# Understand Close Loop Automation in Cloud Based Software Defined Network

## Contents

## Introduction

This document describes how close-loop automation works in cloud-based software-defined networks in a 5G deployment scenario.

## Background Information

Cloud is revolutionizing the way technology functions in the traditional world. With the advent of 5G, the paradigm has shifted in the service provider environments. Most of the manual and legacy ways of operating a network are making way for complete automation, that gives a proactive edge to the networks, taking them on a self-healing route. The document provides an SDN-based close loop automation construct that combines different products of the ecosystem of Cisco in order to provide a real-time analysis, visualization, and remediation, all of this with the solutions themselves deployed on the cloud.

5G is not only transforming mobile technology but also creating tremendous opportunities for numerous industries and setting the stage for large-scale disruption.

5G is drastically enhancing day-to-day work and experience with faster speed, greater bandwidth, and ultra-low latency.

Not just the mobile world, 5G extends beyond mobile communication to address all forms of communication services; in fact, it is truly supporting the future of the digital world by enabling all types of services, promoting economic change across all sectors, and utilizing diverse technologies (WIFI, 4G, and radio technologies).

The document does not focus on the deployment phases. The focus is 5G automation and orchestration architecture in terms of functionality and observability end-to-end.

# Necessity of Automation

At this stage, 5G is mostly in the initial stage of testing and deployment but there is a need to understand the associated challenges. The number of network elements needed to run a 5G network in all domains is huge. The deployment of most 5G networks demands automation to ensure cost-effective and efficient implementation with seamless operation of all components involved.

In an automated deployment scenario, most of the heavy pre-planning manual work can be eliminated.

Artificial Intelligence (AI) Systems, based on machine learning (ML), can model how network functions perform under normal and high-load conditions.

Using run-time performance data, the system can ensure automatic deployment of new elements as needed. For ongoing optimization and service assurance, the system can collect and analyze equipment feeds of all types and examine their performance, determining if they match the parameters that Service Providers require and expect.

There are three critical components for successful automation.

1. Visibility – If performance degradation cannot be detected, which impacts service quality without real-time visibility into what is happening in the network every second, then you cannot automate it.
2. Insight - Network analytics and correlation of relevant data generated insights in order to help detect anomalies.
3. Action – This phase takes action to close the loop in order to know that the change made has the right impact.

The fundamental is to have assurance and next is machine learning which can predict what the network is trying to achieve which leads to the foundation of close-loop automation.

# Solution Overview

The proposed solution is a software solution offering industry-leading automation and assurance capabilities which include:

1. Zero Touch Provisioning – Automated new device activation, configuration generation, and network provisioning.
2. CI/CD Workflow – Configuration management, Device Backup, and restore audit history.
3. Real-time visibility – Dashboards and reports of performance statistics and Key Performance Index (KPIs).
4. Fault analysis – Event deduplication, noise reduction, event correlation, fault management, and root cause analysis.
5. Trending and Prediction – AI/ML pattern recognitions, anomaly detection, statistical trending, and forecasting.

