NSO Subscriber Microservices Infrastructure Core Function Pack

Feature Summary and Revision History

Summary Data

Table 1: Summary Data

Applicable Product(s) or Functional Area	cnBNG
Applicable Platform(s)	SMI
Feature Default Setting	Disabled - Configuration Required
Related Changes in this Release	Not Applicable
Related Documentation	Not Applicable

Revision History

Table 2: Revision History

Revision Details	Release
First introduced.	2024.04.0

Feature Description

The NSO Subscriber Microservices Infrastructure Core Function Pack (NSO SMI CFP) leverages the Network Service Orchestrator (NSO) to automate the deployment and configuration of functions by integrating with the Subscriber Microservices Infrastructure (SMI). This feature is essential for efficiently managing and orchestrating microservices-based applications, particularly in cloud-native environments.

NSO SMI CFP uses NSO to streamline the deployment of clusters and functions via the SMI Cluster Manager. This core function pack automates the setup of Kubernetes (K8s) clusters, enabling the deployment of Containerized Network Functions (CNFs) and other necessary microservices. It is designed to operate on Cisco UCS® bare metal infrastructure and integrates with the Cisco Container Platform for cloud management.

For detailed information about NSO, see NSO User Guide.

Key Components:

- **Cluster Manager (Cisco Unified Communications Manager)**: Manages the creation and deployment of K8s clusters.
- **Ops-Center**: Provides operational support.
- **Common Execution Environment (CEE)**: Standardized environment for running microservices.
- **Common Data Layer (CDL)**: Centralized data management layer.

Benefits of NSO SMI CFP

These are the benefits of using NSO SMI CFP:

- **Automated Deployment**: Simplifies the setup and configuration of clusters and microservices.
- **Scalability**: Supports deployment across multiple clusters, tailored to customer requirements.
- **Efficiency**: Reduces delays and rework during configuration, ensuring faster time-to-market.
- **Integrated Management**: Provides a unified interface for managing both infrastructure and applications.

Supported Scenarios

NSO SMI CFP is applicable in various scenarios, particularly where there is a need for automated and scalable deployment of microservices in cloud-native environments. This includes:

- **Enterprise Data Centers**: For large-scale deployment and management of microservices.
- **Service Providers**: To dynamically adopt orchestration solutions with changes in service portfolio.
- **Cloud Environments**: Leveraging Kubernetes clusters to manage containerized network functions.

Prerequisites for NSO SMI CFP

These are the prerequisites for using NSO SMI CFP:

1. **NSO Minimum Version**: 6.1.11
2. **Python Version**: Python 3.8 or above
3. **SMI Inception/Deployer Minimum Version**: 2024.04.1
4. **Dependent NEDs**:
   - ncs-6.1.11.2-cisco-smi-nc-2024.04.1
   - ncs-6.1.11.2-cisco-cee-nc-2024.04.1
   - ncs-6.1.11.2-cisco-bng-nc-1.1

Initial Configuration

To begin using NSO SMI CFP, you must add the SMI Cluster Manager as a device in the NSO device tree. This allows NSO to instruct the SMI Cluster Manager to create a cluster and then onboard the cluster into the NSO device tree.

Add the SMI Cluster Manager as a device to NSO

Procedure

Step 1 Log in to NSO.

Example:

```
<nacm xmlns="urn:ietf:params:xml:ns:yang:ietf-netconf-acm">
    <exec-default>permit</exec-default>
    <groups>
        <group>
            <name>ncsadmin</name>
            <user-name>admin</user-name>
        </group>
    </groups>
</nacm>
<smi xmlns="http://cisco.com/ns/nso/cfp/cisco-smi">
    <settings>
        <deployment xmlns="http://cisco.com/ns/nso/cfp/cisco-smi-deployment">
            <local-user>admin</local-user>
        </deployment>
```

```
    </settings>
</smi>
```

Step 2 Configure the global settings on NSO. Set the **<out-of-sync-commit-behaviour>** parameter to accept so that NSO does not track any transactions on the device from multiple users.

Example:

```
<config xmlns="http://tail-f.com/ns/config/1.0">
    <devices xmlns="http://tail-f.com/ns/ncs">
        <global-settings>
            <trace>pretty</trace>
            <out-of-sync-commit-behaviour>accept</out-of-sync-commit-behaviour>
            <trace-dir>/var/log/ncs</trace-dir>
        </global-settings>
    </devices>
</config>
</config>
```

Step 3 Configure the device authgroup.

Example:

```
<config xmlns="http://tail-f.com/ns/config/1.0">
    <devices xmlns="http://tail-f.com/ns/ncs">
        <authgroups>
            <group>
                <name>smi-auth</name>
                <default-map>
                    <remote-name>admin</remote-name>
                    <remote-password>xyz</remote-password>
                </default-map>
            </group>
        </authgroups>
    </devices>
</config>
```

Step 4 Add the SMI Cluster Manager to the NSO device tree.

