Configuration Drifts

Configuration Drift Notifications and Faults

When you deploy Cisco ACI in a public cloud, you will perform most of the fabric configuration from the Cloud APIC. However, there may be cases where you or another cloud administrator changes the deployed configuration directly in the cloud provider's GUI using the tools provided by AWS or Azure. In these cases, the intended configuration you deployed from the Cloud APIC and the actual configuration in the cloud site may become out of sync, we call this a configuration drift.

Starting with Release 5.0(2), Cloud APIC provides visibility into any security policy (contracts) configuration discrepancy between what you deploy from the Cloud APIC and what is actually configured in the cloud site. Future releases will provide the configuration drift visibility into the other Cloud APIC objects as well as information about extraneous configurations deployed in the cloud but not defined in the Cloud APIC.

There are two aspects to analyzing configuration drift:

- Have all the fabric elements configured in the Cloud APIC and intended to be deployed in the cloud fabric been properly deployed?

  This scenario can occur due to user configuration errors in Cloud APIC that could not be deployed in the cloud, connection or API issues on the cloud provider end, or if a cloud administrator manually deletes or modifies security rules directly in the cloud provider's UI. Any intended but missing configurations may present an issue for the Cloud APIC fabric.

- Are there any additional configurations that exist in the cloud but were not intended to be deployed from the Cloud APIC?

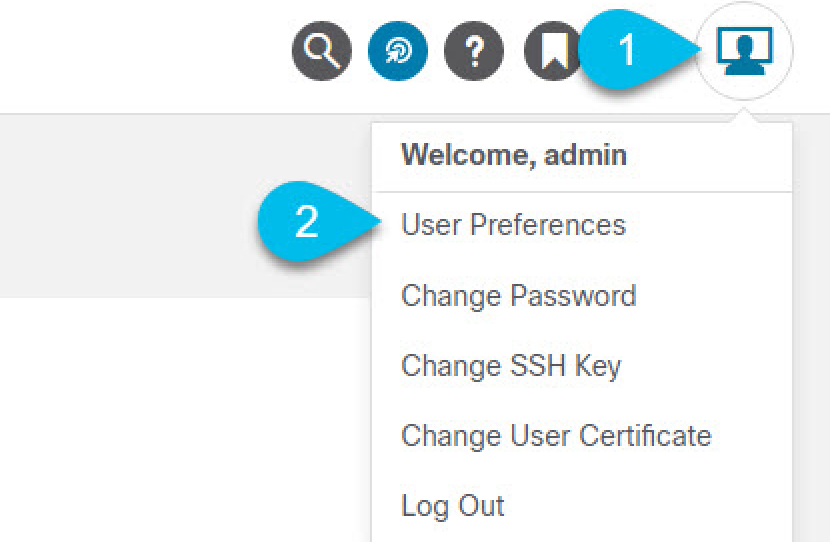
  Similarly to the previous scenario, this can occur if there are connection or API issues or if a cloud administrator manually creates additional security rules directly in the cloud provider's UI. Any existing but not intended configuration may present issues.

Enabling Configuration Drift Detection

In this release, configuration drift detection is in beta stage, as such it is disabled by default. This section describes how to enable configuration drift detection in your Cloud APIC user preferences.

Step 1 Log in to your Cloud APIC GUI.

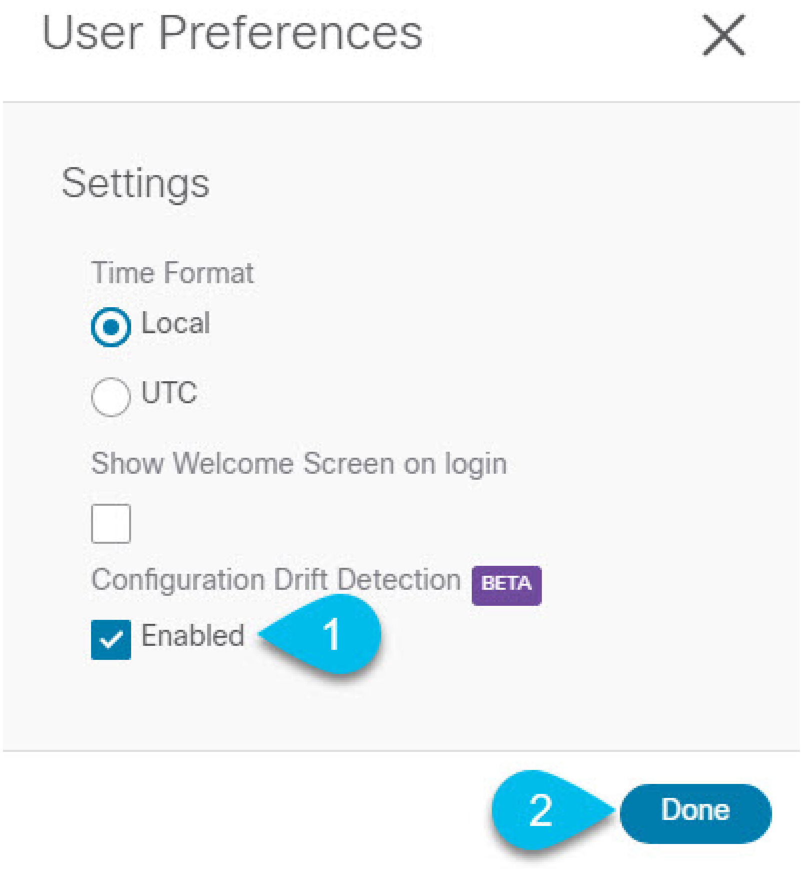
Step 2 Open the **User Preferences** dialog.



