Configurer la restauration sur SFTD lorsque SFMC n'est pas accessible

Table des matières

Introduction

Ce document décrit comment annuler une modification de déploiement du SFMC sécurisé qui affecte la connectivité au SFTD.

Conditions préalables

Exigences

L'utilisation de cette fonctionnalité est prise en charge à partir de la version 6.7 de Secure FirePOWER Threat Detection®.

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Secure Firewall Management Center (SFMC®)
- Configuration de Cisco Secure FirePOWER Threat Defense (SFTD)

Composants utilisés

- Secure Firewall Management Center pour VMware version 7.2.1
- Secure Firepower Threat Defense pour VMware version 7.2

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

Il existe des scénarios dans lesquels la communication avec SFMC, SFTD ou entre SFMC et SFTD est perdue lorsqu'une modification de déploiement affecte la connectivité réseau. Vous pouvez restaurer la configuration sur le SFTD à la dernière configuration déployée pour restaurer la connectivité de gestion.

Utilisez la commande configure policy rollback pour restaurer la configuration sur la défense contre les menaces à la dernière configuration déployée.

Remarque : la commande configure policy rollback a été introduite dans la version 6.7

Reportez-vous aux instructions :

- Seul le déploiement précédent est disponible localement sur la défense contre les menaces ; vous ne pouvez pas revenir à des déploiements précédents.
- La restauration est prise en charge pour la haute disponibilité à partir de Management Center 7.2.
- La restauration n'est pas prise en charge pour les déploiements en cluster.
- La restauration affecte uniquement les configurations que vous pouvez définir dans le centre de gestion. Par exemple, la restauration n'affecte aucune configuration locale liée à l'interface de gestion dédiée, que vous pouvez configurer uniquement à l'interface de ligne de commande de défense contre les menaces. Notez que si vous avez modifié les paramètres de l'interface de données après le dernier déploiement du centre de gestion à l'aide de la commande configure network management-data-interface, puis que vous utilisez la commande rollback, ces paramètres ne sont pas conservés ; ils sont restaurés aux derniers paramètres du centre de gestion déployés.
- Impossible de restaurer le mode UCAPL/CC.
- Les données de certificat SCEP hors bande mises à jour lors du déploiement précédent ne peuvent pas être restaurées.
- Pendant la restauration, les connexions peuvent être abandonnées car la configuration actuelle est effacée.

Configurer

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

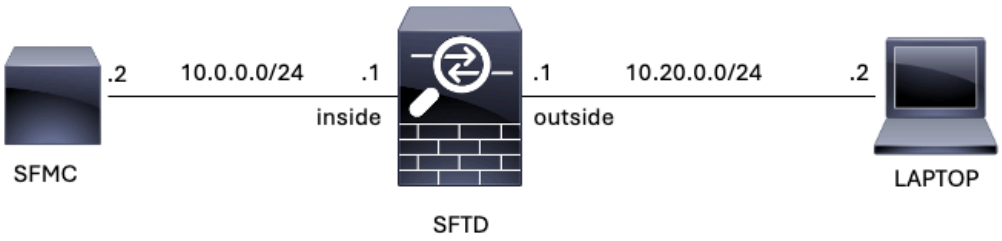


Image 1. Diagramme

Scénario

Dans cette configuration, SFTD est géré par le SFMC à l'aide de l'interface interne du pare-feu. Il existe une règle qui permet l'accessibilité de l'ordinateur portable au SFMC.

Procédure

Étape 1. La règle nommée FMC-Access a été désactivée sur le SFMC, après le déploiement, la communication de l'ordinateur portable vers le SFMC est bloquée.

