Dépannage des déploiements de politiques de défense Firepower

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Présentation du déploiement des politiques

Exemple de présentation

Dépannage

- Interface graphique utilisateur (GUI) FMC
- Dépannage avec les journaux FMC
- Dépannage des périphériques gérés
- Exemple

Messages d'échec courants

Informations connexes

Introduction

Ce document décrit une présentation générale du processus de déploiement des stratégies sur le FTD et les techniques de dépannage de base.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

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

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

Avec Cisco Firepower Threat Defense (FTD), les fonctionnalités de pare-feu avec état traditionnelles offertes par Adaptive Security Appliances (ASA) et les fonctionnalités de Next-Gen pare-feu (optimisées par Snort) sont désormais combinées en un seul produit. En raison de cette modification, Policy Deployment Infrastructure sur FTD gère désormais les modifications de configuration à la fois pour le code ASA (également appelé LINA) et Snort dans un seul bundle.

Présentation du déploiement des politiques

Cisco FTD utilise Policy Deployments pour gérer et diffuser les configurations des périphériques enregistrés auprès du Firewall Management Center (FMC) lui-même.

À l'intérieur du déploiement, une série d'étapes sont divisées en phases.

Les phases FMC peuvent être résumées dans cette liste.

Phase 0	Initialisation du déploiement
Phase 1	Database Object, collection
Phase 2	Collection Policy and Object
Phase 3	Génération de la configuration de ligne de commande NGFW
Phase 4	Génération de package de déploiement de périphérique
Phase 5	Envoi et réception du package de déploiement
Phase 6	Messages de déploiement, d'actions de déploiement et de réussite de déploiement en attente

La connaissance des phases et de l'emplacement des pannes dans le processus peut aider à dépanner les pannes auxquelles un Firepower système est confronté.

Dans certaines situations, il peut s'agir d'un conflit dû à des configurations précédentes ou d'un

problème causé par un Advanced Flex Configuration qui manque d'un mot clé pouvant entraîner des défaillances que le rapport de périphérique ne traite pas.

Exemple de présentation

Étape 1. Cliquez sur **Deployment**, qui spécifie le périphérique à sélectionner.

Étape 2. Lorsque le déploiement d'un périphérique est validé, le FMC commence à collecter toutes les configurations pertinentes pour le périphérique.

Étape 3. Lorsque les configurations sont collectées, le FMC crée le package et l'envoie au capteur via son mécanisme de communication appelé SFTunnel.

Étape 4. Le FMC notifie le capteur de démarrer le processus de déploiement avec la stratégie fournie pendant qu'il écoute les réponses individuelles.

Étape 5. Le périphérique géré déballe l'archive et commence à appliquer les configurations et packages individuels.

R. La première moitié du déploiement est la configuration dans laquelle Snort la Snort configuration est testée localement afin de s'assurer de sa validité.

Une fois la validation prouvée, la nouvelle configuration est déplacée vers le répertoire de production pour que, Snort. en cas d'échec de la validation, le déploiement de la stratégie échoue à cette étape.

B. La seconde moitié de la charge du package de déploiement concerne la configuration LINA, où elle est appliquée directement au processus LINA par le processus ngfwManager.

En cas d'échec, les modifications sont annulées et un échec du déploiement de la stratégie se produit.

Étape 6. Si les deux packages, Snort et LINA, réussissent, le périphérique géré indique de redémarrer ou de redémarrer, Snort afin de charger la nouvelle configuration et d'enregistrer toutes les configurations actuelles.

Étape 7. Si tous les messages aboutissent, le capteur envoie un message de réussite et attend qu'un accusé de réception soit envoyé par le centre de gestion.

Étape 8. Une fois reçu, le FMC marque la tâche comme un succès et permet à l'ensemble de politiques de se terminer.

Dépannage

Les problèmes rencontrés pendant Policy Deployment peuvent être dus, mais ne sont pas limités à :

1. Mauvaise Configuration
2. Communication entre le CSP et le DFT
3. Intégrité de la base de données et du système
4. Défauts logiciels et avertissements
5. Autres situations uniques

Certains de ces problèmes peuvent être facilement résolus, tandis que d'autres peuvent nécessiter l'assistance de Cisco Technical Assistance Center (TAC).

L'objectif de cette section est de fournir des techniques permettant d'isoler le problème ou de déterminer la cause première.

