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.

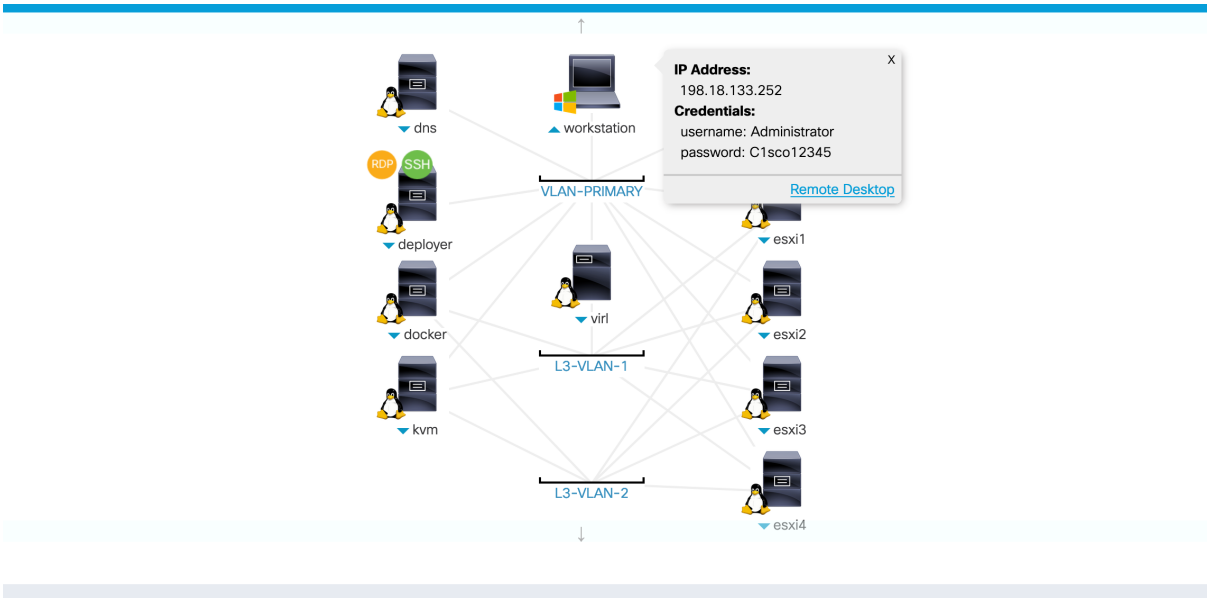
Credentials:

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	C!sco12345
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.



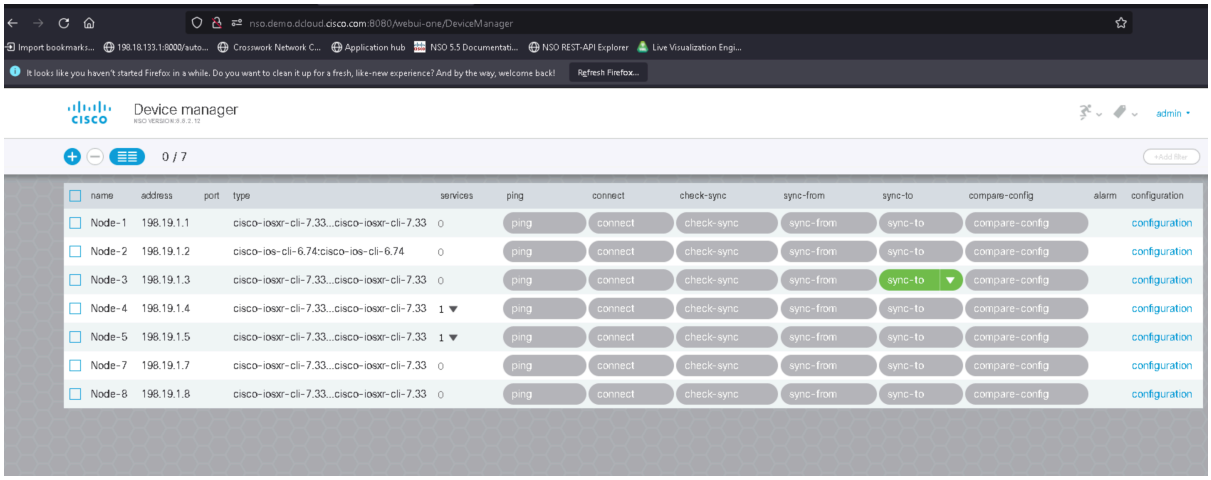
Step 1: Login to NSO GUI.

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**

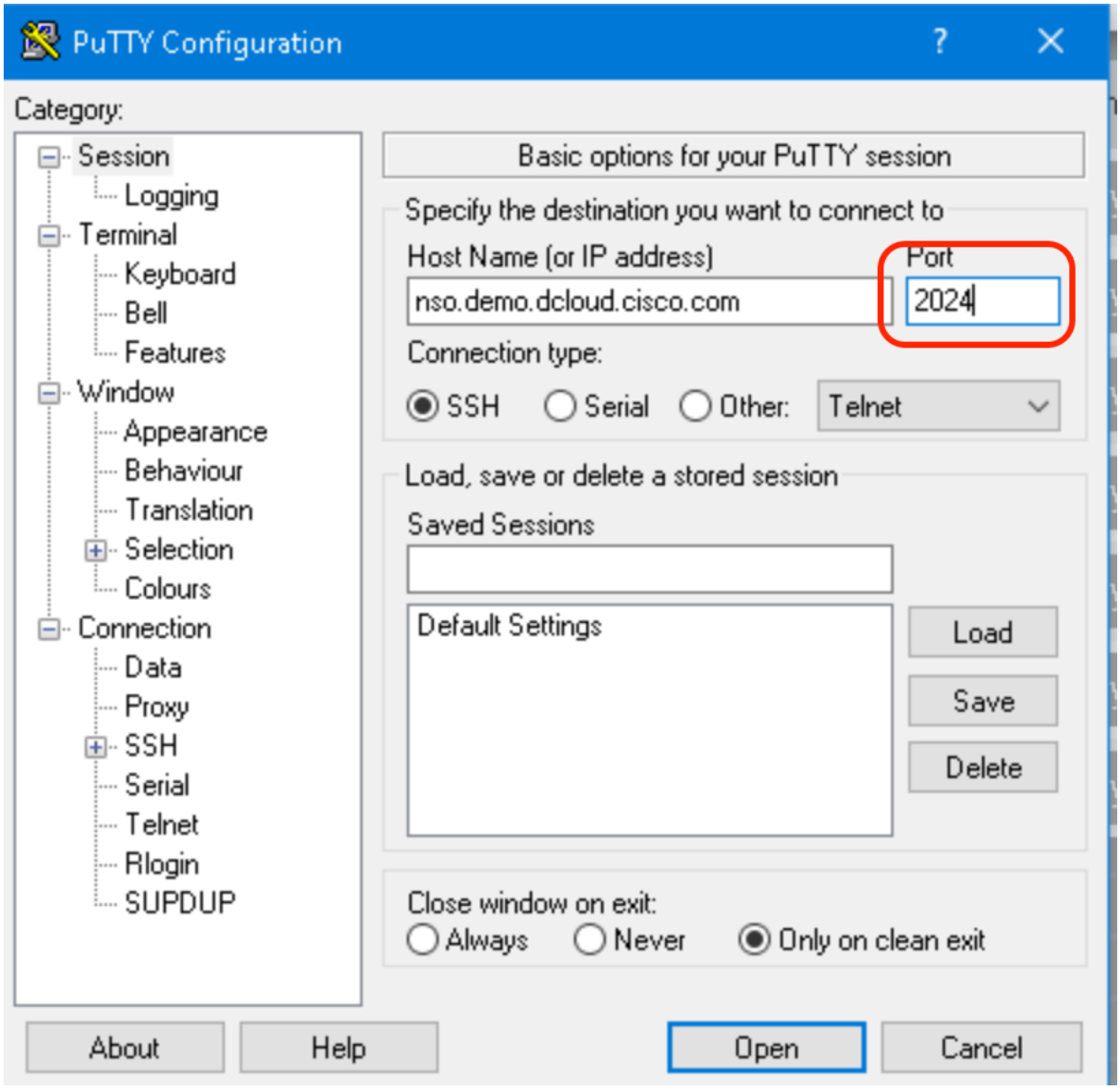
Click on Device manager and you will see below page. At this page we have all the devices which are connected to NSO. The buttons shown here do the following.

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.



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.

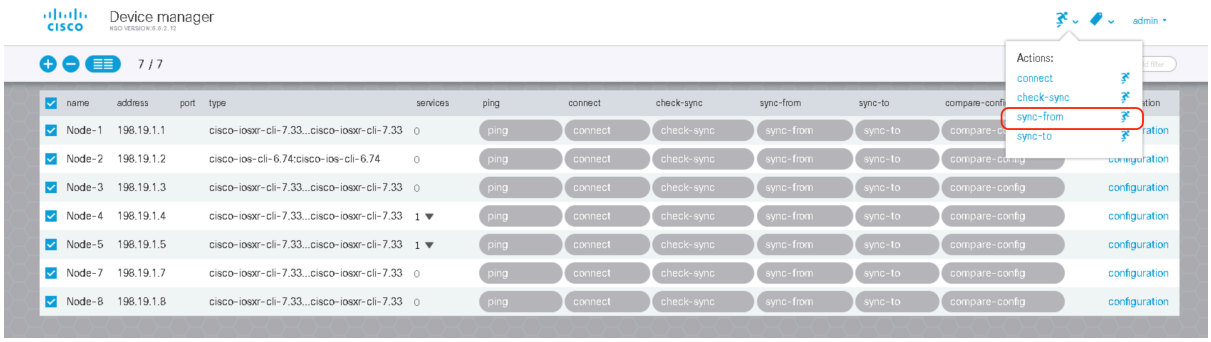
```
nso@ncs# show devices list
NAME  ADDRESS         DESCRIPTION  NED ID                ADMIN STATE
-----------------------------------------------------------------------
NCS1  172.31.187.211  -            cisco-iosxr-cli-7.33  unlocked
NCS2  172.31.187.212  -            cisco-iosxr-cli-7.33  unlocked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

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.



