

# Getting Your DCNM Network Sites Ready for Nexus Dashboard Insights

---

## Introduction

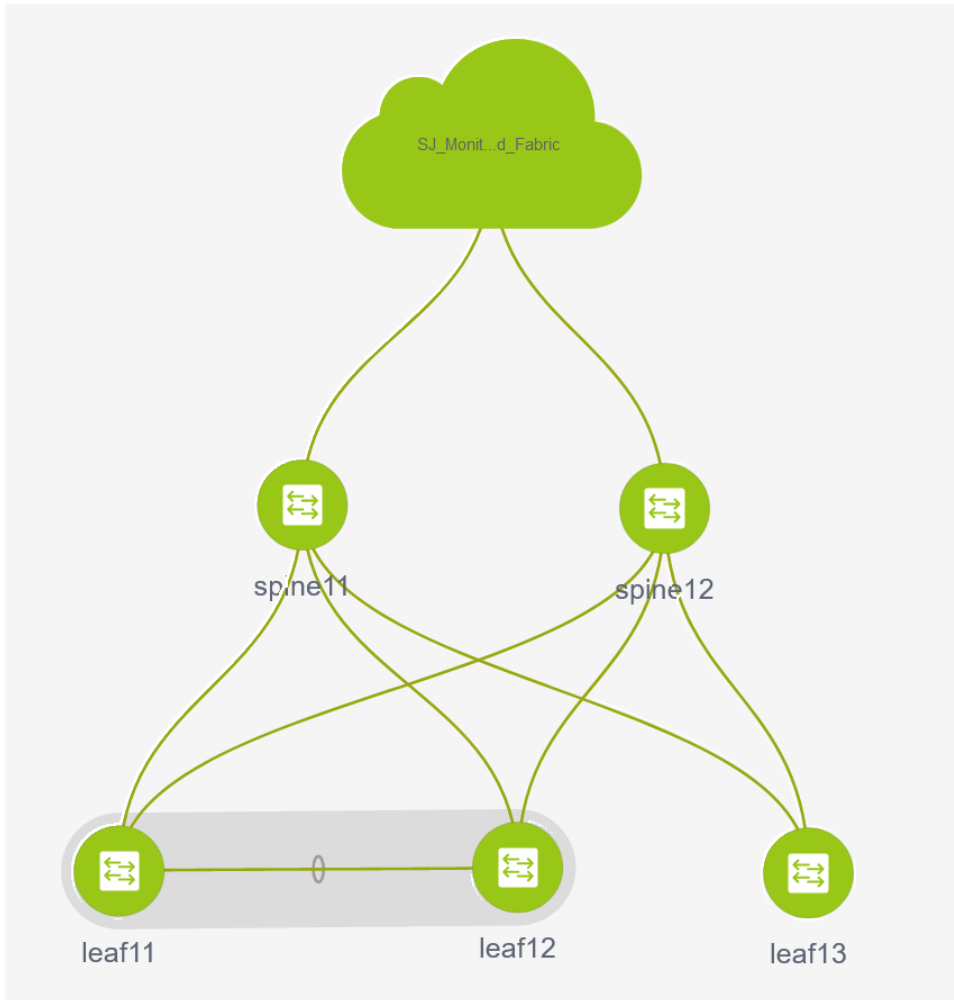
Nexus Dashboard Insights (NDI) is a unified monitoring and analytics tool that reduces mean time to detect (MTTD) and mean time to resolve (MTTR) network issues by providing

- comprehensive visibility into the infrastructure,
- reliable issue analysis, and,
- definitive suggestions for addressing day2 operation challenges in complex data center networks.

Nexus Dashboard Insights processes and analyzes telemetry data continuously streamed from all the devices in the infrastructure to provide network operators with real-time monitoring and analytics of the network besides being able to proactively provide lifecycle management suggestions and foresight into infrastructure change management.

**Note:** The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

This paper details the best deployment configurations and settings to implement Nexus Dashboard Insights for your DCNM managed or monitored NX-OS network sites. To enable streaming telemetry data from all the devices on the sites, specific configurations, you must configure DCNM and devices. We use a typical two-tier (spine and leaf) network fabric as an example in this white paper to illustrate the necessary configurations, either on the DCNM controller or the switches themselves to prepare the site for Nexus Dashboard Insights. As a network site can be fully managed or monitored by DCNM, the white paper also explains the configuration for both DCNM managed mode and the monitored mode.



### Software and Hardware Product Versions

The example in this white paper has the following product software versions:

- DCNM version 11.5.2
- Nexus Dashboard version 6.0.1.23
- Nexus Dashboard Insights version 2.1(1d)

For more information about supported software versions and compatibilities of related products, refer to the Cisco Nexus Dashboard and Services Compatibility Matrix at the following link:

<https://www.cisco.com/c/dam/en/us/td/docs/dcn/tools/dcn-apps/index.html>

For support of the required features, we're using all cloud scale switches.

### Pre-Requirement Configuration for DCNM Sites

Cisco DCNM enables controlling, automating, monitoring, and visualization and troubleshooting of networks built of the Nexus Data Center switches. To configure DCNM, refer to the configuration guide:

<https://www.cisco.com/c/en/us/td/docs/dcn/dcnm/1151/configuration/lanfabric/cisco-dcnm-lanfabric-configuration-guide-1151.html>

---

The following requirements enable to prepare DCNM and its managed or monitored network sites ready for onboarding on Nexus Dashboard and use with Nexus Dashboard Insights:

- **Configure DCNM in-band Network**

Nexus Dashboard onboarding and telemetry data transfer use the DCNM in-band data network. IP reachability between the data network of the Nexus Dashboard and the DCNM in-band IP addresses is required.

- **Configure routable loopback interfaces on switches for Nexus Dashboard data network connectivity**

Nexus Dashboard data network needs IP reachability to the network site and the DCNM. A routable loopback interface is used on the network site switches for this connectivity and to source telemetry data. We could use a dedicated loopback interface or an existing loopback interface on the switches. Configuring/usage of a loopback interface for both monitored and managed modes are discussed in further sections.

The Round-trip time (RTT) between the Nexus Dashboard cluster and the network site must not exceed 50m for Nexus Dashboard Insights to run for the network site properly.

- **Configure DCNM in-band Network**

Nexus Dashboard onboarding and telemetry data transfer uses the DCNM in-band data network. IP reachability between the data network of the Nexus Dashboard and the DCNM in-band IP addresses is required.

- **Enable and Configure NTP (Network Time Protocol) in the network**

NTP is an essential clock service that syncs all the elements of the network site. NTP service is not only required for setting up the DCNM cluster and managing network site switches but also for software telemetry to work. It maintains consistency and coherence of logs between the switches and the DCNM controller. NTP configurations and verifications for monitored and managed modes are discussed in the further sections.

- **Enable and Configure PTP (Precision Time protocol) in the network**

Nexus Dashboard Insights requires a microsecond-level accurate PTP clock for the network site in order to perform flow analytics across the site and calculate the end-to-end network latency of the flows.

For a DCNM managed or monitored NX-OS network site, the PTP grandmaster needs to be an external device that can provide at least a microsecond-level clock.

The PTP configurations and verifications are explained in further sections for both DCNM managed and monitored network sites.

The following sections discuss in detail about the configuration and verification for each of the prerequisite requirements.

## **Configure DCNM In-band Network**

Nexus Dashboard onboarding and telemetry data transfer use the DCNM in-band data network. You must establish IP reachability from the data network of the Nexus Dashboard to the DCNM in-band IP addresses. This is a part of DCNM installation and initial setup; however, this section provides instructions to configure DCNM in-band network.

DCNM uses eth2 interface for in-band connectivity. For Nexus Dashboard and Nexus Dashboard Insights, you must configure eth2 interface and must be reachable from the Nexus Dashboard data network for a single standalone instance or in-band eth2 VIP interfaces for DCNM in HA mode (Active/Standby) installation. The rest of this section discusses the procedure of configuring and verifying the DCNM in-band network.

## Procedure

### Step 1. Configure the IP address on 'eth2' interface.

```
[sysadmin@DCNM]$ ifconfig eth2 192.168.1.201 netmask 255.255.255.0
```

### Step 2. Verify that the IP address and netmask configuration.

```
[sysadmin@DCNM]$ ifconfig eth2
eth2: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.201 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::250:56ff:feaf:a4b0 prefixlen 64 scopeid 0x20<link>
    ether 00:50:56:af:a4:b0 txqueuelen 1000 (Ethernet)
    RX packets 1406372 bytes 316914681 (302.2 MiB)
    RX errors 0 dropped 10 overruns 0 frame 0
    TX packets 1488439 bytes 669987921 (638.9 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

### Step 3. Verify the reachability to the Nexus Dashboard cluster :

1. On the DCNM, check the route to the Nexus Dashboard data network. Make sure that there is a valid route for the Nexus Dashboard data network via the DCNM eth2 interface. In the following example, the IP address 192.168.1.101 is one of the Nexus Dashboard node data network IP address.

```
[sysadmin@DCNM]$ ip route get 192.168.1.101
192.168.1.101 dev eth2 src 192.168.1.201
```

2. On the DCNM, ping one of the Nexus Dashboard data network IP address. As long as there is no firewall or other network devices blocking the ICMP traffic, the ping should succeed.

