

Solución de problemas de implementaciones de políticas de Firepower Threat Defence

Contenido

[Introducción](#)

[Antecedentes](#)

[Prerequisites](#)

[Componentes Utilizados](#)

[Descripción general de implementación de políticas](#)

[Ejemplo de descripción general](#)

[Resolución de problemas](#)

[Interfaz gráfica de usuario \(GUI\) de FMC](#)

[Utilizar Las Transcripciones De Implementación](#)

[Resolución de problemas con registros FMC](#)

[/var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log](#)

[/var/log/sf/policy_deployment.log](#)

[Solución de problemas de dispositivos administrados](#)

[/ngfw/var/log/ngfwManager.log](#)

[/ngfw/var/log/sf/policy_deployment.log](#)

[Ejemplo:](#)

[Mensajes de fallos comunes](#)

[Póngase en contacto con TAC para obtener asistencia](#)

Introducción

Este documento describe una descripción general de alto nivel del proceso de implementación de políticas en FTD, así como técnicas básicas de solución de problemas.

Antecedentes

Con Cisco Firepower Threat Defense (FTD), las funciones de firewall stateful tradicionales ofrecidas por Adaptive Security Appliances (ASA) y Next-Gen funciones de firewall (con tecnología Snort) ahora se combinan en un solo producto.

Debido a este cambio, Policy Deployment Infrastructure en FTD ahora gestiona los cambios de configuración tanto para el código ASA (también denominado LINA) como para Snort en un paquete.

Prerequisites

Cisco recomienda conocer estos productos:

- Firepower Management Center (FMC)

- Firepower Threat Defense (FTD)

Componentes Utilizados

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Descripción general de implementación de políticas

Cisco FTD utiliza **Policy Deployments** para administrar y desplegar las configuraciones de los dispositivos registrados en el **Firepower Management Center (CSP)**.

Dentro de la implementación, hay una serie de pasos que se dividen en "fases".

Las fases del CSP pueden resumirse en esta lista.

Fase 0	Inicialización de implementación
Fase 1	Colección de objetos de base de datos
Fase 2	Colección de políticas y objetos
Fase 3	Generación de configuración de línea de comandos NGFW
Fase 4	Generación de paquetes de implementación de dispositivos
Fase 5	Enviar y recibir el paquete de implementación
Fase 6	Mensajes de implementación, acciones de implementación y éxito de implementación pendiente

El conocimiento de las fases y de la ubicación de los fallos en el proceso puede ayudar a solucionar los fallos que **Firepower** causa del sistema.

En algunas situaciones, puede ser un conflicto debido a configuraciones anteriores o causado por un **Advanced Flex Configuration** que carece de una palabra clave que puede causar fallas que el informe del dispositivo no aborda.

Ejemplo de descripción general

Paso 1. Haga clic en **Deployment**, que especifica el dispositivo que se va a seleccionar.

Paso 2. Cuando se confirma la implementación de un dispositivo, el FMC comienza a recopilar todas las configuraciones relevantes para el dispositivo.

Paso 3. Cuando se recopilan las configuraciones, el FMC crea el paquete y lo envía al sensor a través de su mecanismo de comunicación llamado **SFTunnel**.

Paso 4. El FMC notifica al sensor que inicie el proceso de despliegue con la política proporcionada mientras escucha las respuestas individuales.

Paso 5. El dispositivo administrado desempaqueta el archivo y comienza a aplicar las configuraciones y paquetes individuales.

R. La primera mitad del despliegue es el **snort** donde el **snort** la configuración se prueba localmente para garantizar su validez.

Cuando se demuestra que es válida, la nueva configuración se traslada al directorio de producción para **snort**. Si la validación falla, la implementación de políticas falla en este paso.

B. La segunda mitad de la carga del paquete de implementación corresponde a la configuración LINA, donde el proceso **ngfwManager** la aplica directamente al proceso LINA.

Si se produce un error, los cambios se deshacen y se produce un error en la implementación de directivas.

Paso 6. Si ambos **snort** y los paquetes LINA son correctos, el dispositivo administrado indica **snort** para reiniciar o recargar para cargar la nueva configuración y guardar todas las configuraciones actuales.

