Buffer: 100 GB Estimated total storage needed (GB): 2000 + 100 = 2100 GB

It is recommended to allocate a 20% buffer for CPU and memory resources, along with an additional 100 GB of storage per VM. This approach helps ensure smooth performance and minimizes the risk of resource-related issues during operation.

Note

- Ensure the networks required for the Crosswork Management and Data networks are built and configured in the data centers. These networks must allow low-latency L2 communication with a round-trip time (RTT) of 10 ms or less.
- You must use and configure the same network name on the RHEL bare metal host machine that is hosting the Cisco Crosswork Planning VM.

IOS XR and IOS XE version support

Cisco Crosswork Planning supports these Cisco IOS XR and IOS XE software versions.

Table 5: IOS XR/XE version support

Device	Tested with version
SR-PCE (XRv 9000)	IOS XR: 25.4.1
ASR 9000	IOS XR: 25.4.1, 25.3.2, 25.2.2
NCS 5500	IOS XR: 25.4.1, 25.3.2, 25.2.2
Cisco 8000	IOS XR: 25.4.1, 25.3.2, 25.2.2
ASR 920	IOS XE: 17.16.2

Supported web browsers

This table lists the supported browser versions for Cisco Crosswork Planning.

Browser	Version
Google Chrome	131 or later
Mozilla Firefox	136 or later

Port requirements

This table lists the ports used by Cisco Crosswork Planning deployment on the management network.

Table 6: Ports used by Cisco Crosswork Planning

Port	Protocol	Used for	Direction
30602	TCP	Monitoring the installation (Cisco Crosswork Planning)	Inbound
30603	TCP	Cisco Crosswork Planning Web user interface (NGINX server listens for secure connections on port 443)	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
179	TCP	NetFlow BGP	Inbound
830	TCP	Initiating NETCONF	Outbound
30742	TCP	WAE Modeling Daemon (WMD)	Inbound
30744	TCP	OPM/RPC	Inbound
31210	UDP	NetFlow packets	Inbound

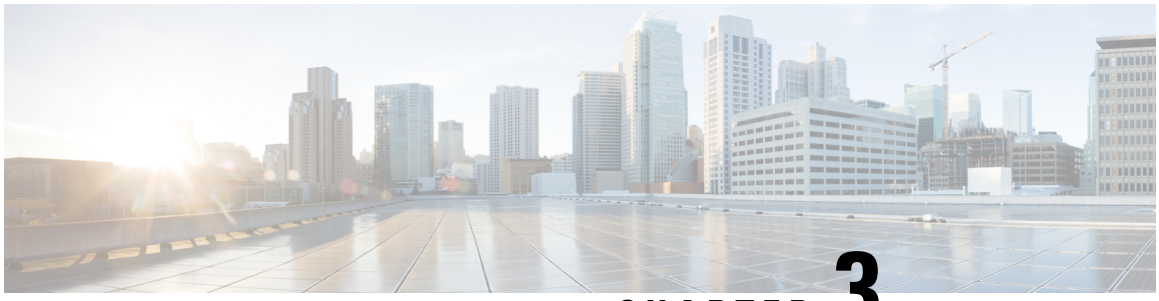
Disk requirements

The VM datastore(s) need to have disk access latency < 10 ms and > 4000 IOPS. For more information on diagnostic checks, see Diagnostic assessment, on page 37.

Table 7: IOPS requirements

IOPS value	Status	Response
IOPS value > 4000	PASS	Installation proceeds without the need for user acknowledgment.

IOPS value	Status	Response
1000 < IOPS value > 4000	BLOCK	For production deployments, the installation requires ~ 4000 IOPS for optimal scaling performance. If the system operates in the suboptimal range of 1000 to 4000 IOPS, the installation process requires user acknowledgment before continuing. If the installation is blocked, you can choose to ignore the failure and continue. You must explicitly acknowledge the report before proceeding, and by doing so, you acknowledge this warning and accept the risks.
IOPS value < 1000	FAIL	Installation is blocked irrespective of user response.



CHAPTER 3

Install Cisco Crosswork Planning

Installation methods

Cisco Crosswork Planning is installed on a single VM or node. In a single VM-based solution, these components are bundled together in a single OVA image. Once you complete the installation procedure, all these components are installed on your machine by default.

- Cisco Crosswork Platform Infrastructure: a microservices-based platform and is the foundation required for running Crosswork applications.
- Cisco Crosswork Planning Collector: provides a set of microservices to create, maintain, and archive a model of the current network.
- Cisco Crosswork Planning Design: provides a set of microservices for network planning, designing, and visualization.
- Cisco Crosswork Planning Infrastructure: provides a set of microservices to manage Smart Licensing and Archive services.

Available installation methods

You can install Cisco Crosswork Planning using these methods:

- vCenter vSphere UI
- OVF tool

- Docker installer tool

Note Installing using the Docker installer tool is less recommended compared to using the vCenter UI or the OVF tool.

For more information on each method, refer to:

- Install Cisco Crosswork Planning using the vCenter vSphere UI, on page 22
- Install Cisco Crosswork Planning using the OVF tool, on page 29
- Install Cisco Crosswork Planning using the Docker installer tool, on page 31

Installation parameters

This section explains the parameters you must specify to install Cisco Crosswork Planning. Ensure you have the relevant information for each parameter mentioned in the table.

Attention Use the latest template file that comes with the Cisco Crosswork Planning build file.

Table 8: General parameters

Parameter	Description
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.
ClusterIPStack	The IP stack protocol: IPv4

vm_sizes	You can create a custom profile. The two profiles supported in Cisco Crosswork Planning are:
	`vm_sizes = {`
	`  "large" = {`
	`  vcpus = 16,`
	`  cpu_reservation = 24000,`
	`  memory = 128000`
	`  },`
	`  "xlarge" = {`
	`  vcpus = 24,`
	`  cpu_reservation = 32000,`
	`  memory = 256000`
	`  }`
	`}`

vcpus	The number of virtual CPU instances allocated for VM.
cpu_reservation	The guaranteed minimum CPU resource allocation for VM.

Parameter	Description
memory	The amount of memory allocation for VM.
ManagementVIP	The Management Virtual IP address for the Crosswork VM.
ManagementIPAddress	The Management IP address of the VM (IPv4).
ManagementIPNetmask	The Management IP subnet in dotted decimal format (IPv4).
ManagementIPGateway	The Gateway IP on the Management Network (IPv4). The address must be reachable; otherwise, the installation will fail.
DataVIP	The Data Virtual IP address for the Crosswork VM.
DataIPAddress	The Data IP address of the VM (IPv4).
DataIPNetmask	The Data IP subnet in dotted decimal format (IPv4).
DataIPGateway	The Gateway IP address on the Data Network (IPv4). The address must be reachable; otherwise, the installation will fail.
DNS	The IP address of the DNS server (IPv4). The address must be reachable; otherwise, the installation will fail.
DomainName	The domain name used for the VM.
CWPassword	Password to log in to Crosswork. When setting up a VM, ensure the password is strong and meets these criteria. • It must be at least eight characters long and include uppercase and lowercase letters, numbers, and at least one special character. • Special characters such as backslash (\), single quote ('), or double quote (") are not allowed. • Avoid using passwords that resemble dictionary words (for example, "Pa55w0rd!") or relatable words. Even if they meet the specified criteria, such passwords are considered weak and will be rejected, resulting in failure to set up the VM.
VMSize	VM size. Cisco Crosswork Planning supports the "Large" and "XLarge" profiles. For more information, see Profile specifications, on page 3.
NTP	NTP server address or name. The address must be reachable; otherwise, the installation will fail.
VMName	Name of the VM.
NodeType	Type of VM. Select "Hybrid".
IsSeed	Set the value to "True".
InitNodeCount	Set the value to 1.

Parameter	Description
InitMasterCount	Set the value to 1.
bckup_min_percent	Minimum percentage of the data disk space to be used for the size of the backup partition. The default is 35. The valid range is from 1 to 80. Use the default value unless recommended otherwise. **Note** The final backup partition size will be calculated dynamically. This parameter defines the minimum.
ThinProvisioned	Set the value to "false" for production deployments.
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.
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"`. 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 /16.
K8sPodNetwork	The network address for the kubernetes pod network. By default, the CIDR range is /16.

Parameter	Description
IgnoreDiagnosticsCheckFailure	Used to set the system response in case of a diagnostic check failure. If set to "false" (default value), 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. We recommend selecting the default value. This parameter accepts a string value, so be sure to enclose the value in double quotes. **Note** • You can find the log files (diagnostic_stdout.log and diagnostic_stderr.log) 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 Crosswork Management VIP via 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 Crosswork Data VIP via 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. The default value is "true", if not explicitly specified. If set to "true", the VM's resources are provided exclusively. In this state, the installation fails if there are insufficient CPU cores, memory or CPU cycles. If set to "false" (used only for lab installations), the VM's resources are allocated on a best-effort basis. In this state, insufficient CPU cores may impact performance or cause installation failure.
corefs	Core partition size in gigabytes (GB). The default is 18 GB and the maximum value is 1000 GB. We recommend using the default value.
ddatafs	Data disk size for the nodes in gigabytes. This is an optional parameter. The default is 485. The valid range is from 450 to 8000. Use the default value unless recommended otherwise.
logfs	Log partition size in gigabytes. The default is 20 GB and the maximum value is 1000 GB. We recommend using the default value.

Parameter	Description
RamDiskSize	Size of the RAM disk. This parameter is only used for lab installations. The value must be at least 2. If you provide a non-zero value for `RamDiskSize`, the `HSDatastore` value is not used.
Timezone	Enter the time zone. Input is a standard IANA time zone. For example, "America/Chicago". If left blank, the default value (UTC) is selected. This is an optional parameter.
UseNonDefaultCalicoBgpPort	Determines whether Calico should use the default port 179 for BGP or an alternative port. Set the value to "True".

Table 9: VMware template parameters

Parameter	Description
VCenterAddress	The vCenter IP or host name.
VCenterUser	The username needed to log in to vCenter.
VCenterPassword	The password needed to log in to vCenter.
DCname	The name of the Data Center resource to use. Example: `DCname = "cp"`
MgmtNetworkName	The name of the vCenter network to attach to the VM 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 Data interface. This network must already exist in VMware or the installation will fail. However, if this is a single NIC installation using only the Management interface, then you need to specify `DataNetworkName = ""`.
HostedCwVMs	The ID of the VM to be hosted by the ESXi host or resource.
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 hosts should be under the data center). If hosts are under a VM in the data center, provide only the VM name to include all hosts within that VM. The subsequent option is to use a resource group. In this case, you must provide a full path. Example: `Host = "Main infrastructure/Resources/00_trial"`

Parameter	Description
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. If the vCenter server has a separate high-speed datastore, set this to the name of that high-speed data store. If the vCenter server uses only a high-speed datastore, then both Datatore and HSDatastore can be set to the same name. **Note** The use of high-speed datastore is mandatory for Cisco Crosswork Planning.

Table 10: Parameters for KVM deployment

Parameter	Description
AdminIPv4Address	The admin IP address of the VM (IPv4).
AdminIPv4Netmask	The admin IP subnet in dotted decimal format (IPv4).
AwsIamRole	The Amazon Web Services IAM role name for the VIP update.
CWPassword	Password to log in to Cisco Crosswork. Password to log in to Crosswork. When setting up a VM, ensure the password is strong and meets these criteria. • It must be at least eight characters long and include uppercase and lowercase letters, numbers, and at least one special character. • Avoid using passwords that resemble dictionary words (for example, "Pa55w0rd!") or relatable words. Even if they meet the specified criteria, such passwords are considered weak and will be rejected, resulting in failure to set up the VM.
CWUsername	Username to log in to Cisco Crosswork.
ClusterCaKey	The CA private key. Use the default value (Empty).
ClusterCaPubKey	The CA public key. Use the default value (Empty).
CwInstaller	Set as "False".
DNSv4	The IP address of the DNS server (IPv4). The address must be reachable; otherwise, the installation will fail.
DataIPv4Address	The Data IP address of the VM (IPv4).

Parameter	Description
DataIPv4Gateway	The Gateway IP address on the Data Network (IPv4). The address must be reachable, otherwise the installation will fail.
DataIPv4Netmask	The Data IP subnet in dotted decimal format (IPv4).
DataPeerIPs	The Data peer IP addresses (IPv4) for the VM.
DataVIP	The Data Virtual IP address for the Crosswork VM.
DataVIPName	Name of the Data Virtual IP address for the Crosswork VM. This is an optional parameter used to reach Crosswork Data VIP via DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server.
Deployment	Enter the deployment type.
Disclaimer	Enter the disclaimer message.
Domain	The domain name used for the VM.
EnableSkipAutoInstallFeature	Pods marked as "skip auto install" will not be brought up until a dependent application or pod explicitly asks for it. Set the value to "True".
EnforcePodReservations	Enforces minimum resource reservations for the pod. If left blank, the default value ("True") is selected.
InitNodeCount	Set the value to 1.
InitMasterCount	Set the value to 1.
IsSeed	Set the value to "True".
K8Orch	Enforces minimum resource reservations for the pod. If left blank, the default value ("True") is selected.
K8sPodNetwork	The network address for the kubernetes pod network. By default, the CIDR range is /16.
K8sServiceNetwork	The network address for the kubernetes service network. By default, the CIDR range is /16.
ManagementIPv4Address	The Management IP address of the VM (IPv4).
ManagementIPv4Gateway	The Gateway IP address on the Management Network (IPv4). The address must be reachable; otherwise, the installation will fail.
ManagementIPv4Netmask	The Management IP subnet in dotted decimal format (IPv4).
ManagementVIP	The Management Virtual IP address for the Crosswork VM.

Parameter	Description
ManagementVIPName	Name of the Management Virtual IP for the Crosswork VM. This is an optional parameter used to reach Crosswork Management VIP via DNS name. If this parameter is used, the corresponding DNS record must exist in the DNS server.
ManagementPeerIPs	The Management peer IP addresses (IPv4) for the VM.
NBIIPv4Address	The NBI IP address of the VM (IPv4).
NBIIPv4Gateway	The Gateway IP address on the NBI Network (IPv4). The address must be reachable; otherwise, the installation will fail.
NBIIPv4Netmask	The NBI IP subnet in dotted decimal format (IPv4).
NBIVIP	The NBI Virtual IP address (IPv4) for the VM.
NTP	NTP server address or name. The address must be reachable; otherwise, the installation will fail.
Timezone	Enter the time zone. Input is a standard IANA time zone. For example, "America/Chicago". If left blank, the default value (UTC) is selected. This is an optional parameter.
VMLocation	Location of the VM.
VMType	Type of VM. Select "Hybrid".
bckup_min_percent	Minimum percentage of the data disk space to be used for the size of the backup partition. The default is 35. The valid range is from 1 to 80. Use the default value unless recommended otherwise. **Note** The final backup partition size will be calculated dynamically. This parameter defines the minimum.
corefs	Core partition size in gigabytes. The default is 18 GB and the maximum value is 1000 GB. We recommend using the default value.
ddatafs	Data disk size for the nodes in gigabytes. This is an optional parameter. The default is 485. The valid range is from 450 to 8000. Use the default value unless recommended otherwise.
logfs	Log partition size in gigabytes. The default is 20 GB and the maximum value is 1000 GB. We recommend using the default value.
ramdisk	Size of the RAM disk. This parameter is only used for lab installations. The value must be at least 2. If you provide a non-zero value for `RamDiskSize`, the `HSDatastore` value is not used.

