

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, triangular rays in various shades of blue and cyan, creating a sunburst effect that spreads across the right half of the image.

cisco *Live!*

Let's go

#CiscoLiveAPJC



The bridge to possible

Cisco Catalyst Center-as-Code Network Compliance Use Cases

Gabi Zapodeanu
Principal Technical Marketing Engineer, Cisco Systems
@zapodeanu
DEVNET-2634

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

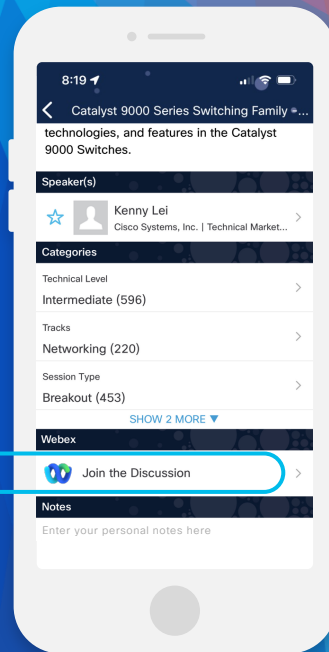
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-2634>

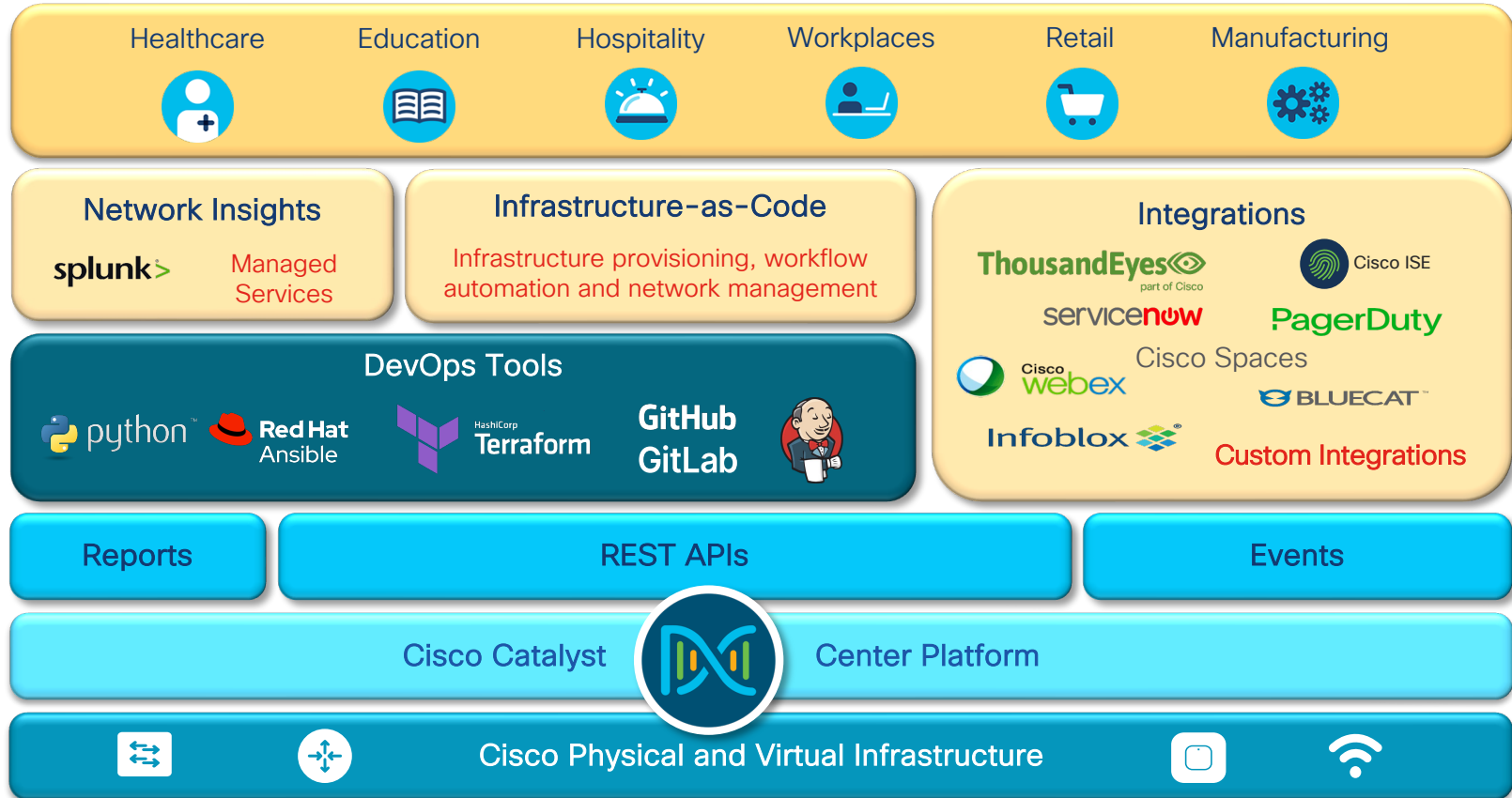
Agenda

- Platforms
- Catalyst Center Compliance
- Custom Network Compliance
- Developer Resources
- Lessons Learned

Agenda

- Platforms
- Catalyst Center Compliance
- Custom Network Compliance
- Developer Resources
- Lessons Learned

Cisco Catalyst Center Platform



Catalyst Center Platform – Overview

Platform / Overview

Welcome to the Cisco DNA Center Platform. Programmatically access your network through Intent APIs, integrate with your preferred IT systems to create end-to-end solutions and add support for multi-vendor devices.

Bundles

Bundles are easy to use feature sets for consuming Intent APIs, integrations, events and notifications. View all the available bundles, enable relevant bundles and customize the configuration preferences to consume events as per your application(s) or IT system(s) needs.

Developer Toolkit

Discover APIs to manage your network, configure integration flows and access network data to analyze, export and visualize complex reports.

Runtime Dashboard

Get insights into API usage, view events published to IT systems such as number of API calls, response time(s), events published, bundles activated etc.

Configurations

View and set global or bundle specific settings to manage your integration configurations and modify event specific settings.

Notifications

Find

BUNDLE UPDATE

The Cisco DNA Center REST API bundle is enabled.

Nov 17 2023, 07:51 pm

[View Details](#) | [Dismiss](#)

BUNDLE UPDATE

A new version of Cisco DNA Center REST API bundle is auto-updated and made available.

Nov 17 2023, 07:50 pm

[View Details](#) | [Dismiss](#)

BUNDLE UPDATE

Cisco DNA Center Automation events for ITSM (ServiceNow) successfully configured.

Version Control

Ref: <https://git-scm.com/>



The screenshot shows the Git website homepage. At the top, it says "git --local-branching-on-the-cheap" with a search bar. Below this, a paragraph describes Git as a "free and open source" distributed version control system. Another paragraph mentions it is "easy to learn" and has a "tiny footprint with lightning fast performance". To the right, there is a diagram showing a branching model with stacks of files and colored arrows representing branches. Below the text, there are four circular icons with labels: "About", "Documentation", "Downloads", and "Community". At the bottom right, there is a section for the "Latest source Release 2.40.1" with a "Download for Mac" button and links for "Mac GUIs", "Tarballs", "Windows Build", and "Source Code".

- Git manages files on your computer, tracking changes, authors, creating diffs. This aspect of file management is called Version Control
- These files can be applications, data or documentation that is part of a software development project
- Git enables collaboration, role-based access and security
- Support for major operating systems – macOS, Linux, Windows, Containers

Notes:

- There are many Version Control Tools – Git, CVS, Apache Subversion, Mercurial, ...
- This presentation will use GitHub
- We will version control applications, and device configurations and network policies

GitHub APIs

<https://docs.github.com/en/rest>

GitHub Docs | Version: Free, Pro, & Team

Search GitHub Docs

← All products

REST API

API Version: 2022-11-28 (latest)

Quickstart Overview

GitHub REST API documentation

To create integrations, retrieve data, and automate your workflows, build with the GitHub REST API.

Start here View all →

Popular

What's new View all →

- Getting started with the REST API
Learn how to use the GitHub REST API.
- Authenticating to the REST API with an OAuth App
Learn about the different ways to authenticate with some examples.
- Best practices for integrators
Build an app that reliably interacts with the GitHub API and provides the best experience for your users.
- Resources in the REST API
- API Versions
- Authenticating to the REST API
- Troubleshooting
- Scripting with the REST API and JavaScript
- Repository archive date in C
April 11
- Delete Organizations with R
March 30
- SAMLIdentity GraphQL object now supports 'read' scope
March 30

- Comprehensive REST API catalog, very well documented
- PyGithub library if developing in Python

Why Cisco Catalyst Center and Version Control?



+

Version Control
Platforms
GitHub

Git Version Control Platforms

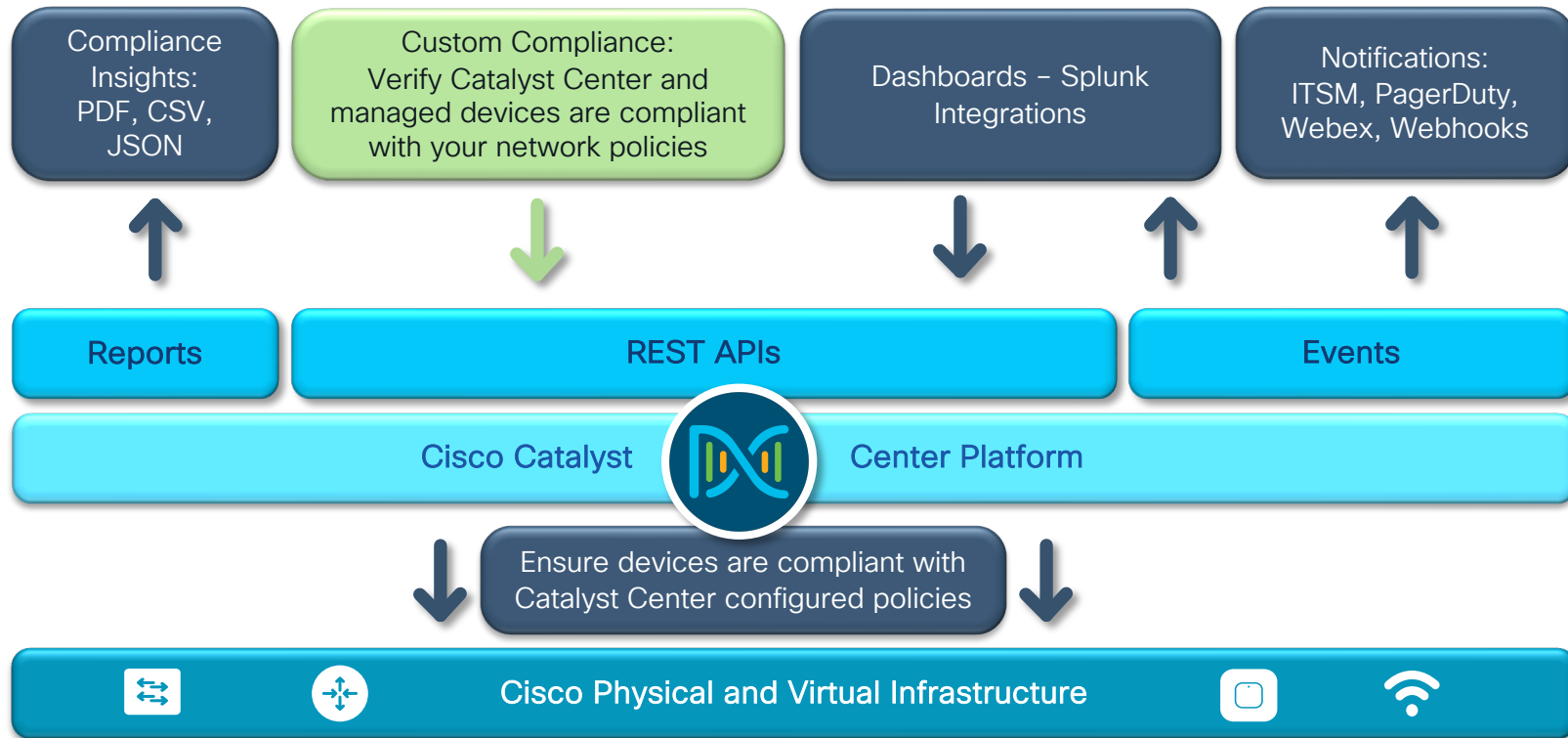
- Track changes of your automation apps, network state, and Cisco Catalyst Center intent configs
- May be used as single source of truth for your network compliance policies
- Robust role-based access for teams and developers

