

Le service de base de données de l'agent utilisateur Cisco Firepower ne redémarre pas après un arrêt

Contenu

[Introduction](#)

[Symptômes](#)

[Solution](#)

[Références](#)

Introduction

Un agent utilisateur Cisco peut surveiller le serveur Microsoft Active Directory (AD) et signaler les activités de connexion et de déconnexion authentifiées par un serveur LDAP. Un Centre de gestion Firepower (FMC) intègre ces activités aux événements de sécurité qu'il collecte à partir d'un périphérique géré Firepower. Ce document fournit une solution à un problème lorsque l'Agent utilisateur ne démarre pas après avoir arrêté son service.

Symptômes

Vous pouvez utiliser la solution de ce document si vous remarquez les symptômes suivants avec votre service Agent utilisateur :

- L'interface Agent utilisateur affiche le service comme Non en cours d'exécution.
- La console de service Windows, services.msc, affiche l'état de Cisco User Agent comme vide et ne démarre pas le service.
- Le journal des événements Windows affiche une erreur similaire à « Échec de la relation d'approbation entre le domaine principal et le domaine approuvé »
- Un fichier UserEncryptionBytes.bin est créé à l'adresse C:\ avec une taille zéro octet.
- Le mode de débogage d'un client Agent utilisateur affiche les messages d'erreur suivants dans l'onglet Journal de l'Agent utilisateur :

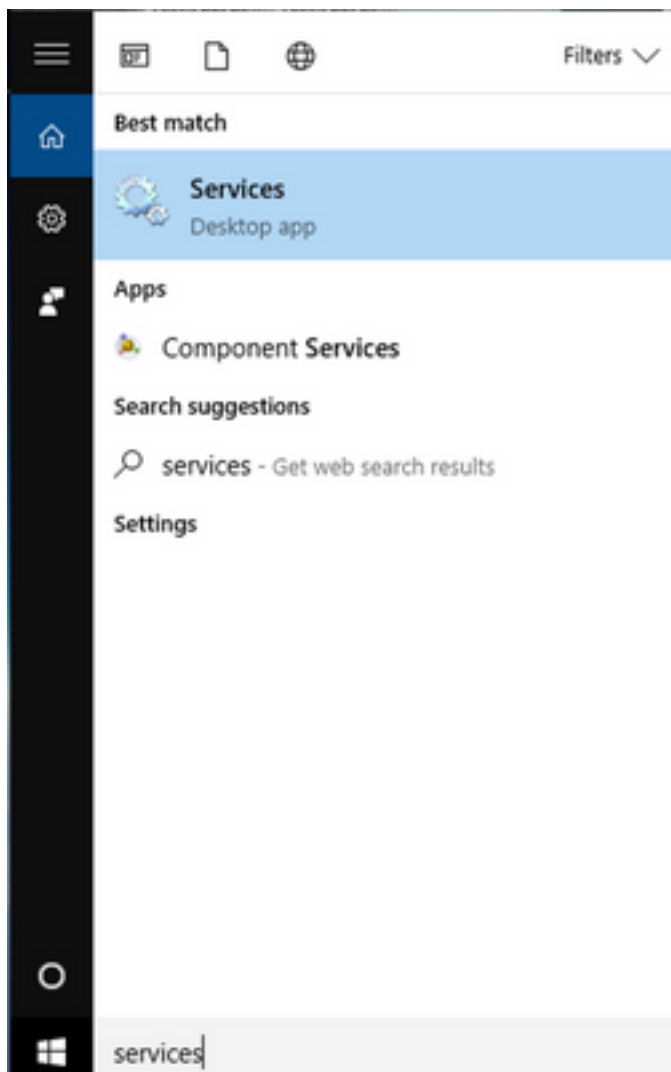
```
,"debug", "[0102] - An error occurred while fetching encryption bytes from  
'C:\UserAgentEncryptionBytes.bin':  
The trust relationship between the primary domain and the trusted domain failed.."
```

```
,"error", "[0102] - An error occurred while fetching encryption bytes from  
'C:\UserAgentEncryptionBytes.bin':  
Specified key is not a valid size for this algorithm.."
```