Paso 7. Si todos los mensajes son correctos, el sensor envía un mensaje de éxito y espera a que el Management Center lo confirme.

Paso 8. Una vez recibido, el FMC marca la tarea como un éxito y permite que el paquete de políticas finalice.

Resolución de problemas

Problemas encontrados durante **Policy Deployment** puede deberse, entre otros motivos:

1. Configuración errónea
2. Comunicación entre el CSP y el FTD
3. Base de datos y estado del sistema
4. Defectos y advertencias del software
5. Otras situaciones únicas

Algunos de estos problemas pueden solucionarse fácilmente, mientras que otros pueden requerir la ayuda de Cisco Technical Assistance Center (TAC).

El objetivo de esta sección es proporcionar técnicas para aislar el problema o determinar la causa raíz.

Interfaz gráfica de usuario (GUI) de FMC

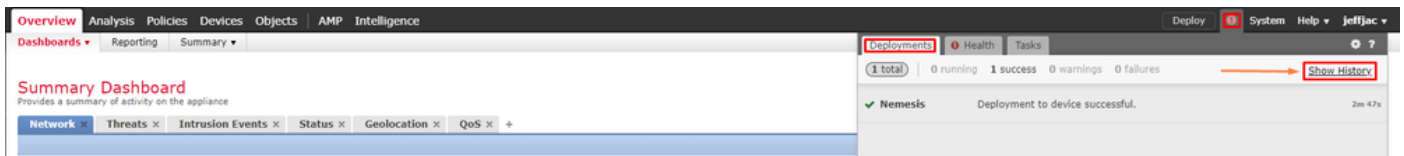
Cisco recomienda iniciar cada sesión de solución de problemas para los fallos de implementación en el dispositivo FMC.

En la ventana de notificación de fallas, en todas las versiones posteriores a la 6.2.3, hay herramientas adicionales que pueden ayudar con otros posibles errores.

Utilizar Las Transcripciones De Implementación

Paso 1. Tire hacia arriba del **Deployments** en la **interfaz de usuario web de FMC**.

Paso 2. Mientras que el **Deployments** está seleccionada, haga clic en **Show History**.



Paso 3. Dentro del **Deployment History** , puede ver todas las implementaciones anteriores desde su FMC. Seleccione la implementación en la que desea ver más datos.

Paso 4. Una vez seleccionado un elemento de despliegue, el **Deployment Details** muestra una lista de todos los dispositivos del interior del **Transaction**. Estas entradas se dividen en las siguientes columnas: **Device Number**, **Device Name**, **Status**,y **Transcript**.

Deployment History

Deployment ID	Start	End	Status
1	2019-11-20 07:01 PM	2019-11-20 07:04	Success
2	2019-11-20 01:10 AM	2019-11-20 01:12	Success
3	2019-11-16 01:11 AM	2019-11-16 01:14	Success
4	2019-11-13 01:07 AM	2019-11-13 01:09	Success
5	2019-11-08 01:06 AM	2019-11-08 01:08	Success
6	2019-11-06 01:23 AM	2019-11-06 01:25	Success
7	2019-11-03 01:10 AM	2019-11-03 01:12	Success
8	2019-11-01 01:27 AM	2019-11-01 01:29	Success

Deployment details for jeffjac at 2019-11-20 07:01 PM

Device	Status	Transcript
1 Nemesis	Success	[Download Icon]

Paso 5. Seleccione el dispositivo en cuestión y haga clic en la opción de transcripción para ver la transcripción de implementación individual que puede informarle de los fallos, así como de las configuraciones que se colocan en los dispositivos administrados.

Deploy Transcript

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

FMC >> clear configuration session OBJECT
Nemesis >> [info] : Session OBJECT does not exist.

FMC >> clear configuration session FMC_SESSION_1
Nemesis >> [info] : Session FMC_SESSION_1 does not exist.

FMC >> clear configuration session FMC_SESSION_2
Nemesis >> [info] : Session FMC_SESSION_2 does not exist.