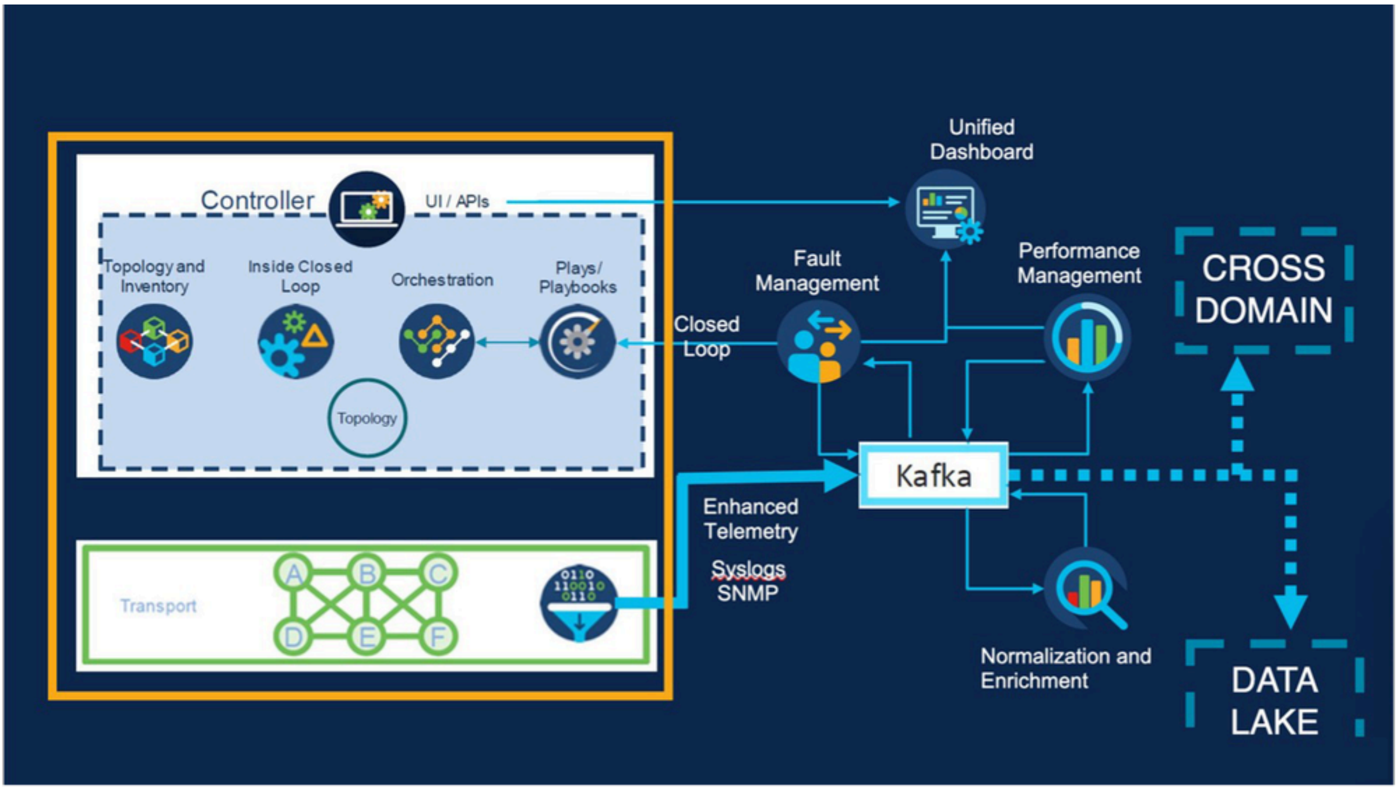
### 1. Solution Capabilities and Benefits

- Zero Touch Provisioning – Enables massive-scale deployment
- Zero Touch Onboarding – Faster time to market
- Automated workflows (CICD) – More control, fewer errors
- Observability (Fault Management, Performance management, Topology) – Effective management and capacity planning
- Event correlation and Noise reduction – Closed loop remediation and self-healing network

## 2. Solution Components

- Matrix (Performance Management)
- Vitria (Fault management and assurance)
- CNC- Crosswork Network Controller (collection, assurance, topology)
- Kafka – Message Bus
- Zero-touch Provisioning (ZTP) Service Assurance Components
- Test Automation Framework (TAF)
- Unified Portal

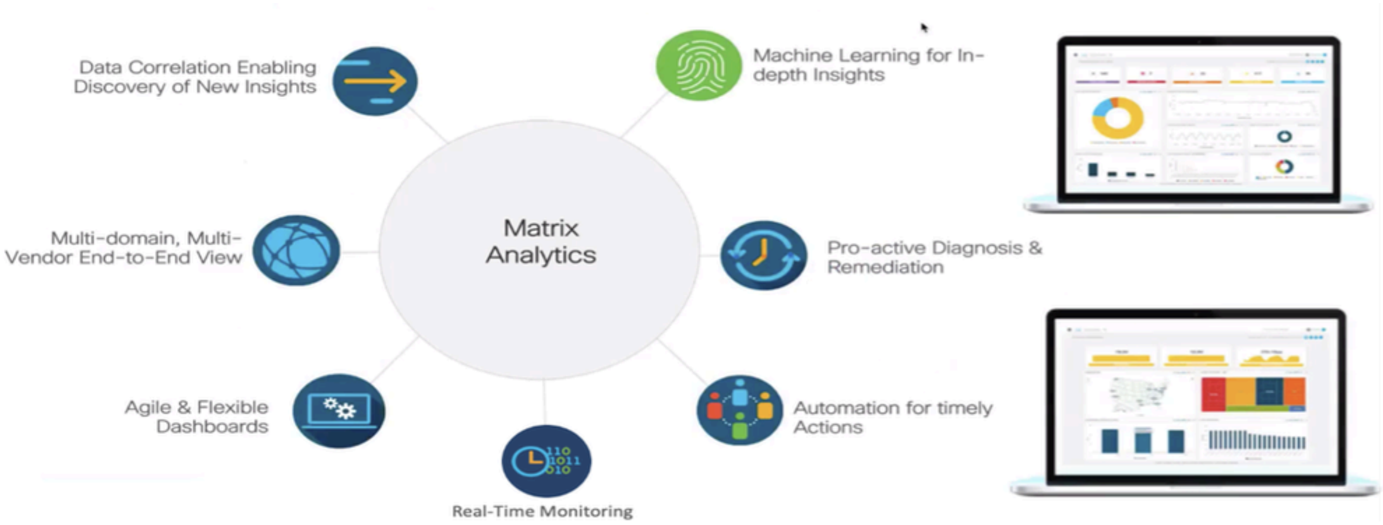
Even though Vitria can do performance management as well for the best solution both Matrix and Vitria are part of the proposed solution where Matrix is best for performance management as a tool and Vitria is best for its fault management capability.



