

# Firepower Threat Defense 정책 구축 문제 해결

## 목차

[소개](#)

[배경 정보](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[정책 구축 개요](#)

[개요 예](#)

[문제 해결](#)

[FMC 그래픽 사용자 인터페이스\(GUI\)](#)

[구축 스크립트 활용](#)

[FMC 로그 문제 해결](#)

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

[/var/log/sf/policy\\_deployment.log](#)

[관리되는 디바이스 문제 해결](#)

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

[/ngfw/var/log/sf/policy\\_deployment.log](#)

[예](#)

[일반적인 실패 메시지](#)

[TAC에 지원을 문의하십시오.](#)

## 소개

이 문서에서는 FTD의 정책 구축 프로세스에 대한 개요와 기본적인 문제 해결 기법에 대해 설명합니다.

## 배경 정보

포함 Cisco Firepower Threat Defense FTD(Stateful Firewall) 기능, Adaptive Security Appliances (ASA) 및 Next-Gen 방화벽 기능(제공: Snort)가 하나의 제품으로 통합되었습니다.

이번 변경으로, Policy Deployment Infrastructure 이제 FTD에서 두 ASA 코드(LINA라고도 함) 모두에 대한 컨피그레이션 변경 사항을 처리합니다. Snort 단일 번들로

## 사전 요구 사항

Cisco에서는 다음 제품에 대한 지식을 권장합니다.

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

## 사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 정책 구축 개요

Cisco FTD는 Policy Deployments 에 등록된 디바이스의 컨피그레이션을 관리하고 푸시아웃하려면 Firepower Management Center (FMC) 자체

구축 내부는 "단계"로 구분되는 일련의 단계가 있습니다.

이 목록에는 FMC 단계가 요약되어 있습니다.

0단계	구축 초기화
1단계	데이터베이스 개체 컬렉션
2단계	정책 및 개체 컬렉션
3단계	NGFW 명령줄 컨피그레이션 생성
4단계	디바이스 구축 패키지 생성
5단계	배포 패키지 보내기 및 받기
6단계	보류 중인 구축, 구축 작업 및 구축 성공 메시지

프로세스의 단계 및 장애 위치를 알면 Firepower 시스템 면.

이전 컨피그레이션으로 인한 충돌 또는 Advanced Flex Configuration 디바이스 보고서에서 다루지 않는 오류를 일으킬 수 있는 키워드가 없습니다.

## 개요 에

1단계. Deployment- 선택할 디바이스를 지정합니다.

2단계. 디바이스에 대한 구축이 커밋되면 FMC는 디바이스와 관련된 모든 컨피그레이션을 수집하기 시작합니다.

3단계. 컨피그레이션이 수집되면 FMC는 패키지를 만들고 SFTunnel이라는 통신 메커니즘을 통해 센서로 전송합니다.

4단계. FMC는 센서에 개별 응답을 듣는 동안 제공된 정책을 사용하여 구축 프로세스를 시작하도록 알립니다.

5단계. 관리되는 디바이스가 아카이브의 압축을 풀고 개별 컨피그레이션 및 패키지를 적용하기 시작합니다.

A. 구축의 전반부는 Snort 구성 Snort 구성이 유효한지 확인하기 위해 로컬에서 테스트됩니다.

유효한 것으로 판명되면 새 컨피그레이션이 운영 디렉토리로 이동하여 Snort. 검증이 실패하면 이 단계에서 정책 구축이 실패합니다.

B. 구축 패키지 로드 후 후반부는 LINA 컨피그레이션에 대한 것으로, 여기서는 ngfwManager 프로세스에 의해 LINA 프로세스에 직접 적용하게 됩니다.

오류가 발생하면 변경 사항이 롤백되고 정책 구축에 오류가 발생합니다.

6단계. 둘 다 Snort LINA 패키지가 성공적이면 관리되는 디바이스가 Snort 새 컨피그레이션을 로드하고 모든 현재 컨피그레이션을 저장하기 위해 다시 시작하거나 다시 로드합니다.

7단계. 모든 메시지가 성공하면 센서는 성공 메시지를 전송하고 Management Center에서 승인될 때까지 기다립니다.

8단계. 작업이 수신되면 FMC는 작업을 성공으로 표시하고 정책 번들을 마칠 수 있게 합니다.

