Fehlerbehebung bei Bereitstellungen von Firepower Threat Defense-Richtlinien

Inhalt

Einleitung

Dieses Dokument beschreibt einen allgemeinen Überblick über den Richtlinienbereitstellungsprozess für FTD sowie grundlegende Fehlerbehebungstechniken.

Hintergrundinformationen

Mit **Cisco Firepower Threat Defense** (FTD), den herkömmlichen Stateful-Firewall-Funktionen von **Adaptive Security Appliances** (ASA) und **Next-Gen** Firewall-Funktionen (unterstützt durch **Snort**) werden nun zu einem Produkt zusammengefasst.

Aufgrund dieser Änderung **Policy Deployment Infrastructure** auf FTD verarbeitet jetzt Konfigurationsänderungen für ASA-Code (auch als LINA bezeichnet) und **Snort** in einem Paket.

Voraussetzungen

Cisco empfiehlt, mit folgenden Produkten vertraut zu sein:

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

Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Übersicht über die Richtlinienbereitstellung

Cisco FTD nutzt **Policy Deployments** Sie dient zum Verwalten und Übertragen von Konfigurationen für Geräte, die beim **Firepower Management Center** (FMC) selbst.

Innerhalb der Bereitstellung gibt es eine Reihe von Schritten, die in "Phasen" unterteilt sind.

Die FMC-Phasen können in dieser Liste zusammengefasst werden.

Phase 0	Initialisierung der Bereitstellung
Phase 1	Datenbankobjektsammlung
Phase 2	Richtlinien- und Objektsammlung
Phase 3	NGFW - Befehlszeilenkonfiguration
Phase 4	Paketgenerierung für die Gerätebereitstellung
Phase 5	Senden und Empfangen des Bereitstellungspake
Phase 6	Ausstehende Meldungen zu Bereitstellung, Bereitstellungsaktionen und erfolgreichen Bereitstellungen

Die Kenntnis der Phasen und des Standorts von Fehlern im Prozess kann bei der Fehlerbehebung helfen, wenn ein **Firepower** Systemseiten.

In einigen Fällen kann es sich um einen Konflikt aufgrund früherer Konfigurationen oder aufgrund eines **Advanced Flex Configuration** das kein Schlüsselwort hat, das Fehler verursachen kann, die im Gerätebericht nicht behandelt werden.

Beispielübersicht

Schritt 1: Klicken Sie auf **Deployment**, der das auszuwählende Gerät angibt.

Schritt 2: Wenn die Bereitstellung für ein Gerät bestätigt wird, beginnt das FMC mit der Erfassung aller für das Gerät relevanten Konfigurationen.

Schritt 3: Wenn die Konfigurationen erfasst werden, erstellt das FMC das Paket und sendet es über seinen Kommunikationsmechanismus namens SFTunnel an den Sensor.

Schritt 4: Das FMC benachrichtigt den Sensor, den Bereitstellungsprozess mit der bereitgestellten Richtlinie zu starten, während es die einzelnen Antworten abhört.

Schritt 5: Das verwaltete Gerät entpackt das Archiv und beginnt mit der Anwendung der einzelnen Konfigurationen und Pakete.

> Antwort: Die erste Hälfte der Bereitstellung besteht aus dem **Snort** Konfiguration, bei der **Snort** - Konfiguration lokal getestet, um ihre Gültigkeit zu gewährleisten.

Wenn sich herausstellt, dass die neue Konfiguration gültig ist, wird sie in das Produktionsverzeichnis für **Snort**. Wenn die Validierung fehlschlägt, schlägt die Richtlinienbereitstellung in diesem Schritt fehl.

B. Die zweite Hälfte der Bereitstellungspaketlast betrifft die LINA-Konfiguration, in der sie vom **ngfwManager-**Prozess direkt auf den LINA-Prozess angewendet wird.

Wenn ein Fehler auftritt, werden die Änderungen zurückgesetzt, und es tritt ein Fehler bei der Richtlinienbereitstellung auf.

Schritt 6: Wenn beide **Snort** und LINA-Pakete erfolgreich sind, signalisiert das verwaltete Gerät **Snort** , um die neue Konfiguration zu laden und alle aktuellen Konfigurationen zu speichern.

Schritt 7: Wenn alle Meldungen erfolgreich sind, sendet der Sensor eine Erfolgsmeldung und wartet darauf, dass diese vom Management Center bestätigt wird.

Schritt 8: Nach Eingang markiert das FMC die Aufgabe als erfolgreich und ermöglicht das Fertigstellen des Richtlinienpakets.

Fehlerbehebung

Probleme während **Policy Deployment** Gründe hierfür sind u. U.:

1. Fehlkonfiguration
2. Kommunikation zwischen FMC und FTD
3. Datenbank- und Systemstatus
4. Softwarefehler und Hinweise
5. Andere spezielle Situationen

Einige dieser Probleme können leicht behoben werden, während andere die Unterstützung von Cisco erfordern. **Technical Assistance Center (TAC)**.

In diesem Abschnitt sollen Verfahren zur Isolierung des Problems und zur Ermittlung der Ursache beschrieben werden.