## 3. Solution Components in Detail

### 3.1. Matrix: Performance Management

Matrix is a generic analytics framework developed by Cisco that allows easy adaption to different kinds of data sources and allows application analytics functions built into the solution. Matrix has these key capabilities which allow you to build or customize the use cases as per the requirements.


Data Correlation Enabling Discovery of New Insights
Machine Learning for In-depth Insights
Matrix Analytics
Multi-domain, Multi-Vendor End-to-End View
Pro-active Diagnosis & Remediation
Agile & Flexible Dashboards
Automation for timely Actions
Real-Time Monitoring

### 3.2. Vitria: Fault Management and Assurance

With the complex web of interconnected systems composed of virtual and physical infrastructure, internal and public networks, and interdependent applications, fault management is a constant challenge.

Traditional fault management relies upon siloed monitoring tools that each address a separate layer within the technology stack. Each monitoring system generates volumes of alarms. Service Reliability Engineers (SRE) review the alarms and determine if a ticket must be opened.

Interrelated issues across systems result in multiple tickets being opened and separate teams taking actions that might not address the true root cause, wasting time and resources. When it is finally determined that the seemingly independent issues can be related, a cross-functional team is formed in order to determine the true root cause and engage the appropriate fix-agent or task in order to resolve the issue. While this traditional fault management process plays out, customer frustration climbs. This slow, labor-intensive process is no longer effective. It is excessively time-consuming and costly.

In order to reduce the time to detect issues, accelerate resolution, and reduce cost, signals across the operating environment from the IT elements to the network and the application must be ingested, correlated, and analyzed. Effective fault management requires noise reduction across service layers, automation to reduce the level of human intervention, and integration with existing processes and management systems.

### 3.3. Crosswork Network Controller (CNC): Collection, Assurance, Topology

A new turn in the networking world was the advent of segment routing, which simplified operations by replacing the traditional ways like Multi-Protocol Label Switching (MPLS). Segment routing has reduced the complexity of operations by eliminating a host of protocols and resulted in a significant reduction in overall operational expenses.

The new line of solution of Cisco called the CNC is an SDN controller for segment routing networks. Once a network is SR enabled, the CNC gets into the picture with an array of solutions that help one visualize the network, deploy services, and policies, and a host of other functionalities.

