Overview

This document provides a high-level description of the steps that are required to set up and start using Cisco Crosswork Cloud.

About Crosswork Cloud Network Insights

Your network can be a complex and often times unpredictable environment. Routing events that are caused by automated systems, malicious attacks, or simply operational errors can have unforeseen effects on network services. Routing protocol event information can be difficult to comprehend when not organized, analyzed, and displayed logically.

Crosswork Cloud Network Insights is a SaaS application that provides rich analysis, visualization, and alerting on actionable network events. Crosswork Cloud Network Insights operates as a hosted service and helps you assess the routing health of your network. Crosswork Cloud Network Insights provides you with the information you need to determine the stability of your networks and potential risks to your IP routing assets. Crosswork Cloud Network Insights aggregates global and local routing information and identifies the source of anomalies based on a consensus of the routing databases. You can track live and historical activity of your own global BGP and IP information. You can also quickly and easily investigate other entities that might be the cause of issues based on the information provided by the platform

The service provides a secure and low-risk method of collecting route information at a global scale.

Crosswork Cloud Network Insights Tools

In addition to monitoring routing information, Crosswork Cloud Network Insights provides a set of tools to help validate ROA information and graphically visualize AS paths:

- Path Topology—Provides a topology view of all peer, transit, and origin ASN that are advertised in AS paths for a prefix. For more information, see View Prefix Topology.
- Route Origin Validation—Compares ROA information against BGP updates. If the ROA information does not match the data retrieved from a BGP update, it is considered a violation. By default, the tool displays all prefix ROAs in violation (ROA Status filter is set to **Invalid**). For more information, see Validate Route Origin Information.

About Traffic Analysis

Crosswork Cloud Traffic Analysis provides helpful insight about how traffic is affecting your network. By providing traffic statistics on the ASNs, prefixes, and interfaces in your network, Crosswork Cloud Traffic Analysis can give you real-time information on how your devices are performing.

With Crosswork Cloud Traffic Analysis, you can help prevent and address network edge congestion as well as answer the following questions:

- Can we quickly manage congestion at network edge?
- Can we proactively identify network edge congestion? What small changes could help network edge congestion?
- How do IP Routing tables relate to traffic flow in congested devices?
- Who should we peer with and what changes should we make to achieve a Peering Traffic load balance?
- What is the impact of moving traffic between edge devices?

Crosswork Cloud Traffic Analysis aggregates traffic flow data across multiple devices, giving operators a view of the traffic matrix across the whole network. It adds critical context to observed traffic flows based on the existing rich data sets of external routing data from the Crosswork Cloud Network Insights service. This allows operators to gain a deeper understanding of the origins of traffic flows on their networks, as well as the impacts of changes in external routing state and policy. By effectively extracting and managing huge amounts of data, operators can rapidly address and even proactively avoid disrupting events and impending security threats.

Cisco Crosswork Cloud Traffic Analysis also provides actionable recommendations for optimizing traffic at congested network edges. As the number of peering points expand in today's distributed networks, delivering this end-to-end traffic visibility at scale becomes a critical requirement for effective network optimization. This visibility allows network operators to drive manual or automated changes that are clear and easy to implement based on defined policies – throughout the network.

View Traffic Information

- View Device Traffic Details
- View Interface Traffic Details
- View ASN Traffic Details
- View Prefix Traffic Details

Use Crosswork Cloud Traffic Analysis Tools

- Optimize Interface Utilization—Provides a suggested list of prefixes where traffic from overutilized edge interfaces can be diverted to underutilized edge interfaces to normalize overall utilization.
- Visually Compare Traffic—Compares traffic between like objects such as ASNs, prefixes, devices, and interfaces.
- Traffic Drilldown—Allows you to easily view interface capacity and what traffic sources are contributing to it.

- Peer Prospecting—Shows you on which peer ASNs large amounts of traffic are being transmitted and received. It helps you select a current peer and quickly see other peers to which you could move traffic.

About Trust Insights

Crosswork Cloud Trust Insights provides a way to protect and test the integrity of Cisco IOS XR devices on your network. Crosswork Cloud Trust Insights gathers secure measurements and proves that the data was collected at a certain time, which allows you to measure, verify, and audit the integrity of your network. Crosswork Cloud Trust Insights automatically interprets and verifies the integrity of Known-Good-Values (KGVs) measurements from IOS XR routers. This provides a unique visibility into hardware and software integrity and trustworthy status of production routers in your environment.

Crosswork Cloud Trust Insights helps you understand what is true on your network now and what was true in the past. It also helps you answer the following questions:

- How do I know that my router is running the software I want it to be running?
- How can I track what hardware and software has changed?
- How do I know if someone has modified the hardware or software running in my network?
- How can I prove where and when critical security updates were applied and are currently active?
- How can I be sure that the running software was built by Cisco?
- How can I verify what hardware and software was running in a particular date in the past?
- How can I prove that my systems are running compliant hardware and software?

About Cisco Crosswork Data Gateway

Crosswork Data Gateway is designed as an easy to deploy and maintain gateway within customer networks to facilitate secure collection of data from devices, without requiring direct connectivity to external cloud resources. Crosswork Data Gateway is designed for streamlined deployment in common virtualization environments like Vmware ESXi, and once deployed is completely managed by the Crosswork Cloud service. This is designed to minimize the operational and maintenance requirements of deploying and managing Crosswork Cloud applications. Since Crosswork Cloud can manage multiple Cloud Data Gateways, Crosswork Cloud Traffic Analysis and Crosswork Cloud Trust Insights can easily support scalable deployments of peering traffic data and trust evidence collection from large production networks with easy geographical separation of collection, and minimal cost of management.