a) In the top right corner of the screen, click the user icon.

b) From the menu, select **User Preferences**.

Step 3 In the **User Preferences** dialog, enable **Configuration Drift Detection**.



User Preferences

Settings

Time Format

● Local

○ UTC

Show Welcome Screen on login

□

Configuration Drift Detection BETA

☑ Enabled

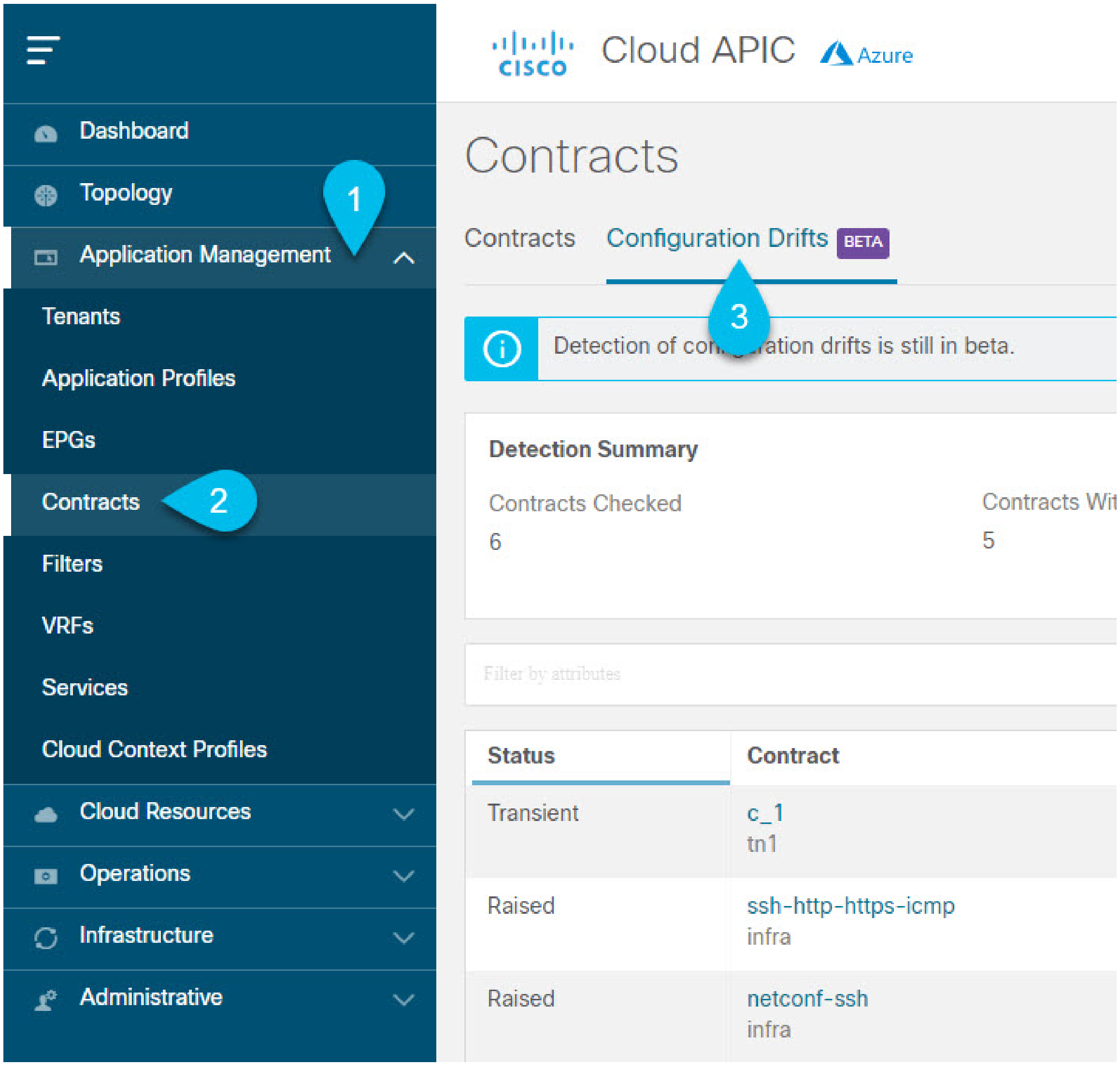
a) Check the **Enabled** checkbox.
b) Click **Done** to save the change.