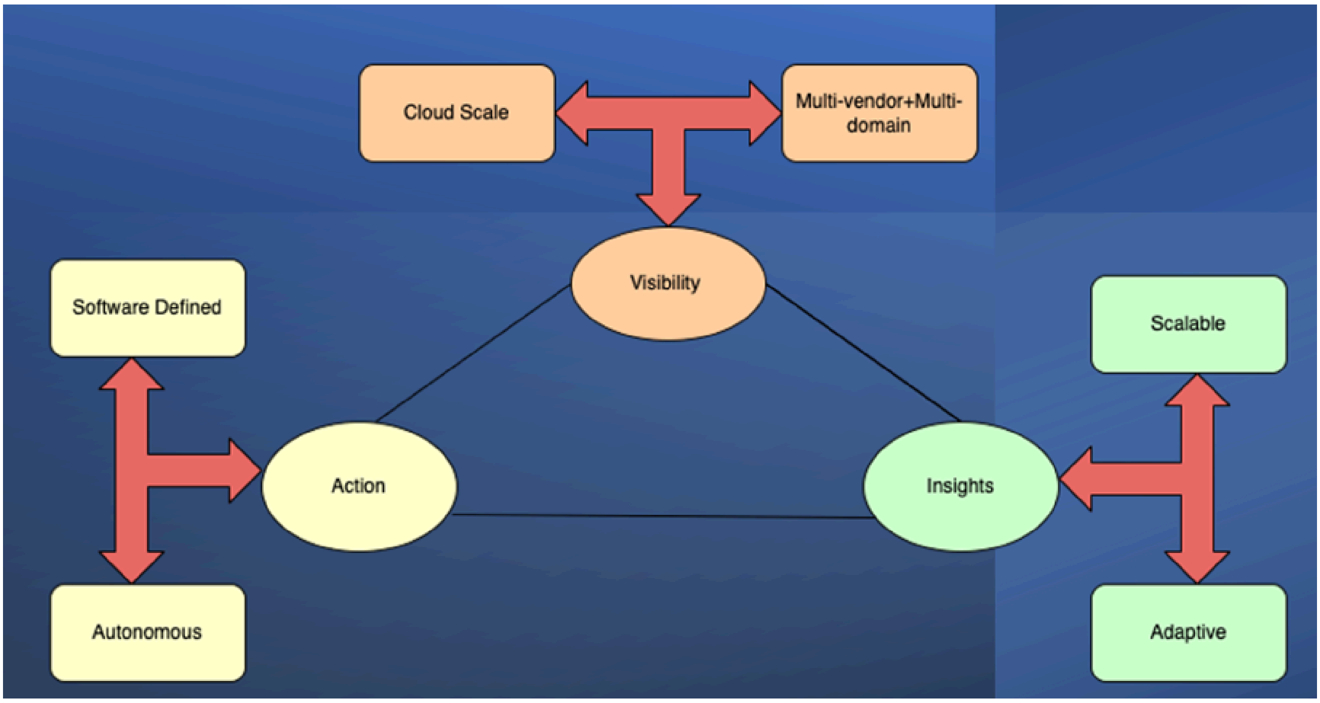
Cisco CNC empowers customers to simplify and automate intent-based network service provisioning, monitoring, and optimization in a multi-vendor network environment with a common GUI and API.

The solution combines intent-based network automation in order to deliver critical capabilities for service orchestration and fulfillment including network optimization, service path computation, device deployment and management, and anomaly detection with automatic remediation.

The fully integrated solution combines core capabilities from multiple innovative, industry-leading products including Cisco Network Services Orchestrator (NSO), Cisco Segment Routing Path Computation Element (SR-PCE), Cisco Crosswork Data Gateway (CDG), and infrastructure of Cisco Crosswork and a suite of applications. Its unified user interface allows real-time visualization of the network topology and services, as well as service and transport provisioning, via a single pane of glass.

The principles of Crosswork can be summarised into three principles of automation:

- Visibility
- Insights
- Action



CNC with its powerful suite of solutions provides a comprehensive mechanism for the overall control of the network. The solutions vary across spectrums and provide wide-ranging capabilities, that satisfy the three principles mentioned earlier.

1. Active Topology

Traditional networking did not have components that provided visualization of the networks once deployed. Operators had to physically log in to the routers to check various things. With the Active Topology of the Crosswork, the operators get a live/real-time visualization of the entire network along with the links, utilization, traffic rates, nodes and links health status, Segment Routing (SR), and RSVP policies status along with path visualization. All that the operator must do now is to log into an intuitive GUI, and have the network at hand.

2. Crosswork Optimisation Engine (COE)

A solution to provide real-time optimization of the network that helps operators to manage the utilization of their network efficiently. The end goal of COE is to enable self-healing networks without much manual intervention.

3. Crosswork Data Gateway (CDG)

Imagine having huge networks with thousands of devices that generate a ton of data. With data being the new oil, the CDG provides a mechanism for collecting all this data from devices that can be leveraged by

Crosswork itself or can even be sent to many other third-party applications for analysis and other transformations. CDG supports data collection through multiple protocols like SNMP, CLI, gRPC Network Management Interface (GNMI), MDT, syslog, and so on.