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.

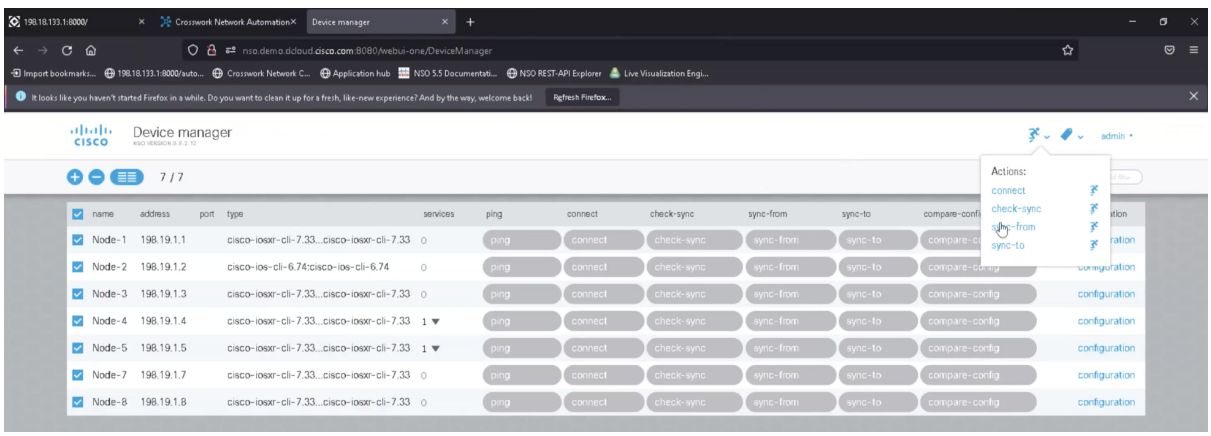
TASK-2 Close-Loop Automation

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.

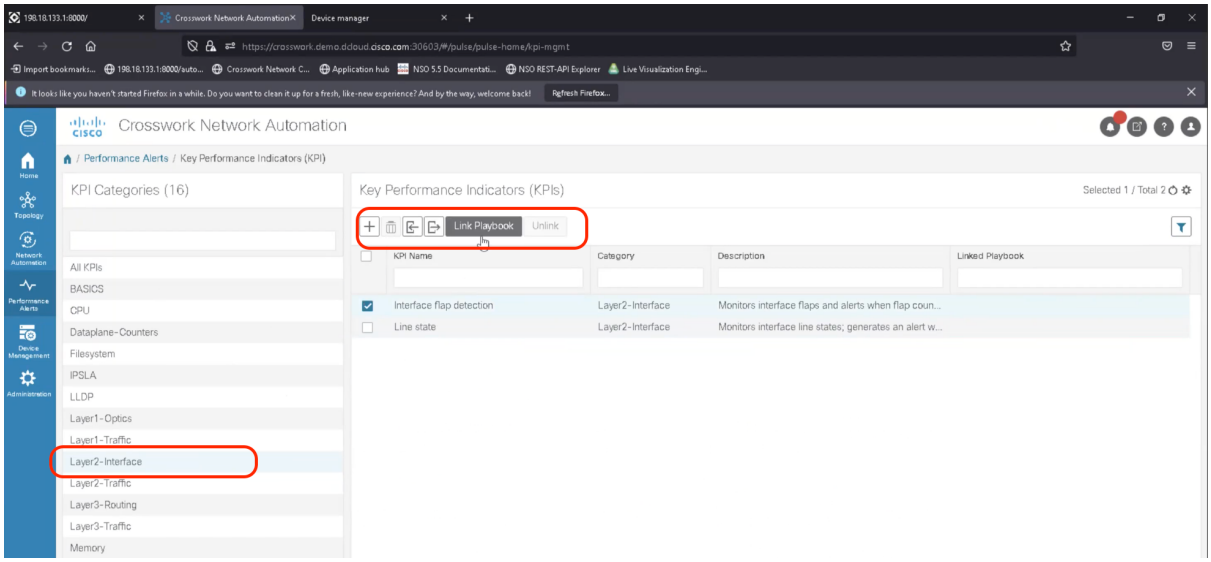
In this case we will define a playbook for interface flap. Crosswork will come to know about the flapping interface with the help of Dial-in Telemetry based KPI monitoring. Once Crosswork identifies the issue it will attach the remediation playbook with the event which can be executed easily with few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

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

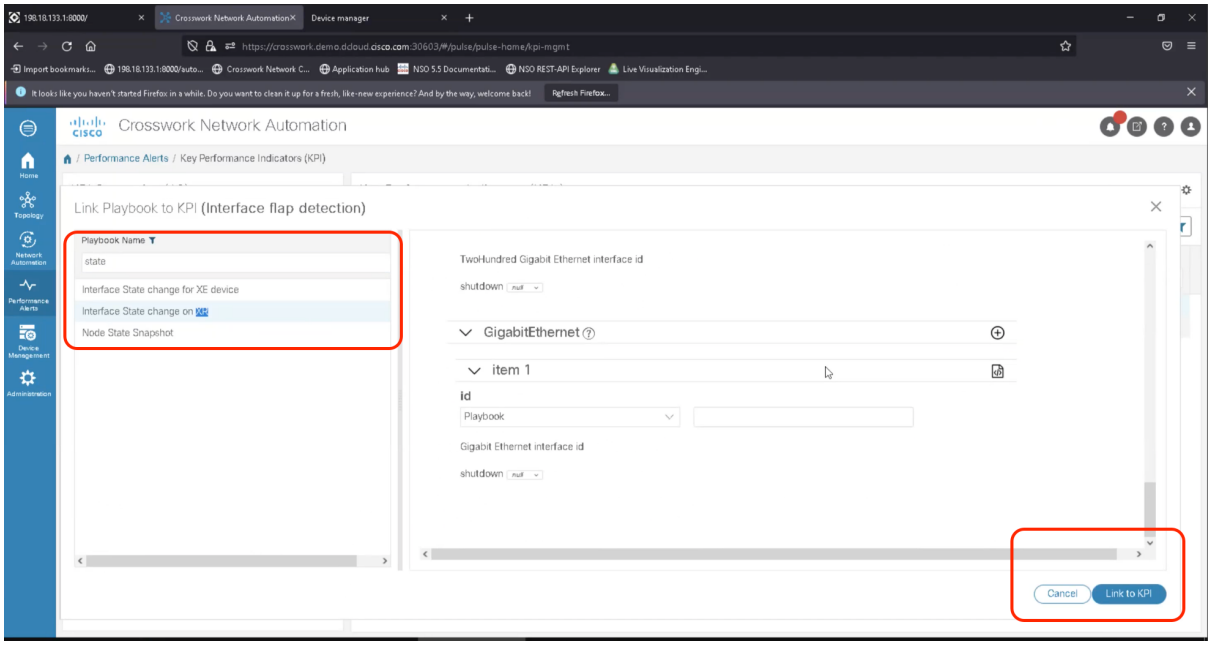


Step 2: Crosswork Configuration.

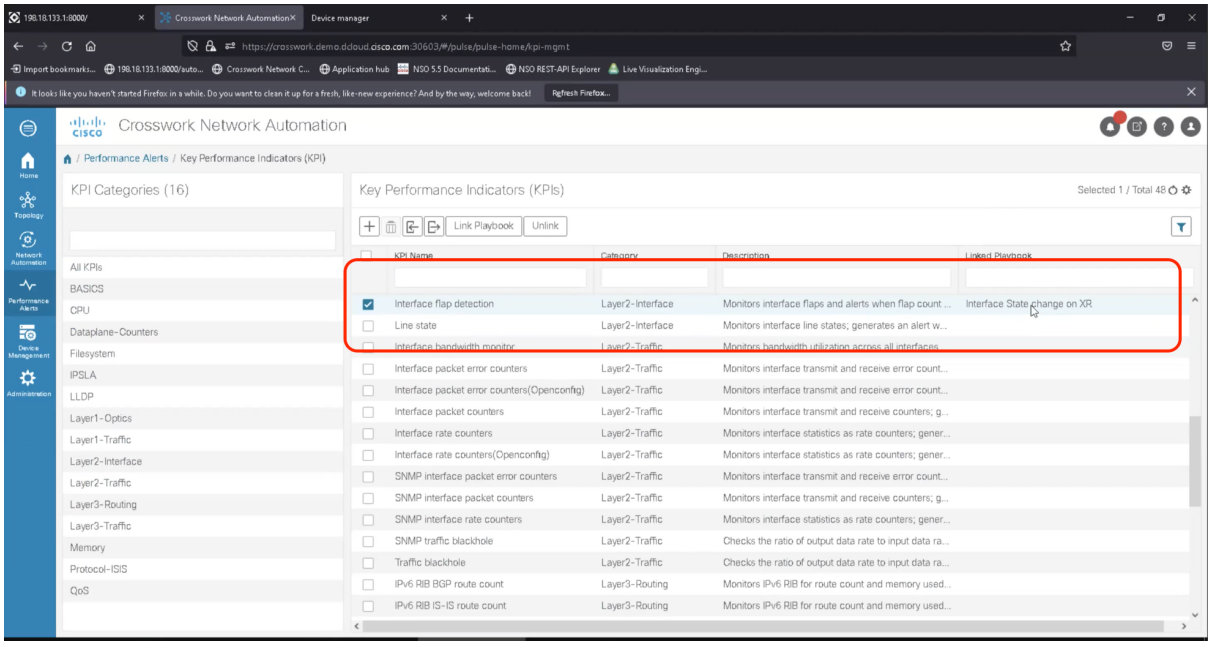
Identify the KPI and link it to the action playbook.



