Troubleshoot Firepower Threat Defense Policy Deployments

Contents

Introduction

This document describes a high-level overview of the Policy Deployment process on FTD and as well as basic troubleshooting techniques.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- **Firewall Management Center (FMC)**
- **Firepower Threat Defense (FTD)**

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

With **Cisco Firepower Threat Defense** (FTD), traditional stateful firewall features offered by **Adaptive Security**

Appliances (ASA) and **Next-Gen** firewall features (powered by **Snort**) are now combined into one product.

Due to this change, **Policy Deployment Infrastructure** on FTD now handles configuration changes for both ASA code (also referred to as LINA), and **Snort** in one bundle.

Policy Deployment Overview

Cisco FTD utilizes **Policy Deployments** to manage and push out configurations for devices that are registered to the **Firewall Management Center** (FMC) itself.

Inside the deployment, there are a series of steps that are broken into "Phases".

The FMC phases can be summarized in this list.

Phase 0	Deployment Initialization
Phase 1	Database Object Collection
Phase 2	Policy and Object Collection
Phase 3	NGFW Command Line Configuration Generation
Phase 4	Device Deployment Package Generation
Phase 5	Send and Receive the Deployment Package
Phase 6	Pending Deployment, Deployment Actions, and Deployment Success Messages

Knowledge of the phases and of the location of failures in the process can help troubleshoot the failures that a **Firepower** system faces.

In some situations, it be a conflict due to previous configurations or caused by an **Advanced Flex Configuration** which lacks a keyword which can cause failures that the device report does not address.

Example Overview

Step 1. Click **Deployment**, which specifies the device to be selected.

Step 2. When the deployment for a device is committed, the FMC begins to collect all the configurations relevant to the device.

Step 3. When the configurations are collected, the FMC creates the package and sends it to the sensor over its communication mechanism called **SFTunnel**.

Step 4. The FMC notifies the sensor to start the deployment process with the provided policy while it listens for the individual responses.

Step 5. The managed device unpacks the archive and starts to apply the individual configurations and packages.

> A. The first half of the deployment is the **Snort** configuration where the **Snort** configuration is tested locally to ensure its validity.
>
> When proved to be valid, the new configuration is moved to the production directory for **Snort**. If validation fails, the policy deployment fails at this step.
>
> B. The second half of the deployment package load is for the LINA configuration where it is applied directly to the LINA process by the **ngfwManager** process.

If a failure occurs, the changes are rolled back and a policy deployment failure occurs.

Step 6. If both **Snort** and LINA packages are successful, the managed device signals **Snort** to restart or reload in order to load the new configuration and save all current configurations.

Step 7. If all messages are successful, the sensor sends a success message and waits for it to be acknowledged by the Management Center.

Step 8. Once received, the FMC marks the task as a success and allows the policy bundle to finish.

Troubleshooting

Problems encountered during **Policy Deployment** can be due to, but are not limited to:

1. Misconfiguration
2. Communication between FMC and FTD
3. Database and System health
4. Software defects and Caveats
5. Other Unique situations

Some of these issues can be easily fixed, while others can require assistance from the Cisco **Technical Assistance Center (TAC).**

The goal of this section is to provide techniques to isolate the issue or determine the root cause.

FMC Graphical User Interface (GUI)

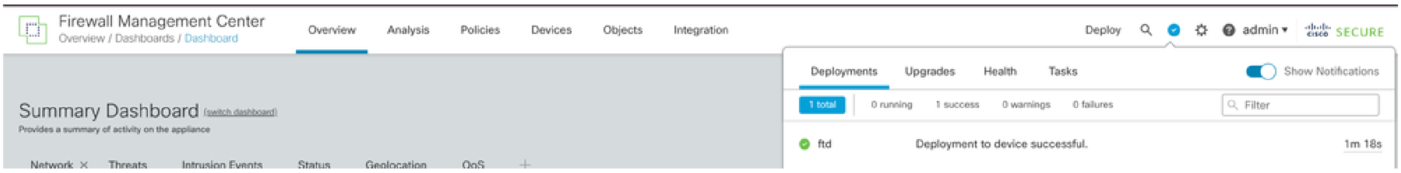
Cisco recommends each troubleshooting session for deployment failures to start on the FMC appliance.

On the failure notification window, on all versions beyond 6.2.3, there are additional tools that can assist with other possible failures.

Utilize the Deployment Transcripts

Step 1. Pull up the **Deployments** list on the **FMC Web UI**.

