

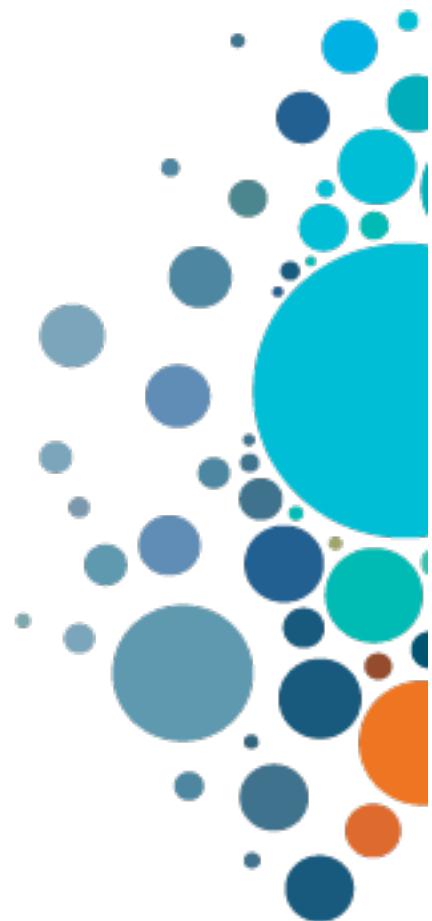


Las Vegas + Digital | June 12-16, 2022

Achieve Closed-loop Automation with IOS-XR Telemetry Monitoring

DEVWKS-2265

Speakers: Shambhu Mishra



Learning Objectives.

In this workshop we are going to focus on two objectives.

1. Introduction of NSO and hands-on with the GUI and CLI.
2. Deploy Close loop automation with Cisco crosswork and NSO.

How to access the lab environment.

We have one dcloud pod lab for each candidate. To access the lab, the system must be connected to dcloud vpn. Below are the necessary credentials for VPN access.

Session Id	Usernames	Password
465900	v945user1	fc0db8
465901	v1023user1	d761c1
465902	v791user1	7c1396
465903	v241user1	17b45c
465904	v1455user1	b786e9
465905	v922user1	cb9894
465906	v288user1	036aa2
465907	v769user1	5fa267
465908	v19user1	3ec235
465909	v842user1	62354d
465910	v49user1	f32d40
465911	v756user1	7a909c

Please check if your laptop is connected to vpn dcloud-sng-anyconnect.cisco.com.

In the following table we have node and application credentials, use them when you need to login to crosswork, nso or routers.

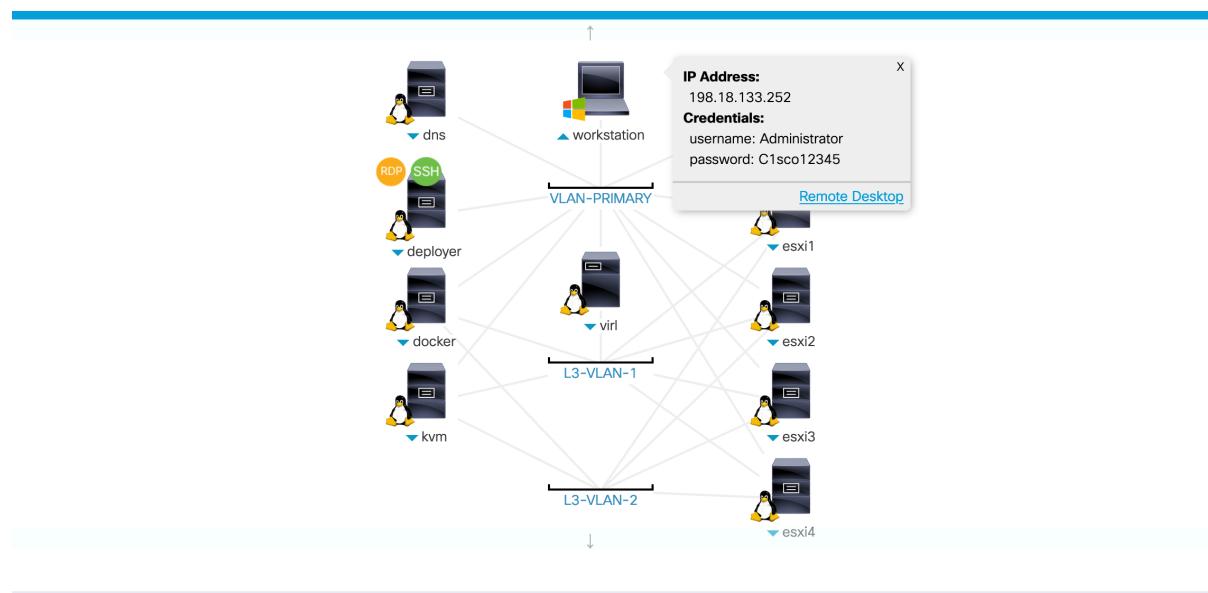
Credentials:

Name	Description	Host Name (FQDN)	IP Address	Username	Password
Node-1 to Node-8	Cisco IOS Xrv	Name.demo.dcloud.cisco.com	198.19.1.1-8	cisco	cisco
Crosswork	Crosswork VM login ssh port 22	Crosswork.demo.dcloud.cisco.com	198.18.134.219	cw-admin	cRo55work!
Crosswork UI	https://198.18.134.219:30603	Crosswork.demo.dcloud.cisco.com	198.18.134.219	admin	C1sco12345
Crosswork DG	Crosswork Data Gateway	cdg2.demo.dcloud.cisco.com	198.18.134.221	dg-admin	cRo55work!
NSO	NSO Host login port 22	Nso.demo.dcloud.cisco.com	198.18.134.28	cisco	C1sco12345
NSO Cli	NSO Cli port 2024	Nso.demo.dcloud.cisco.com	198.18.134.28	admin	admin

Task 1: NSO Hands-on

In this task we are going to make ourselves familiar with the NSO as product and try some hands-on with it. Click the remote desktop link and it will take you to the browser based remote desktop session.