Will support **Cisco Catalyst Center**
Infrastructure-as-Code solutions

Agenda

- Platforms
- Catalyst Center Compliance
- Custom Network Compliance
- Developer Resources
- Lessons Learned

Network Compliance + Custom Compliance



Catalyst Center Network Compliance

Configuration

Power

Fans

SFP Modules

User Defined Fields

Config Drift

REP Rings

Wireless Info

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

COMPLIANCE

Summary

DNA Center

☆ 🔍 🔄 ? 🔔 | 👤 admin ▼

Compliance Summary

View Preference for Acknowledged Violations

No events detected to trigger compliance check [Run Compliance Check](#)

⚠️ EoX - End of Life ⓘ

Compliance last run on: Nov 24th, 2023, 10:10:22 PM

Software : ⚠️ **Compliant**

Hardware : ✅ **Compliant**

Module : ✅ **Compliant**

❌ Network Settings ⓘ

Non-Compliant since Nov 22nd, 2023, 11:23:38 PM

Compliance last run on: Nov 22nd, 2023, 11:23:38 PM

1 General: 1

Open Violations

❌ Startup vs Running Configuration ⓘ

Compliance last run on: Nov 29th, 2023, 08:43:45 PM

3 mins since out of sync

Lines added: 0

Lines removed: 0

Lines modified: 1

❌ Network Profiles ⓘ

Non-Compliant since Aug 18th, 2023, 02:52:22 PM

Compliance last run on: Nov 22nd, 2023, 11:23:39 PM

1 CLI Template: 1

Open Violations

✅ Fabric **BETA** ⓘ

Compliant since Nov 22nd, 2023, 11:24:45 PM

Compliance last run on: Nov 22nd, 2023, 11:24:45 PM

0

Open Violations

✅ Application Visibility ⓘ

Compliant since Nov 22nd, 2023, 11:24:45 PM

Compliance last run on: Nov 22nd, 2023, 11:24:45 PM

0

Open Violations

✅ Software Image ⓘ

Compliant since Oct 25th, 2023, 03:12:18 PM

Compliance last run on: Nov 22nd, 2023, 11:23:38 PM

17.09.04a Golden Image Version

Running Version: 17.9.4a

✅ Critical Security Advisories ⓘ

Compliant since Aug 15th, 2023, 04:24:19 PM

Compliance last run on: Nov 24th, 2023, 08:37:21 PM

0

Notes:

- Not all devices will have the same compliance validations
- Example: Fabric compliance is available only for fabric devices

Startup vs Running Configuration

Configuration

Power

Fans

SFP Modules

User Defined Fields

Config Drift

REP Rings

Wireless Info

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

COMPLIANCE

Summary

DNA Center

☆ 🔍 🔄 ? 🔔 | 👤 admin ▼

Compliance Summary

No events detected to trigger compliance check [Run Compliance Check](#)

🚩 EoX - End of Life ⓘ

Compliance last run on: Nov 24th, 2023, 10:10:22 PM

Software : 🚩 **Compliant**

Hardware : 🟢 **Compliant**

🔴 Network Settings ⓘ

Non-Compliant since Nov 22nd, 2023, 11:23:38 PM

Compliance last run on: Nov 22nd, 2023, 11:23:38 PM

[View Preference for Acknowledged Violations](#)

🔴 Startup vs Running Configuration ⓘ

Compliance last run on: Nov 29th, 2023, 08:43:45 PM

3 mins

since out of sync

Lines added: 0

Lines removed: 0

Lines modified: 1

🟢 Application Visibility ⓘ

Compliant since Nov 22nd, 2023, 11:24:45 PM

Compliance last run on: Nov 22nd, 2023, 11:24:45 PM

0

Open Violations

Compliance Summary / Startup vs Running Configuration

Change History

No. of Lines

12K

10K

8K

6K

4K

2K

0

Aug 20

Aug 27

Sep 03

Sep 10

Sep 17

Sep 24

October

Oct 08

Oct 15

Oct 22

Oct 29

Nov 05

Nov 12

Nov 19

Nov 26

Aug 20 12:00

Aug 27 12:00

Sep 03 12:00

Sep 10 12:00

Sep 17 12:00

Sep 24 12:00

Oct 01 12:00

Oct 08 12:00

Oct 15 12:00

Oct 22 12:00

Oct 29 12:00

Nov 05 12:00

Nov 12 12:00

Nov 19 12:00

Nov 26 12:00

● In Sync

● Out of Sync

Startup Config (1000 Lines) - Nov 29, 2023 08:43 PM

Running Config (1000 Lines) - Nov 29, 2023 08:43 PM

19 !

20 address-family ipv6

21 exit-address-family

22 logging buffered 81920

23 logging console emergencies

24 aaa new-model

25 aaa authentication login default local

19 !

20 address-family ipv6

21 exit-address-family

22 logging buffered 41920

23 logging console emergencies

24 aaa new-model

25 aaa authentication login default local

Sync Device Config, will allow the system to overwrite startup config with running config to make the device configuration compliant.

Cancel

Sync Device Config

CISCO *Live!*

#CiscoLiveAPJC

DEVNET-2634

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

22

Network Settings

Configuration

Power

Fans

SFP Modules

User Defined Fields

Config Drift

REP Rings

Wireless Info

SECURITY

Advisories

FIELD NOTICE

Field Notices

Potential Field

COMPLIANCE

Summary

DNA Center

☆ 🔍 🔄 ? 🔔 | 👤 admin ▾

Compliance Summary

View Preference for Acknowledged Violations

No events detected to trigger compliance check [Run Compliance Check](#)

🚩 EoX - End of Life ⓘ

Compliance last run on: Nov 24th, 2023, 10:10:22 PM

Software : 🚩 **Compliant**

Hardware : 🟢 **Compliant**

Module : 🟢 **Compliant**

🔴 Network Settings ⓘ

Non-Compliant since Nov 22nd, 2023, 11:23:38 PM

Compliance last run on: Nov 22nd, 2023, 11:23:38 PM

1 General: 1

Open Violations

🔴 Startup vs Running Configuration ⓘ

Compliance last run on: Nov 29th, 2023, 08:43:45 PM

3 mins since out of sync

Lines added: 0

Lines removed: 0

Lines modified: 1

🔴 on Visibility ⓘ

Nov 22nd, 2023, 11:24:45 PM

Nov 22nd, 2023, 11:24:45 PM

Compliance Summary / Network Settings

View Preference for Acknowledged Violations

General (1)

Open Violations (1)

Acknowledged Violations (0)

0 Selected [Acknowledge](#)

☐	Model Name ▾	Attribute	Status ⓘ	Intended Value ⓘ	Actual Value ⓘ	Action
☐	Syslog Server/Interface Name	Interface Name	Changed	Loopback0	Loopback1	Acknowledge

17.09.04a

Running Version: 17.9.4a

Golden Image Version

0

CISCO *Live!*

#CiscoLiveAPJC

DEVNET-2634

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

23

Software Image

Configuration

Power

Fans

SFP Modules

User Defined Fields

Config Drift

REP Rings

Wireless Info

SECURITY

Advisories

FIELD NOTICES

Field Notices

Potential Field Notices

COMPLIANCE

Summary

DNA Center

☆ 🔍 🔄 ⓘ 🔔 | 👤 admin ▼

Compliance Summary

[View Preference for Acknowledged Violations](#)

No events detected to trigger compliance check [Run Compliance Check](#)

🚩 EoX - End of Life ⓘ

Compliance last run on: Nov 24th, 2023, 10:10:22 PM

Software : 🚩 **Compliant**

Hardware : 🟢 **Compliant**

Module : 🟢 **Compliant**

🔴 Network Settings ⓘ

Non-Compliant since Nov 22nd, 2023, 11:23:38 PM

Compliance last run on: Nov 22nd, 2023, 11:23:38 PM

1 General: 1

Open Violations

🔴 Startup vs Running Configuration ⓘ

Compliance last run on: Nov 29th, 2023, 08:43:45 PM

3 mins since out of sync

Lines added: 0

Lines removed: 0

Lines modified: 1

🔴 Network Profiles ⓘ

Non-Compliant since Aug 18th, 2023, 02:52:00 PM

Compliance last run on: Nov 22nd, 2023, 11:23:38 PM

1 CLI Template: 1

Open Violations

🟢 Software Image ⓘ

Compliant since Oct 25th, 2023, 03:12:18 PM

Compliance last run on: Nov 22nd, 2023, 11:23:38 PM

17.09.04a Golden Image Version

Running Version: 17.9.4a

🟢 Critical Security Advisories ⓘ

Compliant since Aug 15th, 2023, 04:24:19 PM

Compliance last run on: Nov 24th, 2023, 08:37:21 PM

0

Compliance Summary / Software Image

GOLDEN IMAGE

Image Name cat9k_iosxe.17.09.04a.SPA.bin

Version 17.09.04a.0.6

DEVICE IMAGE

Image Name cat9k_iosxe.17.09.04a.SPA.bin

Version 17.09.04a.0.6

CISCO *Live!*

#CiscoLiveAPJC

DEVNET-2634

© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

25

Compliance Events, Reports and Dashboards

Webex Notifications

DNAC_Notifications 9:13 PM

Cisco DNA Center Notification

Source DNA: 10.93.141.45
Center IP: 5
Severity: INFO
Category: INFO
Timestamp: 2023-11-30 05:13:46
Issue Name: Device config collection event
Issue Description: Shows a config drift event across the selected list of devices : 6a812b05-1c89-4d0a-a4d3-94ec5e5a7a57

Cisco DNA Center Issue

Device config collection event (3)

Last 6 hours ▾

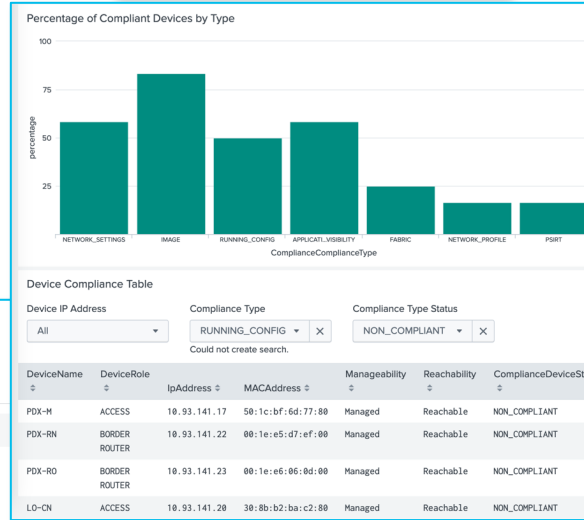
Search Table

Retry

Last In-Event Flow

Event Id	Source	Destination	ITSM Workflow	DNA Event Status	ITSM Status	ITSM Id	ITSM Link
☐ ac5dfdd0-bfc7-4858-bb26-8392ec72b0e9	ServiceNow	Cisco DNA Center	Incident	NA	New	INC0016474	https://ven03092.service-now.com/nav_to.do?uri=incident.do?sys_id=ca
☐ 2a13a479-4dfe-4729-87b6-fdd8ba40ba7b	ServiceNow	Cisco DNA Center	Incident	NA	New	INC0016475	https://ven03092.service-now.com/nav_to.do?uri=incident.do?sys_id=f1
☐ 4a72c5c4-ba40-424e-8524-2ec691a5ed09	ServiceNow	Cisco DNA Center	Incident	NA	New	INC0016476	https://ven03092.service-now.com/nav_to.do?uri=incident.do?sys_id=e5