Parameter	Description
ssd	SSD disk size. This is an optional parameter. The default value is 15. Use the default value unless recommended otherwise.
ThinProvisioned	Set the value to "false" for production deployments.
UseNonDefaultCalicoBgpPort	Determines whether Calico should use the default port 179 for BGP or an alternative port. Set the value to "True".
bootOptions.efiSecureBootEnabled	The default is "False".

Guideline: Use supported settings for custom profiles

Ensure that the vm_sizes parameter is set in accordance with your deployment profile. Supported profiles in Cisco Crosswork Planning include:

```
vm_sizes = {
  "large" = {
    vcpus = 16,
    cpu_reservation = 24000,
    memory = 128000
  },
  "xlarge" = {
    vcpus = 24,
    cpu_reservation = 32000,
    memory = 256000
  }
}
```

Using unsupported settings may result in deployment failure.

Install Cisco Crosswork Planning using the vCenter vSphere UI

This topic explains how to deploy Cisco Crosswork Planning on a single VM using the vCenter user interface.

This is the recommended method for installing Cisco Crosswork Planning on a single VM.

Note When you install Cisco Crosswork Planning using the vCenter vSphere UI, you must import the inventory file manually. For details on importing an inventory file, see Import an inventory file, on page 28.

Procedure

Step 1 Download the latest available Cisco Crosswork Planning image file (*.ova) to your system.

Step 2 Log in to the vSphere web client and select the ESXi host.

a) With VMware ESXi running, log in to the VMware vSphere web client.

b) On the left navigation pane, choose the ESXi host where you want to deploy the VM.

Step 3 Configure virtual switches and networking.

a) 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.

b) In the virtual switch, select **Edit** > **Security**, and configure these DVS port group properties:

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

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

c) 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 Customer Experience team for assistance.

Step 4 Begin the OVF deployment process.

a) 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, and so on) so that you can enter the information quickly and avoid any issues with the VMware configuration.

The VMware **Deploy OVF Template** page appears. The first step, **1 - Select an OVF template**, is highlighted.

Step 5 Specify the VM details, select the resource, and validate the configuration.

a) 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.

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

We recommend that you include the Cisco Crosswork Planning version and build number in the name. For example, Cisco Crosswork Planning 7.2 Build 152.

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

d) 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.

e) Review the OVF template that you are deploying. Note that this information is gathered from the OVF, and cannot be modified.

Note
Even though the **Product** field displays as "Cisco Crosswork Network Automation", once the installation procedure completes, the product name is displayed as "Cisco Crosswork Planning" in the application UI. The term "Cisco Crosswork Network Automation" is used universally for all of the products in the Crosswork portfolio.

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.

f) Click **Next**.
The **Deploy OVF Template** window is refreshed, with **5 - License agreements** highlighted.

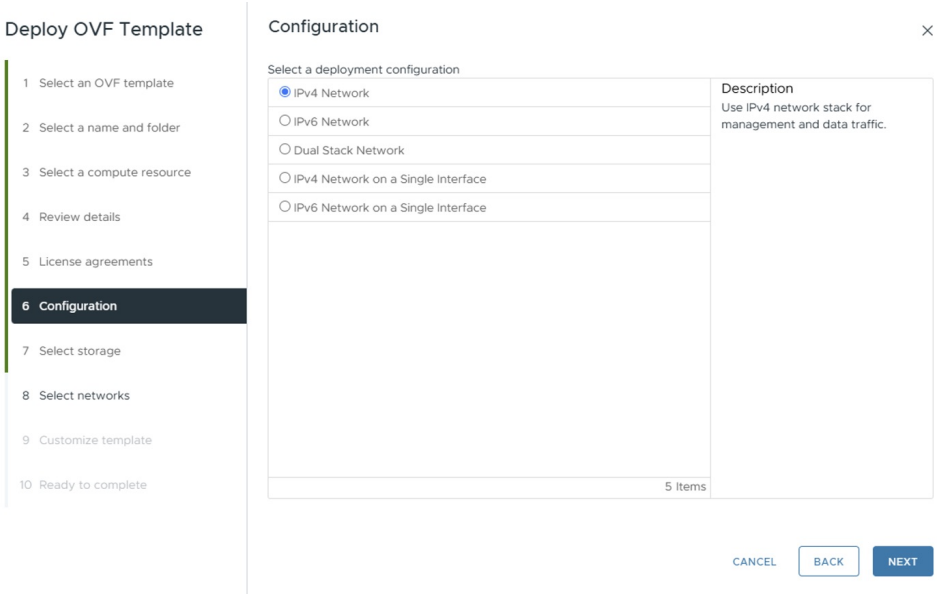
Step 6 Accept the license agreement. Then, select the deployment configuration, storage, and networks.

a) Review the End User License Agreement and if you agree, click the **I accept all license agreements** checkbox. Otherwise, contact your Cisco Customer Experience team for assistance.

b) Click **Next**. The **Deploy OVF Template** window is refreshed, with **6 - Configuration** highlighted. Select the desired deployment configuration.

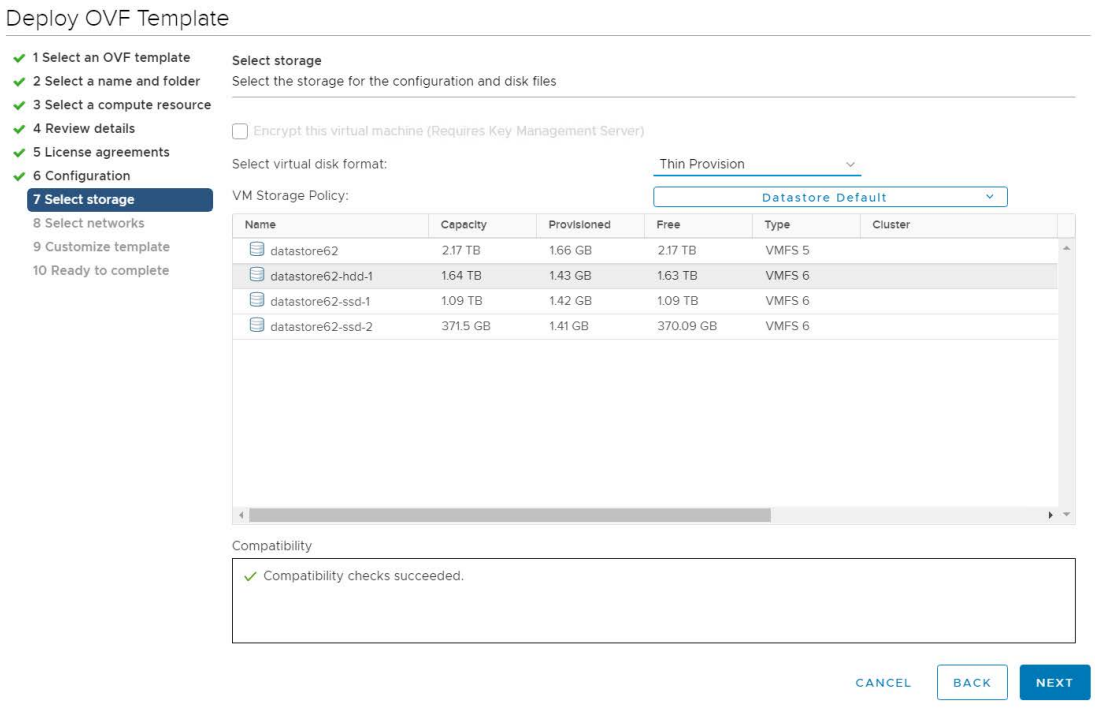
Important
For Cisco Crosswork Planning deployment, the supported configuration is **IPv4 Network** using two NICs.

Figure 1: Select a deployment configuration



c) 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.

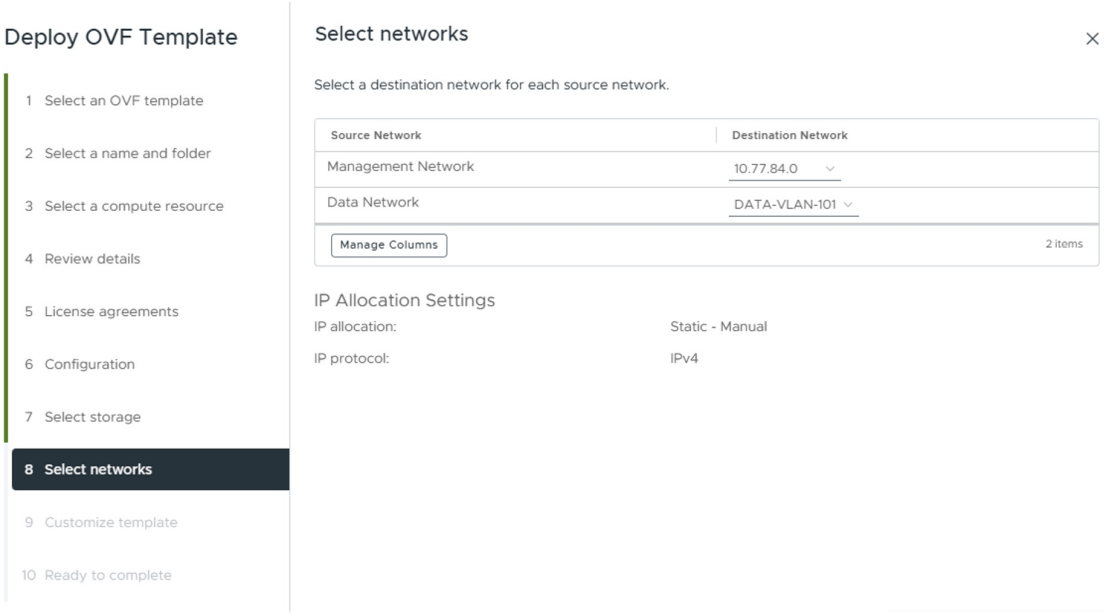
Figure 2: Select storage



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.

d) 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



Step 7 Customize the template.

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

b) Expand the **Management Network** settings. Provide information for the deployment, such as IP address, IP netmask, IP gateway, virtual IP address, and virtual IP DNS name.

c) Expand the **Data Network** settings. Provide information for the deployment, such as IP address, IP netmask, IP gateway, virtual IP address, and virtual IP DNS name.

d) 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 eight characters that combines uppercase and lowercase letters, numbers, and special characters in a non-predictable sequence.

e) Expand the **DNS and NTP Servers** settings. Provide information in these 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.

f) 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.

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

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

- VM Type: Select Hybrid.
- Cluster Seed node: Select 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 location of VM.
- Disclaimer: Enter your legal disclaimer text (you will see this text if you 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 Diagnostics Failure?: Use the default value (False).

Step 8 Complete the deployment.

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

b) After you review your settings, click **Finish** to begin deployment. Wait until the deployment finishes before continuing. To check the deployment status:

1. Open the VMware vCenter client.
2. In the **Recent Tasks** tab of the host VM, view the status of the **Deploy OVF template** and **Import OVF package** jobs.

Step 9 Update the VM settings and power on the VM.

a) After the deployment is complete, right-click the VM and select **Edit Settings**. In the **Edit Settings** dialog box, under the **Virtual Hardware** tab, update these attributes based on your profile requirements.

- CPU: Change to **16** (for Large profile) or **24** (for XLarge profile)
- Memory: Change to **125 GB** (for Large profile) or **256 GB** (for XLarge profile)

For more information, see Profile specifications, on page 3.

Click **OK** to save the changes.

b) Power on the Cisco Crosswork Planning VM. To do this, expand the host's entry, click the Cisco Crosswork Planning VM, and then choose **Actions** > **Power** > **Power On**.

The VM creation time can vary based on your deployment profile size and the performance characteristics of your hardware.

Import an inventory file

If you have installed your VM manually using the vCenter UI, you must import an inventory file (.tfvars file) to Cisco Crosswork Planning to reflect the details of your VM. The inventory file contains information about the VM along with the data center parameters. A sample inventory file can be downloaded from the Cisco Crosswork Planning UI.

Note If the manual installation was performed to replace a failed VM, you must delete the original VM after importing the inventory file.

Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager**.

Step 2 On the **Crosswork Summary** tab, click the **System summary** tile to display the **System Summary** page.

Step 3 Click ••• > **Import inventory** to display the Import Inventory page.

Step 4 (Optional) Click **Download sample template file** to download the template.

Step 5 Update the file with information about the VM in your single VM environment, and include the data center parameters. Then, verify the contents of the template file. For more details on the installation parameters, see Installation parameters, on page 14.

Note
Uncomment or set the "*OP_Status = 2*" parameter while importing the inventory file manually. If you fail to do this, the VM may incorrectly appear as "Initializing" even after becoming functional.

Step 6 Click **Browse** and select the inventory file.

Step 7 Click **Import** to complete the operation.

Install Cisco Crosswork Planning using the OVF tool

This topic explains how to deploy Cisco Crosswork Planning on a single VM using the OVF tool. You must modify the mandatory and optional parameters in the deployment script to match your requirements, and then run the OVF tool.

Note The file names mentioned in this topic are sample names and may differ from the actual file names on cisco.com.

Before you begin

- Ensure you are using the OVF tool version 4.4 or higher.
- In your vCenter data center, perform these steps:
  1. Go to **Host** > **Configure** > **Networking** > **Virtual Switches**.
  2. In the selected virtual switch, select **Edit** > **Security**.
  3. Set **Promiscuous mode** as Reject
  4. Set **MAC address changes** as Reject
  5. Confirm the settings. Repeat the process for each virtual switch used by Cisco Crosswork Planning.

Procedure

Step 1 On the machine where you have the OVF tool installed, use this command to confirm that you have OVF tool version 4.4.

```
ovftool --version
```

Step 2 Create the script file for your target environment. Enter relevant information, such as IP addresses, gateway, netmask, password, VCENTER_PATH, and so on.

Important
Sample script, on page 30 is a sample script for deploying an `XLarge` VM profile. To deploy a `Large` VM profile, replace the `XLarge` values with corresponding values for the `Large` profile.

- **XLarge profile**:

```
--numberOfCpus:"*"=24 --viCpuResource=:32000: \
--memorySize:"*"=256000 --viMemoryResource=:256000: \
```

- **Large profile**:

```
--numberOfCpus:"*"=16 --viCpuResource=:24000: \
--memorySize:"*"=128000 --viMemoryResource=:128000: \
```

Step 3 Download the OVA and install scripts from cisco.com. For the purpose of these instructions, we use the file name as **crosswork-planning-single-node-deployment-7.2.0-45**.

Use this command to extract the files from the tar bundle.

```
tar -xvzf crosswork-planning-single-node-deployment-7.2.0-45.ova
```

The OVA is extracted.

```
cp]# ls -al
-rw-r--r--   1 root root 15416145920 Mar 28 11:12 crosswork-planning-single-node-deployment-7.2.0-45.ova
-rwxr-xr-x   1 root root        2324 Apr  2 14:06 cp_install.sh
```

Step 4 Use this command to make the scripts executable.

```
chmod +x {filename}
```

For example:

```
chmod +x cp_install.sh
```

Step 5 Execute the script with the OVA file name as parameter.

```
cp]# ./cp_install.sh crosswork-planning-single-node-deployment-7.2.0-45.ova
                        VMware ovftool 4.4.0 (build-16360108)
                        Opening OVA source: crosswork-planning-single-node-deployment-7.2.0-45.ova
                        <Removed some output >
                        Completed successfully
```

VM creation time may vary depending on the size of your deployment profile and your hardware performance characteristics.