Or use the **remmina remote desktop** to connect to the windows workstation.



Step 1: Login to NSO GUI.

On the remote desktop Firefox tab-3 should have NSO GUI opened. Login to the GUI with username password.

URL: **nso.demo.dcloud.cisco.com**

Credentials: **cisco/C1sco12345**

Click on Device manager and you will see below page. At this page we have all the devices which are connected to NSO. The buttons shown here do the following.

Ping: To check the device reachability.

Connect: Connects NSO with the Routers. Here the ned, credentials etc will be verified. If all the information given is correct the device will connect to the NSO.

Sync-from: Sync the configuration from the router.

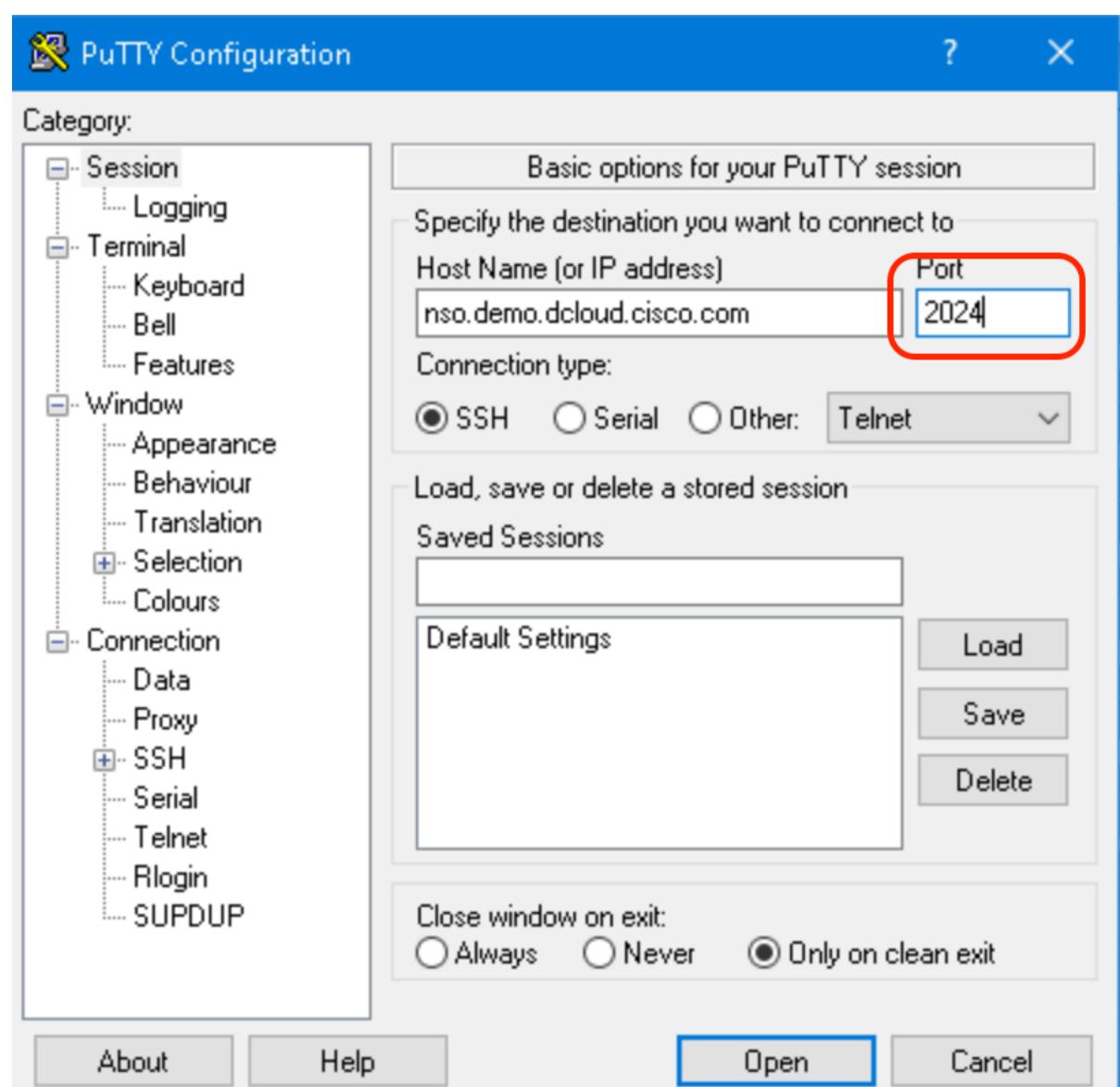
Sync-to: Sync the configuration to the Router.