Checking for Missing Contracts Configuration

This section describes how to check for any contract settings you have configured from the Cloud APIC, but which have not been properly deployed to the cloud fabric.

Step 1 Log in to your Cloud APIC GUI.

Step 2 Navigate to the **Configuration Drifts** screen.



Contracts

Detection of configuration drifts is still in beta.

Detection Summary

Contracts Checked	Contracts Wit
6	5

Status	Contract
Transient	c_1 tn1
Raised	ssh-http-https-icmp infra
Raised	netconf-ssh infra

a) In the **Navigation** sidebar, expand the **Application Management** category.
b) From the **Application Management** category, select **Contracts**.
c) In the **Contracts** screen, select the **Configuration Drifts** tab.

In the **Configuration Drifts** tab, you can see a summary of any configuration issues with the contracts in your fabric.

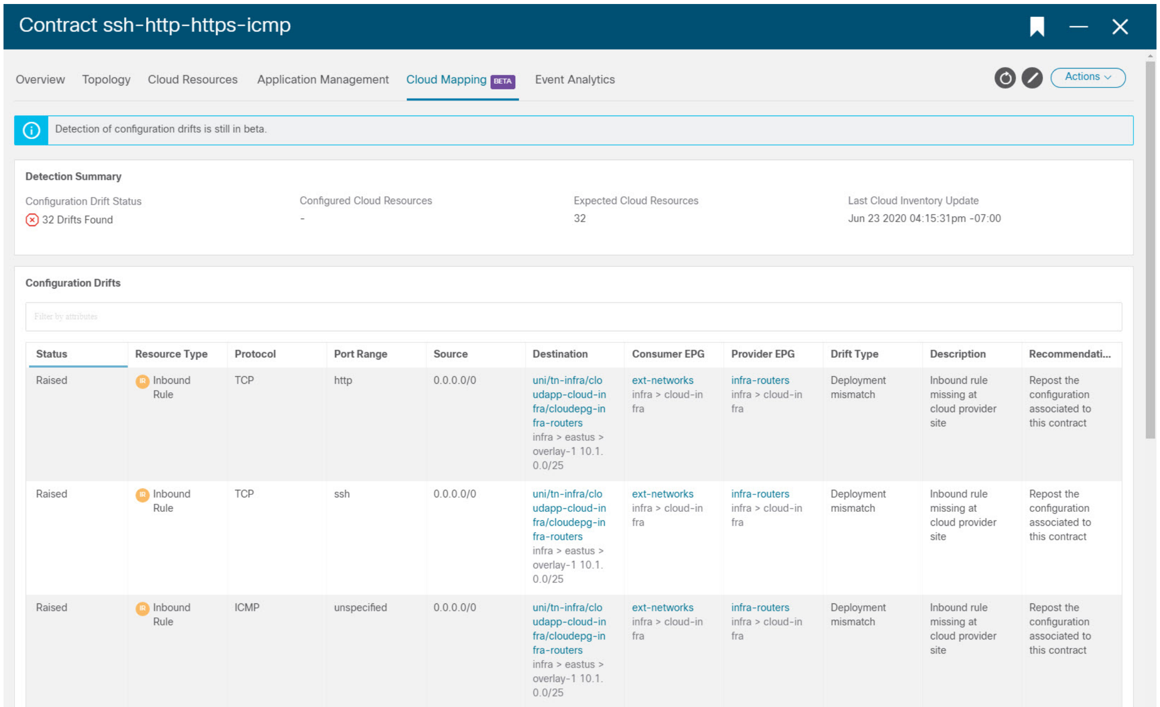
For each contract with a drift, you will see the number of missing configurations and the severity of the issue.

You can refresh the information by clicking the refresh button in the top right of the main window.

Step 3 In the **Configuration Drifts** screen, click the name of a contract to view its details, including the configuration drift issues.

Step 4 In the **Contract details** view that opens, select the **Cloud Mapping** tab.

The **Cloud Mapping** view displays all the information about the contract and the cloud resources it uses.



Detection of configuration drifts is still in beta.

