Device and Credentials Sync With Cisco NSO

This section contains the following topics:

Add Devices and Credential Profiles By Synchronizing With Cisco NSO

If you are currently using Cisco Network Services Orchestrator (Cisco NSO) to manage your network devices, you may be able to perform a bulk upload of your Cisco NSO devices to Cisco Crosswork Change Automation and Health Insights by synchronizing the two systems. Cisco strongly recommends that you undertake this synchronization only once, and only with the direct assistance of your Cisco CX account team.

Note If you encounter NSO read timeout error while pushing configuration, increase the NSO timeout from 20 to 120 seconds by editing the `ncs.conf` file with `set devices global-settings read-timeout 120`.

Before you begin

To perform this task, you will need:

- A Cisco NSO server that is fully populated with the devices you want to add.
- The protocol, IP address, port, administrative user name and password needed to connect to the Cisco NSO server.
- Access to a text editor that you can use to edit the Cisco NSO server `ncs.conf` file.
- The parameters required to add Cisco NSO as a Cisco Crosswork Change Automation and Health Insights provider.
- The SNMP community strings and other credentials that Cisco NSO uses to access the devices you want to add to Cisco Crosswork Change Automation and Health Insights.

You will also need to ensure that you have pre-configured your devices to work with Cisco Crosswork Change Automation and Health Insights, as explained in Prerequisites for Onboarding Devices, Sample Configuration for Devices in Cisco NSO and Prerequisites for Device Model Driven Telemetry.

Step 1 On the Cisco NSO server: Access and edit the `ncs.conf` file to enable port 8080 and then restart the server with a package reload:

a) Access the Cisco NSO command line interface (CLI) via SSH. For example: `myname@host$:ssh NSOadmin@`*`NSOServerIPAddress`*. Supply the Cisco NSO administrator password when prompted.

b) Navigate to the `ncs.conf` file, which is usually located under `/./home/nso/`.

c) Make a backup copy of the current `ncs.conf`. Use the date in the file name to identify it as a backup. For example: `cp ncs.conf ncs.conf-1-1-2019`.

d) Edit the `ncs.conf` file's `<webui>` parameters to include the following (the critical enabling command is **highlighted**):

```
<webui>
  <enabled>true</enabled>
    <transport>
      <tcp>
        <enabled>true</enabled>
        <ip>0.0.0.0</ip>
        <port>8080</port>
     </tcp>
```

e) Restart the server and its packages by running the following commands in this order:

```
[root@localhost ncs-run]# source /home/nso/nso-5.2/ncsrc
```

To start NSO:

```
[root@localhost ncs-run]# ncs
```

To stop NSO:

```
[nso@localhost ncs-run]$ ncs --stop
```

Step 2 Log into Cisco Crosswork Change Automation and Health Insights and set up Cisco NSO as a provider, with the credentials needed to connect to Cisco NSO and to the imported devices:

a) Create a credential profile for the Cisco NSO devices, as explained in Create Credential Profiles. Be sure to include in the credential profile at least the SNMP credentials that Cisco NSO uses to manage these devices; you can create multiple sets of SNMP credentials in the profile, as well as credentials for other protocols.

b) Create an HTTP credential profile for the Cisco NSO server.

c) Add Cisco NSO as a provider, as explained in Add Providers Through the UI. Be sure to assign to the Cisco NSO provider the HTTP credential profile you just created.

d) Before logging out of the Cisco Crosswork Change Automation and Health Insights user interface, take note of the names you assigned to the Cisco NSO provider. You will need them to finish the next step.

Step 3 Synchronize Cisco Crosswork Change Automation and Health Insights's Inventory Management application with Cisco NSO's inventory services, as follows:

a) Access the Cisco Crosswork Change Automation and Health Insights CLI using SSH and the administrator ID. For example: `myname@host$:ssh cw-admin@`*`CrossworkServerIPAddress`*.

```
myname@host$:ssh cw-admin@CrossworkServerIPAddress
```

When prompted, enter the administrator password.

b) Switch to superuser status:

```
myname@host$:sudo su
```

When prompted, enter the administrator password.

c) Enter the following command to find the component ID for the Inventory Management Kubernetes pod container:

```
kubectl get pods | grep dlmi
```

The response will contain the component ID as a hash appended to the pod name: `robot-dlminvmgr-componentID`

d) Enter the following command to access the Inventory Management Kubernetes container:

```
kubectl exec -it robot-dlminvmgr-componentID bash
```

Where *componentID* is the ID you retrieved in the previous step.

e) Synchronize Cisco NSO inventory services with Inventory Management using the following command:

```
bash# syncsvc --cwhost CrossworkServerIPAddress --cwuser CrossworkAdminUser --cwpass
'CrossworkAdminPassword' --provpass NSOAdminPassword --provider ProviderName --oper get
```

Where:

- *CrossworkServerIPAddress* is the IP address of the Cisco Crosswork Change Automation and Health Insights server.
- *CrossworkAdminUser* is the user name of the Cisco Crosswork Change Automation and Health Insights administrator (**cw-admin**).
- *CrossworkAdminPassword* is the password for the Cisco Crosswork Change Automation and Health Insights cw-admin user.
- *NSOAdminPassword* is the password for the Cisco NSO admin user.
- *ProviderName* is the name of the Cisco NSO provider you created.

Synchronization will begin as soon as connection is established. When device processing is finished, verify that the sync added all the Cisco NSO devices to Cisco Crosswork Change Automation and Health Insights successfully.

Device and Credentials Sync With Cisco NSO