Deploy Cisco DNA Center Platform

Overview

To deploy the Cisco DNA Center platform, perform the following steps:

1. Install Cisco DNA Center, Release 2.2.3. For information, see Install Cisco DNA Center Platform, on page 1.

2. Configure the integration settings. For information, see Configure Integration Settings, on page 2.

After deploying the Cisco DNA Center platform, perform the following tasks:

- Review the API prerequisites. For information, see API Prerequisites, on page 2.

- Proceed to **Overview** in the GUI to review the brief feature descriptions to better understand the Cisco DNA Center platform. For information, see About Platform Overview.

- Proceed to **Bundles** in the GUI to enable, configure, and activate any of the bundles necessary for your network. For information, see Bundle Features.

Install Cisco DNA Center Platform

For this release, when performing a fresh install of Cisco DNA Center, you also install the Cisco DNA Center platform. A separate installation procedure for the Cisco DNA Center platform is no longer required. For information about installing Cisco DNA Center, see the Cisco DNA Center Installation Guide.

After the installation, a **Platform** option appears in the **Navigation** slide-in pane in the GUI. Click **Platform** to access the Cisco DNA Center platform. The Cisco DNA Center platform is accessible to a user with a SUPER-ADMIN-ROLE. You can log in and view the Cisco DNA Center platform, as well as perform actions through its GUI after logging in as a user with a SUPER-ADMIN-ROLE. Additionally, as a user with a SUPER-ADMIN-ROLE, you are able to create a custom role with read, write, or deny permissions to various

platform functionality (APIs, bundles, events, and reports). Click the **Menu** icon (≡) and choose **System** > **Users & Roles** > **Role Based Action Access Control** to access this feature.

The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE have more limited and restricted capabilities with Cisco DNA Center platform. For example, these two roles do not permit the user to perform the following actions:

- Generate reports

- Subscribe to events

- Configure event settings

- Enable and configure bundles

- Configure users and roles

Configure Integration Settings

In cases where firewalls or other rules exist between Cisco DNA Center and any third-party apps that need to reach Cisco DNA Center platform, you will need to configure **Integration Settings**. These cases occur when the IP address of Cisco DNA Center is internally mapped to another IP address that connects to the internet or an external network.

Important   After a backup and restore of Cisco DNA Center, you need to access the **Integration Settings** page and update (if necessary) the **Callback URL Host Name** or **IP Address** using this procedure.

Step 1   Click the menu icon (≡) and choose **System** > **Settings** > **System Configuration** > **Integration Settings**.

Step 2   Enter the **Callback URL Host Name** or **IP Address** that the third-party app needs to connect to when communicating with Cisco DNA Center platform.

Note   The **Callback URL Host Name** or **IP Address** is the external facing hostname or IP address that is mapped internally to Cisco DNA Center. Configure the VIP address for a three-node cluster setup.

Step 3   Click the **Apply** button.

What to do next

Review the API prerequisites for Cisco DNA Center platform.

API Prerequisites

To work with the Cisco DNA Center APIs and the Cisco DNA Center platform, you must meet the following API prerequisites.

Supported Programming Language

In order to use the code previews that Cisco DNA Center platform generates, you must use a supported programming language and perform any other necessary language-specific tasks to use the generated code.

For example, to use Python scripts generated by Cisco DNA Center platform, you must install the requests library. You can use pip (Pip Installs Packages) to install using a CLI command:

```
pip install requests
```

Cisco DNA Center platform is able to generate code previews for the following languages in the GUI:

- **Shell**

- **Node - HTTP**

- **Node - Unirest**

- **Node - Request**

- **Python**

- **Ruby**

- **JavaScript**

- **JQuery**

- **PHP**

- **Go**

- **Ansible**

Authentication

The Cisco DNA Center APIs use token-based authentication. You need to log into the APIs using an authentication script (using the supported programming language of your choice). As an example, run the following Python script to log in:

```
def get_token():
    token = requests.post(
        'https://<cluster IP>/api/system/v1/auth/token',
        auth=HTTPBasicAuth(
            username=<username>,
            password=<password>
        ),
    headers={'content-type': 'application/json'},
    verify=False,
     )
     data = token.json()
     return data['Token']
```

Role-Based Access Control Support for Platform

Cisco DNA Center platform supports role-based access control (RBAC), which enables a user with SUPER-ADMIN-ROLE privileges to define custom roles that permit or restrict users access to certain platform features.

Use this procedure to define a custom role and then assign a user to that role.

✎

Note The Cisco DNA Center platform is accessible to a user with a SUPER-ADMIN-ROLE. You can log in and view the Cisco DNA Center platform, as well as perform actions through its GUI after logging in as a user with a SUPER-ADMIN-ROLE. The NETWORK-ADMIN-ROLE and the OBSERVER-ROLE have more limited and restricted capabilities with Cisco DNA Center platform. For example, these two roles do not permit the user to perform the following actions:

- Generate reports

- Subscribe to events

- Configure event settings

- Enable and configure bundles

- Configure users and roles

For more information, see the "Manage Users" chapter in the *Cisco Digital Network Architecture Center Administrator Guide*.

Before you begin

Only a user with SUPER-ADMIN-ROLE permissions can perform this procedure.

Step 1 Define a custom role.

a) Click the menu icon (≡) and choose **System** > **Users and Roles** > **Role Based Access Control**.

b) Click ⊕ **Create New Role**.

The **Create a Role** window appears. If this is your first iteration of RBAC, after you have created the new role, you will be asked to assign users to the new role.

c) Click **Let's Do it**.

If you want to skip this screen in the future, check the **Don't show this to me again** check box.

The **Create a New Role** window appears.

d) Enter a name for the role and then click **Next**.

The **Define the Access** window appears with a list of options.

e) Click > next to **Platform** to expand it.

The following options listed below appear, which allow you to set **Deny** (the default), **Read**, or **Write** permissions for the new role.

- **APIs**: Allows you to view and try out the APIs.

- **Bundles**: Allows you to configure and activate the bundles and ITSM integration settings.

- **Events**: Allows you to configure event settings for email, REST API endpoints, and SNMP traps.

- **Reports**: Allows you to schedule, view, and download reports.

f) Click **Next**.

The **Summary** window appears.

g) Review the summary. If the summary information is correct, click **Create Role**. Otherwise, click **Edit** and make the appropriate changes.

The **Done,** *Role-Name* window appears.

Step 2 To assign a user to the custom role you just created, click **Add Users**.

The **User Management** > **Internal Users** window appears, which allows you to either assign the custom role to an existing user or to a new user.

- To assign the custom role to an existing user, do the following:

  a. In the **Internal Users** window, click the radio button next to the user to whom you want to assign the custom role, and then click **Edit**.

  The **Update Internal User** slide-in pane appears.

  b. From the **Role List** drop-down list, choose the custom role, and then click **Save**.

- To assign the custom role to a new user, do the following:

  a. Click ⊕ Add .

  The **Create Internal User** slide-in pane appears.

  b. Enter the first name, last name, and username in the fields provided.

  c. From the **Role List** drop-down list, choose the custom role to assign to the new user.

  d. Enter the password and then confirm it.

  e. Click **Save**.

Step 3 If you are an existing user who was logged in when the administrator was making changes to your access permissions, you must log out of Cisco DNA Center and then log back in for the new permission settings to take effect.