Compare-config: Compare the configuration on router with the configuration on NSO.

name	address	port	type	services	ping	connect	check-sync	sync-from	sync-to	compare-config	alarm	configuration
Node-1	198.19.1.1		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config		configuration
Node-2	198.19.1.2		cisco-ios-cli-6.74:cisco-ios-cli-6.74	0	ping	connect	check-sync	sync-from	sync-to	compare-config		configuration
Node-3	198.19.1.3		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config		configuration
Node-4	198.19.1.4		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	1 ▾	ping	connect	check-sync	sync-from	sync-to	compare-config		configuration
Node-5	198.19.1.5		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	1 ▾	ping	connect	check-sync	sync-from	sync-to	compare-config		configuration
Node-7	198.19.1.7		cisco-iosr-cli-7.33...cisco-iosr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config		configuration
Node-8	198.19.1.8		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config		configuration

Step 2: Login to NSO CLI.

At this step we will be login to NSO CLI and explore available commands line for NSO.
Credential: **admin/admin**



To change the cli from non-cisco style to cisco style.

```
nso@ncs> switch cli  
nso@ncs#
```

To see the packages installed on NSO.

```
nso@ncs# show packages package package-version  
          PACKAGE  
NAME      VERSION  
-----  
cisco-dc-connector-rfs      1.1.0  
cisco-flat-L3vpn-fp-internal 4.0.0  
cisco-iosxr-cli-7.33        7.33  
cisco-iosxr-cli-7.36        7.36.3  
cisco-sr-te-cfp-internal    4.0.0  
cisco-tsdn-core-fp-common   4.0.0  
core-fp-common               1.26.0  
core-fp-delete-tag-service   1.0.5  
core-fp-plan-notif-generator 1.0.6  
custom-template-utils        2.0.6  
lsa-utils                   1.0.0
```

To know the version of NSO we are running.

```
nso@ncs# show ncs-state version  
ncs-state version 5.5.4.1  
nso@ncs#
```

To know the devices connected to NSO.

```
nso@ncs# show devices list  
NAME  ADDRESS      DESCRIPTION  NED ID      ADMIN STATE  
-----  
NCS1  172.31.187.211 -           cisco-iosxr-cli-7.33  unlocked  
NCS2  172.31.187.212 -           cisco-iosxr-cli-7.33  unlocked
```

How to add a device in NSO

```
nso@ncs# #Show run devices device Node-8.  
!  
devices authgroups group demo  
default-map remote-name admin  
default-map remote-password admin  
default-map remote-secondary-password admin  
!  
devices device Node-8  
address 198.19.1.8  
ssh host-key-verification none  
authgroup demo  
device-type cli ned-id cisco-iosxr-cli-7.33  
device-type cli protocol ssh  
state admin-state unlocked  
config  
!
```

Step 3: Understand configuration management in NSO.

In this example we will try to explore a real time situation and try to mitigate it with the help of NSO. Before we start, we need to sync the configuration from all the devices to NSO. For that, go to NSO device manager and select the device to run sync-from operation.

name	address	port	type	services	ping	connect	check-sync	sync-from	sync-to	compare-config	configuration
Node-1	198.19.1.1		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config	configuration
Node-2	198.19.1.2		cisco-iosr-cl-6.74:cisco-iosr-cl-6.74	0	ping	connect	check-sync	sync-from	sync-to	compare-config	configuration
Node-3	198.19.1.3		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config	configuration
Node-4	198.19.1.4		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	1 ▼	ping	connect	check-sync	sync-from	sync-to	compare-config	configuration
Node-5	198.19.1.5		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	1 ▼	ping	connect	check-sync	sync-from	sync-to	compare-config	configuration
Node-7	198.19.1.7		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config	configuration
Node-8	198.19.1.8		cisco-iosxr-cli-7.33...cisco-iosxr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config	configuration

At this moment the config on router is in sync with the config in NSO.

Now, let's go and make any configuration change on the router.

```
Node-8(config)#hostname Ciscolive
Node-8(config)#commit
```

We see the config instance running on the router and different from the config instance running on NSO. NSO has the previous working version. Suppose that this change has broken the network, and as a network engineer you don't have the idea of **last change** in the network. You can perform following two steps to fix the issue.

- 1- Compare config: This will provide you the differences between the config that we have on router and NSO. Verify the config if that is something you need to push to router to fix the issue.
- 2- Sync-to: Run a sync-to to make the router and nso config same.

Once this is done verify config on router.

TASK-2 Close-Loop Automation

Scenario

In this step we are going to create a problem in the network and remediate with the help of Crosswork predefined playbooks. The whole idea behind this task to understand that a network engineer now has the capabilities to define remediation playbooks prior to the issue occurrence and hence save time to act at the time of the issue to minimize the overall impact time.

In this case we will define a playbook for interface flap. Crosswork will come to know about the flapping interface with the help of Dial-in Telemetry based KPI monitoring. Once Crosswork identifies the issue it will attach the remediation playbook with the event which can be executed easily with few simple changes.

Step 1: Sync all devices with NSO like we did in previous task.

The screenshot shows the Cisco Crosswork Network Automation Device manager interface. The main table lists 8 nodes with their details:

name	address	port	type	services	ping	connect	check-sync	sync-from	sync-to	compare-config
Node-1	198.19.1.1		cisco-iosr-cli-7.33...cisco-iosr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config
Node-2	198.19.1.2		cisco-iosr-cli-6.74:cisco-iosr-cli-6.74	0	ping	connect	check-sync	sync-from	sync-to	compare-config
Node-3	198.19.1.3		cisco-iosr-cli-7.33...cisco-iosr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config
Node-4	198.19.1.4		cisco-iosr-cli-7.33...cisco-iosr-cli-7.33	1 ▾	ping	connect	check-sync	sync-from	sync-to	compare-config
Node-5	198.19.1.5		cisco-iosr-cli-7.33...cisco-iosr-cli-7.33	1 ▾	ping	connect	check-sync	sync-from	sync-to	compare-config
Node-7	198.19.1.7		cisco-iosr-cli-7.33...cisco-iosr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config
Node-8	198.19.1.8		cisco-iosr-cli-7.33...cisco-iosr-cli-7.33	0	ping	connect	check-sync	sync-from	sync-to	compare-config

A context menu is open over the last row (Node-8), showing options: connect, check-sync, sync-from, sync-to, compare-config, and configuration. The 'configuration' option is highlighted.