Grafische Benutzeroberfläche (GUI) von FMC

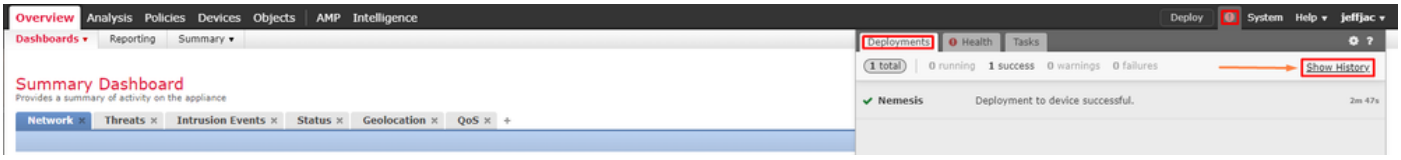
Cisco empfiehlt für Bereitstellungsfehler, jede Fehlerbehebungssitzung auf der FMC-Appliance zu starten.

Im Fehlerbenachrichtigungsfenster gibt es für alle Versionen nach 6.2.3 zusätzliche Tools, die bei anderen möglichen Fehlern helfen können.

Verwendung der Bereitstellungsprotokolle

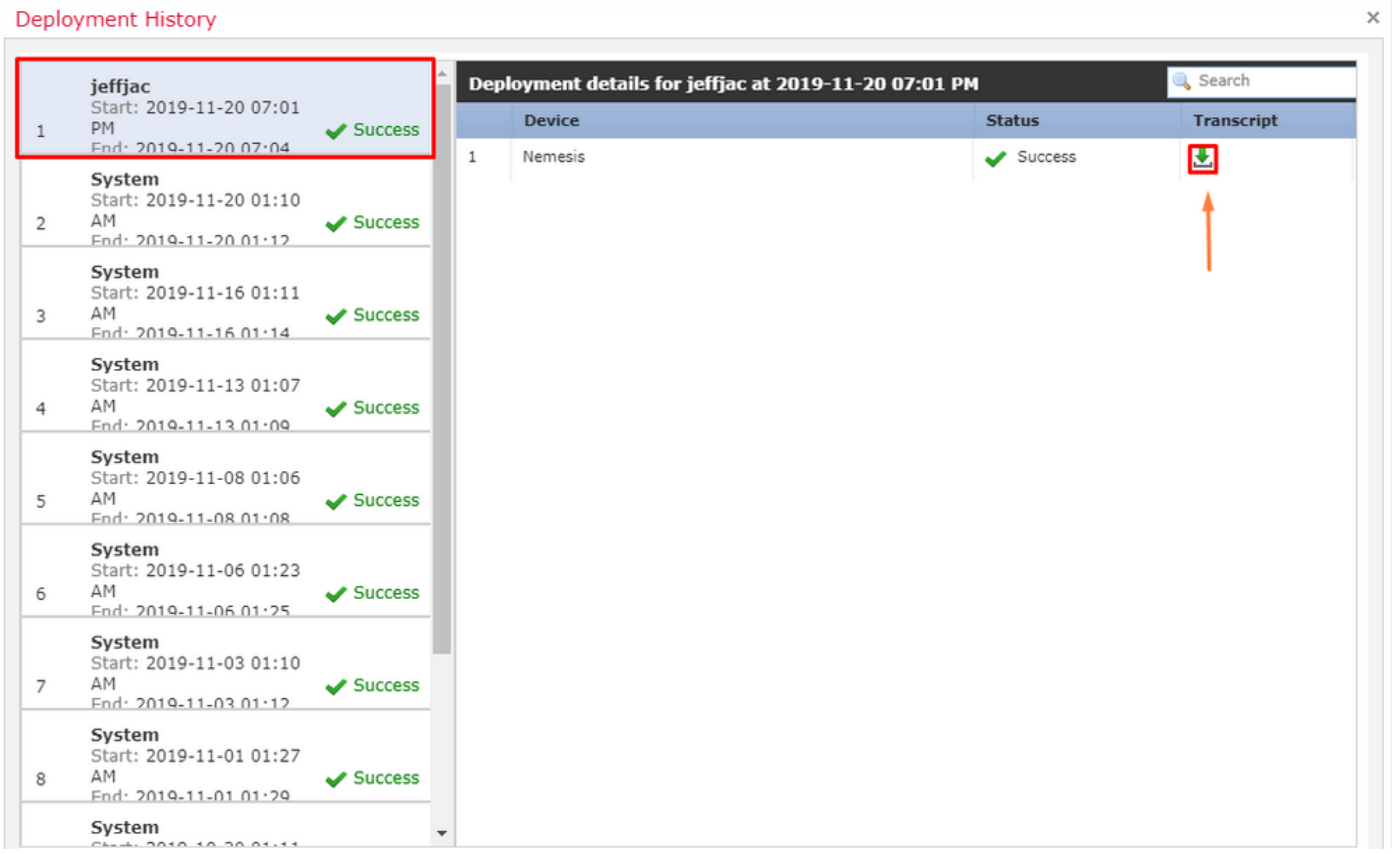
Schritt 1: Ziehen Sie **Deployments** in der **FMC-Webbenutzeroberfläche**.