4. Crosswork Health Insights (HI)

With the network in operation, the traditional mode was to reactively take actions after a particular network event had elapsed. This often comes at a huge cost to the customers. HI enables the automatic performance of live KPI monitoring, generation of alerts, and troubleshooting. The user can define his own logic and HI then raises alerts based on its monitoring. This enables an automated insight into the network health.

5. Crosswork Change Automation

Routinely manual operations like applying configuration changes, installing new versions of software, upgrades, and others can be automated and speeded up with the usage of Change Automation. This makes use of Ansible playbooks that are embedded within, and the configuration changes are then pushed to the devices by leveraging Cisco NSO.

6. Crosswork Zero Touch Provisioning (ZTP)

Customers are always in favor of cutting down the deployment and operations timeline. When you have tens to thousands of new devices that are to be deployed to the network, instead of the usual manual process that could be riddled with mistakes and time-consuming, the Crosswork ZTP boosts the whole process with a completely automated solution for provisioning and to onboard new Cisco IOS® XR devices. The devices can be brought up with a day-0 configuration and then quickly added to the CNC device inventory after which the monitoring, as well as managing of these devices becomes easier.

There are a few other slews of products that work in tandem with the CNC in order to achieve the objectives. Primary among them is the Segment Routing Path Computation Element (SR-PCE) which is a Cisco IOS XR PCE that supports both SR and RSVP. In fact, it is the SR-PCE that facilitates the collection of topologies through the BGP-LS protocol and calculates the path in order to enable the CNC to function as a controller.

The CNC can also interface with the NSO which helps to translate a network intent into configurations specific to a device. The CNC, when used in conjunction with the NSO becomes a force multiplier.

### 3.4. Kafka: Message Bus

The Kafka monitoring is enabled with the help of the Burrow tool. Burrow is a monitoring companion for Apache Kafka that provides consumer lag checking as a service without the need for specifying thresholds.

It monitors committed offsets for all consumers and calculates the status of those consumers on demand. An HTTP endpoint is provided in order to request status on-demand, as well as provide other Kafka cluster information. These APIs are polled by the Performance Monitoring (PM) tool in order to generate consumer lag monitoring and to provide Kafka cluster information.

CPU utilization, storage utilization, and memory utilization of Kafka nodes are also available in Matrix - which sends alarms if thresholds are crossed, or anomalies are detected.

### 3.5. ZTP: Device Activation and Network Provisioning

This is the process of automated new device activation, configuration generation, and network provisioning.

### 3.6.TAF*:* Test Automation Framework

The advanced test automation framework (TAF) provides a way to run test suites parallelly on thousands of devices at the same time, thus eliminating the need for manual validation. A huge deployment of a network can never scale with only manual validation and an automated framework like this helps validate the device configurations and other checks in the most efficient and time-bound manner.

An operator can start hundreds of tests on thousands of devices with just the click of a button. The test suite performs all the configured tests, validates the data, and then shows the entire results with PASS/FAIL criteria in a detailed web-based report. Based on the report, the operator can take further steps in order to alleviate those errors in the devices with the help of other automated solutions.

### 3.7. Unified Portal: Common Dashboard

This is an open UI for all applications which provides the flexibility to add, remove, and modify applications and icons without development.

This provides LDAP authentication support and access to product documentation.

# Orchestrating the Solution

In order to achieve the goals of 5G automation, a cross-domain orchestration is needed to connect the parts between different domains composing the network.

Once the transport devices are configured and up in the network, instead of pursuing the legacy or traditional way of manual management of devices, cross-domain orchestration can be capitalized on to drive with simplicity, agility, and efficiency.

The network active devices can be onboarded to CNC with the specification of the protocols through which the CDG can collect data from the devices. Once the devices get onboarded to CNC, the real-time visualization of the entire L2 and L3 network gets easy. The monitoring of the devices eases up with the display on the GUI related to many facets of the health of the device. The collection of data from the devices starts at predetermined intervals and this data is of rich analytical value. The data is collected through SNMP, SSH, MDT, telemetry, and various other modes as outlined previously.

This data can then be passed on to the other applications within the ecosystem. The CNC makes it possible to send the collected data to the Matrix system through a Kafka bus. The collection is subscribed to a Kafka topic and the CDG keeps distributing the data it collects to this topic, the endpoint of which is to Matrix.