Example:

```
<config xmlns="http://tail-f.com/ns/config/1.0">
    <devices xmlns="http://tail-f.com/ns/ncs">
        <device>
            <name>smi</name>
            <address>5.5.5.5</address>
            <port>830</port>
            <authgroup>smi-auth</authgroup>
            <device-type>
                <netconf>
                    <ned-id xmlns:cisco-smi-nc-1.1="http://tail-f.com/ns/ned-id/cisco-smi-nc-1.1">
                        cisco-smi-nc-1.1:cisco-smi-nc-1.1
                    </ned-id>
                </netconf>
            </device-type>
            <trace>pretty</trace>
            <state>
                <admin-state>unlocked</admin-state>
            </state>
        </device>
    </devices>
</config>
```

Step 5 Perform SMI Device Connect and sync.

Example:

```
admin@ncs# devices fetch-ssh-host-keys
fetch-result {
device smi
result updated
fingerprint {
algorithm ssh-rsa
value e6:9d:6d:f8:bc:50:46:9a:00:c0:23:1e:bd:5e:c4:9a
}
admin@ncs# devices device smi connect
result true
admin@ncs# devices device smi sync-from
result true
```

Step 6 Set up notification subscriptions.

Example:

```
<config xmlns="http://tail-f.com/ns/config/1.0">
    <devices xmlns="http://tail-f.com/ns/ncs">
        <device>
            <name>cm-1</name>
            <netconf-notifications>
                <subscription>
                    <name>download-status</name>
                    <stream>download-status</stream>
                    <local-user>admin</local-user>
                </subscription>
                <subscription>
                    <name>node-state</name>
                    <stream>node-state</stream>
                    <local-user>admin</local-user>
                </subscription>
                <subscription>
                    <name>node-status</name>
                    <stream>node-status</stream>
                    <local-user>admin</local-user>
                </subscription>
                <subscription>
                    <name>sync-state</name>
                    <stream>sync-state</stream>
                    <local-user>admin</local-user>
                </subscription>
                <subscription>
                    <name>sync-status</name>
                    <stream>sync-status</stream>
                    <local-user>admin</local-user>
                </subscription>
            </netconf-notifications>
        </device>
    </devices>
</config>
```

Deployment Services

Deployment services help you effectively deploy CNDP clusters by reducing delays, rework, and other problems during configuration. These services use the SMI Cluster Manager to set up the infrastructure on the nodes defined in the cluster.

Deploying Clusters

Clusters are the resources that applications need, and they include the worker nodes that run the applications. You can deploy multiple clusters based on your requirements.

NSO communicates with the SMI deployer, instructing it to create a cluster and then onboard the cluster into the NSO device tree.

Deploy the Kubernetes Cluster

The Kubernetes (K8s) cluster is used to install a new Cluster Manager or to install CNF functions services. You can deploy a cluster, such as a control-plane node, using the SMI Cluster Manager.

Note The valid K8s cluster configurations are either an All-in-One configuration (a single control-plane node) or a cluster with three control-plane nodes, with or without worker nodes (zero to N worker nodes).

Procedure

Step 1 The following is a sample payload to deploy a K8s cluster with a single control-plane node.

Example:

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <smi xmlns="http://cisco.com/ns/nso/cfp/cisco-smi">
    <deployment xmlns="http://cisco.com/ns/nso/cfp/cisco-smi-deployment">
      <name>bng-cfp-deployment</name>
      <local-user>admin</local-user>
      <cluster-manager>
        <manager-device>smi-cm-109</manager-device>
      </cluster-manager>
      <clusters>
        <cluster>
          <name>bng-cfp-cluster-53</name>
          <type>k8s</type>
          <environment>ucs-server</environment>
          <ipv6-mode>dual-stack</ipv6-mode>
          <bind-ip-address>10.81.103.86</bind-ip-address>
          <bind-ip-address-internal>203.203.203.101</bind-ip-address-internal>
          <bind-ipv6-address>2001:420:27c1:903::86</bind-ipv6-address>
          <bind-ipv6-address-internal>2002:4888:203:203::203:101</bind-ipv6-address-internal>
          <istio>true</istio>
          <master-vip>203.203.203.101</master-vip>
          <master-vip-cidr>24</master-vip-cidr>
          <master-vip-ipv6>2002:4888:203:203::203:101</master-vip-ipv6>
          <master-vip-interface>bd0.k8s.303</master-vip-interface>
          <additional-master-vip>10.81.103.86</additional-master-vip>
          <additional-master-vip-ipv6>2001:420:27c1:903::86</additional-master-vip-ipv6>
          <additional-master-vip-interface>bd0.mgmt.3103</additional-master-vip-interface>
          <virtual-ip-vrrp-router-id>60</virtual-ip-vrrp-router-id>
          <pod-subnet>192.203.0.0/16</pod-subnet>
          <pod-subnet-ipv6>2002:4888:192:203::/96</pod-subnet-ipv6>
          <node-pod-subnet-ipv6-mask>112</node-pod-subnet-ipv6-mask>
          <allow-insecure-registry>true</allow-insecure-registry>
          <restrict-logging>false</restrict-logging>
          <enable-network-policy>true</enable-network-policy>
```