Step 2: Crosswork Configuration.

Identify the KPI and link it to the action playbook.

The screenshot shows the Crosswork Network Automation interface. On the left, there's a sidebar with icons for Home, Topology, Network Automation, Performance Alerts, and Administration. The main area has a title bar "Performance Alerts / Key Performance Indicators (KPI)". Below it, a table lists "Key Performance Indicators (KPIs)". A red box highlights the "Link Playbook" button in the toolbar above the table. The table has columns for "KPI Name", "Category", and "Description". One row is selected, showing "Interface flap detection" under "Layer2-Interface". The "Category" column also lists "Layer2-Interface".

Search the right playbook with keyword “state” and link the KPI with “Interface state change on XR” playbook.

The screenshot shows the "Link Playbook to KPI" dialog. It has a title "Link Playbook to KPI (Interface flap detection)". On the left, a list of playbooks is shown, with "Interface State change on XR" highlighted by a red box. The main area shows the configuration for linking this KPI. It includes fields for "Playbook Name" (set to "state"), "Interface State change for XE device", and "Interface State change on XR". Below these, a "GigabitEthernet" section is expanded, showing "item 1" with "Id" set to "Playbook". At the bottom right of the dialog, a red box highlights the "Link to KPI" button.

We can see below the KPI is now linked with the playbook.

KPI Name	Category	Description	Linked Playbook
<input checked="" type="checkbox"/> Interface flap detection	Layer2-Interface	Monitors interface flaps and alerts when flap count ...	Interface State change on XR
<input type="checkbox"/> Line state	Layer2-Interface	Monitors interface line states; generates an alert w...	
<input type="checkbox"/> Interface bandwidth monitor	Layer2-Traffic	Monitors bandwidth utilization across all interfaces	
<input type="checkbox"/> Interface packet error counters	Layer2-Traffic	Monitors interface transmit and receive error count...	
<input type="checkbox"/> Interface packet error counters(Openconfig)	Layer2-Traffic	Monitors interface transmit and receive error count...	
<input type="checkbox"/> Interface packet counters	Layer2-Traffic	Monitors interface transmit and receive counters; q...	
<input type="checkbox"/> Interface rate counters	Layer2-Traffic	Monitors interface statistics as rate counters; gener...	
<input type="checkbox"/> Interface rate counters(Openconfig)	Layer2-Traffic	Monitors interface statistics as rate counters; gener...	
<input type="checkbox"/> SNMP interface packet error counters	Layer2-Traffic	Monitors interface transmit and receive error count...	
<input type="checkbox"/> SNMP interface rate counters	Layer2-Traffic	Monitors interface statistics as rate counters; gener...	
<input type="checkbox"/> SNMP traffic blackhole	Layer2-Traffic	Checks the ratio of output data rate to input data ra...	
<input type="checkbox"/> Traffic blackhole	Layer2-Traffic	Checks the ratio of output data rate to input data ra...	
<input type="checkbox"/> IPv6 RIB BGP route count	Layer3-Routing	Monitors IPv6 RIB for route count and memory used...	
<input type="checkbox"/> IPv6 RIB IS-IS route count	Layer3-Routing	Monitors IPv6 RIB for route count and memory used...	

Now we need to create a KPI profile and add the profile to the node for which we need the KPI to be monitored .i.e interface flap monitoring.

Name	Devices Enabled	Description
Alert Dashboard		
Key Performance Indicators (KPI)		
KPI Profiles		
Enable/Disable KPI Profiles		
KPI Job History		

The screenshot shows the 'KPI Profiles' section of the Crosswork Network Automation interface. A single profile named 'i3vpn' is listed. The profile details are as follows:

- Description:** i3vpnProfile
- Destination:** Not Found
- Server Type:** -
- Topic:** -
- #KPIs on Profile:** 12
- Enabled Devices:** 2

The 'KPI On Profile' section contains six KPI definitions:

- CPU threshold:** Alerts ON, Cadence(sec) 60, Alert Frequency 1, Alert Type Two Level...
- CPU utilization:** Alerts ON, Cadence(sec) 60, Alert Frequency 1, Alert Type Statistica...
- Interface QoS (egress):** Alerts ON, Cadence(sec) 60, Alert Frequency 1, Alert Type No Operati...
- IPv6 RIB BGP route count:** Alerts ON, Cadence(sec) 60, Alert Frequency 1, Alert Type Statistica...
- Memory utilization:** Alerts ON, Cadence(sec) 60, Alert Frequency 1, Alert Type Statistica...
- IP SLA UDP jitter monitorin...** (Partial view)

On the right side of the interface, there are summary counts: 12 KPIs on Profile and 2 Enabled Devices.