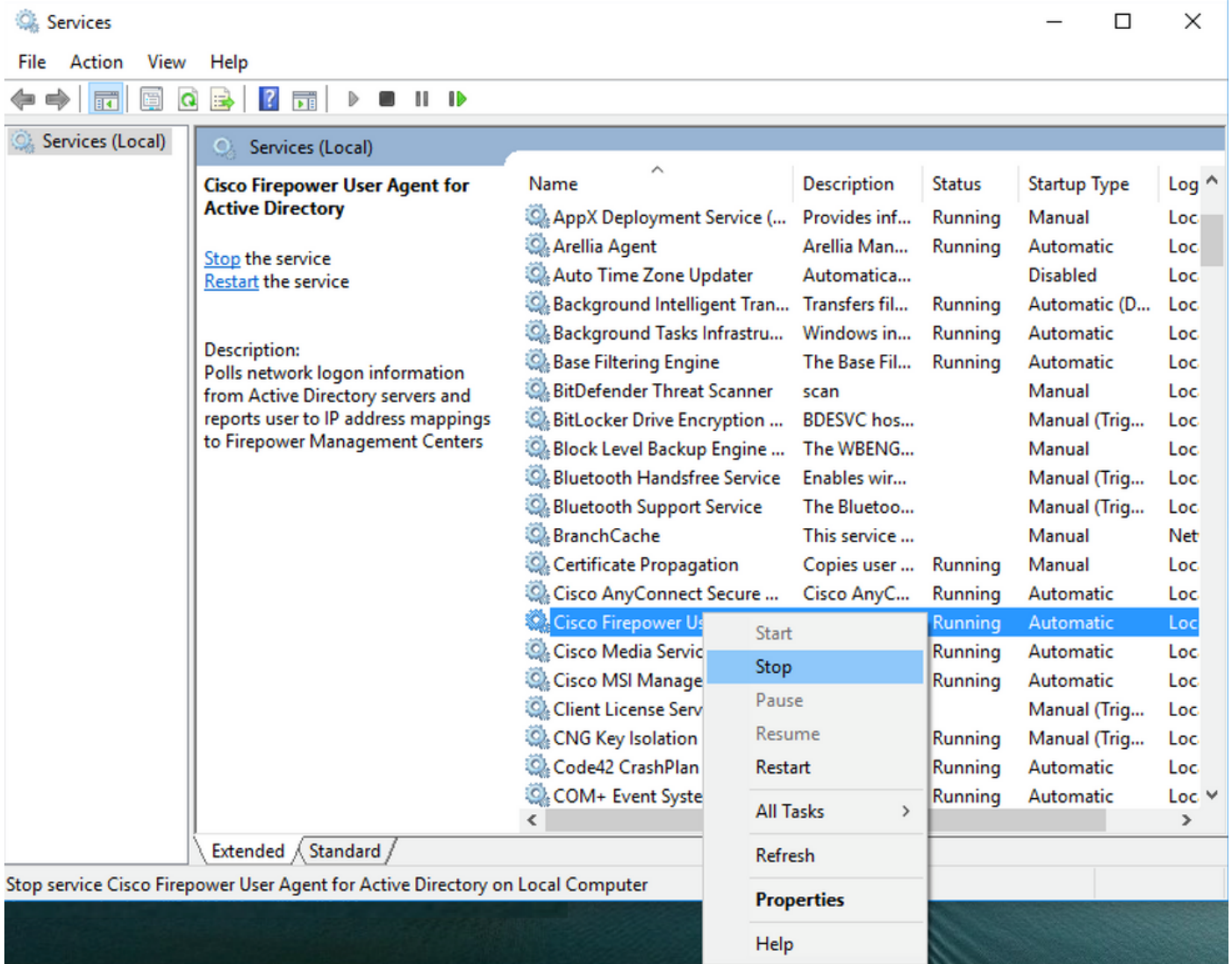
```
,"error", "[0002] - Error connecting to 10.85.3.122: System.UnauthorizedAccessException:  
Access is denied. (Exception from HRESULT: 0x80070005 (E_ACCESSDENIED))
```

