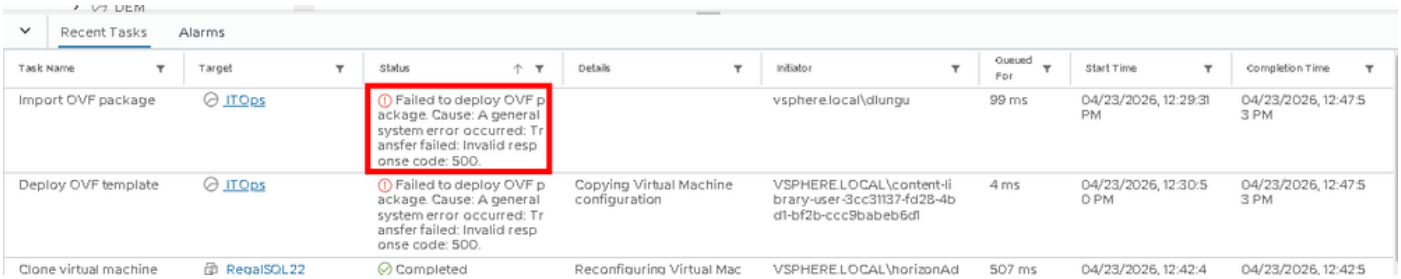
Échec du déploiement virtuel du pare-feu sécurisé en raison de Windows File Extractor