Schritt 2: Während der **Deployments** ist ausgewählt. Klicken Sie auf **Show History**.

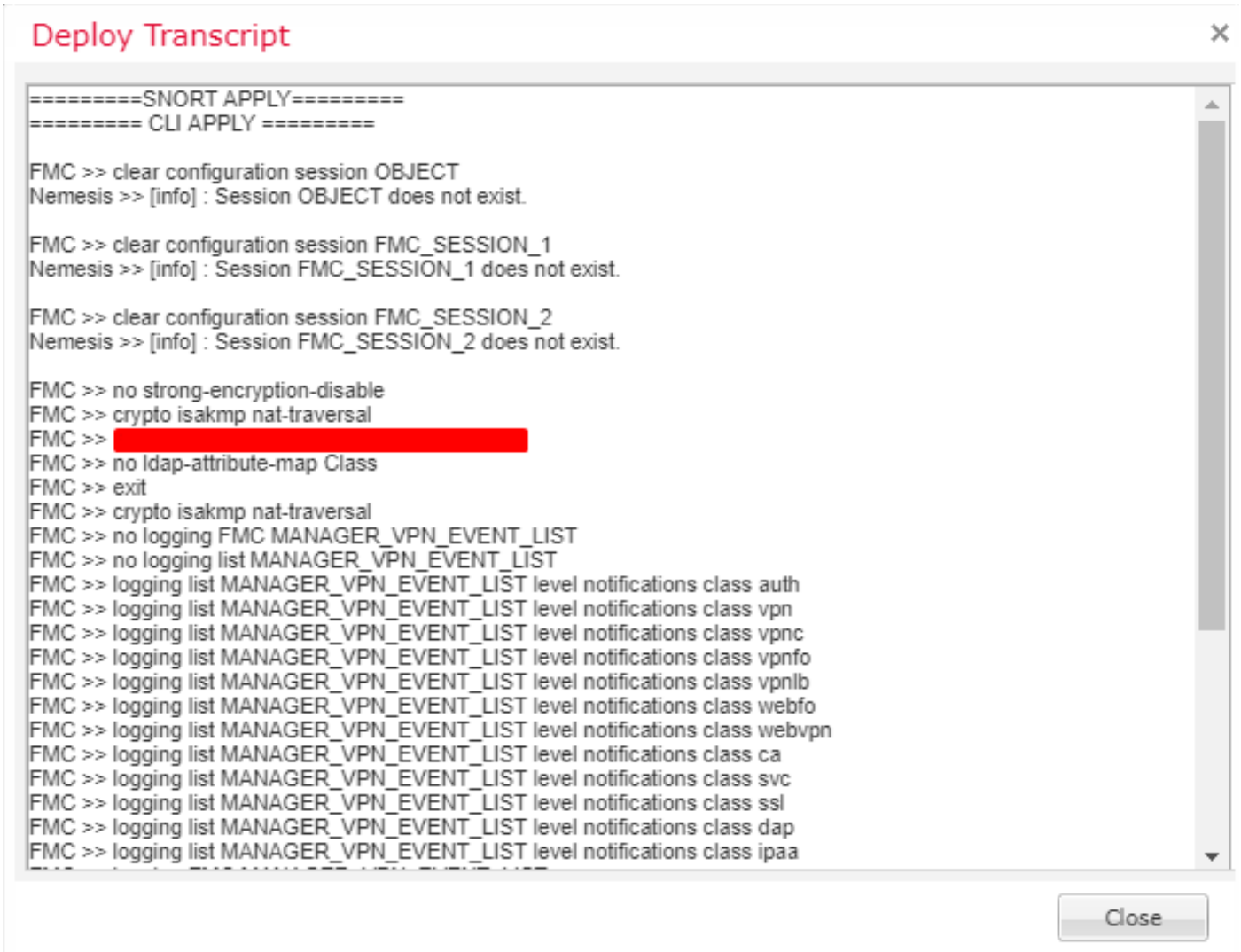


Schritt 3: Innerhalb des **Deployment History** alle früheren Bereitstellungen von Ihrem FMC aus sehen. Wählen Sie die Bereitstellung aus, in der Sie weitere Daten anzeigen möchten.