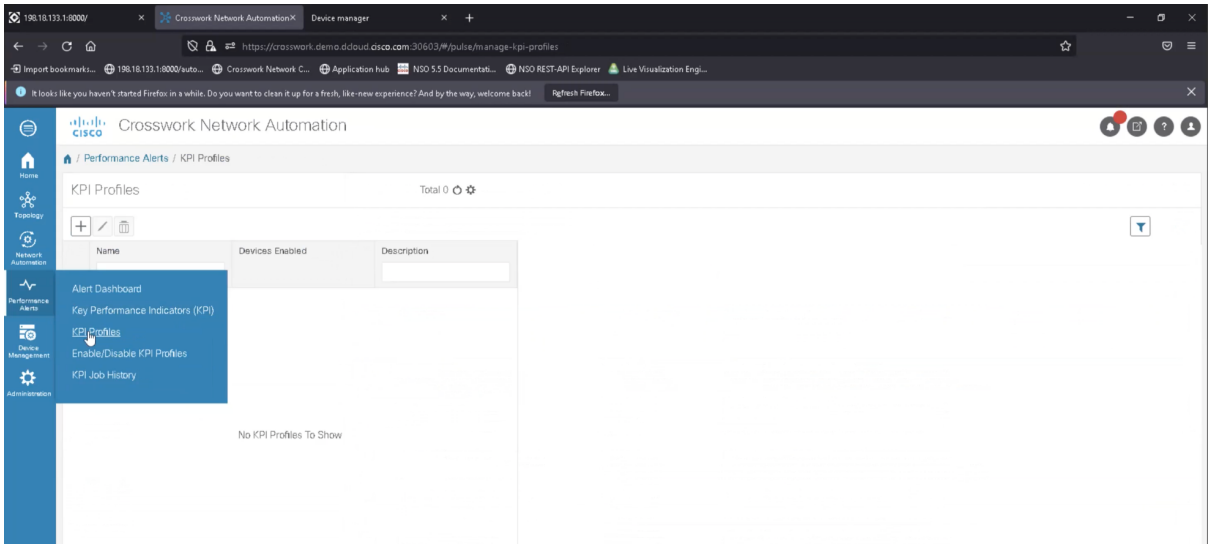
Search the right playbook with keyword “state” and link the KPI with “Interface state change on XR” playbook.

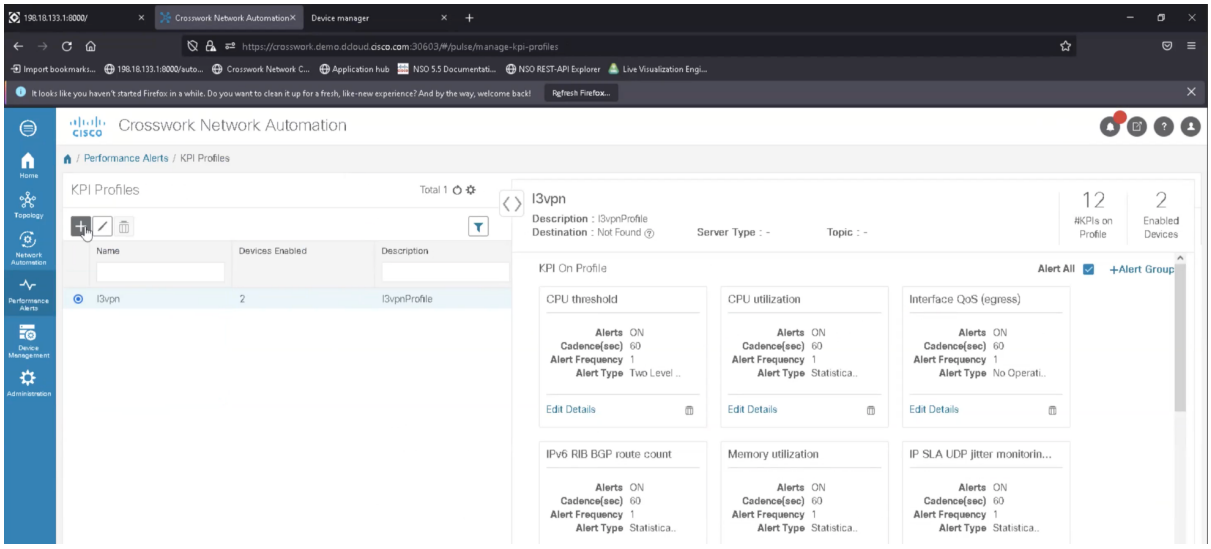


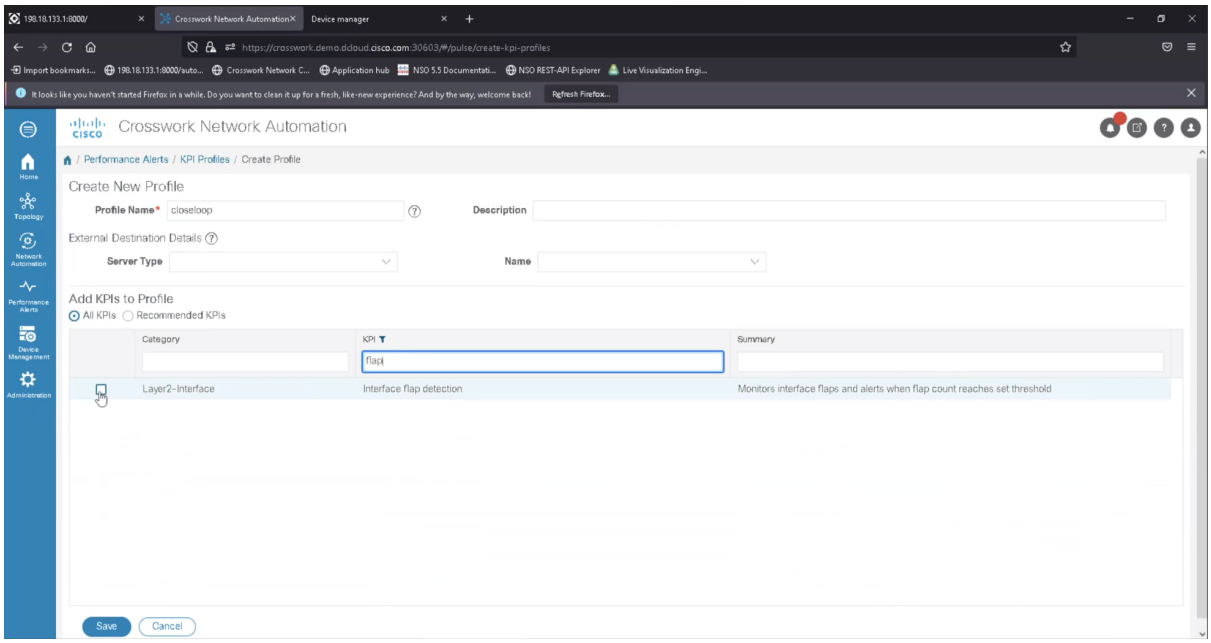
We can see below the KPI is now linked with the playbook.

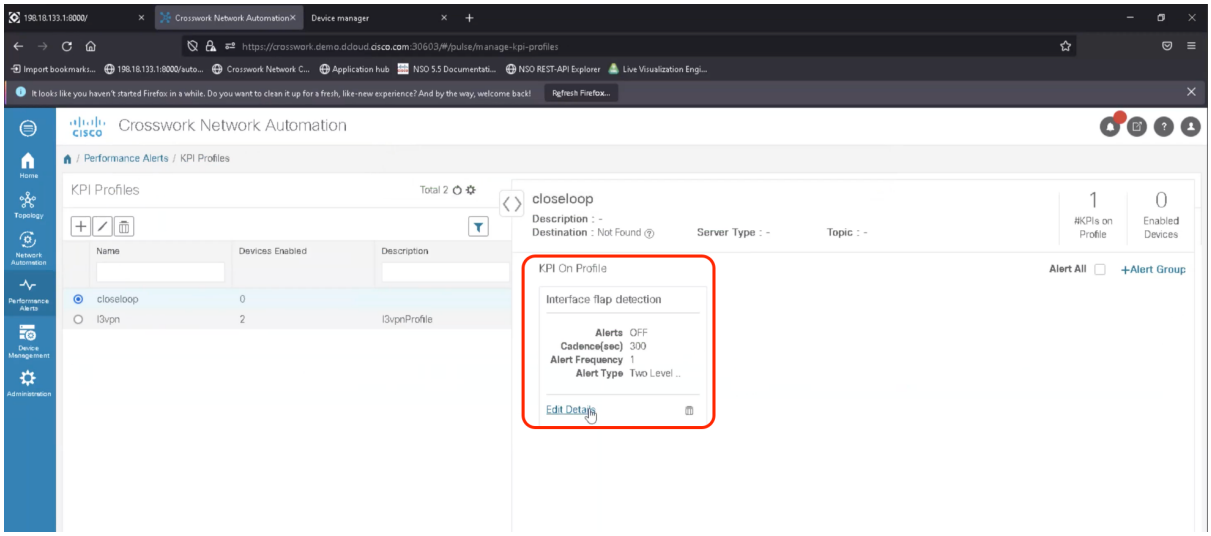


Now we need to create a KPI profile and add the profile to the node for which we need the KPI to be monitored .i.e interface flap monitoring.