Matrix has several intuitive dashboards from where this data can be visualized, and several analytical operations can also be performed. This data can then be crunched together by the Cisco Vitria AIOps solution for fault monitoring. Whenever any faults or anomalies are detected, the Vitria tool generates alarms proactively so that the requisite remediations can be taken up, thus averting major failures.

Within the crosswork suite, some applications can proactively orchestrate the traffic in a transport network, thus alleviating significant downtimes in peak load times. Feature packs of COE like Local Congestion Mitigation (LCM) and Bandwidth on Demand (BWoD) come to the rescue in such scenarios.

The LCM is a very handy tool in order to mitigate congestion within a network and drive policies that take alternate paths freeing up the overloaded interface. All this happens automatically without a user trying to detect congestion after it has already happened. LCM makes use of a configurable threshold beyond which is considered congested.

Once an interface utilization exceeds this threshold, LCM provides recommendations to ease the congestion on a local interface level. The solution takes care to steer only the requisite amount of traffic that just about takes the congestion under the threshold. The benefit of this is that the entire traffic in the interface is not diverted. The user can analyze the set of recommendations and then choose the one that is best suited. Thus, tactical traffic-engineered policies get kicked off by LCM with the help of the SR-PCE component that helps in the automated clearing of congestion in real-time.

The BWoD solution can work in conjunction with LCM. If there is a high-priority interface carrying voice or video traffic, an operator wants to ensure that the path always has a specified amount of bandwidth available. COE enables a user to create a BWoD policy path, and when the BWoD is also configured with a threshold, the monitoring kicks off every second. As soon as the interface threshold is breached, BWoD jumps in to create new SR policies or reoptimize the existing path that strives to maintain the allotted bandwidth.

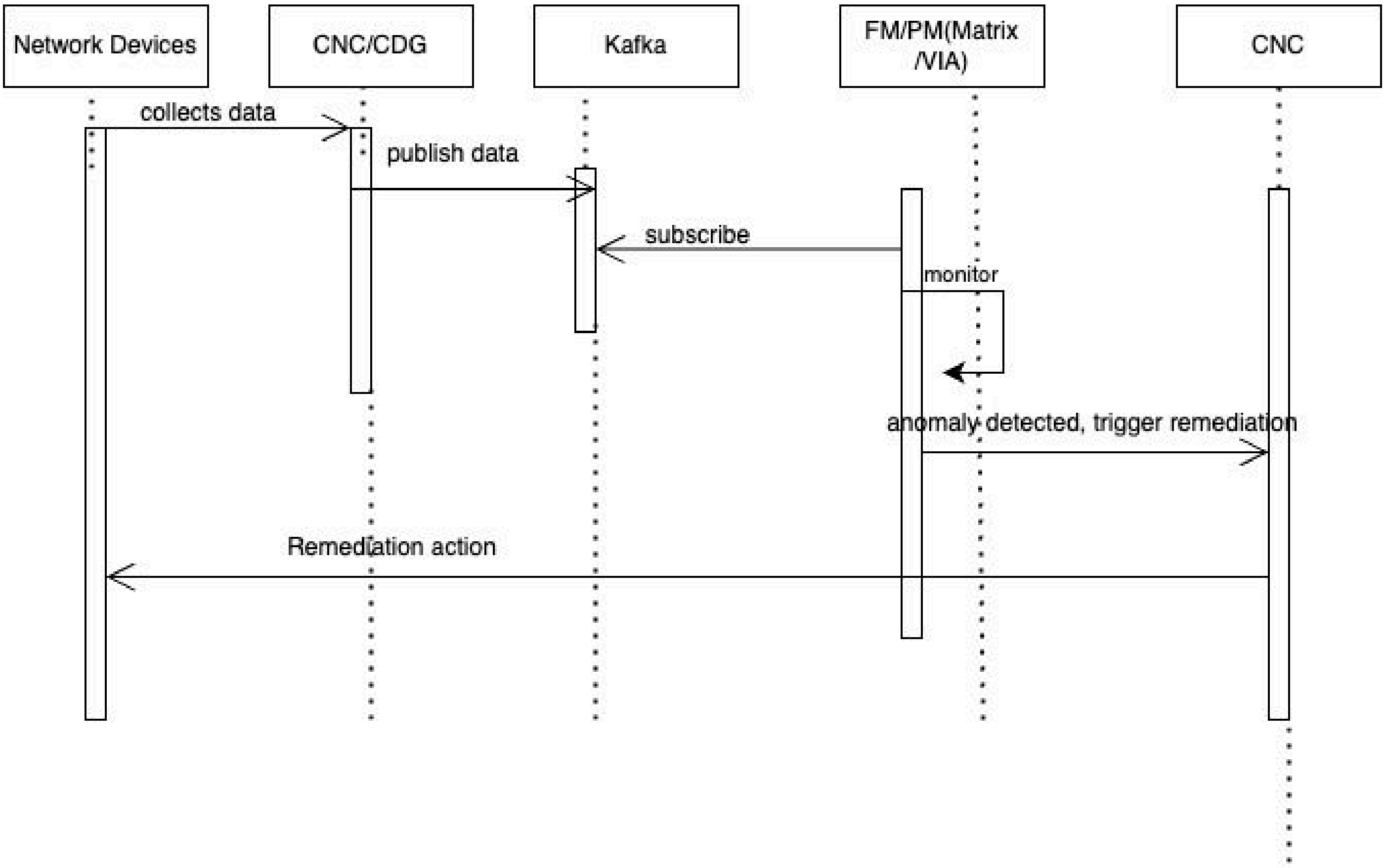
These are a couple of scenarios that optimize the transport path and ease transport automation. While CNC can be used along with other solutions in order to process and analyze the data, the internal components of CNC can also play a big role in the nurturing of the transport network with high-end automation that scales up the availability and reliability of the network.