Detection Summary

Configuration Drift Status	Configured Cloud Resources	Expected Cloud Resources	Last Cloud Inventory Update
⊗ 32 Drifts Found	-	32	Jun 23 2020 04:15:31pm -07:00

Configuration Drifts

Filter by attributes

Status	Resource Type	Protocol	Port Range	Source	Destination	Consumer EPG	Provider EPG	Drift Type	Description	Recommendati...
Raised	IR Inbound Rule	TCP	http	0.0.0.0/0	uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers infra > eastus > overlay-1 10.1.0.0/25	ext-networks infra > cloud-infra	infra-routers infra > cloud-infra	Deployment mismatch	Inbound rule missing at cloud provider site	Repost the configuration associated to this contract
Raised	IR Inbound Rule	TCP	ssh	0.0.0.0/0	uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers infra > eastus > overlay-1 10.1.0.0/25	ext-networks infra > cloud-infra	infra-routers infra > cloud-infra	Deployment mismatch	Inbound rule missing at cloud provider site	Repost the configuration associated to this contract
Raised	IR Inbound Rule	ICMP	unspecified	0.0.0.0/0	uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers infra > eastus > overlay-1 10.1.0.0/25	ext-networks infra > cloud-infra	infra-routers infra > cloud-infra	Deployment mismatch	Inbound rule missing at cloud provider site	Repost the configuration associated to this contract

The screen is divided into three sections, **Detection Summary**, **Configuration Drifts**, and **Mapped Cloud Resources**. Each section contains a table that lists the respective information about the contract you selected.

The **Detection Summary** table provides an overview of how many configuration drifts were detected, number of intended and actual cloud resources configured, and the time when this information was last updated. If the inventory update timestamp is out of date, you can refresh the information by clicking the **Refresh** icon in the top right corner of this screen.

The **Configuration Drifts** table lists all the issues with the contract rules. Specifically, all the contract rules that were intended to be deployed but are missing in the actual fabric configuration. The table contains detailed information, such as the protocol used, port ranges, source and destination IP or group, consumer and provider EPGs, description of the issue, and the recommended action to resolve it. For each configuration drift, the **Status** field will indicate the severity and recommended action:

- `Transient` (low): drifts that are likely due to recent configuration changes. We recommend waiting for the fabric to stabilize and the drift will likely resolve on its own after the next configuration refresh.
- `Presumed` (medium): drifts that may or may not be transient. We recommend monitoring the status and troubleshoot the configuration should the drift persist.

  `Raised` (high): critical drifts. We recommend verifying the configuration on Cloud APIC and checking for any associated faults. Redeploying the configuration may help resolve communication issues between the Cloud APIC and cloud services. If the issue persists, check the tech-support logs.

The **Mapped Cloud Resources** table shows the information about all the resources that were properly configured in your cloud. This table is designed to provide you with better visibility into what rules are configured in your cloud for a specific contract.

Configuration Drift Troubleshooting

This section provides a few useful command to verify that the configuration drift processes are up and running on your Cloud APIC, check the application logs, and if necessary generate tech support information.

Step 1 Log in to the Cisco Cloud APIC via console as a `root` user.

Step 2 Check the status of the configuration drift application.

```
ACI-Cloud-Fabric-1# moquery -d pluginContr/plugin-Cisco_CApicDrift | egrep "dn |pluginSt |operSt
|version"
dn: pluginContr/plugin-Cisco_CApicDrift
operSt: active
pluginSt: active
Verison: 5.1.0
```

Step 3 Check the status of the application container.

```
ACI-Cloud-Fabric-1# docker ps | grep drift
CONTAINER ID    IMAGE           COMMAND                  CREATED          STATUS
        NAMES
649af6feb72c    a5ea08bbf541    "/opt/bin/conit.bi..."  13 hours ago    Up 13
hours     drift-api-b703e569-0aa6-859f-c538-a5fecbc5708f
```

Step 4 Check memory consumed by all Docker containers.

Total amount of memory consumed must be under 12GB.

```
ACI-Cloud-Fabric-1# systemctl status ifc-scheduler_allocations.slice| grep Memory
```

Step 5 If necessary, collect the tech support logs.

Logs will be saved in the `/data/techsupport` directory on the controller.

```
ACI-Cloud-Fabric-1# trigger techsupport controllers application CApicDrift
ACI-Cloud-Fabric-1# trigger techsupport controllers application CApicDrift vendorName Cisco
```

Step 6 Check the application logs.

The logs for configuration drift process are stored in the `/data2/logs/Cisco_CApicDrift` directory.

The `runhist.log` file provides information about each time the application was started, for example:

```
# cat runhist.log
1 - Thu Jun 11 23:55:59 UTC 2020
2 - Fri Jun 12 01:19:41 UTC 2020
```

The `drift.log` file is the application log file and can be used to view the number of times configuration drift was updated and how long each update took.

```
# cat drift.log | grep ITER
{"file":"online_snapshot.go:178","func":"Wait","level":"info","msg":"ITER# 109
ENDED ===  RDFGEN TIME: 1m40.383751649s,  MODEL UPLOAD TIME 5m54.245550374s; TOTAL
       TIME:: 7m34.629447083s","time":"2020-06-12T19:53:13Z"}
```