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.

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.

Prerequisites

Cisco recommends knowledge of these products:

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

Components Used

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.

Policy Deployment Overview

Cisco FTD utilizes **Policy Deployments** to manage and push out configurations for devices that are registered to the **Firepower 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 failues 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 proven 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** might be due to, but 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 might be easily fixed, while others might 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)

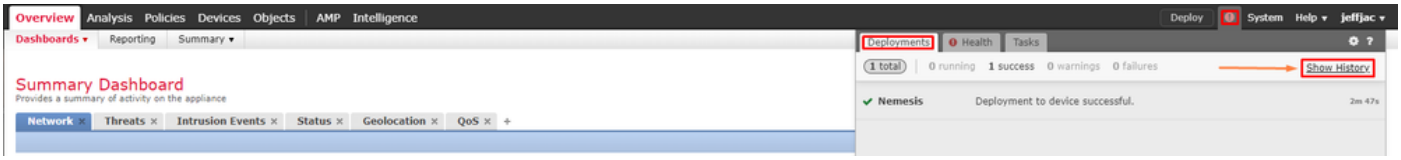
Cisco recommends each troubleshooting session for deployment failures to start on the FMC appliance.

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

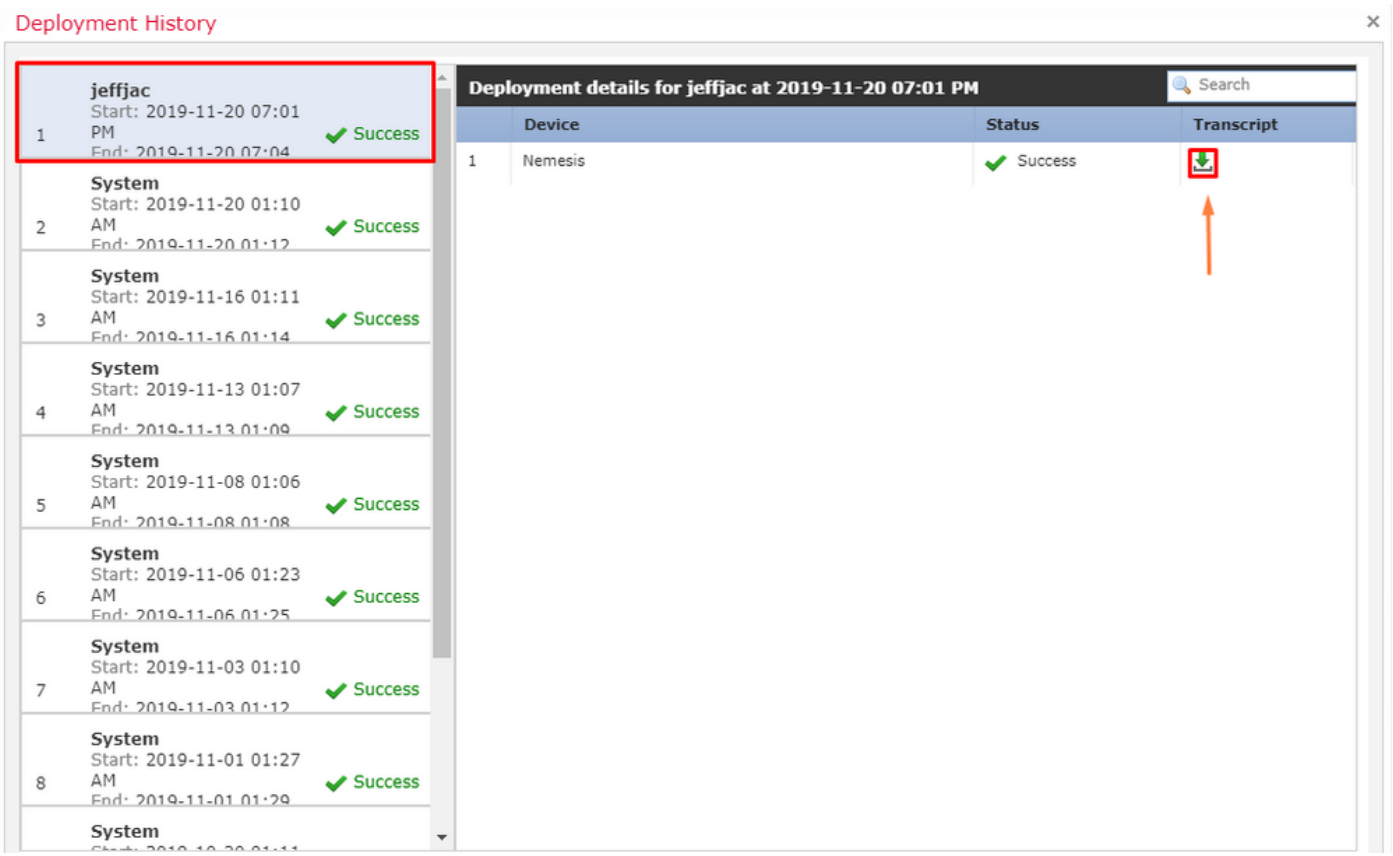
Step 1. Pull up the **Deployments** list on the **FMC Web UI**.