## 문제 해결

문제 발생 Policy Deployment 다음과 같은 이유 때문일 수 있습니다.

1. 잘못된 컨피그레이션
2. FMC와 FTD 간의 통신
3. 데이터베이스 및 시스템 상태
4. 소프트웨어 결함 및 주의 사항
5. 기타 고유한 상황

이러한 문제 중 일부는 쉽게 해결할 수 있는 반면, 다른 문제는 Cisco의 지원이 필요할 수 있습니다 Technical Assistance Center (TAC).

이 섹션의 목표는 문제를 격리하거나 근본 원인을 확인하는 기술을 제공하는 것입니다.

## FMC 그래픽 사용자 인터페이스(GUI)

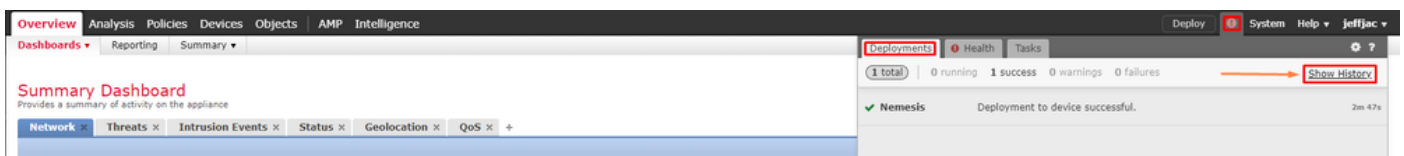
Cisco에서는 구축 실패에 대한 각 문제 해결 세션을 FMC 어플라이언스에서 시작할 것을 권장합니다.

오류 알림 창에는 6.2.3을 초과하는 모든 버전에서 다른 가능한 오류를 지원할 수 있는 추가 도구가 있습니다.

### 구축 스크립트 활용

1단계. Deployments FMC 웹 UI에 나열합니다.

2단계. Deployments 탭을 선택하고 Show History.




3단계. 내부 Deployment History 이 상자에서는 FMC의 모든 이전 구축을 볼 수 있습니다. 더 많은 데이터를 보려는 구축을 선택합니다.

4단계. 배포 요소를 선택하면 Deployment Details 선택 항목에 내부 모든 장치의 목록이 표시됩니다. Transaction. 이러한 항목은 다음 열로 구분됩니다. Device Number, Device Name, Status, 및 Transcript.

Deployment History

The screenshot displays the 'Deployment History' window. On the left, a list of deployment events is shown, with the first event (ID 1) highlighted in a red box. This event is for 'jeffjac' and occurred on 2019-11-20 at 07:01 PM, with a status of 'Success'. The right pane shows 'Deployment details for jeffjac at 2019-11-20 07:01 PM'. It contains a table with columns for 'Device', 'Status', and 'Transcript'. The first row shows device 'Nemesis' with a 'Success' status. A red arrow points to a download icon in the 'Transcript' column for this device.

Device	Status	Transcript
1 Nemesis	✓ Success	

5단계. 문제가 있는 디바이스를 선택하고 Transcript(기록) 옵션을 클릭하면 관리되는 디바이스에 있는 컨피그레이션 및 장애에 대해 알려줄 수 있는 개별 구축 기록을 확인할 수 있습니다.

## 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 >> 
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 vpnc
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

6단계. 이 녹취록은 특정 장애 조건을 지정하고 다음 단계를 위해 매우 중요한 번호를 지정할 수 있습니다. **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

7단계. **Firepower Deployment**, 이 **Transaction ID** 정책 구축의 각 개별 섹션을 추적하는 데 사용할 수 있는 기능입니다. 이를 통해 디바이스의 **Command-Line**에서 교정 및 분석을 위해 이 데이터의 더욱 상세한 버전을 얻을 수 있습니다.

**팁:** 트랜잭션 ID를 찾을 수 없거나 트랜잭션 ID가 인쇄되기 이전 버전인 경우 이 로그를 사용하여 개별 오류 메시지를 찾을 수 있습니다.

## FMC 로그 문제 해결

로그를 분석하기 위해 Cisco TAC와 협력하는 것이 적절하지만 로그를 통해 검색하면 초기 문제 격리 및 신속한 해결에 도움이 될 수 있습니다. FMC에는 정책 구축 프로세스에 대한 세부 정보를 표시하는 여러 로그 파일이 있습니다.

