Integrate Cisco NSO

This chapter contains the following topics:

NSO Integration Workflow

This section explains the steps in integrating Cisco NSO with Crosswork Network Controller.

1. Install the compatible version of Cisco NSO

Ensure that you have installed the compatible version of Cisco NSO:

- If you are a VMware user, follow the instructions in NSO documentation.
- If you are a AWS EC2 user, follow the instructions in Install Cisco NSO on Amazon EC2.

Additionally, for Cisco NSO LSA setup, see (Optional) Set up Cisco NSO Layered Service Architecture, on page 12.

Table 1: Cisco NSO - compatible versions

Software/Driver	Version
Cisco Network Services Orchestrator (Cisco NSO)	6.1
Cisco Network Element Driver (NED) **Note** Cisco NEDs must be installed only for the device types and versions that you are managing. For example, if you are using NETCONF, then you must install the NED that corresponds to your IOS XR version(s). Similarly, Cisco IOS CLI NED must be installed if you have IOS devices in the network.	**Cisco IOS XR:** • CLI: 7.46.3 • NETCONF: 7.3.2, 7.315, 7.4.2, 7.5.2, 7.6.2, 7.7.2, 7.8, 7.9 **Cisco IOS:** • CLI: 6.86.6

2. Install the mandatory NSO core function packs

Depending on the Cisco Crosswork application or solution that you are using, there are mandatory Core Function Packs (CFPs) that must be installed on Cisco NSO to make the products compatible.

The NSO core function packs are bundled in cisco.com as follows:

Table 2: NSO Core Function Packs

Package Name	Contents
Cisco Crosswork Network Controller Essential Function Pack **File name:** *cw-cnc-essential-fp-5.0.0-101-release-230503.tar.gz*	• *Cisco NSO Transport SDN Function Pack Bundle* • *Cisco NSO DLM Service Pack* • *Cisco NSO Telemetry Traffic Collector Function Pack*
Cisco Crosswork Change Automation Function Pack **File name:** *cw-ca-fp-5.0.0-5-release-230511.tar.gz*	• *Cisco Crosswork Change Automation NSO Function Pack*

You can install the CFPs using either of the following methods:

- Install Cisco NSO Function Packs using Ansible playbook, on page 2 (Recommended)
- Install Cisco NSO Function Packs manually , on page 9

Note The Cisco Crosswork Network Controller Function Pack SDK Application (*cw-na-platform-5.0.0-signed-tsdn-sdk.tar.gz*) is also available for download on cisco.com. The SDK provides tools and source-code examples you can use to develop, build, package and deploy the TSDN function pack on Crosswork Network Controller.

3. Add the NSO provider and verify connectivity

Follow the instructions in Add Cisco NSO Providers, on page 9.

Install Cisco NSO Function Packs using Ansible playbook

This section explains how to install the Cisco NSO Core Function Packs (CFPs) using Ansible playbooks.

The Ansible playbook installs the NSO CFPs on existing NSO VM instance(s), running compatible NSO version. The playbook is executed from an Ansible controller with the NSO instance(s) as managed node(s). This feature supports the following NSO deployment configurations:

- LSA, on page 4
- LSA HA (High Availability), on page 5
- Standalone, on page 7
- Standalone HA (High Availability), on page 8

See each deployment configuration for information on the required paramaters and the scripts for installation and uninstallation.

To install or uninstall a CFP, perform the following:

Before you begin

Assumptions:

- Supports only the clean installation of CFPs.
- Upgrade is not supported.
- NSO is already installed along with HA configuration (per deployment requirement).
- The Ansible script installs all CFP packages (Transport SDN (TSDN), Change Automation (CA), Device Lifecycle Management (DLM), and Telemetry Traffic Controller (TM-TC) and bootstrapping.
- The LSA configuration requires 3 VMs (1 CFS node and 2 RFS nodes).
- NSO is installed in system-install mode (local install is not supported), in standard locations:
  - ncsdir: `/opt/ncs/current`
  - confdir: `/etc/ncs`
  - rundir: `/var/opt/ncs`
  - logdir: `/var/log/ncs`
- As upgrade is not supported, the installation will fail with the presence of the CFP package (for example, `cisco-tsdn-core-fp-common` package) which indicates that the CFP is already installed. This mechanism prevents accidentally installing packages on a working setup.
- If an installation attempt fails or you want to reinstall the CFP, run the uninstallation script first to remove (unlink) old packages.