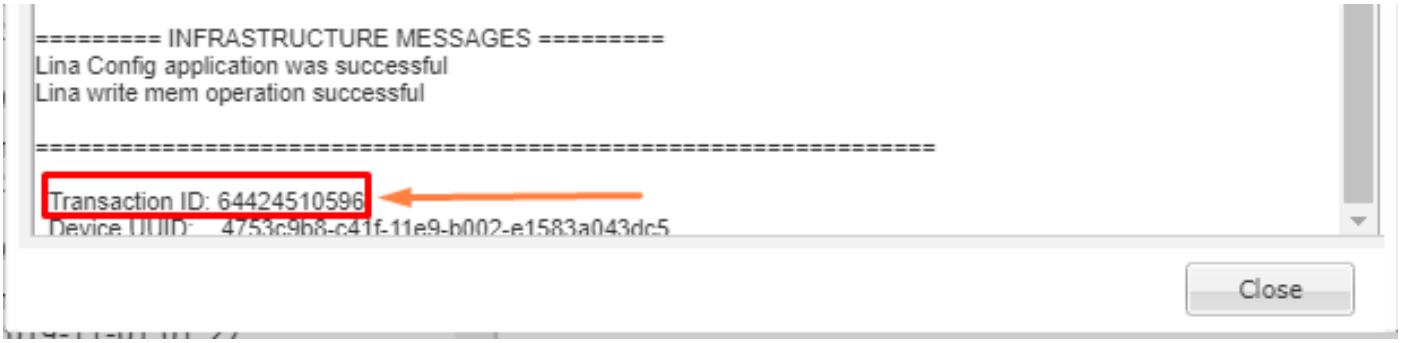
Schritt 4: Nachdem ein Bereitstellungselement ausgewählt wurde, **Deployment Details** zeigt eine Liste aller Geräte im **Transaction**. Diese Einträge werden in folgende Spalten unterteilt: **Device Number, Device Name, Status,**und **Transcript**.



Schritt 5: Wählen Sie das betreffende Gerät aus, und klicken Sie auf die Transkriptionsoption, um das jeweilige Bereitstellungsprotokoll anzuzeigen, das Sie über Fehler und Konfigurationen auf den verwalteten Geräten informieren kann.



Schritt 6. Dieses Transkript kann bestimmte Fehlerbedingungen festlegen und eine sehr wichtige Zahl für den nächsten Schritt angeben: **Transaction ID**.



Schritt 7: In einem **Firepower Deployment**,Die Fehlermeldung **Transaction ID** kann verwendet werden, um die einzelnen Abschnitte einer Richtlinienbereitstellung zu verfolgen. Dadurch können Sie über die **Befehlszeile** des Geräts eine detailliertere Version dieser Daten für die Sanierung und Analyse erhalten.

Tipp: Für den Fall, dass Sie die Transaktions-ID nicht finden können, oder wenn Sie sich in einer Version befinden, bevor diese gedruckt wurde, kann dieses Protokoll weiterhin zum Auffinden einzelner Fehlermeldungen verwendet werden.

Fehlerbehebung mit FMC-Protokollen

Obwohl es angemessen ist, das Cisco TAC für die Analyse der Protokolle zu beauftragen, kann eine Suche anhand der Protokolle bei der anfänglichen Problemisolierung und der schnelleren Behebung helfen. Es gibt mehrere Protokolldateien auf FMC, in denen die Details des Richtlinienbereitstellungsprozesses aufgezeigt werden.

Die beiden am häufigsten genannten Protokolle sind **policy_deployment.log** und **usmsharedsvcs.log**.

Alle in diesem Dokument erwähnten Dateien können mit mehreren Linux-Befehlen angezeigt werden, z. B. **more**, **less** und **vi**. Es ist jedoch sehr wichtig, dass nur **read** Aktionen ausgeführt werden. Alle Dateien benötigen Root-Zugriff, um sie anzeigen zu können.

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

Dieses Protokoll kennzeichnet den Beginn der Richtlinienbereitstellungsaufgabe auf dem FMC und den Abschluss jeder Phase. So kann festgestellt werden, in welcher Phase die Bereitstellung fehlschlug, und der Fehlercode angegeben werden.

Die Fehlermeldung **transactionID** -Wert im JSON-Teil des Protokolls verwendet werden, um Protokolleinträge zu finden, die sich auf einen bestimmten Bereitstellungsversuch beziehen.

```
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

Diese Protokolldatei existiert bereits in 6.x Versionen, die bei 6.4 beginnen, aber ihre Abdeckung wurde erweitert.

Es beschreibt nun die detaillierten Schritte, die von FMC zur Erstellung der Bereitstellungspakete unternommen wurden. Daher wird es am besten für die Analyse von Ausfällen aus Phase 1 - 4 verwendet.

Der Beginn jeder Phase ist durch eine Zeile mit "**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)
...
```

Fehlerbehebung für verwaltete Geräte

Es gibt weitere Phasen und Abschnitte, die vom Gerätepaket, der Hochverfügbarkeitskonfiguration und dem Ergebnis früherer Phasen für jedes verwaltete Gerät abhängen.

Wenn ein Bereitstellungsproblem auf einen Fehler auf dem verwalteten Gerät zurückgeführt wird, kann eine weitere Fehlerbehebung auf dem Gerät mit zwei Protokollen auf dem Gerät durchgeführt werden: **policy_deployment.log** und **ngfwManager.log**.

/ngfw/var/log/ngfwManager.log

Diese Protokolldatei enthält detaillierte Schritte, die von **Config Communication Manager** und **Config Dispatcher** um mit FMC zu kommunizieren, mit dem Bereitstellungspaket zu arbeiten und die Validierung und Anwendung von **Snort-** und LINA-Konfigurationen zu orchestrieren.