Splunk Dashboard



Report

DNA Center

Reports / Compliance Report - Network Device Compliance - Nov 29 2023 at 17:12

Nov 29, 2023 at 5:13 pm

Generated Reports (1) ▾

```
{
  "root": {
    "Compliance": {
      "0": {
        "rownum": 3
      },
      "1": {
        "hostname": "LO-BN"
      },
      "2": {
        "family": "Switches and Hubs"
      },
      "3": {
        "type": "Cisco Catalyst 9300 Switch"
      },
      "4": {
        "managementIpAddress": "10.93.141.28"
      },
      "5": {
        "complianceStatus": "NON_COMPLIANT"
      },
      "6": {
        "IMAGE": "NON_COMPLIANT"
      },
      "7": {
        "RUNNING_CONFIG": "COMPLIANT"
      },
      "8": {
        "PSIRT": "NON_COMPLIANT"
      },
      "9": {
        "NETWORK_PROFILE": "NON_COMPLIANT"
      },
      "10": {
        "NETWORK_SETTINGS": "NON_COMPLIANT"
      },
      "11": {
        "EOX": "COMPLIANT"
      }
    }
  }
}
```

ServiceNow Incidents

Catalyst Center Compliance APIs

Platform / Developer Toolkit

☆ 🔍 ↻ ? 🔔 | 👤 admin ▾

APIs

Integration Flows

Event Notifications

🔍 Search

Authentication

Cisco DNA Center System >

Connectivity >

Ecosystem Integrations >

Event Management

Integrations >

Know Your Network ▾

Applications

Clients

Compliance

Devices

EoX

Issues

Security Advisories

Sensors

Sites

Topology

Method	Name	Description	
GET	Get Compliance Detail Count ^{Intent}	Return Compliance Count Detail	
GET	Compliance Details of Device ^{Intent}	Return compliance detailed report for a device	
POST	Commit device configuration ^{Intent}	This operation would commit device running configuration to startup by issuing "write memory" to device	/network-device-config/write-memory ... ▾
GET	Device Compliance Status ^{Intent}	Return compliance status of a device.	/compliance/\${deviceUuid} ... ▾
GET	Get config task details ^{Intent}	Returns a config task result details by specified id	/network-device-config/task ... ▾
GET	Get Compliance Status ^{Intent}	Return compliance status of device(s).	/compliance ... ▾
GET	Get Compliance Status Count ^{Intent}	Return Compliance Status Count	/compliance/count ... ▾
GET	Get Compliance Detail ^{Intent}	Return Compliance Detail	/compliance/detail ... ▾
POST	Run Compliance ^{Intent}	Run compliance check for device(s).	/compliance/ ... ▾

- The compliance APIs support:
- Trigger a compliance check
 - Retrieve the task details
 - Get counts for all compliance checks
 - Status, summary and details for device compliance

Get Compliance Details API

Includes all the compliance validations for all devices
Filters may be used
Pagination likely required

Try 'Get Compliance Detail '

Method: **GET** Public URL :https://10.93.141.45/dna/intent/api/v1/compliance/detail

PARAMETERS

QUERY PARAMETERS

☐ Select All

☐ complianceType ⓘ

☐ complianceStatus ⓘ

☐ deviceUid ⓘ

☒ offset ⓘ
1

☒ limit ⓘ
500

Reset Run

Response Headers Status Code: 200

```
1 {
2   "response": [
3     {
4       "deviceUid": "20937bce-b8d8-42c2-b3a0-08cda93fae1e",
5       "complianceType": "RUNNING_CONFIG",
6       "status": "COMPLIANT",
7       "state": "SUCCESS",
8       "lastSyncTime": 1700707248485,
9       "lastUpdateTime": 1700724218678
10    },
11    {
12      "deviceUid": "db05ad49-2c8d-4094-9df6-3a03f9b28069",
13      "complianceType": "PSIRT",
14      "status": "NON_COMPLIANT",
15      "state": "SUCCESS",
16      "lastSyncTime": 1700887041491,
17      "lastUpdateTime": 1700887041491
18    },
19    {
20      "deviceUid": "01f7cdf2-2298-42c7-bb74-dc68e3c3a051",
21      "complianceType": "EOX",
22      "status": "COMPLIANT_WARNING",
23      "state": "SUCCESS",
24      "lastSyncTime": 1700287827198,
25      "lastUpdateTime": 1701359318734
26    },
27    {
28      "deviceUid": "657008e6-6160-481e-aa7d-a5b3513b1f7c",
29      "complianceType": "IMAGE",
30      "status": "COMPLIANT",
```

Device Compliance Details API

Includes compliance checks details for a device
Device Id param required
Filters may be used

Try 'Compliance Details of Device'

Method: **GET** Public URL : <https://10.93.141.45/dna/intent/api/v1/compliance/6a612b05-1c89-4d0a-a4d3-94ec5e5a7a57/detail>

PARAMETERS

PATH PARAMETERS

deviceUuid*

6a612b05-1c89-4d0a-a

QUERY PARAMETERS

☐ Select All

☐

category

☒

complianceType
NETWORK_PROFILE

☐

diffList

false

Reset

Run

Response

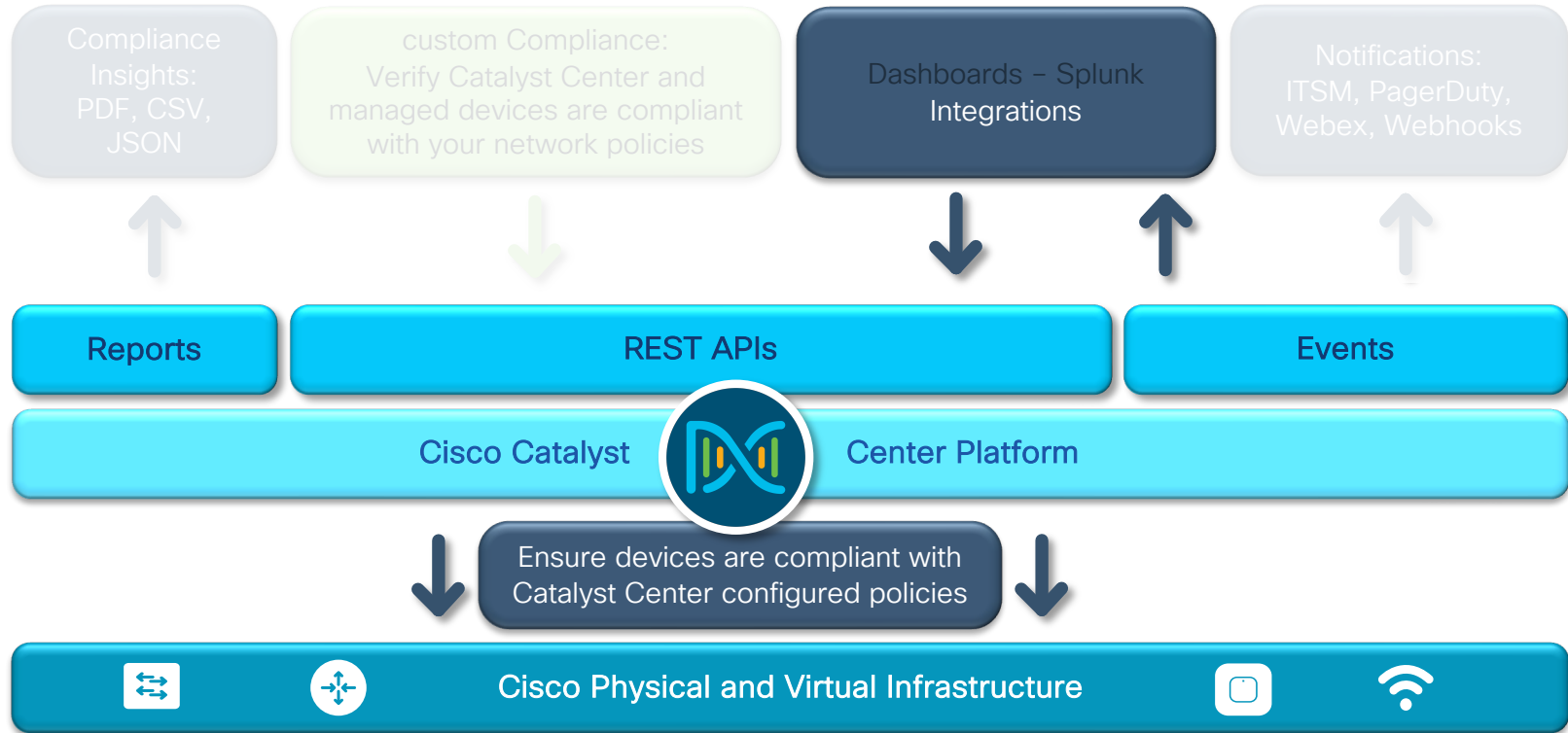
Headers

Status Code: 200

```
1 {
2   "response": [
3     {
4       "deviceUuid": "6a612b05-1c89-4d0a-a4d3-94ec5e5a7a57",
5       "complianceType": "NETWORK_PROFILE",
6       "status": "NON_COMPLIANT",
7       "state": "SUCCESS",
8       "lastSyncTime": 1692395542784,
9       "lastUpdateTime": 1701338019125,
10      "sourceInfoList": [
11        {
12          "name": "73aab375-30ef-4a41-90de-a110a072ea12",
13          "nameWithBusinessKey": "73aab375-30ef-4a41-90de-a110a072ea12-logging_profile",
14          "sourceEnum": "NETWORK_PROFILE",
15          "type": "CLI_TEMPLATE",
16          "appName": "CLI Template",
17          "count": 1,
18          "ackStatus": "UNACKNOWLEDGED",
19          "businessKey": {
20            "resourceName": "73aab375-30ef-4a41-90de-a110a072ea12",
21            "businessKeyAttributes": {
22              "profileName": "logging_profile",
23              "owningEntityId": "59fe66a2-23c5-4368-bf11-17f512182e3b"
24            },
25            "otherAttributes": {
26              "name": "rfs"
27            },
28            "cfsAttributes": {
29              "displayName": "TemplateCompliance",
30              "appName": "CLI Template",
31              "description": "This is the description of CLI Template",

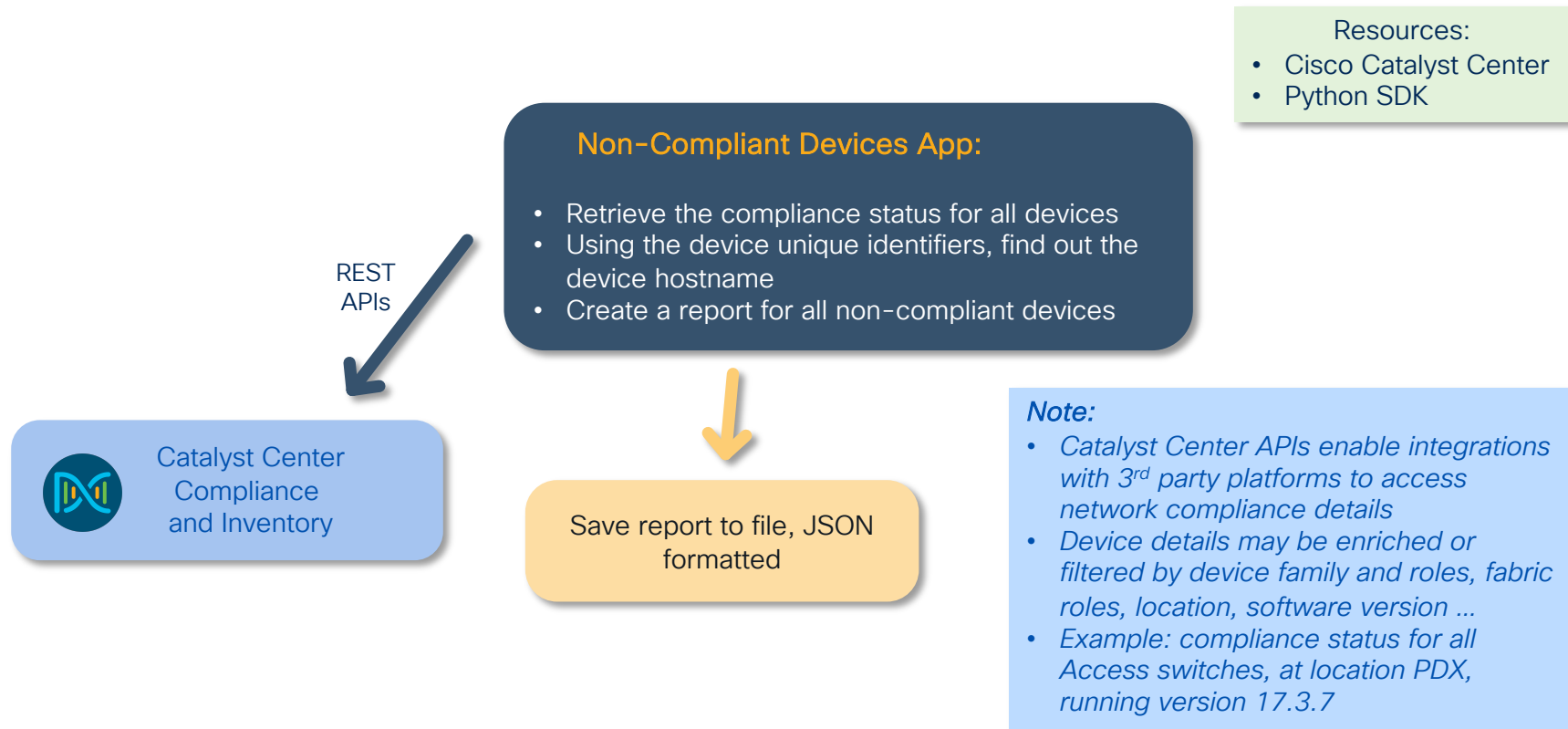
```