Interface graphique utilisateur (GUI) FMC

Cisco recommande que chaque session de dépannage pour les échecs de déploiement démarre sur l'appliance FMC.

Dans la fenêtre de notification de panne, sur toutes les versions au-delà de 6.2.3, il y a des outils supplémentaires qui peuvent aider avec d'autres pannes possibles.

Utiliser les transcriptions de déploiement

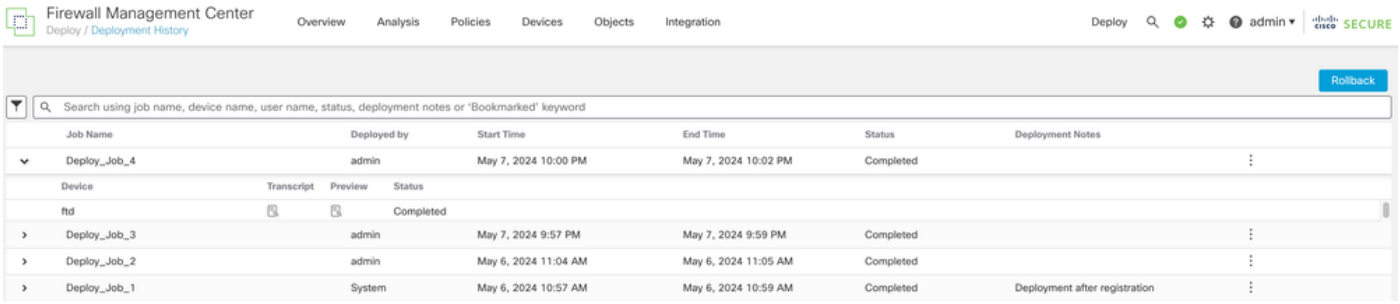
Étape 1. Affichez la **Deployments** liste sur l'interface utilisateur Web de FMC.

Étape 2. Lorsque l'**Deployments**onglet est sélectionné, cliquez sur **Show History**.