The Cisco Crosswork Planning is deployed.

Sample script

This section provides a sample script for deploying Cisco Crosswork Planning (`XLarge` VM profile).

```
cat cp_install.sh
#!/usr/bin/env bash
Host="X.X.X.X"
DM="thick"
DS="DS36"
Deployment="cw_ipv4"
DNSv4="10.10.0.99"
NTP="<NTP-Server>"
Timezone="US/Pacific"
EnforcePodReservations="True"
EnableSkipAutoInstallFeature="True"
Domain="cisco.com"
Disclaimer="ACCESS IS MONITORED"
VM_NAME="cp"
DataNetwork="DataNet"
ManagementNetwork="MgmtNet"
DataIPv4Address="x.x.x.x"
DataIPv4Gateway="x.x.x.x"
DataIPv4Netmask="x.x.x.x"
ManagementIPv4Address="x.x.x.x"
ManagementIPv4Gateway="x.x.x.x"
ManagementIPv4Netmask="x.x.x.x"
K8sServiceNetworkV4="10.75.0.0"
K8sPodNetworkV4="10.225.0.0"
Password="CLI Password"
Username="cw-admin"
ManagementVIP="x.x.x.x"
DataVIP="x.x.x.x"
```

```
VMType="Hybrid"
IsSeed="True"
InitNodeCount="1"
InitMasterCount="1"

CP_OVA_PATH=$1

VCENTER_LOGIN="Administrator%40vsphere%2Elocal:Password%40123%21@x.x.x.x"
VCENTER_PATH="DC1/host"

ovftool --version
ovftool --acceptAllEulas --skipManifestCheck --X:injectOvfEnv -ds=$DS \
--numberOfCpus:"*"=24 --viCpuResource=:32000: \
--memorySize:"*"=256000 --viMemoryResource=:256000: \
--diskMode=$DM --overwrite --powerOffTarget --powerOn --noSSLVerify \
--allowExtraConfig \
--deploymentOption=$Deployment \
--prop:"DNSv4=${DNSv4}" \
--prop:"NTP=${NTP}" \
--prop:"Timezone=${Timezone}" \
--prop:"EnforcePodReservations=${EnforcePodReservations}" \
--prop:"EnableSkipAutoInstallFeature=${EnableSkipAutoInstallFeature}" \
--prop:"Domain=${Domain}" \
--prop:"Disclaimer=${Disclaimer}" \
--name=$VM_NAME \
--net:"Data Network=${DataNetwork}" \
--net:"Management Network=${ManagementNetwork}" \
--prop:"DataIPv4Address=${DataIPv4Address}" \
--prop:"DataIPv4Gateway=${DataIPv4Gateway}" \
--prop:"DataIPv4Netmask=${DataIPv4Netmask}" \
--prop:"ManagementIPv4Address=${ManagementIPv4Address}" \
--prop:"ManagementIPv4Gateway=${ManagementIPv4Gateway}" \
--prop:"ManagementIPv4Netmask=${ManagementIPv4Netmask}" \
--prop:"K8sServiceNetworkV4=${K8sServiceNetworkV4}" \
--prop:"K8sPodNetworkV4=${K8sPodNetworkV4}" \
--prop:"CWPassword=${Password}" \
--prop:"CWUsername=${Username}" \
--prop:"ManagementVIP=${ManagementVIP}" \
--prop:"DataVIP=${DataVIP}" \
--prop:"VMType=${VMType}" \
--prop:"IsSeed=${IsSeed}" \
--prop:"InitNodeCount=${InitNodeCount}" \
--prop:"InitMasterCount=${InitMasterCount}" \
$CP_OVA_PATH \
vi://$VCENTER_LOGIN/$VCENTER_PATH/$Host
```

Install Cisco Crosswork Planning using the Docker installer tool

This section explains the procedure to install Cisco Crosswork Planning on a single VM using the docker installer tool.

This method is less recommended compared to using the vCenter UI or the OVF tool for installation.

Before you begin

- Make sure that your environment meets all the vCenter requirements specified in VMware settings, on page 4.

- The edited template in the `/data` directory contains sensitive information (VM passwords and the vCenter password). The operator needs to manage access to this content. Store the templates used for your install in a secure environment or edit them to remove the passwords.
- The `install.log`, `install_tf.log`, and `.tfstate` files will be created during the install and stored in the `/data` directory. If you encounter any trouble with the installation, provide these files to the Cisco Customer Experience team when opening a case.
- 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 installer tool multiple times may result in the deletion and re-creation of VMs.
- In case you are using the same installer tool for multiple Cisco Crosswork Planning 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 for each deployment on the host machine and map each one to the container accordingly.
- Docker version 19 or higher is required while using the installer tool. For more information on Docker, see https://docs.docker.com/get-docker/.
- To change the install parameters or to correct the parameters following the installation errors, it is important to distinguish whether the installation has managed to deploy the VM or not. Deployed VM is evidenced by the output of the installer similar to:

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

- If you do not have Python installed, go to python.org and download the version of Python that is appropriate for your workstation.

Known limitations:

- The vCenter host VMs defined must use the same network names (vSwitch) across all hosts in the data center.
- The vCenter storage folders or datastores organized under a virtual folder structure, are not supported currently. Ensure that the datastores referenced are not grouped under a folder.

Procedure

Step 1 Create a directory for installation files and download the required files.

a) 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.

b) Download the installer bundle (.tar.gz file) and the OVA file from cisco.com to the directory you created previously. For the purpose of these instructions, we will use the file name as **crosswork-planning-single-node-docker-deployment-7.2.0-45.tar.gz** and **crosswork-planning-single-node-deployment-7.2.0-45.ova**.

Attention
The file names mentioned in this topic are sample names and may differ from the actual file names on cisco.com.

Step 2 Unzip and review the installer bundle.

a) Use this command to unzip the installer bundle:

```
tar -xvf crosswork-planning-single-node-docker-deployment-7.2.0-45.tar.gz
```

The installer bundle is unzipped to a new directory. This directory will contain the installer image (cw-na-planning-7.2.0-45-releasecnc720-260127.tar.gz) and the files needed to validate the image.

b) 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 3 Verify the signature of the installer image using this command.

Note
Use `python --version` to find out the version of python on your machine.

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

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s
<.tar.gz.signature file> -v dgst -sha512
```

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

```
python3 cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s
<.tar.gz.signature file> -v dgst -sha512
```

Step 4 Load the installer image into Docker and get the image ID.

a) Use this command to load the installer image file into your Docker environment.

```
docker load -i <.tar.gz file>
```

For example:

```
docker load -i cw-na-planning-7.2.0-45-releasecnc720-260127.tar.gz
```

b) 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: (section we will need is underlined for clarity)

```
My Machine% docker images
REPOSITORY                          TAG                       IMAGE ID      CREATED    SIZE
dockerhub.cisco.com/cw-installer  cw-na-planning-7.2.0-45-
                                    releasecnc720-260127      59c350e0cdf2 7 days ago 414MB
```

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

Step 5 Launch the Docker container using this command:

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

To run the image loaded in our example, use this command:

```
docker run --rm -it -v `pwd`:/data 4b99cf7d0684
```

Note

- You do not have to enter that full value. In this case, `docker run --rm -it -v `pwd`:/data 4b9` was adequate. Docker requires enough of the image ID to uniquely identify the image you want to use for the installation.

- In the above command, we are using the backtick (`). Do not use the single quote or apostrophe (') as the meaning to the shell is very different. By using the backtick (recommended), the template file and OVA will be stored in the directory where you are on your local disk when you run the commands, instead of inside the container.
- CentOS/RHEL 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 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 these 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 4b9
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 6 Prepare the deployment template.

a) Navigate to the directory with the VMware template.

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

b) 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 `deployment.tfvars` in all the examples.

c) Edit the template file located in the `/data` directory in a text editor, to match your planned deployment (for reference, see Sample manifest template, on page 35). The <sample manifest template> includes an example that you can reference for proper formatting. The example is more compact due to the removal of descriptive comments.

Step 7 From the `/opt/installer` directory, run the installer.

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

For example:

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

Step 8 Accept the license agreement and complete the installation.

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

b) Enter "yes" when prompted to confirm the operation.

Note

It is not uncommon to see some warnings like this 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'.
```

If the install process proceeds to a successful conclusion (see sample output below), these warnings can be ignored.

Sample output:

```
cw_vms = <sensitive>
INFO: Copying day 0 state inventory to CW
INFO: Waiting for deployment status server to startup on 10.90.147.66.
Elapsed time 0s, retrying in 30s
Crosswork deployment status available at http://{VIP}:30602/d/NK1bwVxGk/crosswork-
deployment-readiness?orgId=1&refresh=10s&theme=dark
Once deployment is complete login to Crosswork via: https://{VIP}:30603/#/
logincontroller
INFO: Cw Installer operation complete.
```

Note
If the installation fails, open a case with Cisco and provide the .log files that were created in the /data directory (and the local directory where you launched the installer Docker container), to Cisco for review. The two most common reasons for the install to fail are: (a) password that is not adequately complex, and (b) errors in the template file. If the installer fails for any errors in the template (for example, mistyped IP address), correct the error and rerun the install script.

Sample manifest template

This section provides the manifest template example for deploying Cisco Crosswork Planning on a single VM.

```
Cw_VM_Image = "crosswork-planning-single-node-deployment-7.2.0-45"  # Line added automatically
 by installer.
ClusterIPStack = "IPv4"
ManagementVIP = "172.20.118.86"
ManagementIPNetmask = "255.255.255.0"
ManagementIPGateway = "172.20.118.1"
DataVIP = "172.20.118.87"
DataIPNetmask = "255.255.255.0"
DataIPGateway = "172.20.118.1"
DNS = "172.24.97.250"
DomainName = "cisco.com"
CWPassword = "*****!"
VMSize = "Large"
NTP = "ntp.esl.cisco.com"
Timezone = "Asia/Calcutta"
ThinProvisioned = true
EnableHardReservations = false
EnableSkipAutoInstallFeature = "True"
ManagementVIPName = "CP-svm"
EnforcePodReservations = "True"
ThinProvisioned = "true"
ManagerDataFsSize = "2000"
bckup_min_percent = "35"

CwVMs = {
```

```
    "0" = {
        VMName = "vm1",
        ManagementIPAddress = "172.20.118.88",
        DataIPAddress = "172.20.118.89",
        NodeType = "Hybrid"
    }
}

VCentreDC = {
    VCentreAddress = "172.20.118.84",
    VCentreUser = "<your-username>",
    VCentrePassword = "******",
    DCname = "cp",
    MgmtNetworkName = "VM Network",
    DataNetworkName = "vlan101",
    VMs = [
        {
            HostedCwVMs = ["0"],
            Host = "172.20.118.81",
            Datastore = "datastore1 (2)",
            HSDatastore = "datastore1 (2)"
        }
    ]
}
# VM size definitions
UseNonDefaultCalicoBgpPort = "true"
vm_sizes = {
    "large" = {
        vcpus = 16,
        cpu_reservation = 24000,
        memory = 128000
    }
}
SchemaVersion = "7.2.0"
```

Monitor the installation

This topic explains how to monitor and verify if the 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 whether you want to continue the installation. After you confirm, the installation will progress. Any possible errors will be logged in either installer.log or installer_tf.log. If the VM is built and is able to boot, the errors in applying the operator specified configuration will be logged on the VM in the /var/log/firstboot.log file.

Note During installation, Cisco Crosswork Planning will create a special administrative ID (virtual machine (VM) administrator, *cw-admin*, with the password that you provided in the manifest template. In case the installer is unable to apply the password, it creates the administrative ID with the default password *cw-admin*). The first time you log in using this administrative ID, you will be prompted to change the password.

The administrative username is reserved and cannot be changed. Data center administrators use this ID to log in to and troubleshoot the Cisco Crosswork Planning application VM.

These are the steps you can watch for to be certain that things are progressing as expected:

Procedure

Step 1 The installer uploads the Cisco Crosswork Planning image file (.ova file) to the data center.

Step 2 The installer creates the VM and displays a success message, such as "Creation Complete".

Step 3 After the VM is created, it is powered on—either automatically when the installer completes or after you power on the VM during manual installation. The parameters specified in the template are applied to the VM and it is then rebooted.

Step 4 Once the VM becomes accessible, a success message, such as "Crosswork Installer operation complete" appears. The installer script will exit and return you to a prompt on the screen.

Step 5 You can monitor startup progress using the following methods:

Using browser accessible dashboard:

a) While the VM is being created, monitor the setup process from a browser accessible dashboard.
b) The URL for this Grafana dashboard is in the format http://{VIP}:30602/d/NK1bwVxGk/crosswork-deployment-readiness?orgId=1&refresh=10s&theme=dark. This URL is displayed once the installation completes. This URL is temporary and will be available only for a limited period of approximately 30 minutes.
c) At the end of the deployment, the Grafana dashboard will report a "Ready" status. If the URL is inaccessible, use the SSH console described in this section to monitor the installation process.

Using the console:

a) Check the progress from the console of the VM or by using SSH to the Virtual IP address.
b) In the latter case, log in using the *cw-admin* user name and the password you assigned to that account in the install template.
c) Switch to super user using `sudo su -` command.
d) Run `kubectl get nodes` to see if the nodes are ready. Run `kubectl get pods` to see the list of active running pods.
e) Repeat the `kubectl get pods` command until you see robot-ui in the list of active pods.
f) At this point, you can try to access the Cisco Crosswork Planning UI.

What to do next

In the event of any of these failure scenarios, 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 complete, but the VM is not functional
- Installation is complete, but you are directed to check /var/log/firstBoot.log or /opt/robot/bin/firstBoot.log file.

Diagnostic assessment

This topic explains the diagnostic checks performed during the Cisco Crosswork Planning deployment.

During deployment, the system checks the VM datastore(s) for disk latency and IOPS. If a fetched value is lower than the recommended value for any parameter, the diagnostic assessment reports a failure. You can then choose to either ignore the report and proceed with the installation, accepting the risk of failure, or update your VM resources to meet the required criteria and retry installation.

The outcome of the diagnostic assessment depends on the value set for the **IgnoreDiagnosticsCheckFailure** parameter:

- If set to "false" (default value), the installation will be blocked if the diagnostic check reports an error.
- If set to "true", the diagnostic check result is ignored, and the installation will proceed.

Diagnostic failure scenario

This is a breakdown of the failure scenario for the diagnostic assessment when set to its default value, (**IgnoreDiagnosticsCheckFailure** = **false**).