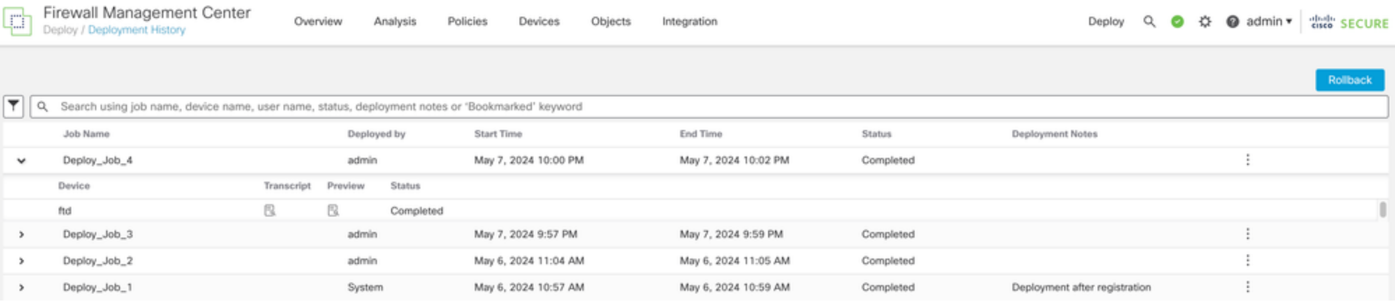
Step 2. While the **Deployments** tab is selected, click **Show History**.



ftd Deployment to device successful. 1m 18s

Step 3. Inside the **Deployment History** box, you can see all previous deployments from your FMC. Select the deployment in which you would like to see more data.

Step 4. Once a deployment element is selected, the **Deployment Details** selection displays a list of all devices inside the **Transaction**. These entries are broken down into these columns: **Device Number, Device Name, Status,**and **Transcript.**

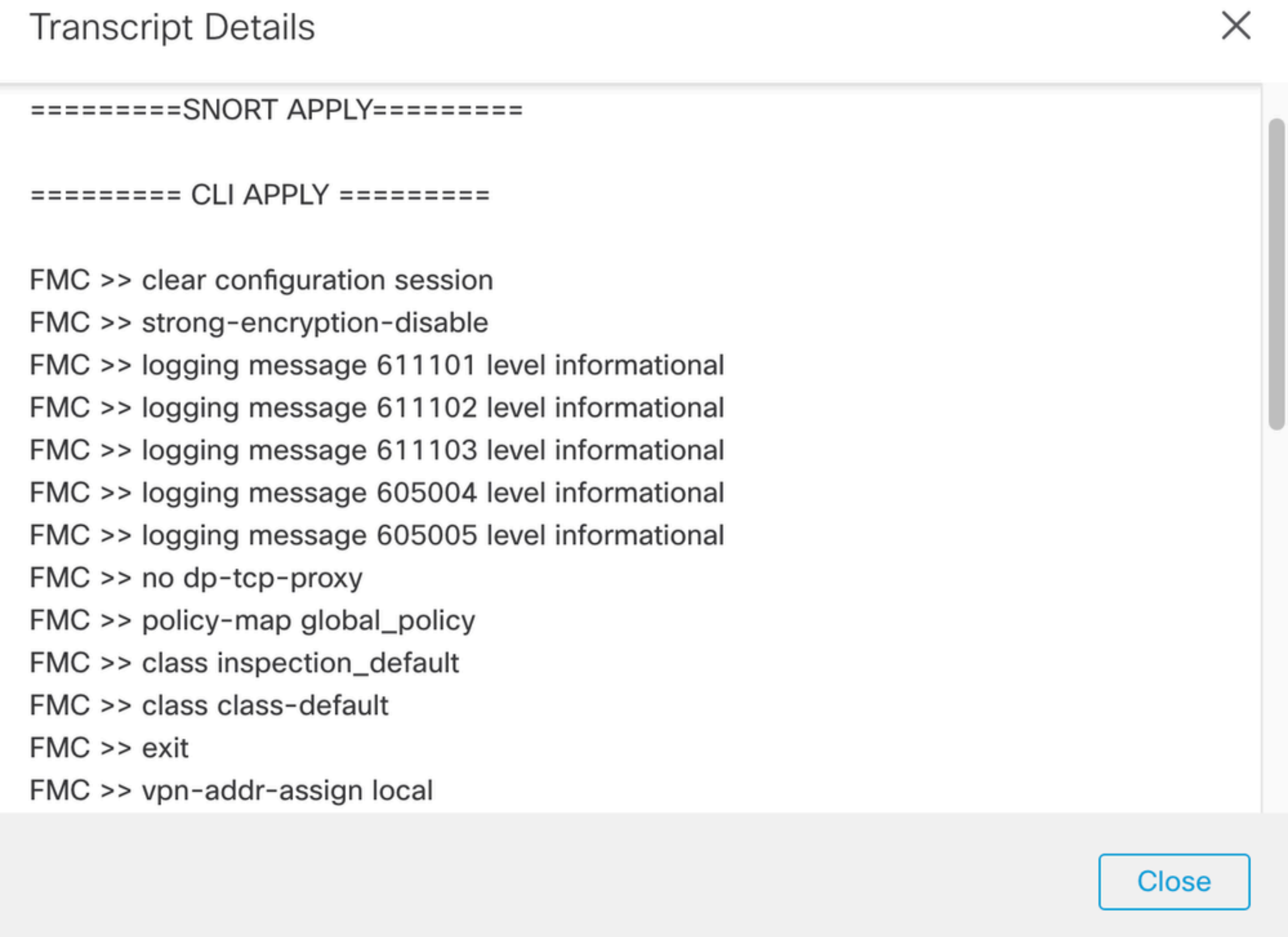

Firewall Management Center
Deploy / Deployment History
Overview
Analysis
Policies
Devices
Objects
Integration
Deploy
admin
SECURE
Rollback
Search using job name, device name, user name, status, deployment notes or 'Bookmarked' keyword

