Cisco NSO Crosswork Hierarchical Controller - Function Pack

Installation Guide

Version 8.0.0

Contents

Preface

Abstract

This Cisco Network Service Orchestrator Crosswork Hierarchical Controller - Function Pack (NSO CHCO FP) Installation Guide includes information to help you install Cisco NSO CHCO FP.

Audience

This document is intended for Cisco Advanced Services developers, network engineers, and system engineers to install the CHCO FP functionalities to Cisco customers.

Additional Documentation

This documentation requires the reader to have a good understanding of NSO and its usage as described in the NSO documentation.

Sl. No.	Documentation
1.	Cisco NSO CHCO FP User Guide
2.	Cisco NSO Installation Guide
3.	Cisco NSO User Guide

Bias-free Documentation Policy

Cisco follows a bias-free documentation policy. According to this policy, Cisco treats all persons with respect—regardless of race, color, ancestry, national origin, age, sex, citizenship, veteran status, marital status, sexual orientation, physical or mental ability, religious creed, or medical condition. Language or graphic elements that offend others violate our business philosophy and our company policy.

Installation Methods

You can perform CHCO FP installation on NSO in two ways:

- System Installation
- Local Installation

The system installation is for a real-time production environment and is the preferred installation method. The local installation is the demo version of the installation.

You require sudo user privileges to perform the installation and to run the installation commands. You can perform CHCO FP installation on a single machine or multiple machines at a given time. System installation is used for NSO installation on multiple hosts/VMs from a Single Controller host.

This documentation describes how to perform the CHCO FP system installation. For information on local installation, contact your Cisco representative.

Installation Requirements

This topic discusses the requirements to install CHCO FP.

Note: CHCO function package uses L2NM and L3NM IETF models as NBI service yang. Therefore, the function pack cannot be installed on NSO which has any other IETF L2NM/L3NM function packages.

System Requirements

This section outlines the hardware requirements, software requirements, and platform dependencies to successfully install Cisco NSO CHCO FP v2.0.0 on NSO v6.1.4.

Item	Requirement
Operating systems	NSO and CHCO FP are available for all Linux distributions and supported on the following operating systems: Ubuntu v18.04 LTS (Bionic) RedHat Linux v8.x
Software	Open JDK v11.0.7 or higher Python v3.11 or higher
NSO version	6.1.4
NSP NED	1.0.4
CNC NED	1.0.0
ulimit value for NSO	64000 (minimum)
User account	User account requires sudo privileges.

Prerequisites

1. Make sure to have sudo privileges to perform the CHCO FP installation. A sudo user has administrator privileges. This user must also be part of the **ncsadmin** group.

2. Perform a system installation of NSO v6.1.4. For more information on the NSO installation procedure, see the ***NSO Installation Guide***.

3. Make sure JDK-11 or higher is installed.

4. Make sure Python v3.11 or higher is installed.

5. Add ulimit level value for NSO in **/etc/init.d/ncs** as follows:

```
...
ncsdir=/opt/ncs/current
confdir=/etc/ncs
rundir=/var/opt/ncs
logdir=/var/log/ncs

ncs=${ncsdir}/bin/ncs
ulimit -n 65535
prog=ncs
conf="-c ${confdir}/ncs.conf"
heart="--heart"
...
```

6. Add and verify the ulimit value for the operating system. The following is an example to add the ulimit for the operating system in the **/etc/security/limits.conf** file.

   Note: For large scale or container deployments, set the ulimit value for the operating system to 65536. This prevents resource exhaustion and improves performance.

```
* soft nproc 65535
* hard nproc 65535
* soft nofile 65535
* hard nofile 65535
```

7. Run the `sysctl -p` script to set the parameters.

8. Log out of the system and log in again to apply the new values.

9. Verify the ulimit values are applied.

```
$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority            (-e) 0
file size               (blocks, -f) unlimited
```

```
pending signals                 (-i) 63407
max locked memory       (kbytes, -l) unlimited
max memory size         (kbytes, -m) unlimited
open files                      (-n) 65535
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
real-time priority              (-r) 0
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) unlimited
max user processes              (-u) 4096
virtual memory          (kbytes, -v) unlimited
file locks                      (-x) unlimited
```

10. Install confluent Kafka for the Kafka connector class to manage Kafka integrations with other systems. Kafka libraries are bundled with the package in the event that access to external networks is not available.

```
pip3 install confluent_kafka
```

Performing CHCO FP System Installation

CHCO FP is installed on NSO. Make sure the system requirements are met for the installation. For more information, see **System Requirements**.

Note: The NSO CHCO NSP function package uses L2NM and L3NM IETF models as NBI service yang. Therefore, the function package cannot be installed on NSO which has any other IETF L2NM/L3NM function packages.