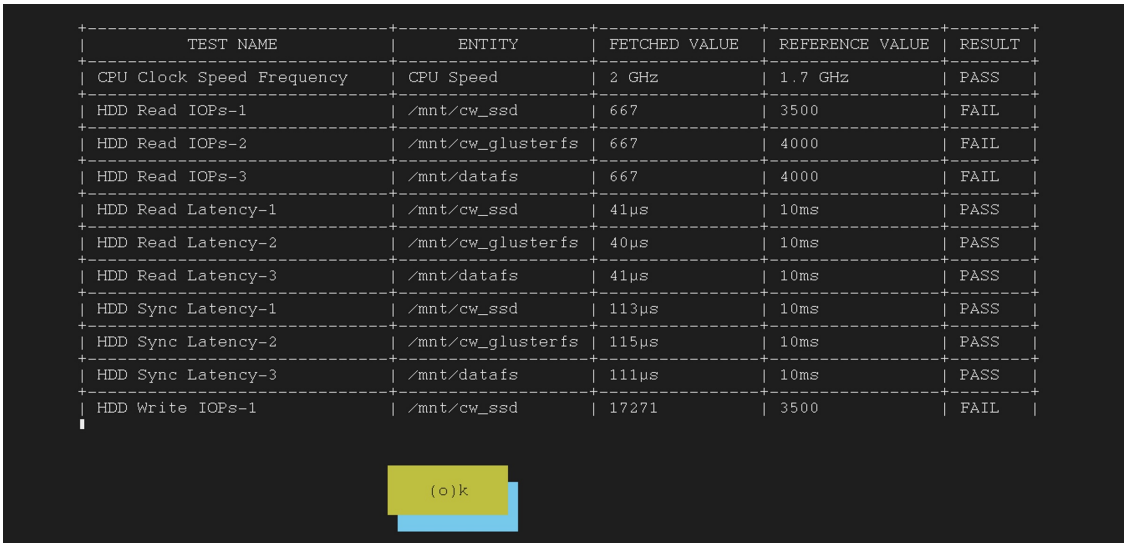
In this scenario, the fetched value is lower than the recommended value (such as IOPS < 4000), resulting in a diagnostic assessment failure.

1. A banner message is displayed to notify you about the failure.

   Figure 4: Sample diagnostic failure report

2. You can use `diagnostics all` and `diagnostics history` commands to view the detailed diagnostic report.

   Figure 5: Diagnostic all output

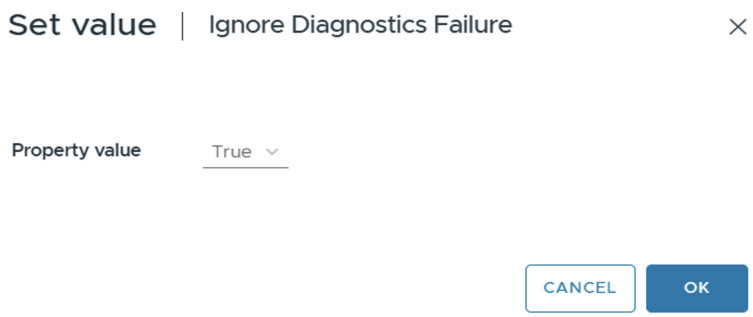


3. To ignore the failure report and proceed with the installation, you must change the value of the **IgnoreDiagnosticsCheckFailure** parameter.
   a. Log in to the vCenter UI.
   b. Power off the VM reporting the failure. Right-click on the VM, and click **Power** > **Power Off**. Click **Yes** in the confirmation pop-up window.
   c. Click on the **Configure** tab and click **vApp Options** in the **Settings** drop-down menu.
   d. Under **Properties**, select the **IgnoreDiagnosticsCheckFailure** parameter and click **Set Value**.

      Figure 6: Select parameter

   e. Set the **Property value** as **True**. Click **OK** to confirm.

      Figure 7: Set value



   f. Power on the VM. Right-click on the VM, and click **Power** > **Power On**. Click **Yes** in the confirmation pop-up window.

4. (Optional) If the diagnostic check reports failures and the installation is blocked, you can also proceed with a full installation using the skip option (**-s**) command in the Docker installer.

   Example:

   ```
   ./cw-installer.sh install -p -m /data/<template file name> -o /data/<.ova file> -y -s
   ```

5. After **IgnoreDiagnosticsCheckFailure** is set to **True**, a banner message appears to inform you that the diagnostic check failure will be skipped.

Figure 8: Skip install check banner message

Important If the parameter value is lower than suboptimal (IOPS < 1000), the installation will fail irrespective of your choice to ignore the diagnostic check.

Diagnostic success scenario

The diagnostic check is successful and the installation will proceed without requiring any user action.

Backend checks

This backend check is used to verify the resource values of the VM:

- Directory IOPS:

```
fio --randrepeat=1  --fdatasync=1 --ioengine=sync --name=test --rw=rw
--filename=<DIR>/mytest --bs=8k --size=600M --runtime=10 --time_based=1
```

Replace `<DIR>` with `/mnt/cw_ssd/`, `/mnt/datafs`, or `/mnt/cw_glusterfs`, as appropriate.

Log in to Cisco Crosswork Planning

This topic describes how to access the UI after installing Cisco Crosswork Planning.

Cisco Crosswork Planning is a browser-based application. For details on supported browser versions, see Supported web browsers, on page 9.

Procedure

Step 1 Open a web browser and enter `https://<Crosswork Management Network Virtual IP (IPv4)>:30603/`.

When you access Cisco Crosswork Planning from your browser for the first time, you may see a warning that the site is untrusted. If this occurs, follow the prompts to add a security exception and download the self-signed certificate from the server. After you do this, the browser accepts the Cisco Crosswork Planning server as a trusted site in all subsequent logins.

Step 2 Log in to Cisco Crosswork Planning.

a) Enter the administrator username **admin** and the default password **admin**.
b) Click **Login**.
c) When prompted to change the administrator's default password, enter the new password in the fields provided and then click **OK**.

Note
Use a strong VM password (a minimum of eight characters, including uppercase and lowercase letters, numbers, and at least one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words.

The **Crosswork Manager** page appears.

Step 3 Click the **Crosswork Health** tab, and click the **Crosswork Platform Infrastructure** tab to view the health status of the microservices running on Cisco Crosswork Planning.

Step 4 (Optional) Change the name assigned to the admin account to something more relevant.

Step 5 In case of manual installation: After logging into the UI, ensure the VM is healthy. Download the inventory sample (.tfvars file) from the Cisco Crosswork Planning UI and update it with information about the VM, along with the data center parameters. Then, import the file back into the Cisco Crosswork Planning UI. For more information, see Import an inventory file, on page 28.

You gain access to Cisco Crosswork Planning and you can begin planning or managing tasks as needed.

What to do next

To log out, in the top-right corner of the main page, click > **Logout**.

Note Logging out does not close the plan file you are working on; the file remains open.

Installation workflow for Cisco Crosswork Planning on KVM

This table summarizes the high-level workflow for installing Cisco Crosswork Planning on KVM manually using CLI. Use the links in the Action column for detailed instructions.

Table 11: Installation workflow

Step	Action
1. Ensure that your KVM host meets all the requirements.	See KVM host bare metal requirements, on page 7.
2. Ensure you have performed the preliminary checks.	See Preliminary checks for KVM installation, on page 42.
3. Set up and validate the KVM environment.	See Set up and validate KVM on RHEL, on page 42.
4. Configure network bridges (for example, Linux bridge or Open vSwitch (OVS) or SRIOV.	See Configure network bridges or SRIOV, on page 43.
5. Install Cisco Crosswork Planning on KVM.	See Install Cisco Crosswork Planning on KVM using CLI, on page 46.

Known limitations

If you use a non-root user ID for deployment on bare metal systems, ensure to add this user ID to the sudoers list (`/etc/sudoers`).

Preliminary checks for KVM installation

This section describes the preliminary checks required for installing Cisco Crosswork Planning on KVM.

- Virtualization: Verify that your system supports virtualization. This is typically enabled in the BIOS.

  You can confirm virtualization support by using these commands:

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

- KVM modules: Confirm that the KVM modules are loaded by running `lsmod | grep kvm`.

Set up and validate KVM on RHEL

This topic describes how to install KVM on RHEL.

Before you begin

Confirm you have administrator (sudo) privileges.

Procedure

Step 1 Refresh repositories and install updates.

```
sudo dnf update -y
```

This command updates all the packages on your system to their latest versions.

Step 2 Reboot the system after all the updates are installed successfully.

```
sudo reboot
```

Step 3 Install the required virtualization tools.

a) Install virt-install and virt-viewer.

```
sudo dnf install virt-install virt-viewer -y
```

virt-install is a command-line tool for creating virtual machines.

virt-viewer is a lightweight UI for interacting with VMs.

b) Install libvirt virtualization daemon, which is necessary for managing 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
```

Step 4 Start and enable the libvirtd virtualization daemon.

a) Start the libvirtd daemon.

```
sudo systemctl start libvirtd
```

b) Enable the libvirtd daemon.

```
sudo systemctl enable libvirtd
```

c) Verify that the daemon is running.

```
sudo systemctl status libvirtd
```

Step 5 Add users to the required groups, such as libvirt and qemu.

In these commands, replace *your_username* with the actual username.

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

Step 6 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
```

Step 7 Check IOMMU and validate the setup. Ensure that all checks show as PASS.

```
virt-host-validate
```

If the IOMMU check is not PASS, then use these commands to enable it.

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

KVM is successfully installed on RHEL and validated.

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 43
- Configure SRIOV, on page 45

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 Cisco Crosswork Planning on KVM using CLI, on page 46).

Install Cisco Crosswork Planning on KVM using CLI

This topic describes how to install Cisco Crosswork Planning on KVM manually using CLI.

Before you begin

- Ensure the KVM host meets all the requirements specified in KVM host bare metal requirements, on page 7.
- Ensure you have performed the preliminary checks specified in Preliminary checks for KVM installation, on page 42.
- Set up your KVM environment. For details, see Set up and validate KVM on RHEL, on page 42.
- Configure the network bridge or SRIOV. For details, see Configure network bridges, on page 43 or Configure SRIOV, on page 45.

Procedure

Step 1 Prepare the configuration ISO file for Cisco Crosswork Planning.

a) Update the `ovf-env.xml` file as needed. For a sample configuration file, see Sample configuration file, on page 47. For installation parameter descriptions, see Installation parameters, on page 14. Note that you cannot change the file name, ovf-env.xml.

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

b) Generate the ISO file.

```
$ mkisofs -R -relaxed-filenames -joliet-long -iso-level 3 -l -o cp1.iso ovf-env.xml
```

Note
In the above command, "cp1" is the host name of the Cisco Crosswork Planning VM.

Step 2 Download the installer bundle (.tar.gz file) from cisco.com and extract it.

```
tar -xvf crosswork-planning-single-node-deployment-7.2.0-45-qcow2.tar.gz
```

This command creates three qcow2 files:

- crosswork-planning-single-node-deployment-7.2.0-45_rootfs.qcow2
- crosswork-planning-single-node-deployment-7.2.0-45_dockerfs.qcow2
- crosswork-planning-single-node-deployment-7.2.0-45_extrafs.qcow2

Step 3 Navigate to your installation directory and create three disks.

```
cd cp1/
qemu-img create -f qcow2 disk3 20G
qemu-img create -f qcow2 disk4 485G
qemu-img create -f qcow2 disk6 15G
```

Step 4 Install Cisco Crosswork Planning using the network bridge or SRIOV.

- For network bridge:

```
virt-install --boot uefi --boot hd,cdrom --connect qemu:///system --virt-type kvm --name cp1
--ram 128000 --vcpus 16 --os-type linux --disk
path=crosswork-planning-single-node-deployment-7.2.0-45_rootfs.qcow2,format=qcow2,bus=scsi --disk
 path=crosswork-planning-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=crosswork-planning-single-node-deployment-7.2.0-45_extrafs.qcow2,format=qcow2,bus=scsi --disk
 path=disk6,format=qcow2,bus=scsi --disk=cp1.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
```

- For SRIOV:

```
virt-install --boot uefi --boot hd,cdrom --connect qemu:///system --virt-type kvm --name cp1
--ram 128000 --vcpus 16 --cpu host-passthrough --disk
path=cw_rootfs.vmdk.qcow2,format=qcow2,bus=scsi --disk
path=cw_dockerfs.vmdk.qcow2,format=qcow2,bus=scsi --disk path=disk3,format=qcow2,bus=scsi --disk
 path=disk4,format=qcow2,bus=scsi --disk path=cw_extrafs.vmdk.qcow2,format=qcow2,bus=scsi --disk
 path=disk6,format=qcow2,bus=scsi --disk=cp1.iso,device=cdrom,bus=scsi --import --network none
--host-device=pci_0000_17_00_0 --host-device=pci_0000_17_00_2 --os-variant ubuntu-lts-latest &
```

Cisco Crosswork Planning is installed on KVM and ready for use.

Sample configuration file

This section provides the sample `ovf-env.xml` file for installing Cisco Crosswork Planning on KVM.

```
<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>
      <Locale>en</Locale>
   </PlatformSection>
    <PropertySection>
```

```
            <Property oe:key="AdminIPv4Address" oe:value="0.0.0.0"/>
            <Property oe:key="AdminIPv4Netmask" oe:value="0.0.0.0"/>
            <Property oe:key="AwsIamRole" oe:value=""/>
            <Property oe:key="CWPassword" oe:value="Cwork123!"/>
            <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="72.163.128.140"/>
            <Property oe:key="DataIPv4Address" oe:value="10.225.120.180"/>
            <Property oe:key="DataIPv4Gateway" oe:value="10.225.120.129"/>
            <Property oe:key="DataIPv4Netmask" oe:value="255.255.255.128"/>
            <Property oe:key="DataPeerIPs" oe:value=""/>
            <Property oe:key="DataVIP" oe:value="10.225.120.179"/>
            <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="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="10.225.120.111"/>
            <Property oe:key="ManagementIPv4Gateway" oe:value="10.225.120.1"/>
            <Property oe:key="ManagementIPv4Netmask" oe:value="255.255.255.128"/>
            <Property oe:key="ManagementVIP" oe:value="10.225.120.56"/>
            <Property oe:key="ManagementVIPName" oe:value=""/>
            <Property oe:key="ManagerPeerIPs" oe:value=""/>
            <Property oe:key="NBIIPv4Address" oe:value="0.0.0.0"/>
            <Property oe:key="NBIIPv4Gateway" oe:value="0.0.0.0"/>
            <Property oe:key="NBIIPv4Netmask" oe:value="0.0.0.0"/>
            <Property oe:key="NBIVIP" oe:value="NBI VIP address"/>
            <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="ThinProvisioned" oe:value="true"/>
            <Property oe:key="UseNonDefaultCalicoBgpPort" oe:value="True"/>
            <Property oe:key="bootOptions.efiSecureBootEnabled" oe:value="False"/>
    </PropertySection>
</Environment>
```

Commands to manage Cisco Crosswork Planning VM on KVM

This section provides the commands to manage the Cisco Crosswork Planning VM on KVM. In these examples, "cp1" is the host name of Cisco Crosswork Planning VM.

- To access the Cisco Crosswork Planning VM console from KVM:

  ```
  [root@KVM-41 cp1]# virsh console cp1
  ```

- To show the current status of Cisco Crosswork Planning in KVM:

```
[root@KVM-41 cp1]# virsh list --all
Id   Name   State
----------------------
2    cp1    running
```

- To shut down the Cisco Crosswork Planning VM:

```
[root@KVM-41 cp1]# virsh shutdown cp1
Domain 'cp1' is being shutdown

[root@KVM-41 cp1]# virsh list --all
Id   Name      State
---------------------------
-    cp1   shut off
```

- To restart the Cisco Crosswork Planning VM:

```
[root@KVM-41 ~]# virsh start cp1
Domain 'cp1' started

[root@KVM-41 cp1]# virsh list --all
Id   Name   State
----------------------
1    cp1    running
```

- To configure the Cisco Crosswork Planning VM to start automatically after a power reset of KVM:

```
[root@KVM-41 ~]# virsh autostart cp1

Domain 'cp1' marked as autostarted
```

Uninstall the Cisco Crosswork Planning VM in a KVM deployment

This topic describes how to uninstall the Cisco Crosswork Planning VM in a KVM deployment.