Prerequisites:

- The latest ansible and ansible-playbook is installed on the host designated as the Ansible controller.
- The Java and Python versions (OpenJDK 11, python3) required for the CFP are already installed in the NSO VM.
- In case of HA deployment, the Cisco Tail-f HCC (Tail-f High Availability Cluster Communications) package must be already installed, configured, and operational prior to executing the CFP installation.

Caveats:

1. If `ssh`, `netconf-north-bound`, or `webui transport` have previously been enabled, running the install will not add the `dual-stack config` and it will need to be manually enabled. The following config is used to add IPv6 listener with the appropriate port:

```
<extra-listen>
      <ip>::</ip>
      <port>2024</port>
    </extra-listen>
```

2. Before initiating the uninstallation, you must remove all services and devices added in the CDB; otherwise, NSO will attempt the upgrade process which causes uninstallation failure.

3. Do not use an NSO instance as Ansible controller to install CFPs on itself. This deployment configuration is not supported.

Step 1 Edit the `host` and `vars.yml` files with the relevant parameters to configure NSO.

Step 2 To install the CFP, run the installation command (see each deployment configuration for details).

Example:

```
ansible-playbook -v -i hosts tsdn-lsa-ha-install.yml
```

The CFP files are copied to the install directory (`/opt/ncs/packages/`) and symbolic links are created in the runtime directory (`/var/opt/ncs/packages/`). NSO is then restarted to apply the package.

Step 3 To uninstall a CFP, run the uninstallation command (see each deployment configuration for details).

Example:

```
ansible-playbook -v -i hosts tsdn-lsa-ha-uninstall.yml
```

The symbolic links are removed in runtime directory and NSO is restarted without the CFP package.

What to do next

Return to the installation workflow:

- VMware: Install Cisco Crosswork Network Controller on VMware vCenter
- AWS EC2: Install Cisco Crosswork Network Controller on AWS EC2

LSA

This playbook installs the CFP packages and configures LSA cluster as per the node roles described in the `vars.yml` file.

Dir: lsa

Installation: `ansible-playbook -v -i hosts tsdn-lsa-install.yml`

Uninstallation: `ansible-playbook -v -i hosts tsdn-lsa-uninstall.yml`

Required Parameters:

File: `lsa/vars.yml`

Table 3: Required parameters for LSA deployment configuration

Parameter	Description
`ansible_user`	SSH username
`ansible_ssh_pass`	SSH password
`ansible_sudo_pass`	sudo password

Parameter	Description
nbi_port	NSO north bound interface port (Example: 8888)
restconf_port	Restconf interface port (Example: 2022)
lsa_ned_id	NSO Netconf NED ID (Example: cisco-nso-nc-6.1:cisco-nso-nc-6.1)
image_location	CFP package location on Ansible server, Crosswork (Example: /tmp/image)
tsdn_image	TSDN image name (Example: nso-6.1_230124-tsdn-5.0.0-M6)
ca_image	CA image name (Example: cw-na-fp-ca-5.0.0-nso-6.1)
dlm_image	DLM image name (Example: cw-na-dlm-fp-5.0.0-nso-6.1-eng)
tmtc_image	TM-TC image name (Example: cw-na-fp-tmtc-5.0.0-333-nso-6.1)
tmtc_internal	TM-TC internal directory name (Example: TM-TC-5.0.0-333. You may need to untar to get this)
cli_ned_version	IOS XR NED version required by TM-TC (Example: 7.45)
rfs_nodes	- name: rfs-1: ip: <RFS 1 IP address> - name: rfs-2: ip: <RFS 2 IP address> - name: rfs-x: ip: <RFS x IP address>

File: `lsa/hosts`

```
[all]

[cfs_node]
10.0.0.2

[rfs_node]
10.0.0.3
10.0.0.4
10.0.0.x
```

After you prepare the `host` and `vars.yml` files, follow the instructions in Install Cisco NSO Function Packs using Ansible playbook, on page 2 to complete the CFP installation.

LSA HA (High Availability)

This playbook installs the CFP packages and configures LSA cluster as per the node roles described in the `vars.yml` file.