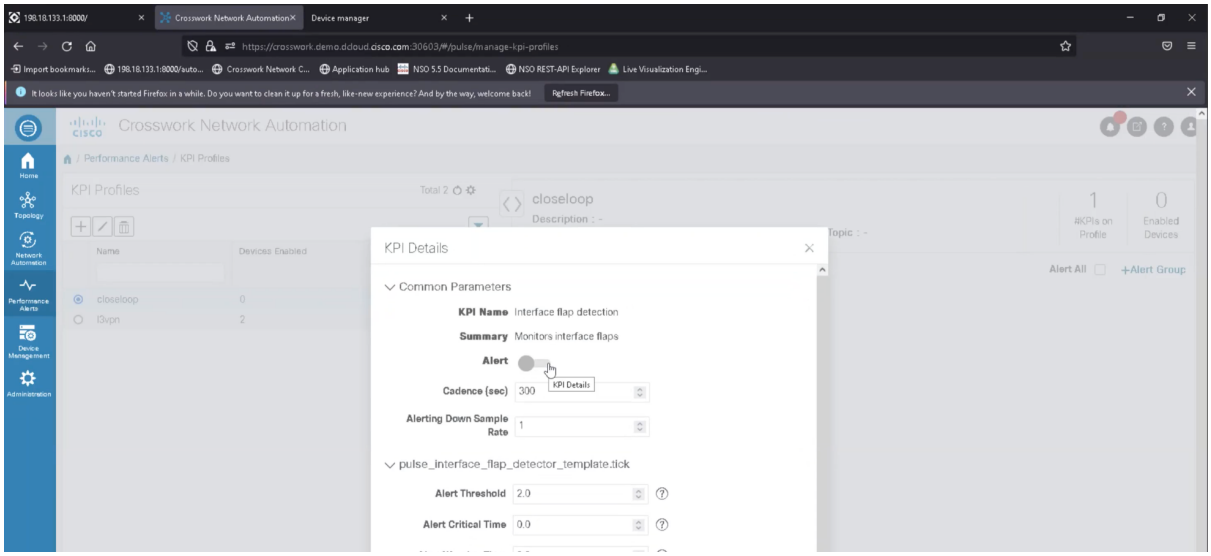



Crosswork Network Automation
Performance Alerts / KPI Profiles
KPI Profiles
Total 1
Name
Devices Enabled
Description
I3vpn
2
I3vpnProfile
I3vpn
Description : I3vpnProfile
Destination : Not Found
Server Type : -
Topic : -
12
#KPIs on Profile
2
Enabled Devices
KPI On Profile
Alert All
+Alert Group
CPU threshold
CPU utilization
Interface QoS (egress)
IPv6 RIB BGP route count
Memory utilization
IP SLA UDP jitter monitorin...
Edit Details

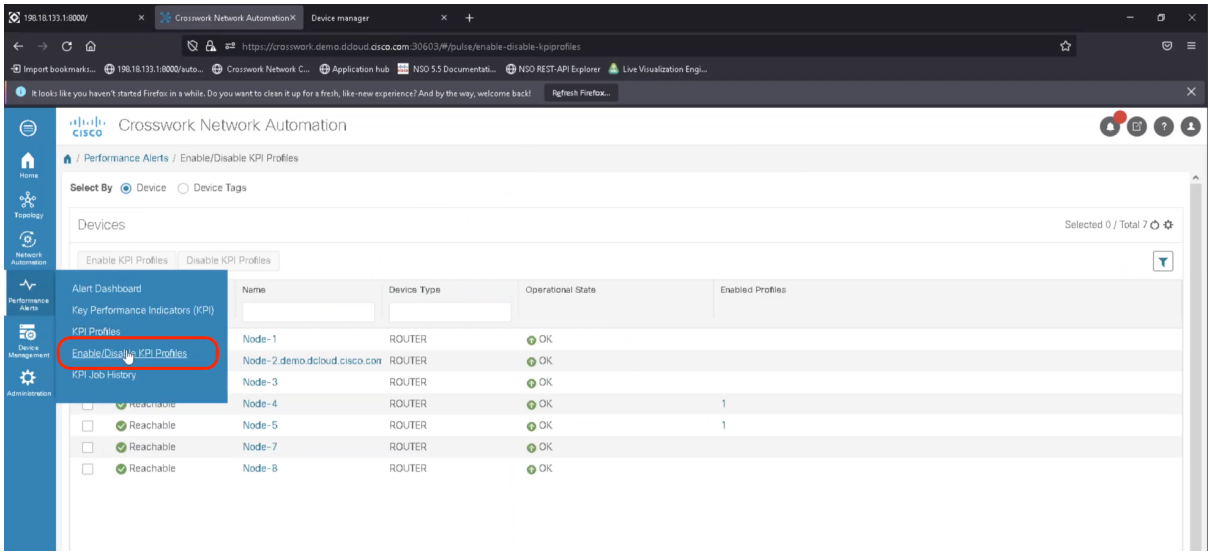

Crosswork Network Automation
Performance Alerts / KPI Profiles / Create Profile
Create New Profile
Profile Name*
closeloop
Description
External Destination Details
Server Type
Name
Add KPIs to Profile
All KPIs
Recommended KPIs
Category
KPI
Summary
flap
Layer2-Interface
Interface flap detection
Monitors interface flaps and alerts when flap count reaches set threshold
Save
Cancel



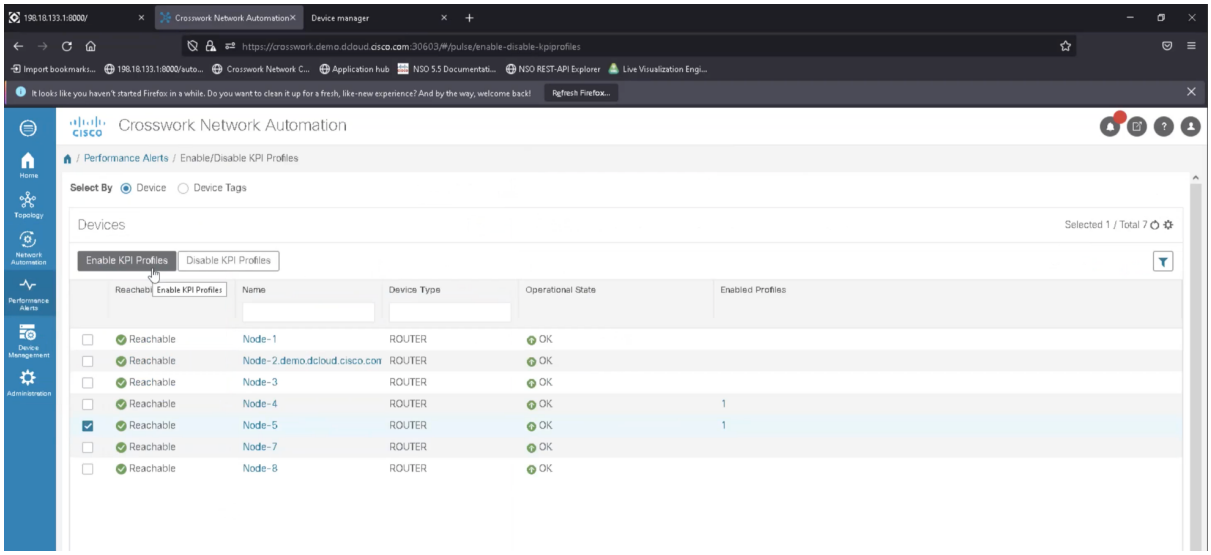
Enable the alert and set the cadence to 60 secs.

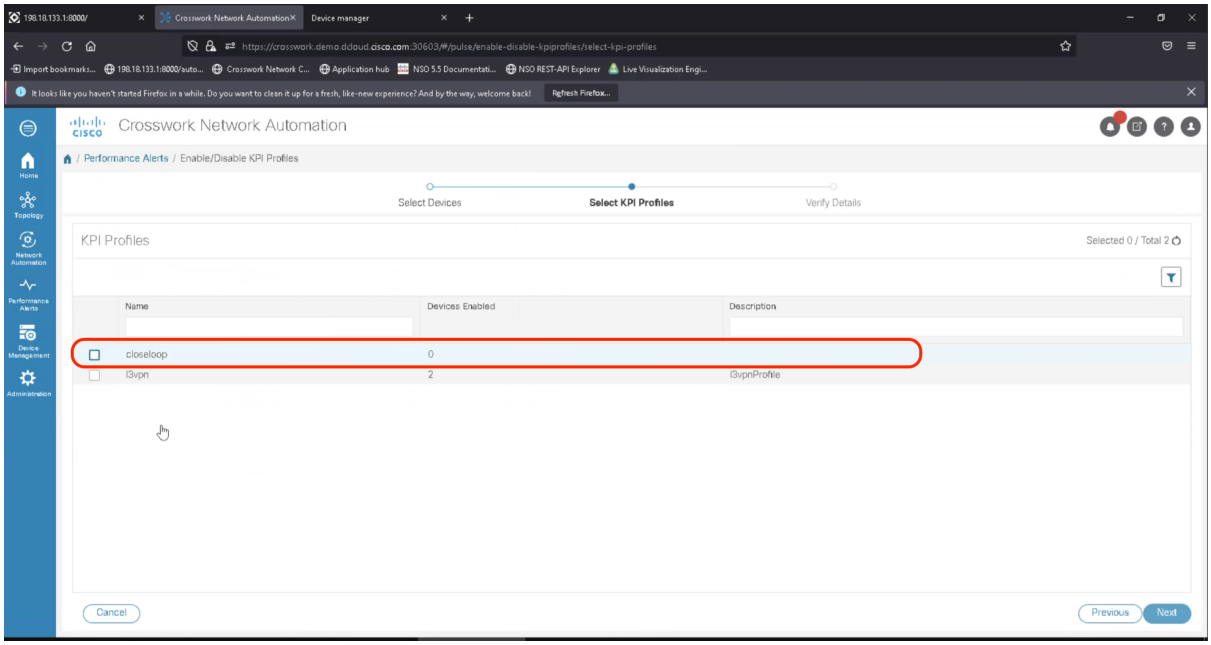


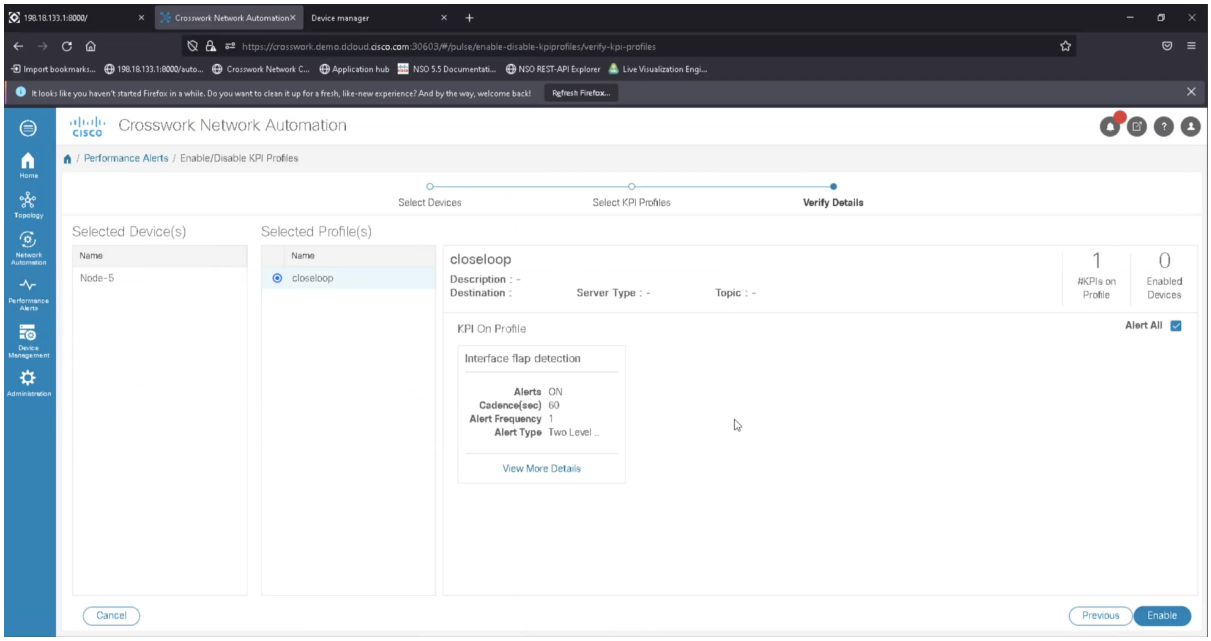
Now we need to select the node where we need to enable the KPI. In our case we are going to do this for Node-5.