Do the following to install CHCO FP on NSO:

1. Log in to the host machine as the sudo user.

2. Obtain and download the **nso-<*version*>-hco-<*version*>.signed.bin** package from Cisco website and copy it to the host server. (For example, **nso-6.1.4-hco-2.0.0.signed.bin**).

3. Extract the content of the bin file to the current directory.

   ```
   $ sh nso-<version>-hco-<version>.signed.bin
   ```

   This verifies the authenticity of the product. However, if you encounter any network connectivity issues, run the following command to skip this verification.

   ```
   $ sh nso-<version>-hco-<version>.signed.bin --skip-verification
   ```

   Note: Ensure the software is authentic before you skip verification.

4. Extract the TAR file to the current directory. If the folder already exists, create a backup of the existing folder before extracting the file.

   ```
   $ tar -vxf nso-<version>-hco-<version>.tar.gz
   ```

5. Stop NSO.

```
$ sudo /etc/init.d/ncs stop
```

6. Go to the **function-packages** directory.

```
$ cd nso-<version>-hco-<version>/function-packages
```

7. Copy and link the following packages to install the FP.

```
sudo cp ncs-<version>-nokia-nsp_rc-<version>.tar.gz /opt/ncs/packages

sudo cp ncs-<version>-cisco-nsp-fp-<version>.tar.gz /opt/ncs/packages

sudo cp ncs-<version>- cisco-hco-fp-<version>.tar.gz /opt/ncs/packages

sudo cp ncs-<version>-cisco-cnc_rc-gen-<version>.tar.gz /opt/ncs/packages
```

8. Restart NSO with the **package-reload** option.

```
$ sudo /etc/profile.d/ncs.sh

$ sudo /etc/init.d/ncs restart-with-package-reload
```

9. Set NACM rules.

```
admin@ncs% set nacm groups group ncsadmin user-name <Linux-user>
admin@ncs% commit
Commit complete.

admin@ncs% show nacm
read-default     deny;
write-default    deny;
exec-default     deny;
groups {
    group ncsadmin {
        user-name [ admin private <Linux-user>];
    }
    group ncsoper {
        user-name [ public ];
    }
}
...
```

10. Configure global settings for ssh-rsa algorithms public key.

```
% show devices global-settings ssh-algorithms public-key

public-key [ ssh-ed25519 ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-
sha2-nistp521 rsa-sha2-512 rsa-sha2-256 ];

% set devices global-settings ssh-algorithms public-key [ ssh-ed25519
ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521 rsa-sha2-512
rsa-sha2-256 ssh-rsa ]

% commit

 % show device global-settings ssh-algorithms public-key
```

```
public-key [ ssh-ed25519 ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-
sha2-nistp521 rsa-sha2-512 rsa-sha2-256 ssh-rsa ];
```

11. Configure the local ncsadmin user as a hco-nm-settings local-user for the FP to identify the user to push the configurations.

12. Verify the packages are up and running.

```
admin@ncs> show packages package oper-status

                                                                     PACKAGE
                      PROGRAM                                        META    FILE
                      CODE      JAVA           PYTHON      BAD NCS PACKAGE PACKAGE CIRCULAR     DATA    LOAD    ERROR
NAME               UP ERROR     UNINITIALIZED  UNINITIALIZED VERSION NAME    VERSION DEPENDENCY   ERROR   ERROR   INFO    WARNINGS
---------------------------------------------------------------------------------------------------------------------------------
cisco-cnc_rc-gen-1.0  X   -         -              -           -       -       -       -            -       -       -       -
cisco-hco-fp          X   -         -              -           -       -       -       -            -       -       -       -
nokia-nsp_rc-gen-1.0  X   -         -              -           -       -       -       -            -       -       -       -

[ok][2024-02-23 09:40:37]
```

Uninstalling CHCO FP

The user performing the uninstallation must be part of the **ncsadmin** group. Before you uninstall CHCO FP, remove the associated services and any associated devices from the system. Make sure no zombie services are running for the services and all the devices are removed from the NSO device tree.

To uninstall CHCO FP:

1. Delete the deployed devices and services.

```
ncs_cli -u <linux-user>
configure
delete l2vpn-ntw vpn-services vpn-service
commit

delete l3vpn-ntw vpn-services vpn-service
commit

delete hco-nm-settings default-hco-controller
commit

## Delete any HCO controller devices ##
delete devices device <hco-controller>
commit
```

2. Stop NSO.

```
sudo /etc/init.d/ncs stop
```

3. Remove all packages and restart NSO.

```
sudo rm -rf /var/opt/ncs/packages/ncs-<version>-nokia-nsp_rc-
<version>.tar.gz
sudo rm -rf /var/opt/ncs/packages/ncs-<version>-cisco-nsp-fp-
<version>.tar.gz
```

```
sudo NCS_RELOAD_PACKAGES=force /etc/init.d/ncs start
```

CHCO FP is now uninstalled.