Solution

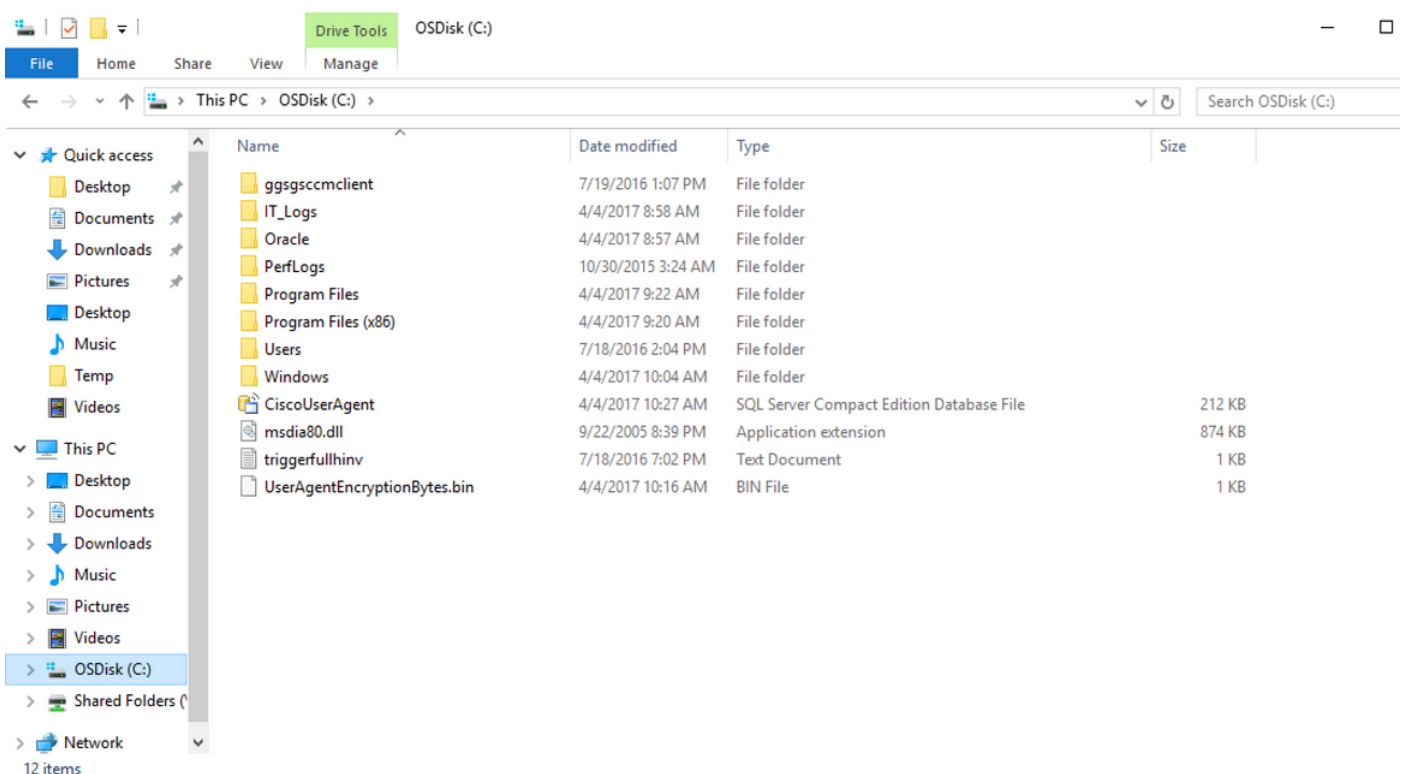
Étape 1 : Exécutez Microsoft Windows Services Console, services.msc. Il vous permet de désactiver ou d'activer un service Windows.