```
[sysadmin@DCNM]$ ping 192.168.1.101 -> verifying reachability to ND
PING 192.168.1.101 (192.168.1.101) 56(84) bytes of data.
64 bytes from 192.168.1.101: icmp_seq=1 ttl=64 time=1.16 ms
64 bytes from 192.168.1.101: icmp_seq=2 ttl=64 time=2.34 ms
64 bytes from 192.168.1.101: icmp_seq=3 ttl=64 time=0.682 ms
64 bytes from 192.168.1.101: icmp_seq=4 ttl=64 time=0.130 ms
64 bytes from 192.168.1.101: icmp_seq=5 ttl=64 time=0.288 ms
^C
--- 192.168.1.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 0.130/0.922/2.346/0.796 ms
```

## Prepare DCNM-Managed Network Sites for Nexus Dashboard Insights

DCNM supports managed mode which requires discovering nodes, adding them to a fabric and assigning fabric roles. In managed mode, DCNM manages the switch configuration. It deploys the config-profiles as configured in the fabric building process and monitors the network site.

This section provides information to prepare a DCNM-managed network site for Nexus Dashboard and Nexus Dashboard Insights. The task flow is as listed below:

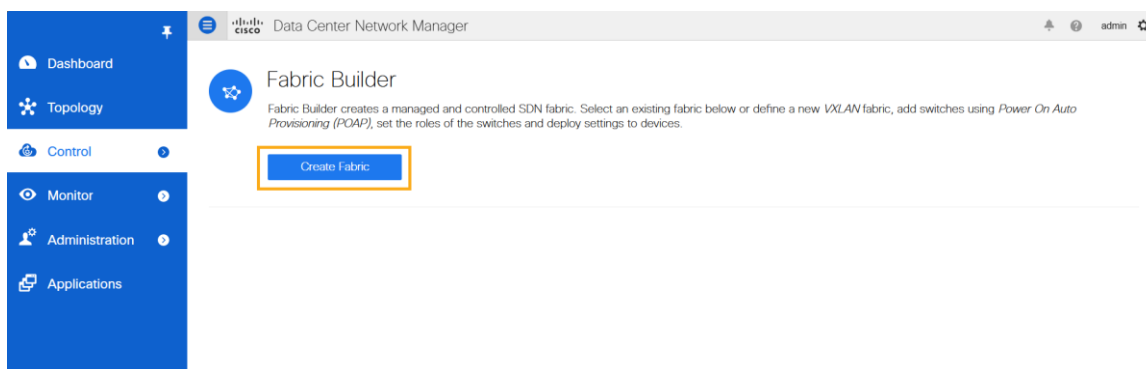
- Create fabric
- Discover switches
- Create/Use routable loopback interfaces on switches
- Configure NTP
- Configure PTP

### Create a Network Fabric

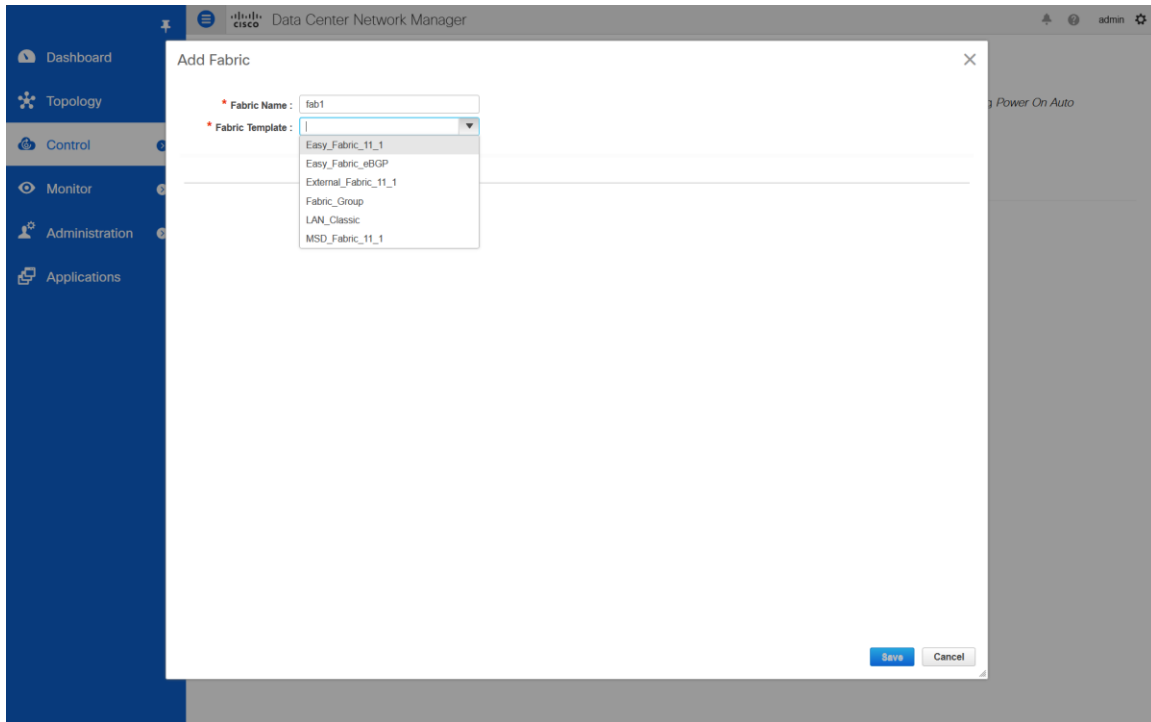
To create a controlled SDN fabric that can be managed and monitored by the DCNM, perform the following steps:

#### Procedure:

**Step 1.** Click Control > Create Fabric.

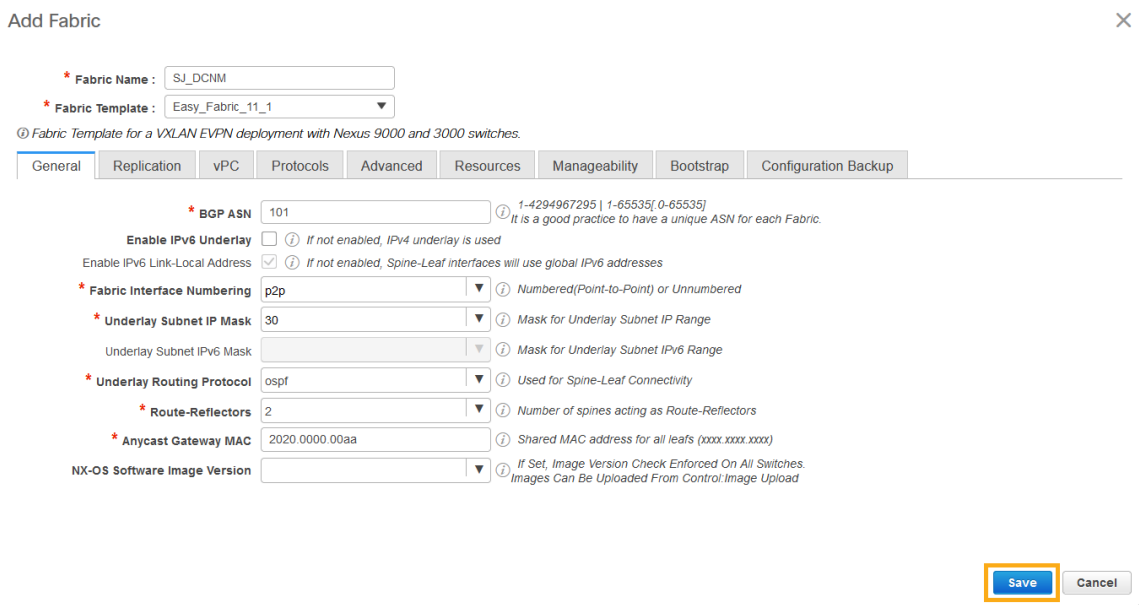


DCNM supports multiple fabric types of fabrics (for example: LAN classic, VxLAN fabrics and so on). Select the template of interest. For this paper, we use a VxLAN fabric as the example. In the Add Fabric page enter Fabric Name and choose 'Easy\_Fabric\_11\_1' template to add a managed VxLAN fabric.



For this paper, we use a VxLAN fabric as the example. In the Add Fabric page enter Fabric Name and choose 'Easy\_Fabric\_11\_1' template to add a managed VxLAN fabric.

**Step 2.** Fill in the details in different fields populated for the chosen template. Ex: Easy\_Fabric\_11\_1. Click Save to submit the configuration.



Refer to 'Easy Provisioning of VxLAN BGP EVPN Fabrics' in the DCNM configuration guide <https://www.cisco.com/c/en/us/td/docs/dcn/dcnm/1151/configuration/lanfabric/cisco-dcnm-lanfabric-configuration-guide-1151.html>.

## Discover Switches in the Fabric

DCNM can use a single seed or multiple IPs in the fabric and dynamically discover the switches for a set number of hops defined in 'Max Hops'. DCNM can also list all the switch IPs in the fabric with a hop count '0'. You can select the switches to add to the fabric.

### Procedure:

**Step 1.** Click on **Add switches** and provide a seed IP (management IP) of any switch in the fabric to be discovered. Add all the switches DCNM discovers pertaining to the fabric.

Inventory Management ✕

Discover Existing Switches | PowerOn Auto Provisioning (POAP)

Discovery Information > Scan Details >

Seed IP   
*Ex: 2.2.2.20 (or) 10.10.10.40-60 (or) 2.2.2.20, 2.2.2.21*

Authentication Protocol

Username

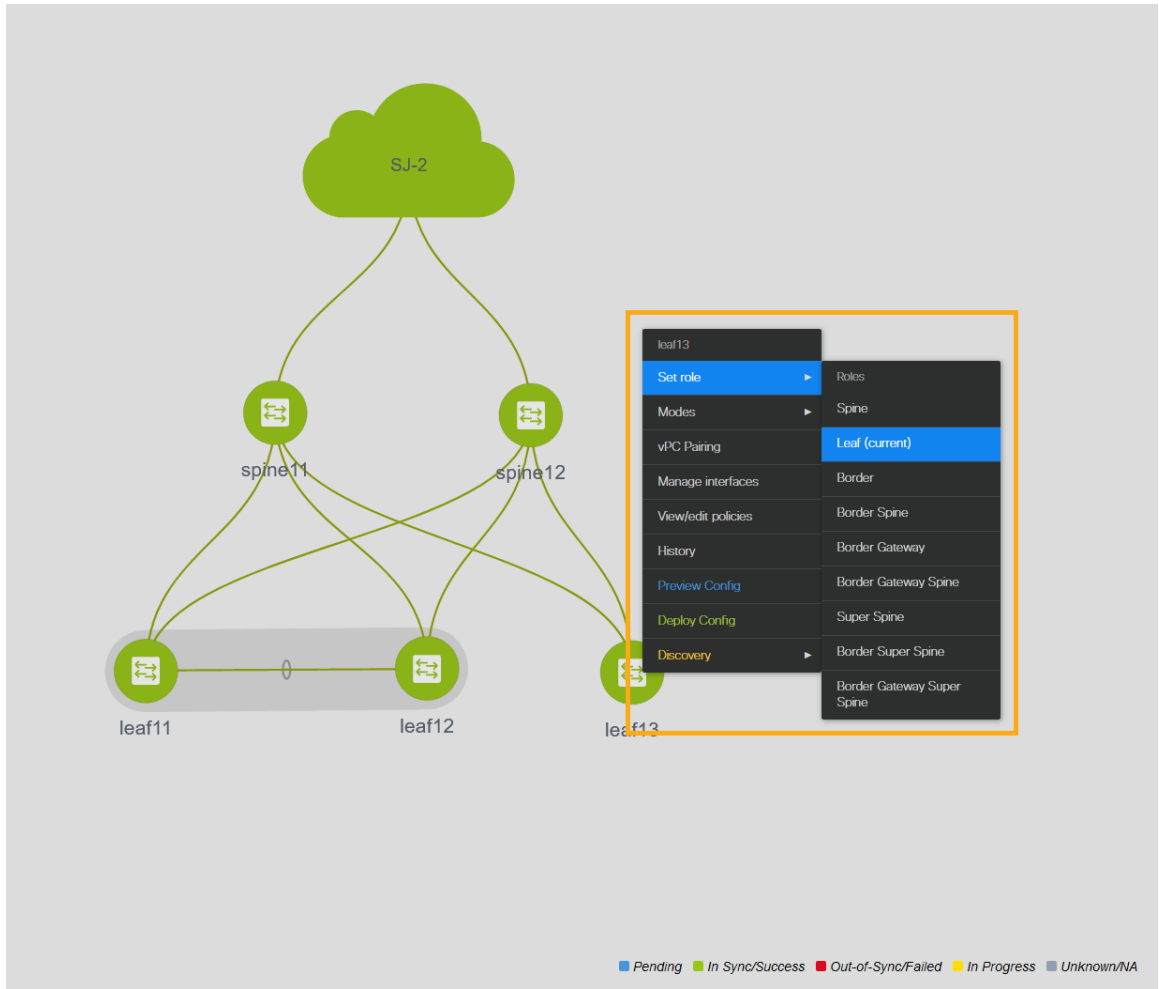
Password

Max Hops  hop(s)

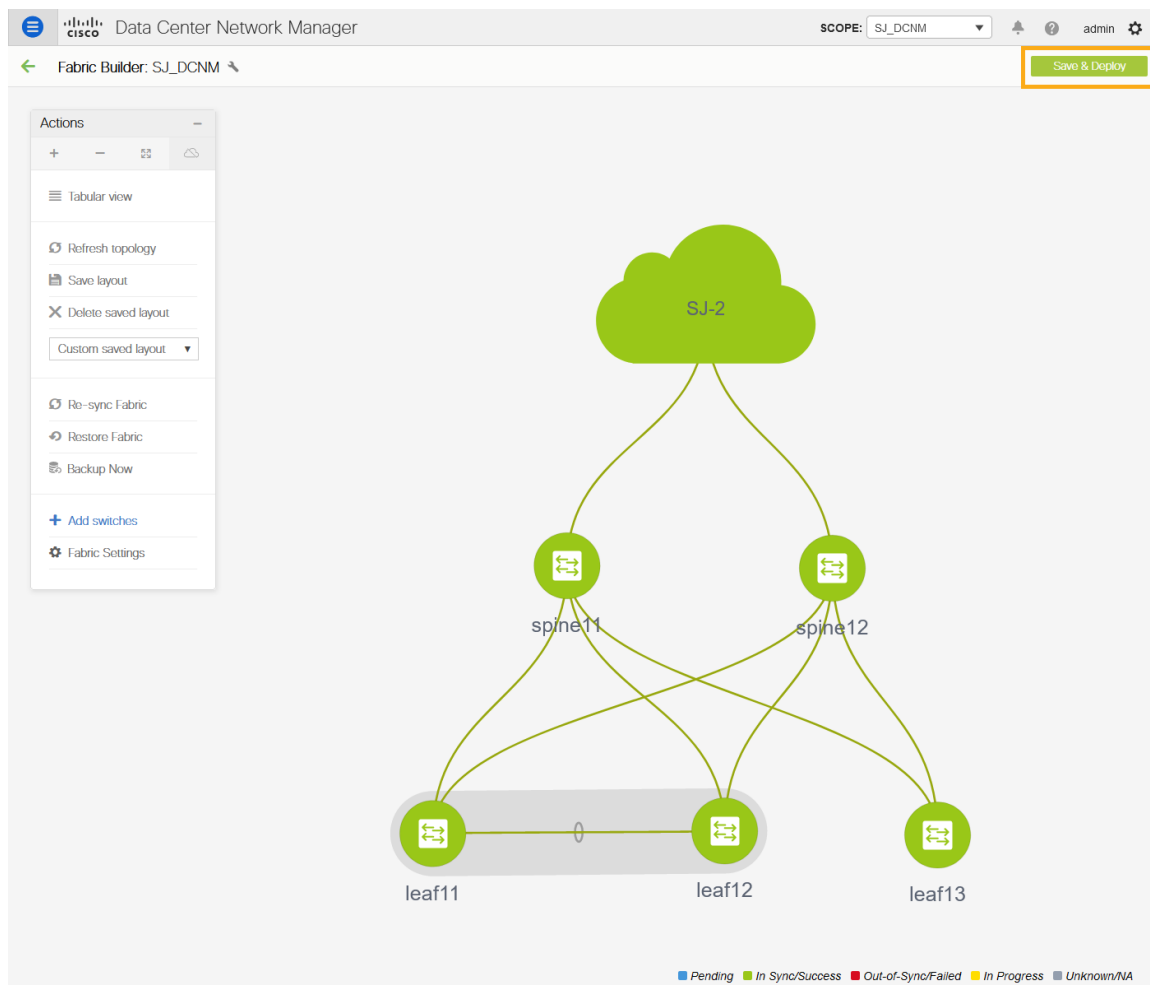
Preserve Config  no  yes  
*Selecting 'no' will clean up the configuration on switch(es)*

**Step 2.** After the switches are added to the fabric, assign roles to the switches by right-clicking on any of the switches and choosing the intended role, such as Spine, Leaf, Border Gateway and etc.





**Step 3.** Click Save & Deploy

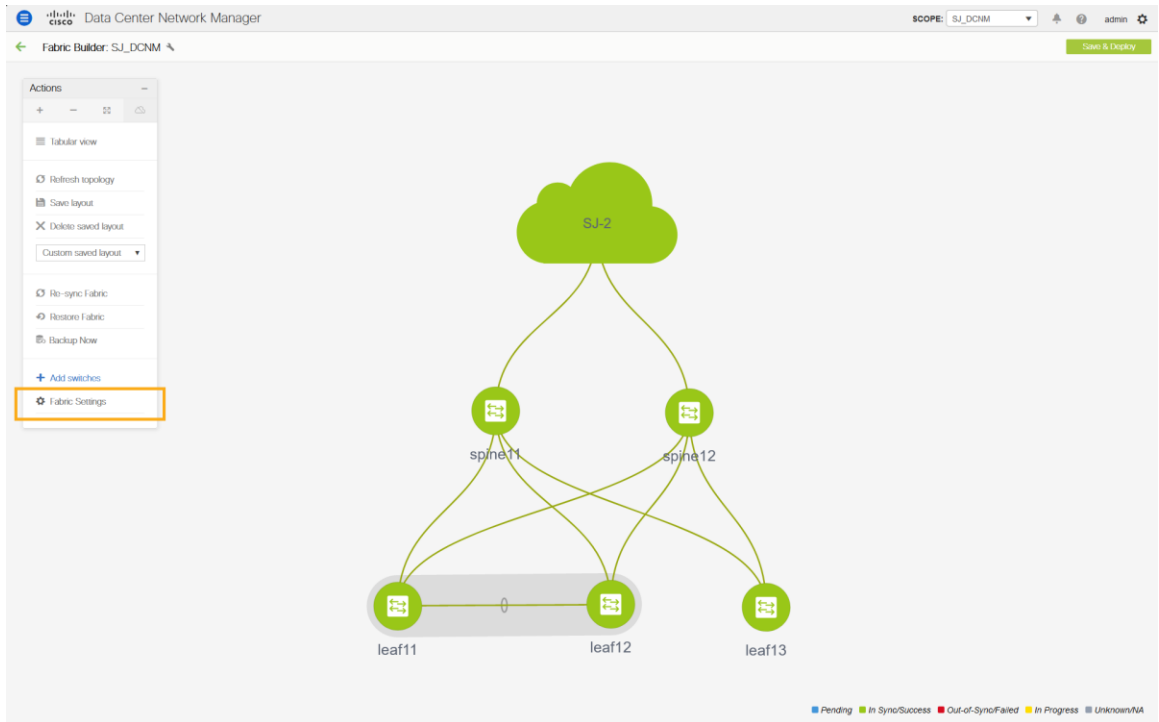


### Configure a routable loopback interface on the switches

For a managed easy fabric, DCNM deploys an underlay routing loopback and a VTEP loopback on the switches. To deploy Nexus Dashboard Insights for the DCNM site, you can use either of the loopback if it is reachable to the data network of the Nexus Dashboard cluster.

#### Procedure:

**Step 1.** Navigate to the fabric settings by choosing the managed fabric that you deployed.



**Step 2.** Go to the Protocols tab and enable loopback IDs and Save

Edit Fabric

\* Fabric Name :

\* Fabric Template :

① Fabric Template for a VXLAN EVPN deployment with Nexus 9000 and 3000 switches.

General	Replication	vPC	Protocols	Advanced	Resources	Manageability	Bootstrap	Configuration Backup
<p>* Underlay Routing Loopback Id <input type="text" value="0"/> ⓘ (Min:0, Max:1023)</p> <p>* Underlay VTEP Loopback Id <input type="text" value="1"/> ⓘ (Min:0, Max:1023)</p> <p>Underlay Anycast Loopback Id <input type="text"/> ⓘ Used for vPC Peering in VXLANv6 Fabrics (Min:0, Max:1023)</p> <p>* Underlay Routing Protocol Tag <input type="text" value="UNDERLAY"/> ⓘ Underlay Routing Process Tag</p> <p>* OSPF Area Id <input type="text" value="0.0.0.0"/> ⓘ OSPF Area Id in IP address format</p> <p>Enable OSPF Authentication <input type="checkbox"/> ⓘ</p> <p>OSPF Authentication Key ID <input type="text"/> ⓘ (Min:0, Max:255)</p> <p>OSPF Authentication Key <input type="text"/> ⓘ 3DES Encrypted</p> <p>IS-IS Level <input type="text"/> ⓘ Supported IS types: level-1, level-2</p> <p>Enable IS-IS Network Point-to-Point <input type="checkbox"/> ⓘ This will enable network point-to-point on fabric interfaces which are numbered</p> <p>Enable IS-IS Authentication <input type="checkbox"/> ⓘ</p> <p>IS-IS Authentication Keychain Name <input type="text"/> ⓘ</p> <p>IS-IS Authentication Key ID <input type="text"/> ⓘ (Min:0, Max:65535)</p> <p>IS-IS Authentication Key <input type="text"/> ⓘ Cisco Type 7 Encrypted</p> <p>Enable BGP Authentication <input type="checkbox"/> ⓘ</p> <p>BGP Authentication Key Encryption Type <input type="text"/> ⓘ BGP Key Encryption Type: 3 - 3DES, 7 - Cisco</p> <p>BGP Authentication Key <input type="text"/> ⓘ Encrypted BGP Authentication Key based on type</p> <p>Enable PIM Hello Authentication <input type="checkbox"/> ⓘ Valid for IPv4 Underlay only</p> <p>PIM Hello Authentication Key <input type="text"/> ⓘ 3DES Encrypted</p> <p>Enable BFD <input type="checkbox"/> ⓘ Valid for IPv4 Underlay only</p>								
								<p><input type="button" value="Save"/> <input type="button" value="Cancel"/></p>

**Step 3.** Save and deploy the fabric to get loopback IDs created.

**Step 4.** Log in to the switch to check if the loopback mentioned above is created on the switches and can ping the Nexus Dashboard cluster.

```
leaf11# show run interface loopback 0
```

```
interface loopback0 >>> Check if the loopback 0 is created
  description Routing loopback interface
  ip address 10.2.0.1/32 >>> IP address dynamically allocated
  ip router ospf UNDERLAY area 0.0.0.0
  ip pim sparse-mode
```

```
leaf11# show interface loopback 0
```

```
loopback0 is up >>> Check status of the loopback 0
admin state is up,
  Hardware: Loopback
  Description: Routing loopback interface
  Internet Address is 10.2.0.1/32
  MTU 1500 bytes, BW 8000000 Kbit , DLY 5000 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, medium is broadcast
  Auto-mdix is turned off
    346284 packets input 30982434 bytes
    0 multicast frames 0 compressed
    0 input errors 0 frame 0 overrun 0 fifo
    0 packets output 0 bytes 0 underruns
    0 output errors 0 collisions 0 fifo
    0 out_carrier_errors
```

```
leaf11# ping 192.168.1.201 source-interface loopback 0 >> checking reachability to
the Nexus Dashboard
```

```
PING 192.168.1.201 (192.168.1.201): 56 data bytes
64 bytes from 192.168.1.201: icmp_seq=0 ttl=62 time=0.738 ms
64 bytes from 192.168.1.201: icmp_seq=1 ttl=62 time=0.45 ms
64 bytes from 192.168.1.201: icmp_seq=2 ttl=62 time=0.483 ms
64 bytes from 192.168.1.201: icmp_seq=3 ttl=62 time=0.429 ms
64 bytes from 192.168.1.201: icmp_seq=4 ttl=62 time=0.367 ms
```