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

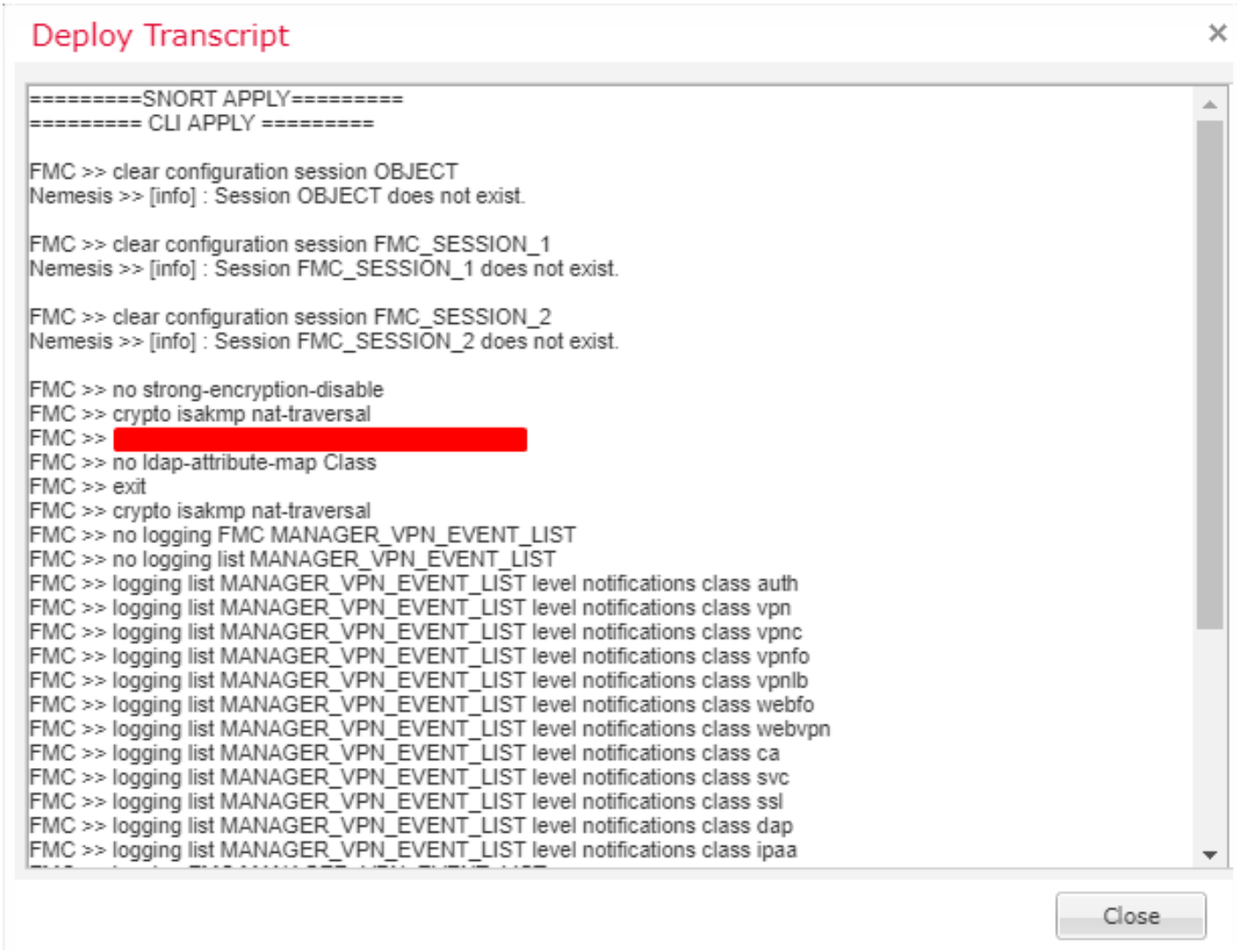


Step 3. Inside the **Deployment History** box, you can see all previous deployments from your FMC. Select the deployment in which you would like to see more data.

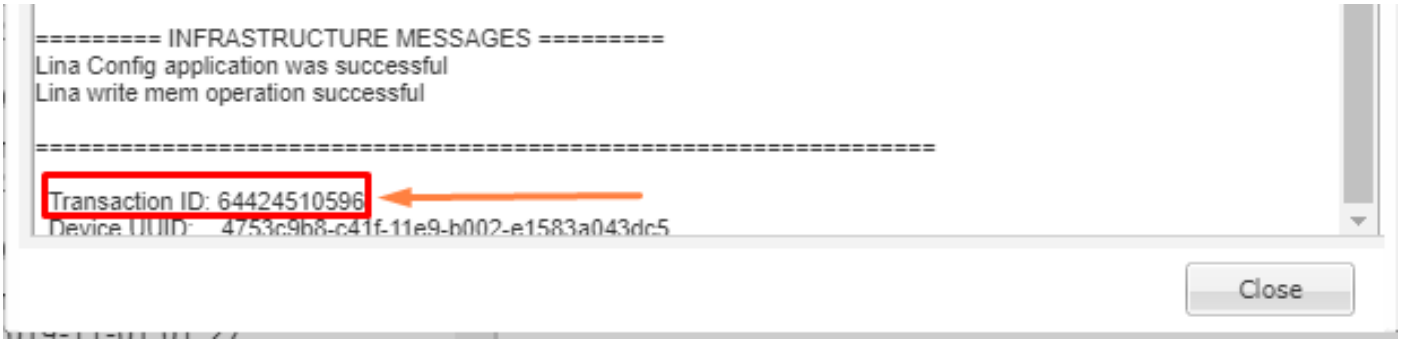
Step 4. Once a deployment element is selected, the **Deployment Details** selection displays a list of all devices inside the **Transaction**. These entries are broken down into these columns: **Device Number, Device Name, Status,** and **Transcript.**



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.



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



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 might 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.

```
22-Nov-2019 01:28:52.844,[INFO],(DefenseCenterServiceImpl.java:1372)
com.cisco.nm.vms.api.dc.DefenseCenterServiceImpl, ajp-nio-127.0.0.1-9009-exec-4
** REST Request [ CSM ]
** ID : e1c84364-0966-42eb-9356-d2914be2b4a3
** URL: Broadcast message.send.deployment
{
  "body" : {
    "property" : "deployment:deployment_initiated_for_the_device",
    "argumentList" : [ {
      "key" : "PHASE",
      "value" : "Phase-0"
    } ]
  },
  "user" : "68d03c42-d9bd-11dc-89f2-b7961d42c462",
  "type" : "deployment",
  "status" : "running",
  "progress" : 5,
  "silent" : true,
  "restart" : true,
  "transactionId" : 12884916552,
  "devices" : [ "93a2089a-fa82-11e9-8219-e1abeec81dc9" ]
}
```

/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 analuze failures from Phase 1 - 4.