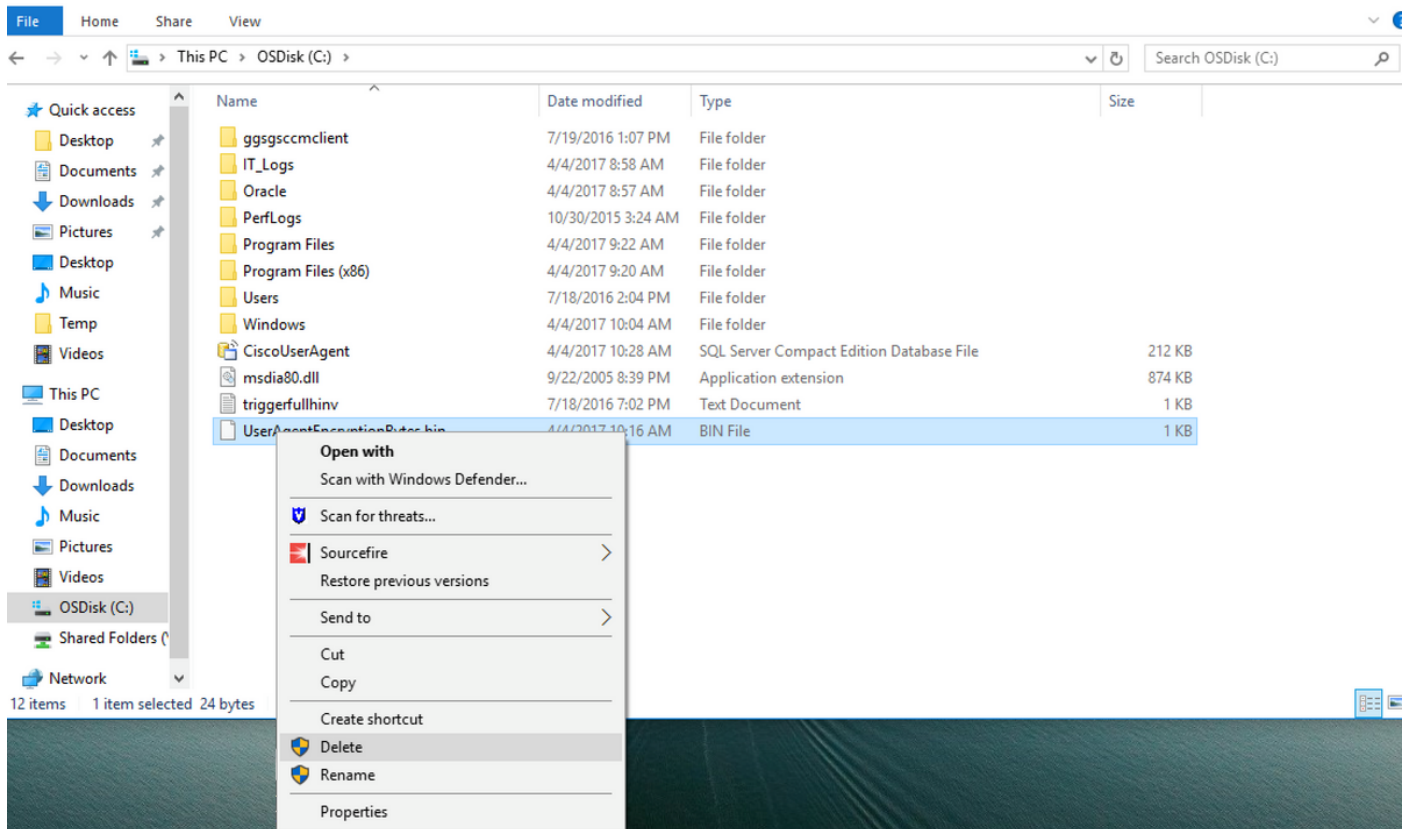
Étape 2 : Cliquez avec le bouton droit sur le service Cisco User Agent et sélectionnez **Arrêter** pour arrêter le service.