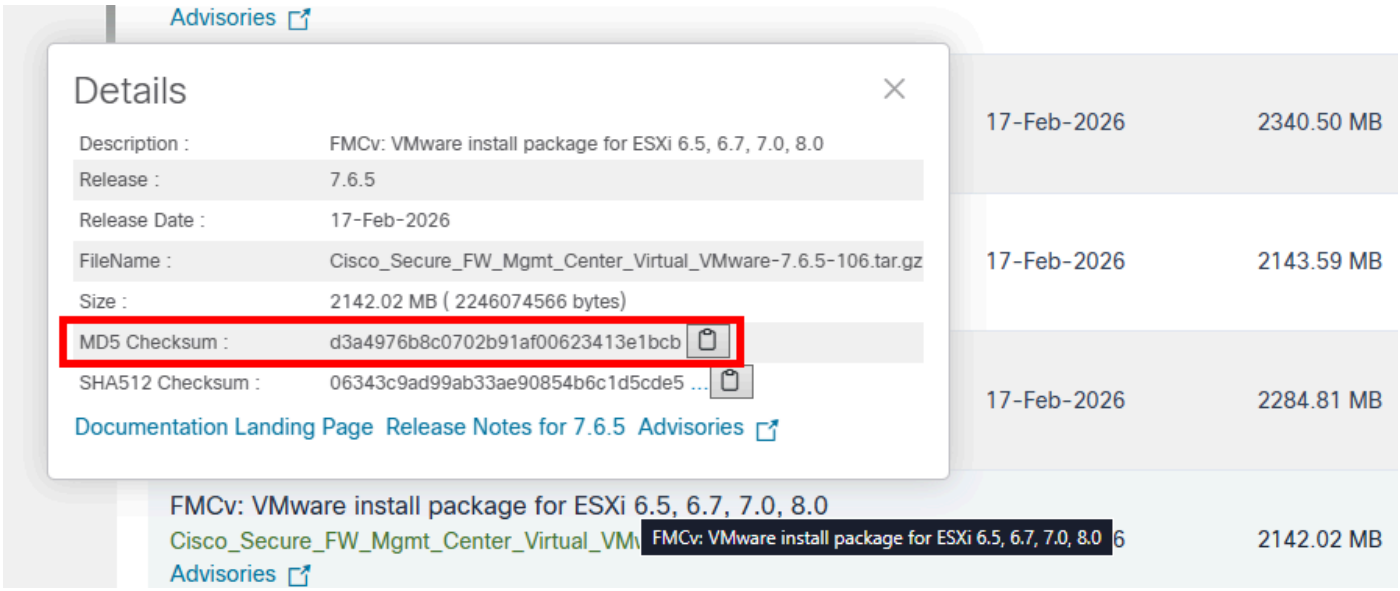
Table des matières

Problème

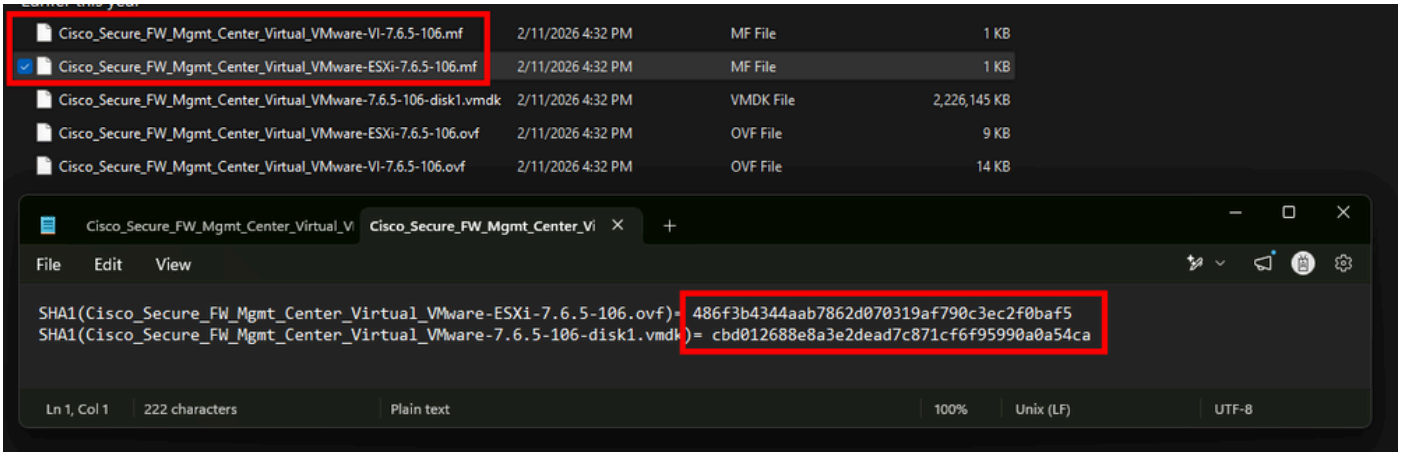
Le déploiement du périphérique virtuel Cisco Secure Firewall (ASAv, FTDv, FMCv ou FMCv300) dans VMware vCenter ou ESXi échoue avec cette erreur affichée pendant le déploiement de la machine virtuelle :



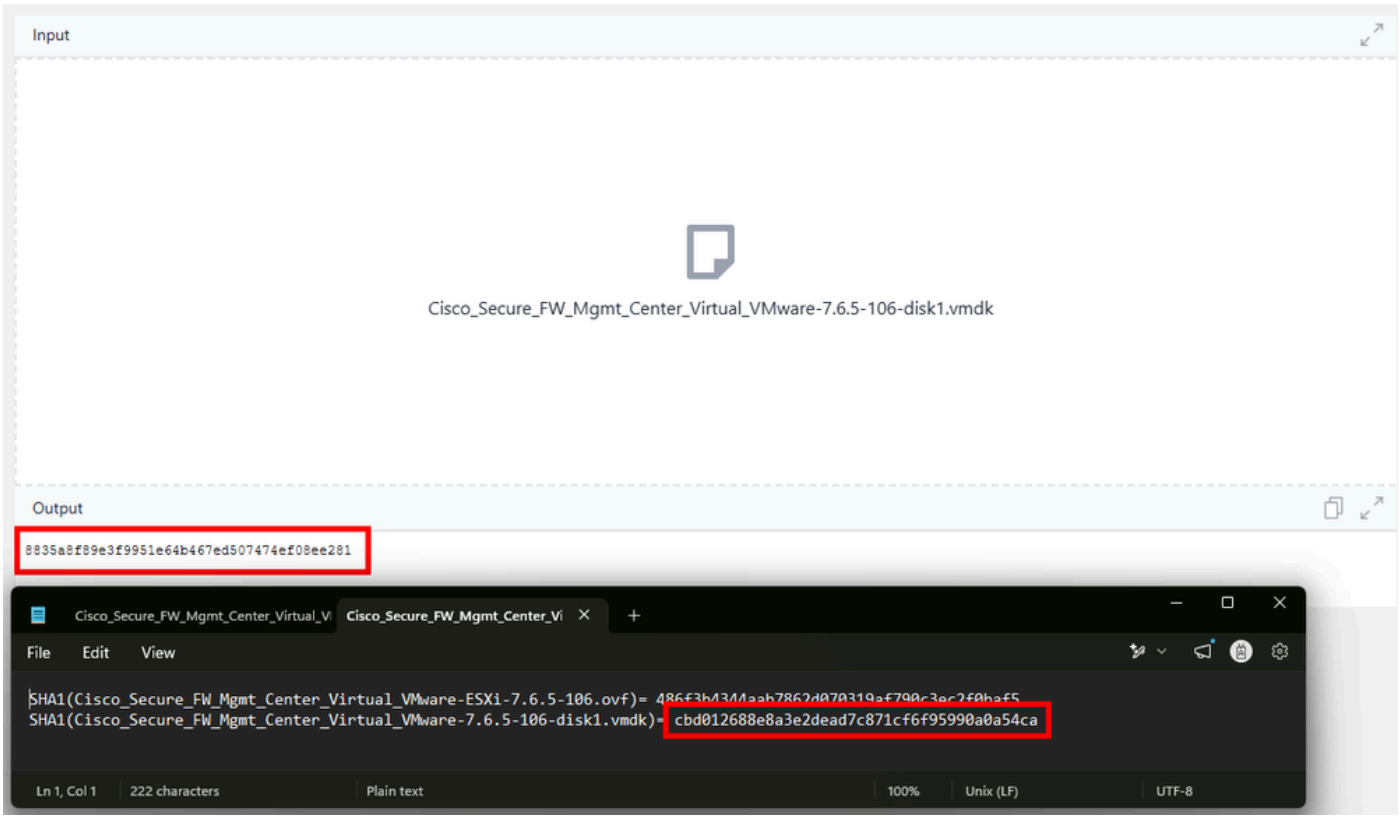
La somme de contrôle MD5 du package est vérifiée sur Cisco Software Central. Après avoir téléchargé le fichier à partir du site, le MD5 reste le même et il n'y a pas encore de preuve d'un fichier corrompu.