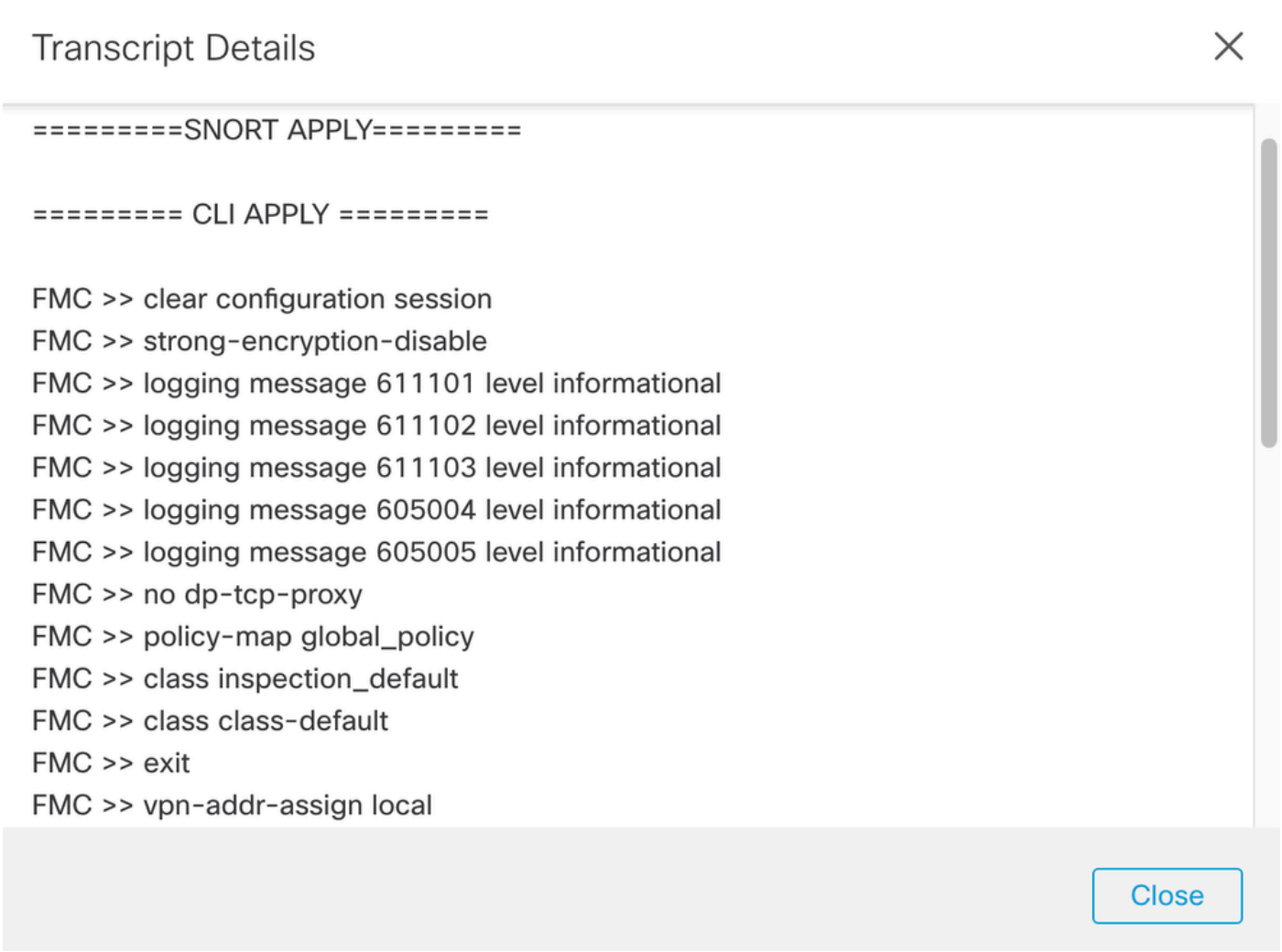


Étape 3. À l'intérieur de la Deployment History boîte, vous pouvez voir tous les déploiements précédents de votre FMC. Sélectionnez le déploiement dans lequel vous souhaitez afficher plus de données.

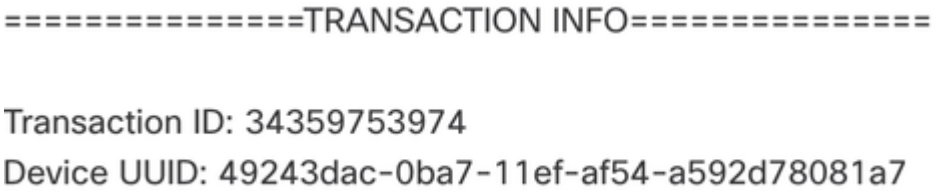
Étape 4. Une fois qu'un élément de déploiement est sélectionné, Deployment Details la sélection affiche la liste de tous les périphériques à l'intérieur du Transaction. Ces entrées sont réparties dans les colonnes suivantes : Device Number, Device Name, Status,et Transcript.



Étape 5. Sélectionnez le périphérique en question et cliquez sur l'option transcript pour voir le transcript de déploiement individuel qui peut vous informer des échecs ainsi que des configurations qui sont placées sur les périphériques gérés.



Étape 6. Ce relevé de notes peut indiquer certaines conditions d'échec et indiquer un nombre très important pour l'étape suivante : Transaction ID.



Étape 7. Dans un Firepower Deploymentexemple, la Transaction ID permet de suivre chaque section individuelle d'un déploiement de stratégie. Grâce à cela, sur la ligne de commande du périphérique, vous pouvez obtenir une version plus approfondie de ces données à des fins de

correction et d'analyse.

Conseil : Si vous ne parvenez pas à localiser l'ID de transaction ou si vous disposez d'une version antérieure à l'impression, ce journal peut toujours être utilisé pour localiser les messages d'échec individuels.

Dépannage avec les journaux FMC

Bien qu'il soit approprié de faire appel au centre d'assistance technique Cisco pour analyser les journaux, une recherche dans les journaux peut vous aider à isoler les problèmes et à accélérer leur résolution. Il existe plusieurs fichiers journaux sur FMC qui révèlent les détails du processus de déploiement de la stratégie.

Les deux journaux les plus souvent référencés sont policy_deployment.log et usmsharedsvcs.log.

Tous les fichiers mentionnés dans ce document peuvent être visualisés avec plusieurs commandes Linux telles que **more**, **less** et **vi**. Cependant, il est très important de s'assurer que seules **read** les actions sont exécutées. Tous les fichiers nécessitent un accès racine pour pouvoir les afficher.