FMC >> no strong-encryption-disable
FMC >> crypto isakmp nat-traversal
FMC >> [REDACTED]
FMC >> no ldap-attribute-map Class
FMC >> exit
FMC >> crypto isakmp nat-traversal
FMC >> no logging FMC MANAGER_VPN_EVENT_LIST
FMC >> no logging list MANAGER_VPN_EVENT_LIST
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class auth
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class vpn
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class vpncc
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class vpnfo
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class vpnlb
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class webfo
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class webvpn
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class ca
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class svc
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class ssl
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class dap
FMC >> logging list MANAGER_VPN_EVENT_LIST level notifications class ipaa
```

Close

Paso 6. Esta transcripción puede designar ciertas condiciones de falla e indicar un número muy importante para el siguiente paso: **Transaction ID**.

```
===== INFRASTRUCTURE MESSAGES =====
Lina Config application was successful
Lina write mem operation successful

-----
Transaction ID: 64424510596
Device UUID: 4753c9b8-c41f-11e9-b002-e1583a043dc5
```

Close

Paso 7. En un **Firepower Deployment**, el **Transaction ID** es lo que se puede utilizar para realizar un seguimiento de cada sección individual de una implementación de políticas. Con esto, en la **línea de comandos** del dispositivo, puede obtener una versión más detallada de estos datos para su remediación y análisis.

Consejo: En caso de que no pueda localizar el ID de transacción o si se encuentra en una versión anterior a la impresión de este registro, este registro puede seguir siendo útil para localizar mensajes de error individuales.

Resolución de problemas con registros FMC

Aunque resulta adecuado que el TAC de Cisco analice los registros, una búsqueda a través de los registros puede ayudar con el aislamiento inicial del problema y acelerar la resolución. Existen varios archivos de registro en FMC que revelan los detalles sobre el proceso de implementación de políticas.

Los dos registros a los que más se hace referencia son `policy_deployment.log` y `usmsharedsvcs.log`.

Todos los archivos mencionados en este documento se pueden ver con varios comandos de Linux como `more`, `less` y `vi`. Sin embargo, es muy importante garantizar que solo `read` se le realizan acciones. Todos los archivos requieren acceso raíz para poder verlos.

`/var/opt/CSCOpX/MDC/log/operation/usmsharedsvcs.log`

Este registro marca claramente el inicio de la tarea de implementación de políticas en FMC y la finalización de cada fase, lo que ayuda a determinar la fase en la que la implementación se ha topado con un fallo, junto con el código de fallo.

`transactionID` El valor incluido en la parte JSON del registro se puede utilizar para buscar entradas del registro relacionadas con un intento de implementación concreto.

```
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`

Aunque este archivo de registro ha existido a lo largo de las versiones 6.x, que comienzan en 6.4, su cobertura se amplió.

Ahora se describen los pasos detallados que se han dado a FMC para crear los paquetes de implementación, por lo que es mejor utilizar para analizar los fallos de las fases 1 a 4.