```
<enable-ssh-firewall-rules>false</enable-ssh-firewall-rules>
<tuned>true</tuned>
<ntp-address>2001:420:27c1:903::109</ntp-address>
<initial-boot>
  <default-user>cloud-user</default-user>
  <default-user-password>Starent@123</default-user-password>
  <netplan>
    <ethernet>
      <device-id>eno1</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
    </ethernet>
    <ethernet>
      <device-id>eno2</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
    </ethernet>
    <ethernet>
      <device-id>eno5</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
    </ethernet>
    <ethernet>
      <device-id>eno6</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
    </ethernet>
    <ethernet>
      <device-id>enp216s0f0</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
    </ethernet>
    <ethernet>
      <device-id>enp216s0f1</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
    </ethernet>
    <ethernet>
      <device-id>enp94s0f0</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
    </ethernet>
    <ethernet>
      <device-id>enp94s0f1</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
    </ethernet>
    <bond>
      <device-id>bd0</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
      <optional>true</optional>
      <interface>eno5</interface>
      <interface>eno6</interface>
      <parameters>
        <mode>active-backup</mode>
        <mii-monitor-interval>100</mii-monitor-interval>
        <fail-over-mac-policy>active</fail-over-mac-policy>
      </parameters>
    </bond>
    <bond>
      <device-id>bd1</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
```

```
      <optional>true</optional>
      <interface>enp216s0f1</interface>
      <interface>enp94s0f0</interface>
      <parameters>
        <mode>active-backup</mode>
        <mii-monitor-interval>100</mii-monitor-interval>
        <fail-over-mac-policy>active</fail-over-mac-policy>
      </parameters>
    </bond>
    <bond>
      <device-id>bd0</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
      <optional>true</optional>
      <interface>enp216s0f0</interface>
      <interface>enp94s0f1</interface>
      <parameters>
        <mode>active-backup</mode>
        <mii-monitor-interval>100</mii-monitor-interval>
        <fail-over-mac-policy>active</fail-over-mac-policy>
      </parameters>
    </bond>
    <vlan>
      <device-id>bd0.k8s.303</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
      <id>303</id>
      <link>bd0</link>
    </vlan>
    <vlan>
      <device-id>bd0.mgmt.3103</device-id>
      <dhcp4>false</dhcp4>
      <dhcp6>false</dhcp6>
      <id>3103</id>
      <link>bd0</link>
      <nameservers>
        <search>cisco.com mitg-bxb300.cisco.com</search>
        <address>2001:420:200:1::a</address>
        <address>2001:420:210d::a</address>
      </nameservers>
    </vlan>
  </netplan>
</initial-boot>
<cimc>
  <user>admin</user>
  <password>Starent@123</password>
    <ntp-address>2001:420:27c1:903::109</ntp-address>
    <storage-adaptor>
      <create-virtual-drive>true</create-virtual-drive>
    </storage-adaptor>
    <bios>
      <configured-boot-mode>Uefi</configured-boot-mode>
      <uefi-secure-boot>yes</uefi-secure-boot>
    </bios>
</cimc>
<node>
  <name>server-1</name>
  <host-profile>
    <repository>bng-ht-sysctl-enable</repository>
  </host-profile>
  <type>control-plane</type>
  <ssh-ip>203.203.203.11</ssh-ip>
  <ssh-ipv6>2002:4888:203:203::203:11</ssh-ipv6>
  <node-ip>203.203.203.11</node-ip>
```

```
<node-ipv6>2002:4888:203:203::203:11</node-ipv6>
<node-label>
  <key>smi.cisco.com/node-type</key>
  <value>oam</value>
</node-label>
<node-label>
  <key>smi.cisco.com/proto-type</key>
  <value>protocol</value>
</node-label>
<node-label>
  <key>comp-type</key>
  <value>mcollector-ssd</value>
</node-label>
<cimc>
  <ip-address>2001:420:27c1:903::53</ip-address>
</cimc>
<initial-boot>
  <netplan>
    <vlan>
      <device-id>bd0.k8s.303</device-id>
      <address>203.203.203.11/24</address>
      <address>2002:4888:203:203::203:11/112</address>
    </vlan>
    <vlan>
      <device-id>bd0.mgmt.3103</device-id>
      <address>10.81.103.72/24</address>
      <address>2001:420:27c1:903::72/64</address>
      <gateway4>10.81.103.1</gateway4>
      <gateway6>2001:420:27c1:903::1</gateway6>
    </vlan>
    <vlan>
      <device-id>bd1.n4.319</device-id>
      <address>219.219.219.11/24</address>
      <address>2002:4888:219:219::219:11/112</address>
      <id>319</id>
      <link>bd1</link>
    </vlan>
    <vlan>
      <device-id>bd1.radius.320</device-id>
      <address>220.220.220.11/24</address>
      <address>2002:4888:220:220::220:11/64</address>
      <id>320</id>
      <link>bd1</link>
    </vlan>
  </netplan>
</initial-boot>
<netplan-additions>
  <vlan>
    <device-id>bd1.n4.319</device-id>
    <route>
      <to>101.101.101.0/24</to>
      <via>219.219.219.1</via>
    </route>
    <route>
      <to>192.69.0.0/16</to>
      <via>219.219.219.1</via>
    </route>
    <route>
      <to>2002:4888:101:101::101:0/64</to>
      <via>2002:4888:219:219::219:1</via>
    </route>
    <route>
      <to>2002:4888:192:69::/64</to>
      <via>2002:4888:219:219::219:1</via>
```