Dies sind einige Beispiele für **ngfwManager.log**, die den Beginn der Hauptphasen darstellen:

```
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

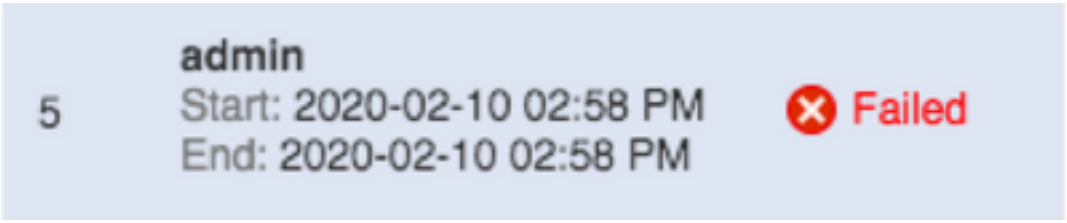
Dieses Protokoll enthält die Details der Richtlinie, auf die **Snort**. Obwohl der Inhalt des Protokolls größtenteils fortgeschritten ist und eine Analyse durch das TAC erfordert, ist es immer noch möglich, den Prozess mit einigen Schlüsseleinträgen zu verfolgen:

```
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:
```

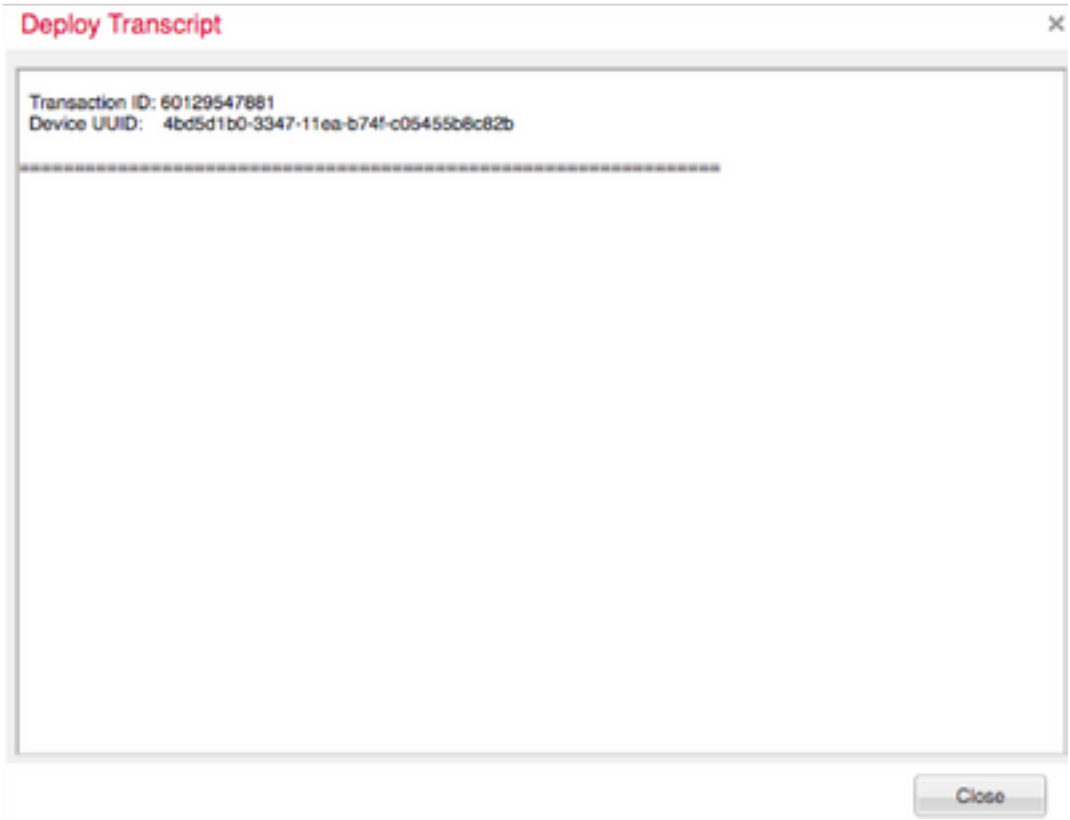
```
Jul 18 17:21:54 firepower policy_apply.pl[26571]: INFO  -> calling
SF::UMPD::Plugins::NGFWPolicy::Device::publishExportedFiles  (Plugin 230 <- Framework 822 <-
Transaction 1662)



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)
```

Beispiel

Schritt 1: Fehler bei der Bereitstellung



Schritt 2: Rufen Sie die **Deploy Transcript** und **Transaction ID**.



Schritt 3: SSH in Ihre **Management Center** und verwende das Linux-Dienstprogramm **less** um die Datei wie auf Ihrem FMC angezeigt zu lesen:

Beispiel:"**sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log**" (Das sudo-Kennwort ist Ihr Benutzerkennwort für SSH)

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

Password:
```

Schritt 4: Wenn Sie **less**verwenden Sie einen Schrägstrich und geben Sie die Nachrichten-ID ein, um nach Protokollen zu suchen, die sich auf die **Bereitstellungstransaktions-ID** beziehen.