El inicio de cada fase está marcado por una línea con "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)
...
```

Solución de problemas de dispositivos administrados

Existen fases y secciones adicionales que dependen del paquete del dispositivo, la configuración de alta disponibilidad y el resultado de las fases anteriores para cada dispositivo administrado.

Si un problema de implementación se aísla en un error en el dispositivo administrado, se puede realizar un troubleshooting adicional en el dispositivo con dos registros en el dispositivo: **policy_deployment.log** y **ngfwManager.log**.

/ngfw/var/log/ngfwManager.log

Este archivo de registro proporciona los pasos detallados que ha realizado **Config Communication Manager** y **Config Dispatcher** para comunicarse con FMC, trabajar con el paquete de implementación y organizar la validación y aplicación de las configuraciones de **Snort** y **LINA**.

Estos son algunos ejemplos de **ngfwManager.log** que representan el inicio de las fases principales:

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>-
753133537443151390</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

Este registro contiene los detalles de la política aplicada a Snort. Aunque el contenido del registro es en su mayoría avanzado y requiere un análisis por parte del TAC, todavía es posible rastrear el proceso con algunas entradas clave:

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:

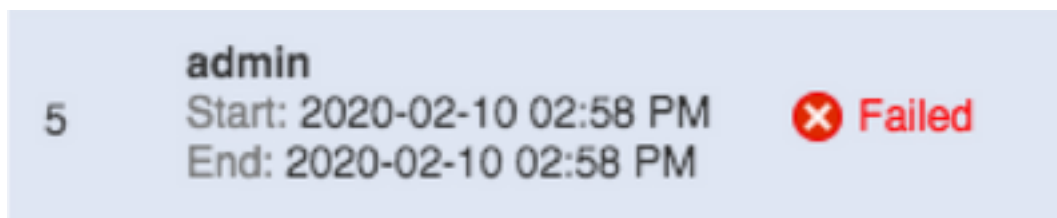
```
Jul 18 17:22:14 firepower policy_apply.pl[26571]: INFO notifyProcesses - sandbox =  
/var/cisco/deploy/sandbox/exported-files took 16 (memory = 169.52 MB, change = 16.95 MB)  
(Framework 3976<964 <- Transaction 1680 <- main 200)
```

After LINA config apply finishes, Snort deployment is finalized:

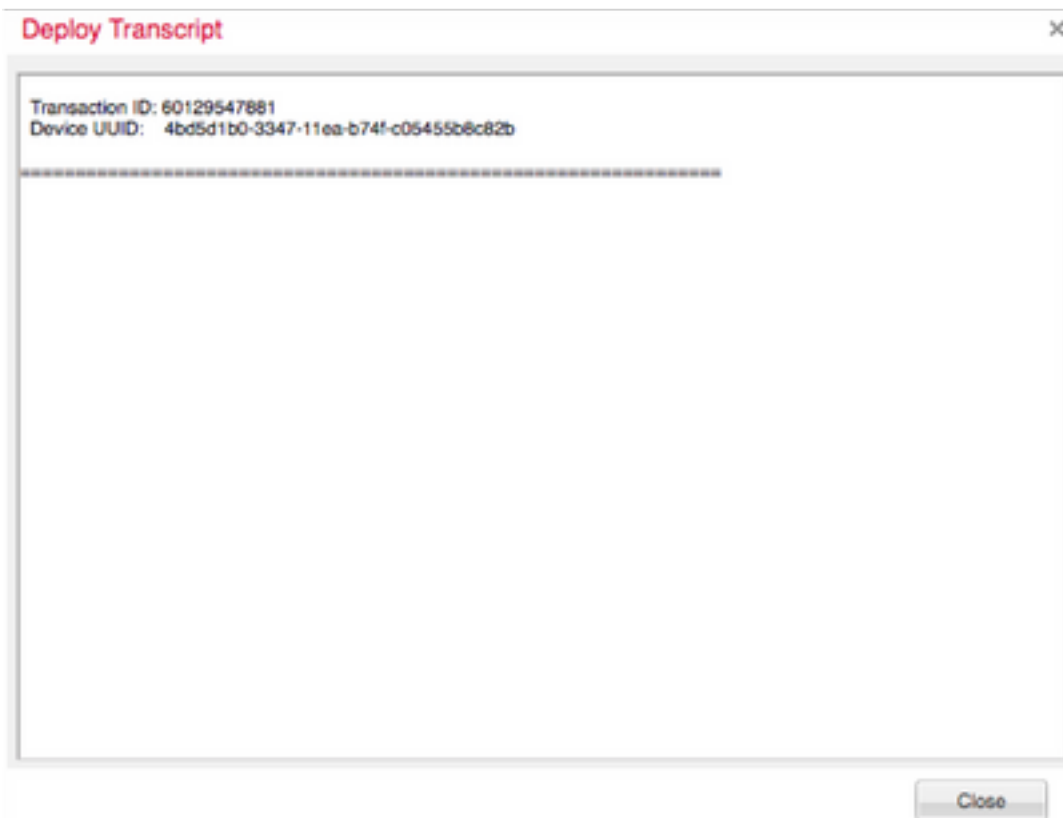
```
Jul 18 17:23:32 firepower policy_apply.pl[26913]: INFO starting finalizeDeviceDeployment -  
sandbox = /var/cisco/deploy/sandbox (memory = 101.14 MB) (Framework 3950<980 <- Transaction  
1740 <- main 206)
```

Ejemplo:

Paso 1. Falla una implementación



Paso 2. Obtenga el Deploy Transcript y Transaction ID.



Paso 3. SSH en su **Management Center** y utilizar la utilidad Linux `less` para leer el archivo como se muestra en el FMC:

Ejemplo:"`sudo less /var/opt/CSCOPx/MDC/log/operation/usmshredsvcs.log`" (La contraseña `sudo` es la contraseña de usuario para ssh)