가장 일반적으로 참조되는 두 로그는 다음과 같습니다 `policy_deployment.log` 및 `usmshredsvcs.log`.

이 문서에서 언급된 모든 파일은 다음과 같은 여러 Linux 명령으로 볼 수 있습니다 `more`, `less` 및 `vi`. 그러나, 단지 `read` 작업이 수행됩니다. 모든 파일을 보려면 루트 액세스가 필요합니다.

### `/var/opt/CSCOpX/MDC/log/operation/usmshredsvcs.log`

이 로그는 FMC에서 정책 구축 작업을 시작하고 각 단계가 완료되었음을 명확히 표시하며, 이를 통해 장애 코드와 함께 구축에 장애가 발생한 단계를 확인할 수 있습니다.

이 `transactionID` 로그의 JSON 부분에 포함된 값을 사용하여 하나의 특정 배포 시도와 관련된 로그 항목을 찾을 수 있습니다.

```
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`

이 로그 파일은 6.4에서 시작되는 6.x 릴리스에 걸쳐 존재했지만 범위가 확장되었습니다.

이제 구축 패키지를 구축하기 위해 FMC에서 수행하는 자세한 단계에 대해 설명합니다. 따라서 1단계 - 4단계의 실패를 분석하는 데 가장 적합합니다.

각 단계의 시작 부분은 **"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)
...
```

## 관리되는 디바이스 문제 해결

각 관리되는 디바이스에 대한 디바이스 패키지, 고가용성 컨피그레이션, 이전 단계의 결과에 따라 달라지는 추가 단계 및 섹션이 있습니다.

관리 대상 디바이스에서 구축 문제가 장애로 격리된 경우, 디바이스에 두 개의 로그가 있는 디바이스에서 추가 트러블슈팅을 수행할 수 있습니다. **policy\_deployment.log** 및 **ngfwManager.log**입니다.

### /ngfw/var/log/ngfwManager.log

이 로그 파일은 다음 작업을 수행하는 자세한 단계를 제공합니다. **Config Communication Manager** 및 **Config Dispatcher fmc**와 통신하려면 구축 패키지와 함께 Snort 및 LINA 구성의 검증 및 애플리케이션을 조정합니다.

다음은 주요 단계의 시작을 나타내는 **ngfwManager.log**의 몇 가지 예입니다.

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**

이 로그에는 적용된 정책의 세부사항이 포함되어 있습니다 Snort. 로그의 내용은 대부분 고급이며 TAC에서 분석해야 하지만 몇 가지 주요 항목으로 프로세스를 추적할 수 있습니다.

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:

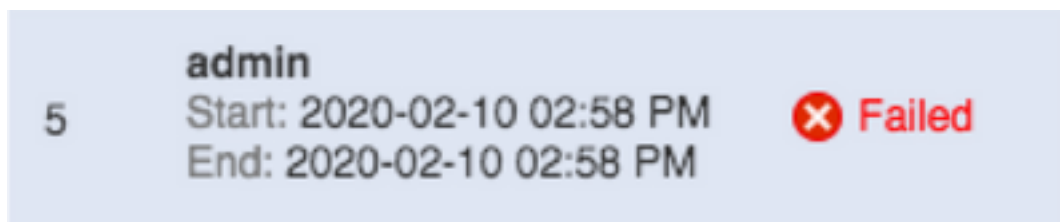
```
Jul 18 17:22:14 firepower policy_apply.pl[26571]: INFO notifyProcesses - sandbox =  
/var/cisco/deploy/sandbox/exported-files took 16 (memory = 169.52 MB, change = 16.95 MB)  
(Framework 3976<964 <- Transaction 1680 <- main 200)
```

After LINA config apply finishes, Snort deployment is finalized:

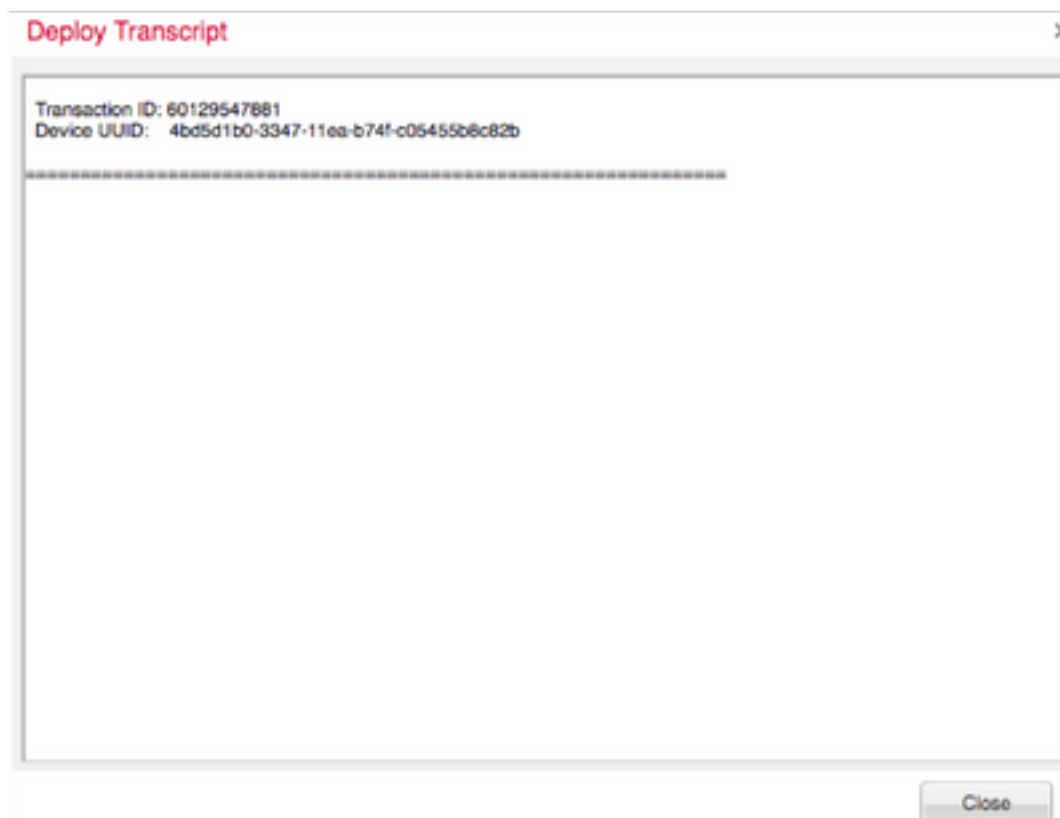
```
Jul 18 17:23:32 firepower policy_apply.pl[26913]: INFO starting finalizeDeviceDeployment -  
sandbox = /var/cisco/deploy/sandbox (memory = 101.14 MB) (Framework 3950<980 <- Transaction  
1740 <- main 206)
```

## 예

1단계. 구축이 실패합니다.



2단계. Deploy Transcript 및 Transaction ID.



3단계. Management Center Linux 유틸리티 사용 less fmc에 표시된 대로 파일을 읽으려면

예: "sudo less /var/opt/CSC0px/MDC/log/operation/usmsharedsvcs.log"(sudo 비밀번호는 ssh용 사용자 비밀번호입니다.)

```
admin@firepower:~$ sudo less /var/opt/CSC0px/MDC/log/operation/usmsharedsvcs.log
Password: _
```

4단계. less에서는 슬래시를 사용하고 메시지 ID에 를 입력하여 deployment transactionID와 관련된 로그를 검색합니다.

예: "/60129547881"(While in less, n을 사용하여 다음 결과로 이동)

실행 중인 메시지의 예:

```
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" ]
}
```