```
--- 192.168.1.201 ping statistics ---
```

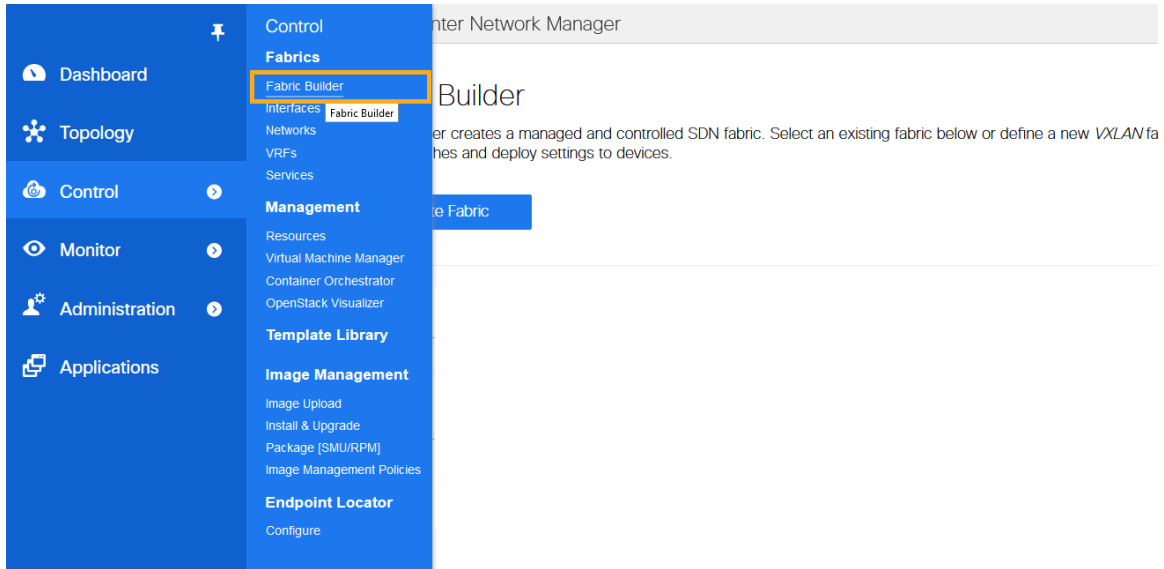
```
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.367/0.493/0.738 ms
```

## NTP (Network Time Protocol) Configuration

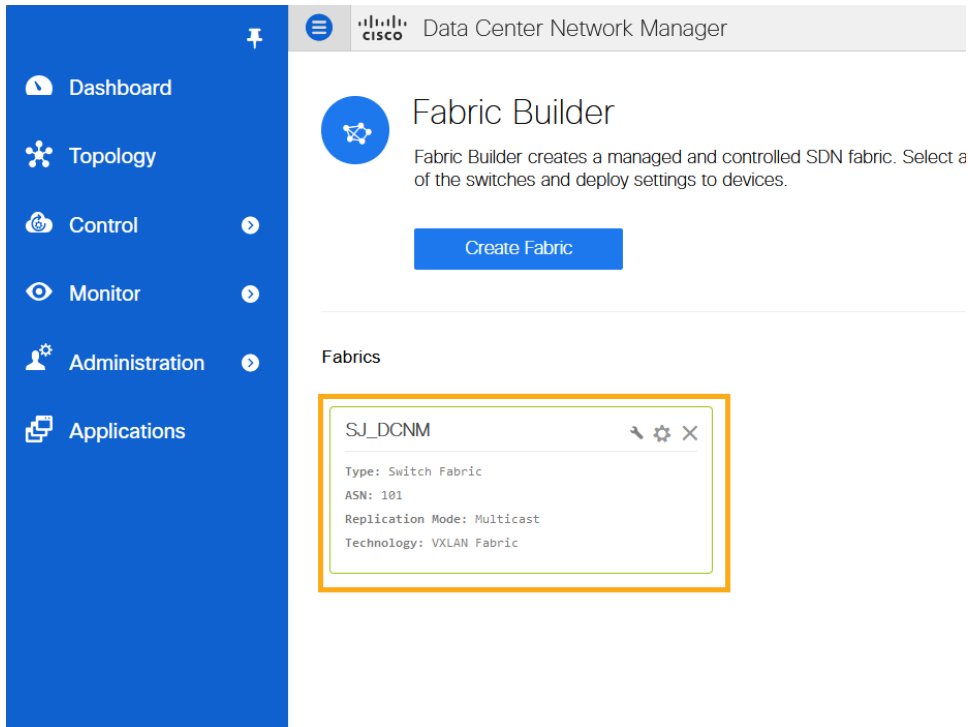
For a network site managed by the DCNM, enable and configure NTP on the DCNM. The DCNM pushes the NTP configs to all the switches.

### Procedure:

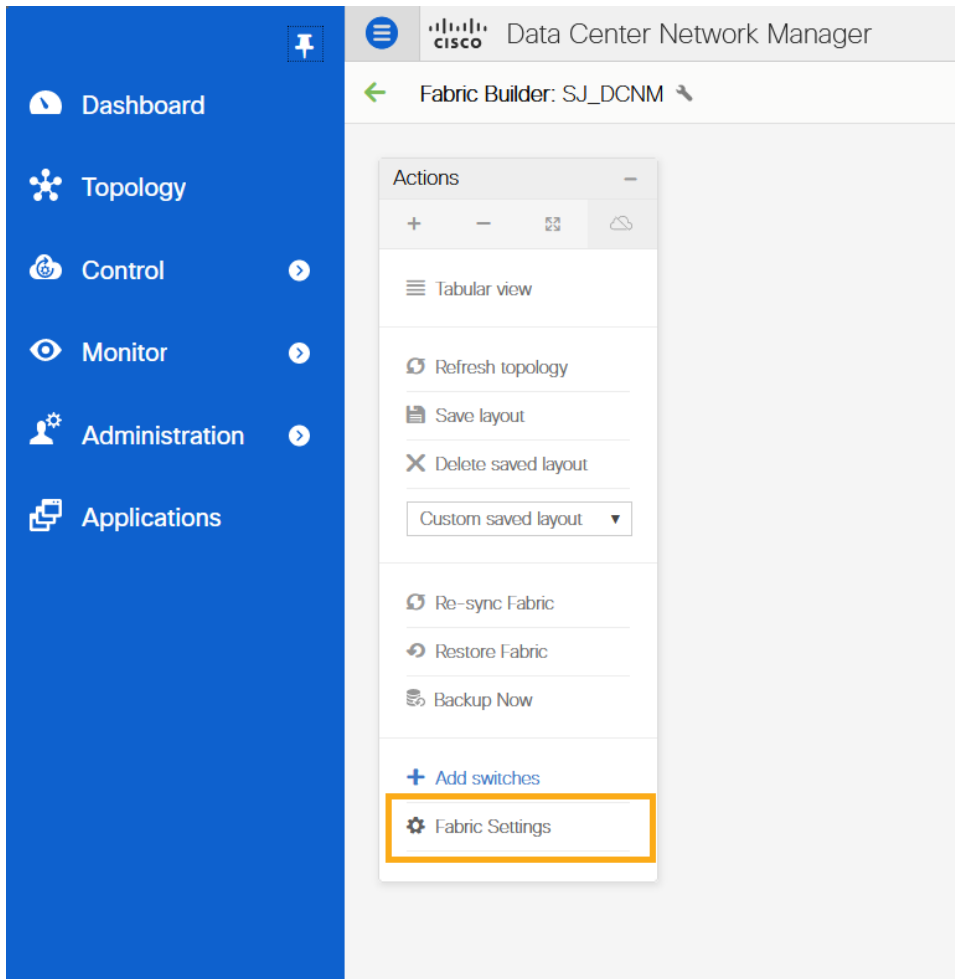
**Step 1.** From the DCNM homepage Click on Control -> Fabric Builder to go to the fabric builder page.



**Step 2.** Click on the fabric to setup NTP. The following example selects the fabric named “SJ\_DCNM”.



**Step 3.** Click on Fabric Settings.



**Step 4.** Navigate to the 'Manageability' tab to enter NTP server IP and VRF details and click **Save**.

Edit Fabric
✕

\* Fabric Name:

\* Fabric Template:

© Fabric Template for a VXLAN EVPN deployment with Nexus 9000 and 3000 switches.

General
Replication
vPC
Protocols
Advanced
Resources
Manageability
Bootstrap
Configuration Backup

DNS Server IPs  ⓘ Comma separated list of IP Addresses(v4/v6)

\* DNS Server VRFs  ⓘ One VRF for all DNS servers or a comma separated list of VRFs, one per DNS server

NTP Server IPs  ⓘ Comma separated list of IP Addresses(v4/v6)

\* NTP Server VRFs  ⓘ One VRF for all NTP servers or a comma separated list of VRFs, one per NTP server

Syslog Server IPs  ⓘ Comma separated list of IP Addresses(v4/v6)

Syslog Server Severity  ⓘ Comma separated list of Syslog severity values, one per Syslog server (Min:0, Max:7)

Syslog Server VRFs  ⓘ One VRF for all Syslog servers or a comma separated list of VRFs, one per Syslog server

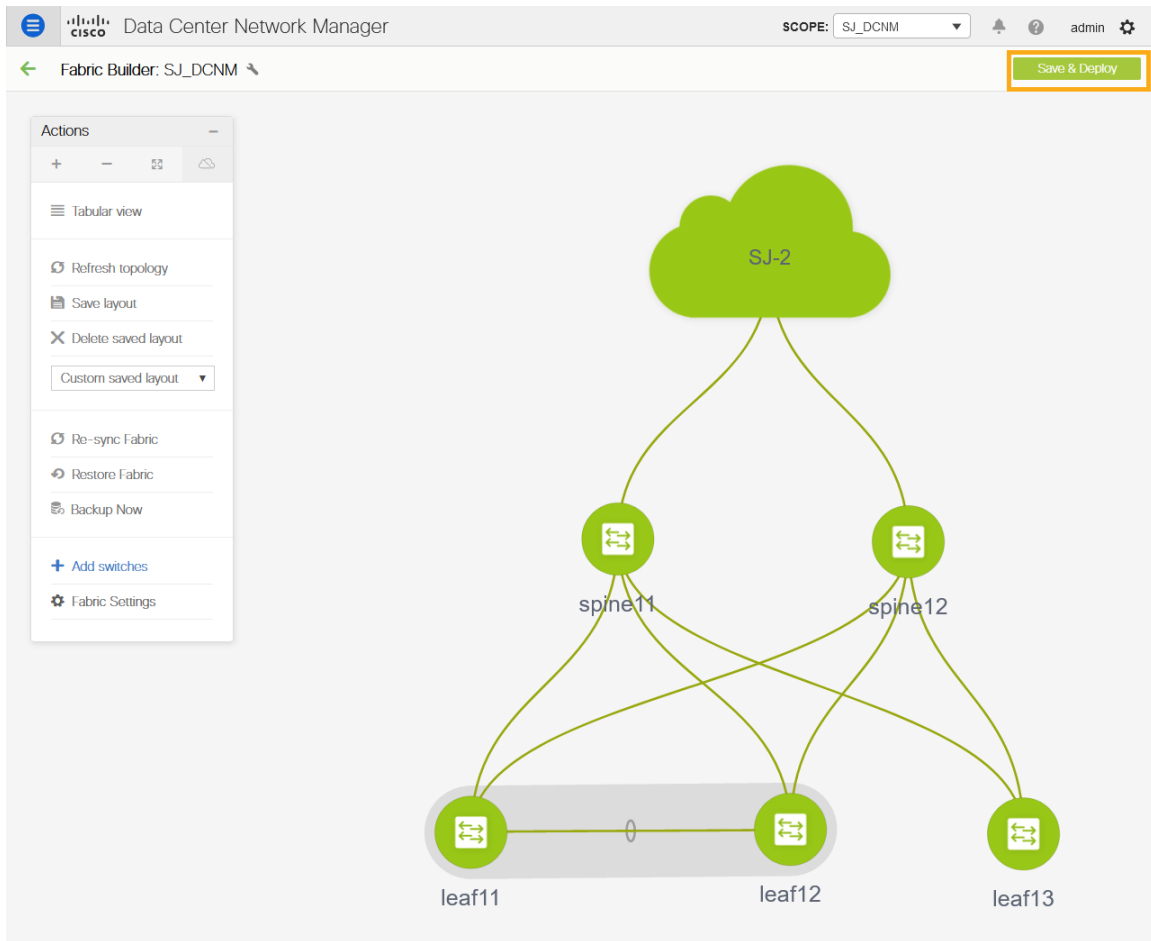
AAA Freeform Config

*Note ! All configs should strictly match 'show run' output, with respect to case and newlines. Any mismatches will yield unexpected diffs during deploy.*

Save

Cancel

**Step 5.** Click on **Save & Deploy** to ensure that switches are configured with the required NTP server settings as configured in the DCNM. Click on **Deploy Config** in the popup.



The switches turn green to indicate **In Sync** or **Success**.

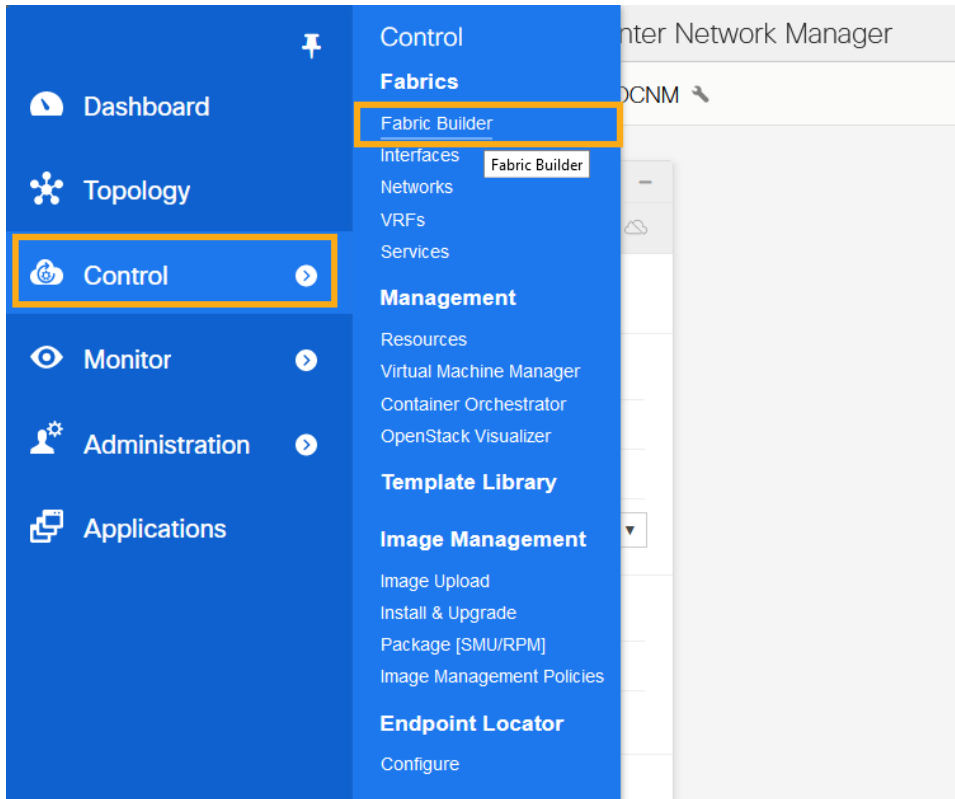
### PTP (Precision Time Protocol) Configuration

When PTP is enabled, it becomes the default clock even if NTP is enabled on the switches. PTP requires a source loopback used for exchanging PTP packets and a PTP domain ID that defines the boundaries of the PTP messages.

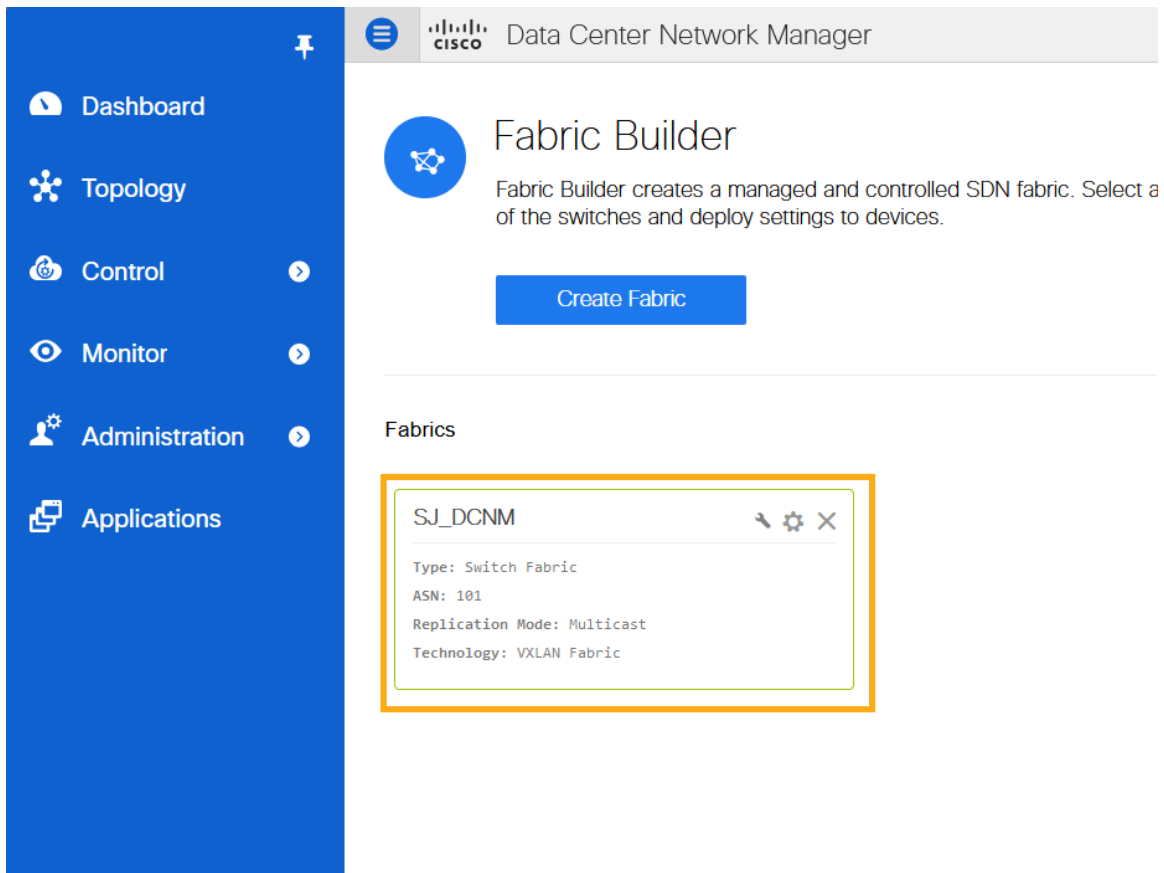
DCNM offers easy site setup for enabling PTP.

#### Procedure:

**Step 1.** From the DCNM homepage Click on Control -> Fabric Builder to go to the fabric builder page.

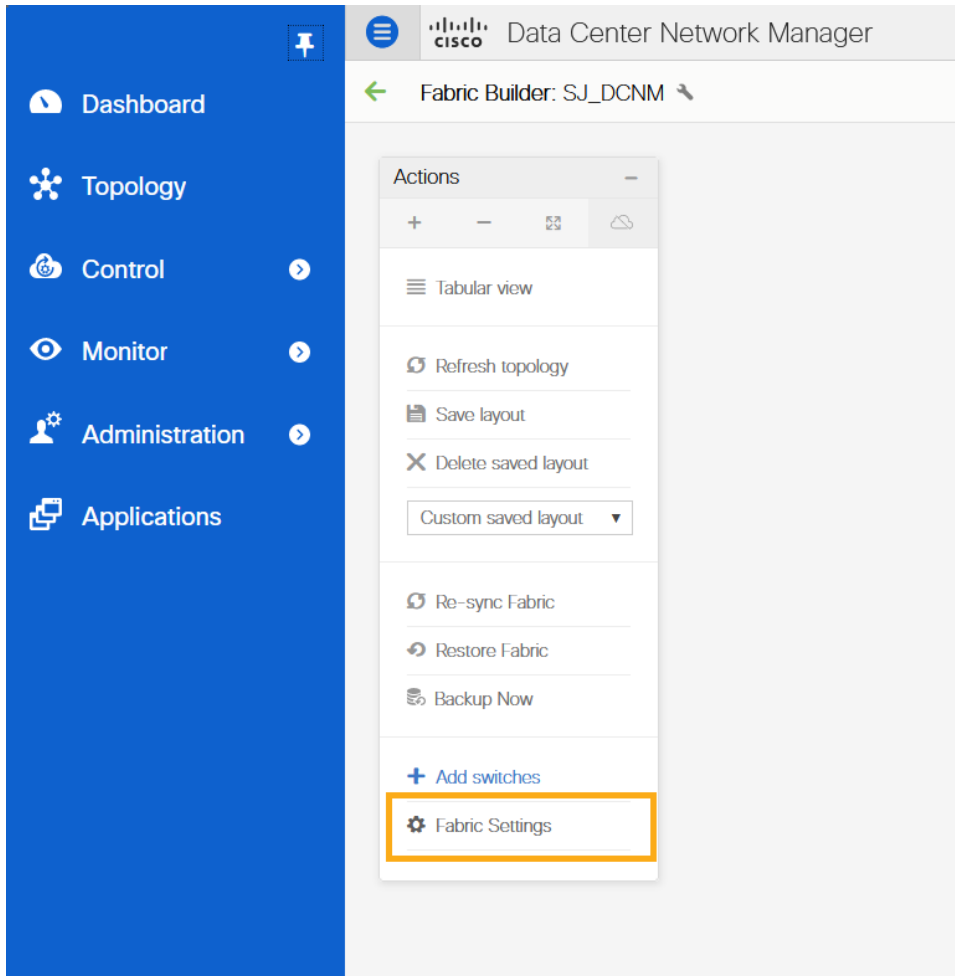


**Step 2.** Click on the fabric to setup PTP. The example shown below selects the fabric named “SJ\_DCNM”.





**Step 3.** Click on Fabric Settings



**Step 4.** Navigate to the 'Advanced' tab and select 'Enable Precision Time Protocol (PTP)'. Provide the 'PTP Source Loopback Id', the 'PTP Domain Id' and click **Save**. This enables PTP globally and on core-facing interfaces.

\* Fabric Name :

\* Fabric Template :

*① Fabric Template for a VXLAN EVPN deployment with Nexus 9000 and 3000 switches.*

General | Replication | vPC | Protocols | **Advanced** | Resources | Manageability | Bootstrap | Configuration Backup

\* Greenfield Cleanup Option  *① Switch Cleanup Without Reload When PreserveConfig=no*

Enable Precision Time Protocol (PTP)  *①*

\* PTP Source Loopback Id  *① (Min:0, Max:1023)*

\* PTP Domain Id  *① Multiple Independent PTP Clocking Subdomains on a Single Network (Min:0, Max:127)*

Enable MPLS Handoff  *①*

Underlay MPLS Loopback Id  *① Used for VXLAN to MPLS SR/LDP Handoff (Min:0, Max:1023)*

Enable TCAM Allocation  *① TCAM commands are automatically generated for VxLAN and vPC Fabric Peering when Enabled*

Enable Default Queuing Policies  *①*

N9K Cloud Scale Platform Queuing Policy  *① Queuing Policy for all 92xx, -EX, -FX, -FX2, -FX3, -GX series switches in the fabric*

N9K R-Series Platform Queuing Policy  *① Queuing Policy for all R-Series switches in the fabric*

Other N9K Platform Queuing Policy  *① Queuing Policy for all other switches in the fabric*

Enable MACsec  *① Enable MACsec in the fabric*

MACsec Primary Key String  *① Cisco Type 7 Encrypted Octet String*