Job Name	Deployed by	Start Time	End Time	Status	Deployment Notes
Deploy_Job_4	admin	May 7, 2024 10:00 PM	May 7, 2024 10:02 PM	Completed	

Device	Transcript	Preview	Status
ftd			Completed

Job Name	Deployed by	Start Time	End Time	Status	Deployment Notes
Deploy_Job_3	admin	May 7, 2024 9:57 PM	May 7, 2024 9:59 PM	Completed	
Deploy_Job_2	admin	May 6, 2024 11:04 AM	May 6, 2024 11:05 AM	Completed	
Deploy_Job_1	System	May 6, 2024 10:57 AM	May 6, 2024 10:59 AM	Completed	Deployment after registration

Step 5. Select the device in question and click on the transcript option to see the individual deployment transcript which can inform you of failures as well as configurations that are placed on the managed devices.

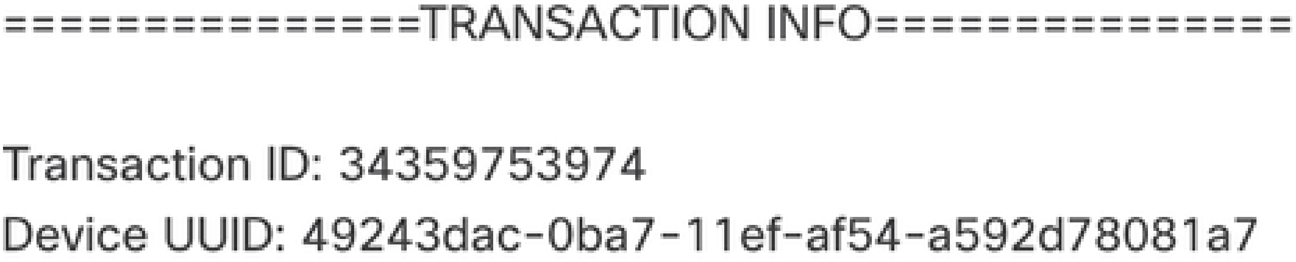


```
=========SNORT APPLY=========

========= CLI APPLY =========

FMC >> clear configuration session
FMC >> strong-encryption-disable
FMC >> logging message 611101 level informational
FMC >> logging message 611102 level informational
FMC >> logging message 611103 level informational
FMC >> logging message 605004 level informational
FMC >> logging message 605005 level informational
FMC >> no dp-tcp-proxy
FMC >> policy-map global_policy
FMC >> class inspection_default
FMC >> class class-default
FMC >> exit
FMC >> vpn-addr-assign local
```

Step 6. This transcript can designate certain failure conditions as well as indicate a very important number for the next step: **Transaction ID.**



```
================TRANSACTION INFO================

Transaction ID: 34359753974
Device UUID: 49243dac-0ba7-11ef-af54-a592d78081a7
```

Step 7. In a **Firepower Deployment**, the **Transaction ID** is what can be used to track each individual section of a policy deployment. With this, on the **Command-Line** of the Device, you can obtain a more in-depth version of this data for remediation and analysis.

Tip: In the event that you are unable to locate the transaction ID or if you are on a version before this was printed, this log can still be of use to locate individual failure messages.

Troubleshoot with FMC Logs

Though it is appropriate to engage Cisco TAC to analyze the logs, a search through logs can help with initial problem isolation and expedite resolution. There are multiple log files on FMC that reveal the details about the policy deployment process.

The two most commonly referenced logs are **policy_deployment.log** and **usmsharedsvcs.log**.

All the mentioned files in this document can be viewed with multiple Linux commands such as **more**, **less** and **vi**. However, it is very important to ensure that only **read** actions are performed to it. All files require root access to be able to view them.

/var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

This log clearly marks the start of the policy deployment task on FMC and the completion of each phase, which helps to determine the phase where deployment ran into a failure, along with the failure code.

The **transactionID** value included in the JSON portion of the log can be used to find log entries related to one particular deployment attempt.

```
10-May-2024 18:05:31.249,[INFO],(JsonRESTServerResource.java:111)
com.cisco.nm.vms.api.rest.DeploymentServerResource, ajp-nio-127.0.0.1-9009-exec-3
** REST Request [ DC ]
** ID : e45c6abd-0fff-4341-bdad-ddd5fee10034
** URL: POST https://localhost6/csm/api/deploy/GetTranscript
{
"data": {},
"deviceUUID": "49243dac-0ba7-11ef-af54-a592d78081a7",
"jobID": 34359753974,
"offset": {
"size": 20,
"start": 0
},
"requestID": "e3be908a0ef711ef9d519da21f9032fa",
"version": "7.2.5"
}
```

/var/log/sf/policy_deployment.log

While this log file has existed throughout 6.x releases, which start at 6.4, its coverage was expanded.

It now describes the detailed steps taken on FMC to build the deployment packages, therefore it is best used for to analyze failures from Phase 1 - 4.