## Close Loop Automation (CLA) Use Case

In any CLA use case, the basic steps involve:

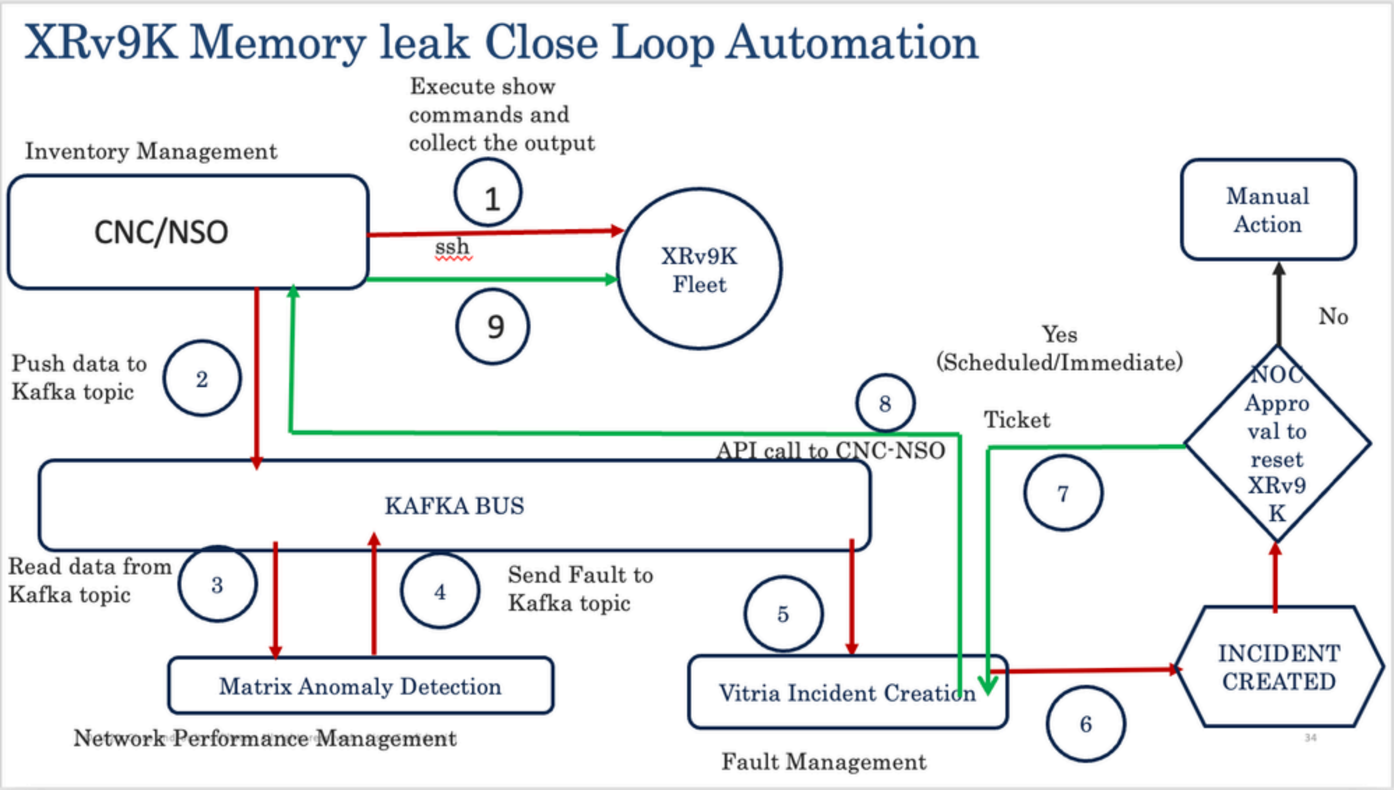
1. Data collection from the device or source and forwarding the same to the Message bus.
2. Performance management system to implement the ingestion logic (parser), enhance the processing pipeline, and define KPI threshold in order to detect anomalies for specific processes.
3. Fault Management Systems to ingest the detected anomalies and wait for any occurrences to invoke API calls to take action.
4. Once the remediation is done, the anomalies of the performance management system detection flow send an anomaly alert with a clear state.
5. Fault management Systems to ingest the alert, clear the anomaly, and close the incident.