Network Compliance Integrations



Catalyst Center Non-Compliant Devices

App Workflow



Compliance App Python Code

```
65
66 get_compliance_response = catalyst_center_api.compliance.get_compliance_detail()
67 network_compliance_info = get_compliance_response['response']
68 logging.info(' Collected Catalyst Center network compliance state')
69
70 # sort the list of compliance status, by device Id
71 network_compliance = sorted(network_compliance_info, key=lambda x: x['deviceUuid'])
72
73 # identify all compliance checks in environment
74 compliance_type = []
75 for item in network_compliance:
76     item_compliance = item['complianceType']
77     if item_compliance not in compliance_type:
78         compliance_type.append(item_compliance)
79
80 logging.info(' Type of compliance checks: ' + json.dumps(compliance_type))
81
82 # create report for non-compliant devices for each compliance type
83 compliance_report = {}
84 for item in compliance_type:
85     compliance_report.update({item: []})
86
87 # loop through each item in compliance and append to report, to the specific category
88 for item in network_compliance:
89     if item['status'] == 'NON_COMPLIANT':
90         item_compliance = item['complianceType']
91         device_id = item['deviceUuid']
92         device_info = catalyst_center_api.devices.get_device_by_id(id=device_id)
93         device_hostname = device_info['response']['hostname']
94         compliance_report[item_compliance].append(device_hostname)
95
96 logging.info(' Non-compliant devices report completed: ')
```

Get all devices
compliance and **sort**
output

Identify all types of
compliance types

Create non-compliant
devices report by
identifying the device
hostnames

Notes:

- Only two API endpoints called
- **Sorting the compliance API response by device Id, minimizes the number of API calls made to identify the device hostname**

Compliance App Run

```
INFO:root: Application "catalyst_center_compliance.py" Start, 2023-12-03 15:37:30
INFO:root: Collected Catalyst Center network compliance state
INFO:root: Type of compliance checks: [
```

```
    "EOX",
    "NETWORK_SETTINGS",
    "PSIRT",
    "IMAGE",
    "RUNNING_CONFIG",
    "APPLICATION_VISIBILITY",
    "NETWORK_PROFILE",
    "FABRIC"
]
```

```
INFO:root: Non-compliant de
```

```
INFO:root: {
  "EOX": [
    "LO-EDGE"
  ],
  "NETWORK_SETTINGS": [
    "PDX-M",
    "LO-CN",
    "LO-EDGE",
    "PDX-CORE1",
    "LO-BN"
  ],
```

```
    "IMAGE": [
      "LO-BN"
    ],
    "RUNNING_CONFIG": [
      "PDX-RO",
      "PDX-M",
      "NYC-RO",
      "SP",
      "PDX-RN",
      "LO-CN"
    ],
    "APPLICATION_VISIBILITY": [],
    "NETWORK_PROFILE": [
      "NYC-ACCESS",
      "PDX-STACK",
      "PDX-M",
      "PDX-RN",
      "LO-CN",
      "LO-EDGE",
      "PDX-CORE1",
      "LO-BN"
    ],
    "FABRIC": []
  ]
}
```

```
INFO:root: Saved the non-compliant devices report to file "compliance_report.json"
```

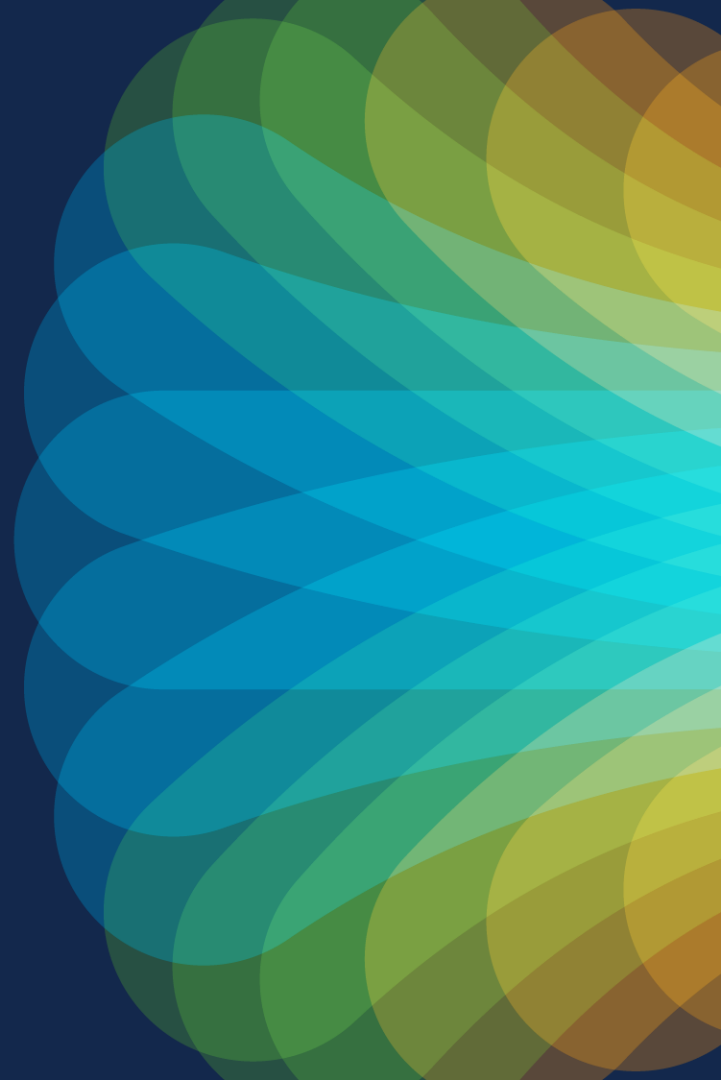
```
INFO:root: Non-compliant Core devices report completed:
INFO:root: {
  "EOX": [],
  "NETWORK_SETTINGS": [
    "PDX-CORE1"
  ],
  "PSIRT": [
    "PDX-CORE1"
  ],
  "IMAGE": [],
  "RUNNING_CONFIG": [],
  "APPLICATION_VISIBILITY": [],
  "NETWORK_PROFILE": [
    "PDX-CORE1"
  ],
  "FABRIC": []
}
```

```
INFO:root: Saved the Core non-compliant devices report to file "compliance_report.json"
INFO:root: End of Application "catalyst_center_compliance.py" Run: 2023-12-03 15:37:47
```

Use this file for:

- ITSM change management
- Remediation IaC workflows

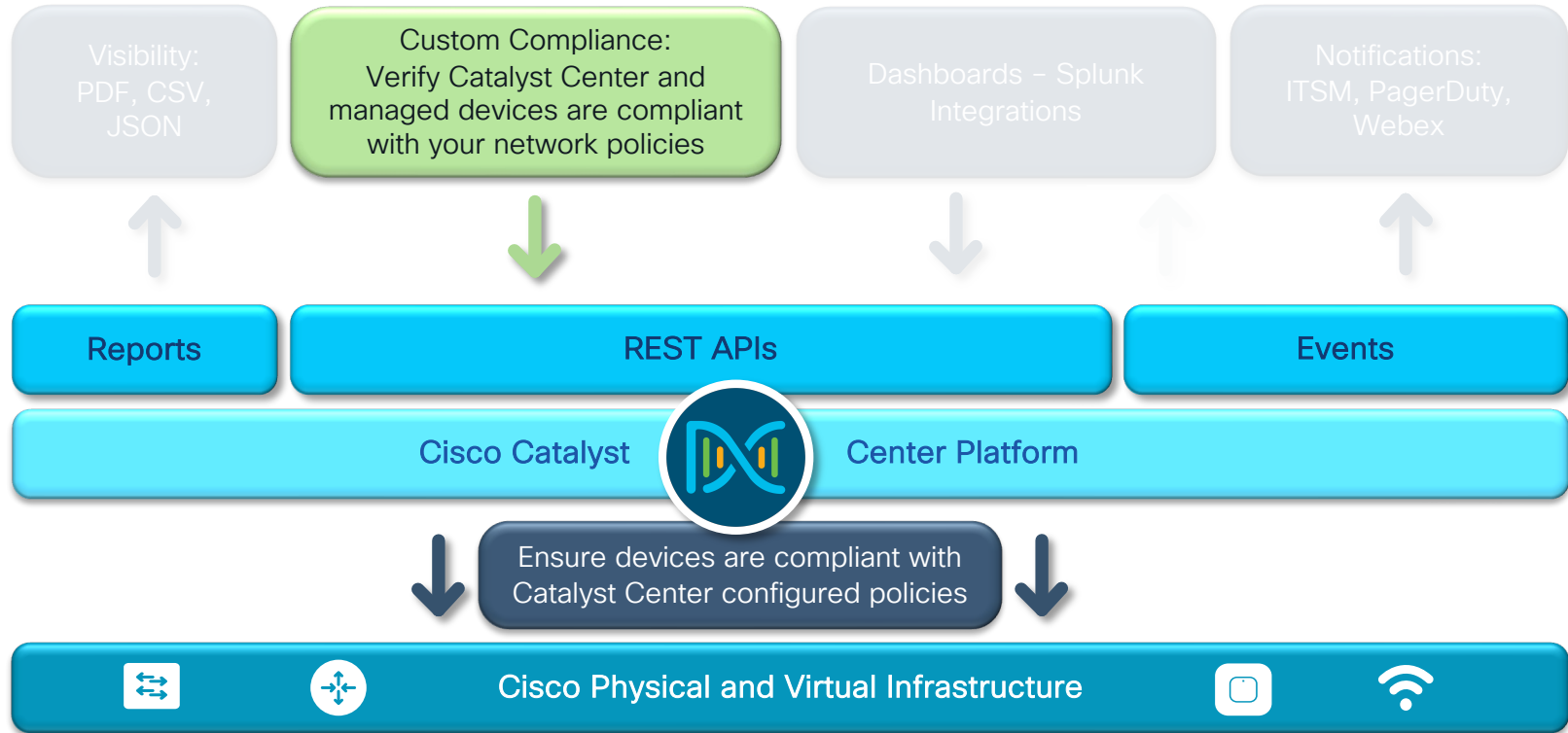
Catalyst Center Compliance Demo



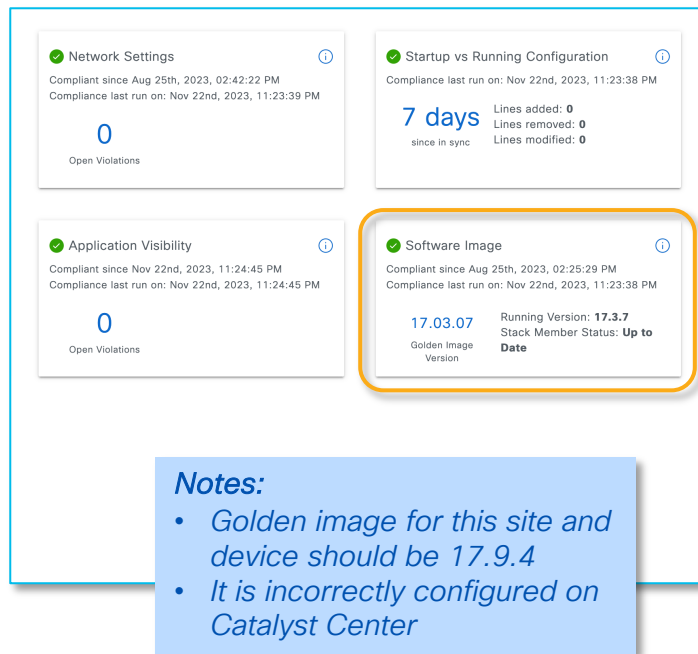
Agenda

- Platforms
- Catalyst Center Compliance
- Custom Network Compliance
- Developer Resources
- Lessons Learned