MACsec Primary Cryptographic Algorithm  *① AES\_128\_CMAC or AES\_256\_CMAC*

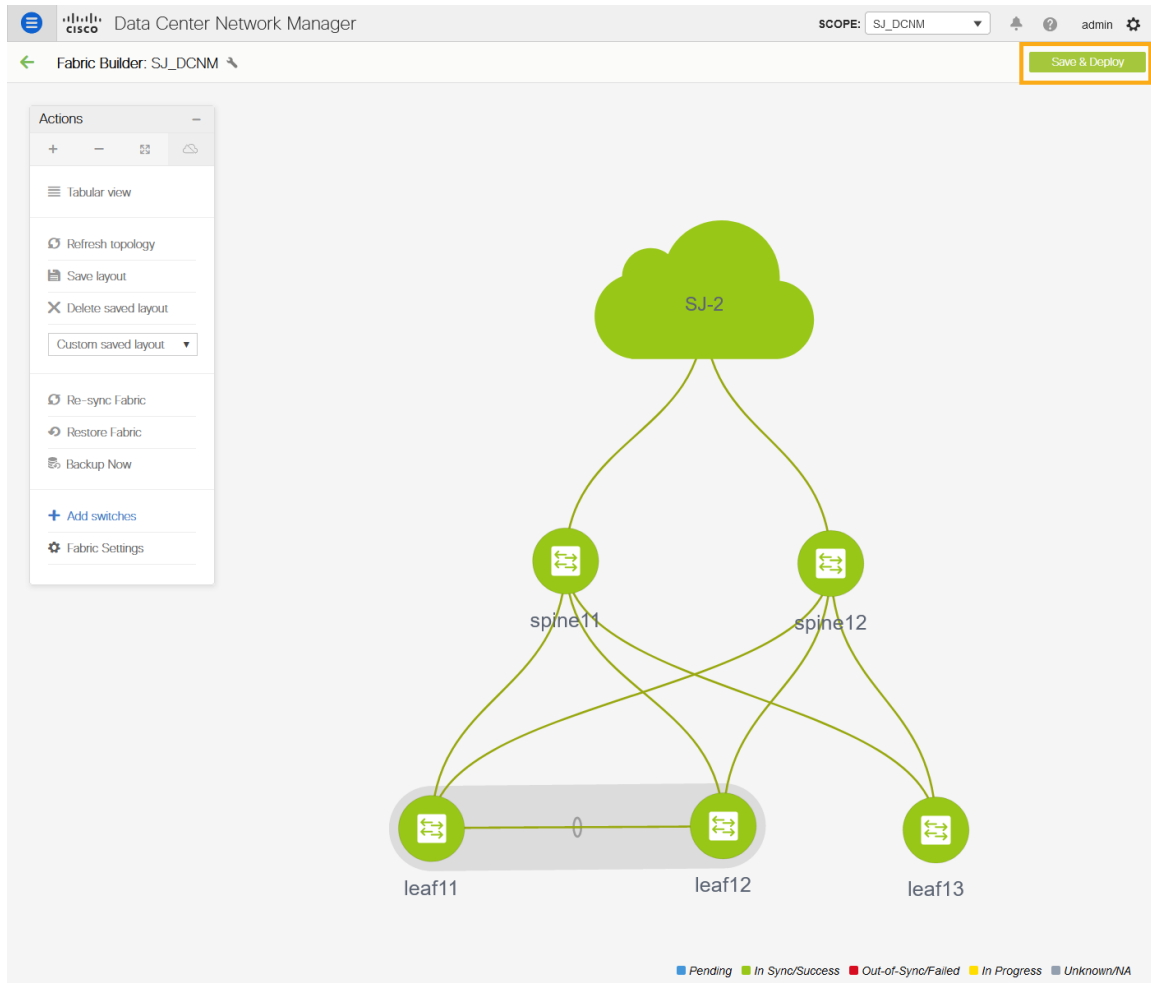
MACsec Fallback Key String  *① Cisco Type 7 Encrypted Octet String*

MACsec Fallback Cryptographic Algorithm  *① AES\_128\_CMAC or AES\_256\_CMAC*

MACsec Cipher Suite  *① Configure Cipher Suite*

MACsec Status Report Timer  *① MACsec Operational Status periodic report timer in minutes*

**Step 5.** Click on Save & Deploy to ensure that switches are configured with the required PTP settings as configured in the DCNM. Click on Deploy Config in the popup page



**Step 6.** After the switches turn green (In Sync/Success). Log in to the switches to confirm the configuration and clock settings.

## Prepare DCNM Monitored Network Sites for Nexus Dashboard Insights

DCNM supports monitored mode which requires discovering nodes and adding them to a fabric. In monitored mode, DCNM does not manage the switch configuration and typically only helps monitor the fabric. This mode can work complementary to any configuration tools and methods used as it is agnostic of the switch configurations. For a DCNM monitored network site, users need to deploy and verify the needed switch configuration for Nexus Dashboard and Nexus Dashboard Insights by themselves.

This section provides information to prepare the DCNM monitored fabric for Nexus Dashboard and Nexus Dashboard Insights. The task flow is as follows:

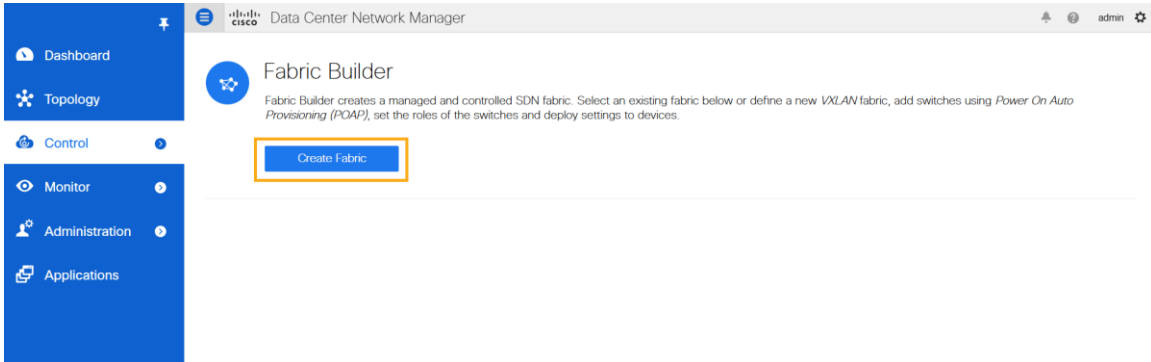
- Create fabric
- Discover switches
- Create/Use routable loopback interfaces on the switches
- Configure NTP
- Configure PTP

## Create Fabric

This section shows you how to create a DCNM monitored fabric.

### Procedure:

**Step 1.** Click Control > Create Fabric.



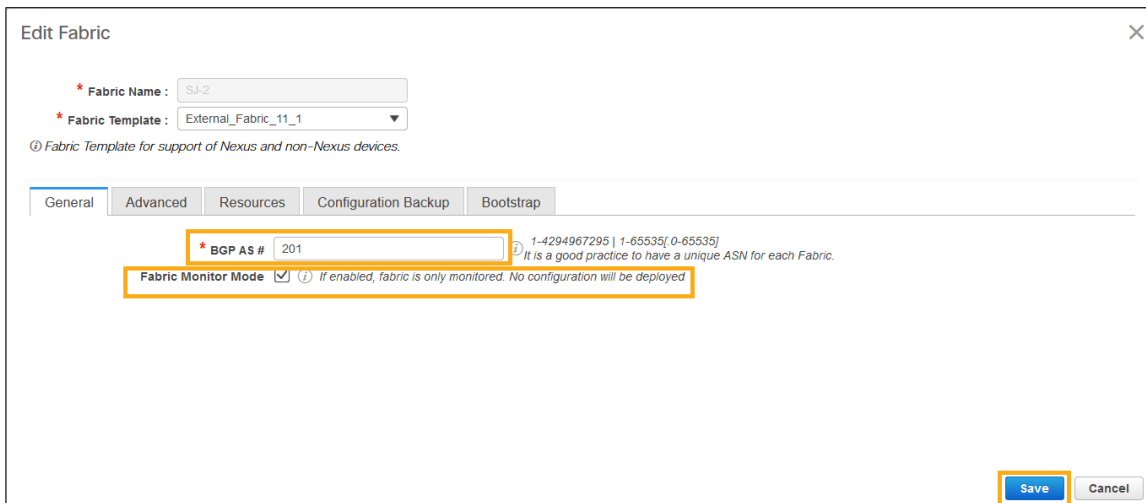
**Step 2.** In the Add Fabric page enter Fabric Name and choose 'External\_Fabric\_11\_1' template to add a monitored VxLAN fabric.



**Step 3.** Fill in the BGP AS# used in the site.

**Step 4.** Check the box next to "Fabric Monitor Mode".

**Step 5.** Click **Save**.



**Note:** As the fabric is only monitored by the DCNM, the switches in this fabric are configured by the user. DCNM does not deploy any configurations to the switches in this mode.

### Discover Switches in the Fabric

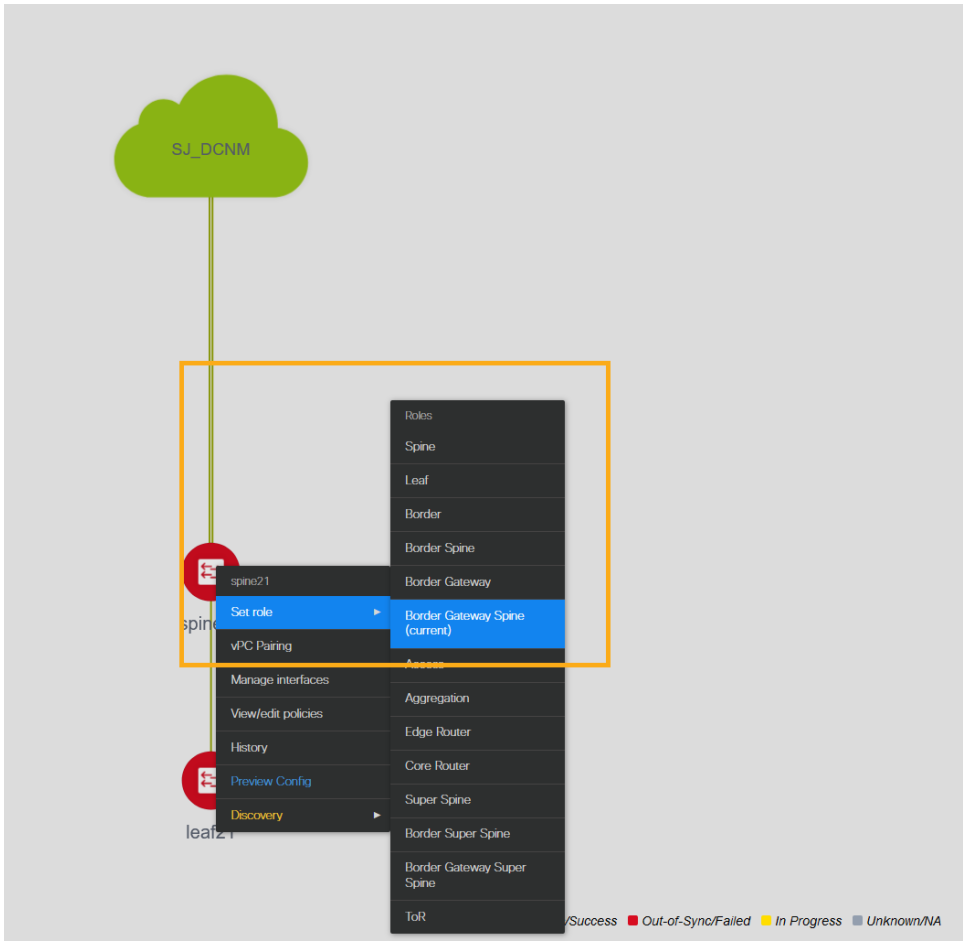
DCNM can use a single seed or multiple IPs in the fabric and dynamically discover the switches for a set number of hops defined in 'Max Hops'. DCNM can also list of all switch IPs in the fabric with a hop count '0'. It allows selection of switches to be added to the fabric.

#### Procedure:

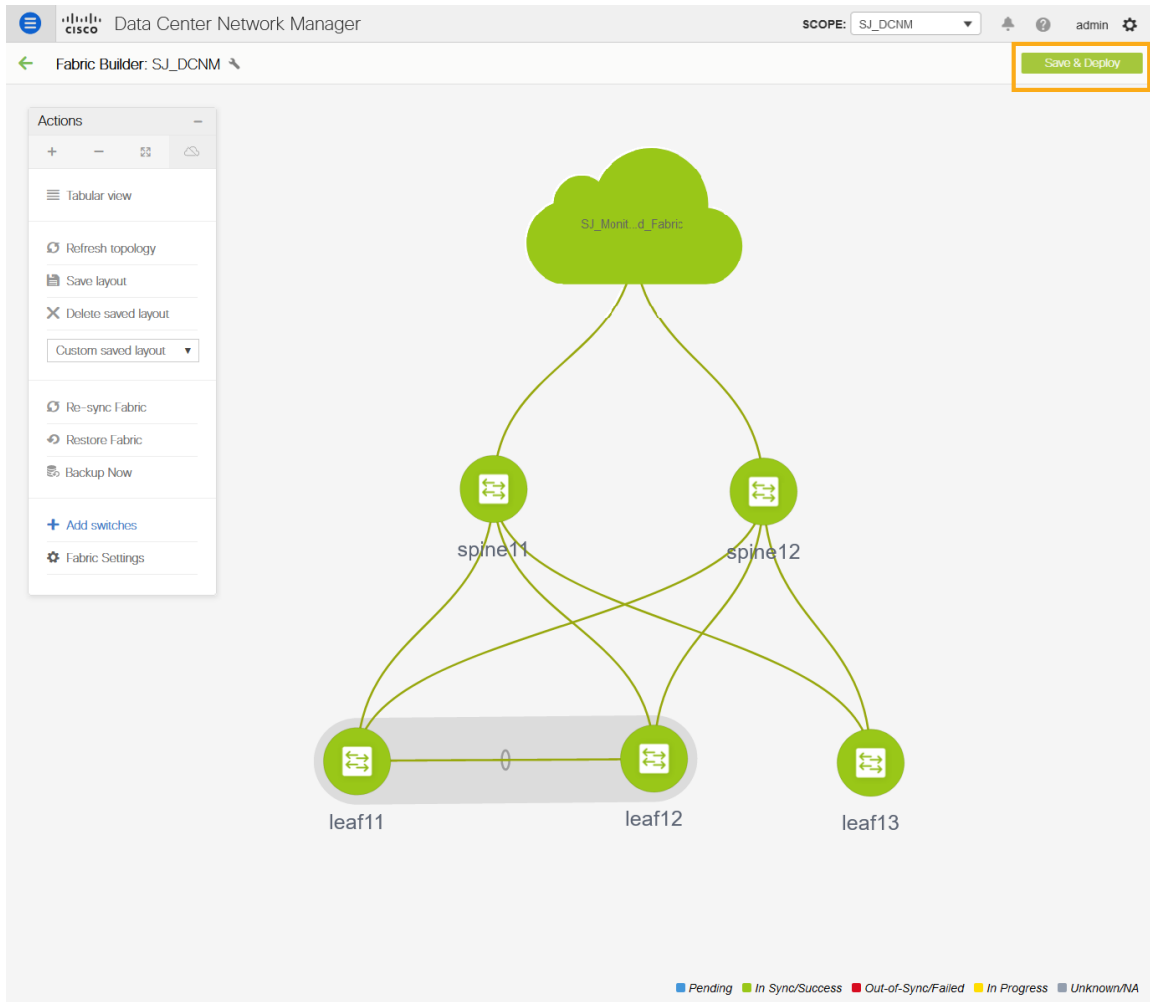
**Step 1.** Click on **Add switches** and provide a seed IP (management IP) of any switch in the fabric to be discovered. Add all the switches DCNM discovers pertaining to the fabric.

The screenshot shows the 'Inventory Management' window with a close button (X) in the top right. There are two tabs: 'Discover Existing Switches' (active) and 'PowerOn Auto Provisioning (POAP)'. Below the tabs are two breadcrumb links: 'Discovery Information' and 'Scan Details'. The main configuration area includes several fields: 'Seed IP' with the value '10.1.1.1' and a note 'Ex: 2.2.2.20 (or) 10.10.10.40-60 (or) 2.2.2.20, 2.2.2.21'; 'Authentication Protocol' set to 'MD5'; 'Username' set to 'admin'; 'Password' field with masked characters; 'Max Hops' set to '2' with a note 'hop(s)'; and 'Preserve Config' set to 'no' with a note 'Selecting 'no' will clean up the configuration on switch(es)'. A blue 'Start discovery' button is located at the bottom of the form.

**Step 2.** After the switches are added to the fabric, assign roles to the switches, such as Spine, Leaf, Border Gateway and etc.



**Step 3.** Click Save & Deploy



## Configure a Routable Loopback Interface on Switches

Each switch in the network site needs a routable loopback interface to source the telemetry data to the Nexus Dashboard Insights. Any existing loopback on the switches with the required IP connectivity to the Nexus Dashboard data network could be used or users can create a new loopback for the purpose.

For a DCNM monitored fabric, users need to configure and manage such a loopback interface on the switches by themselves. Below shows the procedure.

### Procedure:

#### Step 1. Configure a loopback interface on the switches