```
      </route>
    </vlan>
    <vlan>
      <device-id>bd1.radius.320</device-id>
      <route>
        <to>192.71.0.0/16</to>
        <via>220.220.220.1</via>
      </route>
      <route>
        <to>2002:4888:192:71::100:0/64</to>
        <via>2002:4888:220:220::220:1</via>
      </route>
    </vlan>
  </netplan-additions>
</node>
<node>
  <name>server-2</name>
  <host-profile>
    <repository>bng-ht-enable</repository>
  </host-profile>
  <type>control-plane</type>
  <ssh-ip>203.203.203.12</ssh-ip>
  <ssh-ipv6>2002:4888:203:203::203:12</ssh-ipv6>
  <node-ip>203.203.203.12</node-ip>
  <node-ipv6>2002:4888:203:203::203:12</node-ipv6>
  <node-label>
    <key>smi.cisco.com/node-type</key>
    <value>oam</value>
  </node-label>
  <node-label>
    <key>smi.cisco.com/sess-type</key>
    <value>cdl-node</value>
  </node-label>
  <node-label>
    <key>smi.cisco.com/svc-type</key>
    <value>service</value>
  </node-label>
  <node-label>
    <key>comp-type</key>
    <value>prom-ssd</value>
  </node-label>
  <cimc>
    <ip-address>2001:420:27c1:903::54</ip-address>
  </cimc>
  <initial-boot>
    <netplan>
      <vlan>
        <device-id>bd0.k8s.303</device-id>
        <address>203.203.203.12/24</address>
        <address>2002:4888:203:203::203:12/112</address>
      </vlan>
      <vlan>
        <device-id>bd0.mgmt.3103</device-id>
        <address>10.81.103.73/24</address>
        <address>2001:420:27c1:903::73/64</address>
        <gateway4>10.81.103.1</gateway4>
        <gateway6>2001:420:27c1:903::1</gateway6>
      </vlan>
    </netplan>
  </initial-boot>
</node>
<node>
  <name>server-3</name>
  <host-profile>
```

```
    <repository>bng-ht-enable</repository>
  </host-profile>
  <type>control-plane</type>
  <ssh-ip>203.203.203.13</ssh-ip>
  <ssh-ipv6>2002:4888:203:203::203:13</ssh-ipv6>
  <node-ip>203.203.203.13</node-ip>
  <node-ipv6>2002:4888:203:203::203:13</node-ipv6>
  <node-label>
    <key>smi.cisco.com/node-type</key>
    <value>oam</value>
  </node-label>
  <node-label>
    <key>smi.cisco.com/sess-type</key>
    <value>cdl-node</value>
  </node-label>
  <node-label>
    <key>smi.cisco.com/svc-type</key>
    <value>service</value>
  </node-label>
  <node-label>
    <key>comp-type</key>
    <value>loki-ssd</value>
  </node-label>
  <cimc>
    <ip-address>2001:420:27c1:903::55</ip-address>
  </cimc>
  <initial-boot>
    <netplan>
      <vlan>
        <device-id>bd0.k8s.303</device-id>
        <address>203.203.203.13/24</address>
        <address>2002:4888:203:203::203:13/112</address>
      </vlan>
      <vlan>
        <device-id>bd0.mgmt.3103</device-id>
        <address>10.81.103.74/24</address>
        <address>2001:420:27c1:903::74/64</address>
        <gateway4>10.81.103.1</gateway4>
        <gateway6>2001:420:27c1:903::1</gateway6>
      </vlan>
    </netplan>
  </initial-boot>
</node>
<node>
  <name>server-4</name>
  <host-profile>
    <repository>bng-ht-sysctl-enable</repository>
  </host-profile>
  <type>worker</type>
  <host-profile>
    <repository>bng-ht-enable</repository>
  </host-profile>
  <ssh-ip>203.203.203.14</ssh-ip>
  <ssh-ipv6>2002:4888:203:203::203:14</ssh-ipv6>
  <node-ip>203.203.203.14</node-ip>
  <node-ipv6>2002:4888:203:203::203:14</node-ipv6>
  <node-label>
    <key>smi.cisco.com/proto-type</key>
    <value>protocol</value>
  </node-label>
  <cimc>
    <ip-address>2001:420:27c1:903::56</ip-address>
  </cimc>
  <initial-boot>
```

```
    <netplan>
      <vlan>
        <device-id>bd0.k8s.303</device-id>
        <address>203.203.203.14/24</address>
        <address>2002:4888:203:203::203:14/112</address>
      </vlan>
      <vlan>
        <device-id>bd0.mgmt.3103</device-id>
        <address>10.81.103.75/24</address>
        <address>2001:420:27c1:903::75/64</address>
        <gateway4>10.81.103.1</gateway4>
        <gateway6>2001:420:27c1:903::1</gateway6>
      </vlan>
      <vlan>
        <device-id>bd1.n4.319</device-id>
        <address>219.219.219.12/24</address>
        <address>2002:4888:219:219::219:12/112</address>
        <id>319</id>
        <link>bd1</link>
      </vlan>
      <vlan>
        <device-id>bd1.radius.320</device-id>
        <address>220.220.220.12/24</address>
        <address>2002:4888:220:220::220:12/64</address>
        <id>320</id>
        <link>bd1</link>
      </vlan>
    </netplan>
  </initial-boot>
  <netplan-additions>
    <vlan>
      <device-id>bd1.n4.319</device-id>
      <route>
        <to>101.101.101.0/24</to>
        <via>219.219.219.1</via>
      </route>
      <route>
        <to>192.69.0.0/16</to>
        <via>219.219.219.1</via>
      </route>
      <route>
        <to>2002:4888:101:101::101:0/64</to>
        <via>2002:4888:219:219::219:1</via>
      </route>
      <route>
        <to>2002:4888:192:69::/64</to>
        <via>2002:4888:219:219::219:1</via>
      </route>
    </vlan>
    <vlan>
      <device-id>bd1.radius.320</device-id>
      <route>
        <to>192.71.0.0/16</to>
        <via>220.220.220.1</via>
      </route>
      <route>
        <to>2002:4888:192:71::100:0/64</to>
        <via>2002:4888:220:220::220:1</via>
      </route>
    </vlan>
  </netplan-additions>
</node>
<virtual-ip>
  <name>udpvip</name>
```