The screenshot shows the 'Create New Profile' page. The profile name is 'closeloop'. The 'External Destination Details' section includes a 'Server Type' dropdown set to 'Name' and a 'Description' field. The 'Add KPIs to Profile' section shows a table with one row selected:

Category	KPI	Summary
Layer2-Interface	Interface flap detection	Monitors interface flaps and alerts when flap count reaches set threshold

At the bottom of the page are 'Save' and 'Cancel' buttons.

The screenshot shows the 'KPI Profiles' section of the Crosswork Network Automation interface. There are two profiles listed: 'closeloop' (selected) and 'l3vpn'. The 'closeloop' profile has an alert for 'Interface flap detection' with the following settings:

- Alerts: OFF
- Cadence(sec): 300
- Alert Frequency: 1
- Alert Type: Two Level...

Enable the alert and set the cadence to 60 secs.

The screenshot shows the 'KPI Details' dialog for the 'closeloop' profile. In the 'Alert' section, the 'Cadence (sec)' field is set to 300. Other alert parameters shown include 'Alerting Down Sample Rate' (1), 'Alert Threshold' (2.0), and 'Alert Critical Time' (0.0).

Now we need to select the node where we need to enable the KPI. In our case we are going to do this for Node-5.

The screenshot shows the Crosswork Network Automation Device manager interface. The main title bar says "Crosswork Network Automation" and "Device manager". The URL in the address bar is "https://crosswork.demo.dcloud.cisco.com:30603/#/pulse/enable-disable-kpi-profiles". The left sidebar has icons for Home, Topology, Network Automation, Performance Alarms, Device Management, and Administration. Under "Performance Alarms", the "Enable/Disable KPI Profiles" button is highlighted with a red box. The main content area is titled "Performance Alerts / Enable/Disable KPI Profiles". It has tabs for "Select By Device" and "Device Tags". Below is a table with columns: Name, Device Type, Operational State, and Enabled Profiles. The table lists nodes: Node-1 (ROUTER, OK, 0), Node-2 (ROUTER, OK, 0), Node-3 (ROUTER, OK, 0), Node-4 (ROUTER, OK, 0), Node-5 (ROUTER, OK, 1), Node-6 (ROUTER, OK, 1), Node-7 (ROUTER, OK, 0), and Node-8 (ROUTER, OK, 0). A status bar at the bottom right says "Selected 0 / Total 7".

Select the node and click on enable KPI profiles.

This screenshot shows the same interface as the previous one, but with a node selected. In the table, Node-5 is checked under the "Reachable" column. The "Enable KPI Profiles" button in the table header is highlighted with a red box. The rest of the interface is identical to the first screenshot.

The screenshot shows the 'Performance Alerts / Enable/Disable KPI Profiles' page. The navigation bar at the top includes links for Import bookmarks, Crosswork Network C..., Application hub, NSO 5.5 Documentation, NSO REST-API Explorer, and Live Visualization Engine. Below the navigation is a breadcrumb trail: Home > Performance Alerts > Enable/Disable KPI Profiles. The main content area has three tabs: 'Select Devices' (disabled), 'Select KPI Profiles' (selected), and 'Verify Details'. On the left is a sidebar with icons for Home, Topology, Network Automation, Performance Alerts, Device Management, and Administration. The central part shows a table titled 'KPI Profiles' with columns: Name, Devices Enabled, and Description. Two profiles are listed: 'closeloop' (Devices Enabled: 0) and 'iSvpn' (Devices Enabled: 2). The 'closeloop' row is highlighted with a red box. At the bottom are 'Cancel', 'Previous', and 'Next' buttons.

The screenshot shows the 'Performance Alerts / Enable/Disable KPI Profiles' page, specifically the 'Verify Details' step. The navigation bar and sidebar are identical to the previous screen. The main content area shows 'Selected Device(s)' (Node-5) and 'Selected Profile(s)' (closeloop). The 'closeloop' profile details are displayed: Description: -, Destination: -, Server Type: -, Topic: -. Under 'KPI On Profile', there is a section for 'Interface flap detection' with settings: Alerts ON, Cadence(sec) 60, Alert Frequency 1, Alert Type Two Level. There are 'View More Details' and 'Enable' buttons at the bottom. The sidebar on the left remains the same.

Click on enable, this will create and executable job and take almost 30 seconds to finish the job. Click on KPI job history to see the job status.

The screenshot shows the Crosswork Network Automation interface. On the left is a navigation sidebar with icons for Home, Topology, Network Automation, Performance Alerts, Device Management, and Administration. The main content area is titled 'KPI Profiles'. It displays a table with two rows: 'closetloop' (Status: Enabled, Devices Enabled: 1) and 'i3vpn' (Status: Pending, Devices Enabled: 2). To the right of the table is a 'KPI On Profile' section for 'Interface flap detection' with settings like 'Alerts ON', 'Cadence(sec): 60', 'Alert Frequency: 1', and 'Alert Type: Two Level'. A green success message box at the top right says 'The enable KPI profile job 0002 was successfully initiated. Go to KPI Job History...'. This message box is circled with a red border.

This screenshot shows the 'KPI Job History' page. The left sidebar is identical to the previous one. The main area shows 'Job Sets' with two entries: '0002' (Status: Success, Start Time: 09-JUN-2022 01:42:12 PM EDT) and '0001' (Status: Pending, Start Time: 05-JUN-2022 02:03:51 PM EDT). Below this is a 'Jobs (1)' section. A 'Job Details' box is open for job '0002', showing 'Status: Success', '0 Failures', and a timestamp from 'Start Time: 09-JUN-2022 01:42:12 PM EDT' to 'End Time: 09-JUN-2022 01:43:17 PM EDT'. The 'Status' box in the 'Job Details' section is circled with a red border.