The start of each phase is marked by a line with **INFO start** .

```
May 8 02:00:58 RTP-vFMC-Pod-09 ActionQueueScrape.pl[10413]: > SF::UMPD::CSMData::getPolicyRollbackInfo
May 8 02:00:58 RTP-vFMC-Pod-09 ActionQueueScrape.pl[10413]: < SF::UMPD::CSMData::getPolicyRollbackInfo
...
```

Managed Device Troubleshooting

There are additional phases and sections which depend on the device package, High Availability configuration, and the outcome of prior phases for each managed device.

If a deployment issue is isolated to a failure on the managed device, further troubleshooting can be performed on the device with two logs on the device: **policy_deployment.log** and **ngfwManager.log**.

/ngfw/var/log/ngfwManager.log

This log file provides detailed steps taken by **Config Communication Manager** and **Config Dispatcher** to communicate with FMC, work with the deployment package, and orchestrate the validation and application of **Snort** and LINA configurations.

These are a few examples of **ngfwManager.log** that represent the start of major phases:

```
FTD receives FMC's request for running configuration:

May 30 16:37:10 ccm[4293] Thread-10: INFO  com.cisco.ccm.ConfigCommunicationManager- Passing CD-Message
May 30 16:37:10 ccm[4293] Thread-10: DEBUG com.cisco.ccm.ConfigCommunicationManager- <?xml version="1.0
```

```
FTD receives FMC's request to download the deployment package:

May 30 16:37:18 ccm[4293] Thread-9: INFO  com.cisco.ccm.ConfigCommunicationManager- Downloading databas
May 30 16:37:18 ccm[4293] Thread-9: DEBUG com.cisco.ccm.DownloadManager- handle record: 8589938211, sta
May 30 16:37:18 ccm[4293] Thread-9: DEBUG com.cisco.ccm.DownloadManager- begin downloading database
```

```
FTD begins the deployment of policy changes:
```

```
May 30 16:37:21 ccm[4293] Thread-9: INFO  com.cisco.ccm.ConfigCommunicationManager- Starting deployment
May 30 16:37:21 ccm[4293] Thread-11: INFO  com.cisco.ccm.ConfigCommunicationManager- Sending message: D
```

```
FTD begins LINA deployment:

May 30 16:37:42 ccm[4293] Thread-19: DEBUG com.cisco.ngfw.configdispatcher.communicators.LinaCommunicat
```

```
FTD begins finalizing the deployment:

May 30 16:38:48 ccm[4293] Thread-19: DEBUG com.cisco.ngfw.configdispatcher.communicators.LinaCommunicat
Name:Cluster-App-Conf-Finalize-Request
```

/ngfw/var/log/sf/policy_deployment.log

This log contains the details of the policy applied to **Snort**. Though the content of the log is mostly advanced and requires analysis by TAC, it is still possible to trace the process with a few key entries:

```
Config Dispatcher begins extracting the packaged policies for validation:

Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO  -> calling SF::UMPD::Plugins::NGFWPolicy::Devic
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO  found NGFWPolicy =>   (NGFWPolicy::Util 32 <- N
...
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO export FTD platform settings... (PlatformSetting
```

```
Config validation begins:

Jul 18 17:21:37 firepower policy_apply.pl[25122]: INFO  starting validateExportedFiles - sqlite = /var/
```

```
Validation has completed successfully:

Jul 18 17:21:49 firepower policy_apply.pl[25122]: INFO validateExportedFiles - sqlite = /var/cisco/depl
```

```
Config Dispatcher begins moving the validated configuration to the Snort directories in production:

Jul 18 17:21:54 firepower policy_apply.pl[26571]: INFO  -> calling SF::UMPD::Plugins::NGFWPolicy::Devic
```

```
Snort processes will reload to apply the new configurations:

Jul 18 17:22:02 firepower policy_apply.pl[26571]: INFO  Reconfiguring DE a3bcd340-992f-11e9-a1f1-ac829f
Jul 18 17:22:02 firepower policy_apply.pl[26571]: INFO  sending SnortReload to a3bcd340-992f-11e9-a1f1-
```

```
Snort reload has completed successfully:
```