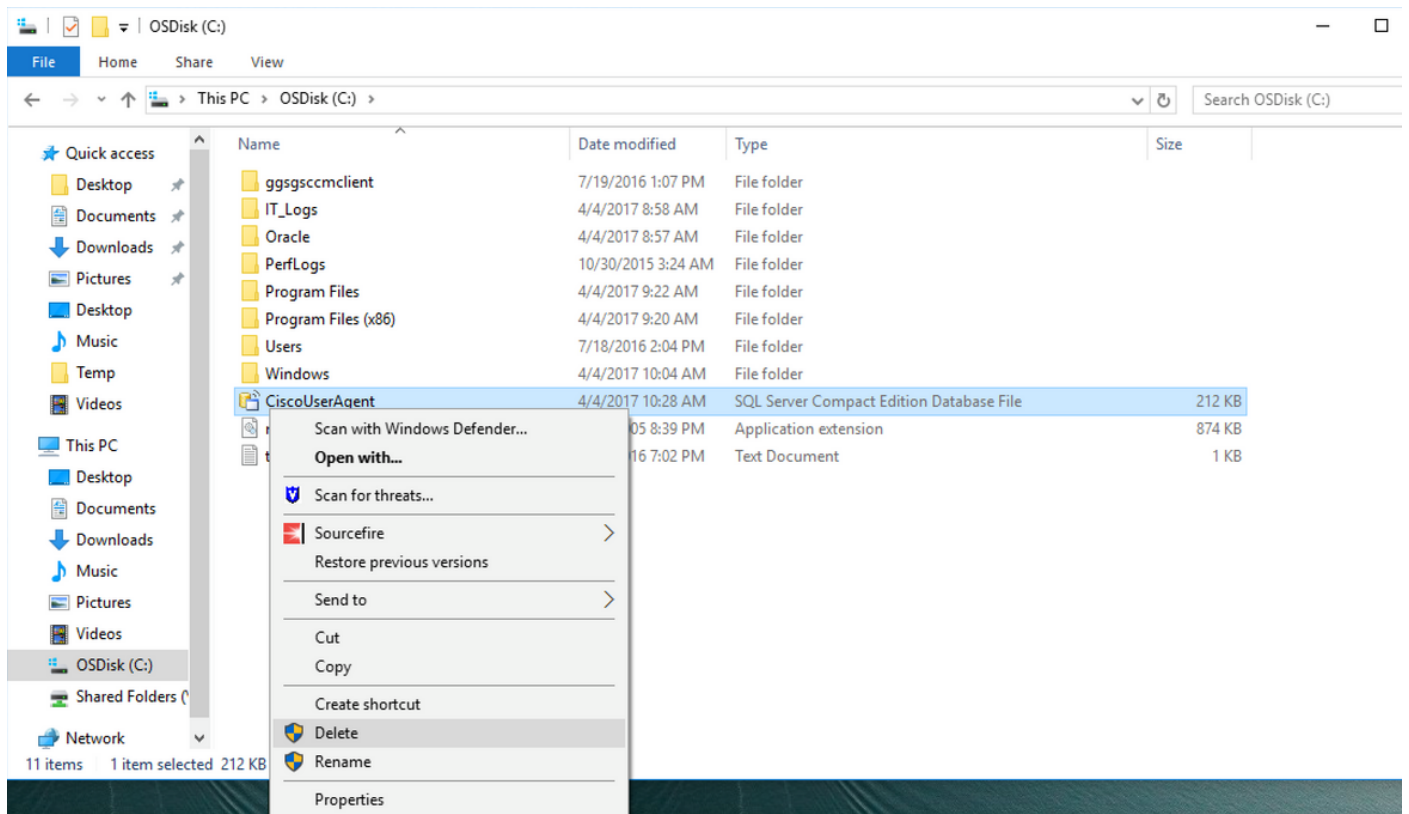
Étape 3 : Accédez à C : lecteur.



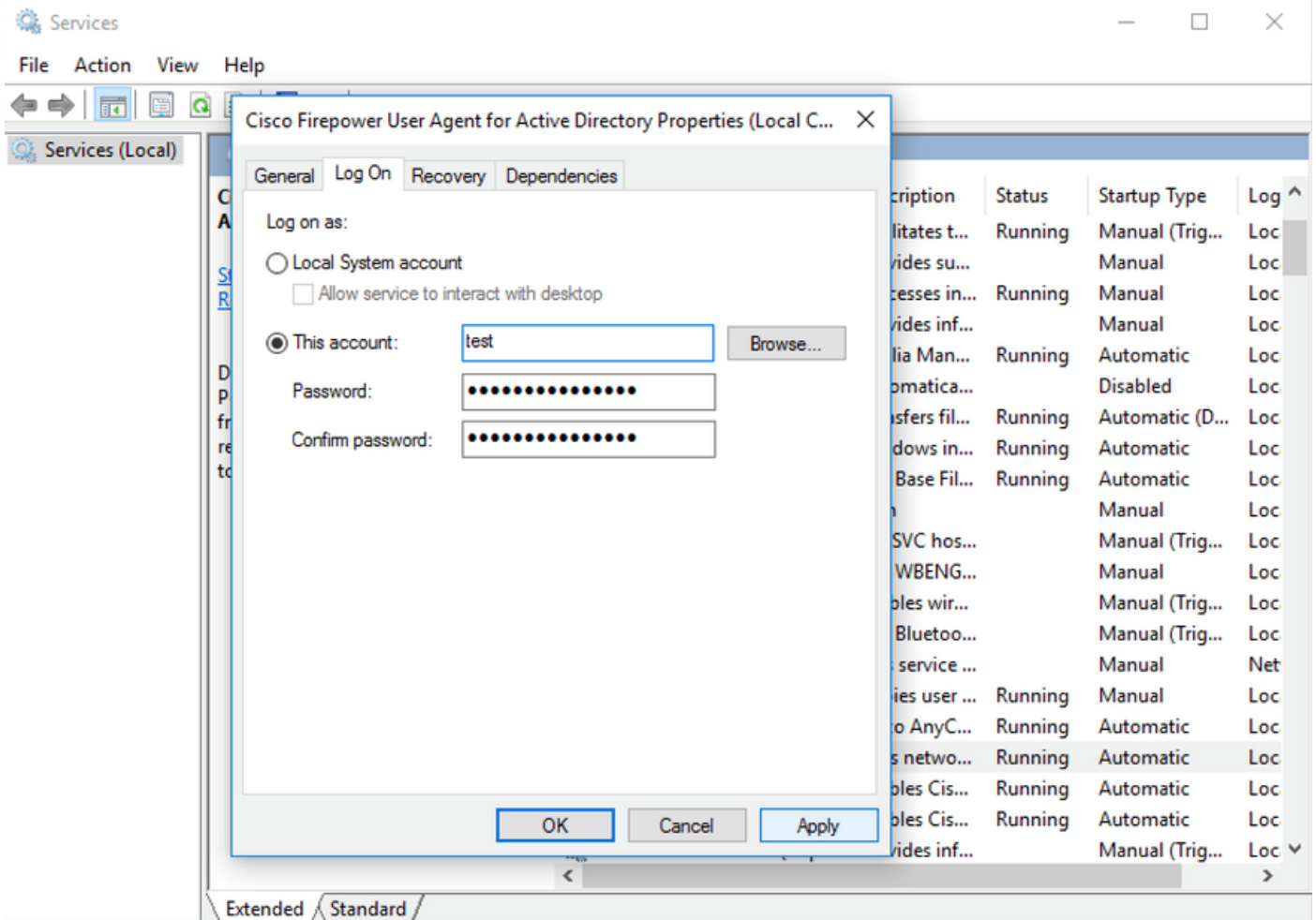
Étape 4 : Supprimez ce fichier UserAgentEncryptionBytes.bin.