After you prepare the `host` and `vars.yml` files, follow the instructions in Install Cisco NSO Function Packs using Ansible playbook, on page 2.

Dir: lsa-ha

Installation: `ansible-playbook -v -i hosts lsa-ha-install.yml`

Uninstallation: `ansible-playbook -v -i hosts lsa-ha-uninstall.yml`

Required Parameters:

File: `lsa-ha/vars.yml`

Table 4: Required parameters for LSA HA deployment configuration

Parameter	Description
`ansible_user`	SSH username
`ansible_ssh_pass`	SSH password
`ansible_sudo_pass`	sudo password
`nbi_port`	NSO north bound interface port (Example: 8888)
`restconf_port`	Restconf interface port (Example: 2022)
`lsa_ned_id`	NSO Netconf NED ID (Example: cisco-nso-nc-6.1:cisco-nso-nc-6.1)
`image_location`	CFP package location on Ansible server, Crosswork (Example: /tmp/image)
`tsdn_image`	TSDN image name (Example: nso-6.1_230124-tsdn-5.0.0-M6)
`ca_image`	CA image name (Example: cw-na-fp-ca-5.0.0-nso-6.1)
`dlm_image`	DLM image name (Example: cw-na-dlm-fp-5.0.0-nso-6.1-eng)
`tmtc_image`	TM-TC image name (Example: cw-na-fp-tmtc-5.0.0-333-nso-6.1)
`tmtc_internal`	TM-TC internal directory name (Example: TM-TC-5.0.0-333. You may need to untar to get this)
`cli_ned_version`	IOS XR NED version required by TM-TC (Example: 7.45)

`rfs_nodes`	`- name: rfs-1:`
	`  ip: <RFS 1 IP address>`
	`- name: rfs-2:`
	`  ip: <RFS 2 IP address>`
	`- name: rfs-x:`
	`  ip: <RFS x IP address>`

File: `lsa-ha/hosts`

```
[all]

[cfs_primary]
10.0.0.2

[cfs_secondary]
10.0.0.3

[rfs1_primary]
10.0.0.4

[rfs1_secondary]
```

```
10.0.0.5

[rfs2_primary]
10.0.0.7

[rfs2_secondary]
10.0.0.8

[rfsx_primary]
10.0.0.x1

[rfsx_secondary]
10.0.0.x2
```

After you prepare the `host` and `vars.yml` files, follow the instructions in Install Cisco NSO Function Packs using Ansible playbook, on page 2 to complete the CFP installation.

Standalone

This playbook installs the CFP packages to a standalone NSO node.

Dir: standalone

Installation: `ansible-playbook -v -i hosts standalone-install.yml`

Uninstallation: `ansible-playbook -v -i hosts standalone-uninstall.yml`

Required Parameters:

File: `standalone/vars.yml`

Table 5: Required parameters for standalone deployment configuration

Parameter	Description
`ansible_user`	SSH username
`ansible_ssh_pass`	SSH password
`ansible_sudo_pass`	sudo password
`nbi_port`	NSO north bound interface port (Example: 8888)
`image_location`	CFP package location on Ansible server, Crosswork (Example: /tmp/image)
`tsdn_image`	TSDN image name (Example: nso-6.1_230124-tsdn-5.0.0-M6)
`ca_image`	CA image name (Example: cw-na-fp-ca-5.0.0-nso-6.1)
`dlm_image`	DLM image name (Example: cw-na-dlm-fp-5.0.0-nso-6.1-eng)
`tmtc_image`	TM-TC image name (Example: cw-na-fp-tmtc-5.0.0-333-nso-6.1)
`tmtc_internal`	TM-TC internal directory name (Example: TM-TC-5.0.0-333. You may need to untar to get this)

Parameter	Description
cli_ned_version	IOS XR NED version required by TM-TC (Example: 7.45)

File: `standalone/hosts`

```
[all]
10.0.0.2
```

After you prepare the `hosts` and `vars.yml` files, follow the instructions in Install Cisco NSO Function Packs using Ansible playbook, on page 2 to complete the CFP installation.

Standalone HA (High Availability)

This playbook installs CFP packages to a NSO node in HA configuration as described in the `vars.yml` file.