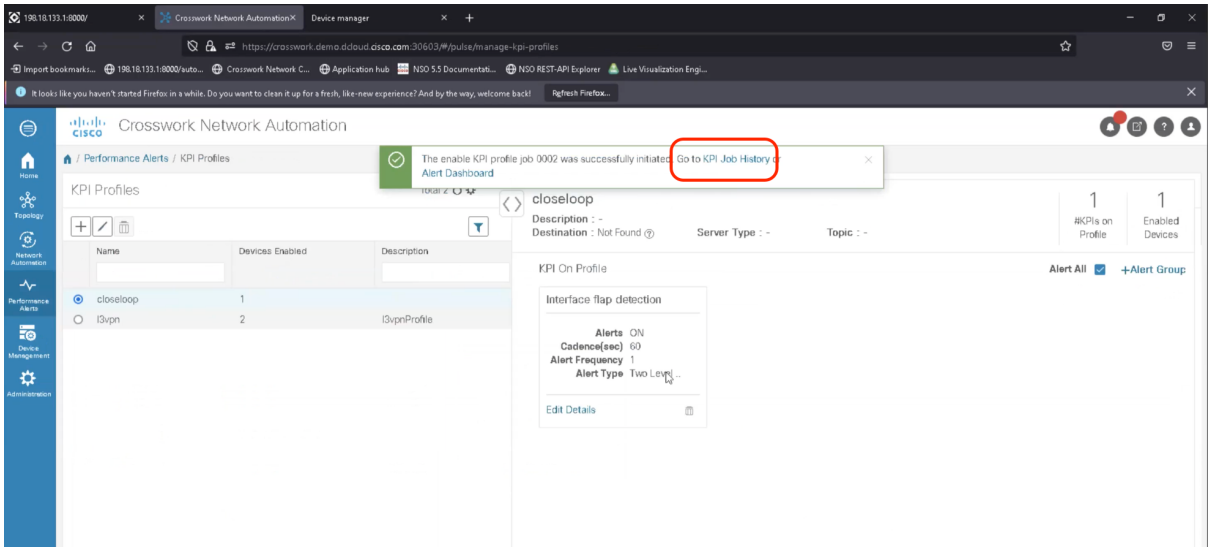
Select the node and click on enable KPI profiles.

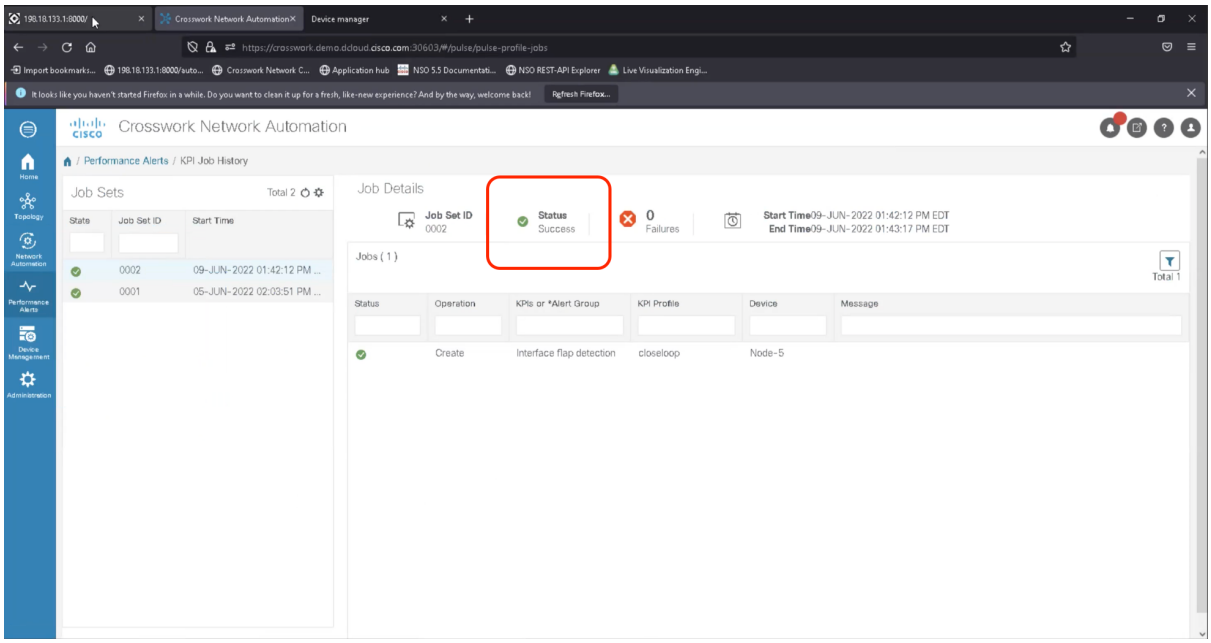






Click on enable, this will create and executable job and take almost 30 seconds to finish the job. Cick on KPI job history to see the job status.





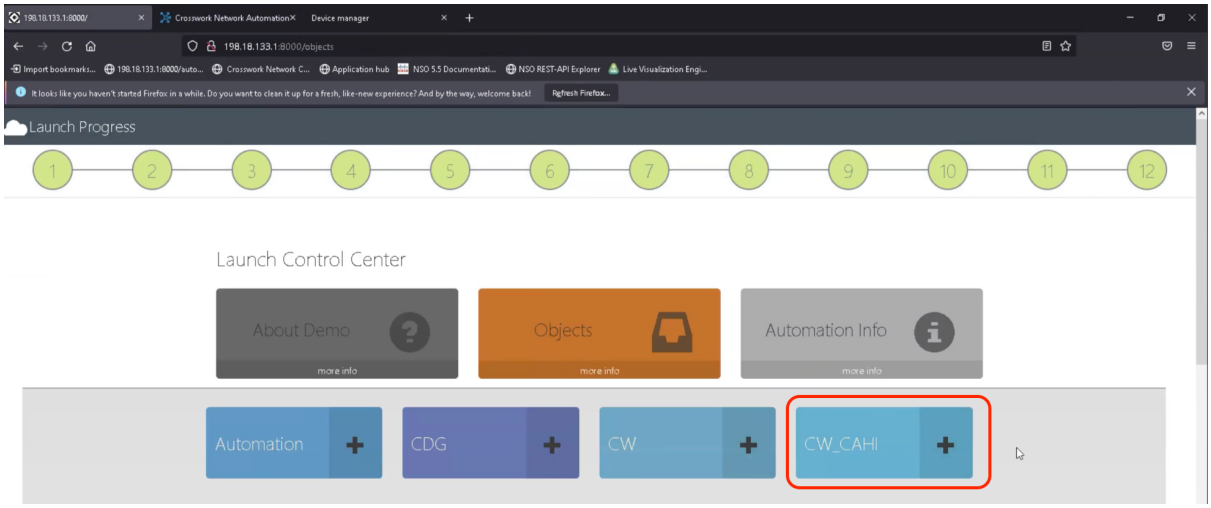
At this point if we login to the node-5 it should have a dial-in type telemetry subscription. Which means that the router is listening on a TCP port for dial-in connections from the collector, which in this case is 198.18.1.220.