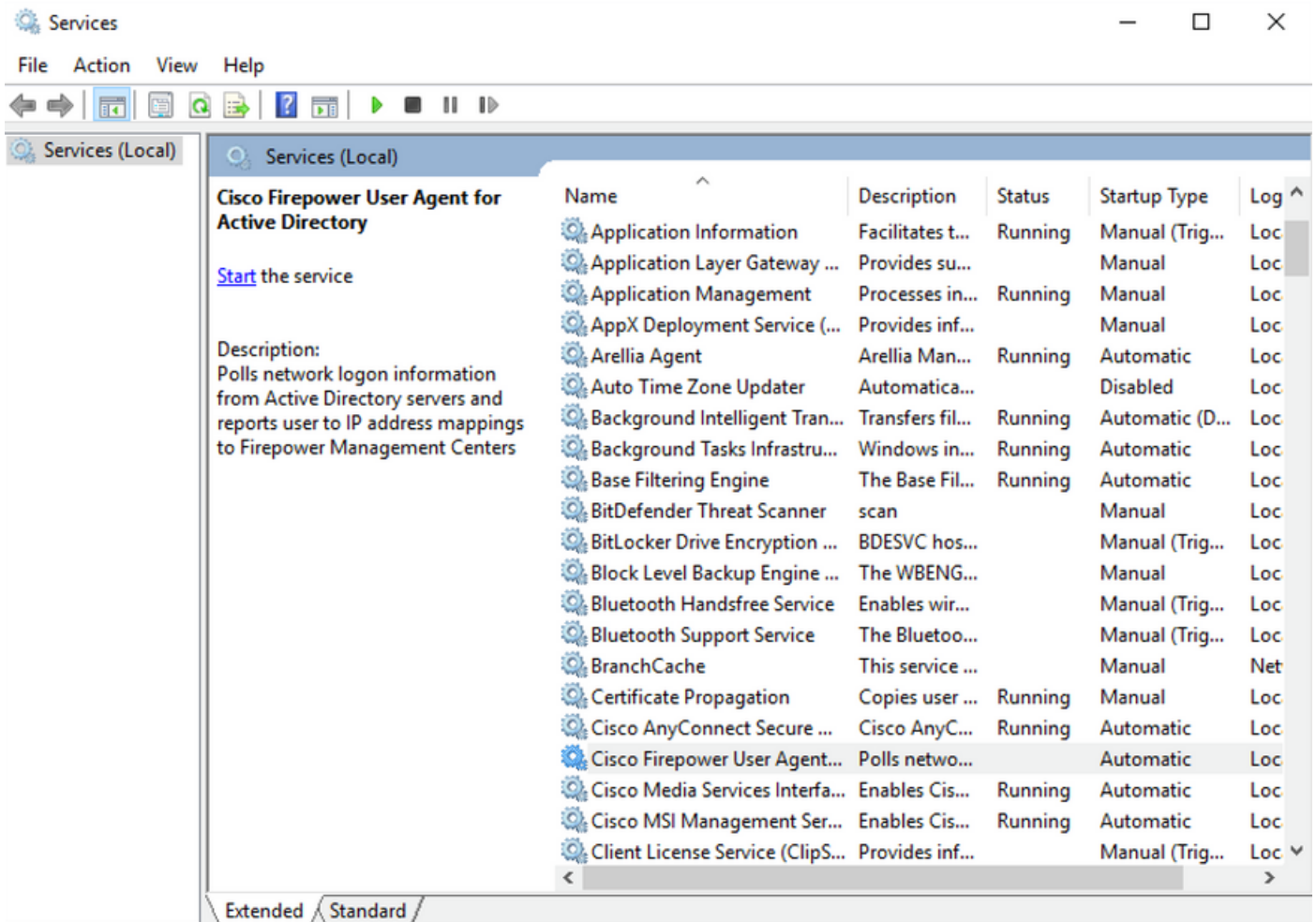
Étape 5 : Supprimez le fichier CiscoUserAgent, qui est un fichier de base de données SQL Server Compact Edition.