```
leaf21(config)# interface loopback 0
leaf21(config-if)# description Routing loopback interface
leaf21(config-if)# ip address 20.2.0.1/32
leaf21(config-if)# ip router ospf underlay area 0.0.0.0

leaf21# show run interface loopback 0 >> check for interface loopback0
description Routing loopback interface
ip address 20.2.0.1/32
```

```
ip router ospf underlay area 0.0.0.0
```

```
leaf21# show interface loopback 0
```

```
loopback0 is up
admin state is up,
  Hardware: Loopback
  Description: Routing loopback interface
  Internet Address is 20.2.0.1/32
  MTU 1500 bytes, BW 8000000 Kbit , DLY 5000 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, medium is broadcast
  Auto-mdix is turned off
    1031148 packets input 96462171 bytes
    0 multicast frames 0 compressed
    0 input errors 0 frame 0 overrun 0 fifo
    0 packets output 0 bytes 0 underruns
    0 output errors 0 collisions 0 fifo
    0 out_carrier_errors
```

- Step 2.** Check if the loopback created can reach the Nexus Dashboard Data Network by pinging the Nexus Dashboard Data Network IP address from the loopback interface. In the example below, the IP address 192.168.1.201 is one of the Nexus Dashboard Data Network IP address. If there is no firewalls or other network devices blocking the ICMP traffic, the ping should succeed.

```
leaf21# ping 192.168.1.201 source-interface loopback 0
```

```
PING 192.168.1.201 (192.168.1.201): 56 data bytes
64 bytes from 192.168.1.201: icmp_seq=0 ttl=62 time=0.56 ms
64 bytes from 192.168.1.201: icmp_seq=1 ttl=62 time=0.431 ms
64 bytes from 192.168.1.201: icmp_seq=2 ttl=62 time=0.38 ms
64 bytes from 192.168.1.201: icmp_seq=3 ttl=62 time=0.449 ms
64 bytes from 192.168.1.201: icmp_seq=4 ttl=62 time=0.379 ms

--- 192.168.1.201 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 0.379/0.439/0.56 ms
```

**Note:** For an effective verification, make sure that the ping is sourced from the Loopback interface.

### NTP (Network Time Protocol) Configuration

You must enable NTP and configure the NTP server on each switch in the network site monitored by the DCNM. Ensure that all the switches have the consistent NTP configuration and in synchronization with the same NTP server.

#### Procedure:

In DCNM monitored mode, all the switches in the network site must be configured with an NTP server.



```
spine12# config terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
spine12(config)# ntp server 72.163.32.44 use-vrf management
```

## PTP (Precision Time Protocol) Configuration

To provide flow analytics functions, Nexus Dashboard Insights s microsecProtocol(PTP).

For a DCNM managed or monitored network site, it is required to have an external PTP grandmaster that provides a clock source with at least microsecond accuracy.

When PTP is enabled, it becomes the default clock even if NTP is enabled on the switches. PTP requires a source loopback used for exchanging PTP packets and a PTP domain ID that defines the boundaries of the PTP messages.

For a DCNM monitored network site, you must configure PTP on each network switch by themselves since the DCNM does not manage the switch configuration. This section discusses how to configure PTP on an NX-OS switch.

### Procedure:

#### Step 1. Enable feature PTP:

```
leaf21# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
leaf21(config)# feature ptp -> Enabling feature ptp
```

#### Step 2. Configure PTP domain ID and PTP source interface (a routable loopback)

```
leaf21(config)# ptp domain 1 -> PTP domain ID
```

```
leaf21(config)# ptp source 10.2.0.1-> PTP source IP
```

#### Step 3. Configure PTP under core facing interfaces and ttag under Host facing interfaces:

```
interface Ethernet1/1 -> Core facing interface
```

```
ptp
```

```
interface Ethernet1/33 -> host facing interface
```

```
ttag
```

```
ttag-strip
```

## NTP and PTP verifications

With either managed or monitored mode fabrics, verifications on the switch remain the same.

### NTP verifications

Log in to the switches to confirm the configuration and clock settings. Verify below commands for NTP setup on the switch as the clock time source.

```
Leaf21(config)# show running configuration ntp
```

```
!Command: show running-config ntp
```

```
!No configuration change since last restart
```

```
!Time: Thu Aug 26 21:54:40 2021
```

```
version 9.3(7) Bios:version 05.40
```

```
ntp server 72.163.32.44 use-vrf management -> Verify the configuration
```

```
Leaf11(config)# show clock
```

```
21:53:34.997 UTC Thu Aug 26 2021
```

```
Time source is NTP -> Verify that NTP is the time source
```

```
Leaf11(config)# show ntp peers
```

```
-----  
Peer IP Address          Serv/Peer  
-----  
72.163.32.44            Server (configured) -> Verify that the server is configured
```

### PTP Verifications

After enabling PTP using DCNM or CLI configurations, use the following commands to verify PTP on the switch as the clock time source.

```
leaf11# show run ptp
```

```
feature ptp. -> Verify that PTP is enabled and configured on the interfaces
```

```
ptp source 10.2.0.1
```

```
ptp domain 0
```

```
interface Ethernet1/1
```

```
    ptp
```

```
interface Ethernet1/33
```

```
    ttag
```

```
    ttag-strip
```

```
leaf11# show clock
```

```
01:56:04.353 UTC Fri Aug 27 2021
```

```
Time source is PTP -> Verify that PTP is the time source
```

```
leaf11# show ptp clock foreign-masters record
```

P1=Priority1, P2=Priority2, C=Class, A=Accuracy,  
OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed  
GM=Is grandmaster

```
-----  
Interface          Clock-ID          P1  P2  C  A  OSLV  SR  
-----  
-----
```

---

Eth1/1 2c:4f:52:ff:fe:56:61:1f 255 255 248 254 65535 1

-> Verify it can reach the grand master on its ptp configured interfaces

leaf11# show ptp clock

PTP Device Type : boundary-clock

PTP Device Encapsulation : NA

PTP Source IP Address : 10.2.0.1 -> Verify that source loopback IP is as configured

Clock Identity : d4:78:9b:ff:fe:19:87:c3

Clock Domain: 0

Slave Clock Operation : Two-step

Master Clock Operation : Two-step

Slave-Only Clock Mode : Disabled

Number of PTP ports: 3

Priority1 : 255

Priority2 : 255

Clock Quality:

Class : 248

Accuracy : 254

Offset (log variance) : 65535

Offset From Master : 12

Mean Path Delay : 168

Steps removed : 2

Correction range : 100000

MPD range : 1000000000

Local clock time : Fri Aug 27 01:56:08 2021

PTP Clock state : Locked

leaf11# **show ptp parent**

PTP PARENT PROPERTIES

Parent Clock:

Parent Clock Identity: 2c:4f:52:ff:fe:56:61:1f

Parent Port Number: 4

Observed Parent Offset (log variance): N/A

Observed Parent Clock Phase Change Rate: N/A

Parent IP: 10.2.0.4

Grandmaster Clock:

Grandmaster Clock Identity: 00:ee:ab:ff:fe:3a:16:e7 -> Get the GM clock ID

Grandmaster Clock Quality:

```

Class: 248
Accuracy: 254
Offset (log variance): 65535
Priority1: 255
Priority2: 255

```