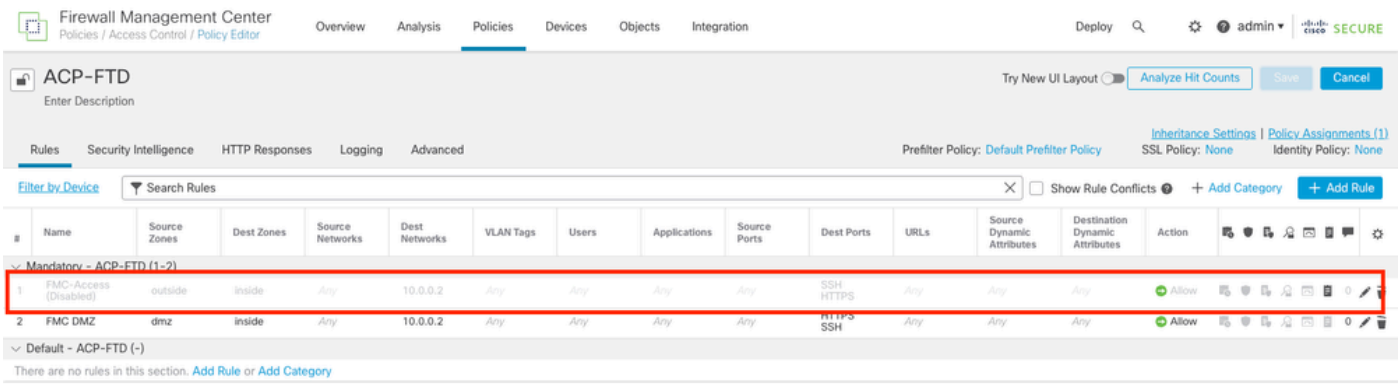


Image 2. La règle qui autorise l'accessibilité SFMC est désactivée

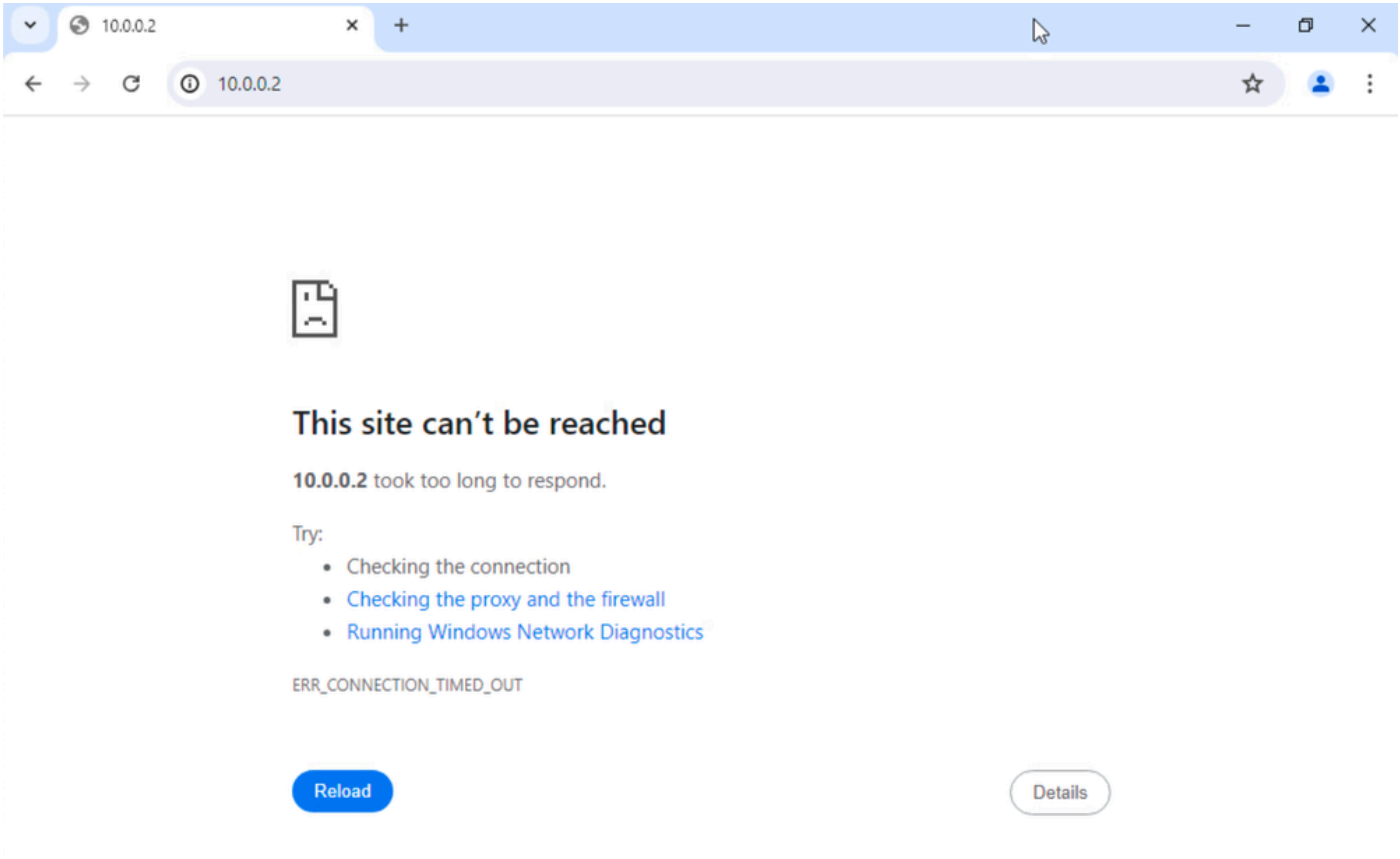


Image 3. Accessibilité SFMC de l'ordinateur portable inopérante

Étape 2. Connectez-vous au SFTD via SSH ou la console, puis utilisez la commande configure policy rollback.

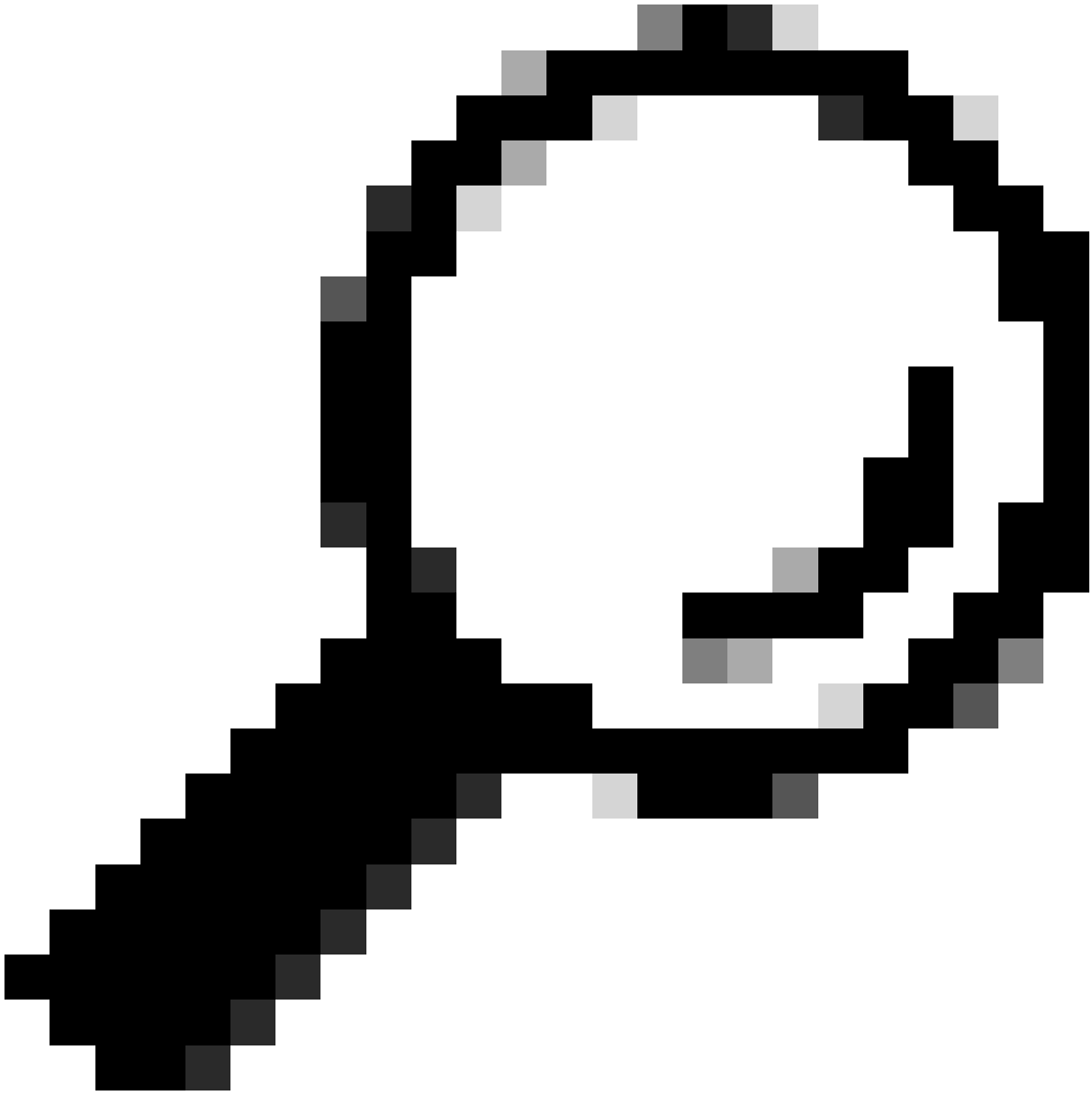
Remarque : si l'accès via SSH n'est pas possible, connectez-vous via Telnet.

```
<#root>

>

configure policy rollback


----------------------------------------------------------------------------------------------
[Warning] Perform a policy rollback if the FTD communicates with the FMC on a data interface, and it ha
and you want to perform a policy rollback for other purposes, then you should do the rollback on the FM

Checking Eligibility ....
============= DEVICE DETAILS =============
Device Version: 7.2.0
Device Type: FTD
Device Mode: Offbox
Device in HA: false
Device in Cluster: false
Device Upgrade InProgress: false
==========================================
Device is eligible for policy rollback

This command will rollback the policy to the last deployment done on Jul 15 20:38.
[Warning] The rollback operation will revert the convergence mode.
```

```
Do you want to continue (YES/NO)?
```