Procedure

Step 1 Use the **virsh destroy** command to stop the Cisco Crosswork Planning VM forcefully.

Example:

```
[root@KVM-41 cp1]# virsh destroy cp1
Domain 'cp1' destroyed
```

Step 2 Use the **virsh undefine** command to remove the configuration of the Cisco Crosswork Planning VM.

Example:

```
[root@KVM-41 cp1]# virsh undefine --nvram cp1
Domain 'cp1' has been undefined
```

The Cisco Crosswork Planning VM is successfully removed from the KVM deployment.

Installation workflow for deploying SR-PCE (Cisco IOS XRv 9000) on RHEL 8.10 KVM

Cisco Crosswork Planning supports the deployment of SR-PCE running on the Cisco IOS XRv 9000 (XRv9k) platform in RHEL 8.10 KVM environments.

This table provides the necessary steps to launch and manage the XRv9k virtual router on RHEL 8.10 using KVM/QEMU and the libvirt virtualization API.

Table 12: Workflow for deploying SR-PCE (Cisco IOS XRv 9000) on RHEL 8.10 KVM

Step	Action
1. Ensure that the host meets all the prerequisites.	See Prerequisites and setup for Cisco IOS XRv 9000 virtualization, on page 50.
2. Configure network bridges.	See Configure network bridges, on page 51.
3. Prepare the VM storage.	See Prepare VM storage, on page 52.
4. Modify the `virsh` XML template to match your requirements	See Update the VM configuration, on page 52.
5. Deploy the VM and verify the status.	See Deploy and verify the VM, on page 53.
6. Connect to the router console.	See Connect to the router console, on page 53.

Prerequisites and setup for Cisco IOS XRv 9000 virtualization

This topic describes the prerequisites, requirements, and procedures for enabling virtualization and preparing a host machine to deploy SR-PCE running on the Cisco IOS XRv 9000 (XRv9k) platform in RHEL 8.10 KVM environments.

Host machine requirements

Ensure that the host machine meets these requirements:

- Operating System: RHEL 8.10 with virtualization enabled in the BIOS/UEFI.
- Required Packages:
  - qemu-kvm
  - libvirt
  - virt-install
  - virt-manager
  - bridge-utils

Enabling KVM

Verify that the host supports virtualization and that the necessary services are active.

1. Verify CPU virtualization support.

   ```
   egrep -c '(vmx|svm)' /proc/cpuinfo
   ```

2. Check if the KVM modules are loaded.

   ```
   lsmod | grep kvm
   ```

3. Install virtualization packages.

   ```
   sudo dnf install -y qemu-kvm libvirt virt-install virt-manager bridge-utils
   ```

4. Start and enable the libvirt daemon.

   ```
   sudo systemctl enable --now libvirtd
   ```

Required files for deployment

Obtain these files from the Cisco software portal:

- Cisco IOS XRv 9000 ISO Image (for example, `xrv9k-fullk9-x.vrr-25.3.1.iso`): The bootable image required for installation.
- Virsh XML Template: The configuration file used to define the VM properties.

Configure network bridges

You must create network bridges to allow the SR-PCE to communicate with the management network and the IGP topology.

This example creates `intData` for management and `br501` for IGP traffic (using VLAN 501 on interface `ens1f3`).

Procedure

Step 1 Create the VLAN interface.

```
sudo nmcli connection add type vlan con-name ens1f3.501 ifname ens1f3.501 dev ens1f3 id 501 ipv4.method
 disabled ipv6.method ignore
```

Step 2 Create the bridge.

```
sudo nmcli connection add type bridge con-name br501 ifname br501 ipv4.method disabled ipv6.method
ignore
```

Step 3 Add the VLAN interface as a bridge port.

```
sudo nmcli connection add type bridge-slave con-name ens1f3.501-port ifname ens1f3.501 master br501
```

Step 4 Bring the interfaces up.

```
sudo nmcli connection up br501
sudo nmcli connection up ens1f3.501
sudo nmcli connection up ens1f3.501-port
```

Step 5 Verify the bridge mapping.

```
bridge link
ens1f3.501@ens1f3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 master br501 state forwarding priority
 32 cost 2
```

Network bridges for SR-PCE are successfully created, enabling connectivity to both management and IGP networks.

Prepare VM storage

The XRv9k requires a dedicated virtual disk and access to the installation ISO. This topic describes creating a virtual disk, organizing the installation files within the host system's libvirt directory, and setting the appropriate ownership permissions for the Hypervisor to access the files.

Procedure

Step 1 Create the virtual disk.

```
qemu-img create -f qcow2 pcedisk1.qcow2 64G
```

Step 2 Organize files in the libvirt directory.

```
sudo mkdir -p /var/lib/libvirt/images/xrv9k
sudo cp pcedisk1.qcow2 /var/lib/libvirt/images/xrv9k/
sudo cp xrv9k-fullk9-x.vrr-25.3.1.iso /var/lib/libvirt/images/xrv9k/
```

Step 3 Set permissions.

```
sudo chown qemu:qemu /var/lib/libvirt/images/xrv9k/pcedisk1.qcow2
sudo chown qemu:qemu /var/lib/libvirt/images/xrv9k/xrv9k-fullk9-x.vrr-25.3.1.iso
```

Update the VM configuration

Modify the `virsh` XML template to match your environment's file paths and hardware requirements.

Procedure

Step 1 Set the source file path for the HDA disk and the CDROM.

```
<!-- HDA Disk -->
<disk type='file' device='disk'>
  <driver name='qemu' type='qcow2'/>
  <source file='/var/lib/libvirt/images/xrv9k/pcedisk1.qcow2'/>
  <target dev='vda' bus='virtio'/>
</disk>

<!-- CDROM -->
<disk type='file' device='cdrom'>
  <driver name='qemu' type='raw'/>
```

```
  <source file='/var/lib/libvirt/images/xrv9k/xrv9k-fullk9-x.vrr-25.3.1.iso'/>
  <target dev='hdc' bus='ide'/>
</disk>
```

Step 2 Update the `<os>` section to enable UEFI boot.

```
<os>
  <type arch='x86_64' machine='pc'>hvm</type>
  <boot dev='hd'/>
<loader readonly='yes' secure='no' type='pflash'>/usr/share/edk2/ovmf/OVMF_CODE.fd</loader>
  <nvram>/usr/share/edk2/ovmf/OVMF_VARS.fd</nvram>
  <bootmenu enable='yes'/>
</os>
```

Step 3 Map the virtual interfaces to the bridges created in Configure network bridges, on page 51.

Deploy and verify the VM

This topic describes how to deploy the VM using a specified XML configuration file and verify the status of the VM.

Procedure

Step 1 Create the VM.

```
virsh create xrv9k-config.xml
```

Step 2 Verify the status of the VM.

```
virsh list --all
```

Connect to the router console

Once the VM is running, you can access the IOS XR console via telnet.

Procedure

Step 1 Identify the console port by examining the serial section in your XML.

```
<serial type='tcp'>
   <source mode="bind" host="0.0.0.0" service="13914"/>
   <protocol type="telnet"/>
   <target port="0"/>
</serial>
```

Step 2 Wait approximately 10–15 minutes for the router to boot. Then, run this command to connect to the console.

```
telnet localhost 13914
```

Step 3 Configure the initial username, password, and system configurations as prompted.

Installing Cisco Crosswork Planning on Amazon EC2

This process describes how to install Cisco Crosswork Planning on Amazon Elastic Compute Cloud (EC2) using a customized CF template. Amazon EC2 is a web service that provides compute resources in the cloud to host your Cisco Crosswork Planning applications.

Summary

The installation procedure involves deploying this Crosswork resource using the corresponding CF template (YAML file):

- EC2 VM: The main stack (cp-singlenode.yaml) which will deploy the Cisco Crosswork Planning EC2 instance.

Workflow

These are the stages of installing Cisco Crosswork Planning on Amazon EC2.

1. Ensure that your AWS EC2 environment meets all the requirements.

Note Once you have determined the subnet for your Cisco Crosswork Planning node, confirm that there are enough available IP addresses to support the node (and virtual IP addresses) needed.

2. Extract the CF template package. For details, see Extract CF template image, on page 60.
3. Install Cisco Crosswork Planning on Amazon EC2 by customizing the CF template. For a list of important parameters that you must specify in the CF template, see CF template parameters for installing Cisco Crosswork Planning VM, on page 57.
4. Deploy the CF template using the steps in Deploy a CF template, on page 62.
5. Verify that the Cisco Crosswork Planning installation is successful using the steps in Monitor the installation, on page 63.
6. Access the Cisco Crosswork Planning UI. For details, see Access the Cisco Crosswork Planning UI, on page 63.

Result

Cisco Crosswork Planning is successfully installed and accessible on Amazon EC2.

Amazon EC2 settings

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

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

Attention You must review and meet the prerequisites described in this section before installing Cisco Crosswork Planning in the Amazon Web Services (AWS) environment. Most of the requirements discussed in this section are AWS concepts and not imposed exclusively by Cisco Crosswork Planning.

Table 13: AWS prerequisites and settings

Requirement	Description
VPC and Subnets	Virtual Private Cloud (VPC) is created and configured with dedicated subnets for Crosswork interfaces (Management and Data). Direct IP connectivity is required between all subnets.
Endpoints	An endpoint is created in your VPC with these parameters: • **Service name**: EC2 service for the region (availability zone) where you are deploying. • **Private DNS names**: Enabled • **Endpoint type**: Interface • Under **Subnets**, specify the management subnet that you intend to use for the installation. For information on how to configure the endpoints, refer to the AWS documentation.
IAM role	A role is created in Identity and Access Management (IAM) with relevant permission policies. An IAM role is an identity that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust. **Note** • The minimum permissions required for a Crosswork role are ec2:DescribeNetworkInterfaces, ec2:AssignPrivateIpAddresses and ec2:UnassignPrivateIpAddresses. • The trust policy for your role must have the **"Action": "sts:AssumeRole"** condition.
Key pairs	Key pairs (private keys used to log into the VM) are created and configured.
IP addresses	Four IPv4 addresses: One management and one data IP address for the node being deployed, and two additional IP addresses to be used as the management and data Virtual IP (VIP) address (one for the Management network and one for the Data network).
Security group	Create and configure a security group to specify which ports or traffic are allowed.

Requirement	Description
Instance type	The resource profile for your instance deployment. The AWS Instance type should be selected to conform with the VM resource and network requirements listed in Cisco Crosswork Planning resource footprint for AWS EC2, on page 56. • Select **m5.4xlarge** for demos or lab deployments. • Select **m5.8xlarge** or **m6i.8xlarge** for production deployments. • Select **m5.16xlarge** or **m6i.16xlarge** for extra large profiles.
CloudFormation (CF) template	The CF template (.yaml) file for Cisco Crosswork Planning that must be uploaded during installation. For more information, see Extract CF template image, on page 60.
Route53DomainName	Domain name configured for Route53 DNS hosted zone.
User data	The VM-specific parameters script that must be specified during the manual installation procedure.
Hosted Zone ID	Provide the Hosted Zone ID with the domain name (Route53DomainName).

Cisco Crosswork Planning resource footprint for AWS EC2

When deploying in AWS EC2, choose an EC2 instance size that meets or surpasses the resource requirements listed in this table.

Component	vCPU	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data Disks)
Cisco Crosswork Planning node	16	128 GB	10 Gbps	1 TB The VM data store(s) need to have disk access latency < 10 ms and > 5000 IOPS.
Cisco Crosswork Planning node (xLarge profile)	24	256 GB	10 Gbps	1 TB The VM data store(s) need to have disk access latency < 10 ms and > 5000 IOPS.

Component	vCPU	Memory (RAM)	Network Interface Controller (NIC)	Storage (Boot disk + Data Disks)
Cisco SR-PCE **Note** This is the requirement for running a Cisco XRv9K with SR-PCE functionality enabled.	8	24 GB	10 Gbps	120 GB
Basic SCP Server (for storing backups)	-	-	-	At least 25 GB (recommended)

CF template parameters for installing Cisco Crosswork Planning VM

This section describes the parameters that are required for deploying a Cisco Crosswork Planning VM.

Important

- The parameters that are mandatory for creating the template are indicated explicitly. Parameters without this indication are optional and are populated with the default values, which you can alter based on your deployment requirement.
- All IP addresses you enter as parameters should be available.

Table 14: Cisco Crosswork Planning VM deployment parameters

Parameter	Description
VpcId	The Virtual Private Cloud (VPC) ID of your existing VPC. For example, vpc-0f83aac74690101a3.
SecGroup	A pre-created security group that must be applied to the stack. For example, sg-096ff4bc355af16a0. The group must allow ingress access to ports 22, 30160:31560.
CwSSHPassword	The SSH password of the Cisco Crosswork Planning. **Important** We recommend using an external secret store for the password.
SSHKeyName	EC2 key name to use for cw-admin access. This is an optional parameter.
CwAmiId	The Cisco Crosswork Planning AMI ID. This is a mandatory parameter.

Parameter	Description
CwMgmtSubnetId	The management subnet for the Cisco Crosswork Planning VM.
CwMgmtSubnetNetmask	The management subnet netmask in dotted decimal form. For example, 255.255.255.0. This parameter is ignored when deploying in a single interface mode. This is a mandatory parameter.
CwMgmtSubnetGateway	The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed in a single interface mode. This is a mandatory parameter.
InterfaceDeploymentMode	The deployment mode. Options: 1 to deploy the Management interface or 2 to deploy the Management and Data interface.
HostedZoneId	The Hosted Zone ID provided with the domain name (Route53DomainName). The Network Load Balancer (NLB) deployments require a predefined Route53 hosted zone. This is a mandatory parameter.
ManagementVIPName	Cisco Crosswork Planning Management VIP name. For example, dev1-cwmgnt.
DataVIPName	Cisco Crosswork Planning Data VIP name. For example, dev1-cwdata.
Route53DomainName	Domain name used for all Route53 objects. This is a mandatory parameter.
CwDataSubnetId	The data subnet for the Cisco Crosswork Planning VM.
CwDataSubnetNetmask	The data subnet netmask in dotted decimal form. For example, 255.255.255.0. This parameter is ignored when deploying in a single interface mode. This is a mandatory parameter.
CwDataSubnetGateway	The management default gateway on the selected data subnet. Typically, the first address on the subnet. This parameter is ignored when deployed in a single interface mode. This is a mandatory parameter.

Table 15: Optional VM parameters

Parameters	Description
CwMgmtVIP	The current Cisco Crosswork Planning Management VIP address.

Parameters	Description
CwDataVIP	The current Cisco Crosswork Planning Data VIP address. When using an external NLB, you can leave this parameter empty.
Cw1MgmtIP	A free address on the management subnet. If not specified, an address is automatically assigned.
Cw1DataIP	A free address on the data subnet. If not specified, an address is automatically assigned.