```
admin@firepower:~$ sudo less /var/opt/CSCOPx/MDC/log/operation/usmshredsvcs.log
Password: _
```

Paso 4. Cuando esté en `less`, utilice la barra diagonal e introduzca la ID del mensaje para buscar los registros relacionados con la **ID de transacción de** despliegue.

Ejemplo:"/60129547881" (Mientras se encuentre en `less`, utilice `n` para desplazarse al siguiente resultado)

Ejemplo de mensaje en ejecución:

```
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" ]
}
```

Ejemplo de mensaje de error:

```
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 el fallo correcto con la tabla adjunta de mensajes de fallo común.

Es decir, failed_to_retrieve_running_configuration se produce durante los fallos de comunicación

entre los dos dispositivos.

Mensajes de fallos comunes

Estos son mensajes de error comunes que se pueden ver en la parte frontal del **Management Center Task** así como el código de error que se puede ver en el backend.

Estos mensajes se pueden analizar y comparar con las razones comunes para posibles resoluciones.

En caso de que no se vean o no resuelvan su situación, póngase en contacto con el TAC para obtener asistencia.

Código de error	Mensajes de error	Motivo
<code>device_has_changed_domain</code>	Error de implementación: el dispositivo ha cambiado el dominio de {SRCDOMAIN} a {DESTINATIONDOMAIN}. Inténtelo de nuevo más tarde	Este error ocurre generalmente cuando un dispositivo se ha movido o se toma de un segundo dominio. Una reimplementación mientras se produce información en dominios generalmente motiva este problema.
<code>device_currently_under_deployment</code>	Error en la implementación debido a otra implementación en curso para este dispositivo. Inténtelo de nuevo más tarde	Normalmente, esto se produce cuando se activa la implementación en un dispositivo durante la implementación. En algunas versiones, esto se evita sin una notificación de error; sin embargo, esta fase todavía existe para la asistencia de troubleshooting.
<code>device_not_member_of_container</code>	La implementación no se puede realizar en un dispositivo individual que sea miembro de un clúster. Intente implementar el clúster de nuevo más tarde.	Este mensaje se aplica al FMC en dispositivos con el administrador de chasis de sistema operativo extensible (FXOS) Firepower. Si el clúster está construido en FXOS, pero no en el FMC, se muestra este mensaje. Cree el clúster en el dispositivo Management Center antes de intentar la implementación.

policy_altered_after_timestamp_for_other_devices_in_job_error

Las políticas para uno o más dispositivos se han modificado desde {TIMESTAMP}. Reintente la implementación.

Este error se muestra si se altera alguna política u objeto para cualquier dispositivo en el trabajo de implementación después de que se implementen los disparadores de usuario antes de que se creen elementos CSM e instantáneas de dominio. Una reimplementación soluciona este problema. Esto puede ocurrir cuando muchos usuarios utilizan el mismo FMC para editar y guardar objetos durante la implementación.

policy_altered_after_timestamp_error

La política {Policy Name} se ha modificado desde {Timestamp}. Reintente la implementación.

Este error se muestra si se altera alguna política u objeto para el dispositivo en cuestión en el trabajo de implementación después de que se implementen los disparadores de usuario antes de que se creen instantáneas de dominio y CSM. Una reimplementación soluciona este problema.

csm_snapshot_error

Error en la implementación debido a un error en la recopilación de directivas y objetos. Si el problema persiste después de un intento repetido, comuníquese con el TAC de Cisco.

Si se proporciona una importación de directiva reciente, espere aproximadamente una hora e intente realizar otra implementación. Si esto no permite que esto continúe, comuníquese con el TAC ya que es un mensaje relacionado con la base de datos.

domain_snapshot_timeout

Error en la implementación debido al tiempo de espera para recopilar directivas y objetos. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.