Beispiel:"/60129547881" (Während in **less**, verwenden Sie n, um zum nächsten Ergebnis zu navigieren)

Beispiel für eine laufende Nachricht:

```
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" ]
}
```

Beispiel einer Fehlermeldung:

```
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) Vergleichen Sie den ordnungsgemäßen Fehler mit der beigefügten Tabelle mit **häufigen Fehlermeldungen**.

Das heißt, dass failed_to_restore_running_configuration bei Kommunikationsfehlern zwischen den beiden Geräten auftritt.

Häufige Fehlermeldungen

Dies sind häufige Fehlermeldungen, die am Front-End des **Management Center Task** sowie den Fehlercode, der im Backend zu sehen ist.

Diese Botschaften können analysiert und mit den gängigen Gründen für mögliche Lösungen verglichen werden.

Falls diese nicht erkannt werden oder sich Ihre Situation nicht beheben lässt, wenden Sie sich bitte an das TAC.

Fehlercode	Fehlermeldungen	Grund
device_has_changed_domain	Bereitstellungsfehler - Das Gerät hat die Domäne von {SRCDOMAIN} in {DESTINATIONDOMAIN} geändert. Versuchen Sie es später erneut.	Dieser Fehler tritt in der Re dann auf, wenn ein Gerät i zweite Domäne verschobe oder daraus entfernt wurde Eine erneute Bereitstellung ohne domänenübergreifen Informationen ändert diese Problem in der Regel.
device_currently_under_deployment	Fehler bei der Bereitstellung aufgrund einer anderen Bereitstellung für dieses Gerät. Versuchen Sie es später erneut.	Dies wird in der Regel gem wenn die Bereitstellung au einem bereitzustellenden G ausgelöst wird. In einigen Versionen wird dies ohne Fehlermeldung verhindert. Diese Phase besteht jedoc weiterhin für die Fehlerbehebung.
device_not_member_of_container	Die Bereitstellung kann nicht auf einem einzelnen Gerät durchgeführt werden, das zu einem Cluster gehört. Versuchen Sie später erneut, den Cluster bereitzustellen.	Diese Meldung gilt für FTD Geräten mit dem FirePOW eXtensible Operative Syste (FXOS) Chassis Manager. Wenn der Cluster auf FXO jedoch nicht auf dem FMC basiert, wird diese Meldung angezeigt. Erstellen Sie de Cluster auf der Manageme Center-Appliance, bevor Si versuchen, ihn bereitzustel

policy_altered_after_timestamp_for_other_devices_in_job_error	Richtlinien für ein oder mehrere Geräte wurden seit {TIMESTAMP} geändert. Wiederholen Sie die Bereitstellung.	Dieser Fehler wird angezei wenn eine Richtlinie oder e Objekt für ein Gerät im Bereitstellungsauftrag geär wird, nachdem der Benutze Bereitstellung ausgelöst ha bevor CSM-Elemente und Domänen-Snapshots erste werden. Eine erneute Bereitstellung behebt diese Problem. Dies kann auftreten, wenn Benutzer dasselbe FMC verwenden, um Objekte zu bearbeiten und zu speiche während sie bereitgestellt werden.
policy_altered_after_timestamp_error	Die Richtlinie {Policy Name} wurde seit {Timestamp} geändert. Wiederholen Sie die Bereitstellung.	Dieser Fehler wird angezei wenn im Bereitstellungsauf eine Richtlinie oder ein Obj für das betreffende Gerät geändert wird, nachdem de Benutzer die Bereitstellung ausgelöst hat und bevor CS und Domänen-Snapshots erstellt werden. Eine erneu Bereitstellung behebt diese Problem.
csm_snapshot_error	Fehler bei der Bereitstellung aufgrund eines Fehlers bei der Sammlung von Richtlinien und Objekten. Wenn das Problem nach einem wiederholten Versuch weiterhin besteht, wenden Sie sich an das Cisco TAC.	Wenn kürzlich ein Policy In bereitgestellt wurde, warten etwa eine Stunde und versuchen Sie eine andere Bereitstellung. Wenn dies nicht möglich is wenden Sie sich an das TA es sich um eine datenbankbezogene Nachr handelt.

domain_snapshot_timeout	Fehler bei der Bereitstellung aufgrund eines Timeouts beim Erfassen von Richtlinien und Objekten. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Standardmäßig hat der Domänen-Snapshot ein Ti von 5 Minuten. Steht das System unter hoher Auslas oder kommt es zu einem A des Hypervisors, kann dies unnatürlichen Verzögerung des Anrufs führen. Dies kann der Fall sein, we das Management Center o das Gerät nicht über die entsprechende Menge an Speicherressourcen verfüg Wenn dies ohne Last gesc oder zu einem späteren Zeitpunkt nicht mehr gesch wenden Sie sich an das TA
domain_snapshot_errors	Fehler bei der Bereitstellung in Richtlinien- und Objektauflistung. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Kontaktieren Sie das TAC. erweiterte Fehlerbehebung erforderlich.