Table 16: Cisco Crosswork Planning VM customization parameters

Parameter	Description
InstanceType	The EC2 instance type for the node instances. This is a mandatory parameter.
RunAsSpotInstance	A spot instance. Options are: • `True`: to enable the feature • `False`: to disable the feature Default value is `False`. This is a mandatory parameter.
DataDiskSize	Cisco Crosswork Planning data disk size. The default is 450 GB and should be fine for most deployments. Enter the default unless otherwise directed by Cisco Customer Experience team. This is a mandatory parameter.
K8sServiceNetwork	The network address for the Kubernetes service network. The CIDR range is fixed to '/16'. If not provided, the default will be taken, that is, 10.96.0.0. This is a mandatory parameter.
K8sPodNetwork	The network address for the Kubernetes pod network. The CIDR range is fixed to '/16'." This is a mandatory parameter.
SkipAutoInstall	Configures the Skip Auto Install feature. Options are: • `True`: to enable the feature • `False`: to disable the feature Default value is `False`. This is a mandatory parameter.
EnforcePodReservations	Enforces minimum resource reservations for the pod.

Parameter	Description
IgnoreDiagnosticsCheckFailure	Sets the system response in case of a diagnostic check failure.

Table 17: Optional Cisco Crosswork Planning VM customization parameters

Parameter	Description
CreateEni	Select "True" to deploy ENI.
EniStackName	Specify the Cisco Crosswork Planning StackName where ENI is already created, only if CreateEni is False.

Roles and policy permissions

This section describes the roles and the policy permissions required for deploying the CF template on Amazon. For information on how to create and manage the roles, refer to the Amazon documentation.

Table 18: Amazon EC2 Roles and Actions Assigned to the Roles

Role	Actions
EC2	DescribeInternetGateways, DescribeNetworkInterfaces, DescribeImages, DeleteLaunchTemplate, DescribeSubnets, DescribeAccountAttributes, DescribeSecurityGroups, RunInstances, DescribeVpcs, DescribeInstances, CreateNetworkInterface, CreateTags, DescribeKeyPairs, CreateLaunchTemplate, DeleteNetworkInterface, TerminateInstances
ELB	DescribeLoadBalancers, CreateLoadBalancer, ModifyLoadBalancerAttributes, AddTags, DeleteLoadBalancer
ELB v2	DescribeLoadBalancers, CreateLoadBalancer, AddTags, DeleteLoadBalancer, CreateTargetGroup, CreateListener, DeleteListener, DescribeTargetGroups, ModifyLoadBalancerAttributes, DescribeListeners, RegisterTargets, DeleteTargetGroup, ModifyTargetGroupAttributes, DescribeTargetHealth
IAM	CreateNodegroup, DescribeNodegroup, DeleteNodegroup

Extract CF template image

This topic describes how to extract and validate the Cisco Crosswork Planning CF template image.

Attention The file names mentioned in this topic are sample names and may differ from the actual file names in release version.

Procedure

Step 1 Download the Cisco Crosswork Planning CF template package (crosswork-planning-single-node-cft-7.2.0-18.tar.gz) from cisco.com.

Step 2 Unzip the package.

```
tar -xzvf crosswork-planning-single-node-cft-7.2.0-18.tar.gz
```

The package is unzipped into a new directory. This new directory includes the CF template image and files needed for image validation.

For example:

```
tar -xzvf crosswork-planning-single-node-cft-7.2.0-18.tar.gz

x crosswork-planning-single-node-cft-7.2.0-releasecnc720-18.tar.gz
x crosswork-planning-single-node-cft-7.2.0-releasecnc720-18.tar.gz.signature
x README
x CW-CCO_RELEASE.cer
x cisco_x509_verify_release.py3
x cisco_x509_verify_release.py
```

Step 3 Review the contents of the README file to learn what is included in the package and how the package is validated.

Step 4 Go to the newly created directory and verify the signature of the installer image.

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

```
python cisco_x509_verify_release.py -e <.cer file> -i <.tar.gz file> -s
<.tar.gz.signature file> -v dgst -sha512
```

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

```
python cisco_x509_verify_release.py3 -e <.cer file> -i <.tar.gz file> -s
<.tar.gz.signature file> -v dgst -sha512
```

Note
Use `python --version` to find out the version of Python on your machine.

Example:

```
python cisco_x509_verify_release.py3 -e CW-CCO_RELEASE.cer -i crosswork-planning-single-node-
cft-7.2.0-releasecnc720.tar.gz -s
crosswork-planning-single-node-cft-7.2.0-releasecnc720.tar.gz.signature
-v dgst -sha512

Retrieving CA certificate from http://www.cisco.com/security/pki/certs/crcam2.cer ...
Successfully retrieved and verified crcam2.cer.
Retrieving SubCA certificate from http://www.cisco.com/security/pki/certs/innerspace.cer ...
Successfully retrieved and verified innerspace.cer.
Successfully verified root, subca and end-entity certificate chain.
Successfully fetched a public key from CW-CCO_RELEASE.cer.
Successfully verified the signature of crosswork-planning-single-node-cft-7.2.0-releasecnc720.tar.gz
 using CW-CCO_RELEASE.cer
```

The contents of the package is extracted and validated successfully.

Step 5 Unzip the installer package.

```
tar -xzvf crosswork-planning-single-node-cft-7.2.0-releasecnc720.tar.gz
```

Step 6 In the directory (Cloud), locate the "cp-singlenode.yaml" file. This file is used to install Cisco Crosswork Planning on Amazon EC2.

Step 7 Customize the CF template in the directory to install Cisco Crosswork Planning on Amazon EC2 . For a list of installation parameters, see CF template parameters for installing Cisco Crosswork Planning VM, on page 57.

Deploy a CF template

You can install Cisco Crosswork Planning on Amazon EC2 with custom resources. Depending on the configured parameters, the system installs the required components with their respective capabilities.

Before you begin

- Ensure you have met the Amazon EC2 settings, on page 54 prescribed for installing Cisco Crosswork Planning on Amazon EC2 .
- Ensure you have access to the CloudFormation template that is stored in the S3 bucket or on your local machine. If the template is in Amazon S3, keep the URL of the template file copied.

Procedure

Step 1 Log in to the AWS account and navigate to the S3 bucket. If the CF template (cp-singlenode.yaml) is on your local computer, you can upload the template.

Step 2 In the AWS CloudFormation console, navigate to the **Stacks** page and choose **Create stack** > **With new resources (standard)**.
The Create stack page opens.

Step 3 Enter these details:

a. Under **Prerequisite - Prepare template**, select **Template is ready**.

b. Under **Specify template** > **Template source**, select one of these options:

- If you have the YAML file URL directing to the S3 bucket where the CF template is located, select **Amazon S3 URL**. In the **Amazon S3 URL** field, enter the URL and click **Next**.
- If the CF template is saved on your local computer, select **Upload a template file** and click **Choose File** to select the file you want to upload. After you have selected the template, Amazon uploads the file and displays the S3 URL. Click **Next**.

Note
(Optional) Click **View in Designer** to view a visual representation of the execution flow in your CF template.

Step 4 In the **Specify stack details** page, enter the relevant values for the stack name and parameter values. Click **Next**.

Note
The fields visible in this page are defined by the parameters in the CF template.

Step 5 Review the parameter values that you have configured.

Step 6 Under **Capabilities**, select these check boxes:

- **I acknowledge that AWS CloudFormation might create IAM resources with custom names.**
- **I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND.**

Step 7 Submit the changes.

What to do next

The time taken to create the cluster can vary based on the size of your deployment profile and the performance characteristics of your hardware. See Monitor the installation, on page 63 to know how you can check the status of the installation.

Monitor the installation

This section describes how to verify if the deployment is complete without errors.

Procedure

Step 1 In the CloudFormation console, from the left side **Stacks** pane, select the stack that you have deployed.

Step 2 The stack details are displayed on the right. Click on each tab in this window to view details of the stack. If the stack creation is in progress, the status of the stack in the **Events** tab is CREATE_IN_PROGRESS.

Step 3 After the stack is created:

- The status of the stack changes to CREATE_COMPLETE and the **Logical ID** displays the stack name.
- The **Resources** tab displays the details of all the resources created by the CF template, including the physical IDs.
- The **Outputs** tab has details of the interface IP addresses of the VM.

Access the Cisco Crosswork Planning UI

After the stacks are created, you can check if the node is up and running from the Cisco Crosswork Planning UI.

Before you begin

- Ensure that you have a spare Network Load Balancer (NLB). To access Cisco Crosswork Planning UI, use an external NLB that routes requests to its targets using the protocol DNS and port number that you specify.
- Verify that the Cisco Crosswork Planning pods are in the running state. For information on how to view the status, see Monitor the installation, on page 63 .
- Make sure to keep the IP address of the Management node copied. This IP address is used to access the Cisco Crosswork Planning UI. You can copy the IP address from the **Outputs** tab of the CloudFormation console. For information on accessing the **Outputs** tab, see Monitor the installation, on page 63 .

Procedure

Step 1 Log in to the AWS console and navigate to **Target Groups** to register the targets.

Step 2 Under **Targets**, click **Register targets**. The **Register targets** page opens.

Step 3 In the **IPv4 address**, specify the Management IP address that you copied from the CloudFormation console.

Step 4 Specify the port as 30603. Click **Include as pending below**

Step 5 Click **Register pending targets**.

To deregister the targets that are no longer in use, select the target and click **Deregister**.

Step 6 After the target is in the healthy state, click the load balancer name under **Details**.
The Load balancer page opens.

Step 7 Copy the DNS name from the **DNS name** column.

Step 8 Launch a supported browser and enter `https://<DNS_name>:30603/` in the address bar.

Note
When you access Cisco Crosswork Planning for the first time, some browsers display a warning that the site is untrusted. When this happens, follow the prompts to add a security exception and download the self-signed certificate from Cisco Crosswork server. After you add a security exception, the browser accepts the server as a trusted site in all future login attempts.

Step 9 Log in to Cisco Crosswork Planning.

a. Enter the Cisco Crosswork Planning administrator username **admin** and the default password **admin**.

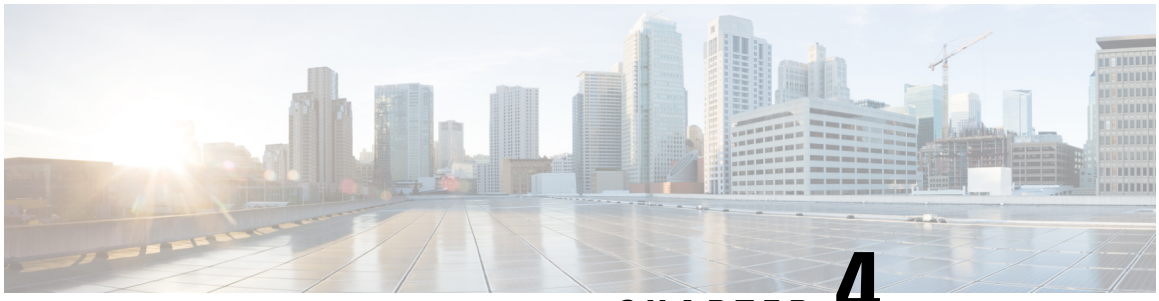
b. Click **Log In**.

c. When prompted to change the administrator's default password, enter the new password in the fields provided, and then click **OK**.

Note
Use a strong VM password (a minimum of eight characters, including uppercase and lowercase letters, numbers, and at least one special character). Avoid using passwords similar to dictionary words (for example, "Pa55w0rd!") or relatable words.

What to do next

Click the **Crosswork Health** tab, and click on the Crosswork Infrastructure tile to view the health status of the microservices running on Cisco Crosswork Planning.



CHAPTER 4

Upgrade Cisco Crosswork Planning

Upgrade methods

Upgrading Cisco Crosswork Planning to the latest version includes upgrading Cisco Crosswork Platform and Cisco Crosswork Planning Applications within a single maintenance window.

Supported upgrade scenarios

The supported upgrade scenario for Cisco Crosswork Planning 7.2 is from Cisco Crosswork Planning 7.1 (IPv4 stack) to Cisco Crosswork Planning 7.2 (IPv4 stack).

Available upgrade methods

You can upgrade Cisco Crosswork Planning using these methods:

- Upgrading using existing hardware, on page 66
- Upgrading using parallel hardware, on page 70

You can also update the Cisco Crosswork Planning applications from the Cisco Crosswork Planning UI in case of minor updates or patch releases. For details, see Upgrade Cisco Crosswork Planning applications (standalone activity), on page 72.

Upgrade limitations and required post-upgrade actions

After upgrading from an earlier version, perform these actions to avoid data loss or system errors:

- Manually register all license tags, as they are not auto-registered as part of the upgrade operation.

- Manually update any custom user roles (Read-Write/Read) created in the earlier version, since these are not migrated.
- Assign new permissions to any user roles with administrative privileges to re-enable their administrative access.
- Always perform a hard refresh or clear your browser cache before proceeding to use the system. Failing to do this step can result in data discrepancies.

Upgrading using existing hardware

Summary

Upgrading to the latest version of Cisco Crosswork Planning using existing hardware is a multi-step process. This process enables you to upgrade Cisco Crosswork Planning on current physical infrastructure without replacing any hardware.

Workflow

These are the stages of upgrading using existing hardware. Execute each stage in sequence to ensure a successful upgrade.

1. Back up your data on the existing hardware. For details, see Create a backup of your system configuration, on page 66.
2. Shut down the system to prepare for upgrade. For details, see Shut down Cisco Crosswork Planning, on page 68.
3. Install the latest version of Cisco Crosswork Planning onto the existing hardware. For details, see Install the latest version of Cisco Crosswork Planning, on page 68.
4. Restore your backed up configuration data to the upgraded system. For details, see Migrate Cisco Crosswork Planning backup, on page 69.

Create a backup of your system configuration

This topic describes how to create a backup of your system configuration, so you can restore it later.

This task is the first stage of the upgrade process. Before upgrading to a new version, you must back up your current system configuration.

Note We recommend that you create a backup only during a scheduled upgrade window. Do not access Cisco Crosswork Planning while the backup operation is running.

Before you begin

- Configure a destination SCP server to store the backup files. This is a one-time activity. Before you begin, have this information ready:
  - The host name or IP address and the port number of a secure SCP server

- A preconfigured path on the SCP server where the backup will be stored
- User credentials with file read and write permissions to the directory
- At least 25 GB of storage on the SCP server

- Ensure that both Cisco Crosswork Planning and the SCP server operate in the same IP environment. For example, if Cisco Crosswork Planning is communicating over IPv4, so must the backup server.

Procedure

Step 1 Log in to the Cisco Crosswork Planning UI.

Step 2 Verify that the Cisco Crosswork Planning VM and applications are healthy.

Step 3 From the main menu, choose **Administration** > **Backup and Restore**.

Step 4 Configure the SCP backup server destination.

a) Click **Destination**.
b) In the Edit Destination dialog box, enter the hostname, port, destination path, and credentials for the SCP server.
c) Click **Save** to confirm the configuration.

Step 5 Create a backup job.

a) Click **Actions** > **Data backup**.
b) In the Data Backup dialog box, provide a relevant name in the **Job Name** field.
c) If the VM or any application is not healthy and you still want to create the backup, check the **Force** check box.

Note
You must use the **Force** option only after consultation with the Cisco Customer Experience team.

d) Complete the remaining fields as needed.

To specify a different remote server upload destination, edit the pre-filled **Host name**, **Port**, **Username**, **Password**, and **Server path/Location** to specify a different destination.

e) (Optional) Click **Verify backup readiness** to verify that Cisco Crosswork Planning has enough free resources to complete the backup.