실패 메시지의 예:

```

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) 적절한 장애를 공통 장애 메시지의 별표와 비교합니다.

즉, failed\_to\_retrieve\_running\_configuration은 두 디바이스 간의 통신 장애 중에 발생합니다.

## 일반적인 실패 메시지

이러한 메시지는 의 프론트 엔드에서 볼 수 있는 일반적인 장애 메시지입니다 Management Center Task 백엔드에서 볼 수 있는 오류 코드도 포함됩니다.

이러한 메시지는 가능한 해결책에 대한 일반적인 이유와 비교 및 분석할 수 있습니다.

이러한 항목이 표시되지 않거나 상황이 해결되지 않을 경우 TAC에 문의하여 도움을 받으십시오.

오류 코드	오류 메시지	이유
device_has_changed_domain	배포 실패 - 장치가 도메인을 {SRCDOMAIN}에서 {DESTINATIONDOMAIN}(으)로 변경했습니다. 나중에 다시 시도하십시오.	이 오류는 일반적으로 장치 동되었거나 두 번째 도메인 가져온 경우에 발생합니다. 인 간 정보가 발생하지 않은 에서 재구축하면 일반적으로 문제가 해결됩니다.
device_currently_under_deployment	이 장치에 대해 다른 배포가 진행 중이므로 배포에 실패했습니다. 나중에 다시 시도하십시오.	이는 일반적으로 구축의 디 스에서 구축이 트리거될 때 됩니다. 일부 버전에서는 장

림 없이 이 기능을 사용할 수 없습니다. 그러나 이 단계는 문제 해결 지원을 위해 여전히 존재합니다.

device\_not\_member\_of\_container

클러스터의 멤버인 개별 디바이스에서는 구축을 수행할 수 없습니다. 나중에 클러스터를 다시 구축해 보십시오.

이 메시지는 FXOS(Firepower eXtensible Operable System) Chassis Manager가 있는 디바이스의 FTD에 적용됩니다. 클러스터가 FMC가 아닌 FXOS에 있는 경우 이 메시지가 표시될 때까지 구축을 시도하기 전에 Management Center 어플리케이션에 클러스터를 생성하십시오.

policy\_altered\_after\_timestamp\_for\_other\_devices\_in\_job\_error

하나 이상의 장치에 대한 정책이 {TIMESTAMP} 이후로 변경되었습니다. 배포를 다시 시도하십시오.

이 오류는 사용자가 배포를 시작한 후 CSM 요소 및 도메인 스코프가 변경되기 전에 배포 작업의 모든 장치에 대해 정책이 변경되는 경우에 표시됩니다. 재구축은 이 문제를 해결합니다. 많은 사용자가 배포하는 동일한 FMC를 사용하여 개체 집합하고 저장하는 경우 이 문제가 발생할 수 있습니다.

policy\_altered\_after\_timestamp\_error

{Timestamp} 이후 {Policy Name} 정책이 변경되었습니다. 배포를 다시 시도하십시오.

이 오류는 사용자가 배포를 시작한 후 CSM 및 도메인 스코프가 변경되기 전에 배포 작업에서 관련 장치에 대한 정책/정책이 변경되는 경우에 표시됩니다. 재구축은 이 문제를 해결합니다.

csm\_snapshot\_error

정책 및 개체 수집이 실패하여 배포에 실패했습니다. 반복 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.

최근 정책 가져오기가 제공된 후 1시간 정도 기다렸다가 재구축을 시도합니다. 이 작업을 계속 진행할 수 없는 경우 데이터베이스 관련 메시지를 참조하십시오. 따라서 TAC에 문의하십시오.

domain\_snapshot\_timeout

정책 및 개체 수집에 대한 시간 초과로 인해 배포에 실패했습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.

도메인 스냅샷의 시간 제한은 기본적으로 5분입니다. 시스템 부하가 높거나 하이퍼바이저가 제대로 작동하지 않을 경우 시간이 부자연스럽게 지연될 수 있습니다. 이는 Management Center 디바이스에 적절한 양의 메모리 리소스도 제공되지 않은 경우 발생할 수 있습니다. 로드 없이 이러한 상황이 발생하거나 나중에 진행되지 않을 경우 TAC에 문의하십시오.

domain\_snapshot\_errors

정책 및 개체 컬렉션에서 배포에 실패했습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.

TAC에 문의하십시오. 고급 해결이 필요합니다.