failed_to_retrieve_running_configuration	Fehler bei der Bereitstellung, da die Informationen zur Ausführungskonfiguration nicht vom Gerät abgerufen werden konnten. Wiederholen Sie die Bereitstellung.	Diese Meldung kann auftre wenn die Verbindung zwisc einem Endsensor und eine FMC nicht wie erwartet funktioniert. Überprüfen Sie Tunnelzustand zwischen d Geräten, und überwachen die Verbindung zwischen d beiden Geräten. Wenn der Tunnel wie erwa funktioniert und die Geräte miteinander kommunizieren können, wenden Sie sich a TAC.
device_is_busy	Fehler bei der Bereitstellung, da das Gerät möglicherweise eine vorherige Bereitstellung oder einen Neustart ausführt. Wenn das Problem nach	Diese Meldung wird angez wenn das FMC eine Bereitstellung versucht, wä auf FTD eine vorherige

	einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Bereitstellung läuft. Tritt in Regel auf, wenn eine vorhe Bereitstellung auf FTD noc nicht abgeschlossen ist un FTD neu gestartet wurde o der ngfwManager-Prozess FTD neu gestartet wurde. E Wiederholungsversuch nac Minuten, um eine formelle Zeitüberschreitung für Proz zu ermöglichen, sollte dies Problem lösen. Wenn die Verzögerung nic akzeptabel ist, wenden Sie an das TAC.
no_response_for_show_cmd	Die Bereitstellung schlug aufgrund von Verbindungsproblemen mit dem Gerät fehl, oder das Gerät reagiert nicht. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	FMC gibt bestimmte LINA- "show"-Befehle aus, um die aktuelle Konfiguration zur Konfigurationsgenerierung abzurufen. Dies kann passieren, wenn Verbindungsprobleme oder Probleme mit dem ngfwManager-Prozess auf Endsensor auftreten. Wenden Sie sich an das TA falls keine Verbindungsprobleme zwis Ihren Einheiten auftreten.
network_latency_or_device_not_reachable	Fehler bei der Bereitstellung aufgrund eines Kommunikationsfehlers mit dem Gerät. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	tritt in der Regel bei hoher Netzwerklatenz zwischen d Geräten auf, um ein Timeo Richtlinien zu verursachen. Überprüfen Sie die Netzwerklatenz zwischen d Geräten, um sicherzustelle dass sie den Mindestwerte die im Benutzerhandbuch

		genannte Version entsprich
slave_app_sync	Fehler bei der Bereitstellung, da die Clusterkonfigurationssynchronisierung ausgeführt wird. Wiederholen Sie die Bereitstellung.	Dies gilt nur für FTD-Cluste Einrichtungen. Wenn eine Bereitstellung auf einem F Cluster versucht wird, wäh eine App-Synchronisierung (Konfigurationssynchronisi) durchgeführt wird, wird di von FTD abgelehnt. Ein Wiederholungsversuch nac Konfigurationssynchronisie sollte dieses Problem löse
asa_configuration_generation_errors	Fehler beim Generieren der Gerätekonfiguration durch die Bereitstellung. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Der aktuelle Clusterstatus mit diesem Befehl in der Cl des verwalteten Geräts ver werden: >Clusterinformationen anz Nach der Überprüfung der USMS-Protokolle, die zuvo erwähnt wurden, können S möglicherweise sehen, wel Konfiguration den Fehler verursacht. In der Regel ha es sich hierbei um Bugs, b denen die Protokolle mithilf Cisco Bug-Tools durchsuch werden können. Alternativ können Sie sich zur weitere Fehlerbehebung an das Ci TAC wenden.
interface_out_of_date	Fehler bei der Bereitstellung, da die Schnittstellen auf dem Gerät veraltet sind. Speichern Sie die Konfiguration auf der Schnittstellenseite, und wiederholen Sie den Vorgang.	Dies ist bei Modellen der S 4100 oder 9300 der Fall, w die Verbindung zwischen Schnittstelle und Gerät wäl oder direkt vor einer Bereitstellung aufgehoben Überprüfen Sie, ob die Schnittstelle vollständig zugeordnet oder nicht zugeordnet ist, bevor Sie d Bereitstellung versuchen.
device_package_error	Fehler beim Generieren der Konfiguration für das Gerät. Wenn das Problem nach einem weiteren	Dieser Fehler zeigt an, das Gerätekonfiguration für das Gerät nicht generiert wurde

	Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Kontaktieren Sie das TAC.
device_package_timeout	Fehler bei der Bereitstellung aufgrund eines Timeouts während der Konfigurationsgenerierung. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Dies kann der Fall sein, we die Latenz zwischen den Geräten über den normale Bereich hinausgeht. Wend Sie sich an das TAC, wenn Problem auch nach der Normalisierung der Latenz weiterhin auftritt.
device_communication_errors	Fehler bei der Bereitstellung aufgrund eines Fehlers bei der Gerätekommunikation. Überprüfen Sie die Netzwerkverbindung, und wiederholen Sie die Bereitstellung.	Diese Nachricht ist der Fall für alle Kommunikationsprobleme zwischen den Geräten. Aufgrund seiner Vague-Eigenschaft wird es als Fal geschrieben, um anzugebe dass ein unbekannter Verbindungsfehler aufgetre ist.