If the check is successful, Cisco Crosswork Planning displays a warning about the time-consuming nature of the operation. Click **OK** to continue.

If the verification fails, contact the Cisco Customer Experience team for assistance.

f) Click **Start Backup** to start the backup operation.

Cisco Crosswork Planning creates the corresponding backup job set and adds it to the Backup and Restore Job Sets table. The Job Details panel reports the status of each backup step as it is completed.

Note
If you do not see your backup job in the list, refresh the Backup and Restore Job Sets table.

Step 6 Monitor the progress of the backup job.

a) To view the progress of a backup job, enter the job details, such as Status or Job Type, in the search fields in the Backup and Restore Job Sets table. Then, click the job set you want.

The Job Details panel displays information about the selected job set, including job status, job type, and start time. If there is a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

b) If the backup fails during upload to the remote server, under the Status icon, click the **Upload backup** button to retry the upload.

Note
Upload can fail due to connectivity problems with the SCP backup server (for example, incorrect credentials, missing directory or directory permissions, missing path, and so on). This is indicated by failure of the task `uploadBackupToRemote`). If this happens, check the SCP server details, correct any mistakes and try again. Alternatively, you can use the **Destination** button to specify a different SCP server and path before clicking **Upload backup**.

Step 7 Navigate to the destination SCP server directory and confirm that the backup file was created. You will need this backup file during later stages of the upgrade process.

The system configuration backup is created and available on the specified SCP server.

Shut down Cisco Crosswork Planning

After a successful backup, shut down Cisco Crosswork Planning by powering down the VM.

Procedure

Step 1 Log in to the VMware vSphere Web Client.
Step 2 In the **Navigator** pane, right-click the VM that you want to shut down.
Step 3 Choose **Power** > **Power Off**.
Step 4 Wait for the VM status to change to **Off**.

Install the latest version of Cisco Crosswork Planning

After you successfully back up the old version of Cisco Crosswork Planning, install the latest version of Cisco Crosswork Planning.

Procedure

Step 1 Install the latest version of Cisco Crosswork Planning using the instructions in Install Cisco Crosswork Planning using the vCenter vSphere UI.

During installation, a special administrative ID (virtual machine (VM) administrator, with the username "cw-admin" and the default password "cw-admin") is created. The administrative username is reserved and cannot be changed.

The first time you log in using this administrative ID, you are prompted to change the password. Data center administrators use this ID to log in to and troubleshoot the Cisco Crosswork Planning VM. Use this ID to verify that the VM has been properly set up.

Step 2 After the installation is complete, verify that all applications display a **Healthy** status.

a) Log in to the Cisco Crosswork Planning UI.
b) From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork summary**.
c) Ensure all applications display **Healthy**.

Migrate Cisco Crosswork Planning backup

After successfully installing the new version of Cisco Crosswork Planning, proceed to migrate the Cisco Crosswork Planning backup taken earlier.

Before you begin

Ensure that you have

- the host name or IP address and the port number of a secure destination SCP server used in Create a backup of your system configuration, on page 66
- name and path of the backup file created in Create a backup of your system configuration, on page 66, and
- user credentials with file read and write permissions to the directory.

Procedure

Step 1 Verify that the Cisco Crosswork Planning VM is healthy.

Step 2 Configure an SCP backup server.

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the Edit Destination drawer panel.
c) Enter the required information in the provided fields. In **Server path/Location**, provide the location of the backup created in Create a backup of your system configuration, on page 66.
d) Save the details of the backup server.

Step 3 Migrate the old Cisco Crosswork Planning backup.

a) Click **Actions** > **Data migration**.
The Data Migration drawer panel opens with the destination server details prefilled.
b) In **Backup file name**, provide the name of the data migration backup (created in Create a backup of your system configuration, on page 66).
c) To perform the data migration backup despite any Cisco Crosswork Planning application or microservice issues, check the **Force** check box.
d) Click **Start migration** to start the data migration operation.

Cisco Crosswork Planning creates the corresponding data migration job set and adds it to the Backup and Restore Job Sets table. The Job Details panel reports the status of each migration step as it is completed.

Note
If you do not see your job in the list, refresh the Backup and Restore Job Sets table.

Step 4 Monitor the progress of the migration job.

a) To view the progress of a data migration job, enter the job details, such as Status or Job Type, in the search fields in the Backup and Restore Job Sets table. Then, click the job set you want.

The Job Details panel displays information about the selected job set, including job status, job type, and start time. If there is a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note
Cisco Crosswork Planning UI might become temporarily unavailable during the data migration operation. When the Cisco Crosswork Planning UI is down, you can view the job status in the Grafana dashboard. The Grafana link is available as View Data Migration Process Dashboard option on the right side of the Job Details panel.

b) If the data migration fails at any point during the process, restart the procedure.

Step 5 After the data migration is successfully completed, ensure that all applications are healthy.

a) From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork summary**.
b) Ensure that all the applications display **Healthy**.

Upgrading using parallel hardware

Summary

Upgrading to the latest version of Cisco Crosswork Planning using new hardware relies on installing the new Cisco Crosswork Planning on new hardware in parallel while the data from the old Cisco Crosswork Planning is being backed up. This method is faster but requires twice the resources for creating the new VM in parallel.

Workflow

The stages of the parallel upgrade workflow are:

1. Install the latest version of Cisco Crosswork Planning on a new VM. For details, see Deploy Cisco Crosswork Planning on a different VM, on page 70.
2. Back up your data on the existing hardware. For details, see Back up your Cisco Crosswork Planning data, on page 71.
3. Update DNS server and migrate your backed up configuration data. For details, see Update DNS server and migrate backup data, on page 71.
4. Shut down the old Cisco Crosswork Planning VM. For details, see Shut down the old Cisco Crosswork Planning, on page 72.

Deploy Cisco Crosswork Planning on a different VM

This topic describes how to install the latest version of Cisco Crosswork Planning on a new VM in parallel.

Note You must install the new Cisco Crosswork Planning with the same FQDN as the old version of Cisco Crosswork Planning.

Procedure

Step 1 Install the latest of Cisco Crosswork Planning on the new VM using the instructions in Install Cisco Crosswork Planning using the vCenter vSphere UI .

During installation, a special administrative ID (virtual machine (VM) administrator, with the username "cw-admin" and the default password "cw-admin") is created. The administrative username is reserved and cannot be changed.

The first time you log in using this administrative ID, you are prompted to change the password. Data center administrators use this ID to log in to and troubleshoot the Cisco Crosswork Planning VM. Use this ID to verify that the VM has been properly set up.

Step 2 After the installation is complete, verify that all applications display a **Healthy** status.

a) Log in to the Cisco Crosswork Planning UI.
b) From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork summary**.
c) Ensure all applications display **Healthy**.

Back up your Cisco Crosswork Planning data

Log in to the old Cisco Crosswork Planning UI and create a backup. For detailed instructions on creating the backup, see Create a backup of your system configuration, on page 66.

Update DNS server and migrate backup data

This topic describes how to migrate the Cisco Crosswork Planning backup taken earlier.

Before you begin

Ensure that you have

- the host name or IP address and the port number of a secure SCP server
- the name and path of the backup file created in Back up your Cisco Crosswork Planning data, on page 71, and
- user credentials with file read and write permissions to the directory.

Procedure

Step 1 Update the DNS server to point the FQDN of the previous version of Cisco Crosswork Planning to the <VIP> of the new Cisco Crosswork Planning VM.

Step 2 Log in to the upgraded Cisco Crosswork Planning UI using https://<new_VIP>:30603.

Step 3 Configure an SCP backup server.

a) From the main menu, choose **Administration** > **Backup and Restore**.
b) Click **Destination** to display the Edit Destination drawer panel.

c) Enter the required information in the provided fields. In **Server path/Location**, provide the location of the backup created in Create a backup of your system configuration, on page 66.
d) Save the details of the backup server.

Step 4 Migrate the old Cisco Crosswork Planning backup.

a) Click **Actions** > **Data migration**.
The Data Migration drawer panel opens with the destination server details prefilled.
b) In **Backup file name**, provide the name of the data migration backup (created in Create a backup of your system configuration, on page 66).
c) To perform the data migration backup despite any Cisco Crosswork Planning application or microservice issues, check the **Force** check box.
d) Click **Start migration** to start the data migration operation.

Cisco Crosswork Planning creates the corresponding data migration job set and adds it to the Backup and Restore Job Sets table. The Job Details panel reports the status of each migration step as it is completed.

Note
If you do not see your job in the list, refresh the Backup and Restore Job Sets table.

Step 5 Monitor the progress of the migration job.

a) To view the progress of a data migration job, enter the job details, such as Status or Job Type, in the search fields in the Backup and Restore Job Sets table. Then, click the job set you want.

The Job Details panel displays information about the selected job set, including job status, job type, and start time. If there is a failed job, hover the mouse pointer over the icon near the **Status** column to view the error details.

Note
Cisco Crosswork Planning UI might become temporarily unavailable during the data migration operation. When the Cisco Crosswork Planning UI is down, you can view the job status in the Grafana dashboard. The Grafana link is available as View Data Migration Process Dashboard option on the right side of the Job Details panel.

b) If the data migration fails at any point during the process, restart the procedure.

Step 6 After the data migration is successfully completed, ensure that all applications are healthy.

a) From the main menu, choose **Administration** > **Crosswork Manager** > **Crosswork summary**.
b) Ensure that all the applications display **Healthy**.

Shut down the old Cisco Crosswork Planning

After a successful backup, shut down the old Cisco Crosswork Planning. For details on shutdown instructions, see Shut down Cisco Crosswork Planning, on page 68.

Upgrade Cisco Crosswork Planning applications (standalone activity)

This section explains how to upgrade Cisco Crosswork Planning applications independently for minor updates or patch releases. This procedure is not part of the upgrade workflow described in previous sections.

Note Cisco Crosswork Planning does not support the downgrade operation of an application file (CAPP). However, to revert to an older application version, you can uninstall the application and install the older version of the application. We recommend taking a backup of your data before starting the operation.

Before you begin

Ensure that you

- take a backup of your data (using the backup and restore functionality) before any critical upgrade
- download the latest version of the Cisco Crosswork Planning application to your local machine, and
- perform upgrade operations in a maintenance window to minimize disruptions.

Procedure

Step 1 Download and validate the CAPP files.

a) Navigate to cisco.com and locate the CAPP files (.tar.gz) that you require.
b) Hover over the file and copy the MD5 or SHA512 checksum to your clipboard.
c) Download the files to a server that can be reached from the Crosswork server.
d) Run a tool of your choice to calculate the checksum, and compare the checksum value in your downloaded file with the value you copied in the clip board.

For example, on a MAC you can use the **md5** command to calculate the MD5 sum on a file:

```
md5 signed-cw-na-design-patch-7.1.1-7-release-250730.tar.gz

6906c4b4d0e93faedc40b59dd2c14261
```

Verify that the result value matches with the posted value on cisco.com.

Step 2 Log in to Cisco Crosswork Planning UI.

Step 3 From the main menu, choose **Administration** > **Crosswork Manager**, and click the **Application management** tab.

The Crosswork Platform Infrastructure and any applications that are added are displayed here as tiles.

Step 4 Click **Add new file** > **Upload application bundle file (.tar.gz)**. The **Add Application Bundle (.tar.gz)** dialog box is displayed.

Step 5 Select either **URL** or **SCP** as your preferred protocol. Based on your selection, fill in the additional fields with the required information. Click **Add** to proceed.

Step 6 To upgrade, click the Upgrade prompt and the new version of the application is installed. Alternatively, click ••• on the tile, and select the **Upgrade** option from the drop-down list.

Step 7 In the Upgrade screen, select the new version that you want to upgrade to, and click **Upgrade**.

Step 8 (Optional) Click **Job History** to see the progress of the upgrade operation.

Note

During an upgrade, only the changed components are installed, with the new version reusing most resources from the older version to ensure a fast and non-disruptive process. However, the application being updated will be degraded until the upgrade is complete, and users will be notified of the upgrade through an alarm.

The application is upgraded to the selected version.

Collector configuration migration

Collector configuration migration is a process that

- transfers collector configurations from Cisco WAE 7.5.x/7.6.x or between different Cisco Crosswork Planning instances
- preserves existing collector settings, and
- facilitates continued operation on the target platform.

Note When using collectors that have file upload options, ensure to upload the correct files after importing the collector configuration. This is necessary because, after you import the configuration, the server restores only the file name and not the actual file. If you do not use the correct file, the collection will fail.

Migrate collector configurations from Cisco WAE

This section explains how to migrate collector configurations from Cisco WAE 7.5.x/7.6.x to Cisco Crosswork Planning.

Note If using the Layout collector, ensure that the **Template file** field is updated with the correct file after importing the collector configuration. This is necessary because, after importing the configuration, the server restores only the file name and not the actual file. If the field is not updated with the correct file, then the collection fails.

Before you begin

- Download the upgrade script from the Cisco Software Download page.

Procedure

Step 1 If you have not backed up the configuration, use these steps to back up and migrate it to a configuration compatible with Cisco Crosswork Planning:

a) Log in to the machine where Cisco WAE 7.x is installed.
b) Enter this command:

```
# ./wae_upgrade --export --install-dir <WAE_7.x_INSTALL_DIR> --cfg-dir
<dir_to_save_exported_config>
Where:
     --install-dir   indicates the directory where 7.x WAE is installed.
     --cfg-dir       indicates the folder where the backup of 7.x configuration
                     must reside. The migrated configurations are saved as
                     wae_networks.cfg in the provided directory.
```

Step 2 If you already have the backed-up configuration, use these steps to convert the file into a format compatible with Cisco Crosswork Planning:

a) Log in to the machine where the Cisco WAE 7.x configuration is backed up.

b) Enter this command:

```
# ./wae_upgrade --migrate --cfg-dir <dir_containing_7.x_config>

Where:
      --cfg-dir   indicates the folder where the 7.x configuation is backed up.
                  This configuration will be migrated to Cisco Crosswork Planning
                  compatible configuration. The migrated configurations are saved as
                  wae_networks.cfg in the provided directory.
```

Step 3 Import the migrated configurations (**wae_networks.cfg**) to Cisco Crosswork Planning using these steps:

Note
Before migration, ensure that configurations are backed up using the upgrade scripts. Otherwise, the migration will fail.

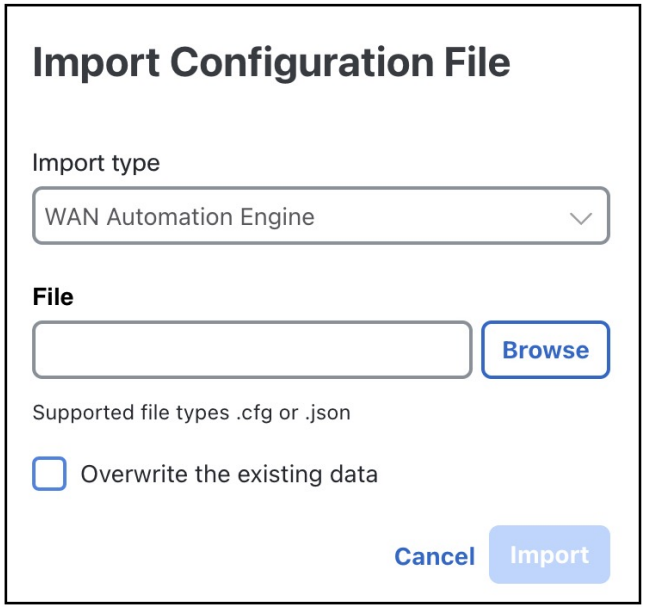
a) Log in to the Cisco Crosswork Planning UI.

b) From the main menu, choose **Collector** > **Migration**.

c) Click **Actions** and select **Configuration migration**.