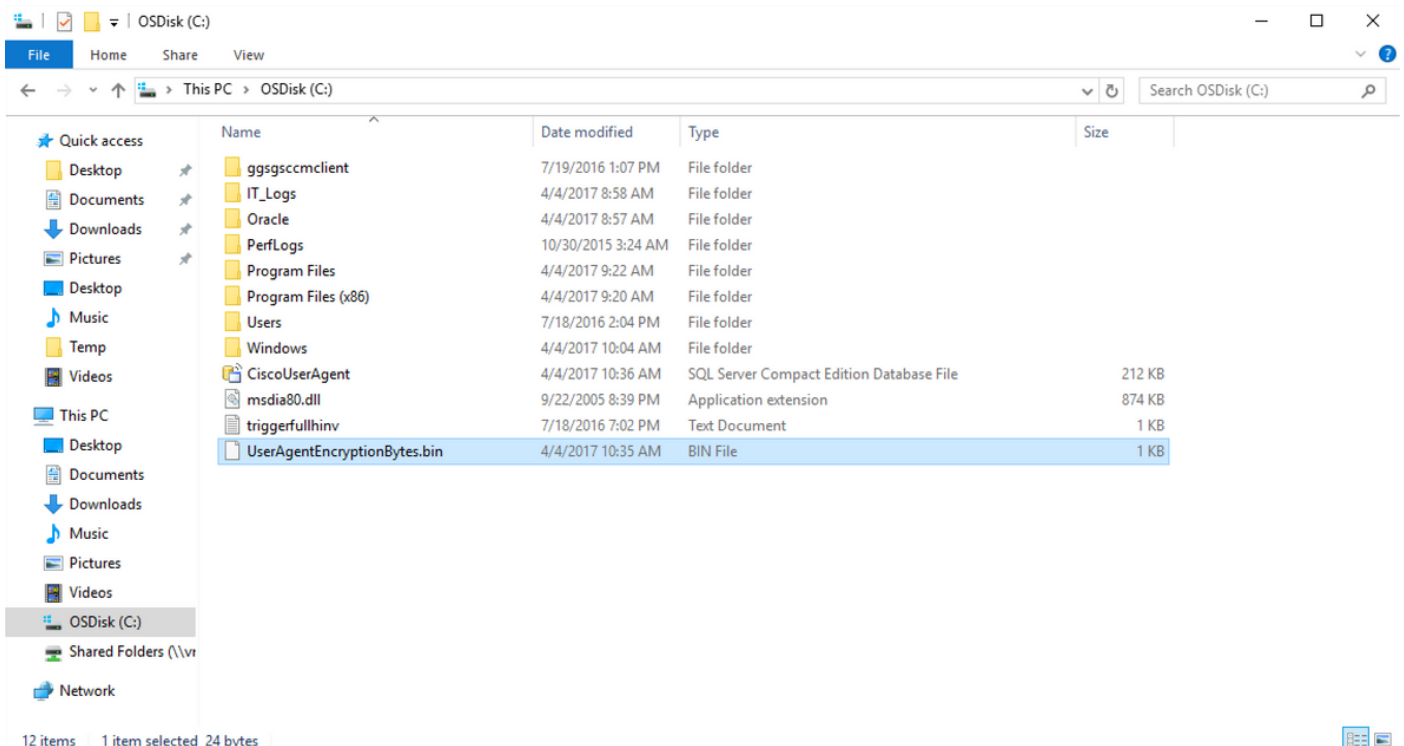
Étape 6 : Revenir à services.msc. Cliquez avec le bouton droit de la souris sur le service Cisco User Agent, sélectionnez **Propriétés**, puis **Ouvrir une session**, puis configurez un utilisateur en tant que connexion utilisateur AD. Cliquez sur **Apply** lorsque vous avez terminé.