At this point if we login to the node-5 it should have a dial-in type telemetry subscription. Which means that the router is listening on a TCP port for dial-in connections from the collector, which in this case is 198.18.1.220.

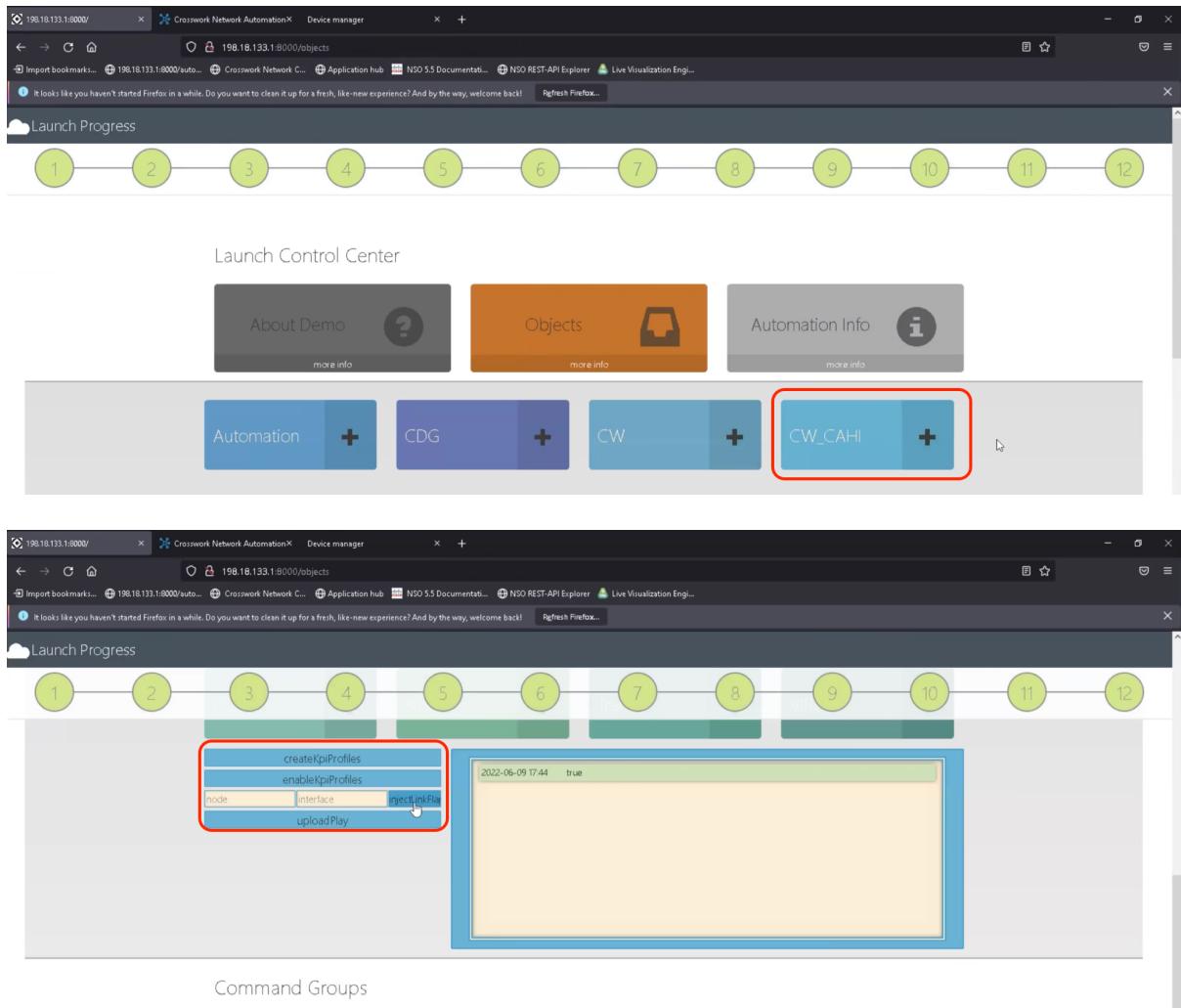
Node-5 : 198.19.1.5
SSH credentials : cisco/cisco

```
RP/0/RP0/CPU0:Node-5#show telemetry model-driven subscription
Sun Jun 12 01:48:47.781 UTC
Subscription: GNMI_5066822812952540038 State: ACTIVE
-----
Sensor groups:
Id          Interval(ms)      State
GNMI_5066822812952540038_0    60000      Resolved

Destination Groups:
Id          Encoding      Transport      State      Port      Vrf
GNMI_1001      gnmi-proto  dialin      Active     55664      IP
TLS :           False        198.18.1.220
```

Step 3: Inject Link Flap and verify.

This is the demo management tool which is going to help us perform the interface flap on the router node-5.



Once you click on injectflap you can go to crosswork alert dashboard to see the flap related logs for interface 0/0/0/2.