La instantánea de dominio tiene un tiempo de espera de 5 minutos de forma predeterminada. Si el sistema está sometido a una carga alta, el hipervisor no funciona correctamente, puede provocar retrasos no naturales en la llamada. Esto puede ocurrir si el Management Center o el dispositivo no dispone de la cantidad adecuada de recursos de memoria. Si esto sucede sin carga, c

continúa más tarde,
comuníquese con el TAC.

domain_snapshot_errors

Error en la implementación de la directiva y la colección de objetos. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.

Póngase en contacto con T Se requiere resolución de problemas avanzada.

failed_to_retrieve_running_configuration

Error en la implementación debido a un error al recuperar la información de configuración de ejecución del dispositivo. Reintente la implementación.

Este mensaje puede aparecer cuando la conectividad entre el sensor final y un FMC no funciona como se espera.

Verifique el estado del túnel entre las unidades y monitoree la conectividad entre los dispositivos.

Si el túnel funciona según lo esperado y los dispositivos pueden comunicarse, comuníquese con el TAC.

device_is_busy

Error en la implementación porque el dispositivo podría estar ejecutando una implementación anterior o reiniciar. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.

Este mensaje aparece cuando un FMC intenta realizar una implementación, mientras que una implementación anterior está en curso en FTD. Suele suceder cuando una implementación anterior no terminada en FTD y el FTD reinició o el proceso ngfwManager en FTD se reinició. Este problema se resuelve mediante un reinicio que se realiza después de unos minutos para permitir que l

procesos se detengan formalmente.

Si tras un retraso o si el retardo no es aceptable, póngase en contacto con el TAC.

no_response_for_show_cmd

Error en la implementación debido a problemas de conectividad con el dispositivo o el dispositivo no responde. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.

FMC emite ciertos comandos "show" de LINA para obtener la configuración en ejecución y la generación de la configuración.

Esto puede suceder cuando hay problemas de conectividad o problemas con el proceso ngfwManager en el sensor. En caso de que no tenga problemas de conectividad con sus unidades, comuníquese con el TAC.

network_latency_or_device_not_reachable

Error en la implementación debido a un error en las comunicaciones con el dispositivo. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.

Suele producirse con una latencia de red alta entre los dispositivos para que se agote el tiempo de espera de la política. Verifique la latencia de red entre los dispositivos para verificar que coincide con los mínimos de la versión mencionada en la guía del

usuario.

slave_app_sync

Error en la implementación porque la sincronización de la configuración del clúster está en curso. Reintente la implementación.

Esto sólo se aplica a las configuraciones de clúster FTD. Si se intenta realizar implementación en un clúster FTD mientras la sincronización de la aplicación (sincronización de la configuración) está en curso, FTD rechaza la misma operación. Un reintento de la sincronización de la configuración debería resolver este problema.

Se puede realizar un seguimiento del estado actual del clúster con este comando en el dispositivo administrado por CLISH:

```
>show cluster info
```

Después de revisar los registros de USMS mencionados anteriormente, es posible que pueda ver qué configuración provoca el error. Estos suelen ser bugs en los que los registros se pueden explorar a través de la herramienta Cisco Bug Tool. Contactar al TAC de Cisco para resolver problemas adicionales.

asa_configuration_generation_errors

La implementación no pudo generar la configuración del dispositivo. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.

Esto ocurre en los modelos 4100 o 9300 si la interfaz no está asociada al dispositivo durante o justo antes de una implementación.

interface_out_of_date

Error en la implementación porque las interfaces del dispositivo están obsoletas. Guarde la configuración en la página de interfaces y vuelva a intentarlo.

Verifique que la interfaz es completamente asociada o asociada antes de intentar la implementación.

device_package_error

La implementación no pudo generar la configuración para el dispositivo. Si el problema persiste después de otro intento, comuníquese con el TAC de

Este error indica una falla al generar la configuración del dispositivo para el dispositivo. Póngase en contacto con T

Cisco.

device_package_timeout

Error en la implementación debido al tiempo de espera durante la generación de la configuración. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.

Esto puede suceder si existe latencia entre los dispositivos por encima de los rangos normales. Póngase en contacto con el TAC si, después de normalizar la latencia, el problema persiste.

device_communication_errors

Error en la implementación debido a un error en la comunicación del dispositivo. Compruebe la conectividad de red y vuelva a intentar la implementación.