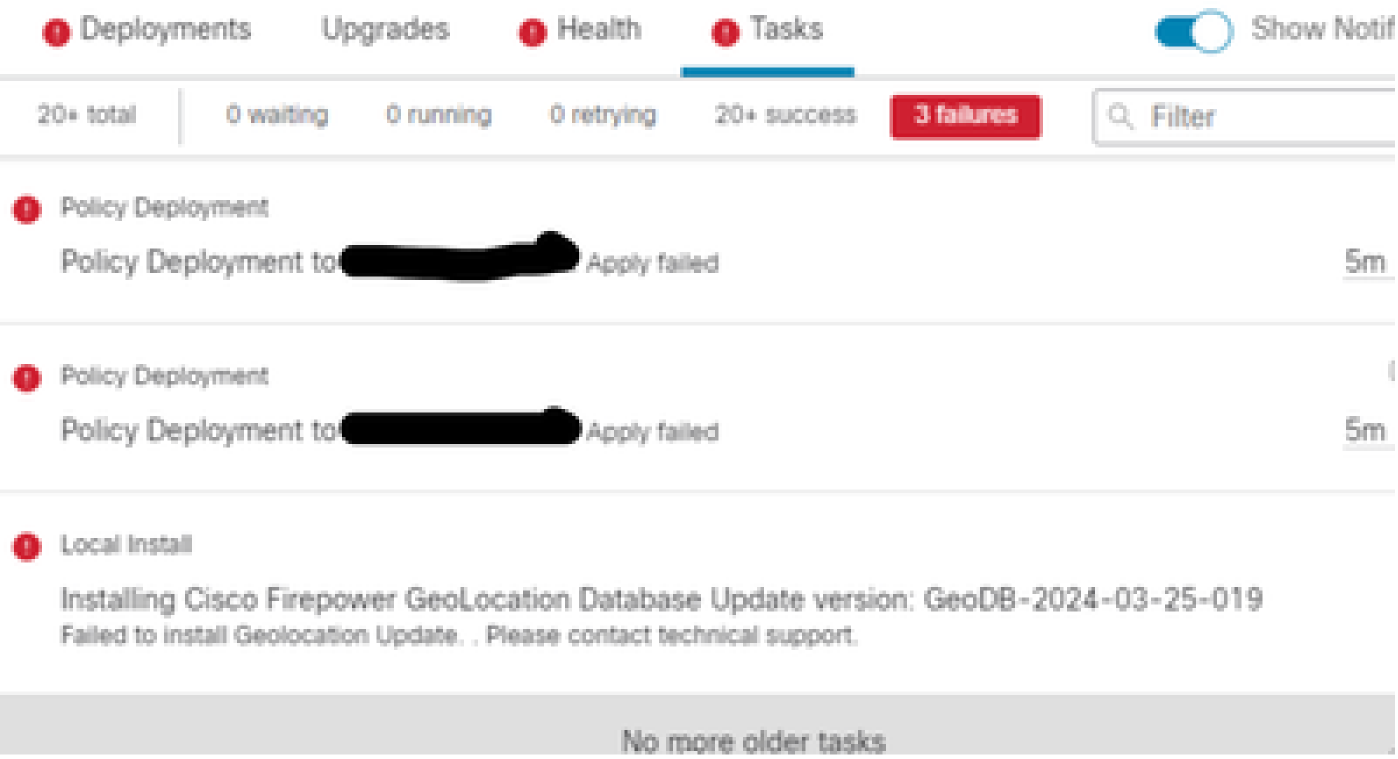
```
Jul 18 17:22:14 firepower policy_apply.pl[26571]: INFO notifyProcesses - sandbox = /var/cisco/deploy/sa
```

```
After LINA config apply finishes, Snort deployment is finalized:

Jul 18 17:23:32 firepower policy_apply.pl[26913]: INFO  starting finalizeDeviceDeployment - sandbox = /
```

Example

Step 1. A deployment fails



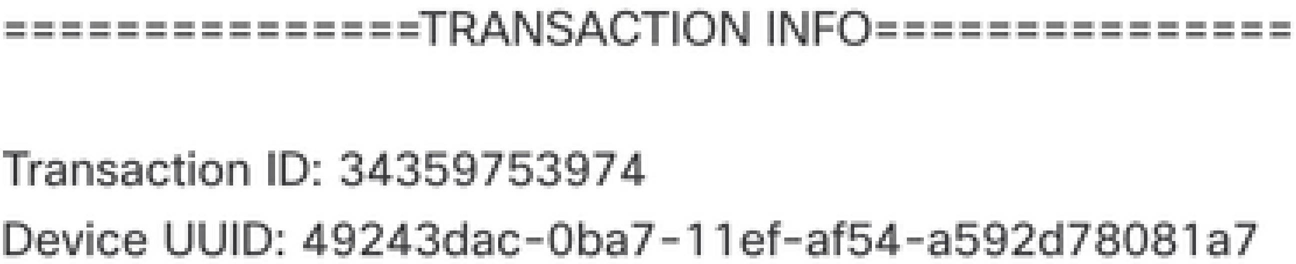
Policy Deployment
Policy Deployment to [redacted] Apply failed
5m

Policy Deployment
Policy Deployment to [redacted] Apply failed
5m

Local Install
Installing Cisco Firepower GeoLocation Database Update version: GeoDB-2024-03-25-019
Failed to install Geolocation Update. . Please contact technical support.

No more older tasks

Step 2. Obtain the **Deploy Transcript** and **Transaction ID**.

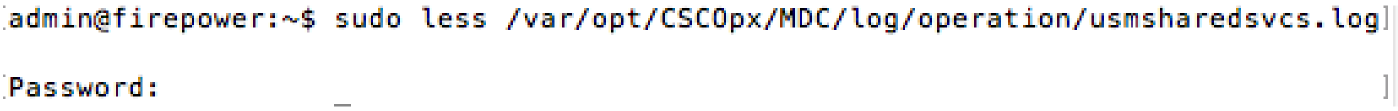


===============TRANSACTION INFO===============

Transaction ID: 34359753974
Device UUID: 49243dac-0ba7-11ef-af54-a592d78081a7

Step 3. SSH into your **Management Center** and utilize the Linux utility **less** to read the file as shown on your FMC:

Example: **sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log** (The sudo password is your user password for ssh.)