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

Ce journal marque clairement le début de la tâche de déploiement de stratégie sur FMC et la fin de chaque phase, ce qui permet de déterminer la phase où le déploiement a rencontré une défaillance, ainsi que le code de défaillance.

La transactionID valeur incluse dans la partie JSON du journal peut être utilisée pour rechercher des entrées de journal associées à une tentative de déploiement particulière.

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

```
"requestID": "e3be908a0ef711ef9d519da21f9032fa",
"version": "7.2.5"
}
```

/var/log/sf/policy_deployment.log

Bien que ce fichier journal ait existé dans toutes les versions 6.x, qui commencent à la version 6.4, sa couverture a été étendue.

Il décrit maintenant les étapes détaillées effectuées sur FMC pour créer les packages de déploiement. Il est donc préférable de l'utiliser pour analyser les échecs des phases 1 à 4.

Le début de chaque phase est marqué par une ligne avec INFO start.

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

Dépannage des périphériques gérés

D'autres phases et sections dépendent du package de périphériques, de la configuration de la haute disponibilité et du résultat des phases précédentes pour chaque périphérique géré.

Si un problème de déploiement est isolé d'une défaillance sur le périphérique géré, un dépannage plus approfondi peut être effectué sur le périphérique avec deux journaux sur le périphérique : policy_deployment.log et ngfwManager.log.

/ngfw/var/log/ngfwManager.log

Ce fichier journal fournit des étapes détaillées prises par Config Communication Manager et Config Dispatcher pour communiquer avec FMC, travailler avec le package de déploiement et orchestrer la validation et l'application des configurations Snort et LINA.

Voici quelques exemples de ngfwManager.log qui représentent le début des phases 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
May 30 16:37:10 ccm[4293] Thread-10: DEBUG com.cisco.ccm.ConfigCommunicationManager- <?xml version="1.0
```

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

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

```
FTD begins the deployment of policy changes:

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

```
FTD begins LINA deployment:

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

```
FTD begins finalizing the deployment:

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

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

Ce journal contient les détails de la politique appliquée à Snort. Bien que le contenu du journal soit principalement avancé et nécessite une analyse par le TAC, il est toujours possible de tracer le processus avec quelques entrées clés :

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

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

```
Config validation begins:

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

```
Validation has completed successfully:
```

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

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

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

Snort processes will reload to apply the new configurations:

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

Snort reload has completed successfully:

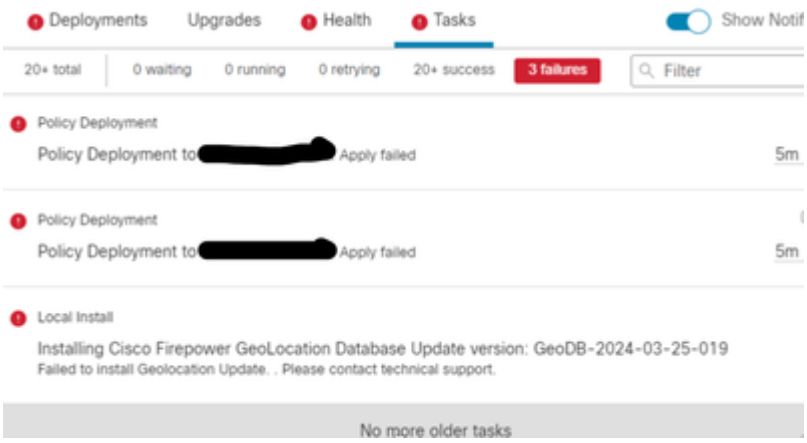
Jul 18 17:22:14 firepower policy_apply.pl[26571]: INFO notifyProcesses - sandbox = /var/cisco/deploy/sa

After LINA config apply finishes, Snort deployment is finalized:

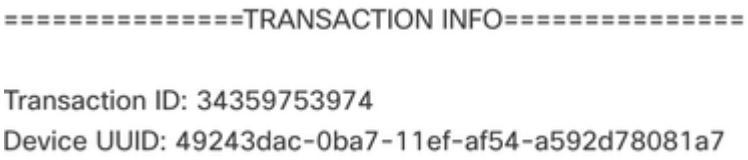
Jul 18 17:23:32 firepower policy_apply.pl[26913]: INFO  starting finalizeDeviceDeployment - sandbox = /
```

Exemple

Étape 1. Un déploiement échoue.