```
            <check-ports>28000</check-ports>
            <interface>bd1.n4.319</interface>
            <router-id>222</router-id>
            <check-interface>bd0.k8s.303</check-interface>
            <check-interface>bd1.n4.319</check-interface>
            <check-interface>bd1.radius.320</check-interface>
            <address>
              <address>203.203.203.51</address>
              <device>bd0.k8s.303</device>
              <prefix-length>24</prefix-length>
            </address>
            <address>
              <address>219.219.219.51</address>
              <device>bd1.n4.319</device>
              <prefix-length>24</prefix-length>
            </address>
            <address>
              <address>220.220.220.51</address>
              <device>bd1.radius.320</device>
              <prefix-length>24</prefix-length>
            </address>
            <address>
              <address>2002:4888:203:203::203:51</address>
              <device>bd0.k8s.303</device>
              <prefix-length>112</prefix-length>
            </address>
            <address>
              <address>2002:4888:219:219::219:51</address>
              <device>bd1.n4.319</device>
              <prefix-length>64</prefix-length>
            </address>
            <address>
              <address>2002:4888:220:220::220:51</address>
              <device>bd1.radius.320</device>
              <prefix-length>64</prefix-length>
            </address>
            <node>
              <name>server-1</name>
              <priority>100</priority>
            </node>
            <node>
              <name>server-4</name>
              <priority>100</priority>
            </node>
          </virtual-ip>
        </cluster>
      </clusters>
    </deployment>
  </smi>
</config>
```

Step 2 View the SMI deployment plan and verify the deployment status of the K8s cluster.

Example:

```
admin@ncs# show smi deployment-plan bng-cfp-l3-deployment plan | tab
                                                BACK
                    POST ACTION
TYPE           NAME                             TRACK  GOAL  STATE                STATUS   WHEN
               ref  STATUS          MESSAGE
-------------------------------------------------------------------------------------------------
self           self                             false  -     init                 reached
2024-09-30T05:00:47  -    -               -
                                                             ready                reached
```

```
2024-09-30T05:42:15  -    -               -
deployment-bm  bng-cfp-l3-deployment           false  -     init                  reached
2024-09-30T05:00:47  -    -               -
                                                           smid-ns:config-apply  reached
2024-09-30T05:00:47  -    create-reached  -
                                                           ready                 reached
2024-09-30T05:00:47  -    -               -
ucs-cluster    bng-cfp-l3-tb02-151             false  -     init                  reached
2024-09-30T05:00:47  -    -               -
                                                           smid-ns:config-apply  reached
2024-09-30T05:00:47  -    -               -
                                                           ready                 reached
2024-09-30T05:42:15  -    -               -
cluster-node   bng-cfp-l3-tb02-151-s1-r1-svr-1  false  -     init                  reached
2024-09-30T05:00:47  -    -               -
                                                           smid-ns:config-apply  reached
2024-09-30T05:00:47  -    -               -
                                                           ready                 reached
2024-09-30T05:42:15  -    -               -
software       cee-smi-cfp-repo                false  -     init                  reached
2024-09-30T05:01:30  -    -               -
                                                           smid-ns:config-apply  reached
2024-09-30T05:01:30  -    -               -
                                                           ready                 reached
2024-09-30T05:01:30  -    -               -
software       cnbng-smi-cfp-repo              false  -     init                  reached
2024-09-30T05:01:30  -    -               -
                                                           smid-ns:config-apply  reached
2024-09-30T05:01:30  -    -               -
                                                           ready                 reached
2024-09-30T05:01:30  -    -               -
```

Functions Services

The functions services deploy functions on the clusters using the Cluster Manager. These services manage various network functions, allowing you to deploy the following:

- Containerized Network Functions (CNFs)
  - Common Execution Environment (CEE)
  - Broadband Network Gateway Function (BNG)

Deploy a CNF

Containerized Network Functions (CNFs) are managed using Kubernetes-style orchestration, ensuring consistent lifecycle management across all containers.

To deploy CNFs, you need to have the CNF images on your system.

These are the steps to deploy a CNF:

Procedure

Step 1 Log in to NSO and configure the SMI deployment software repository auth to deploy the CNF.

Example:

```
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <smi xmlns="http://cisco.com/ns/nso/cfp/cisco-smi">
    <deployment xmlns="http://cisco.com/ns/nso/cfp/cisco-smi-deployment">
      <name>bare-metal</name>
      <software>
        <repository-auth>
          <name>imgcread</name>
          <user>admin</user>
          <password>admin</password>
        </repository-auth>
      </software>
    </deployment>
  </smi>
</config>
```

Note
If you are using a simple HTTP server, authentication credentials are not required.

Step 2 Add the software repository configuration to NSO and commit the changes to deploy the service. The following is a sample payload:

Example:

```
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <smi xmlns="http://cisco.com/ns/nso/cfp/cisco-smi">
    <deployment xmlns="http://cisco.com/ns/nso/cfp/cisco-smi-deployment">
      <name>bng-cfp-deployment</name>
      <local-user>admin</local-user>
      <cluster-manager>
        <manager-device>smi-cm-109</manager-device>
      </cluster-manager>
      <software>
        <repository>
          <name>cee-smi-cfp-repo</name>
          <type>cnf</type>

<url>https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-group/releases/smi-apps/smi-cee-products/2024.03.1.i12-offline/cee-2024.03.1.i12.tar</url>

          <sha256>5d87baee367bbc9fb8184699d73735873b8b7999f347d59f3d01dd99d55ff91e</sha256>
          <repository-auth>imgcread</repository-auth>
         <ned-id xmlns:id="http://tail-f.com/ns/ned-id/cisco-cee-nc-1.1">id:cisco-cee-nc-1.1</ned-id>

        </repository>
        <repository>
          <name>cnbng-smi-cfp-repo</name>
          <type>cnf</type>

<url>https://engci-maven-master.cisco.com/artifactory/mobile-cnat-charts-release/relenv-builds/2024.03.0/bng/2024.03.0.i46/bng.2024.03.0.i46-offline/bng.2024.03.0.i46.SSA.tgz</url>

          <sha256>152c21e2d6c12393d6d557439c438fffae7cc1c623a8426992766acf5b93afec</sha256>
          <repository-auth>imgcread</repository-auth>
         <ned-id xmlns:id="http://tail-f.com/ns/ned-id/cisco-bng-nc-1.1">id:cisco-bng-nc-1.1</ned-id>

        </repository>
        <repository-auth>
```

```
          <name>imgcread</name>
          <user>madhs</user>
          <password>...</password>
          <accept-self-signed-certificate>true</accept-self-signed-certificate>
          <allow-dev-image>true</allow-dev-image>
        </repository-auth>
      </software>
    </deployment>
  </smi>
</config>
```

Step 3 Configure the functions on the CNF using the deployed SMI Cluster Manager and perform a load merge.

Example:

```
<smi xmlns="http://cisco.com/ns/nso/cfp/cisco-smi">
  <functions xmlns="http://cisco.com/ns/nso/cfp/cisco-smi-functions">
    <function>
      <app-name>cee</app-name>
      <name>cee-smi-cfp-109</name>
      <local-user>admin</local-user>
      <first-boot-username>admin</first-boot-username>
      <first-boot-password>Starent@123</first-boot-password>
      <authentication-group>smi-cm-auth-109</authentication-group>
      <deployer>bng-cfp-deployment</deployer>
      <repository>cee-smi-cfp-repo</repository>
      <managed-cluster>bng-cfp-cluster-53</managed-cluster>
      <netconf-port>2027</netconf-port>
      <ssh-ipv6>2001:420:27c1:903::86</ssh-ipv6>
      <netconf-ipv6>2001:420:27c1:903::86</netconf-ipv6>
      <ssh-port>2028</ssh-port>
      <use-volume-claims>true</use-volume-claims>
      <auto-deploy>true</auto-deploy>
      <single-node>false</single-node>
      <ingress-hostname>cnbng-tb3.nip.io</ingress-hostname>
    </function>
  </functions>
</smi>
```

Step 4 Poll the plan component for each function and view the status of the service. The following example shows how to view the status of the service.

Example:

```
admin@ncs# show smi functions function-plan cee cee-smi-cfp-151 plan | tab
                                    BACK
          POST ACTION
TYPE             NAME               TRACK  GOAL  STATE                  STATUS   WHEN
     ref  STATUS          MESSAGE
-------------------------------------------------------------------------------------------------------------
self             self               false  -     init                   reached  2024-09-30T05:01:28
  -    -               -
                                                 ready                  reached  2024-10-03T02:49:13
  -    -               -
function         cee                false  -     init                   reached  2024-09-30T05:01:28
  -    -               -
                                                 smif-ns:cluster-ready  reached  2024-09-30T05:42:14
  -    create-reached  -
                                                 smif-ns:onboarded      reached  2024-09-30T05:43:03
  -    create-reached  -
                                                 validate               reached  2024-10-03T02:49:13
  -    -               -
                                                 ready                  reached  2024-10-03T02:49:13
  -    -               -
managed-cluster  bng-cfp-l3-tb02-151  false  -     init                   reached  2024-09-30T05:01:28
```

```
-    -               -
                                                    deployed              reached  2024-09-30T05:01:28
-    create-reached  -
                                                    ready                 reached  2024-09-30T05:42:14
-    -               -
```

Upgrade a CNF

Before you begin

- Ensure that you have installed the SMI software using the deployment services.

Procedure

Step 1 Create a repository with the newer version of CNF to upgrade the existing CNF. The following is a sample payload:

Example:

```
<config xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
  <smi xmlns="http://cisco.com/ns/nso/cfp/cisco-smi">
    <deployment xmlns="http://cisco.com/ns/nso/cfp/cisco-smi-deployment">
      <name>bng-cfp-deployment</name>
      <local-user>admin</local-user>
      <cluster-manager>
        <manager-device>smi-cm-109</manager-device>
      </cluster-manager>
      <software>
        <repository>
          <name>cee-smi-cfp-repo-04</name>
          <type>cnf</type>

<url>https://engci-maven-master.cisco.com/artifactory/smi-fuse-internal-group/releases/smi-apps/smi-cee-products/2024.04.1.i12-offline/cee-2024.04.1.i12.tar</url>

          <sha256>6d87baee367bbc9fb8184699d73735873b8b7999f347d59f3d01dd99d55ff91e</sha256>
          <repository-auth>imgcread</repository-auth>
         <ned-id xmlns:id="http://tail-f.com/ns/ned-id/cisco-cee-nc-1.1">id:cisco-cee-nc-1.1</ned-id>

        </repository>
      </software>
    </deployment>
  </smi>
</config>
```

Step 2 Set the SMI function to use the new repository.

Example:

```
<smi xmlns="http://cisco.com/ns/nso/cfp/cisco-smi">
  <functions xmlns="http://cisco.com/ns/nso/cfp/cisco-smi-functions">
    <function>
      <app-name>cee</app-name>
      <name>cee-smi-cfp-109</name>
      <local-user>admin</local-user>
      <first-boot-username>admin</first-boot-username>
      <first-boot-password>Starent@123</first-boot-password>
      <authentication-group>smi-cm-auth-109</authentication-group>
```

```
      <deployer>bng-cfp-deployment</deployer>
      <repository>cee-smi-cfp-repo-04</repository>
      <managed-cluster>bng-cfp-cluster-53</managed-cluster>
      <netconf-port>2027</netconf-port>
      <ssh-ipv6>2001:420:27c1:903::86</ssh-ipv6>
      <netconf-ipv6>2001:420:27c1:903::86</netconf-ipv6>
      <ssh-port>2028</ssh-port>
      <use-volume-claims>true</use-volume-claims>
      <auto-deploy>true</auto-deploy>
      <single-node>false</single-node>
      <ingress-hostname>cnbng-tb3.nip.io</ingress-hostname>
    </function>
  </functions>
</smi>
```

Step 3 [Optional] If the auto-sync functionality is disabled, manually trigger a cluster-sync.

Applications Services

The applications layer sits on top of the function services and provides additional functionality once the function is ready. It is used to apply day-1 configuration to the BNG Ops-Center via NSO device templates. This layer ensures that the necessary configurations are in place for the application to operate effectively from the start.

Apply Day-1 Configuration to BNG Ops-center

Procedure

Step 1 Create a device template with day-1 BNG configuration.

Example:

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <devices xmlns="http://tail-f.com/ns/ncs">
    <template>
      <name>template-bng-ops-109</name>
      <ned-id>
        <id xmlns:id="http://tail-f.com/ns/ned-id/cisco-bng-nc-1.1">id:cisco-bng-nc-1.1</id>
        <config>
          <ipam xmlns="http://cisco.com/cisco-cn-ipam">
            <instance>
              <instance-id>1</instance-id>
...
        </config>
      </ned-id>
    </template>
  </devices>
</config>
```

Step 2 Apply the device-template to bng-ops-center.

Example:

```
<smi xmlns="http://cisco.com/ns/nso/cfp/cisco-smi">
    <applications xmlns="http://cisco.com/ns/nso/cfp/cisco-smi-applications">
      <application>
        <bng>
          <name>bng-smi-cfp-109</name>
          <local-user>admin</local-user>
          <deployment>
            <authentication-group>smi-cm-auth-109</authentication-group>
            <deployer>bng-cfp-deployment</deployer>
            <managed-cluster>bng-cfp-cluster-53</managed-cluster>
            <repository>cnbng-smi-cfp-repo</repository>
            <first-boot-password>Starent@123</first-boot-password>
          </deployment>
          <device-template>
            <name>template-bng-ops-109-02</name>
          </device-template>
        </bng>
      </application>
    </applications>
</smi>
```

Step 3 View the application status.

Example:

```
admin@ncs# show smi applications application-plan bng plan | tab

                                POST
                                 LOG                        BACK
                                ACTION
NAME             FAILED  MESSAGE  ENTRY  TYPE         NAME  TRACK  GOAL  STATE
STATUS   WHEN                ref  STATUS  ID
-------------------------------------------------------------------------------------------
bng-smi-cfp-151  -       -        -      self         self  false  -     init
reached  2024-09-30T05:04:56  -    -
                                                                        ready
reached  2024-09-30T05:43:05  -    -
                                       application  bng   false  -     init
reached  2024-09-30T05:04:56  -    -
                                                                        smia-ns:onboarded
reached  2024-09-30T05:43:03  -    -
                                                                        application-configured
reached  2024-09-30T05:43:03  -    -
                                                                        system-configured
reached  2024-09-30T05:43:05  -    -
                                                                        ready
reached  2024-09-30T05:43:05  -    -
```

Disable the auto-sync Feature

The auto-sync feature is enabled by default to automatically trigger cluster-sync on the deployer. You can choose to disable the auto-sync feature and manually trigger cluster-sync by setting the **sync-disabled** flag to true, either at the global level or at the cluster level (for managed clusters).