```
spine12# show ptp clock foreign-masters record
```

```

P1=Priority1, P2=Priority2, C=Class, A=Accuracy,
OSLV=Offset-Scaled-Log-Variance, SR=Steps-Removed
GM=Is grandmaster

```

Interface	Clock-ID	P1	P2	C	A	OSLV	SR	GM
Eth1/4	00:ee:ab:ff:fe:3a:16:e7	255	255	248	254	65535	0	GM

-> Check the GM clock ID and confirm the right GM registration on clients

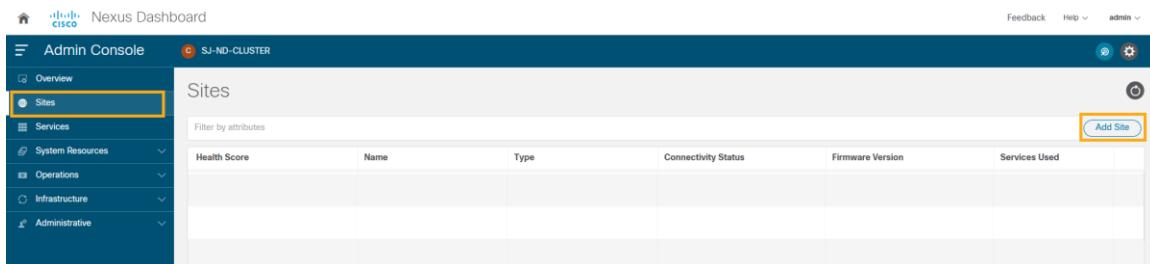
## Onboard a DCNM Network Site to Nexus Dashboard

Before adding a DCNM network site to Nexus Dashboard, ensure the following:

- Both primary and standby DCNM servers must return HA status: OK
- Nexus dashboard cluster has configured fabric connectivity and has cluster health: OK

**Procedure to add a DCNM site to the Nexus Dashboard:**

**Step 1.** From the Nexus Dashboard home page click on **Admin Console > Sites > Add Site**.



**Step 2.** Select 'Site Type' as **DCNM**. In the **Hostname/IP address** field, provide the DCNM in-band IP address configured on the 'eth2' interface of the DCNM server. Provide '**Username**' and '**Password**' of the DCNM server. Click '**Select Sites**' to choose the sites to onboard onto the Nexus Dashboard by clicking '**Save**'.

Chosen sites now are onboarded onto the Nexus Dashboard.

Health Score	Name	Type	Connectivity Status	Firmware Version	Services Used
Minor	SJ-2	DCNM	Up	11.5(2)	0
Healthy	SJ_DCNM	DCNM	Up	11.5(2)	0

## Enable Nexus Dashboard Insights for a DCNM Network Site

Below is the task checklist to enable Nexus Dashboard Insights service for a DCNM network site:

- Configure the required persistent IP addresses on the Nexus Dashboard
- Install and Enable the Nexus Dashboard Insights service on the Nexus Dashboard (only required if the Insights service is not installed or enabled).
- Enable the Nexus Dashboard Insights service for the site

### Configure persistent IP addresses in Nexus Dashboard

Nexus Dashboard Insights requires 6 mandatory persistent IP addresses for software and hardware telemetry services for a DCNM managed or monitored network site. The 6 persistent IP addresses are assigned to:

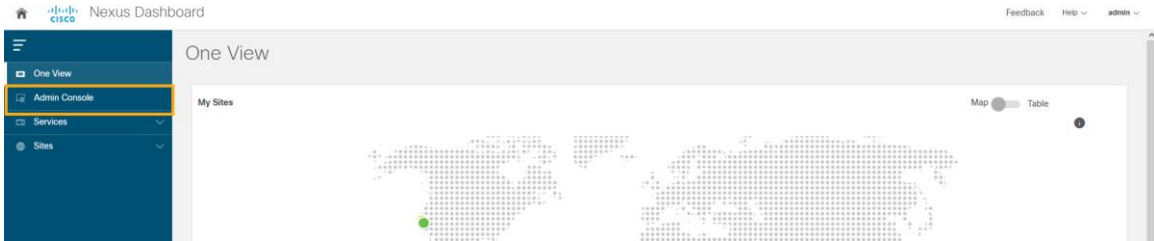
- 3 UTR(Software Telemetry) application services, and,
- 3 flow collector (Hardware Telemetry) application services.

These IP addresses are mandatory for Nexus Dashboard Insights operations. A 7th persistent IP address is required if IPv6 is used for the assurance data collection and transport between the network site and the Nexus Dashboard. These persistent IP addresses allows you to retain the same IP addresses for the Nexus Dashboard Insights services even if the internal microservice pods are relocated to different Nexus Dashboard nodes.

These persistent IP addresses are in the Nexus Dashboard Data Network subnet. They must be configured on the Nexus Dashboard prior to enabling the Nexus Dashboard Insights app.

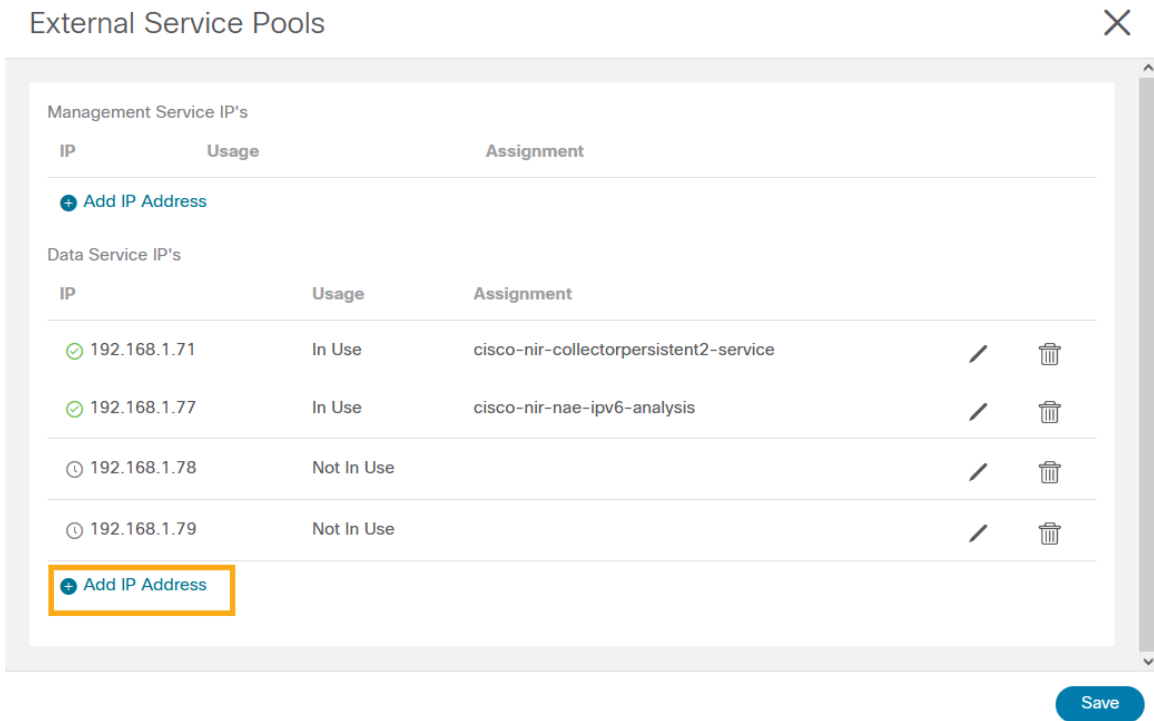
**Procedure:**

**Step 1.** On the Nexus Dashboard home page click ‘Admin Console’



**Step 2.** Navigate to **Infrastructure > Cluster Configuration**.

**Step 3.** Edit ‘**External Service Pools**’ and add six IP addresses from the data network subnet and click **Save**.



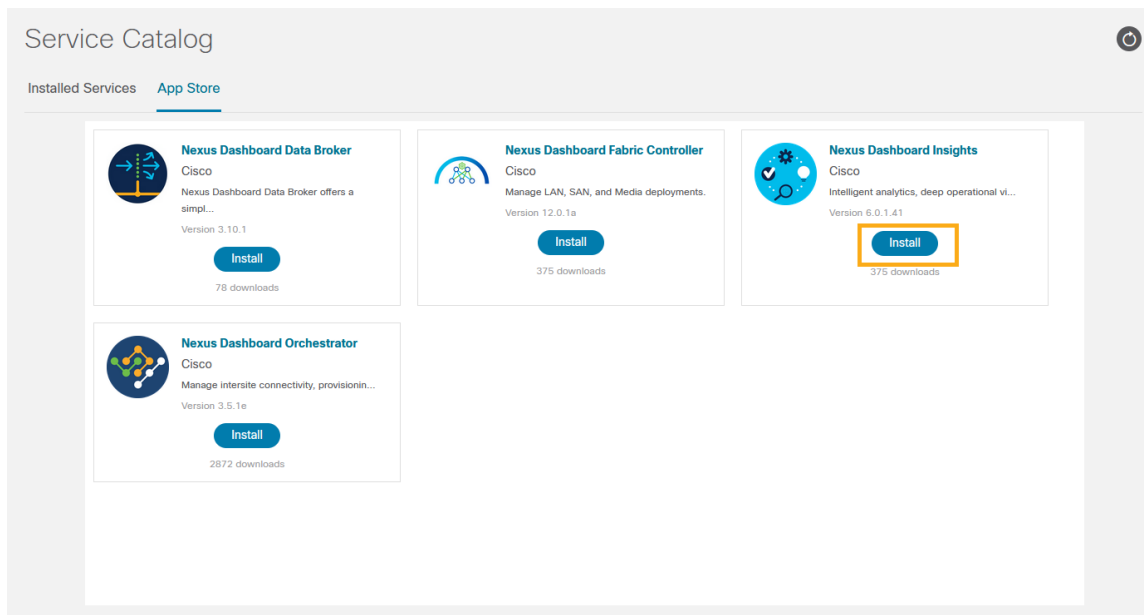
After the persistent IP addresses are added to the Nexus Dashboard, the Nexus Dashboard Insights App can be installed and enabled on the Nexus Dashboard.

**Note:** If Nexus Dashboard Insights is used for a DCNM managed/monitored network site, it's required that the Nexus Dashboard nodes are Layer-2 adjacent to one another in the Data Network. In another word, the Nexus Dashboard nodes need to be in the same IP subnet for their Data Network. This is needed to allow the persistent IP addresses to move among the Nexus Dashboard nodes.

## Install and Enable Nexus Dashboard Insights App

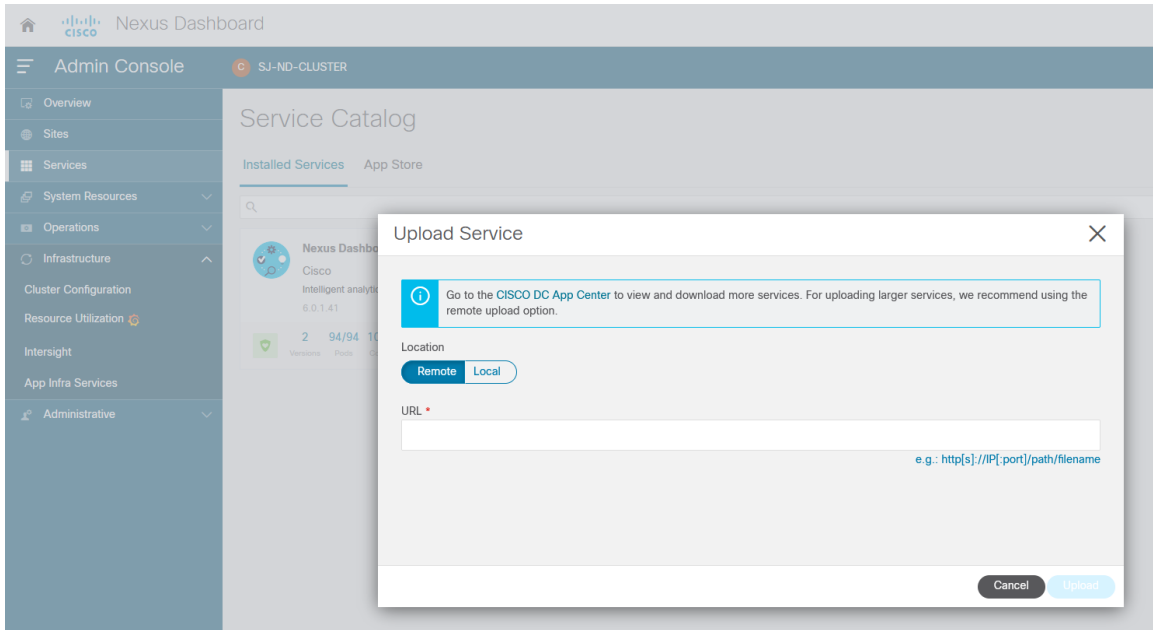
### Procedure:

**Step 1.** On navigating to Admin Console -> Services -> App Store tab, you can Install the Nexus Dashboard Insights App.

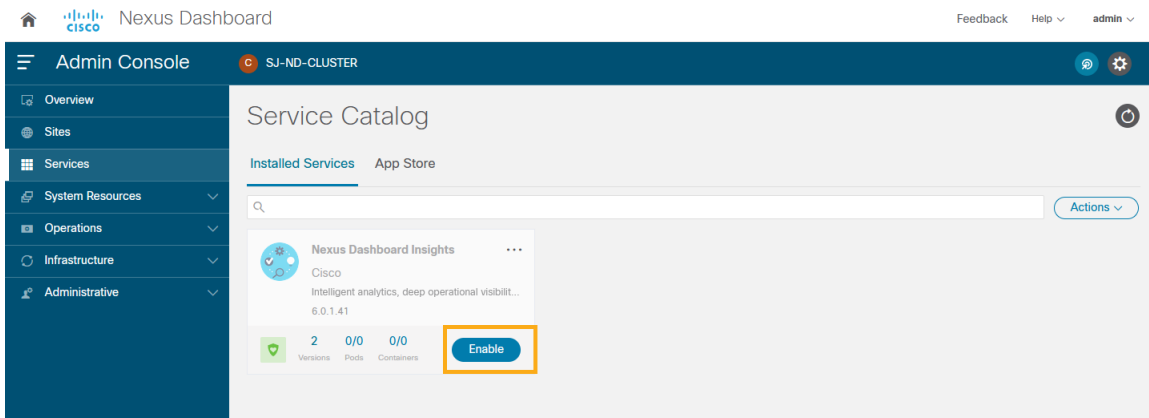


**Step 2.** If the Nexus Dashboard cannot reach the Cisco App Store directly due to network connectivity constraints, users can perform an “offline” installation of the Nexus Dashboard Insights app. First, download the application from the Cisco DC App Center at <https://dcappcenter.cisco.com/> to your local computer or a web server. Next, install the app on the Nexus Dashboard by following the steps in below:

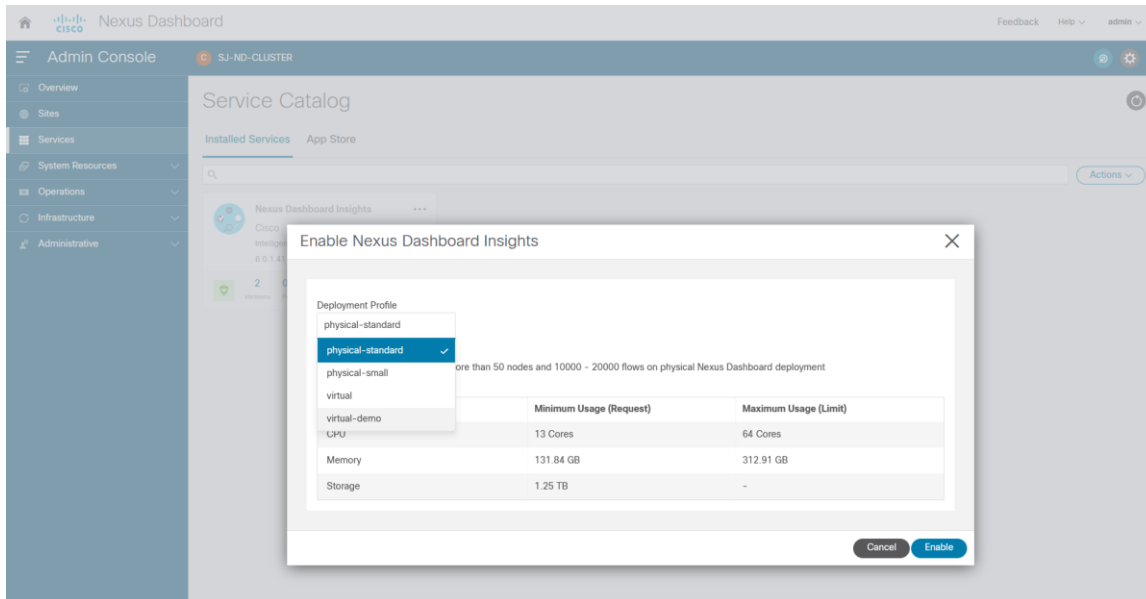
1. On the Nexus Dashboard UI, navigate to Admin Console -> Services -> Installed Services.
2. Click on the “Action” button, then choose “Upload Service”.
3. On the pop-up “Upload Service” screen, choose “Local” for location if the app image file is on your local computer, then choose the file from your local drive. Alternatively, you can choose “Remote” if the app file is on a webserver, then provide the URL for the file.
4. Click on the “Upload” button to start the upload and installation.



**Step 3.** Once Nexus Dashboard Insights is installed, click 'Enable' to get a popup that lets you chose the deployment profile. Select the appropriate profile by reading the description and complying to the Resource Requirement provided for each of the Deployment Profile. Click 'Enable' again to apply certificates and start services required for Nexus Dashboard Insights.







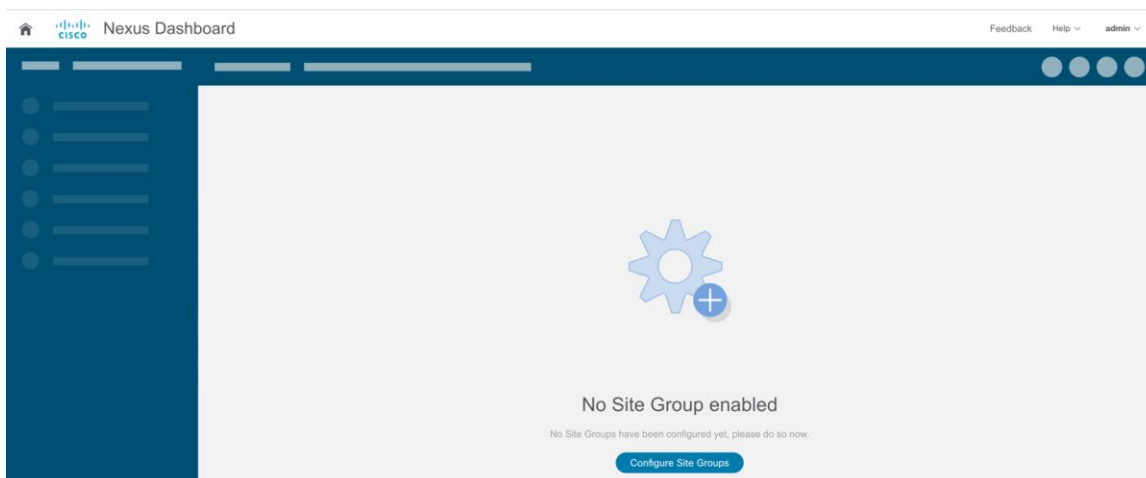
Refer to the detailed guide for Nexus Dashboard Insights Installation App on the Nexus Dashboard: <https://www.cisco.com/c/dam/en/us/td/docs/dcn/ni/5x/user-guide/dcnm/cisco-ni-user-guide-release-511-dcnm.pdf>

## Enable Nexus Dashboard Insights Service for a DCNM Site

This task is performed on the Nexus Dashboard Insights UI.

### Procedure:

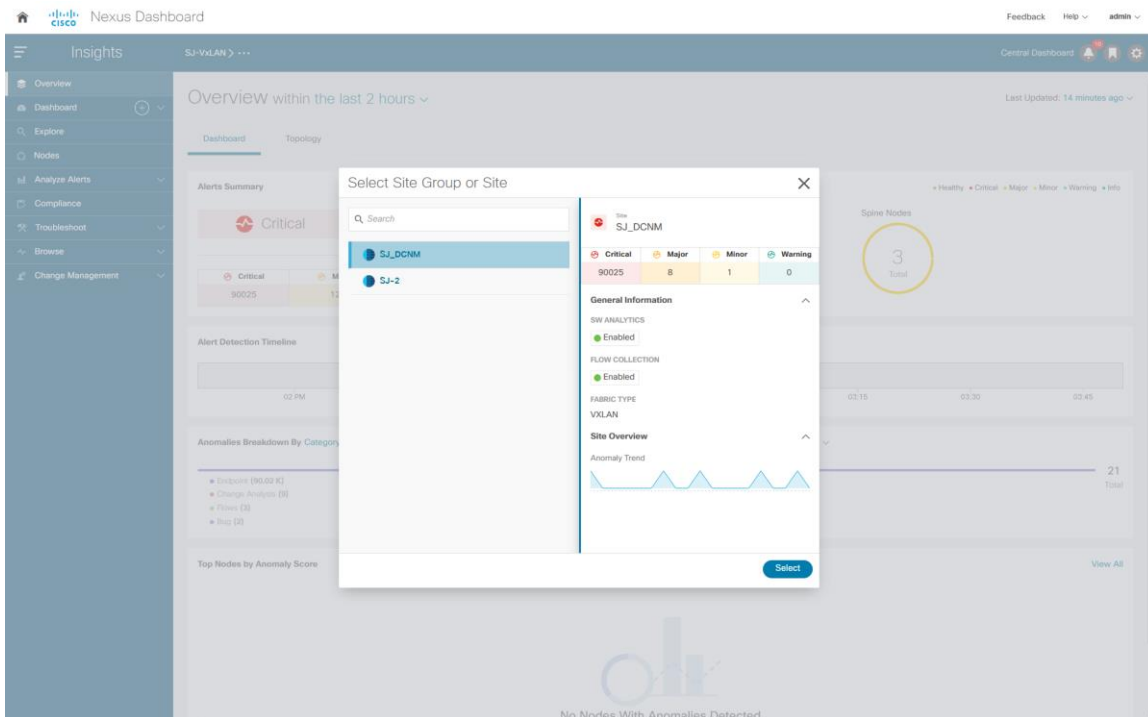
- Step 1.** Create a site group and add the DCNM site to the group.
- Step 2.** If this is the first site group on the Nexus Dashboard Insights, the following screen shows up on the UI to guide the user to add the site group. Click on “Configure Site Group” on the screen to start the process.



Alternative, go to the gearbox on the top-right corner, select “Site Groups” -> “Manage”, then choose “Add New Site Group”.

- Step 3.** Click on ‘Configure Site Groups’ and review the prerequisites for Insights. Click ‘Let’s Get Started > Configure > Add New Site Group’ to provide a ‘Name’ for the Site group. Select ‘Add

**Site(s)** and click **'+Add Member > Select Member'** to select the sites from Nexus Dashboard. Choose the site to be added and click **'Select'**.



**Step 4.** Once the site is added in the Site Group, click 'Enable ' and 'configure' and fill in the fabric type and credentials. Provide the Loopback interface information that is configured in the previous section. This Loopback interface IP address need to be reachable to the Nexus Dashboard Data Network.

## Configuration ✕

### General

Fabric Type\*

Select an Option ▼

Loopback\*

VRP\*

### DCNM Credentials

Username\*

Password\*

i Add switches to the list and specify their credentials only if the switch credentials do not match the default credentials provided above

Switch Credentials

Switch Name	Switch Ip	Switch Username	Switch Password	
				✓ ✕

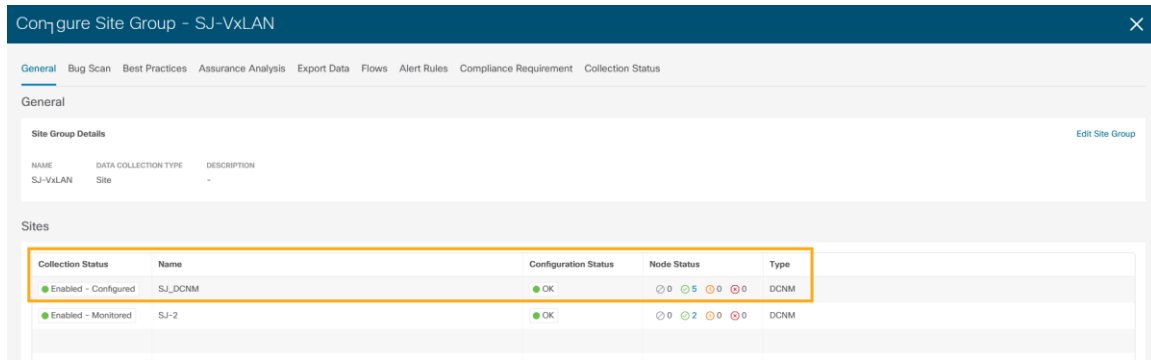
**Step 5.** Click **'Save'** on the pop-up and change the Status to **'Enable'**.

**Step 6.** Click on the menu (...) option **Configure Site Group** to view the sites enabled with Nexus Dashboard Insights services.

The screenshot shows the Cisco Nexus Dashboard Insights interface. The top navigation bar includes 'Insights', 'Overview', 'Dashboard', 'Explore', 'Nodes', 'Analyze Alerts', 'Compliance', 'Troubleshoot', 'Browse', and 'Change Management'. The 'Configure Site Group' menu option is highlighted with a yellow box. The main dashboard displays an 'Alerts Summary' section with a line graph and a table showing 12 Major alerts and 2 Minor alerts. The 'Anomaly Score' section shows 4 Total Leaf Nodes and 3 Total Spine Nodes.

Alert Type	Count
Critical	0
Major	12
Minor	2
Warning	0

Node Type	Total
Leaf Nodes	4
Spine Nodes	3



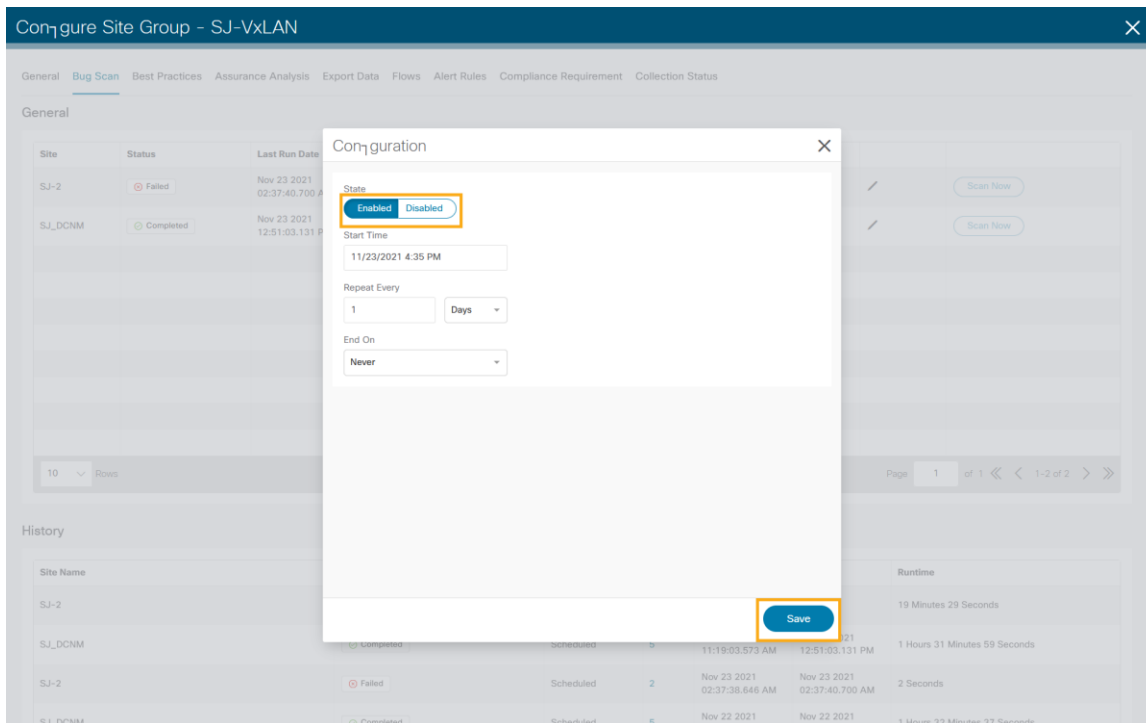
## Enabling Bug Scan, Best Practices and Assurance Analysis

### Procedure:

**Step 1.** After the site-group is configured, to enable Bug Scan feature, click on **Bug Scan > (Edit) > Enabled** and provide parameters for the Start and End time along with frequency of scan.

**Step 2.** Click **Save**.

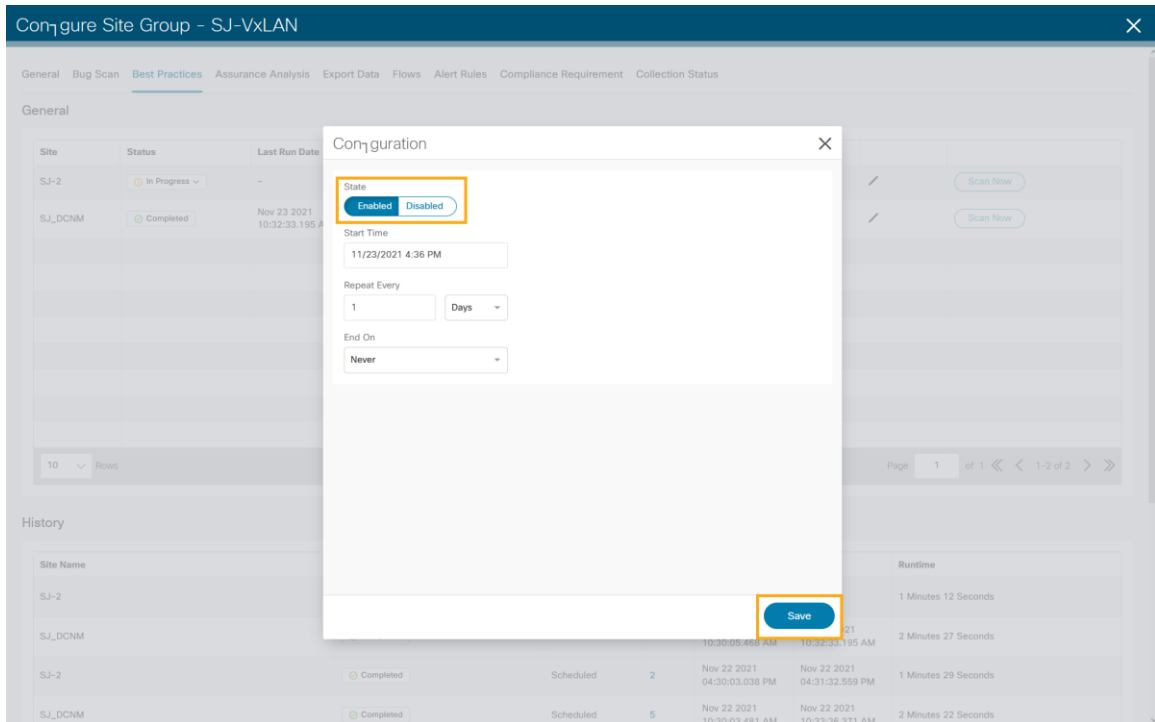
