

# AMPコネクタの回避策の前にWindowsプロセスが開始される – AMP for Endpoints

## 内容

[概要](#)

[要件](#)

[使用するコンポーネント](#)

[制限](#)

[背景説明](#)

[トラブルシューティング](#)

[Windowsサービスの遅延手順](#)

[コマンドラインでプロセスを遅延させる](#)

## 概要

このドキュメントでは、WindowsプロセスがSystem Process Protection(SPP)の前に開始される場合に、Advanced Malware Protection(AMP)for Endpointsでトラブルシューティングを行う手順について説明します。

著者 : Cisco TACエンジニア、Nancy PerezおよびUriel Torres

## 要件

次の項目に関する知識があることが推奨されます。

- Windows OS
- AMPコネクタのエンジン

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Windows 10デバイス
- AMPコネクタ6.2.9バージョン

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 ( デフォルト ) 設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 制限

これは、AMPコネクタ [CSCvo90440](#) より前にプロセスが開始される場合に、[System Process Protection\(PTF\)エンジンに影響を与えるバグ](#) である。

## 背景説明

AMP for Endpoints System Process Protectionエンジンは、重要なWindowsシステムプロセスを他のプロセスによるメモリインジェクション攻撃から保護します。

SPPを有効にするには、AMPコンソールで[Management] > [Policies] > [edit]に移動し、変更するポリシーで[Modes and Engines] > [System Process Protection]をクリックします。次の3つのオプションがあります。

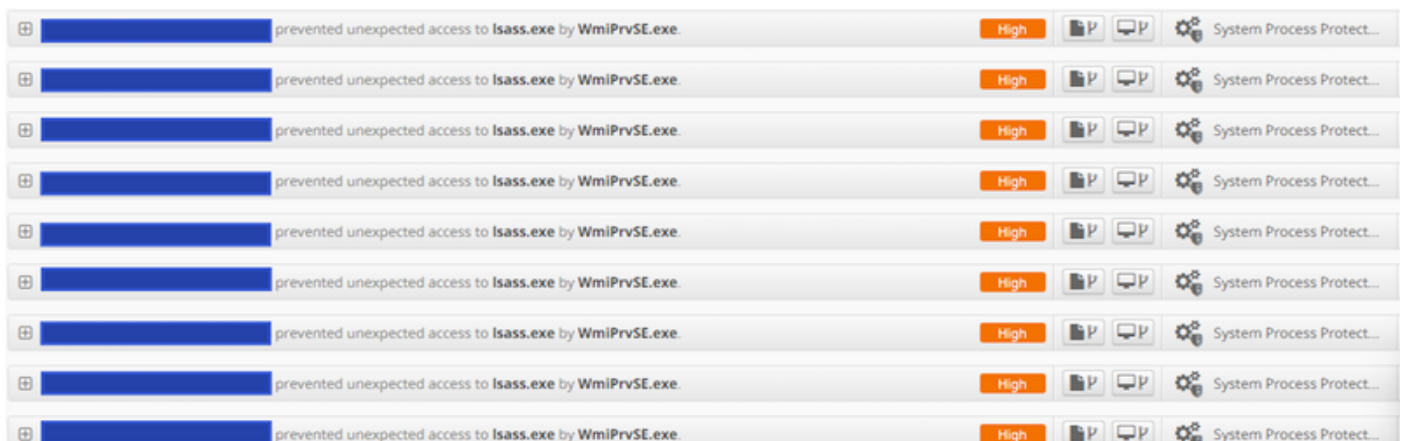
- [Protect]：重要なWindowsシステムプロセスに対する攻撃をブロックする
- 監査：重要なWindowsシステムプロセスに対する攻撃を通知する
- オフ：このモードではエンジンがアクティブではありません

### 保護されたシステムプロセス

システムプロセス保護エンジンは、次のプロセスを保護します。

- セッションマネージャサブシステム(smss.exe)
- クライアント/サーバランタイムサブシステム(csrss.exe)
- ローカルセキュリティ機関サブシステム(lsass.exe)
- Windowsログオンアプリケーション(winlogon.exe)
- Windowsスタートアップアプリケーション(wininit.exe)

WindowsサービスがAMPコネクタ(7.0.5より前のバージョン)より前に開始した場合、システムプロセスの除外が考慮されず、プロセスが除外された場合でも、SPPエンジンはプロセスを停止し、図に示すようにイベントがAMPコンソールに作成されます。



