

Démarrage du processus Windows avant la solution AMP Connector - AMP for Endpoints

Contenu

[Introduction](#)

[Conditions requises](#)

[Components Used](#)

[Limites](#)

[Informations générales](#)

[Dépannage](#)

[Étapes pour retarder un service Windows](#)

[Retarder le processus avec la ligne de commande](#)

Introduction

Ce document décrit les étapes à suivre pour dépanner dans Advanced Malware Protection (AMP) for Endpoints lorsqu'un processus Windows démarre avant System Process Protection (SPP).

Contribution de Nancy Perez et Uriel Torres, ingénieurs du TAC Cisco.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Windows OS
- Moteurs du connecteur AMP

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Périphérique Windows 10
- Connecteur AMP version 6.2.9

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.

Limites

Il s'agit d'un bogue qui affecte le moteur System Process Protection lorsqu'un processus démarre avant le connecteur AMP [CSCvo90440](#).

Informations générales

Le moteur AMP for Endpoints System Process Protection protège les processus système Windows critiques contre les attaques par injection de mémoire par d'autres processus.

Afin d'activer SPP, sur la console AMP, naviguez jusqu'à **Management > Politiques > cliquez sur edit dans la stratégie que vous voulez modifier > Modes and Engines > System Process Protection**, ici vous trouverez trois options :

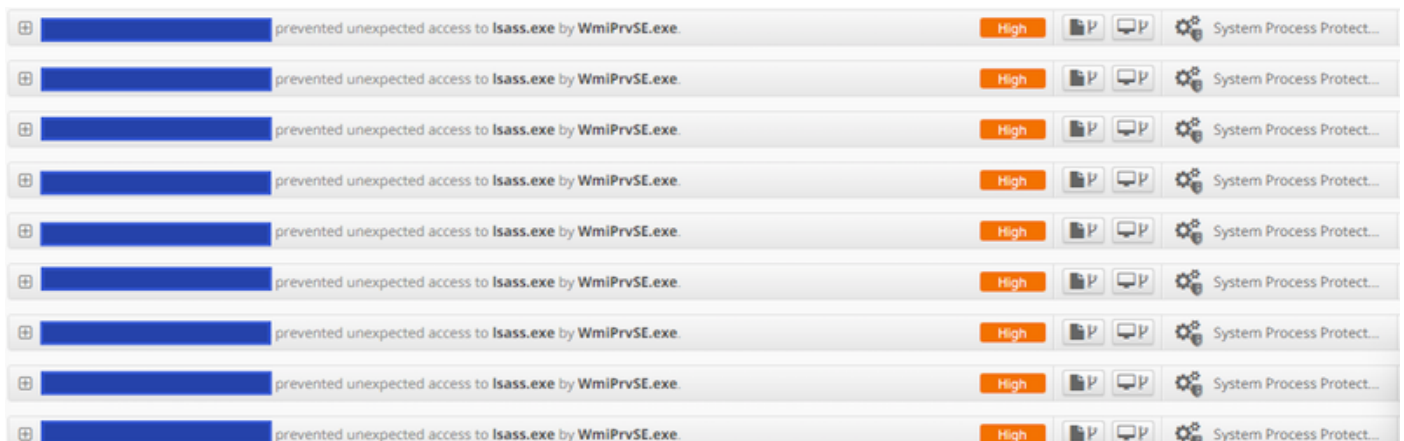
- Protéger : Bloque les attaques sur les processus système Windows critiques
- Audit : avertir les attaques sur les processus système Windows critiques
- Désactivé: le moteur n'est pas actif sur ce mode

Processus système protégés

Le moteur System Process Protection protège les processus suivants :

- Sous-système du Gestionnaire de session (**smss.exe**)
- Sous-système d'exécution client/serveur (**csrss.exe**)
- Sous-système de l'autorité de sécurité locale (**lsass.exe**)
- Application de connexion Windows (**winlogon.exe**)
- Application de démarrage Windows (**wininit.exe**)

Lorsqu'un service Windows démarre avant le connecteur AMP (dans les versions inférieures à la version 7.0.5), les exclusions de processus système ne sont pas respectées et même si un processus est exclu, le moteur SPP arrête le processus et un événement est créé dans la console AMP, comme l'illustre l'image.