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

```
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO starting populateGlobalSnapshot -
sqlite = /var/cisco/umpd/8589938337/DC_policy_deployment.db, transaction = 8589938337, time =
1563470402, running as (memory = 56.35 MB) (Framework 3950<196 <- CSMTasks 223<10 <-
SF::ActionQueue 2457)
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO deployment threading: disabled
(Framework 198 <- CSMTasks 223<10 <- SF::ActionQueue 2457)
Jul 18 17:20:03 firepower ActionQueueScrape.pl[17287]: INFO -> calling
SF::UMPD::Plugins::Correlation::Manager::getPluginDependencies (Plugin 298<90 <- Framework
3579<3566<216 <- CSMTasks 223)
...
```

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-Request to Config Dispatcher...
May 30 16:37:10 ccm[4293] Thread-10: DEBUG com.cisco.ccm.ConfigCommunicationManager- <?xml
version="1.0" encoding="UTF-
8"?><cdMessagesList><timeStamp>1559234230012</timeStamp><cdMessage><name>LinaShowCommand</name><
messageId>-
7531335374431513 90</messageId><contentType>XML</contentType><msgContent><![CDATA[<?xml
version="1.0" encoding="UTF-8"?><message><name>LinaShowCommand</name>...



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
database (transaction 8589938211, version 1559234236)
May 30 16:37:18 ccm[4293] Thread-9: DEBUG com.cisco.ccm.DownloadManager- handle record:
8589938211, status = PENDING
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: DEPLOYMENT_STATUS_CCM to Manager
```

```
FTD begins LINA deployment:

May 30 16:37:42 ccm[4293] Thread-19: DEBUG
com.cisco.ngfw.configdispatcher.communicators.LinaCommunicatorImpl- Trying to send Start-Config-
Sequencerequest to lina
```

```
FTD begins finalizing the deployment:

May 30 16:38:48 ccm[4293] Thread-19: DEBUG
com.cisco.ngfw.configdispatcher.communicators.LinaCommunicatorImpl- Clustering Message sent out
of ConfigDispatcher:
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's 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::Device::exportDeviceSnapshotToSandbox  (Plugin 230 <- Framework
611 <- Transaction 1085)
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO  found NGFWPolicy =>   (NGFWPolicy::Util
32 <- NGFWPolicy::Device 43 <- Plugin 235)
...
Jul 18 17:20:57 firepower policy_apply.pl[25122]: INFO export FTD platform settings...
(PlatformSettings::FTD::Device 29 <- Plugin 235<339 <- PlatformSettings::Device 13)
```

```
Config validation begins:

Jul 18 17:21:37 firepower policy_apply.pl[25122]: INFO  starting validateExportedFiles - sqlite
= /var/cisco/deploy/sandbox/policy_deployment.db, sandbox = /var/cisco/deploy/sandbox/exported-
files (memory = 229.99 MB)  (Framework 3950<687 <- Transaction 1101 <- main 194)
```

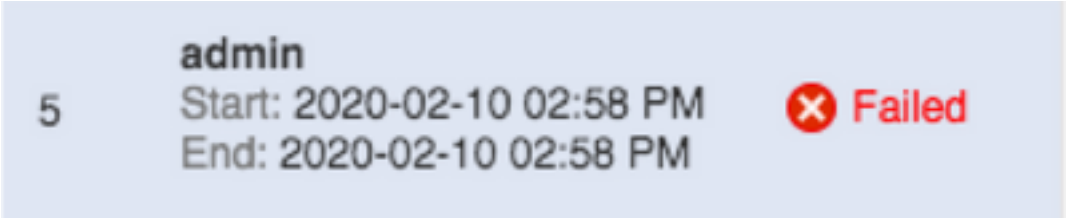
```
Validation has completed successfully:

Jul 18 17:21:49 firepower policy_apply.pl[25122]: INFO validateExportedFiles - sqlite =
/var/cisco/deploy/sandbox/policy_deployment.db, sandbox = /var/cisco/deploy/sandbox/exported-
files took 12 (memory = 238.50 MB, change = 8.51 MB) (Framework 3976<724 <- Transaction 1101 <-
main 194)
```