Este mensaje es el respaldo para cualquier problema de comunicación entre los dispositivos. Debido a su naturaleza vaga, se escribe como el estado alternativo que se ha producido un error de conectividad desconocido.

unable_to_initiate_deployment_dc

Error de implementación de políticas. Reintente la implementación.

Otro intento debería resolver este problema. Esto puede ocurrir cuando FMC no puede iniciar la implementación debido a un bloqueo temporal de la base de datos.

device_failure_timeout

Error en la implementación en el dispositivo debido al tiempo de espera. Reintente la implementación.

Esto está relacionado con la implementación de FTD. Los procesos del FTD esperan minutos a que el envío comience la implementación. Si no, se agota el tiempo de espera. Si esto ocurre, verifique la conectividad entre dispositivos si la conectividad es la esperada, comuníquese con el TAC.

device_failure_download_timeout

Error en la implementación debido al tiempo de espera de descarga de la configuración al dispositivo. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.

Esto está relacionado con la implementación de FTD. El dispositivo no puede descargar todos los archivos de configuración de los dispositivos durante la implementación debido a problemas de conectividad. Vuelva a intentarlo después de verificar la conectividad de los dispositivos. Si se ha verificado, póngase en contacto con el TAC.

device_failure_configuration	Error de implementación debido a un error de configuración. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.	Cualquier error en la configuración generado por el FMC para el dispositivo de destino puede dar lugar a este error después de aplicar la configuración. Esto debe analizarse en los registros de USMS para ver qué problemas se ven e intentar revertirlos. Una vez reparado, esto generalmente requiere la intervención del TAC y la creación de errores si los registros no pueden coincidir con un defecto conocido en la herramienta de búsqueda de errores de Cisco.
deployment_timeout_no_response_from_device	Error en la implementación debido al tiempo de espera de comunicación con el dispositivo. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.	Este tiempo de espera se produce si el FMC no ha recibido respuesta de un dispositivo después de 45 minutos o más. Este es un error de comunicación. Verifique la comunicación y asegúrese de que se verifica, póngase en contacto con el TAC.
device_failure_change_master	Error en la implementación en el clúster porque la unidad principal ha cambiado. Reintente la implementación.	Para una implementación de configuración de clúster de dispositivos, si el nodo principal cambia cuando la implementación está en curso en el dispositivo (después de la notificación de inicio), el dispositivo indica este error. Vuelva a intentarlo cuando el nodo principal esté estable.

device_failure_unknown_master	Error en la implementación en el clúster debido a un error en la identificación de la unidad principal. Reintente la implementación.	Se puede realizar un seguimiento del estado actual del miembro del clúster con el comando en el dispositivo administrado CLISH: >show cluster info
cd_deploy_app_sync	Error en la implementación porque la sincronización de la configuración del clúster está en curso. Reintente la implementación.	FMC no ha podido determinar el nodo principal actual durante la implementación. Esto podría deberse normalmente a un par de posibilidades: Problemas de conectividad o el nodo principal no agregado al clúster en FMC. Debe resolverse después de restablecer la conectividad después de agregar el primer nodo actual al clúster de FMC y realizar un reintento. Se puede realizar un seguimiento del estado actual del clúster con este comando en el dispositivo administrado CLISH: >show cluster info
cd_existing_deployment	Error en la implementación debido a un conflicto con la implementación anterior simultánea. Si el problema persiste después de otro intento, comuníquese con el TAC de Cisco.	Esto puede ocurrir si una implementación es simultánea en un lado, pero no en el otro. Esto suele deberse a problemas de comunicación entre los dispositivos. Póngase en contacto con el TAC si después de que se ha pasado el tiempo de espera sigue sin poder realizar la implementación.

Póngase en contacto con TAC para obtener asistencia

En el caso de que la información anterior no permita que continúe la implementación de una política, o si el problema parece no estar relacionado con un comportamiento documentado previamente, utilice los pasos proporcionados en el siguiente enlace para generar un archivo de

Troubleshooting y comunicarse con el TAC para el análisis y la creación de errores.

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

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).