Custom Network Compliance



Custom Network Compliance



- The device is compliant with Catalyst Center network settings and runs the golden image
- Is it compliant with your network policies?
- For a continuous compliance validation with corporate policies, we need to:
 - Verify intent is configured correctly on Catalyst Center
 - Catalyst Center network compliance will validate devices are compliant with intent

Custom Network Compliance

App Workflow

Resources:

- Cisco Catalyst Center
- Python SDK
- GitHub Repo



REST
APIs



Custom Network Compliance App:

- Retrieve the compliance intent from GitHub
- Verify the Catalyst Center configurations meet the defined intent
- Create a report, save to file, option to push to GitHub

REST
APIs



Catalyst Center
Compliance, Inventory,
Settings, Configs



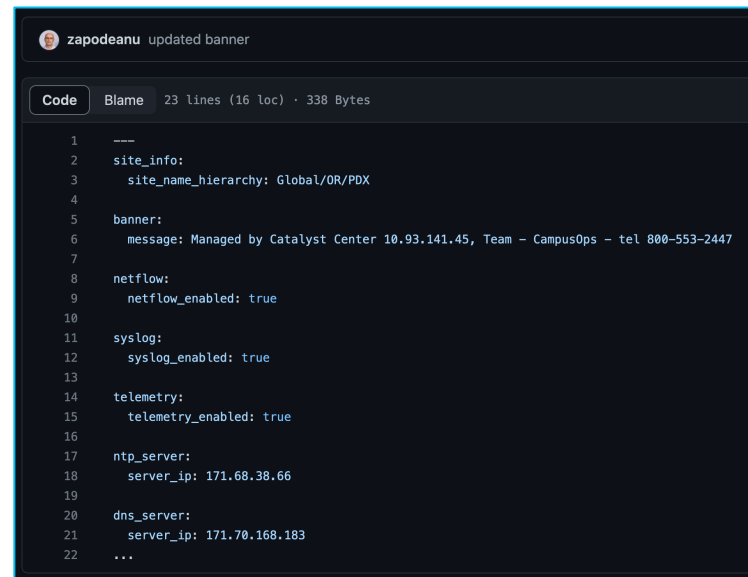
Save report, JSON
formatted, optionally push to
3rd party platform

Notes:

- *Supports multi-Catalyst Center intent compliance validations*
- *App developed by developer + network engineer*

Custom Network Settings Compliance

- Pull from GitHub the file with the custom network settings
- Parse the banner message, NTP and DNS servers' intent configuration
- Verify if intent matches the Catalyst Center configurations



The screenshot shows a GitHub code viewer interface. At the top, it says 'zapodeanu updated banner'. Below that, there are tabs for 'Code', 'Blame', and a summary '23 lines (16 loc) · 338 Bytes'. The code is a JSON configuration file with the following content:

```
1  ---
2  site_info:
3    site_name_hierarchy: Global/OR/PDX
4
5  banner:
6    message: Managed by Catalyst Center 10.93.141.45, Team - CampusOps - tel 800-553-2447
7
8  netflow:
9    netflow_enabled: true
10
11 syslog:
12   syslog_enabled: true
13
14 telemetry:
15   telemetry_enabled: true
16
17 ntp_server:
18   server_ip: 171.68.38.66
19
20 dns_server:
21   server_ip: 171.70.160.183
22 ...
```

Catalyst Center Network Settings API

Try 'Get Network V2'

Method: **GET** Public URL :<https://10.93.141.45/dna/intent/api/v2/network>

PARAMETERS

QUERY PARAMETERS

☒ siteId* ⓘ
15628823-b52e-4564-ε

Reset

Run

Response

Headers

Status Code: 200

```
1 {
2   "response": [
3     {
4       "instanceType": "banner",
5       "instanceUid": "30352a4a-3d2e-48c5-9136-609e7d75f3d9",
6       "namespace": "global",
7       "type": "banner.setting",
8       "key": "device.banner",
9       "version": 37,
10      "value": [
11        {
12          "bannerMessage": "This device is managed by Catalyst Center 10.93.141.45",
13          "retainExistingBanner": false
14        }
15      ],
16      "groupUid": "15628823-b52e-4564-a39c-36a9d45dc180",
17      "inheritedGroupUid": "-1",
18      "inheritedGroupName": "Global"
19    },
20    {
21      "instanceType": "timezone",
22      "instanceUid": "4d1ba8e9-70ee-4b8b-8412-a2ad6ae9c4ab",
23      "namespace": "global",
24      "type": "timezone.setting",
25      "key": "timezone.site",
26      "version": 7,
```

The response includes network settings for banner, AAA, NTP, DNS servers, times zone, SYSLOG and NetFlow config, ...

GitHub APIs

```
62
63 def get_private_repos(username, github_token):
64     """
65     This function will return private repos for user referred by the User Access Token
66     :param username: user for which to return the repos
67     :param github_token: Personal access token for user
68     :return: repos_list
69     """
70     url = GITHUB_URL + '/user/repos?type=private'
71     header = {'Accept': 'application/vnd.github+json', 'Authorization': 'token ' + GITHUB_TOKEN}
72     response = requests.get(url, headers=header, verify=True)
73     response_json = response.json()
74     repos_list = []
75     for repo in response_json:
76         repos_list.append(repo['name'])
77     return repos_list
78
```

```
96
97 def get_repo_file_content(username, repo_name, file_name):
98     """
99     This function will return the content of the file from the repo
100     :param username: GitHub username
101     :param repo_name: GitHub repo
102     :param file_name: file name
103     :return: return the file content
104     """
105     url = GITHUB_URL + '/repos/' + username + '/' + repo_name + '/contents/' + file_name
106     header = {'Authorization': 'token ' + GITHUB_TOKEN}
107     response = requests.get(url, headers=header)
108     response_json = response.json()
109     file_content = response_json['content']
110     file_content_encoding = response_json.get('encoding')
111     if file_content_encoding == 'base64':
112         file_content = base64.b64decode(file_content)
113     return file_content
114
```

Note:

- Verify which GitHub APIs provide private repos info

zapodeanu updated banner

Code Blame 23 lines (16 loc) · 338 Bytes Code 55% faster with GitHub Copilot

```
1 ---
2 site_info:
3     site_name_hierarchy: Global/OR/PDX
4
5 banner:
6     message: Managed by Catalyst Center 10.93.141.45, Team - Campus0ps - tel 800-553-2447
7
8 netflow:
9     netflow_enabled: true
10
11 syslog:
12     syslog_enabled: true
13
14 telemetry:
15     telemetry_enabled: true
16
17 ntp_server:
18     server_ip: 171.68.38.66
19
20 dns_server:
21     server_ip: 171.70.168.183
22 ...
```

- Get all repos, including the private repos, for user
- Retrieve the intent configuration file, in this case for network settings

Network Settings Compliance App Python Code

```
66
67 # get all repos for user
68 repos = github_api.get_private_repos(username=GITHUB_USERNAME, github_token=GITHUB_TOKEN)
69
70 # verify if repo exists
71 if GITHUB_REPO not in repos:
72     logging.info(' Repo ' + GITHUB_REPO + ' not found!')
73     return
74 logging.info(' Repo ' + GITHUB_REPO + ' found!')
75
76 # get the network settings intent file
77 intent_network_settings = github_api.get_repo_file_content(username=GITHUB_USERNAME, repo_name=GITHUB_REPO,
78                                                         file_name=FILE_NAME)
79 logging.info(' File ' + FILE_NAME + ' found!')
80
81 # decode the YAML file
82 intent_config = yaml.safe_load(intent_network_settings)
83
84 # parse the input data
85 site_name_hierarchy = intent_config['site_info']['site_name_hierarchy']
86 banner_message = intent_config['banner']['message']
87 ntp_server = intent_config['ntp_server']['server_ip']
88 dns_server = intent_config['dns_server']['server_ip']
89
90 logging.info(' Intent network settings from GitHub:')
91 logging.info(' Site hierarchy: ' + site_name_hierarchy)
92 logging.info(' Banner: ' + banner_message)
93 logging.info(' NTP server: ' + ntp_server)
94 logging.info(' DNS server: ' + dns_server)
95
```

Get from GitHub,
private repo, the intent
config file

Parse the YAML file, in
this case Network
Settings

Compliance App Python Code - continued

```
100
101 # get the site Id for the site with the name
102 response = catalyst_center_api.sites.get_site(name=site_name_hierarchy)
103 site_id = response['response'][0]['id']
104 logging.info(' The site id for the site: "' + site_name_hierarchy + '" is: ' + site_id)
105
106 # collect the network settings for site
107 response = catalyst_center_api.network_settings.get_network_v2(site_id)
108 site_network_settings = response['response']
109 logging.info(' Collected the site settings')
110
111 # verify the settings for NTP
112 network_settings_ntp_status = {'ntp': 'not_compliant'}
113 for item in site_network_settings:
114     if item['instanceType'] == 'ip' and item['key'] == 'ntp.server' and item['value'][0] == ntp_server:
115         network_settings_ntp_status.update({'ntp': 'compliant'})
116         break
117
118 # verify the settings for DNS
119 network_settings_dns_status = {'dns': 'not_compliant'}
120 for item in site_network_settings:
121     if item['instanceType'] == 'dns' and item['key'] == 'dns.server' and item['value'][0]['primaryIpAddress'] == dns_server:
122         network_settings_dns_status.update({'dns': 'compliant'})
123         break
124
125 # verify the settings for Banner message
126 network_settings_banner_status = {'banner': 'not_compliant'}
127 for item in site_network_settings:
128     if item['instanceType'] == 'banner' and item['value'][0]['bannerMessage'] == banner_message:
129         network_settings_banner_status.update({'banner': 'compliant'})
130         break
131
```

Get the site unique identifier and network settings

Validate the GitHub intent matches the configured settings for site

Intent vs Configured Network Settings

```
zapodeanu updated banner

Code Blame 23 lines (16 loc) · 338 Bytes Code 55% faster with GitHub Copilot

1 ---
2 site_info:
3   site_name_hierarchy: Global/OR/PDX
4
5 banner:
6   message: Managed by Catalyst Center 10.93.141.45, Team - CampusOps - tel 800-553-2447
7
8 netflow:
9   netflow_enabled: true
10
11 syslog:
12   syslog_enabled: true
13
14 telemetry:
15   telemetry_enabled: true
16
17 ntp_server:
18   server_ip: 171.68.38.66
19
20 dns_server:
21   server_ip: 171.70.168.183
22 ...
```

Note:

- Build your data model for your Custom compliance policy

Message of the Day

Customize the message that appears when logging into routers, switches, and hubs.

☐ Use device's existing message

☒ Set custom message

Device login message*

This device is managed by Catalyst Center 10.93.141.45

NTP

Specify one or more NTP servers to facilitate system clock synchronization for your network.

☒ Add NTP servers

IP Address*

171.68.38.66

DNS

Configure your network's domain name and specify DNS servers for hostname resolution.