```
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::Device::publishExportedFiles  (Plugin 230 <- Framework 822 <-
```

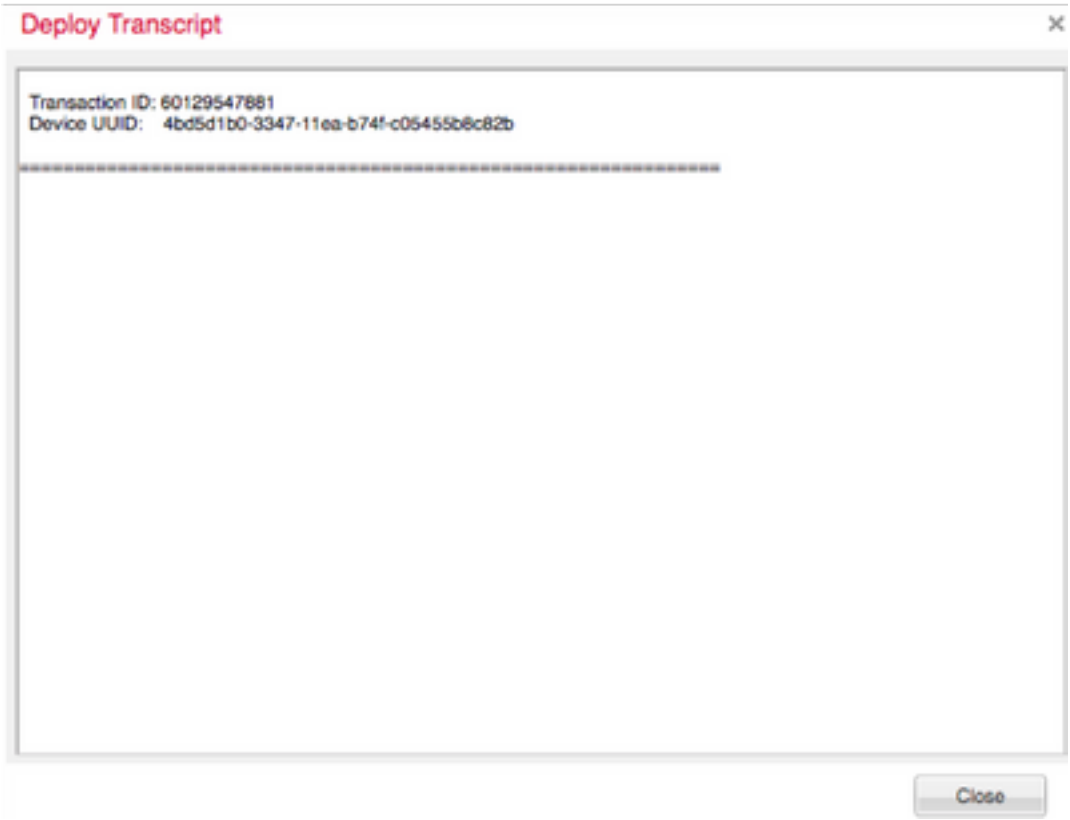
```
Transaction 1662)


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-ac829f31a4f9...  (Snort::SnortNotifications 292<154 <- Snort::Device 343 <- Plugin 235)
Jul 18 17:22:02 firepower policy_apply.pl[26571]: INFO  sending SnortReload to a3bcd340-992f-
11e9-a1f1-ac829f31a4f9  (Snort::SnortNotifications 298<154 <- Snort::Device 343 <- Plugin 235)


Snort reload has completed successfully:

Jul 18 17:22:14 firepower policy_apply.pl[26571]: INFO notifyProcesses - sandbox =
/var/cisco/deploy/sandbox/exported-files took 16 (memory = 169.52 MB, change = 16.95 MB)
(Framework 3976<964 <- Transaction 1680 <- main 200)


After LINA config apply finishes, Snort deployment is finalized:

Jul 18 17:23:32 firepower policy_apply.pl[26913]: INFO  starting finalizeDeviceDeployment -
sandbox = /var/cisco/deploy/sandbox (memory = 101.14 MB)  (Framework 3950<980 <- Transaction
1740 <- main 206)
```

Example

Step 1. A deployment fails



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



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 users 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**.

I.e. 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	Reason
device_has_changed_domain	**Deployment failure - The device has changed domain from {SRCDOMAIN} to {DESTINATIONDOMAIN}. Try again later.**	**This error typically occur when a device has move is taken from a second domain. A re-deploy whil cross-domain information occurs usually amends th issue.**
device_currently_under_deployment	**Deployment failed due to another deployment in progress for this device. Try again later.**	**This is typically reported when deployment is trigg on a device in deploymen some versions, this is prevented without a failu notification; however, thi phase still exists for troubleshooting assistan**
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 message is applicab for FTD on devices with t Firepower eXtensible Operative System (FXOS) Chassis Manager. If the cluster is built on FXOS, not on the FMC, this mes is shown. Please create t cluster on the Manageme Center appliance before y attempt to deploy.**

policy_altered_after_timestamp_for_other_devices_in_job_error	Policies for one or more devices have been altered since {TIMESTAMP}. Retry deployment.	This error is shown If any policy/object is altered fo device in the deployment after user triggers deploy before CSM elements and domain snapshots are created. A redeploy fixes issue. This can occur when mar users use the same FMC edit and save objects wh they deploy.
policy_altered_after_timestamp_error	Policy {Policy Name} has been altered since {Timestamp}. Retry deployment.	This error is shown If any policy/object is altered fo concerned device in the deployment job, after use triggers deploy and befor CSM and domain snapsh are created. A redeploy f this issue.
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 recent Policy Import i provided, wait an hour or and attempt another depl If this does not allow this proceed to, contact TAC is a database related message.
domain_snapshot_timeout	Deployment failed due to timeout to collect policies and objects. If problem persists after another attempt, contact Cisco TAC.	The domain snapshot ha timeout of 5 minutes by default. If the system is u high load, or the hypervis malfunctions, this can ca unnatural delays in the ca This can occur if the Management Center or de is not provided the prope amount of memory resou as well. If this happens without lo or does not proceed at a time, contact TAC.

domain_snapshot_errors	**Deployment failed in policy and object collection. If problem persists after another attempt, contact Cisco TAC.**	**Contact TAC. Advanced troubleshooting is requir**
failed_to_retrieve_running_configuration	**Deployment failed due to failure to retrieve run configuration information from device. Retry deployment.**	**This message can occur connectivity between an sensor and an FMC does function as expected. Ve the tunnel health betwee units and monitor the connectivity between the devices.** **If the tunnel works as expected and the devices communicate, contact TA**
device_is_busy	Deployment failed as device might be running a previous deployment or a restart. If problem persists after another attempt, contact Cisco TAC.	This message is shown, wh FMC attempts a deploy, wh previous deployment is in progress on FTD. Typically happens when a previous deployment is unfinished o FTD and the FTD rebooted the ngfwManager process FTD restarted. A retry after minutes to allow processes formally timeout should res this issue. If after a delay or if the dela not acceptable, contact TA

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 issues certain LINA "s commands to fetch the run configuration for configurat generation. This can happen when ther connectivity problems or is with the ngfwManager proc on the end sensor. In the event that you are no facing connectivity issues between your units, contac TAC.
network_latency_or_device_not_reachable	Deployment failed due to communications failure with device. If problem persists after another attempt, contact Cisco TAC.	Usually occurs with high network latency between th devices to cause a policy timeout. Verify the network latency between devices to verify it matches the minim for the version mentioned i user guide.

slave_app_sync	Deployment failed as cluster configuration synchronization is in progress. Retry deployment.	This is applicable only for F cluster setups. If a deploym is attempted on an FTD clu while app sync(configuratio sync) is in progress, the sa rejected by FTD. A retry aft configuration sync should s this issue. The current cluster status c be tracked with this comma the managed device CLISH >show cluster info