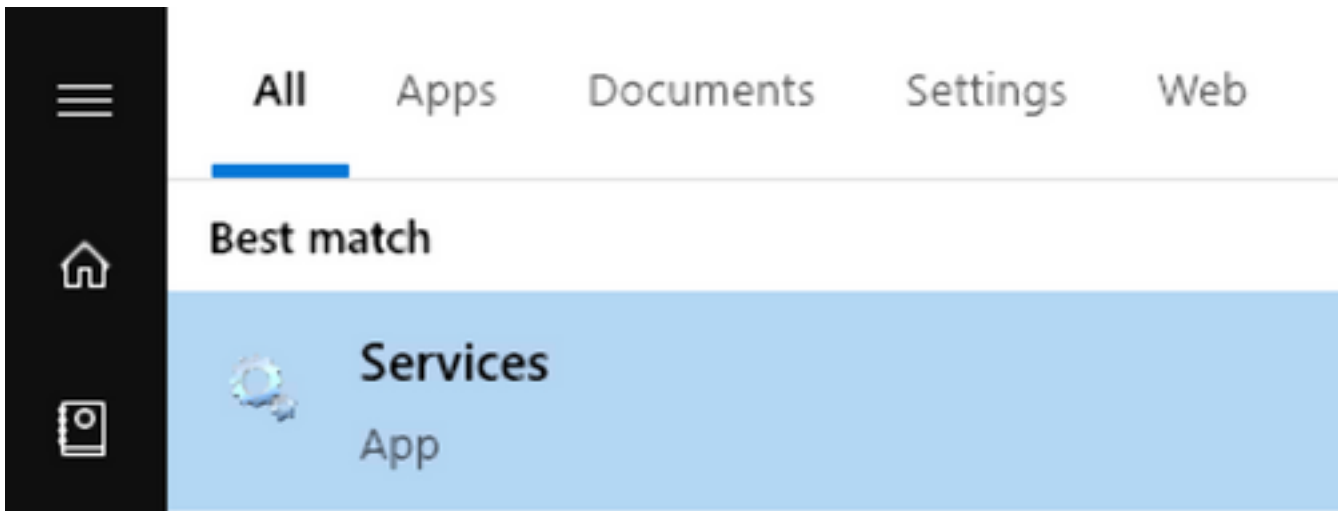
Dépannage

La solution de contournement de ce bogue est de retarder le service Windows qui commence avant le service AMP.

L'application Rosetta Stone est un exemple dans ce document. Cette application est détectée par SPP car elle touche le processus lsass.exe à des fins d'authentification.

Étapes pour retarder un service Windows

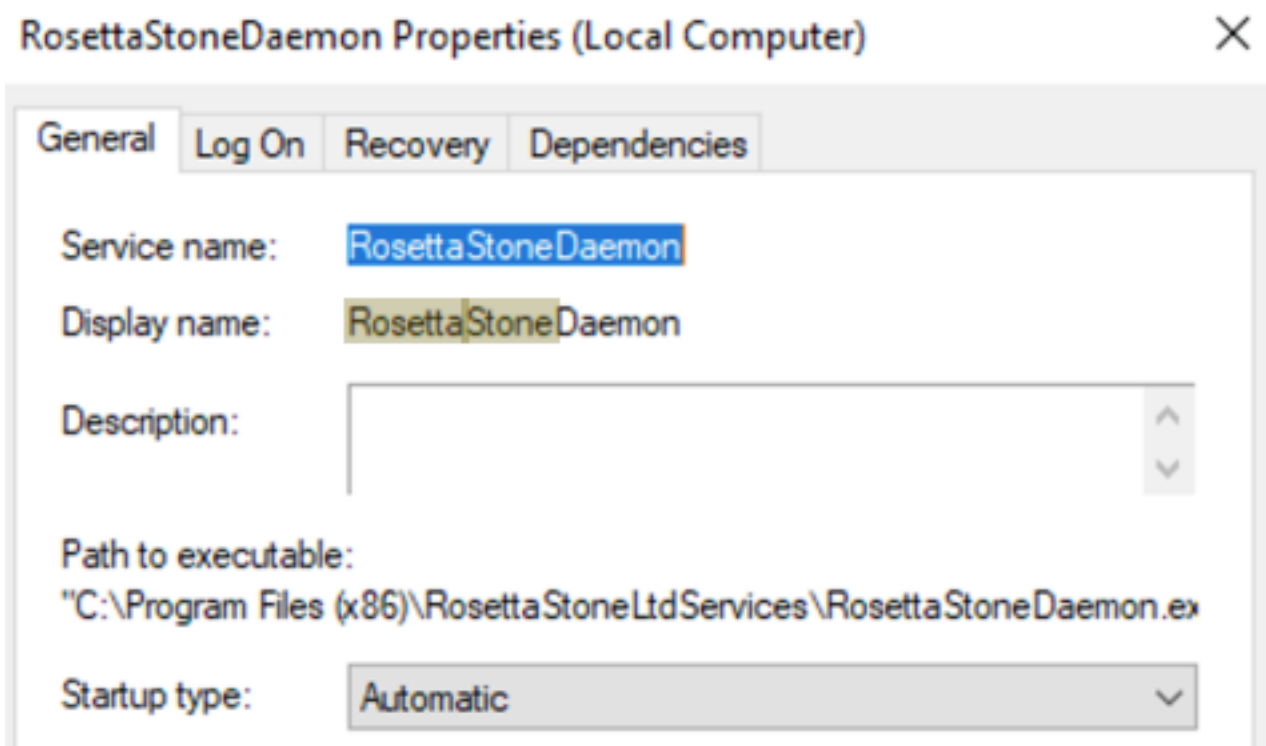
Étape 1. Ouvrez services.msc, comme illustré dans l'image.