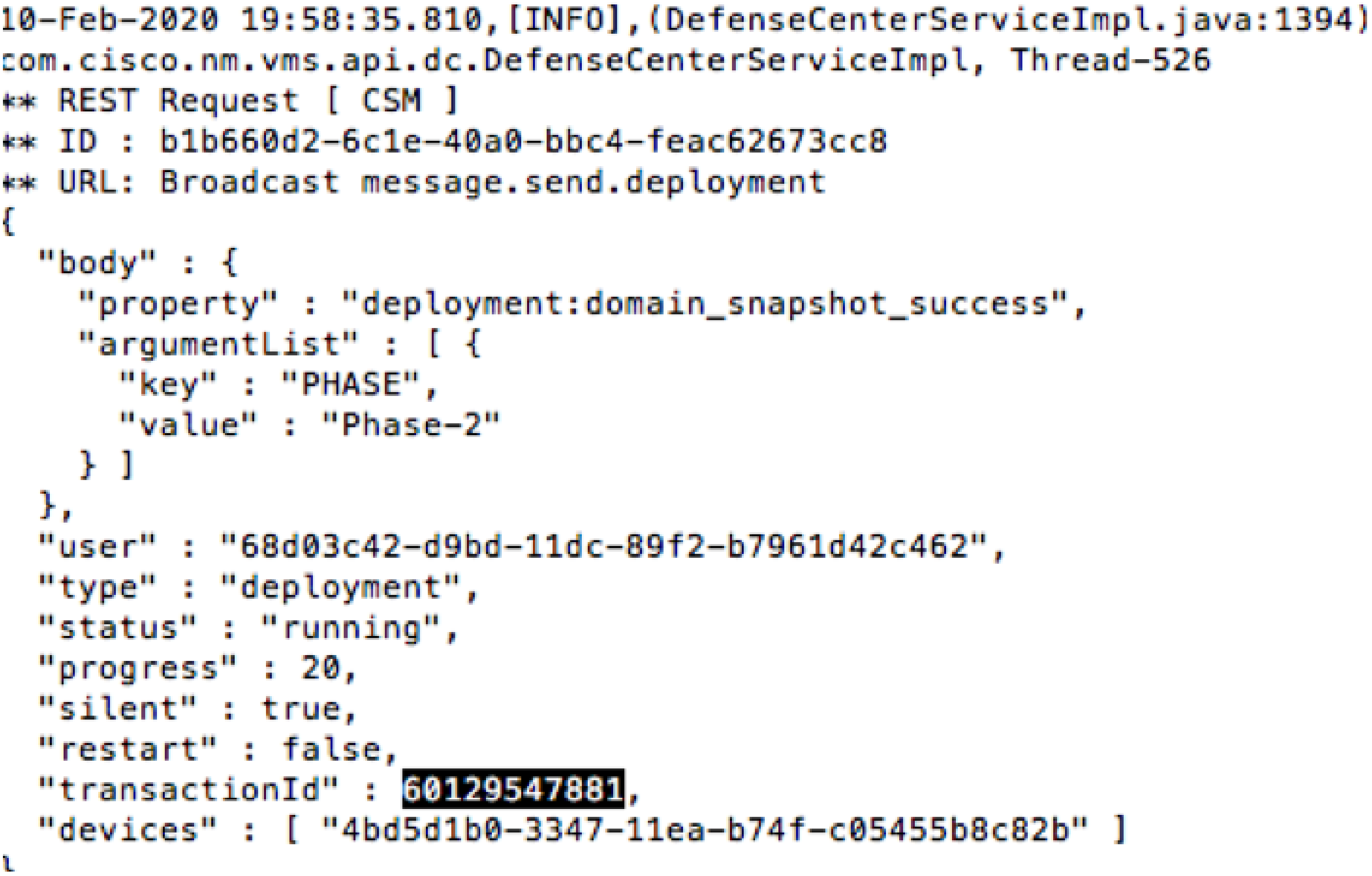
```
admin@firepower:~$ sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log

Password:
```

Step 4. When you are in **less**, use forward slash and enter in the message ID to search for the logs related to the deployment **transactionID**.