asa_configuration_generation_errors	Deployment failed to generate device configuration. If problem persists after another attempt, contact Cisco TAC.	After review of the USMS L mentioned earlier, you mig able to see which configura is causes the error. These usually bugs in which the lo can be browsed through th Cisco Bug Tool or contact TAC to troubleshoot further
interface_out_of_date	Deployment failed because interfaces on device are out of date. Save the configuration on the interfaces page and retry.	This occurs on 4100's or 9 models if the interface is unassociated from the devi during or right before a dep Verify that the interface is f associated or unassociated before you attempt the deployment.
device_package_error	Deployment failed to generate configuration for device. If problem persists after another attempt, contact Cisco TAC.	This error indicates failure t generate the device configuration for the device Contact TAC.
device_package_timeout	Deployment failed due to timeout during configuration generation. If problem persists after another attempt, contact Cisco TAC.	This can happen if latency between the devices beyon normal ranges. Contact TA after the latency is normaliz this issue still occurs.

device_communication_errors	Deployment failed due to failure with device communication. Check network connectivity and retry deployment.	This message is the fallbac any communication issues between the devices. Due Vague nature, it is written a fallback to state that an unknown connectivity error occurred.
unable_to_initiate_deployment_dc	Policy deployment failure. Retry deployment.	Another attempt should sol this issue. This can occur when the F unable to start the deploym due to a temporary lock on database.
device_failure_timeout	Deployment to device failed due to timeout. Retry deployment.	This is related to FTD deployment. Processes on wait 30 minutes for the disp to complete deployment. If times out. If this occurs, verify inter-d connectivity and if the connectivity is as expected Contact TAC.
device_failure_download_timeout	Deployment failed due to configuration download timeout to device. If problem persists after another attempt, contact Cisco TAC.	This is related to FTD deployment. The FTD is ur to download all device configuration files during d due to connectivity issues. Please retry after network connectivity has been verif If this has been verified, co TAC.
device_failure_configuration	Deployment failed due to configuration error. If problem persists after another attempt, contact	Any errors in the configurat generated by FMC for the device should result in this

	Cisco TAC.	post apply. This needs to be analyzed USMS logs to verify what is are seen and attempt to rol them back. Once repaired, this usually requires TAC intervention a bug creation if the logs can be matched with a known c at the Cisco Bug Search To
deployment_timeout_no_response_from_device	Deployment failed due to communication timeout with device. If problem persists after another attempt, contact Cisco TAC.	This timeout occurs if the F has not heard back from a device after 45 minutes or soone. This is a communication er Verify communication and verified, contact TAC.
device_failure_change_master	Deployment to cluster failed as primary unit has changed. Retry deployment.	For an FTD cluster setup deployment, if the primary switches when deployment progress on the device (po notification), this error is indicated. Retry once the primary nod stable. The current cluster membe status can be tracked with command in the managed device CLISH: >show cluster info
device_failure_unknown_master	Deployment to cluster failed due to primary unit identification failure. Retry deployment.	FMC has been unable to determine the current prima node during deploy. This could be typically due couple of possibilities: Eithe connectivity issues or curre primary not added to the cl on FMC. It should get resolved after connectivity is reestablishe

		after addition of the current primary to the FMC cluster a retry is done. The current cluster status c be tracked with this comma the managed device CLISH >show cluster info
cd_deploy_app_sync	Deployment failed as cluster configuration synchronization is in progress. Retry deployment.	This can occur if the device App Sync, once App Sync complete, please retry deployment once more.
cd_existing_deployment	Deployment failed due to conflict with concurrent previous deployment. If problem persists after another attempt, contact Cisco TAC.	This can occur if a deploym is concurrent on one side, not the other. These are usually caused b communication issues betw the devices. Contact TAC if after the tim occurs, you are still unable deploy.

Contact TAC for Assistance

In the event that the previous information does not allow for a policy deployment to proceed, or if the issue appears to not be related to a pre-existing documented behavior, please use the steps provided in the next link to generate a Troubleshoot file and reach out to TAC for analysis and bug creation.

https://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-technote-SourceFire-00.html