Étape 3. Écrivez le mot YES pour confirmer la restauration du dernier déploiement, puis attendez la fin du processus de restauration.

```
<#root>

Do you want to continue (YES/NO)?

YES


Starting rollback...
 Deployment of Platform Settings to device.              Status: success
 Preparing policy configuration on the device.           Status: success
 Applying updated policy configuration on the device.    Status: success
 Applying Lina File Configuration on the device.         Status: success
INFO: Security level for "diagnostic"set to 0 by default.
 Applying Lina Configuration on the device.             Status: success
 Commit Lina Configuration.                             Status: success
 Commit Lina File Configuration.                        Status: success
 Finalizing policy configuration on the device.         Status: success

===============================================

POLICY ROLLBACK STATUS: SUCCESS


===============================================
```



Conseil : en cas d'échec de la restauration, contactez le TAC Cisco

Étape 4. Après la restauration, confirmez l'accessibilité de SFMC. Le SFTD informe le SFMC que la restauration s'est terminée correctement. Dans le SFMC, l'écran de déploiement affiche une bannière indiquant que la configuration a été restaurée.

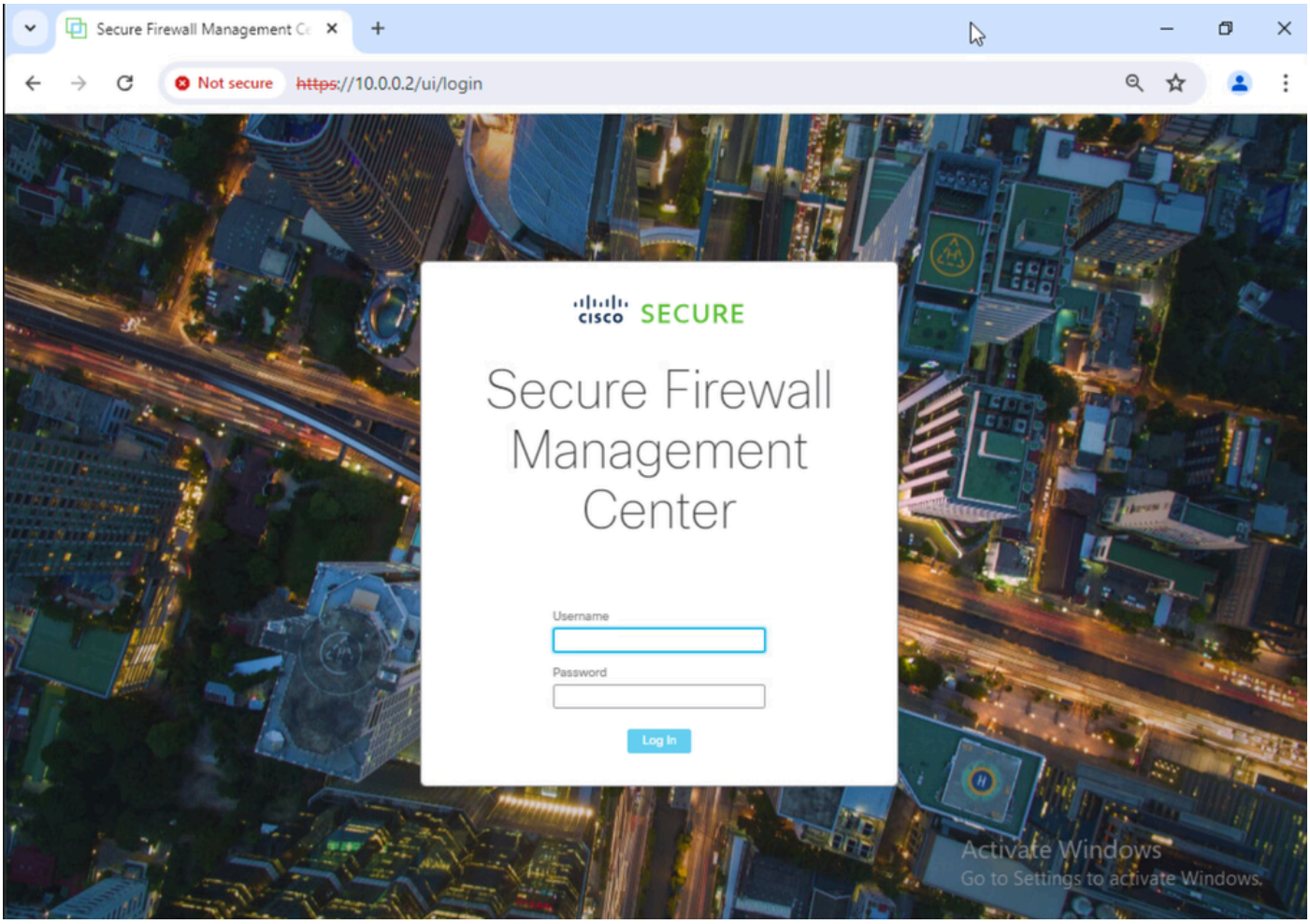


Image 4. Accessibilité SFMC à partir d'un ordinateur portable restauré

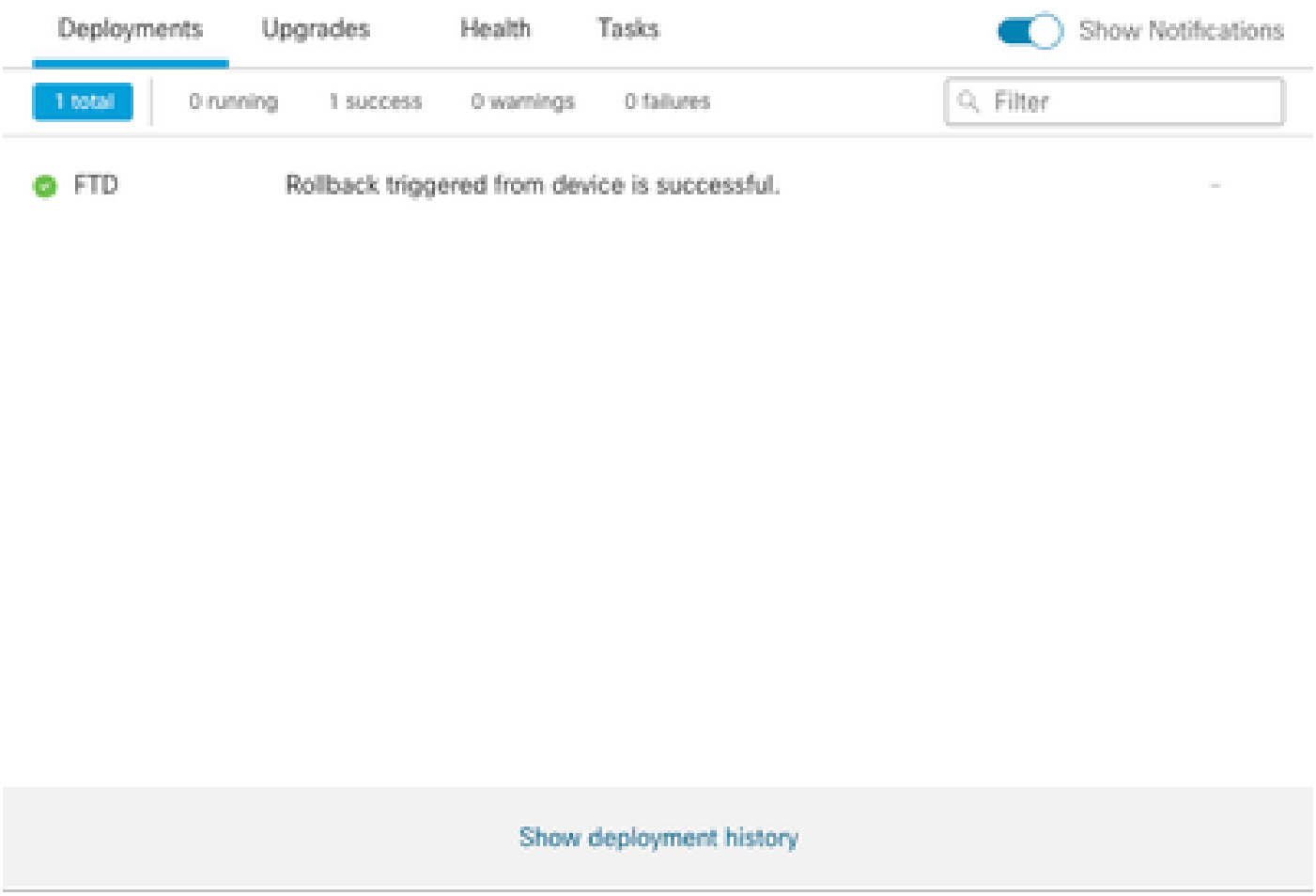


Image 5. Message SFMC confirmant la restauration depuis SFTD

Étape 5. Lorsque l'accès SFMC est restauré, résolvez le problème de configuration SFMC et redéployez.

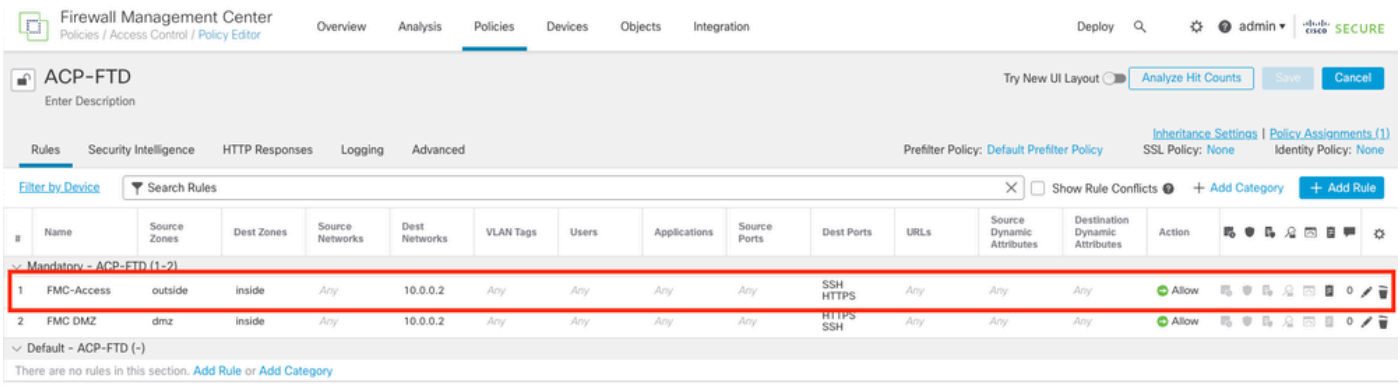


Image 6. Rétablir les modifications

Dépannage

En cas d'échec de la restauration, contactez le centre d'assistance technique Cisco. Pour tout autre problème au cours du processus, consultez l'article suivant :

· Restauration du déploiement

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.