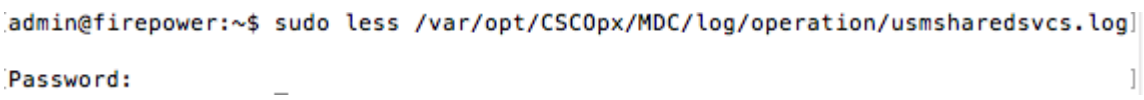


Étape 2. Obtenez les **Deploy Transcript** et **Transaction ID**.



Étape 3 : connexion SSH à votre **Management Center** et utilisation de l'utilitaire Linux **less** pour lire le fichier comme indiqué sur votre FMC :

Exemple : sudo less /var/opt/CSCOpx/MDC/log/operation/usmsharedsvcs.log (Le mot de passe sudo est votre mot de passe utilisateur pour ssh.)



Étape 4. Lorsque vous utilisez **less**, la barre oblique avant et entrez l'ID de message pour rechercher les journaux associés à l'ID de transaction de déploiement.

Exemple : /60129547881 (en cours**less**, d'utilisation n pour accéder au résultat suivant.)

Exemple d'exécution du 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" ]
}
```

Exemple de message d'échec

```
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) Comparez la défaillance appropriée à la table jointe des messages de défaillance courants.

Autrement dit, failed_to_recover_running_configuration se produit lors d'échecs de communication entre les deux périphériques.

Messages d'échec courants

Il s'agit de messages d'échec courants qui peuvent être vus sur le front-end de l'ordinateur, Management Center Task ainsi que du code d'erreur qui peut être vu dans le back-end.

Ces messages peuvent être analysés et comparés avec les raisons communes des résolutions possibles. Si elles ne sont pas vues ou ne résolvent pas votre situation, veuillez contacter le TAC pour obtenir de l'aide.

Code d'erreur	Messages d'erreur	Motif
device_has_changed_domain	Échec du déploiement : le périphérique a changé de domaine. de {SRCDOMAIN} à {DESTINATIONDOMAIN}. Réessayez plus tard.	Cette erreur se produit généralement lorsqu'un périphérique a été déplacé ou est pris à partir d'un second domaine. Un redéploiement alors qu'aucune information interdomaine ne se produit corrige généralement ce problème.
device_currently_under_deployment	Échec du déploiement en raison d'un autre déploiement en cours pour ce périphérique. Réessayez plus tard.	Ceci est généralement signalé lorsque le déploiement est déclenché

		sur un périphérique en cours de déploiement. Dans certaines versions, cela est évité sans notification d'échec ; cependant, cette phase existe toujours pour l'assistance au dépannage.
device_not_member_of_container	Le déploiement ne peut pas être effectué sur un périphérique individuel qui est membre d'un cluster. Réessayez de déployer le cluster ultérieurement.	Ce message s'applique au FTD sur les périphériques équipés du gestionnaire de châssis FXOS (Firepower eXtensible Operative System). Si le cluster est construit sur FXOS, mais pas sur le FMC, ce message s'affiche. Créez le cluster sur l'appliance Management Center avant de tenter le déploiement.
policy_altered_after_timestamp_for_other_devices_in_job_error	Les stratégies d'un ou de plusieurs périphériques ont été modifiées depuis {TIMESTAMP}. Recommencez le	Cette erreur s'affiche si une stratégie/un objet est modifié pour un

	déploiement.	périphérique dans le travail de déploiement après le déploiement des déclencheurs utilisateur et avant la création des éléments CSM et des instantanés de domaine. Un redéploiement corrige ce problème. Cela peut se produire lorsque de nombreux utilisateurs utilisent le même FMC pour modifier et enregistrer des objets pendant leur déploiement.
policy_altered_after_timestamp_error	La stratégie {Policy Name} a été modifiée depuis {Timestamp}. Recommencez le déploiement.	Cette erreur s'affiche si une stratégie/un objet est modifié pour le périphérique concerné dans le travail de déploiement, après le déploiement des déclencheurs utilisateur et avant la

		création des snapshots CSM et de domaine. Un redéploiement corrige ce problème.
csm_snapshot_error	Échec du déploiement en raison de l'échec de la collecte des stratégies et des objets. Si le problème persiste après une tentative répétée, contactez le TAC Cisco.	Si une importation de stratégie récente est fournie, attendez environ une heure et essayez un autre déploiement. Si cela ne vous permet pas de poursuivre, contactez le TAC car il s'agit d'un message lié à la base de données.
domain_snapshot_timeout	Échec du déploiement en raison du délai d'attente pour la collecte des stratégies et des objets. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Par défaut, le délai d'attente de l'instantané de domaine est de 5 minutes. Si la charge du système est élevée ou si l'hyperviseur ne fonctionne pas correctement, cela peut entraîner des retards non naturels dans l'appel.