The Import Configuration File page appears.

Figure 9: Import Configuration File page



d) Select **WAN Automation Engine** from the **Import type** drop-down list.

e) Click **Browse** and select the **wae_networks.cfg** file.
f) (Optional) To overwrite the existing collector configuration, check the **Overwrite the existing data** check box.
g) Click **Import**.

The system proceeds with the import using your configuration. You can monitor the progress on the Migration page (**Collector** > **Migration**). Once the import is successful, the **Import status** column displays **Success**.

What to do next

Note After migrating from Cisco WAE to Cisco Crosswork Planning, the Telnet and SSH settings are not preserved. You need to manually verify and update these settings, if required.

Migrate collector configurations between two instances

This section explains how to migrate collector configurations from one Cisco Crosswork Planning instance (source) to the other (target).

Note
- If using the SR-PCE collector in your configurations, ensure to update the **SR-PCE host** and **Backup SR-PCE host** fields manually after migration. This is necessary because, these fields are not updated while migrating the collector configurations between Cisco Crosswork Planning instances.
- If using the Layout collector, ensure that the **Template file** field is updated with the correct file after importing the collector configuration. This is necessary because, after importing the configuration, the server restores only the file name and not the actual file. If the field is not updated with the correct file, then the collection fails.

Procedure

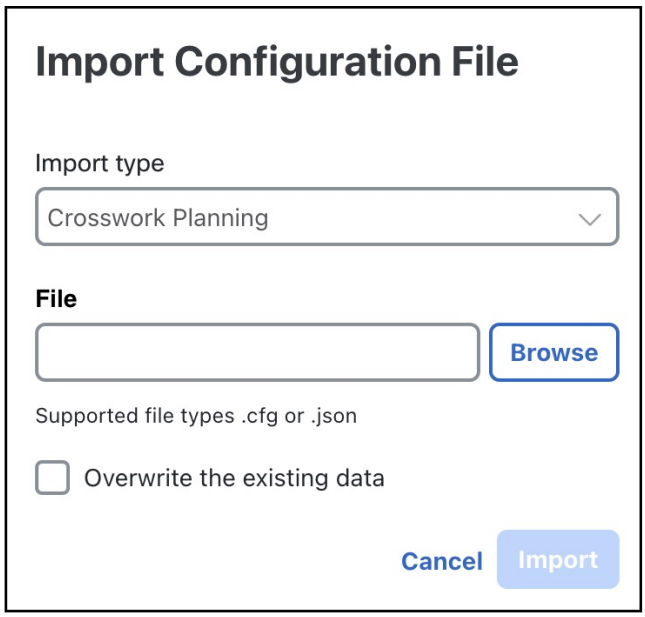
Step 1 Download the collector configuration file from the source machine.
a) Log in to the Cisco Crosswork Planning instance from which you want to migrate the configuration.
b) From the main menu, choose **Collector** > **Migration**.
c) Click **Actions** and select **Configuration backup**.

The collector configuration file is downloaded to your local machine.

Step 2 Import the collector configuration file to the target machine.
a) Log in to the Cisco Crosswork Planning instance to which you want to migrate the configuration.
b) From the main menu, choose **Collector** > **Migration**.
c) Click **Actions** and select **Configuration migration**.

The Import Configuration File page appears.

Figure 10: Import Configuration File page



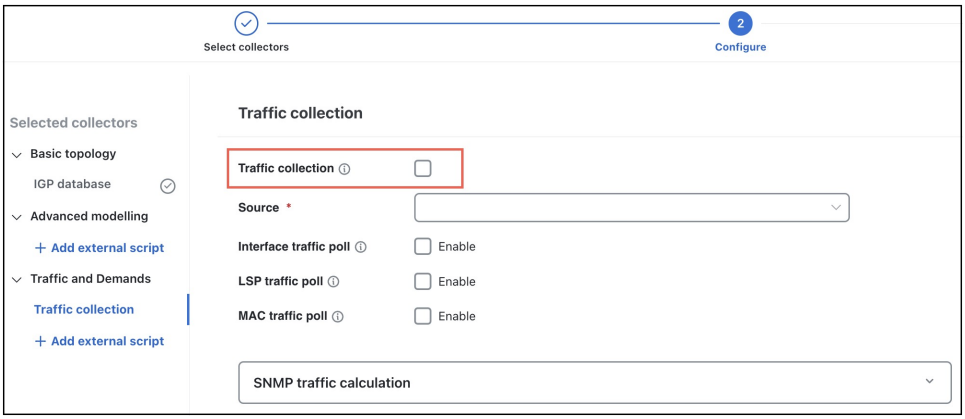
d) Select **Crosswork planning** from the **Import type** drop-down list.
e) Click **Browse** and select the collector configuration file downloaded earlier in the Step 1 (c).
f) (Optional) If you want to overwrite the existing collector configuration, check the **Overwrite the existing data** check box.
g) Click **Import** to import the collector configuration file.

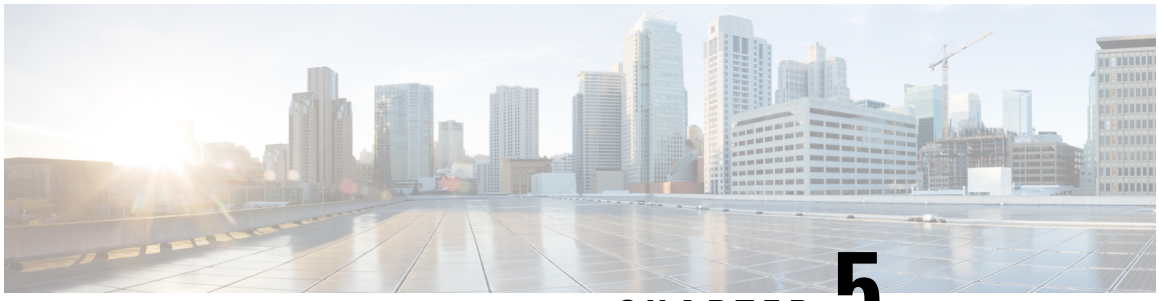
The system proceeds with the import using your configuration. You can monitor the progress on the Migration page (**Collector** > **Migration**). Once the import is successful, the **Import status** column displays **Success**.

What to do next

Note In case of traffic collection, if the traffic poller agent status is displayed as down on the Agent page after migration, even though traffic collection has run successfully, follow these steps:

1. On the Collections page, click **Edit collection** for the collection corresponding to the agent.
2. On the Traffic collection configuration page, uncheck the **Traffic collection** check box and save the configuration.
3. Re-enable the **Traffic collection** check box and save the configuration again.





CHAPTER 5

Next Steps

Cisco Smart Licensing

Cisco Smart Licensing is a flexible licensing model that

- provides an easier, faster, and more consistent way to purchase and manage software across the Cisco portfolio and across your organization
- enables centralized control over license usage and access, and
- is secure allowing you to control what users can access.

Cisco Crosswork Planning supports Smart Licensing, which enables you to monitor the Cisco Crosswork Planning software licenses and endpoint license consumption efficiently. Details of all licenses that you have purchased are maintained in a centralized database called the Cisco Smart Software Manager (CSSM). For more information, refer to the Cisco Smart Licensing Overview on Cisco.com.

A license is required to use all the features in Cisco Crosswork Planning. To install Smart Licensing, follow the steps outlined in the *"Configuring Smart Licensing Configuration" section in the "Manage Licenses" chapter of the Cisco Crosswork Planning 7.2 Collection Setup and Administration guide*.

If you have questions about obtaining a license, contact the Cisco Customer Experience team.

Creating network models

Summary

The Cisco Crosswork Planning UI provides an easy-to-use interface that hides the complexity of creating a model building chain for a network. It combines the configuration of multiple data collectors under one network (collection) and produces a single plan file that contains the consolidated data.

The key components involved in the process are:

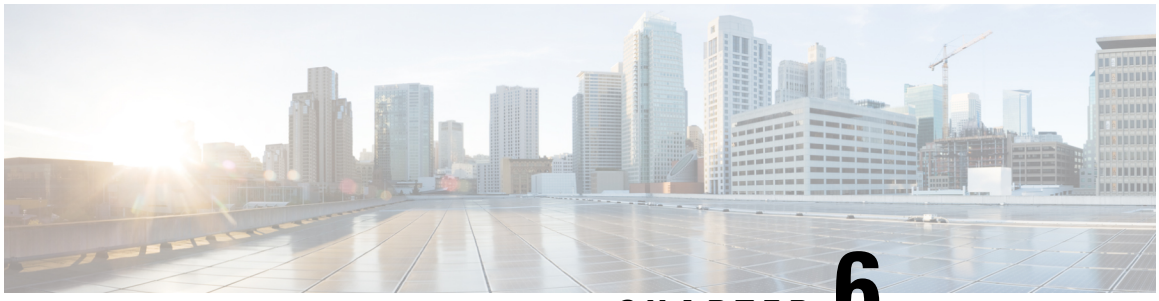
- Cisco Crosswork Planning UI: Provides the interface to configure and manage network modeling activities.
- Data collectors and agents: Gather data from the network as needed.

- Plan files: Contain the consolidated network data for analysis and implementation.

Workflow

These are the stages of creating a network model. For detailed instructions, see the *Cisco Crosswork Planning 7.2 Collection Setup and Administration*.

1. Configure device authentication groups, SNMP groups, and network profile access.
2. (Optional) Configure agents. This step is required only for collecting SR-PCE or NetFlow information.
3. Configure the collections (basic and advanced collections).
4. Schedule when to run collections.
5. (Optional) Manage the aggregation and archiving of network model according to your requirements.
6. View or download the plan files in the Cisco Crosswork Planning Design application.



CHAPTER 6

Uninstall Cisco Crosswork Planning

Uninstallation methods for Cisco Crosswork Planning VM

Cisco Crosswork Planning uninstall procedures are methods to remove the Cisco Crosswork Planning VM and applications from the system.

These methods offer flexible approaches for uninstalling Cisco Crosswork Planning VM depending on your system setup and requirements:

- Uninstall using Docker installer, on page 81: Removes the VM by running the provided Docker uninstallation script. Use this method for Docker-based deployments.
- Uninstall using vSphere, on page 82: Deletes the VM and all associated applications directly from the vSphere interface. Use this method if you manage the VM through VMware vSphere management tools.

Uninstall using Docker installer

This topic describes how to remove a previously created VM after a failed deployment using Docker installer.

This is a critical activity during failed deployments. Any changes made to the VM settings or the data center host requires a cleanup operation before redeployment.

Note The installer cleanup option will delete the VM deployment based on the inventory in `/data` directory.

Procedure

Step 1 Go to the deployment directory. For example, `_cd ~/cw-planning`.

Step 2 Run the container on the host.

```
docker run --rm -it -v `pwd`:/data <cw-installer docker container>
```

Step 3 Edit the copy of the template file (for example, `v4.tfvars`) in a text editor, adding the data center access parameters. Remaining parameters can be provided with dummy values, or entered on the command line during the execution of the operation.

Step 4 Run the `_cw-installer.sh install_` script with the clean directive along with the deployment manifest using the `-m` flag.

Add `-o` option to remove the Cisco Crosswork image template from the data center.

For example:

```
./cw-installer.sh clean -m /data/deployment.tfvars -o
```

Step 5 Enter "yes" when prompted to confirm the operation.

Step 6 (Optional) To clean the VM quickly (without verification), run the installer using this command:

```
docker run --rm -it -v `pwd`:/data <cw installer docker image> -exec
'./cw-installer.sh clean -m /data/deployment.tfvars'
```

The VM and any related files are removed, making the system ready for redeployment.

Uninstall using vSphere

This topic describes how to delete a Cisco Crosswork Planning VM from vCenter using the vSphere web client.

Before you begin

Caution This procedure deletes all of your app data.

Procedure

Step 1 Log into the VMware vSphere web client.

Step 2 In the **Navigator** pane, right-click the app VM that you want to remove.

Step 3 Click **Power** > **Power Off**.

Step 4 Once the VM is powered off, right-click the VM again and select **Delete from Disk**.

The VM and all associated data are permanently deleted from vCenter.

Uninstall Cisco Crosswork Planning applications

This topic describes how to uninstall a Cisco Crosswork Planning application from the UI. The **Uninstall** option removes the application, application-specific menus, and associated data.

Before you begin

Caution Do not uninstall **Crosswork Platform Infrastructure** and **Crosswork Planning Infra**, as this will disrupt the product's functionality. You can only uninstall the Design and Collector applications.

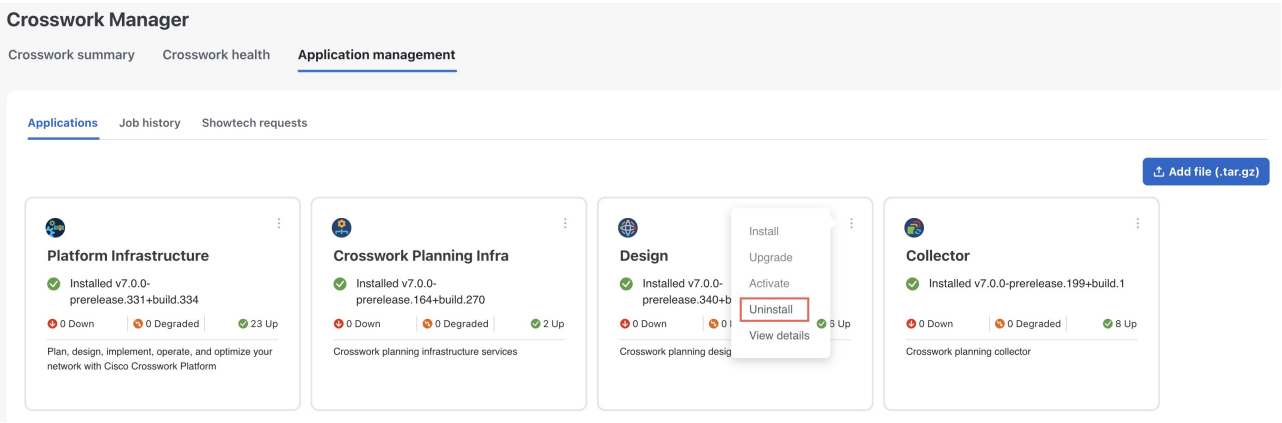
Procedure

Step 1 From the main menu, choose **Administration** > **Crosswork Manager** > **Application Management**.

The Crosswork Platform Infrastructure and any Cisco Crosswork Planning applications that were added during installation are displayed here as tiles.

Step 2 Click ⋮ on the application tile that you want to uninstall, and select the **Uninstall** option.

Figure 11: Application management page



Step 3 Confirm the action when prompted.

The selected application is uninstalled and the application tile is updated to indicate this change.

What to do next

You can also view the progress of uninstallation in the Job History page (**Application Management** > **Job History**). If the uninstall fails, retry using the available options in the Job History page.

Note The uninstall operation does not remove the CAPP file from the repository. The CAPP file will remain visible in the Cisco Crosswork Planning UI, in case you want to install the application in the future.