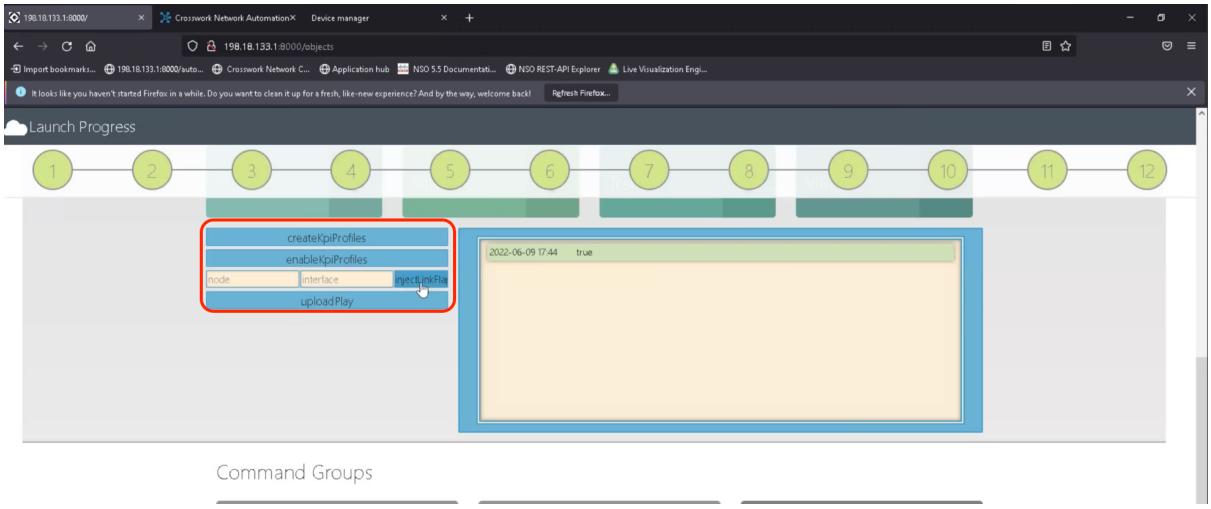
Node-5 : 198.19.1.5
SSH credentials : cisco/cisco

```
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                             IP
  GNMI_1001           gnmi-proto          dialin      Active  55664                                   198.18.1.220
    TLS :              False
```

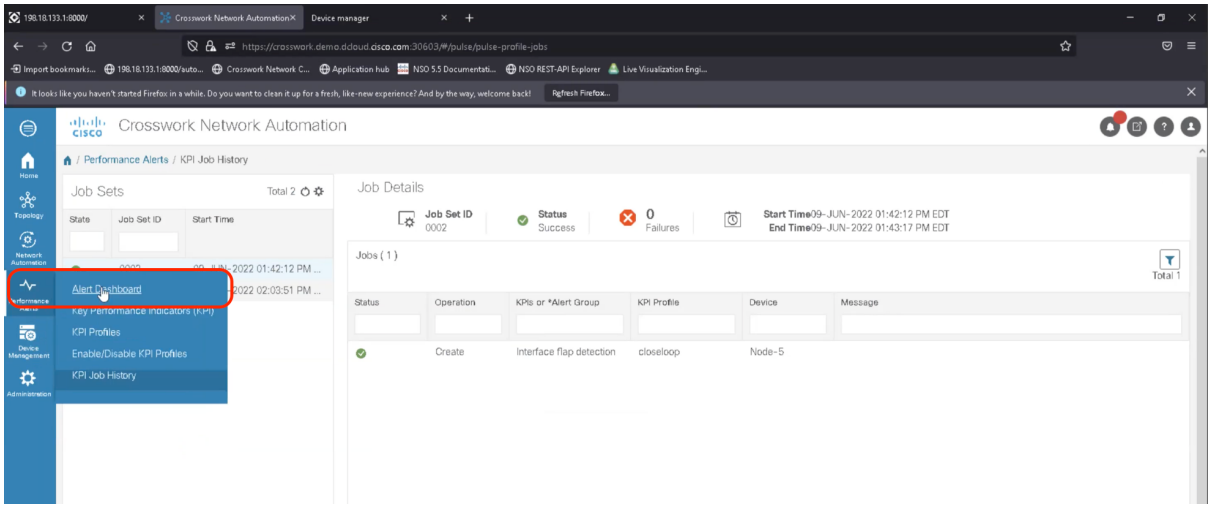
Step 3: Inject Link Flap and verify.

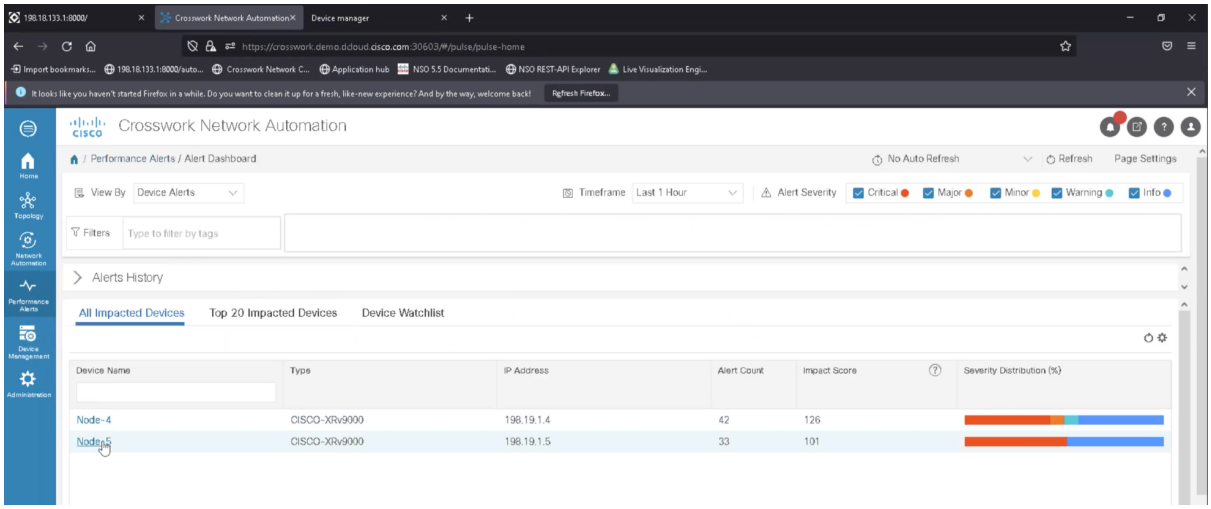
This is the demo management tool which is going to help us perform the interface flap on the router node-5.



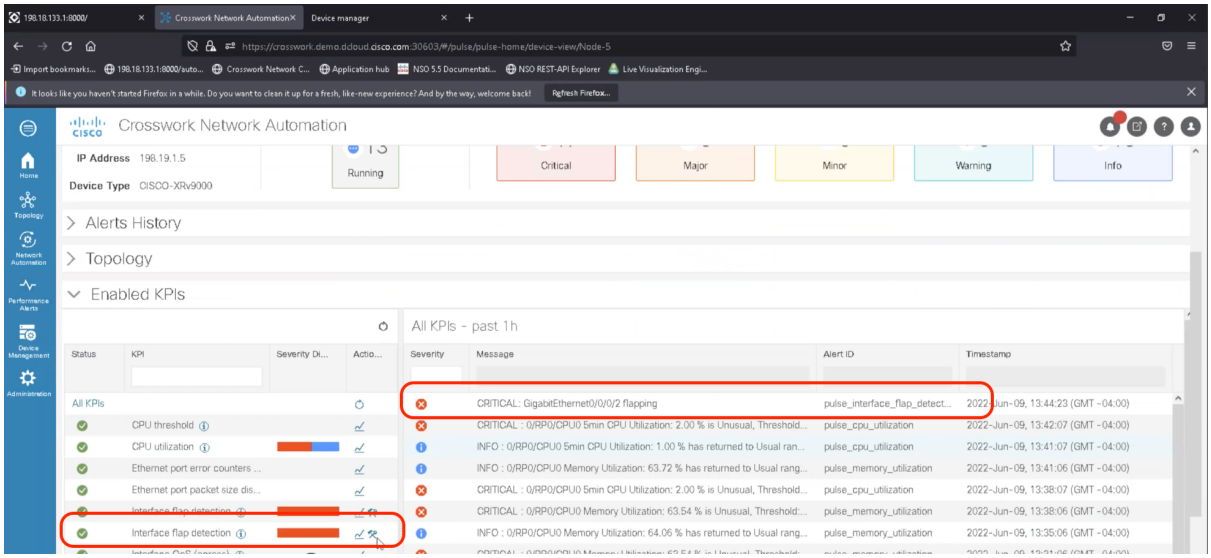


Once you click on injectflap you can go to crosswork alert dashboard to see the flap related logs for interface 0/0/0/2.