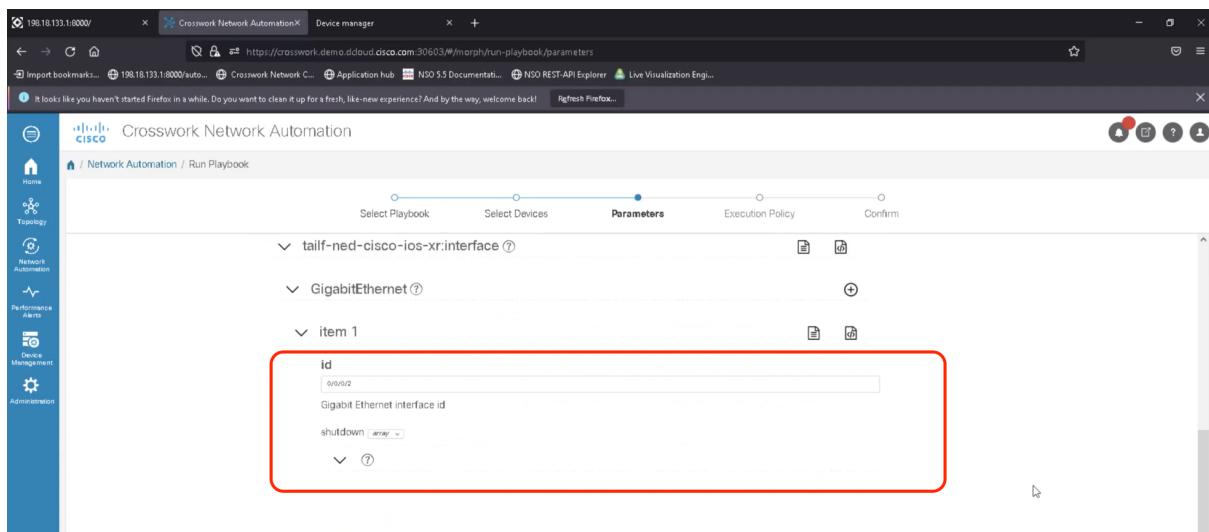
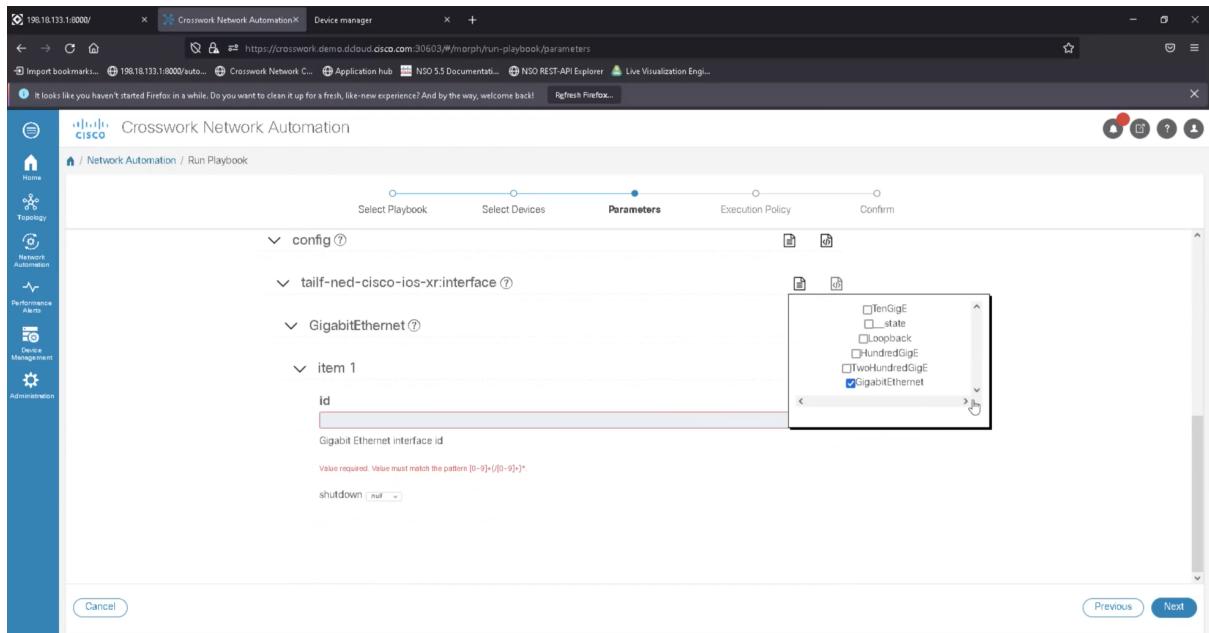
The screenshot shows the Crosswork Network Automation interface. In the left sidebar, under 'Performance Alerts', the 'Alert Dashboard' link is highlighted with a red box. The main content area displays 'Job Details' for a job set ID 0002, which was successful with 0 failures. The 'Jobs (1)' section shows a single entry for a 'Create' operation on 'Interface flap detection' for device 'closeloop'.

The screenshot shows the Crosswork Network Automation interface. The top navigation bar includes a 'View By' dropdown set to 'Device Alerts', which is highlighted with a red box. The main content area displays 'Alerts History' for 'All Impacted Devices'. It lists two devices: 'Node-4' and 'Node-5', both of which are categorized as 'CISCO-XRv9000' with IP addresses 198.19.1.4 and 198.19.1.5 respectively. The 'Severity Distribution (%)' bar for Node-4 is mostly orange, while for Node-5 it is mostly blue.

Click on the hammer symbol to see the playbook that crosswork has chosen for the remediation action. This should be the once that we have linked earlier.