failed\_to\_retrieve\_running\_configuration

디바이스에서 실행 컨피그레이션 정보를 검색하지 못하여 구축에 실패했습니다. 배포를 다시 시도하십시오.

이 메시지는 엔드 센서와 피어 간의 연결이 예상대로 작동하지 않을 때 발생할 수 있습니다. 피어 간의 터널 상태를 확인하고 디바이스 간의 연결을 모니터링하십시오.

터널이 예상대로 작동하고 디바이스가 통신할 수 있는 경우 TAC에 문의하십시오.

device\_is\_busy

디바이스가 이전 구축 또는 재시작을 실행 중일 수 있으므로 구축에 실패했습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.

이 메시지는 FTD에서 이전 이 진행 중인 동안 FMC가 을 시도할 때 표시됩니다. 으로 이전 구축이 FTD에서 되지 않고 FTD가 재부팅되 FTD의 ngfwManager 프로세스가 재시작될 때 발생합니다 후 프로세스를 공식적으로 초과하도록 다시 시도하면 제가 해결됩니다. 지연이 발생했거나 지연을 할 수 없는 경우 TAC에 문의하십시오.

no\_response\_for\_show\_cmd

디바이스 연결 문제로 인해 구축에 실패했거나 디바이스가 응답하지 않습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.

FMC는 특정 LINA "show" 명령을 실행하여 컨피그레이션을 위해 실행 중인 컨피그레이션을 가져옵니다. 이는 엔드 센서의 ngfwManager 프로세스에 연결 문제 또는 가 있을 때 발생할 수 있습니다. 유닛 간 연결 문제가 발생하면 경우 TAC에 문의하십시오.

network\_latency\_or\_device\_not\_reachable

디바이스와의 통신 오류로 인해 구축에 실패했습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.

일반적으로 디바이스 간의 워크 레이턴시가 높으면 시간 초과가 발생합니다. 디바이스 간의 네트워크 레이턴시가 설명서에 언급된 버전의 최시간과 일치하는지 확인합니다.

slave\_app\_sync

클러스터 구성 동기화가 진행 중이므로 배포에 실패했습니다. 배포를 다시 시도하십시오.

이는 FTD 클러스터 설정에 적용됩니다. 앱 동기화(컨피그 동기화)가 진행 중인 동안 FTD 클러스터에서 구축을 하면 FTD에서 이를 거부합니다. 컨피그레이션 동기화 후 다시 시도하면 이 문제가 해결됩니다. 관리되는 디바이스 CLISHC 다음 명령을 사용하여 현재 클러스터 상태를 추적할 수 있습니다.  
>클러스터 정보 표시

asa\_configuration\_generation\_errors

배포에서 장치 구성을 생성하지 못했습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.

앞에서 언급한 USMS 로그를 포함한 후 어떤 컨피그레이션 오류가 발생하는지 확인하십시오. 이러한 로그는 일반적으로 Cisco 버그 툴을 통해 로깅해보거나 Cisco TAC에 문의하십시오.

		여 추가 문제를 해결할 수 있는 버그입니다.
interface_out_of_date	디바이스의 인터페이스가 만료되어 구축하지 못했습니다. 인터페이스 페이지에 컨피그레이션을 저장하고 다시 시도하십시오.	이는 구축 도중 또는 구축 중 디바이스에서 인터페이스가 연결되지 않은 경우 4100 또는 9300 모델에서 발생합니다. 구축을 시도하기 전에 인터페이스가 완전히 연결되었는지 연결되지 않았는지 확인하십시오.
device_package_error	배포에서 장치에 대한 구성을 생성하지 못했습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.	이 오류는 디바이스에 대한 컨피그레이션 생성 실패로 나타납니다. TAC에 문의하십시오.
device_package_timeout	구성 생성 중 시간 초과로 인해 배포에 실패했습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.	이는 디바이스 간에 정상적인 범위를 벗어난 레이턴시가 존재할 경우 발생할 수 있습니다. 레이턴시가 표준화된 후에도 이 문제가 발생하는 경우 TAC에 문의하십시오.
device_communication_errors	장치 통신 오류로 인해 구축에 실패했습니다. 네트워크 연결을 확인하고 구축을 다시 시도하십시오.	이 메시지는 디바이스 간의 통신 문제에 대한 대비책입니다. 이러한 특성 때문에 알 수 없는 통신 오류가 발생했음을 나타내며 백으로 작성됩니다.