When auto-sync is disabled, the SMI deployment plan and the functions plan are updated based on the notifications received.

Procedure

Step 1 At the global level, set the **sync-disabled flag** to true in SMI settings deployment.

Example:

```
ncs_cli -u admin -C
admin@ncs# configure
admin@ncs(config)# load merge cluster-payload-example.xml
admin@ncs(config)# smi deployment settings sync-disabled true
admin@ncs(config)# commit
```

Step 2 At the cluster level, set the **sync-disabled flag** flag to true in the **smi deployment** *depl_name* **clusters** *cluster_name* command.

Example:

```
ncs_cli -u admin -C
admin@ncs# configure
admin@ncs(config)# load merge cluster-payload-example.xml
admin@ncs(config)# smi deployment test clusters cluster c1 sync-disabled
true
admin@ncs(config)# commit
```

In this example, *cluster c1* is deployed under the SMI deployment *test*.

Step 3 Once the cluster is up, view the plan for the deployment, and observe that the clusters are not synced.

Example:

```
admin@ncs# show smi deployment-plan test
smi deployment-plan bng-cfp-l3-deployment
 result smi-device smi-cm-31
 result local-user admin
 result cluster-result bng-cfp-l3-tb02-151
  ha-cluster false
  sync-state state DEPLOYED
  sync-status status DONE
  sync-status event-time 2024-10-03T00:08:53.784+00:00
  node-result s1-r1-svr-1
   drain-status NONE
   node-state state JOINED
   node-state event-time 2024-10-03T00:08:53.785+00:00
   node-state node-sync false
  functions  [ "/smi:smi/smif:functions/function{bng bng-smi-cfp-151}"
"/smi:smi/smif:functions/function{cee cee-smi-cfp-151}" ]
 plan component self self
  back-track false
  state init
   status reached
   when   2024-09-30T05:00:47
  state ready
   status reached
   when   2024-09-30T05:42:15
 plan component deployment-bm bng-cfp-l3-deployment
  back-track false
  state init
   status reached
   when   2024-09-30T05:00:47
  state smid-ns:config-apply
   status             reached
   when               2024-09-30T05:00:47
```

```
  post-action-status create-reached
 state ready
  status reached
  when   2024-09-30T05:00:47
plan component ucs-cluster bng-cfp-l3-tb02-151
 back-track false
 state init
  status reached
  when   2024-09-30T05:00:47
 state smid-ns:config-apply
  status reached
  when   2024-09-30T05:00:47
 state ready
  status reached
  when   2024-09-30T05:42:15
plan component cluster-node bng-cfp-l3-tb02-151-s1-r1-svr-1
 back-track false
 state init
  status reached
  when   2024-09-30T05:00:47
 state smid-ns:config-apply
  status reached
  when   2024-09-30T05:00:47
 state ready
  status reached
  when   2024-09-30T05:42:15
plan component software cee-smi-cfp-repo
 back-track false
 state init
  status reached
  when   2024-09-30T05:01:30
 state smid-ns:config-apply
  status reached
  when   2024-09-30T05:01:30
 state ready
  status reached
  when   2024-09-30T05:01:30
plan component software cnbng-smi-cfp-repo
 back-track false
 state init
  status reached
  when   2024-09-30T05:01:30
 state smid-ns:config-apply
  status reached
  when   2024-09-30T05:01:30
 state ready
  status reached
  when   2024-09-30T05:01:30
```

Trigger the Sync Action

The sync action initiates synchronization on the Cluster Manager and re-deploys the associated functions and clusters. This action also restarts the monitoring services and components accordingly. In managed clusters, NSO triggers a sync-from action once the sync action on the Cluster Manager is complete. If the sync-to flag in NSO is set to true, NSO will also trigger a sync-to action.

To trigger the sync action through the deployment service, use the following command:

```
admin@ncs(config)# smi deployment deployment-name clusters sync [ cluster-name-1
cluster-name-2 ... ]
```

When a sync action is triggered, the plan backtracks and reaches the desired state only after the sync action is complete, and both the functions and the Cluster Manager are reachable.

The sync action supports the following options, which are set to false by default:

- sync-to
- force-vm-redeploy
- force-partition-redeploy
- reset-k8s-nodes
- purge-data-disks

You can use one or all of these options as needed. For example, the following command demonstrates the usage of these options:

```
admin@ncs(config)# smi deployment test clusters sync cluster [ c3 ]
force-partition-redeploy true force-vm-redeploy true purge-data-disks
true reset-k8s-nodes true sync-to true
```

Delete the SMI Deployment

You must first delete the CNF before deleting the SMI deployment. After each deletion, verify that there are no zombie processes.

To delete the SMI deployment, follow these steps:

1. Delete the cnBNG application, if it is installed.

   ```
   admin@ncs(config)# no smi applications application bng bng-1
   ```

2. Delete all applicable functions.

   ```
   admin@ncs(config)# no smi functions function cee cee-test1
   admin@ncs(config)# no smi functions function bng bng-1
   admin@ncs(config)# commit
   ```

3. Delete the software repository associated with the bare-metal deployment.

   ```
   admin@ncs(config)# no smi deployment bare-metal software repository
   admin@ncs(config)# commit
   ```

4. Delete the bare-metal deployment.

   ```
   admin@ncs(config)# no smi deployment bare-metal
   admin@ncs(config)# commit
   ```