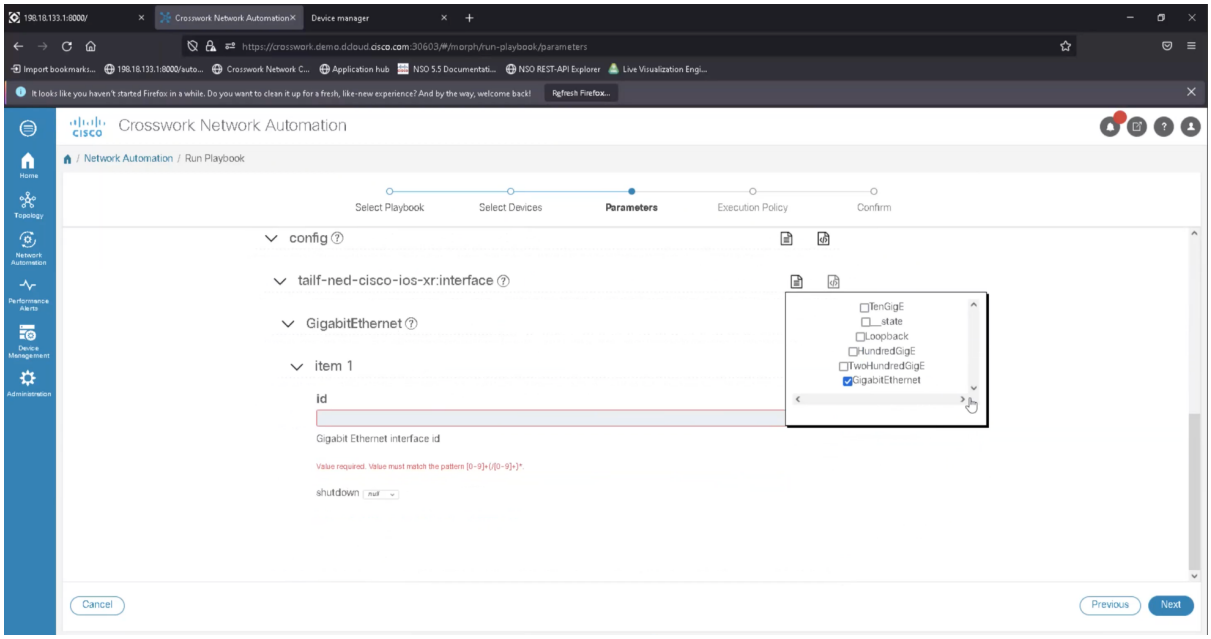


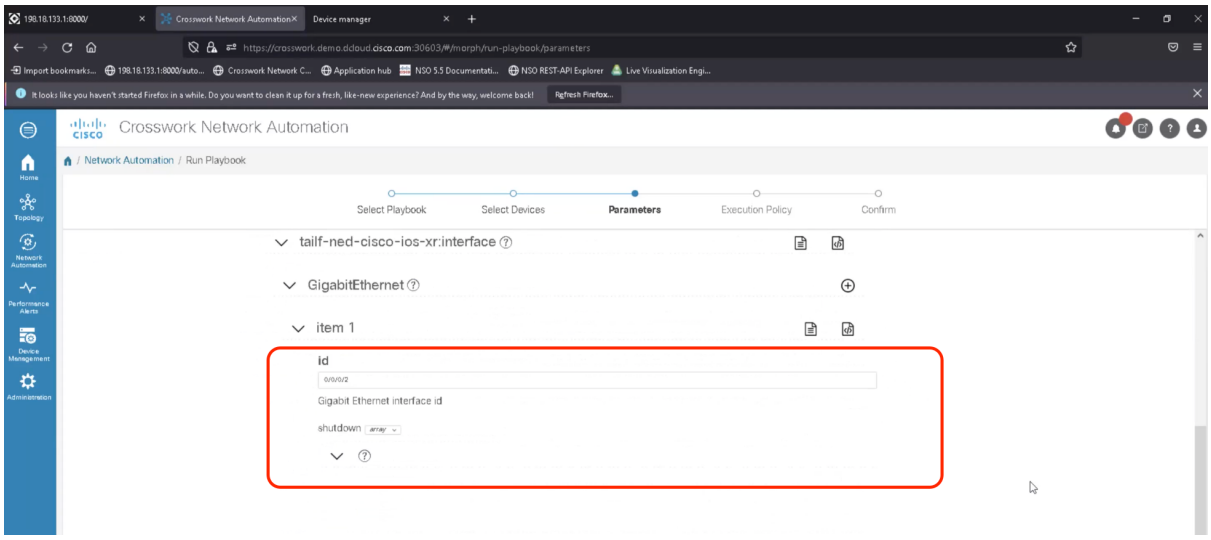


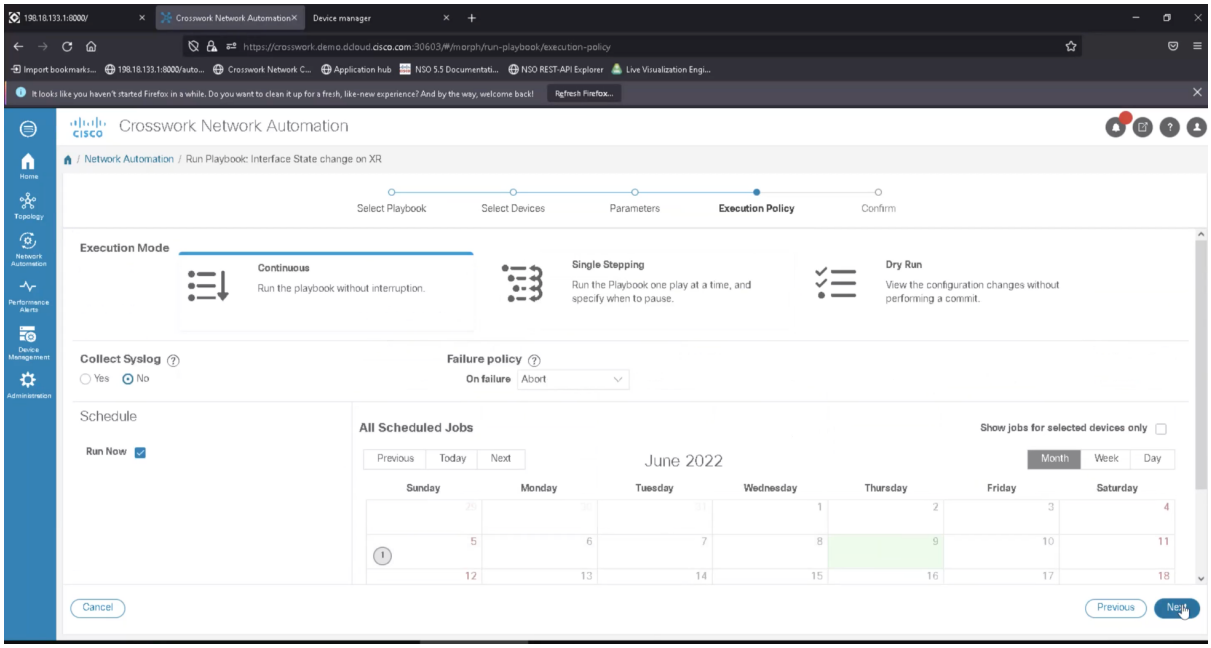
Click on the hammer symbol to see the playbook that corsswork has chosen for the remediation action. This should be the once that we have linked earlier.

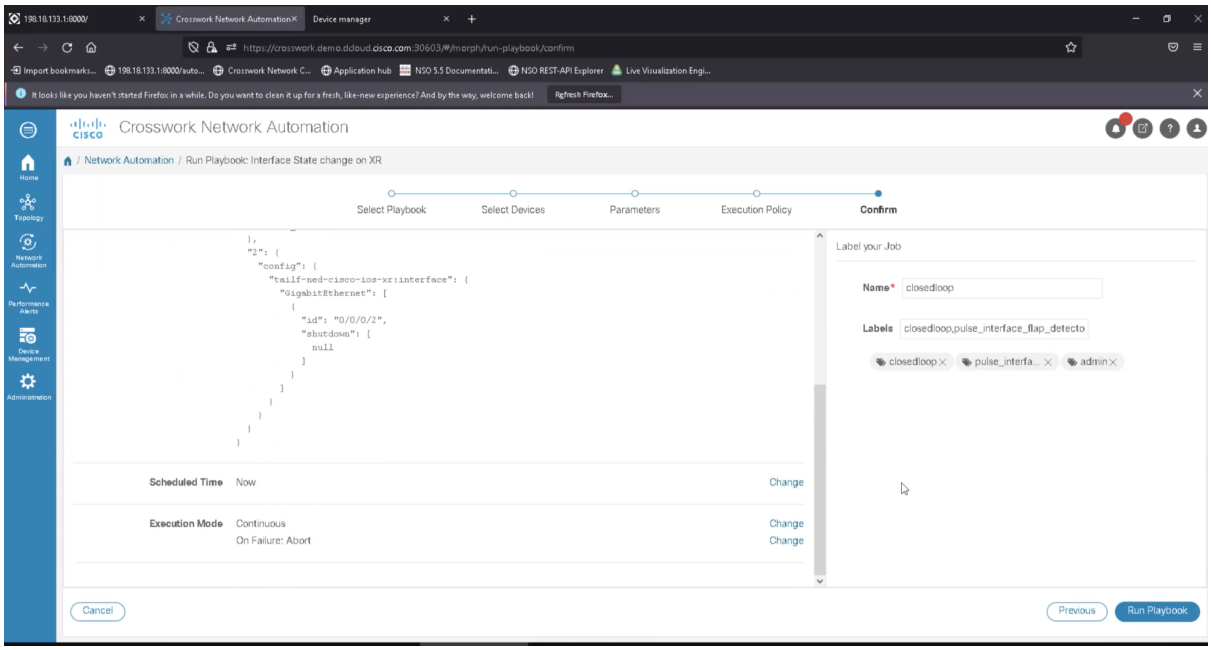


Unselect all the unnecessary interface and select only the gig and put the right value in this case 0/0/0/2 which is flapping.