		Cela peut se produire si le centre de gestion ou le périphérique ne dispose pas de la quantité de ressources mémoire appropriée. Si cela se produit sans charge ou si vous ne continuez pas ultérieurement, contactez le TAC.
domain_snapshot_errors	Échec du déploiement dans la stratégie et la collection d'objets. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Contactez le TAC. Un dépannage avancé est requis.
failed_to_retrieve_running_configuration	Échec du déploiement en raison de l'échec de la récupération des informations de configuration d'exécution du périphérique. Recommencez le déploiement.	Ce message peut s'afficher lorsque la connectivité entre un capteur d'extrémité et un FMC ne fonctionne pas comme prévu. Vérifiez l'intégrité du tunnel entre les unités et surveillez la connectivité entre les deux périphériques.

		Si le tunnel fonctionne comme prévu et que les périphériques peuvent communiquer, contactez le TAC.
device_is_busy	Le déploiement a échoué car le périphérique peut exécuter un déploiement précédent ou un redémarrage. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Ce message s'affiche lorsque FMC tente un déploiement alors qu'un déploiement précédent est en cours sur FTD. Généralement, cela se produit lorsqu'un déploiement précédent est inachevé sur FTD et que le FTD a redémarré ou que le processus ngfwManager sur FTD a redémarré. Une nouvelle tentative après 20 minutes pour permettre aux processus d'expirer officiellement doit résoudre ce problème. Si vous êtes en retard ou si le

		retard n'est pas acceptable, contactez le TAC.
no_response_for_show_cmd	Échec du déploiement en raison de problèmes de connectivité avec le périphérique ou le périphérique ne répond pas. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	FMC exécute certaines commandes LINA show pour récupérer la configuration en cours en vue de la génération de la configuration. Cela peut se produire en cas de problèmes de connectivité ou de processus ngfwManager sur le capteur final. Si vous ne rencontrez pas de problèmes de connectivité entre vos unités, contactez le TAC.
network_latency_or_device_not_reachable	Échec du déploiement en raison d'un échec des communications avec le périphérique. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Se produit généralement avec une latence réseau élevée entre les périphériques pour provoquer un dépassement du délai d'attente de la

		stratégie. Vérifiez la latence du réseau entre les périphériques pour vérifier qu'elle correspond aux valeurs minimales pour la version mentionnée dans le guide de l'utilisateur.
slave_app_sync	Échec du déploiement car la synchronisation de la configuration du cluster est en cours. Recommencez le déploiement.	Ceci s'applique uniquement aux configurations de cluster FTD. Si un déploiement est tenté sur un cluster FTD alors que la synchronisation d'application (synchronisation de configuration) est en cours, la même tentative est rejetée par FTD. Une nouvelle tentative après la synchronisation de la configuration doit résoudre ce problème. L'état actuel du cluster peut être suivi à l'aide de

		cette commande dans le périphérique géré CLISH : > show cluster info
asa_configuration_generation_errors	Le déploiement n'a pas pu générer la configuration du périphérique. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Après avoir examiné les journaux USMS mentionnés précédemment, vous pouvez voir quelle configuration est à l'origine de l'erreur. Il s'agit généralement de bogues dans lesquels les journaux peuvent être consultés via l'outil de bogue Cisco ou contactez le TAC Cisco pour un dépannage plus approfondi.
interface_out_of_date	Le déploiement a échoué car les interfaces sur le périphérique sont obsolètes. Enregistrez la configuration sur la page des interfaces et réessayez.	Cela se produit sur les modèles 4100 ou 9300 si l'interface n'est pas associée au périphérique pendant ou juste avant un déploiement. Vérifiez que l'interface est entièrement