The screenshot shows the Crosswork Network Automation interface for device Node-5. The top header shows the IP address 198.19.1.5 and device type CISCO-XRv9000. The status is 'Running'. Below this, the 'Enabled KPIs' section is expanded, showing various metrics like CPU threshold, CPU utilization, Ethernet port error counters, Ethernet port packet size distribution, and Interface flap detection. The 'Interface flap detection' row is highlighted with a red box. The main content area displays a table titled 'All KPIs - past 1h' showing recent alerts. One alert for 'Interface flap detection' is highlighted with a red box, showing the message 'CRITICAL: GigabitEthernet0/0/0/2 flapping' and timestamp '2022-Jun-09, 13:44:23 (GMT -04:00)'. Other alerts listed include CPU utilization and memory utilization thresholds being crossed.

Unselect all the unnecessary interface and select only the gig and put the right value in this case 0/0/0/2 which is flapping.



The screenshot shows the 'Execution Policy' step of a playbook run. The 'Execution Mode' section offers three options: 'Continuous' (run without interruption), 'Single Stepping' (run one play at a time), and 'Dry Run' (view changes without committing). The 'Collect Syslog' section has 'Yes' selected. The 'Failure policy' dropdown is set to 'On failure: Abort'. A calendar for June 2022 shows a scheduled job for June 9th. Buttons for 'Cancel', 'Previous', and 'Next' are visible.

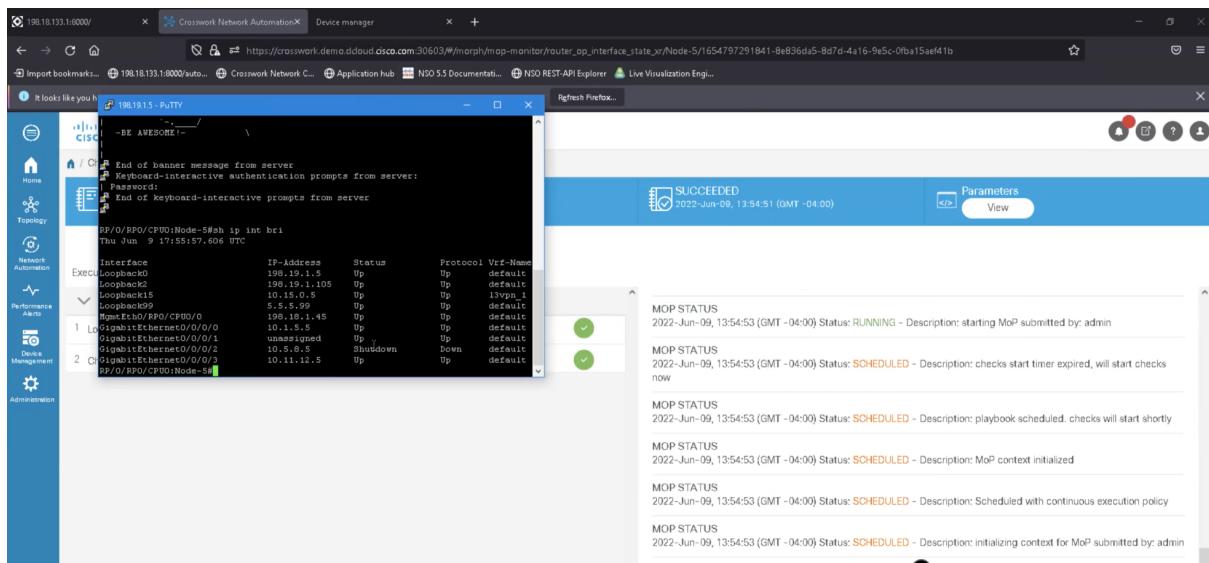
The screenshot shows the 'Confirm' step of a playbook run. The left pane displays the playbook code, which includes a configuration block for an interface. The right pane contains a 'Label your Job' section with fields for 'Name' (closedloop) and 'Labels' (closedloop,pulse_interface_flap_detecto). Buttons for 'Cancel', 'Previous', and 'Run Playbook' are visible.

Run the playbook and it will shut down the interface on Node-5.

The screenshot shows the 'Run Playbook' interface. On the right, there's a 'Confirmation' dialog box with the message: 'Do you want to run the playbook?' and two buttons: 'Confirm' (highlighted) and 'Cancel'. The main page has tabs: 'Select Playbook', 'Select Devices', 'Parameters', 'Execution Policy', and 'Confirm'. The 'Confirm' tab is active. A sidebar on the left lists navigation items: Home, Topology, Network Automation, Performance Alerts, Device Management, and Administration. The URL in the address bar is <https://crosswork.demo.ddcloud.cisco.com:30603/#/morph/run-playbook/confirm>.

The screenshot shows the same 'Run Playbook' interface after the playbook has been submitted. A success message box is displayed with a green checkmark icon and the text: 'Playbook job set has been successfully submitted'. It includes three buttons: 'View Job Set' (highlighted), 'View All Job Sets', and 'New Job Set'. The rest of the interface remains the same, including the tabs, sidebar, and URL.

The screenshot shows the 'Change Automation' interface. At the top, it displays 'Playbook Interface State change on XR' and 'Device Node-5'. The status is 'SUCCEEDED' with a timestamp of '2022-Jun-09, 13:54:51 (GMT -04:00)'. Below this, the 'Execution Mode' section shows 'Maintenance 2/2' with two tasks: 'Lock device in DLM' and 'Change the admin state of an interface', both marked as completed with green checkmarks. To the right, a 'MOP STATUS' log is shown with several entries. The URL in the address bar is https://crosswork.demo.ddcloud.cisco.com:30603/#/morph/mop-monitor/router_op_interface_state_xr/Node-5/1654797291841-8e836da5-8d7d-4a16-9e5c-0fa15ae41b.



Thank You.