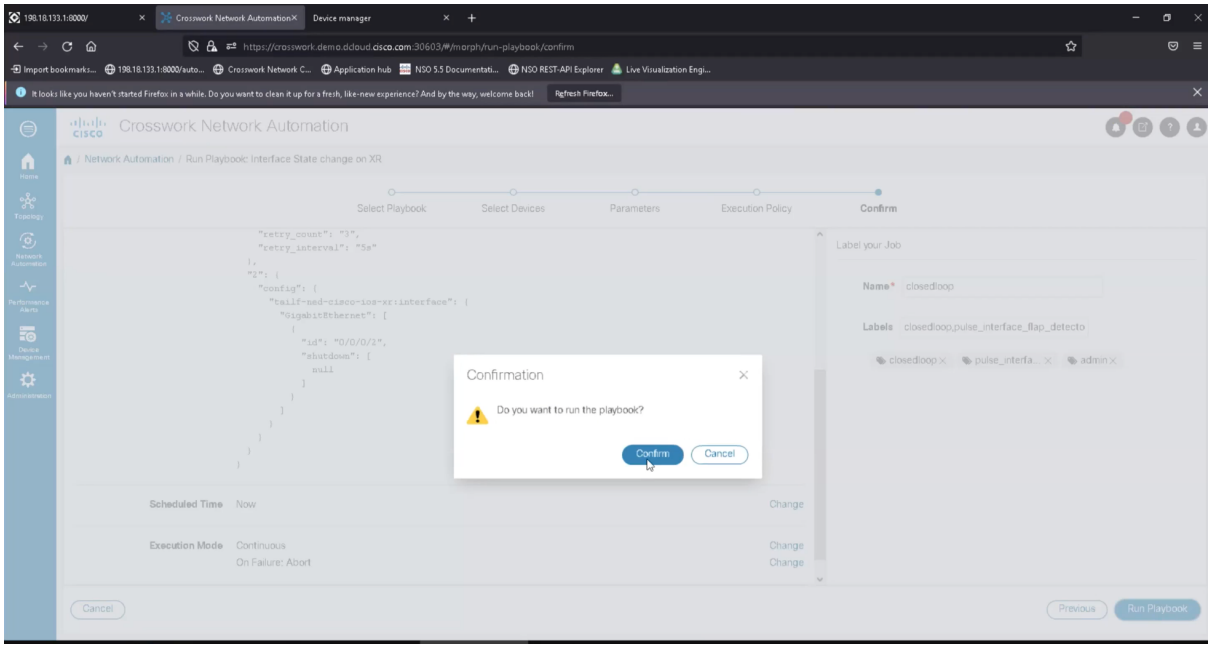


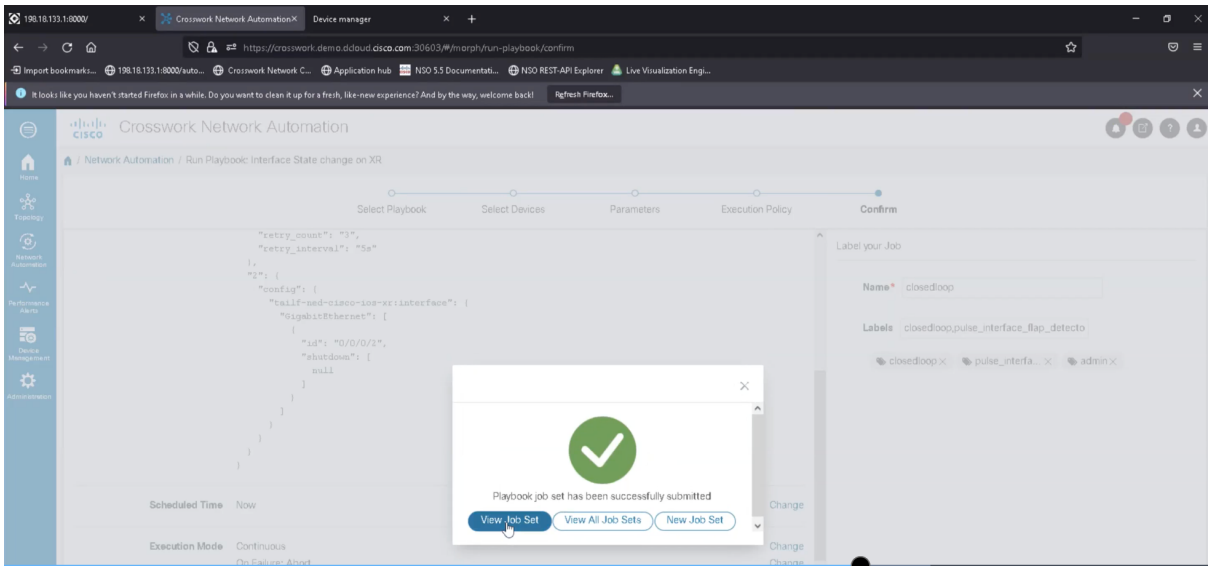


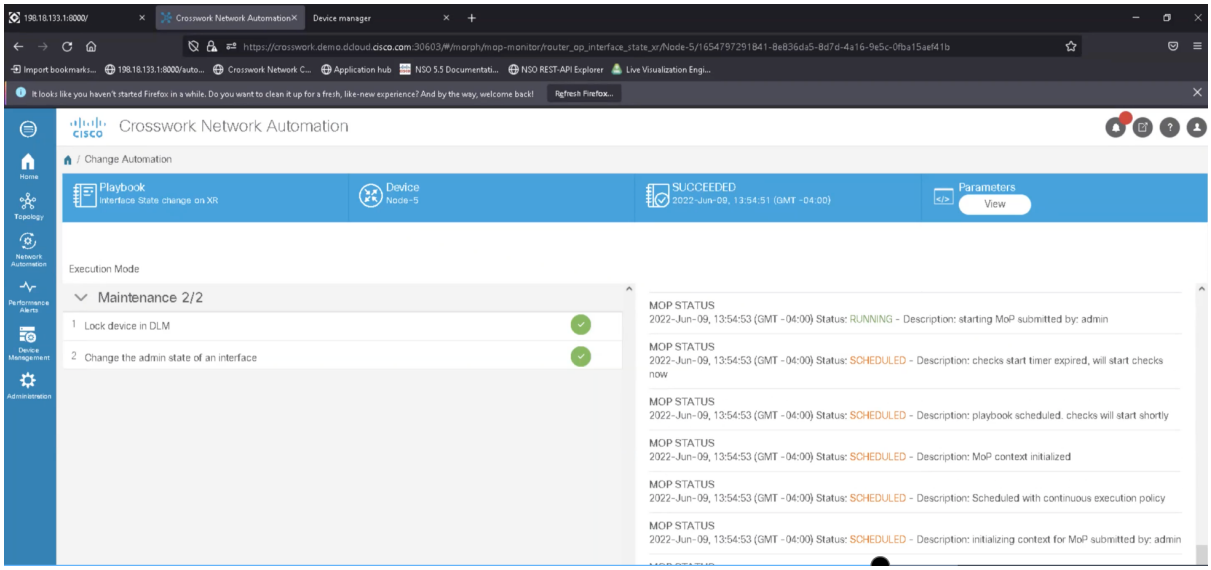


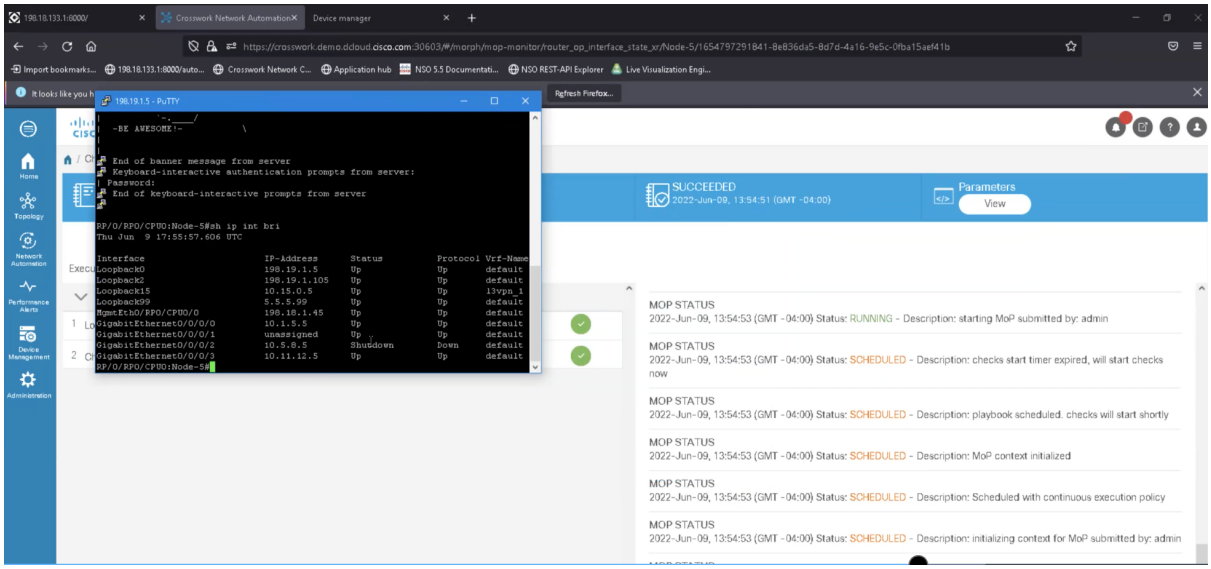


Run the playbook and it will shut down the interface on Node-5.


Crosswork Network Automation
Confirmation
Do you want to run the playbook?
Confirm
Cancel


Crosswork Network Automation
Playbook job set has been successfully submitted
View Job Set
View All Job Sets
New Job Set


Crosswork Network Automation
Change Automation
Playbook
Device
SUCCEEDED
Parameters
View
Maintenance 2/2
1 Lock device in DLM
2 Change the admin state of an interface
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: RUNNING - Description: starting MoP submitted by: admin
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: checks start timer expired, will start checks now
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: playbook scheduled. checks will start shortly
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: MoP context initialized
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: Scheduled with continuous execution policy
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: initializing context for MoP submitted by: admin


198.19.1.5 - PuTTY
-BE AWESOME!-
End of banner message from server
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
RP/0/RP0/CPU0:Node-5#sh ip int bri
Thu Jun 9 17:55:57.606 UTC
Interface IP-Address Status Protocol Vrf-Name
Loopback0 198.19.1.5 Up Up default
Loopback2 198.19.1.105 Up Up default
Loopback15 10.15.0.5 Up Up l3vpn_1
Loopback99 5.5.5.99 Up Up default
MgmtEth0/RP0/CPU0/0 198.18.1.45 Up Up default
GigabitEthernet0/0/0/0 10.1.5.5 Up Up default
GigabitEthernet0/0/0/1 unassigned Up Up default
GigabitEthernet0/0/0/2 10.5.8.5 Shutdown Down default
GigabitEthernet0/0/0/3 10.11.12.5 Up Up default
RP/0/RP0/CPU0:Node-5#
SUCCEEDED
2022-Jun-09, 13:54:51 (GMT -04:00)
Parameters
View
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: RUNNING - Description: starting MoP submitted by: admin
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: checks start timer expired, will start checks now
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: playbook scheduled. checks will start shortly
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: MoP context initialized
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: Scheduled with continuous execution policy
MOP STATUS
2022-Jun-09, 13:54:53 (GMT -04:00) Status: SCHEDULED - Description: initializing context for MoP submitted by: admin

Thank You.