Lorsque le package est extrait, son contenu contient un fichier *.mf tel que « Cisco_Secure_FW_Mgmt_Center_Virtual_VMware-ESXi-7.6.5-106.mf ». Ce fichier contient les hachages SHA1 fournis par Cisco pour les fichiers image.



Lors de l'utilisation de l'option native de Windows « Extraire tout... » au lieu d'un extracteur de fichiers tiers, les images de ces fichiers sont corrompues et les hachages SHA1 de ces fichiers ne correspondent pas aux hachages de fichiers *.mf de Cisco.



Comme les hachages SHA1 ne correspondent pas, les fichiers ne sont plus valides pour une utilisation dans VMWare et génèrent l'erreur 500.

```
! Failed to deploy OVF package.
Cause: A general system error occurred:
Transfer failed: Invalid response code: 500.
```

Environnement

- VMware vCenter Server 9.0, VMware ESXi 8.0.3
- Packages d'installation de périphérique virtuel Cisco Secure Firewall utilisant des fichiers VMDK
- Système d'exploitation Windows utilisé pour l'extraction et le téléchargement des packages vers vCenter ou ESXi

Résolution

Solution de contournement:

1.- Confirmer les hachages MD5 correspondants avant et après le téléchargement du package VMWare compressé.

2.- Téléchargez et installez un extracteur de fichiers tiers tel que 7-Zip à partir d'un site officiel à utiliser à la place de l'outil d'extraction natif de Windows.

3.- Extrayez le package compressé à l'aide de l'extracteur de fichiers tiers et notez les hachages SHA1 pour chaque fichier des fichiers Cisco *.mf dans un bloc-notes.

4.- Générez le hachage SHA1 pour le fichier image requis (OVF/VMDK) avec n'importe quel outil de hachage en ligne et assurez-vous qu'il correspond à celui affiché dans les fichiers Cisco *.mf.

5.- Déployez le FMCv à l'aide du fichier OVF approprié en fonction de votre méthode de déploiement :

- Pour les déploiements vCenter : Utiliser les fichiers VI OVF et VMDK

- Pour les déploiements ESXi autonomes : Utiliser les fichiers ESXi OVF et VMDK

Motif

Le problème est causé par la corruption des fichiers lors de l'extraction lors de l'utilisation de l'extracteur de fichiers Windows natif pour décompresser le package d'installation .tar.gz. Bien que la somme de contrôle MD5 du package téléchargé soit valide, l'utilitaire d'extraction natif de Windows modifie l'intégrité des fichiers pendant l'extraction, ce qui entraîne la création de fichiers OVF/VMDK non valides qui entraînent le renvoi par VMware d'une erreur HTTP 500 générique pendant le déploiement. Ce comportement correspond à l'ID de bogue Cisco CSCwp3802, qui documente les problèmes d'extraction des images virtuelles du pare-feu sécurisé à l'aide des outils natifs de Windows. Ceci est résolu avec les images Firepower 10.0.0.

Autres informations utiles

- ID de bogue Cisco CSCwp33802 - [DOC] Échec du déploiement de la machine virtuelle : échec de postNFCData : [STREAMVMDK] CmpSize non valide lu : 3225899676
- Guide de démarrage virtuel de Cisco Secure Firewall Management Center
- Assistance technique de Cisco et téléchargements
- Extracteur de fichiers 7-zip
- Outil de somme de contrôle des fichiers Github

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.