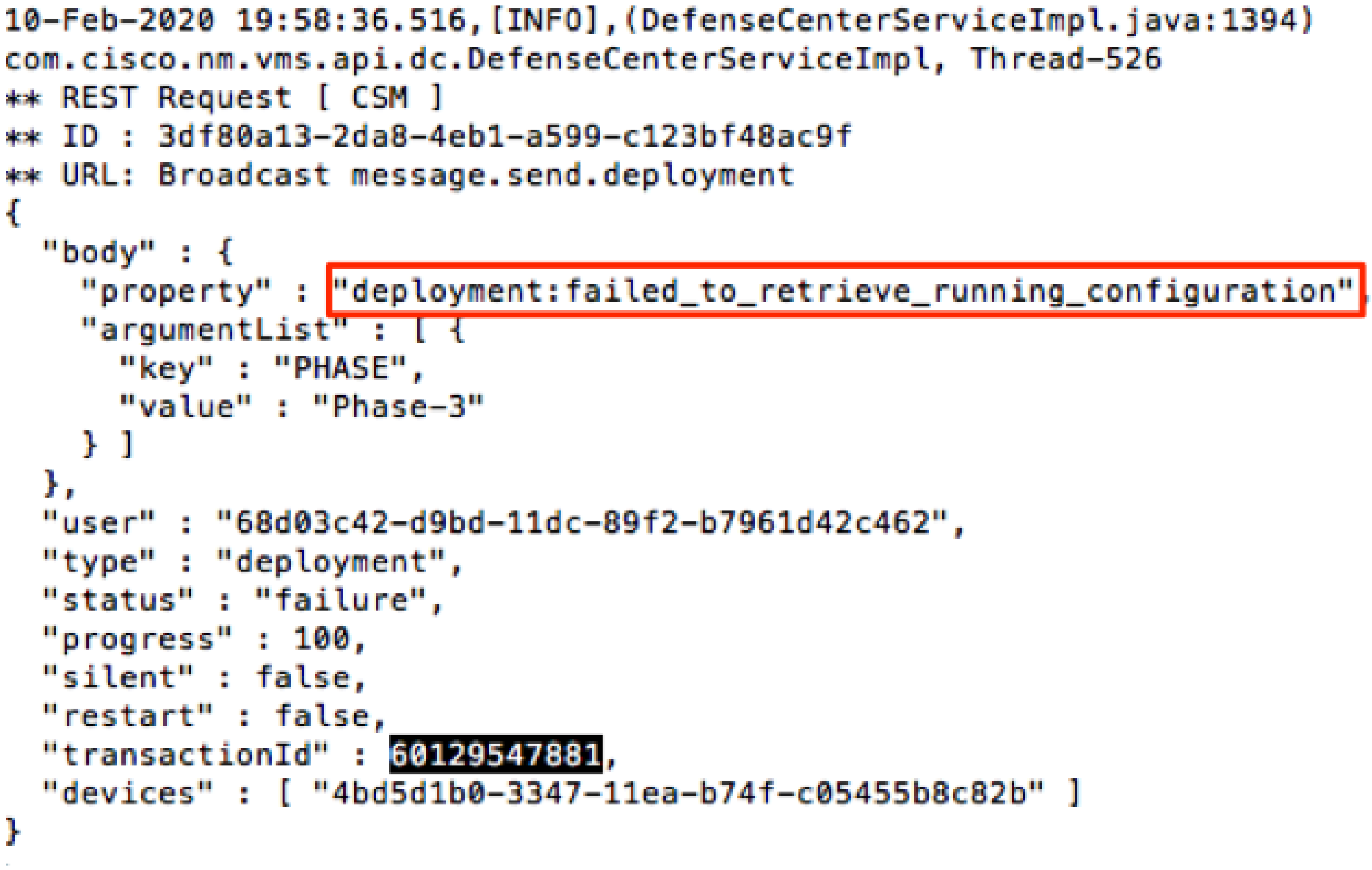
Example: **/60129547881** (While in**less**, use **n** to navigate to the next result.)

Example of Running Message



```
10-Feb-2020 19:58:35.810,[INFO],(DefenseCenterServiceImpl.java:1394)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, Thread-526
** REST Request [ CSM ]
** ID : b1b660d2-6c1e-40a0-bbc4-feac62673cc8
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:domain_snapshot_success",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-2"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "running",
  "progress" : 20,
  "silent" : true,
  "restart" : false,
  "transactionId" : 60129547881,
  "devices" : [ "4bd5d1b0-3347-11ea-b74f-c05455b8c82b" ]
}
```

Example of Failure Message



```
10-Feb-2020 19:58:36.516,[INFO],(DefenseCenterServiceImpl.java:1394)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, Thread-526
** REST Request [ CSM ]
** ID : 3df80a13-2da8-4eb1-a599-c123bf48ac9f
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:failed_to_retrieve_running_configuration",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-3"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "failure",
  "progress" : 100,
  "silent" : false,
  "restart" : false,
  "transactionId" : 60129547881,
  "devices" : [ "4bd5d1b0-3347-11ea-b74f-c05455b8c82b" ]
}
```

5) Compare the proper failure to the attached table of **Common Failure Messages**.

That is, **failed_to_retrieve_running_configuration** occurs during communication failures between the two devices.

Common Failure Messages

These are common failure messages that can be seen on the front end of the **Management Center Task** as well as the error code which can be seen in the backend.

These messages can be analyzed and compared with the common reasons for possible resolutions.

In the event that these are not seen, or do not resolve your situation, please contact TAC for assistance.

Error code	**Error messages**	**Reas**
device_has_changed_domain	**Deployment failure - The device has changed domain from {SRCDOMAIN} to {DESTINATIONDOMAIN}. Try again later.**	**This typica when has m is tak secon A re- while doma**

		infor occur amen issue.
device_currently_under_deployment	**Deployment failed due to another deployment in progress for this device. Try again later.**	**This i repor deplo trigge devic deplo some this is witho notifi howe phase for troub assist**
device_not_member_of_container	**Deployment cannot be performed on an individual device that is a member of a cluster. Try to deploy the cluster again later.**	**This r applic FTD with t Firep eXter Oper Syste Chass Mana cluste FXOS on th messa show create on th Mana Cente befor attem deplo**
policy_altered_after_timestamp_for_other_devices_in_job_error	**Policies for one or more devices have been altered since {TIMESTAMP}. Retry deployment.**	**This c show policy altere devic deplo after**