unable_to_initiate_deployment_dc	Fehler bei der Richtlinienbereitstellung. Wiederholen Sie die Bereitstellung.	Dieses Problem sollte durc einen weiteren Versuch ge werden. Dies kann der Fall sein, we das FMC die Bereitstellung aufgrund einer temporären Sperre der Datenbank nich starten kann.
device_failure_timeout	Die Bereitstellung auf dem Gerät ist aufgrund eines Timeouts fehlgeschlagen. Wiederholen Sie die Bereitstellung.	Dies bezieht sich auf FTD-Bereitstellungen. Die Proze auf FTD warten 30 Minuten der Dispatch die Bereitstell abgeschlossen hat. Wenn wird die Zeit knapp. In diesem Fall überprüfen S die Verbindung zwischen d Geräten, und wenden Sie s an das TAC, wenn die Verbindung erwartungsgem hergestellt wurde.
device_failure_download_timeout	Fehler bei der Bereitstellung aufgrund eines Timeouts beim Herunterladen der Konfiguration auf das Gerät. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Dies bezieht sich auf FTD-Bereitstellungen. Aufgrund Verbindungsproblemen kan FTD während der Bereitste nicht alle Gerätekonfigurationsdateie herunterladen. Versuchen Sie es erneut, nachdem die Netzwerkverbindung überp

		wurde. Wenn dies überprüft wurde wenden Sie sich an das TA
device_failure_configuration	Fehler bei der Bereitstellung aufgrund eines Konfigurationsfehlers. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Alle Fehler in der Konfigura die von FMC für das Gerät generiert werden, müssen dem Auftreten dieses Fehl auftreten. Dies muss in den USMS- Protokollen analysiert werd um festzustellen, welche Probleme aufgetreten sind um ein Rollback zu versuch Nach der Reparatur sind in Regel ein TAC-Eingriff und Erstellung eines Bugs erforderlich, wenn die Prot nicht mit einem bekannten Fehler im Cisco Bug Searc Tool abgeglichen werden können.
deployment_timeout_no_response_from_device	Fehler bei der Bereitstellung aufgrund eines Timeouts für die Kommunikation mit dem Gerät. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Diese Zeitüberschreitung t auf, wenn das FMC nach 4 Minuten oder früher noch k Rückmeldung von einem G erhalten hat. Dies ist ein Kommunikationsfehler. Kommunikation überprüfen falls verifiziert, TAC kontak
device_failure_change_master	Fehler bei der Bereitstellung im Cluster, da die primäre Einheit geändert wurde. Wiederholen Sie die Bereitstellung.	Wenn bei einer FTD-Cluste Einrichtung der Primärknot bei laufender Bereitstellung dem Gerät wechselt (nach Benachrichtigung), wird die Fehler angezeigt. Wiederholen Sie den Vorga sobald der primäre Knoten

		ist. Der aktuelle Cluster-Mitgliederstatus kann mit diesem Befehl in der CLISH verwalteten Geräts verfolgt werden: >Clusterinformationen anz
device_failure_unknown_master	Fehler bei der Bereitstellung für den Cluster aufgrund eines Fehlers bei der Identifizierung der primären Einheit. Wiederholen Sie die Bereitstellung.	FMC konnte den aktuellen Primärknoten während der Bereitstellung nicht ermitte Dies kann in der Regel auf mehrere Möglichkeiten zurückzuführen sein: Verbindungsprobleme oder aktuelle primäre Fehler, die Cluster auf dem FMC nicht hinzugefügt wurden. Dieser Fehler sollte behobe werden, nachdem die Verbindung wiederhergeste wurde oder nachdem dem Cluster die aktuelle primäre Verbindung hinzugefügt wu und ein erneuter Versuch durchgeführt wurde. Der aktuelle Clusterstatus mit diesem Befehl in der CL des verwalteten Geräts ver werden: >Clusterinformationen anz
cd_deploy_app_sync	Fehler bei der Bereitstellung, da die Clusterkonfigurationssynchronisierung ausgeführt wird. Wiederholen Sie die Bereitstellung.	Dies kann passieren, wenn das Gerät in der App-Synchronisierung befindet. Wenn die App-Synchronisi abgeschlossen ist, wiederh Sie die Bereitstellung erneu
cd_existing_deployment	Fehler bei der Bereitstellung aufgrund eines Konflikts mit der gleichzeitigen vorherigen Bereitstellung. Wenn das Problem nach einem weiteren Versuch weiterhin besteht, wenden Sie sich an Cisco TAC.	Dies kann auftreten, wenn Bereitstellung auf einer Sei gleichzeitig ausgeführt wird der anderen Seite jedoch n Diese werden in der Regel durch Kommunikationsprob zwischen den Geräten verursacht. Wenden Sie sich an das TA wenn Sie nach Auftreten de Zeitüberschreitung immer n keine Bereitstellung vorneh können.

TAC-Unterstützung kontaktieren

Falls die vorherigen Informationen keine Fortsetzung der Richtlinienbereitstellung ermöglichen oder das Problem nicht mit einem bereits vorhandenen dokumentierten Verhalten zusammenhängt, verwenden Sie bitte die im nächsten Link aufgeführten Schritte, um eine Problembehebungsdatei zu erstellen und das TAC zur Analyse und zur Fehlererstellung zu kontaktieren.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.