Overview

This chapter contains the following topics:

About this guide

This guide explains the requirements and processes to install or upgrade Crosswork Network Controller solution.

This document does not cover the installation of integrated components (such as Cisco NSO or Cisco SR-PCE) that may already be installed or can be used independently. For more details about these components, please refer to their respective installation documentation.

Audience

This guide is for experienced network users and operators who want to install Crosswork Network Controller solution in their network. This guide assumes that you are familiar with the following:

- Using a Docker container
- Running scripts in Python
- Deploying an OVA file using VMware vCenter
- Deploying an OVA file using VMware OVF tool
- Amazon Web Services (AWS), Amazon EC2 concepts, and creation of CloudFormation templates

Introduction

Cisco Crosswork Network Controller

Cisco Crosswork Network Controller is a transport SDN controller that empowers customers to simplify and automate intent-based network service provisioning, health monitoring, and optimization in a multi-vendor network environment with a common GUI and API. Crosswork Network Controller simplifies operational workflows by consolidating both the service lifecycle and device management functions in a single integrated solution.

For more information on the Crosswork Network Controller solution components and packages, please refer to the *Crosswork Network Controller 7.0 Release Notes*.

Cisco Crosswork Infrastructure

Cisco Crosswork Infrastructure is a resilient and scalable platform on which all Crosswork components can be deployed. The infrastructure is based on a cluster architecture to ensure extensibility, scalability, and high availability. It supports deployment in VMware and AWS EC2 environments. Cisco Crosswork can be deployed as a cluster with associated VMs (like NSO and WAE) and optionally a second cluster for geo redundancy, or as a single VM with limited device capacity.

A cluster deployment includes three hybrid VMs or nodes, with the option to add more worker nodes based on application needs (see Determine How Many VMs You Need for more information). For optimal node configuration, consulting the Cisco Customer Experience team is recommended.

A single VM deployment operates supported functions on one machine, offering limited redundancy. In this setup, Crosswork Network Controller includes Cisco Crosswork Infrastructure, Embedded Collectors, and the Element Management Functions application integrated together to support the targeted use cases.

For more information on the various deployment options, please refer to Plan Your Deployment.

Note In this guide, Cisco Crosswork Infrastructure will be referred to as "Cisco Crosswork".

Crosswork Data Gateway

Cisco Crosswork integrates with data gateways to collect information from managed devices and forward it to Cisco Crosswork, with optional forwarding to external destinations. The applications analyze this information for various use cases, including topology visualization, service health monitoring, element management, and optimizing network performance. The utilization of forwarded data by third-party applications is beyond the scope of this guide.

Forwarding data to external destinations requires an additional license. For information on licensing requirements, see the *Licensing Requirements for External Collection Jobs* section in *Cisco Crosswork Network Controller 7.0 Administration Guide*. For information on how to enable Crosswork to forward data to an external destinations, see the *Create and Manage External Data Destinations* section in *Cisco Crosswork Network Controller 7.0 Administration Guide*.

The number of data gateways deployed in your network depends on factors such as the number of devices, the volume of data being collected, the overall topology, and your redundancy requirements. Each data gateway is deployed on an individual VM. For guidance on your deployment to best meet your needs, please consult with the Cisco Customer Experience team.

Crosswork Data Gateway is an integral part of the Crosswork solution being deployed, and it does not require a separate license. Therefore, this document explains the data gateway as a foundational component that must be installed in tandem with the Crosswork Infrastructure.

Cisco Integrated Components

Cisco Crosswork Network Service Orchestrator (NSO) functions as the provider for Cisco Crosswork to configure the devices according to their expected functions, including optionally configuring MDT sensor paths for data collection. NSO provides the important functions of device management, configuration and maintenance services.

Cisco Segment Routing Path Computation Element (SR-PCE) is configured to run on either a physical or virtual device that runs IOS-XR. The SR-PCE supports both Segment Routing Traffic Engineering (SR-TE) and Resource Reservation Protocol Traffic Engineering (RSVP-TE). Cisco Crosswork uses the combination of telemetry and data collected from the Cisco SR-PCE to analyze and compute optimal paths for TE tunnels and/or to discover devices in the network.

Components that supports integration with Crosswork Network Controller

- TACACS+, LDAP, and RADIUS servers (see *Set Up User Authentication* in *Cisco Crosswork Network Controller 7.0 Administration Guide* for more information).
- DHCP server (when using Crosswork ZTP).
- External Kafka (for external data collection destinations).
- External gRPC (for external data collection destinations).
- Storage server that supports SCP for storage of backups.

Security

Cisco takes great strides to ensure that all our products conform to the latest industry recommendations. We firmly believe that security is an end-to-end commitment and are here to help secure your entire environment. Please work with your Cisco account team to review the security profile of your network.

For details on how we validate our products, see Cisco Secure Products and Solutions and Cisco Security Advisories.

If you have questions or concerns regarding the security of any Cisco products, please open a case with the Cisco Customer Experience team and include details about the tool being used and any vulnerabilities it reports.