☐ Set a domain name

☒ Add DNS servers

IP Address*

171.70.168.183

Network Settings Compliance App Run

```
INFO:root: Application "network_settings_compliance.py" Start, 2023-12-04 01:01:43
INFO:root: Repo "compliance_state" found!
INFO:root: File "intent_network_settings.yaml" found!
INFO:root: Intent network settings from GitHub:
INFO:root:   Site hierarchy: Global/OR/PDX
INFO:root:   Banner: Managed by Catalyst Center 10.93.141.45, Team - CampusOps - tel 800-553-2447
INFO:root:   NTP server: 171.68.38.66
INFO:root:   DNS server: 171.70.168.183
INFO:root: The site id for the site: "Global/OR/PDX" is: 15628823-b52e-4564-a39c-36a9d45dc180
INFO:root: Collected the site settings
INFO:root: Network Settings compliance report:
INFO:root: {
  "site_hierarchy": "Global/OR/PDX",
  "compliance_status": {
    "dns": "compliant",
    "ntp": "compliant",
    "banner": "not_compliant",
    "banner_intent": "Managed by Catalyst Center 10.93.141.45, Team - CampusOps - tel 800-553-2447",
    "banner_configured": "This device is managed by Catalyst Center 10.93.141.45"
  }
}
INFO:root: Saved the network settings report to file "network_settings_report.json"
INFO:root: End of Application "network_settings_compliance.py" Run: 2023-12-04 01:01:48
```

Use the report file for:

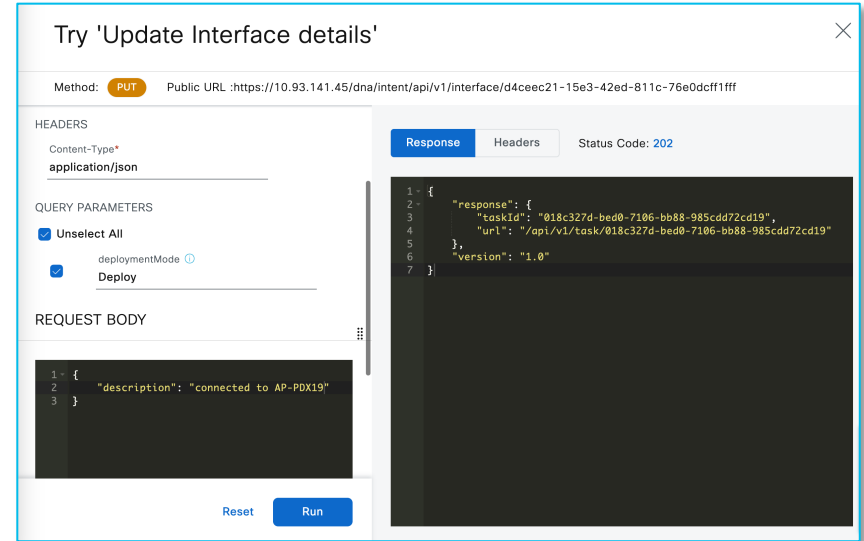
- 3rd party integrations (ITSM)
- Remediation IaC workflow update settings + reprovision devices

Compliant Settings

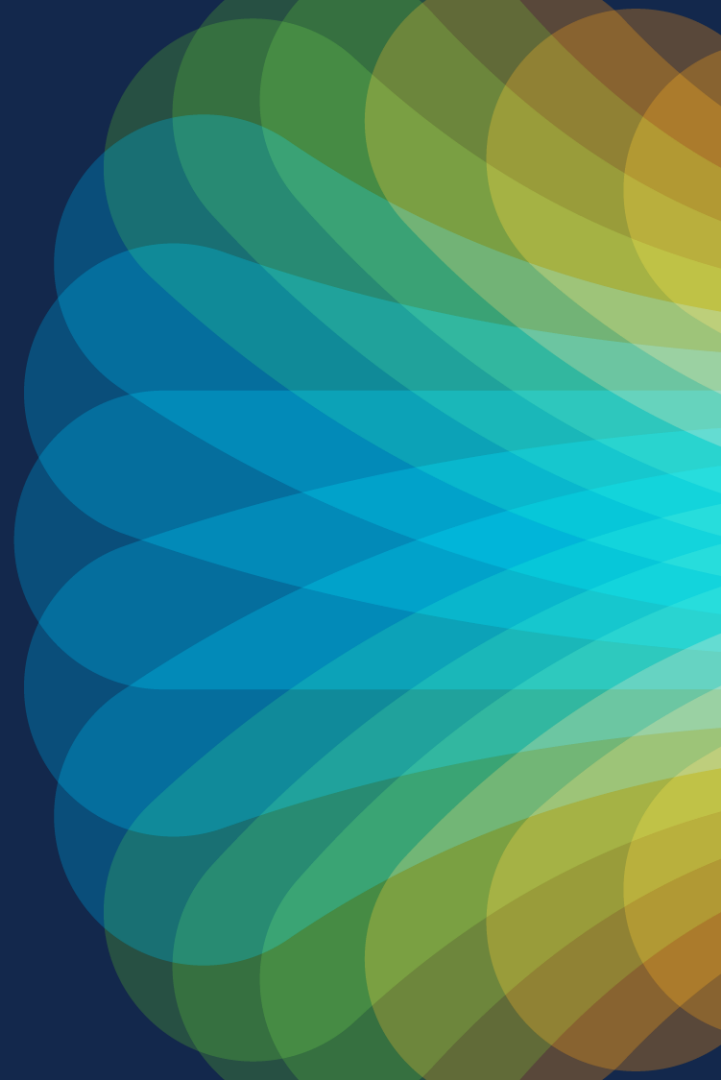
Non-Compliant settings and details for intent and configured

Custom Compliance

- Using the same workflow, we may verify network settings for hundreds or thousands of sites
- Maintain a sync between projects and templates that are configured on Catalyst Center with those defined on GitHub
- Golden software image configuration and tags
- Automate time zone config based on device location
- Interface descriptions and operations based on your policies
- Integrations and ITSM change management



Network Settings Compliance Demo



Camtasia 2023

File

Edit

Modify

Text

View

Export

Window

Help

Home - Cisco DNA Center

compliance_state/intent_netwo...

+

https://10.93.141.45/dna/home

120%

★

Cisco Systems, Inc

APIs

Tools

LAB_Access

CiscoLive

Meraki Dashboard L...

Cisco Box

SFEH-NAS - Synolo...

CDETS

DNACaaP

Cisco.DNA.Center.D...

SharePoint

APIs and Owners - ...

JIRA Engineering SJ...

Uno - MaglevCloud ...

Other Bookmarks

☰

CISCO

DNA Center

☆

🔍

🔄

?

🔔

|

👤

admin

▼

Welcome, [admin](#)

🖥️ Explore

Assurance Summary

Health ⓘ

Healthy as of Dec 4, 2023 8:16 PM

100%

Network Devices

--%

Wireless Clients

100%

Wired Clients

View Details

Critical Issues

Last 24 Hours

0

P1

0

P2

View Details

Trends and Insights

Last 30 Days

0

AP Performance Advisories

0

Trend Deviations

View Details

Network Snapshot

Sites

As of Dec 4, 2023 8:16 PM

17

DNS Servers : 1

NTP Servers : 1

Network Devices

As of Dec 4, 2023 8:16 PM

14

Unclaimed: 1

Unprovisioned: 1

Unreachable: 0

Application QoS Policies

As of Dec 4, 2023 8:18 PM

0

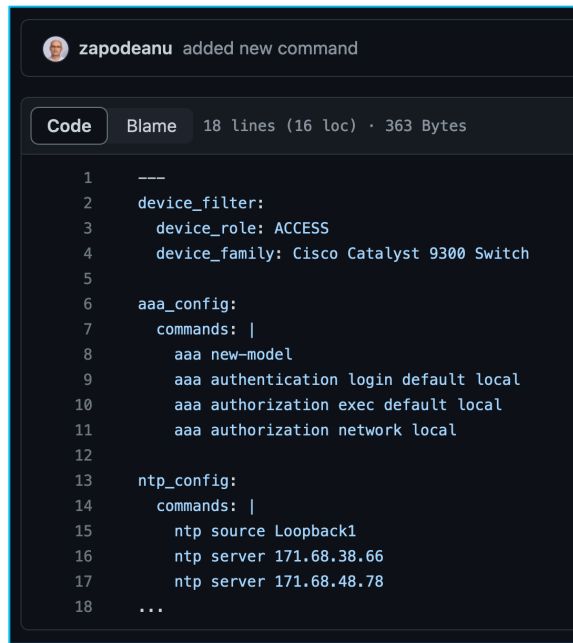
Successful Deploys: 0

Errored Deploys: 0

Stale Policies: 0

Custom Device Config Compliance

- Pull from GitHub the file with the intent device configs
- Verify the desired configuration matches the configuration of devices managed by Catalyst Center
- Create report



The screenshot shows a GitHub commit interface. At the top, a user profile icon and the name 'zapodeanu' are followed by the text 'added new command'. Below this, there are tabs for 'Code' (selected), 'Blame', and a summary '18 lines (16 loc) · 363 Bytes'. The main area displays a code diff with line numbers 1 through 18. The code is a JSON configuration snippet for a Cisco Catalyst 9300 Switch, including sections for 'device_filter', 'aaa_config', and 'ntp_config'.

```
1 ---
2 device_filter:
3   device_role: ACCESS
4   device_family: Cisco Catalyst 9300 Switch
5
6 aaa_config:
7   commands: |
8     aaa new-model
9     aaa authentication login default local
10    aaa authorization exec default local
11    aaa authorization network local
12
13 ntp_config:
14   commands: |
15     ntp source Loopback1
16     ntp server 171.68.38.66
17     ntp server 171.68.48.78
18 ...
```

Custom Device Config Compliance Workflow

```
zapodeanu added new command

Code Blame 18 lines (16 loc) · 363 Bytes

1 ---
2 device_filter:
3   device_role: ACCESS
4   device_family: Cisco Catalyst
5
6 aaa_config:
7   commands: |
8     aaa new-model
9     aaa authentication login default local
10    aaa authorization exec default local
11    aaa authorization network default local
12
13 ntp_config:
14   commands: |
15     ntp source Loopback1
16     ntp server 171.68.38.66
17     ntp server 171.68.48.78
18 ...
```

Pull the device compliance policy from GitHub

```
{
  "hostname": "L0-BN",
  "device_ip": "10.93.141.28",
  "device_id": "db05ad49-2c8d-4094-9df6",
  "version": "17.6.3",
  "device_family": "Cisco Catalyst 9300",
  "role": "DISTRIBUTION",
  "site": "Global/OR/L0/Floor-3",
  "sda_roles": [
    "Border Node"
  ]
},
{
  "hostname": "L0-CN",
  "device_ip": "10.93.141.20",
  "device_id": "6a612b05-1c89-4d0a-a4d3-94ec5e5a7a57",
  "version": "17.9.4a",
  "device_family": "Cisco Catalyst 9300 Switch",
  "role": "ACCESS",
  "site": "Global/OR/L0/Floor-3",
  "sda_roles": [
    "Control Plane"
  ]
},
]
```

Get the device inventory from Catalyst Center

```
35 !
36 logging buffered 20960
37 logging console emergencies
38 aaa new-model
39 !
40 !
41 aaa authentication login default local
42 aaa authorization exec default local
43 !
44 !
45 aaa session-id common
46 clock timezone PST -8 0
47 clock summer-time PDT recurring
48 boot system switch all flash
49 software auto-upgrade enable
50 !
51 switch 1 provision c9300-24u
```

Read from Catalyst Center the config for devices matching the policy

Validate compliance

```
INFO:root: Device: L0-CN :
INFO:root:   - AAA config check failed, missing commands:
INFO:root:   - aaa authorization network local
INFO:root:   - NTP config check failed, missing commands:
INFO:root:   - ntp source Loopback1
INFO:root:   - ntp server 171.68.48.78
INFO:root: Saved the device config PDX-STACK_config.txt
INFO:root: Device: PDX-STACK :
INFO:root:   - AAA config check failed, missing commands:
INFO:root:   - aaa authorization network local
INFO:root:   - NTP config check failed, missing commands:
INFO:root:   - ntp server 171.68.48.78
```

How to Compare Text Files in Python

Python “difflib.Differ” Class

- Compares sequences of lines of text and producing human-readable differences or deltas.
- It will compare sequences of lines, and sequences of characters within similar (near-matching) lines.
- Each line of a Differ delta begins with a two-letter code

Code	Meaning
'- '	line unique to sequence 1
'+'	line unique to sequence 2
' '	line common to both sequences
'? '	line not present in either input sequence

Ref: <https://docs.python.org/3/library/difflib.html>

Config Compliance Check – Calculate Diff

“cli_commands.txt”

```
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa authorization network local
```

“device_config.txt”

```
logging buffered 20960
logging console emergencies
aaa new-model
!
aaa authentication login default local
aaa authorization exec default
!
aaa session-id common
clock timezone PST -8 0
```

“cli_difference”

```
+ logging buffered 20960
+ logging console emergencies
+ aaa new-model
+ !
+ aaa authentication login default local
- aaa authorization exec default local
? -----
+ aaa authorization exec default
- aaa authorization network local
+ !
+ aaa session-id common
+ clock timezone PST -8 0
```

Calculate using the “difflib.Differ” class the delta between CLI commands and the device config

- Lines starting with “+” are in both files
- Lines starting with “-” are missing in the second file
- Lines starting with “+” are missing in the first file

Notes:

- Order of the param files is important
- In this use case: `config_diff.compare (“cli_commands.txt”, “device_config.txt”)`

Config Compliance Check – Create Report

“cli_difference”

```
+ logging buffered 20960
+ logging console emergencies
  aaa new-model
+ !
  aaa authentication login default local
- aaa authorization exec default local
? -----
+ aaa authorization exec default
- aaa authorization network local
+ !
+ aaa session-id common
+ clock timezone PST -8 0
```

Notes:

- The difflib library has few other options to compare text
- There are other libraries that may be used.