Here is a depiction of the flow in this Cisco solution:



A real example of how close loop automation can work leveraging the cross-domain Cisco components is best illustrated in the case of memory leaks of devices. The command show processes memory detail gives the details of the memory consumption of all processes in the router.

A CLI collection job can be created in CNC in order to enable CDG to log into the router at user-specified cadences and run the command show processes memory detail. The CDG gets the output of this command and forwards the data to the Kafka bus. Matrix reads this data from the Kafka bus, and parses and transforms it to display the memory information on its dashboards.


XRv9K Memory leak Close Loop Automation
Execute show commands and collect the output
Inventory Management
CNC/NSO
1
ssh
XRv9K Fleet
9
Manual Action
No
Yes (Scheduled/Immediate)
Push data to Kafka topic
2
8
Ticket
NOC Approval to reset XRv9K
API call to CNC-NSO
7
KAFKA BUS
Read data from Kafka topic
3
4
Send Fault to Kafka topic
5
INCIDENT CREATED
Matrix Anomaly Detection
Vitria Incident Creation
6
Network Performance Management
Fault Management
34

Whenever the memory consumption exceeds a set threshold for the routers, Matrix generates an alarm and forwards the anomaly to the Kafka bus. Vitria AIOps then generates an incident on its dashboard by reading the anomaly from the Kafka bus. This can be visualized in the AIOps dashboard which displays the hostname of the device where the memory utilization has exceeded the safe limits.

From the AIOps GUI, one can take action on this alarm by integrating a Network Service Orchestrator ((NSO) - a configuration management system) device reset API that resets the device.

There is also a cool-down period in Vitria where the incident is still kept open for a duration of time. Within this duration, if there is no reporting of any leak again on the same device by Matrix, then the incident gets closed automatically. If not, the same process of resetting the device is repeated. In the process, there need not be a single manual intervention and the whole remediation is handled by the cross-domain components themselves that act as proof for how the whole loop is automated and solved proactively in the most coherent manner, in real-time.

# Challenges

## 1. Moving to Cloud

Hosting the application in the cloud comes with its challenges:

- New operations management and security solutions are required
- Finding use cases and business models behind the cloud edge
- Clouds must support the required high throughput
- Operations, processes, security, and availability must meet the expectations of SPs and their customers
- Cloud providers offer their solutions in order to ease the design of moving services to the cloud which is sometimes hard to adapt

### 2. Hesitation for Automation

- Not being able to foresee the need for automation
- Complexity of the provider networks

## Summary

Automation and orchestration of a 5G network is a complex task that must be properly planned and implemented from the very beginning of a network design.

The complexity of 5G networks demands automation and orchestration in order to simplify tasks and minimize the probability of error during planning, implementation, and operation.

## Related Information

- https://www.cisco.com/c/dam/m/en_us/customer-experience/collateral/5G-automation-architecture-white-paper.pdf
- https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/crosswork-network-controller/3-0/Solution-Workflow-Guide/CNC-3-0-Solution-workflow-guide.pdf
- Cisco Technical Support & Downloads