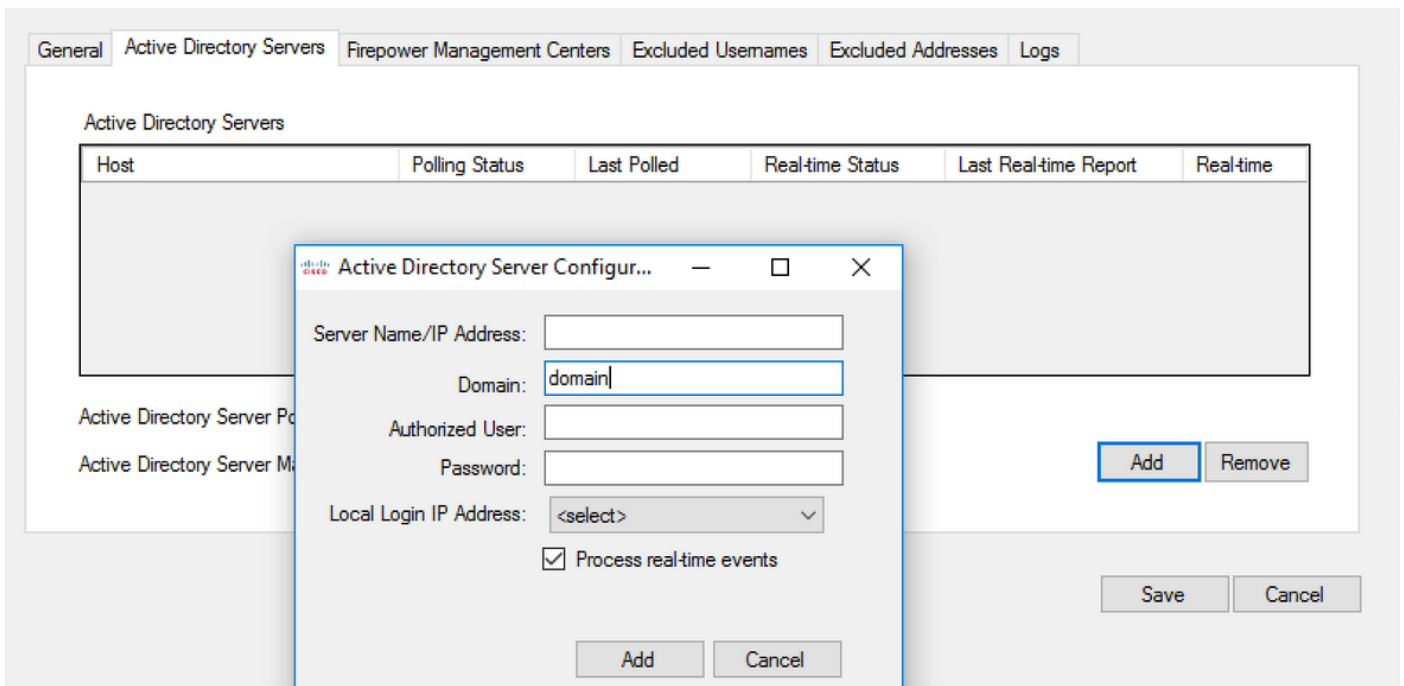
Étape 7 : Sur services.msc, cliquez sur **Démarrer** pour le service **Cisco Firepower User Agent pour Active Directory**.



Étape 8 : Vérifiez la taille du fichier UserAgentEncryptionBytes.bin. Elle ne doit pas être de 0 Ko.



Étape 9 : Ajoutez les contrôleurs de domaine et Firepower Management Center au client Agent utilisateur. Veillez à ajouter les contrôleurs de domaine/hôte local avant d'ajouter Firepower Management Center à l'agent utilisateur.



Références

- [Guide de configuration de Firepower User Agent, 2.3](#)
- [L'agent utilisateur cesse de dériver s'il ne peut pas traduire le compte de service en SecurityIdentifier \(CSCuw20184\)](#)
- [Octroi d'une autorisation minimale à un compte d'utilisateur Active Directory utilisé par l'agent d'utilisateur Sourcefire](#)