- From the “cli_difference” select the lines that start with “- ”
- These are the commands existing in the “cli_commands.txt” and not in the device config
- If there no lines starting with “- ” device is compliant with the Custom policy

Missing commands

```
aaa authorization exec default local
aaa authorization network local
```

Get Device Config By Device ID API

Get Device Config by Id

GET `https://10.93.141.45/dna/intent/api/v1/network-device/${networkDeviceId}/config`

Returns the device config by specified device ID

[Cisco DevNet API Guide](#)

Parameters Responses Code Preview

Request URL Parameters

Name	Description	Data Type
networkDeviceId	networkDeviceId	string

Try 'Get Device Config by Id'

Method: **GET** Public URL : `https://10.93.141.45/dna/intent/api/v1/network-device/db05ad49-2c8d-4094-9df6-3a03f9b28069/config`

PARAMETERS

PATH PARAMETERS

networkDeviceId ⓘ
db05ad49-2c8d-4094-9df6-3a03f9b28069

Response Headers Status Code: 200

```
1 'response': "\nBuilding configuration...\n\nCurrent configuration : 28933 bytes\n2\n3 'version': "1.0"\n4
```

Reset Run

- The configuration of the device is based on the last time Catalyst Center synchronized the device
- To collect real-time device configurations, use the command-runner APIs

Device Config Compliance App Code

Get the device count from Catalyst Center, retrieve the device list, enrich with location and SDA device role

```
# verify if repo exists
if GITHUB_REPO not in repos:
    logging.info(' Repo ' + GITHUB_REPO + ' not found!')
    return
logging.info(' Repo ' + GITHUB_REPO + ' found!')
```

```
# get the device config compliance intent file
file_content = github_api.get_repo_file_content(username=GITHUB_USERNAME,
                                                repo_name=GITHUB_REPO,
                                                file_name=FILE_NAME)
logging.info(' File ' + FILE_NAME + ' found!')
```

```
# parse the input data
intent_config = yaml.safe_load(file_content)
aaa_config = intent_config['aaa_config']['commands']
ntp_config = intent_config['ntp_config']['commands']

# parse the device policy
device_role = intent_config['device_filter']['device_role']
device_family = intent_config['device_filter']['device_family']
```

```
logging.info(' Device config from GitHub:')
logging.info('   aaa:')
logging.info('   ntp:')
```

Pull from GitHub repo and the file with the device compliance policy, and parse data

```
# collect device inventory
# get the device count
response = catalyst_center_api.devices.get_device_count()
device_count = response['response']
logging.info(' Number of devices managed by Catalyst Center: ' + str(device_count))
```

```
# get the device info list
offset = 1
limit = 500
device_list = []
while offset <= device_count:
    response = catalyst_center_api.devices.get_device_list(offset=offset)
    offset += limit
    device_list.extend(response['response'])
logging.info(' Collected the device list from Catalyst Center')
```

```
# create device inventory, add location and fabric roles

device_inventory = []
for device in device_list:
    # select which inventory to add the device to
    if device.family != "Unified AP":...

logging.info(' Retrieved the device location and fabric role')
```

Device Config Compliance App Code - continued

```
# collect the device configs for the devices that match the role
logging.info(' Compliance checks for devices that match the device filter')
for item in device_inventory:
    if item['role'] == device_role and item['device_family'] == device_family:
        response = catalyst_center_api.devices.get_device_config_by_id(item['device_id'])
        device_config = response['response']
        with open(item['hostname'] + '_config.txt', 'w') as f:
            f.write(device_config)
        logging.info(' Saved the device config ' + item['hostname'] + '_config.txt')
        logging.info(' Device: ' + item['hostname'] + ' :')
```

Call Catalyst Center API to get the device config, save config to file
Use the `difflib>Differ` class
Validate the “aaa_config.txt” commands are in the device config

```
# check common lines between the two files - device config compliance commands and running config
aaa_config_file = open('aaa_config.txt', 'r').readlines()
ntp_config_file = open('ntp_config.txt', 'r').readlines()
config_file = open(item['hostname'] + '_config.txt', 'r').readlines()
```

```
aaa_difference = difflib.Differ()
aaa_commands_list = []
for line in aaa_difference.compare(aaa_config_file, config_file):
    if line.startswith('-'):
        clean_line = line.strip()
        aaa_commands_list.append(clean_line)
if len(aaa_commands_list) == 0:
    logging.info(' - AAA config check passed')
else:
    logging.info(' - AAA config check failed, missing commands:')
    for command in aaa_commands_list:
        logging.info(' ' + command)
```

Validate the “ntp_config.txt” commands are in the device config

```
ntp_difference = difflib.Differ()
ntp_commands_list = []
for line in ntp_difference.compare(ntp_config_file, config_file):
    if line.startswith('-'):
        clean_line = line.strip()
        ntp_commands_list.append(clean_line)
if len(ntp_commands_list) == 0:
    logging.info(' - NTP config check passed')
else:
    logging.info(' - NTP config check failed, missing commands:')
    for command in ntp_commands_list:
        logging.info(' ' + command)
```

Device Config Compliance App Logging

```
zapodeanu added new command

Code Blame 18 lines (16 loc) · 363 Bytes

1 ---
2 device_filter:
3   device_role: ACCESS
4   device_family: Cisco Catalyst 9300
5
6 aaa_config:
7   commands: |
8     aaa new-model
9     aaa authentication login default local
10    aaa authorization exec default local
11    aaa authorization network local
12
13 ntp_config:
14   commands: |
15     ntp source Loopback1
16     ntp server 171.68.38.66
17     ntp server 171.68.48.78
18 ...
```

```
INFO:root: Application "device_config_compliance.py" Start, 2023-12-03 17:55:41
INFO:root: Repo "compliance_state" found!
INFO:root: File "custom_network_compliance.yaml" found!
INFO:root: Device configs from GitHub:
```

```
INFO:root:
aaa new-model
aaa authentication login default local
aaa authorization exec default local
aaa authorization network local

INFO:root:
ntp source Loopback1
ntp server 171.68.38.66
ntp server 171.68.48.78
```

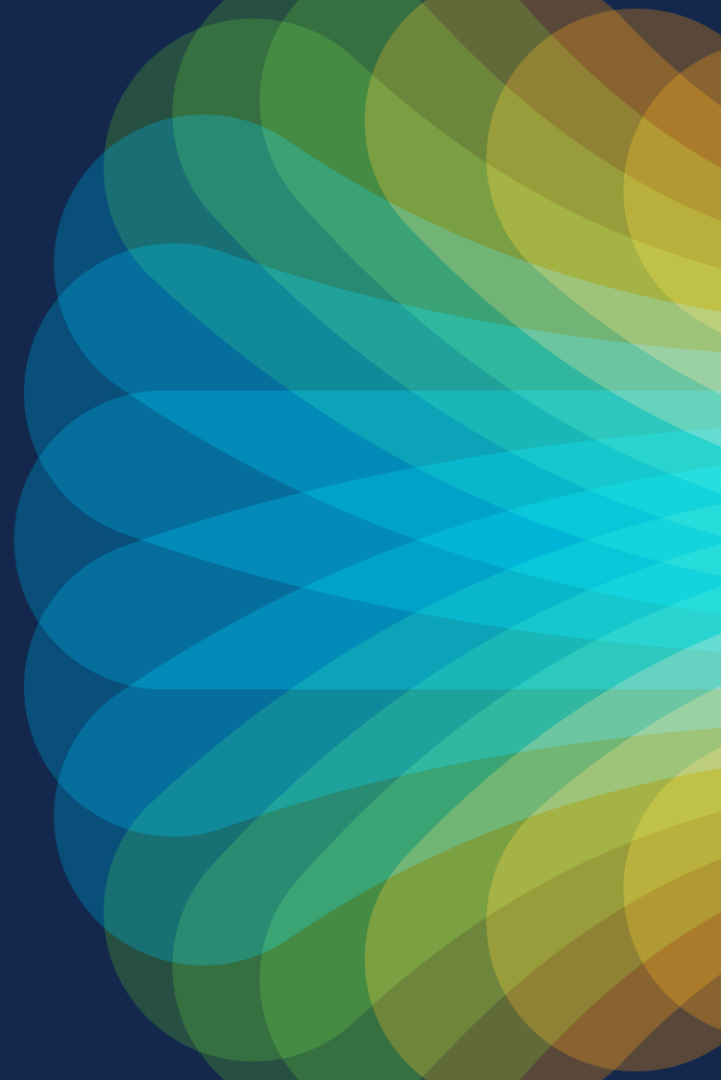
```
INFO:root: Compliance device filter:
INFO:root:   device_role: ACCESS
INFO:root:   device_family: Cisco Catalyst 9300 Switch
INFO:root: Number of devices managed by Cat
INFO:root: Collected the device list from
INFO:root: Retrieved the device location a
INFO:root: Saved the device inventory to f
INFO:root: Compliance checks for devices t
INFO:root: Saved the device config L0-CN_c

INFO:root: Device: L0-CN :
INFO:root:   - AAA config check failed, missing commands:
INFO:root:     - aaa authorization network local
INFO:root:   - NTP config check failed, missing commands:
INFO:root:     - ntp source Loopback1
INFO:root:     - ntp server 171.68.48.78
INFO:root: Saved the device config PDX-STACK_config.txt
INFO:root: Device: PDX-STACK :
INFO:root:   - AAA config check failed, missing commands:
INFO:root:     - aaa authorization network local
INFO:root:   - NTP config check failed, missing commands:
INFO:root:     - ntp server 171.68.48.78
INFO:root: End of Application "device_config_compliance.py" Run: 2023-12-03 17:56:01
```

Use this report for:

- ITSM change management
- Remediation IaC workflows, create the CLI template and deploy to devices

Device Compliance Demo



Camtasia 2023

FileEditModifyTextViewExportWindowHelp

Home - Cisco DNA Center

compliance_state/custom_netv...

https://10.93.141.45/dna/home120%

Cisco Systems, Inc

APIs

Tools

LAB_Access

CiscoLive

Meraki Dashboard L...

Cisco Box

SFEH-NAS - Synolo...

CDETS

DNACaaP

Cisco.DNA.Center.D...

SharePoint

APIs and Owners - ...

JIRA Engineering SJ...

Uno - MaglevCloud ...

Other Bookmarks

☰

DNA Center

☆

🔍

🔄

?