**Step 3.** Click **Run Now** to trigger an instant bug scan.



**Step 4.** To enable Best Practices checks, click on **Best Practices > (Edit) > Enabled** and provide parameters for Start and End time along with frequency of best practice checks.

**Step 5.** Click **Save**.

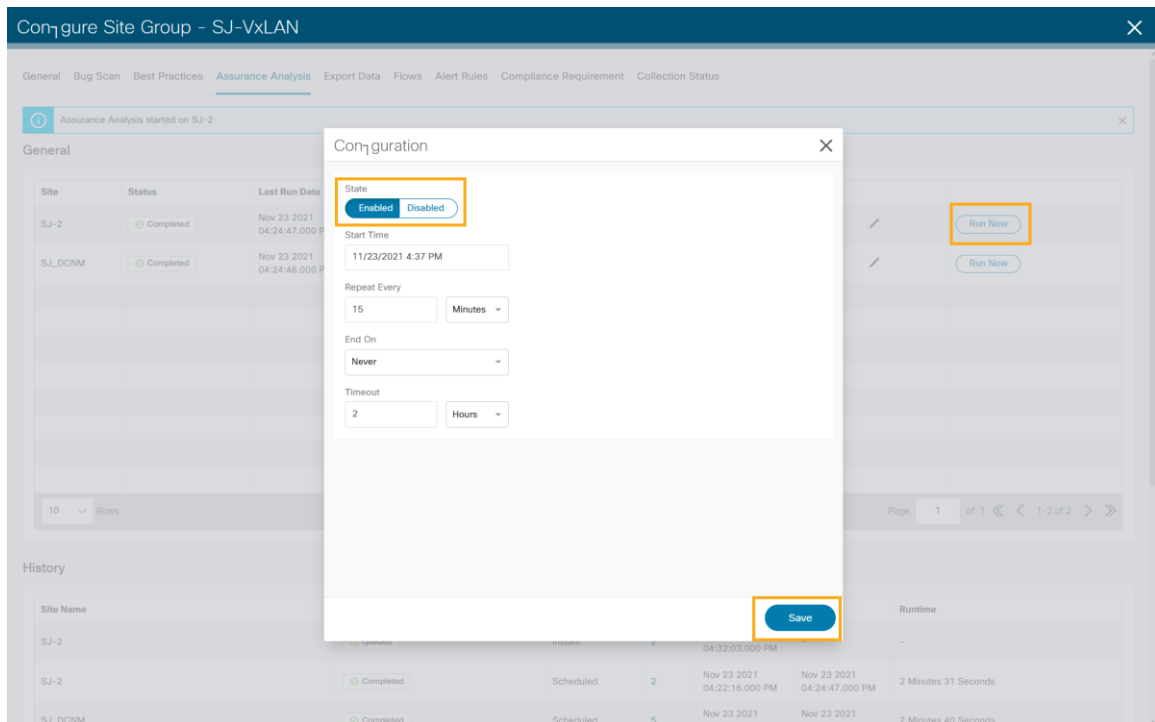
**Step 6.** Click **Run Now** to trigger an instant best practice check in the requested site.



**Step 7.** To enable Assurance Analysis, click on **Assurance Analysis > (Edit) > Enabled**. Provide parameters for Start and End time along with frequency of best practice checks and timeout parameter for how long to run the job.

**Step 8.** Click **Save**.

**Step 9.** Click **Run Now** to trigger an instant Assurance Analysis in the requested site.



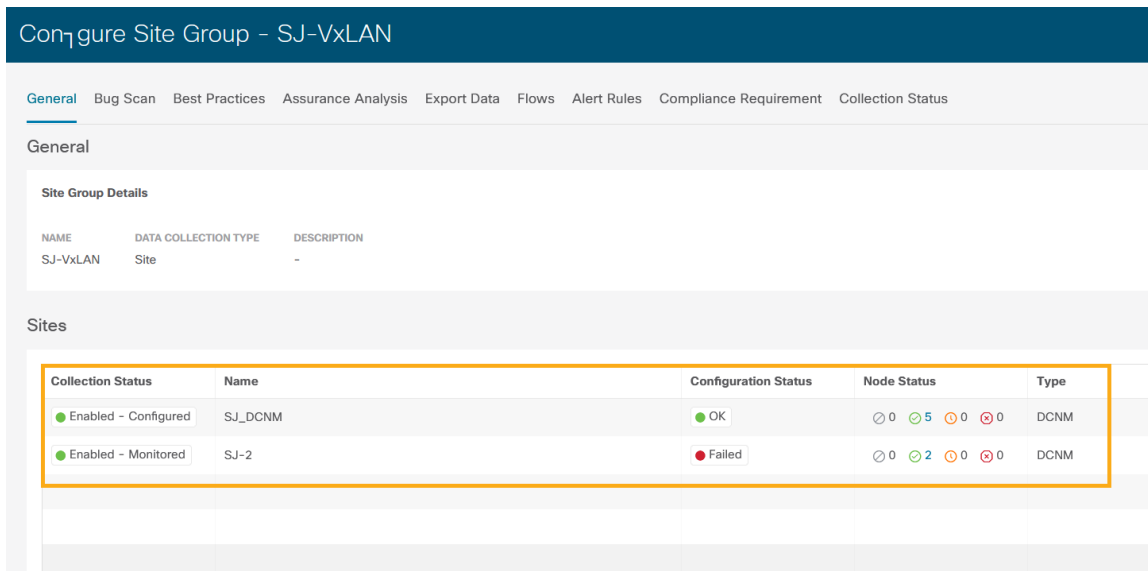
# Enabling Software and Flow Telemetry

Nexus Dashboard Insights provides intuitive and simple software and flow telemetry enabling with DCNM network sites.

## Enable Software Telemetry

### Procedure:

- Step 1.** When configuring the site-group, after the site is enabled and Configuration Status is OK. Nexus Dashboard Insights generates the required configuration per switch to enable software telemetry.
- Step 2.** In DCNM-managed mode, the generated software telemetry configurations are deployed on the switches. However, in DCNM monitored mode, you must configure the switches with the generated configurations.
- Step 3.** To fetch generated configurations to use for DCNM monitored mode network sites, Click on the visual statuses under **Node Status**.



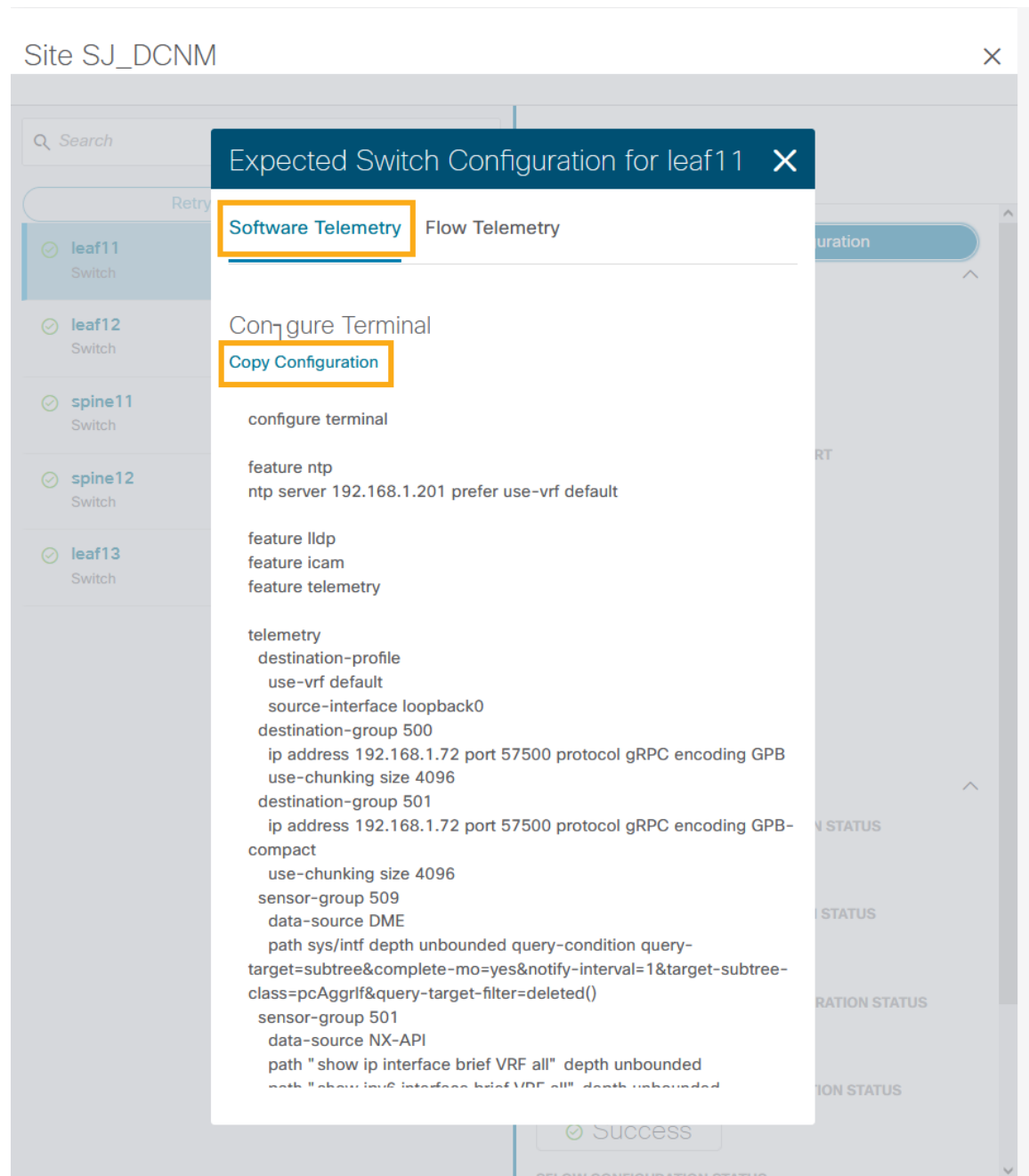
- Step 4.** Click on any switch/node and check for SOFTWARE TELMETRY CONFIGURATION STATUS under Status.

The screenshot shows the Cisco configuration interface for 'Configure Site Group - SJ-VxLAN'. The main window has a 'General' tab selected, showing 'Site Group Details' and a 'Sites' table. The 'Sites' table has the following data:

Collection Status	Name	Configuration Status
Enabled - Configured	SJ_DCNM	OK
Enabled - Monitored	SJ-2	Failed

A modal window titled 'Site SJ\_DCNM' is open, showing a list of switches. The 'View Expected Configuration' button is highlighted with an orange box. The modal also displays 'General Information' for switch 'leaf11' and a 'Status' section with 'Success' indicators for various configuration items.

**Step 5.** To fetch the auto-generated configurations, click on View Expected Configuration -> Software Telemetry tab. To copy the configuration to the clipboard click on Copy Configuration.



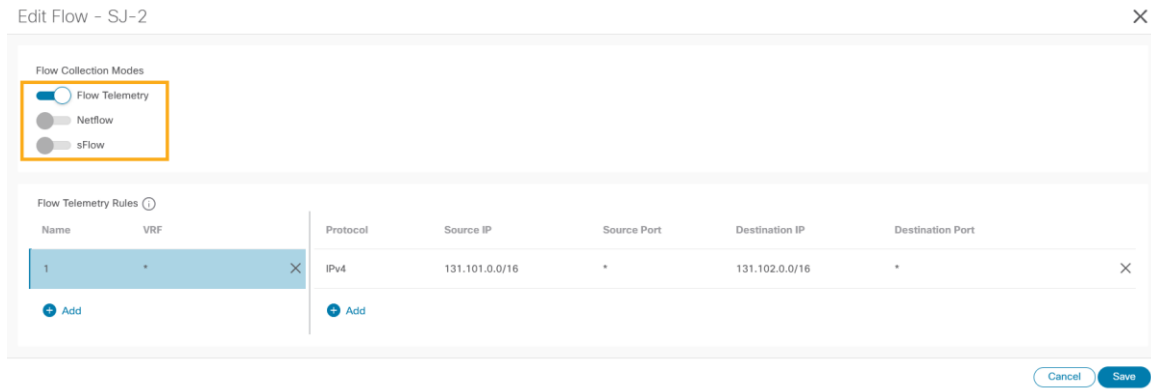
**Step 6.** Repeat the process for each of the switches in the DCNM monitored mode network site.

## Enable Flow Telemetry

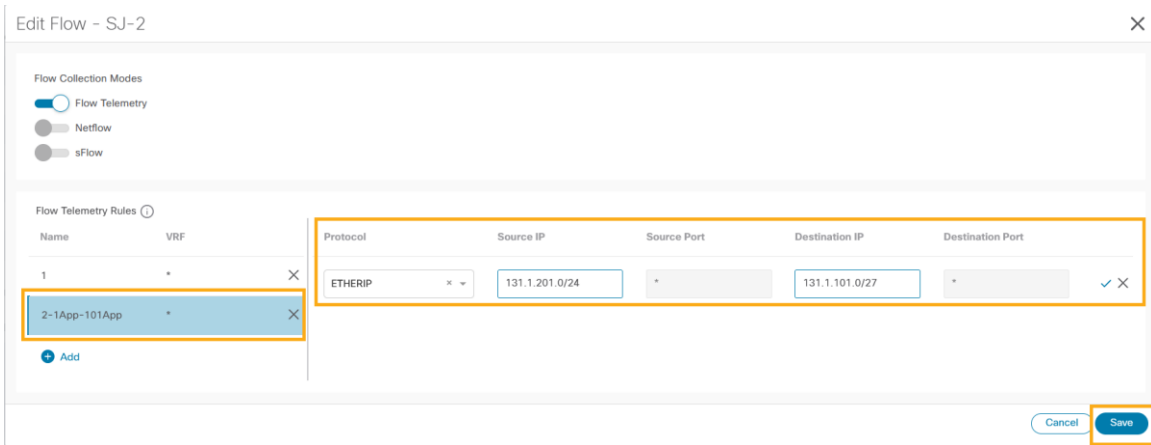
### Procedure:

**Step 1.** In the Configure Site Group page, click **Flows > (Edit)** of the desired site. In the pop-up page,, choose the desired flow collection mode.





**Step 2.** Under the Flow Telemetry Rules, create a rule name and then populate the 5-tuple information



**Step 3.** Click **Save**.

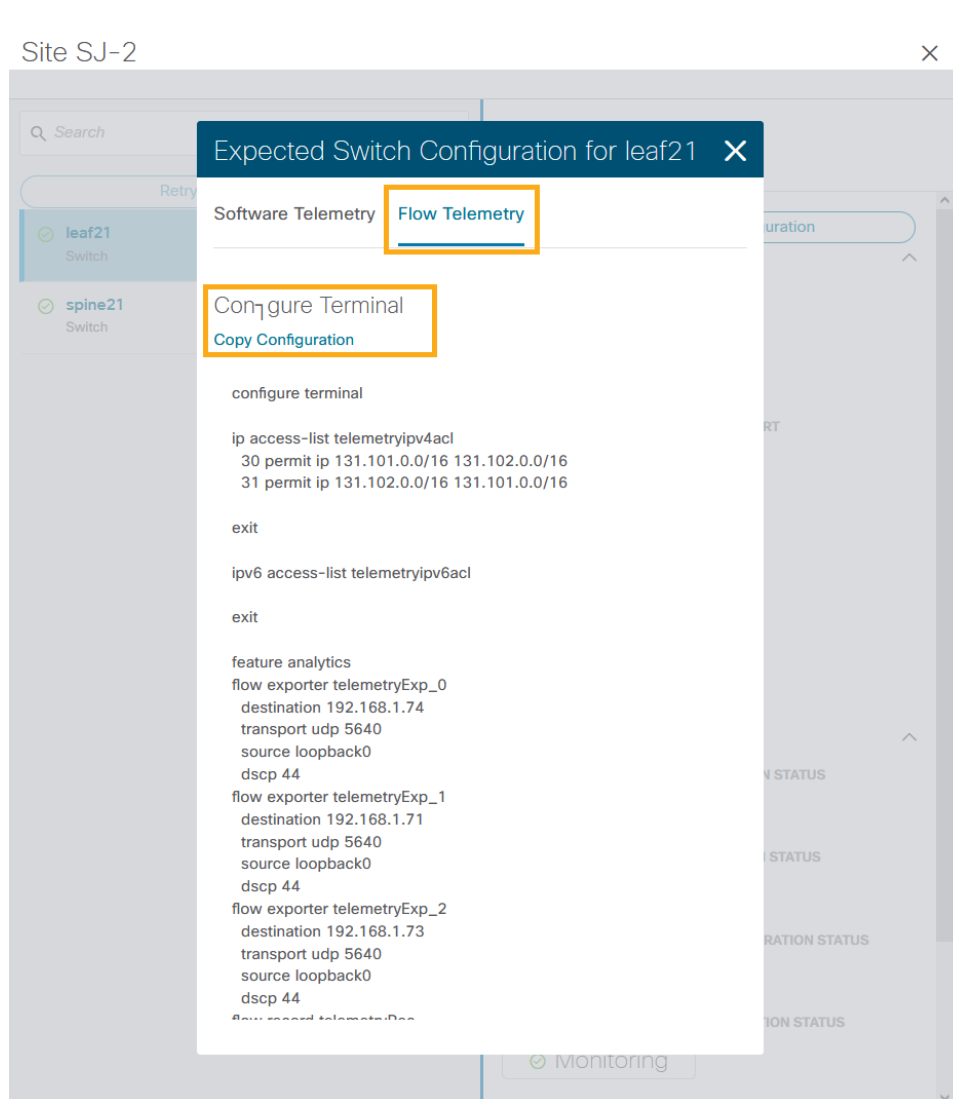
Nexus Dashboard Insights auto-generates the configurations required on the switches in the network sites for enabling the created rules.

**Step 4.** If the network sites are in DCNM-managed mode, the auto-generated flow telemetry configurations are auto deployed on the switches by DCNM. If the sites are in DCNM monitored mode, the required configuration must be deployed to the switches by the users.

**Step 5.** To fetch the auto-generated configuration, in the **Configure Site Group** page, click **General > Site under Collection Status > Node Status > Switch/Node > View Expected Configuration**

The screenshot shows a configuration window for 'Site SJ-2'. On the left, there is a search bar and a list of switches: 'leaf21' (Switch) and 'spine21' (Switch). A 'Retry All Configurations' button is located above the list. The right pane displays the configuration for 'leaf21'. At the top of this pane is a button labeled 'View Expected Configuration', which is highlighted with an orange border. Below this button, the configuration is organized into sections: 'General Information' (with an expand/collapse arrow) and 'Status' (with an expand/collapse arrow). The 'General Information' section lists the following details: SWITCH SERIAL (FDO25070A6N), SWITCH IP (10.23.234.34), SOFTWARE TELEMETRY RECEIVER IP PORT (192.168.1.72:57500), FLOW TELEMETRY RECEIVER IP PORT (192.168.1.74:5640, 192.168.1.71:5640, 192.168.1.73:5640), SWITCH MODEL (N9K-C93240YC-FX2), and SWITCH SOFTWARE VERSION (9.3(8)). The 'Status' section shows three configuration status indicators, all of which are 'Monitoring': SOFTWARE TELEMETRY CONFIGURATION STATUS, FLOW TELEMETRY ACL CONFIGURATION STATUS, and FLOW TELEMETRY ANALYTICS CONFIGURATION STATUS.

**Step 6.** On the pop-up Configuration window, select **Flow Telemetry** tab. Configuration with ACLs per rules created in the previous step are auto-generated along with collector information, bucket IDs, ports, and other parameters such as filters and frequency of information collection.



It copies the configuration to the default clipboard. Use it to configure the switch in the DCNM monitored mode network site.

**Step 7.** Repeat the process for all the switches in the DCNM monitored mode network site.

## Software and Flow Telemetry configuration verifications

### Verifications on the Nexus Dashboard Insights

- In the DCNM-managed mode, the auto-generated configurations by Nexus Dashboard Insights to enable software and flow telemetry is pushed to all switches in the site. The status reflects as success when you click on the status for each switch.

The screenshot displays the Cisco DCNM interface for Site SJ\_DCNM. On the left, a sidebar lists several switches: leaf12, spine11, spine12, leaf13 (highlighted), and leaf11. The main panel shows the configuration for switch leaf13. A 'View Expected Configuration' button is visible at the top. The configuration details are organized into sections: 'General Information' and 'Status'. The 'General Information' section includes fields for SWITCH SERIAL (FDO25070A6S), SWITCH IP (10.23.234.35), SOFTWARE TELEMETRY RECEIVER IP PORT (192.168.1.76:57500), FLOW TELEMETRY RECEIVER IP PORT (192.168.1.74:5640, 192.168.1.71:5640, 192.168.1.73:5640), SWITCH MODEL (N9K-C93240YC-FX2), and SWITCH SOFTWARE VERSION (9.3(8)). The 'Status' section shows four configuration status indicators, all of which are 'Success': SOFTWARE TELEMETRY CONFIGURATION STATUS, FLOW TELEMETRY ACL CONFIGURATION STATUS, FLOW TELEMETRY ANALYTICS CONFIGURATION STATUS, and FLOW TELEMETRY EVENTS CONFIGURATION STATUS. The first two status indicators are highlighted with an orange box.

- In the DCNM monitored mode, although the configurations are auto-generated by Nexus Dashboard Insights to enable software and flow telemetry the configuration on the switches is manual. The status in this case is monitoring.

Site SJ-2 ×

Retry All Configurations

✔ **leaf21**  
Switch

✔ **spine21**  
Switch

Switch  
**leaf21**

View Expected Configuration

**General Information** ^

SWITCH SERIAL  
FDO25070A6N

SWITCH IP  
10.23.234.34

SOFTWARE TELEMETRY RECEIVER IP PORT  
192.168.1.72:57500

FLOW TELEMETRY RECEIVER IP PORT  
192.168.1.74:5640  
192.168.1.71:5640  
192.168.1.73:5640

SWITCH MODEL  
N9K-C93240YC-FX2

SWITCH SOFTWARE VERSION  
9.3(8)

**Status** ^

SOFTWARE TELEMETRY CONFIGURATION STATUS

✔ Monitoring

FLOW TELEMETRY ACL CONFIGURATION STATUS

✔ Monitoring

FLOW TELEMETRY ANALYTICS CONFIGURATION STATUS

✔ Monitoring

**Verifications on the switches in the network site**

Whether the switches are configured manually in DCNM monitored mode or configurations are auto deployed in DCNM-managed mode, switch verification methods remain consistent for the two modes.

**Software Telemetry Configuration Verifications:**

Run ‘show run telemetry’ on each of the switches to match the configuration to Nexus Dashboard Insights generated configuration.

Verify that the correct receiver IP and port are configured on the switch and is connected.