Étape 2. Trouvez le service Rosetta Stone.

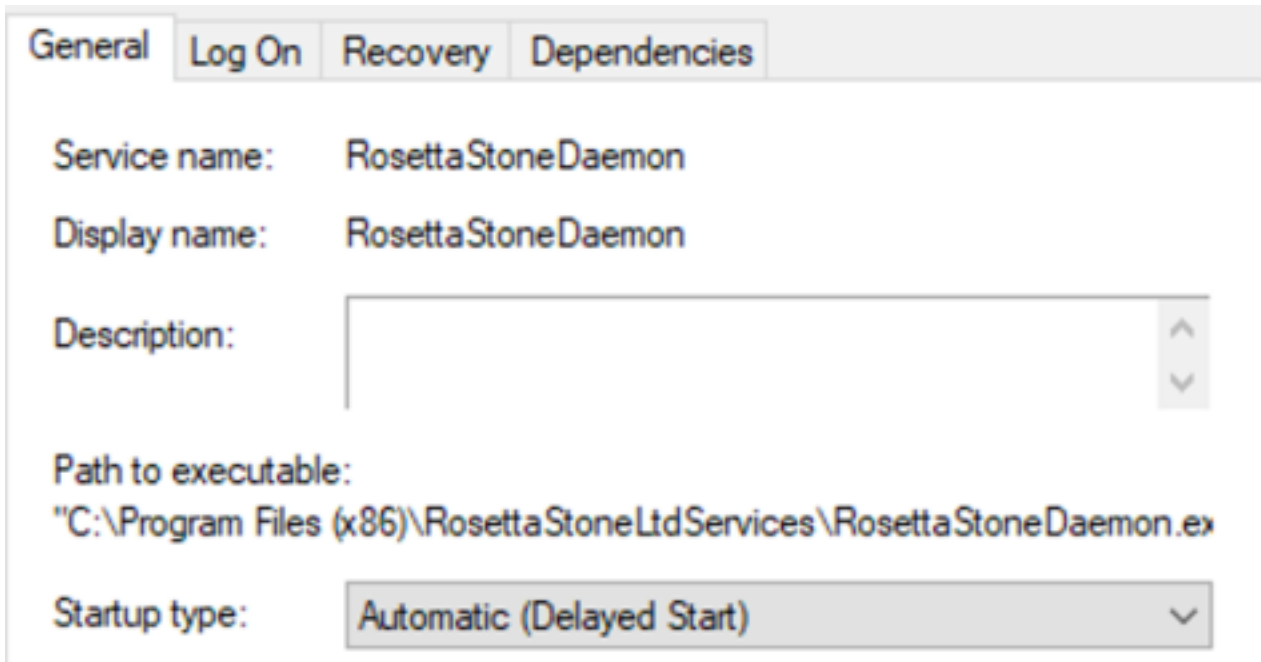
Stop the service	Cisco Security Connector monitoring Service 0.3.3	Cisco Secur...	Running	Automatic
Pause the service	RosettaStoneDaemon		Running	Automatic
Restart the service	VMware Tools	Provides su...	Running	Automatic
	VMware Alias Manager and Ticket Service	Alias Mana...	Running	Automatic

Étape 3. Cliquez avec le bouton droit sur RosettaStoneDaemon et cliquez sur Propriétés.



Le type de démarrage est configuré comme Automatique par défaut, ce qui signifie que RosettaStoneDaemon démarre automatiquement dans le processus de démarrage.

Étape 4. Cliquez sur le menu déroulant et sélectionnez Automatique (Début différé).



Cette configuration empêche le démarrage du service RosettaStoneDaemon avant le connecteur AMP.

Étape 5. Cliquez sur Apply.



Retarder le processus avec la ligne de commande

Pour PowerShell/CMD, les commandes suivantes peuvent être utilisées.

Étape 1. Exécutez PowerShell/CMD en tant qu'administrateur.

Étape 2. Exécutez cette commande :

```
sc.exe config RosettaStoneDaemon start= delayed-auto
```

Note : Rosetta Stone = RosettaStoneDaemon.

Administrator: Windows PowerShell

```
Windows PowerShell  
Copyright (C) 2016 Microsoft Corporation. All rights reserved.  
PS C:\Windows\system32> sc.exe config RosettaStoneDaemon start= delayed-auto  
[SC] ChangeServiceConfig SUCCESS
```

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.15063]  
(c) 2017 Microsoft Corporation. All rights reserved.  
C:\Windows\system32>sc.exe config RosettaStoneDaemon start= delayed-auto  
[SC] ChangeServiceConfig SUCCESS
```

Dans cette section, vous pouvez remplacer le nom d'application de RosettaStoneDaemon pour le processus que vous voulez retarder.

Attention : Connector version 7.0.5 et ultérieures implémentent déjà une solution pour ce bogue. Cette solution de contournement est conçue pour les versions de connecteur inférieures à la version 7.0.5.