In case of HA deployment, the Cisco Tail-f HCC (Tail-f High Availability Cluster Communications) package must be already installed, configured, and operational prior to executing the CFP installation.

Dir: ha

Installation: `ansible-playbook -v -i hosts ha-install.yml`

Uninstallation: `ansible-playbook -v -i hosts ha-uninstall.yml`

Required Parameters:

File: `ha/vars.yml`

Table 6: Required parameters for standalone HA deployment configuration

Parameter	Description
ansible_user	SSH username
ansible_ssh_pass	SSH password
ansible_sudo_pass	sudo password
nbi_port	NSO north bound interface port (Example: 8888)
image_location	CFP package location on Ansible server, Crosswork (Example: /tmp/image)
tsdn_image	TSDN image name (Example: nso-6.1_230124-tsdn-5.0.0-M6)
ca_image	CA image name (Example: cw-na-fp-ca-5.0.0-nso-6.1)
dlm_image	DLM image name (Example: cw-na-dlm-fp-5.0.0-nso-6.1-eng)
tmtc_image	TM-TC image name (Example: cw-na-fp-tmtc-5.0.0-333-nso-6.1)
tmtc_internal	TM-TC internal directory name (Example: TM-TC-5.0.0-333. You may need to untar to get this)
cli_ned_version	IOS XR NED version required by TM-TC (Example: 7.45)

Parameter	Description
`vip_ip`	Virtual IP address
`primary_node_ip`	Primary node IP address
`secondary_node_ip`	Secondary node IP address

File: `ha/hosts`

```
[all]

[primary_node]
  10.0.0.2

[secondary_node]
  10.0.0.3
```

After you prepare the `hosts` and `vars.yml` files, follow the instructions in Install Cisco NSO Function Packs using Ansible playbook, on page 2 to complete the CFP installation.

Install Cisco NSO Function Packs manually

If you need to install individual function packs manually, follow the relevant procedure from the below table:

Table 7: List of mandatory Function Packs

Crosswork Product	Required Function Pack documentation
Crosswork Network Controller Essentials OR Crosswork Network Controller Advantage	• *Cisco NSO Transport SDN Function Pack Bundle 5.0.0 User Guide* • *Cisco NSO Transport SDN Function Pack Bundle 5.0.0 Installation Guide* • *Cisco Network Services Orchestrator DLM Service Pack 5.0.0 Installation Guide* • *Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 5.0.0 Installation Guide* • *Cisco Crosswork Change Automation NSO Function Pack 5.0.0 Installation Guide*
Crosswork Optimization Engine (Standalone)	• *Cisco Network Services Orchestrator DLM Service Pack 5.0.0 Installation Guide* • *Cisco Crosswork NSO Telemetry Traffic Collector Function Pack 5.0.0 Installation Guide*

Add Cisco NSO Providers

The Cisco Network Services Orchestrator (Cisco NSO) provider supplies the following functionality:

- Network services and device configuration services to Cisco Crosswork applications.
- Device management and configuration maintenance services.

Note Crosswork supports Cisco NSO Layered Service Architecture (LSA) deployment. The LSA deployment is constructed from multiple NSO providers, that function as the customer-facing service (CFS) NSO containing all the services, and the resource-facing service (RFS), which contains the devices. Crosswork automatically identifies the NSO provider as CFS or RFS. Only one CFS is allowed. On the **Manager Provider Access** page, the **Type** column identifies the NSO provider as CFS.

Note The Cisco NSO sample function packs are provided as a starting point for VPN service provisioning functionality in Cisco Crosswork Network Controller. While the samples can be used "as is" in some limited network configurations, they are intended to demonstrate the extensible design of Cisco Crosswork Network Controller. Answers to common questions can be found on Cisco Devnet and Cisco Customer Experience representatives can provide answers to general questions about the samples. Support for customization of the samples for your specific use cases can be arranged through your Cisco account team.

Before you begin

You will need to:

- Create a credential profile for the Cisco NSO provider.
- Know the name you want to assign to the Cisco NSO provider.
- Know the Cisco NSO NED device models and driver versions used in your topology.

Note You can find the Cisco NSO version using the `version` command, as shown in the below example:

```
admin@ncs# show ncs-state version
ncs-state version 6.1
```

- Know the Cisco NSO server IP address and hostname. When NSO is configured with HA, the IP address would be management VIP address.
- Confirm Cisco NSO device configurations.