```
spine21# show telemetry transport
```

Session Id	IP Address	Port	Encoding	Transport	Status
0	192.168.1.71	57500	GPB-compact	gRPC	Connected
0	192.168.1.71	57500	GPB	gRPC	Connected

```
Retry buffer Size: 10485760
Event Retry Messages (Bytes): 0
```

```

Timer Retry Messages (Bytes): 0
Total Retries sent: 0
Total Retries Dropped: 0

```

### Hardware Telemetry Configuration Verifications:

Verify that collectors, port and ACL information are configured.

	Expected Running-Configuration	Configured status
Collectors	<pre> flow exporter telemetryExp_0   destination 192.168.1.75   transport udp 5640   source loopback0   dscp 44 flow exporter telemetryExp_1   destination 192.168.1.73   transport udp 5640   source loopback0   dscp 44 flow exporter telemetryExp_2   destination 192.168.1.74   transport udp 5640   source loopback0   dscp 44 </pre>	<pre> spine21# show flow exporter  Flow exporter telemetryExp_0:   Destination: 192.168.1.75   VRF: default      Destination UDP Port 5640   Source Interface loopback0 (20.2.0.2)   DSCP 44 Flow exporter telemetryExp_1:   Destination: 192.168.1.73   VRF: default      Destination UDP Port 5640   Source Interface loopback0 (20.2.0.2)   DSCP 44 Flow exporter telemetryExp_2:   Destination: 192.168.1.74   VRF: default      Destination UDP Port 5640   Source Interface loopback0 (20.2.0.2)   DSCP 44  Feature Prio: Analytics </pre>
Flow Records	<pre> flow record telemetryRec   match ip source address   match ip destination address   match ip protocol   match transport source-port   match transport destination- port   collect counter bytes   collect counter packets </pre>	<pre> spine21# show flow record  Flow record telemetryRec:   No. of users: 1   Template ID: 256   Fields:     match ip source address     match ip destination address     match ip protocol     match transport source-port </pre>

		match transport destination-port
ACL Filters	<pre>ip access-list telemetryipv4acl 31 permit 97 131.1.101.0/27 131.1.201.0/24 30 permit 97 131.1.201.0/24 131.1.101.0/27</pre>	<pre>spine21# show flow filter Filter telemetryFP:   Ipv4 ACL: telemetryipv4acl   Ipv6 ACL: telemetryipv6acl</pre>

## Conclusion

There is a set of prerequisite configuration for a DCNM managed or monitored network site before it can run Nexus Dashboard Insights properly. This white paper discusses the details on such-required configuration. You can use this as a reference to get your DCNM managed or monitored network sites ready for Nexus Dashboard Insights. It also provides the step-by-step guidance on how to add a network site to Nexus Dashboard Insights and how to enable Nexus Dashboard Insights services, such as bug scan, software telemetry, and flow telemetry functions.

## References

### Nexus Dashboard 2.1.x User Guide

<https://www.cisco.com/c/dam/en/us/td/docs/dcn/nd/2x/user-guide/cisco-nexus-dashboard-user-guide-211.pdf>

### Nexus Dashboard Insights 6.0.x User Guide

<https://www.cisco.com/c/dam/en/us/td/docs/dcn/ndi/6x/user-guide/dcnm/cisco-ndi-user-guide-release-601-dcnm.pdf>

### Getting your Cisco ACI Fabrics Ready for Nexus Dashboard Insights

<https://www.cisco.com/c/en/us/td/docs/dcn/whitepapers/getting-aci-ready-for-ndi.html>

---

**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)