🔔

👤 admin

Welcome, admin

Explore

Assurance Summary

Health ⓘ

Healthy as of Dec 4, 2023 2:17 PM

100%

Network Devices

--%

Wireless Clients

100%

Wired Clients

View Details

Critical Issues

Last 24 Hours

0

P1

0

P2

View Details

Trends and Insights

Last 30 Days

0

AP Performance Advisories

0

Trend Deviations

View Details

Network Snapshot

Sites

As of Dec 4, 2023 2:17 PM

17

DNS Servers : 1

NTP Servers : 1

Network Devices

As of Dec 4, 2023 2:17 PM

14

Unclaimed: 1

Unprovisioned: 1

Unreachable: 0

DEVNET-2634

Application QoS Policies

As of Dec 4, 2023 2:17 PM

0

Successful Deploys: 0

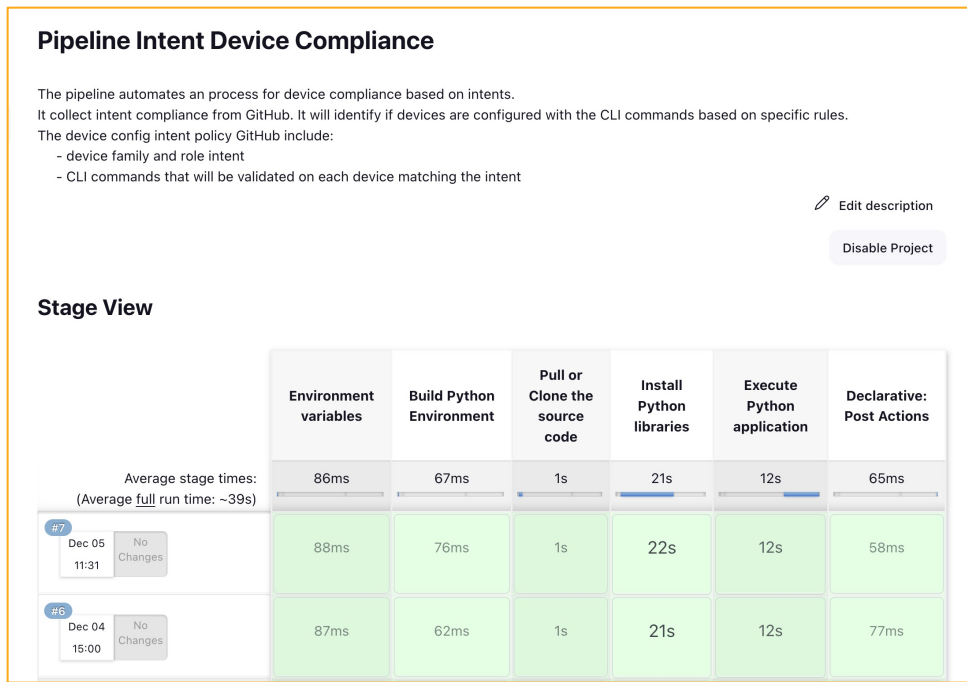
Errored Deploys: 0

Stale Policies: 0

61

Options to Run Compliance Applications

- On-demand or on your automation platform
- Triggered by APIs or events
- Scheduled
- Part of your IaC pipelines, example Jenkins pipeline



Agenda

- Platforms
- Catalyst Center Compliance
- Custom Network Compliance
- Developer Resources
- Lessons Learned

Catalyst Center Network Compliance Use Cases

https://github.com/cisco-en-programmability/catalyst_center_network_compliance

The screenshot shows the GitHub repository page for `catalyst_center_network_compliance`. The repository is public and has 2 forks and 0 stars. The main branch is `main` with 1 branch and 0 tags. The repository contains 20 commits. The file list includes:

File	Commit Message	Time Ago
<code>.gitignore</code>	initial commit	2 weeks ago
<code>CODE_OF_CONDUCT.md</code>	initial commit	2 weeks ago
<code>CONTRIBUTING.md</code>	initial commit	2 weeks ago
<code>LICENSE</code>	initial commit	2 weeks ago
<code>NOTICE</code>	initial commit	2 weeks ago
<code>README.md</code>	updated README.md	4 minutes ago
<code>catalyst_center_compliance.py</code>	added non-compliant report for core devices	17 minutes ago
<code>device_config_compliance.py</code>	reformat logs	16 minutes ago
<code>github_apis.py</code>	updated github function	3 days ago
<code>network_settings_compliance.py</code>	reformat logs	16 minutes ago
<code>requirements.txt</code>	initial commit	2 weeks ago

The right sidebar shows the repository's metadata and links to the README, license, and code of conduct. It also indicates that there are no releases or packages published.

Python SDK

Cisco DNA Center Version Support 1.2.10 to 2.3.5.3

Docs » dnacentersdk [Edit on GitHub](#)

dnacentersdk

Simple, lightweight, scalable Python API wrapper for the DNA Center APIs

Welcome to the docs! dnacentersdk is a community developed Pythonic wrapping of the DNA Center APIs (for API versions: 1.2.10, 1.3.0, 1.3.1, 1.3.3, 2.1.1 and 2.1.2). The package represents all of the Cisco DNA Center API interactions via native Python tools. Making working with the Cisco DNA Center APIs in Python a native and natural experience.

dnacentersdk helps you get things done faster. We take care of the API semantics, and you can focus on writing your code.

With dnacentersdk, you can easily:

- Interact with the DNA Center APIs in an interactive Python session
- Quickly create code that enables you get something done in DNA Center
- Leverage the API wrapper to cleanly add DNA Center functionality to your project without having to write the boilerplate code for working with the DNA Center APIs

To dive in and see how dnacentersdk makes your life better, check out the [Quickstart](#)!

The User Guide

- [Installation](#)
 - [PIP Install](#)
 - [PIP Upgrade](#)
 - [Get the Source Code](#)
- [Introduction](#)
 - [Work with the DNA Center APIs in Native Python!](#)
 - [MIT License](#)
 - [dnacentersdk License](#)
- [Quickstart](#)
 - [Get your DNA Center Access Token](#)
 - [Set credentials as environment variables](#)

- Includes all Cisco Catalyst Center REST APIs
- Support for Cisco Catalyst Center version 2.3.5.3, (2.3.7.3 pending release)
- First SDK version August 2019
- Downloads last month 6,200+

<https://dnacentersdk.readthedocs.io>

Search or jump to... Pull requests Issues Codespaces Marketplace Explore

cisco-en-programmability / dnacentersdk Public

Edit Pins Unwatch 13 Fork 19 Starred 42

Code Issues Pull requests Actions Projects Wiki Security Insights Settings

master 4 branches 31 tags Go to file Add file Code

bvargasre Merge pull request #79 from cisco-en-programmability/develop	7eda9b1 3 weeks ago	186 commits
.github/ISSUE_TEMPLATE	New oncompatibility matrix	3 weeks ago
dnacentersdk	- Offset and limit now support basestring and int	3 weeks ago
docs	New version 2.5.6	3 weeks ago
script	Update LICENSE reference	last year
tests	### Fixed	6 months ago
.flake8	Update tests (lint, mock server order, validators)	last year
.gitattributes	Initial commit	3 years ago
.gitignore	Change some request in the test files and .DS_Store were added to L...	7 months ago
.readthedocs.yml	Update project dependencies & settings	last year

About

Cisco DNA Center Python SDK

[dnacentersdk.readthedocs.io/en/latest/](#)

Readme

MIT license

42 stars

13 watching

19 forks

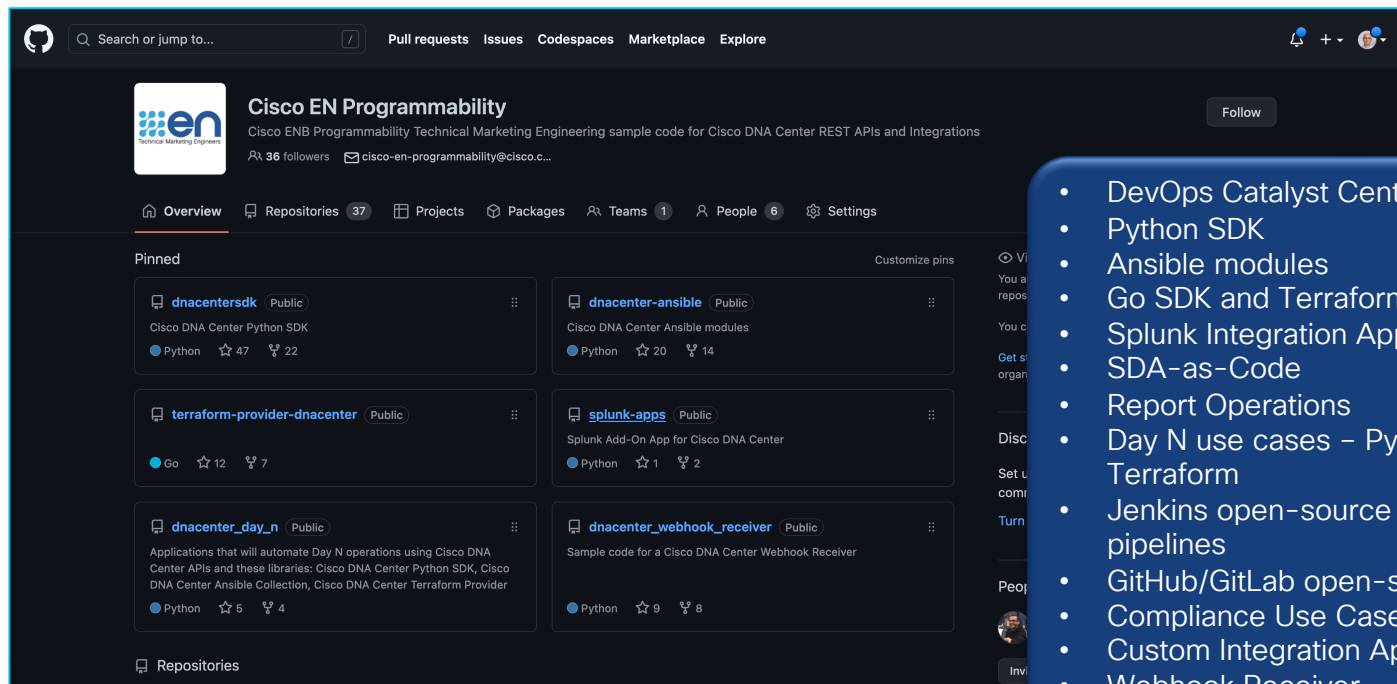
Releases 26

v2.5.6 (Latest) 3 weeks ago

+ 25 releases

<https://github.com/cisco-en-programmability/dnacentersdk>

Cisco EN Programmability GitHub Org



<https://github.com/cisco-en-programmability>

- DevOps Catalyst Center use cases
- Python SDK
- Ansible modules
- Go SDK and Terraform provider
- Splunk Integration Apps
- SDA-as-Code
- Report Operations
- Day N use cases – Python SDK, Ansible, Terraform
- Jenkins open-source Integration and pipelines
- GitHub/GitLab open-source Integrations
- Compliance Use Case
- Custom Integration App
- Webhook Receiver
- Other sample code

Agenda

- Platforms
- Catalyst Center Compliance
- Custom Network Compliance
- Developer Resources
- Lessons Learned

Summary

- Catalyst Center has rich network compliance API, providing consistent intent configurations, profiles and policies
- Use existing compliance features and add your compliance workflows for a continuous compliance process
- Compliance insights and reporting, options to automate compliance drift

Pipeline Intent Device Compliance

The pipeline automates an process for device compliance based on intents. It collect intent compliance from GitHub. It will identify if devices are configured with the CLI commands based on specific rules. The device config intent policy GitHub include:

- device family and role intent
- CLI commands that will be validated on each device matching the intent

Stage View



```
INFO:root: Compliance checks for devices that match the device filter
INFO:root: Saved the device config LO-CN_config.txt
INFO:root: Device: LO-CN :
INFO:root: - AAA config check failed, missing commands:
INFO:root:   - aaa authorization network local
INFO:root: - NTP config check failed, missing commands:
INFO:root:   - ntp source Loopback1
INFO:root:   - ntp server 171.68.48.78
INFO:root: Saved the device config PDX-STACK_config.txt
INFO:root: Device: PDX-STACK :
INFO:root: - AAA config check failed, missing commands:
INFO:root:   - aaa authorization network local
INFO:root: - NTP config check failed, missing commands:
INFO:root:   - ntp server 171.68.48.78
INFO:root: End of Application "device_config_compliance.py" Run: 2023-12-03 19:51:20
```

Other Sessions and Activities This Week

SESSION CODE	SESSION TITLE	ROOM	SESSION DATE	SESSION TIME
DEVNET-2632	Version Control Tools Integrations – Cisco Catalyst Center Infrastructure-as-Code Use Cases	DevNet Theatre	12/08/23	09:15 AM
MTE-1042	Meet the Expert – Gabi Zapodeanu	Meet the Expert 1 – The HUB	12/06/23	03:00 PM

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic featuring a rainbow color palette. On the left, there are horizontal, wavy bands of color transitioning from red at the top to blue at the bottom. On the right, a bright white light source emits a series of sharp, radiating lines in various shades of blue, green, and yellow, creating a sunburst or starburst effect. The overall composition is dynamic and colorful.

cisco *Live!*

Let's go

#CiscoLiveAPJC