Follow the steps below to add a Cisco NSO provider through the UI. Note that you can import several providers at the same time by preparing a CSV file with the details of all the providers and importing it into Crosswork.

Step 1 From the main menu, choose **Administration** > **Manage Provider Access**.

Step 2 Click +.

Step 3 Enter the following values for the Cisco NSO provider fields:

a) Required fields:

- **Provider Name**: Enter a name for the provider.
- **Credential Profile**: Select the previously created Cisco NSO credential profile.
- **Family**: Select **`NSO`**.
- Under Connection Type(s), **Protocol**: Select the protocol that Cisco Crosswork applications will use to connect to the provider. **`HTTPS`** is usually preferred.
- **IP Address/Subnet Mask**: Enter the IP address and subnet mask of the Cisco NSO server.

  Important When you modify or update the NSO provider IP address or FQDN, you need to detach devices from corresponding virtual data gateway, and reattach them. If you fail to do this, the provider changes will not be reflected in MDT collection jobs.

- **Port**: For HTTPS, enter the port that corresponds with what is configured on the NSO VM in etc/ncs/ncs.conf to access NSO using HTTPS. NSO uses 8888 as default port.
- **Model**: Select the model (**Cisco-IOS-XR**, **Cisco-NX-OS**, or **Cisco-IOS-XE**) from the drop-down list and enter its associated NED driver version. Add a model for each type of device that will be used in the topology. If you have more than one, add another supported model.
- **Version**: Enter the NED software version installed for the device model in NSO.

b) Optional values:

- **Timeout**: The amount of time (in seconds) to wait before timing out the connection to the Cisco NSO server. The default is 30 seconds.

Step 4 Under Provider Properties, enter a **Property Key** of **`forward`** and a **Property Value** of **`true`**. This property is necessary when using the Cisco Crosswork Network Controller solution to allow provisioning operations within the UI and to enable the northbound interface to NSO via the Crosswork API gateway.

Note Cisco Crosswork provides the option to cross launch the NSO application from the Crosswork UI (this feature is not available for user roles with read-only permissions). To enable the cross launch feature, add Cisco NSO as a provider with one of the following settings:

- The **Property Key** **`nso_crosslaunch_url`** has a valid URL entered in the **Property Key** field.
- Protocol is **`HTTP`** or **`HTTPS`**, and the provider is reachable.

If any of the above settings are present, the cross launch icon ( ) is displayed in the **Provider Name** column. Alternately, you can cross launch the NSO application using the launch icon located at the top right corner of the window.

Step 5 When you have completed entries in all of the required fields, click **Save** to add Cisco NSO as a provider.

Step 6 In the Providers window, select the NSO provider you created and click **Actions** > **Edit Policy Details**.

The **Edit Policy Details** window for the selected NSO provider is displayed.

Step 7 Edit the configuration fields to match the requirements of your environment. Click **Save** to save your changes.

What to do next

Return to the installation workflow:

- VMware: Install Cisco Crosswork Network Controller on VMware vCenter
- AWS EC2: Install Cisco Crosswork Network Controller on AWS EC2

(Optional) Set up Cisco NSO Layered Service Architecture

This section is applicable only when you have opted for Cisco NSO Layered Service Architecture (LSA) deployment.

Cisco NSO LSA allows you to add arbitrarily many device nodes for improved memory and provisioning throughput. Large service providers or enterprises use Cisco NSO to manage services for millions of subscribers or users, ranging over several hundred thousand managed devices. To achieve this, you can design your services in the layered fashion called LSA.

To position Cisco Crosswork Network Controller for large customers, the solution is made compatible with the existing Cisco NSO LSA architecture.

Follow these steps to decide when to use Cisco NSO LSA:

1. Check if the deployment is stand-alone or Cisco NSO LSA.
2. If the deployment is stand-alone, check the maximum memory that may be utilised. If the maximum memory that may be utilised is more than the current memory state, Cisco NSO LSA needs to be deployed.

Note Migration from stand-alone deployment to Cisco NSO LSA deployment is not currently supported.

To get a detailed information on Cisco NSO LSA and to set up Cisco NSO LSA, see NSO Layered Service Architecture.