		trigge and b eleme doma snaps create redep this is This when use th FMC save while deplo
policy_altered_after_timestamp_error	Policy {Policy Name} has been altered since {Timestamp}. Retry deployment.	This showi policy altere conce in the deplo after trigge and b and d snaps create redep this is
csm_snapshot_error	Deployment failed due to failure of collection of policies and objects. If problem persists after a repeated attempt contact Cisco TAC.	If a re Impo provi hour attem deplo If this allow proce conta is a d relate
domain_snapshot_timeout	Deployment failed due to timeout to collect policies and objects. If problem persists after another attempt, contact Cisco TAC.	The c snaps timeo minu defau

		syster high l hyper malfu this c unnat in the This c the M Cente is not the pr amou memo resou If this witho does r at a la conta
domain_snapshot_errors	Deployment failed in policy and object collection. If problem persists after another attempt, contact Cisco TAC.	Conta Adva troub is req
failed_to_retrieve_running_configuration	Deployment failed due to failure to retrieve run configuration information from device. Retry deployment.	This r occur conne betwe senso FMC funct expec the tu betwe and m conne betwe devic If the work expec devic comn conta

device_is_busy	Deployment failed as device can be running a previous deployment or a restart. If problem persists after another attempt, contact Cisco TAC.	This r showr FMC deplo previc deplo progre Typic when deplo unfini FTD a reboo **ngfwl** proce restar after 2 allow forma must issue. If afte if the accep conta
no_response_for_show_cmd	Deployment failed due to connectivity issues with the device or device does not respond. If problem persists after another attempt, contact Cisco TAC.	FMC certai LINA comm fetch config config gener This c when conne proble with t **ngfwl** proce senso In the you a conne issues your u

		TAC.
network_latency_or_device_not_reachable	Deployment failed due to communications failure with device. If problem persists after another attempt, contact Cisco TAC.	Usual with l latenc the de cause timeo the ne latenc devic match minin versio in the
slave_app_sync	Deployment failed as cluster configuration synchronization is in progress. Retry deployment.	This i only f cluste deplo attem FTD (app sync(sync) progr is reje FTD. confi must issue. The c status tracke comm mana CLIS > **sho** info
asa_configuration_generation_errors	Deployment failed to generate device configuration. If problem persists after another attempt, contact Cisco TAC.	After of the menti you c see w confi cause These

		bugs i logs o brows the Ci Tool conta TAC troubl furthe
interface_out_of_date	Deployment failed because interfaces on device are out of date. Save the configuration on the interfaces page and retry.	This 4100 mode interf unass the de or rig deplo Verify interf assoc unass befor the de
device_package_error	Deployment failed to generate configuration for device. If problem persists after another attempt, contact Cisco TAC.	This e indica gener devic config the de Conta
device_package_timeout	Deployment failed due to timeout during configuration generation. If problem persists after another attempt, contact Cisco TAC.	This latenc betwe devic the no Conta after t norma issue
device_communication_errors	Deployment failed due to failure with device communication. Check network connectivity and retry deployment.	This the fa any comm

		issues devic vague writte fallba that a conne has oc
unable_to_initiate_deployment_dc	Policy deployment failure. Retry deployment.	Anoth must issue. This c when unabl deplo a tem on the
device_failure_timeout	Deployment to device failed due to timeout. Retry deployment.	This i FTD Proce wait 3 for th comp deplo not, it If this verify conne the co as exp Conta
device_failure_download_timeout	Deployment failed due to configuration download timeout to device. If problem persists after another attempt, contact Cisco TAC.	This i FTD The F to dov devic config durin to con issues Please netwo conne been

		If this verifi TAC.
device_failure_configuration	Deployment failed due to configuration error. If problem persists after another attempt, contact Cisco TAC.	Any e config gener for th must **error** This r analy USM verify are se attem them Once this u requir interv bug c logs c match know the C Searc
deployment_timeout_no_response_from_device	Deployment failed due to communication timeout with device. If problem persists after another attempt, contact Cisco TAC.	This t occur has n from after s This i comm error. Verify comm and if conta
device_failure_change_master	Deployment to cluster failed as primary unit has changed. Retry deployment.	For ar cluste

		deplo prima switc deplo progr devic notifi error Retry prima stable The c memb be tra this c the m devic > **sho** info
device_failure_unknown_master	Deployment to cluster failed due to primary unit identification failure. Retry deployment.	FMC unabl deterr curren node deplo Typic due to possil either issues prima added cluste It mus resolv conne reesta after a the cu prima FMC retry The c status tracke comm

		mana CLIS > **sho** info
cd_deploy_app_sync	Deployment failed as cluster configuration synchronization is in progress. Retry deployment.	This c the de App S App S comp retry c once r
cd_existing_deployment	Deployment failed due to conflict with concurrent previous deployment. If problem persists after another attempt, contact Cisco TAC.	This c deplo concu side, l other. These cause comm issues device If afte occur are st deplo TAC.

Related Information

- Troubleshoot Firepower File Generation Procedures
- Cisco Technical Support & Downloads