unable_to_initiate_deployment_dc	정책 배포 실패 배포를 다시 시도하십시오.	다른 시도가 이 문제를 해결하지 않습니다. 이 문제는 FMC가 데이터베이스의 임시 잠금으로 인해 구축을 시작할 수 없을 때 발생할 수 있습니다.
device_failure_timeout	시간 초과로 인해 디바이스에 구축하지 못했습니다. 배포를 다시 시도하십시오.	이는 FTD 구축과 관련이 있습니다. FTD의 프로세스는 디바이스가 구축을 완료할 때까지 30분 이상 기다립니다. 그렇지 않으면



간이 초과됩니다.  
이 경우 장치 간 연결을 확인  
연결이 예상대로 이루어지  
TAC에 문의하십시오.

**device\_failure\_download\_timeout**

디바이스에 대한 컨피그레이션 다운  
로드 시간 초과로 인해 구축에 실패했  
습니다. 다른 시도 후에도 문제가 지속  
되면 Cisco TAC에 문의하십시오.

이는 FTD 구축과 관련이 있  
다. FTD는 연결 문제로 인해  
축 중에 모든 디바이스 컨피  
그레이션 파일을 다운로드할 수  
없습니다.  
네트워크 연결이 확인된 후  
시도하십시오.  
이 사항이 확인되면 TAC에  
문의하십시오.

**device\_failure\_configuration**

구성 오류로 인해 배포에 실패했습니  
다. 다른 시도 후에도 문제가 지속되면  
Cisco TAC에 문의하십시오.

디바이스에 대해 FMC에서  
한 컨피그레이션의 모든 오  
류가 이 오류 후 적용으로 이어지  
지 않습니다.  
USMS 로그에서 이를 분석  
하여 어떤 문제가 발생하는지 확  
인하고 롤백해야 합니다.  
복구되면 Cisco Bug Search  
Tool에서 알려진 결함과 로  
깅을 매칭할 수 없는 경우 일반적  
으로 TAC 개입 및 버그 생성이 필  
요합니다.

**deployment\_timeout\_no\_response\_from\_device**

장치와의 통신 시간 초과로 인해 구축  
에 실패했습니다. 다른 시도 후에도 문  
제가 지속되면 Cisco TAC에 문의하십  
시오.

이 시간 제한은 FMC가 45분  
이상 지난 후 디바이스에서 응  
답이 없는 경우 발생합니다.  
통신 오류입니다.  
통신을 확인하고 확인되면  
TAC에 문의하십시오.

device\_failure\_change\_master

기본 유닛이 변경되어 클러스터에 배포하지 못했습니다. 배포를 다시 시도하십시오.

FTD 클러스터 설정 구축의 디바이스에서 구축이 진행될 때(사후 알림) 기본 노드가 되면 이 오류가 표시됩니다. 기본 노드가 안정되면 다시 시도하십시오.  
관리되는 디바이스 CLISHC에서 현재 클러스터 멤버 상태를 명령으로 추적할 수 있습니다.  
>클러스터 정보 표시

device\_failure\_unknown\_master

기본 유닛 식별 오류로 인해 클러스터에 구축하지 못했습니다. 배포를 다시 시도하십시오.

FMC에서 구축 중에 현재 기본 노드를 확인할 수 없습니다. 이는 일반적으로 몇 가지 기 때문일 수 있습니다. 연결된 또는 현재 기본 항목이 FMC 클러스터에 추가되지 않았을 수 있습니다.  
연결이 다시 설정된 후 또는 기본 노드를 FMC 클러스터에 추가하고 다시 시도한 후 확인되어야 합니다.  
관리되는 디바이스 CLISHC에서 다음 명령을 사용하여 현재 클러스터 상태를 추적할 수 있습니다.  
>클러스터 정보 표시

cd\_deploy\_app\_sync

클러스터 구성 동기화가 진행 중이므로 배포에 실패했습니다. 배포를 다시 시도하십시오.

디바이스가 앱 동기화 상태에 있으면 이 문제가 발생할 수 있습니다. 앱 동기화가 완료되면 배포를 다시 시도하십시오.

cd\_existing\_deployment

동시 이전 배포와 충돌하여 배포에 실패했습니다. 다른 시도 후에도 문제가 지속되면 Cisco TAC에 문의하십시오.

이는 구축이 한 쪽에서 동시 실행되지만 다른 쪽에서 동시 실행되지 않는 경우에 발생합니다.  
이러한 문제는 대개 디바이스

의 통신 문제로 인해 발생합  
시간 초과가 발생한 후에도  
이 불가능한 경우 TAC에 문  
십시오.

## TAC에 지원을 문의하십시오.

이전 정보에서 정책 구축을 진행할 수 없거나 문제가 기존의 문서화된 동작과 관련이 없는 것으로 보이는 경우, 다음 링크에 제공된 단계를 사용하여 문제 해결 파일을 생성하고 분석 및 버그 생성을 위해 TAC에 문의하십시오.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.