		associée ou non associée avant de tenter le déploiement.
device_package_error	Le déploiement n'a pas pu générer de configuration pour le périphérique. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Cette erreur indique l'échec de la génération de la configuration du périphérique pour le périphérique. Contactez le TAC.
device_package_timeout	Échec du déploiement en raison du délai d'attente pendant la génération de la configuration. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Cela peut se produire si la latence existe entre les périphériques au-delà des plages normales. Contactez le TAC si ce problème persiste après la normalisation de la latence.
device_communication_errors	Échec du déploiement en raison d'un échec de communication du périphérique. Vérifiez la connectivité réseau et recommencez le déploiement.	Ce message est le secours pour tout problème de communication entre les périphériques. En raison de sa nature vague, il est écrit comme le secours pour indiquer qu'une erreur de

		connectivité inconnue s'est produite.
unable_to_initiate_deployment_dc	Échec du déploiement de la stratégie. Recommencez le déploiement.	Une autre tentative doit résoudre ce problème. Cela peut se produire lorsque le FMC ne peut pas démarrer le déploiement en raison d'un verrouillage temporaire de la base de données.
device_failure_timeout	Échec du déploiement sur le périphérique en raison du dépassement du délai d'attente. Recommencez le déploiement.	Ceci est lié au déploiement FTD. Les processus sur FTD attendent 30 minutes que la répartition soit terminée. Sinon, il expire. Dans ce cas, vérifiez la connectivité entre les périphériques et, si la connectivité est correcte, contactez le TAC.
device_failure_download_timeout	Échec du déploiement en raison du délai de téléchargement de la	Ceci est lié au déploiement FTD. Le FTD ne

	configuration vers le périphérique. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	peut pas télécharger tous les fichiers de configuration des périphériques pendant le déploiement en raison de problèmes de connectivité. Veuillez réessayer une fois la connectivité réseau vérifiée. Si cela a été vérifié, contactez le TAC.
device_failure_configuration	Échec du déploiement en raison d'une erreur de configuration. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Toute erreur dans la configuration générée par FMC pour le périphérique doit entraîner l'application de ce message d'erreur. Cela doit être analysé dans les journaux USMS pour vérifier quels problèmes sont détectés et tenter de les restaurer. Une fois réparé, cela nécessite

		généralement une intervention du TAC et la création d'un bogue si les journaux ne peuvent pas être associés à un défaut connu dans l'outil de recherche de bogues Cisco.
deployment_timeout_no_response_from_device	Échec du déploiement en raison du délai de communication avec le périphérique. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Ce délai d'attente se produit si le FMC n'a pas reçu de réponse d'un périphérique après ≤ 45 minutes. Il s'agit d'une erreur de communication. Vérifiez la communication et, si elle est vérifiée, contactez le TAC.
device_failure_change_master	Le déploiement vers le cluster a échoué car l'unité principale a changé. Recommencez le déploiement.	Pour un déploiement de configuration de cluster FTD, si le noeud principal bascule lorsque le déploiement est en cours sur le périphérique (post-

		notification), cette erreur est indiquée. Réessayez une fois que le noeud principal est stable. L'état actuel des membres du cluster peut être suivi à l'aide de cette commande dans le périphérique géré CLISH: **>** show cluster info
device_failure_unknown_master	Échec du déploiement vers le cluster en raison d'un échec d'identification de l'unité principale. Recommencez le déploiement.	FMC n'a pas pu déterminer le noeud principal actuel pendant le déploiement. En général, cela est dû aux possibilités suivantes : les problèmes de connectivité ou le principal actuel ne sont pas ajoutés au cluster sur FMC. Il doit être résolu après le rétablissement de la connectivité ou après l’ajout du

		principal actuel au cluster FMC et une nouvelle tentative. L'état actuel du cluster peut être suivi à l'aide de cette commande dans le périphérique géré CLISH : > show cluster info
cd_deploy_app_sync	Échec du déploiement car la synchronisation de la configuration du cluster est en cours. Recommencez le déploiement.	Cela peut se produire si le périphérique est dans App Sync. Une fois la synchronisation des applications terminée, réessayez le déploiement.
cd_existing_deployment	Échec du déploiement en raison d'un conflit avec le déploiement précédent simultané. Si le problème persiste après une nouvelle tentative, contactez le TAC Cisco.	Cela peut se produire si un déploiement est simultané d'un côté, mais pas de l'autre. Ces problèmes sont généralement dus à des problèmes de communication entre les périphériques. Si, après l'expiration du

		délai d'attente, vous ne parvenez toujours pas à effectuer le déploiement, contactez le TAC.

Informations connexes

- Dépannage des procédures de génération de fichiers Firepower
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.