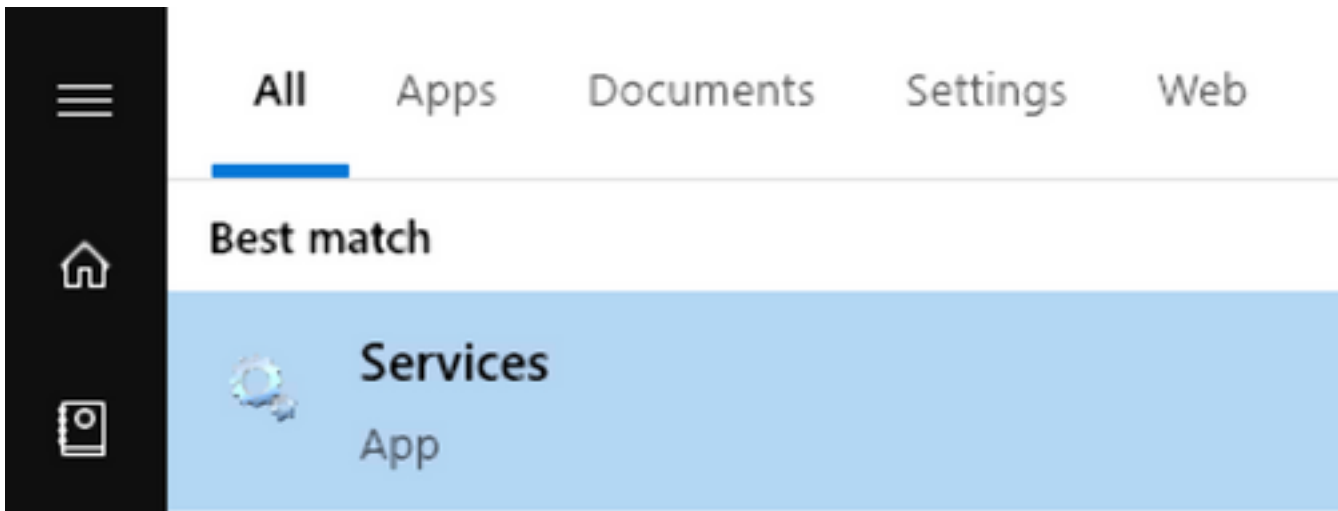
## トラブルシューティング

このバグの回避策は、AMPサービスの前に開始するWindowsサービスを遅延させることです。

Rosetta Stoneアプリケーションは、このドキュメントの例です。このアプリケーションは、認証のためにlsass.exeプロセスに接触するため、SPPによって検出されます。

### Windowsサービスの遅延手順

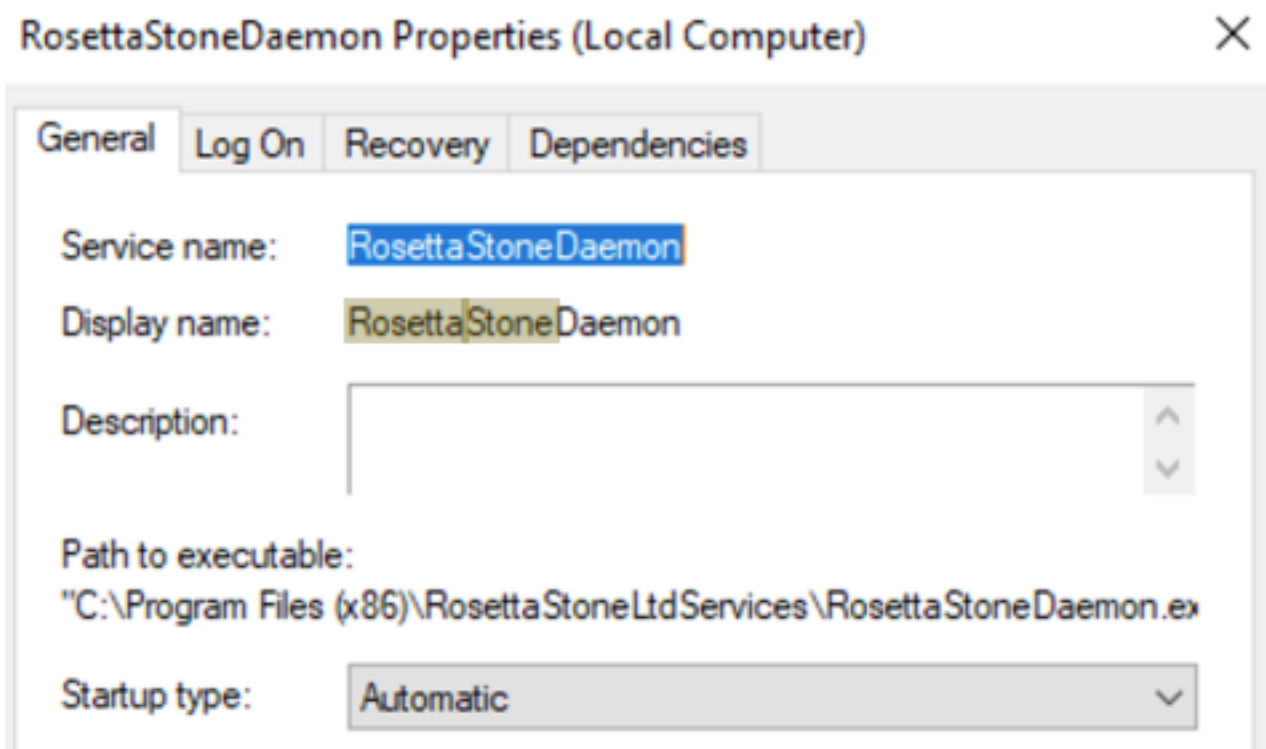
ステップ1：図に示すように、services.mscを開きます。



ステップ2: Rosetta Stoneサービスを検索します。

Service name	Display name	Description	Status	Startup type
RosettaStoneDaemon	RosettaStoneDaemon		Running	Automatic
VMware Tools	VMware Tools	Provides su...	Running	Automatic
VMware Alias Manager and Ticket Service	VMware Alias Manager and Ticket Service	Alias Mana...	Running	Automatic

ステップ3: RosettaStoneDaemonを右クリックし、Propertiesをクリックします。



StartupタイプはデフォルトでAutomaticに設定されており、RosettaStoneDaemonはブートプロセスで自動的に起動します。

ステップ4: ドロップダウンメニューをクリックし、[Automatic (Delayed Start)]を選択します。

General Log On Recovery Dependencies

Service name: RosettaStoneDaemon

Display name: RosettaStoneDaemon

Description:

Path to executable:  
"C:\Program Files (x86)\Rosetta Stone Ltd Services\RosettaStoneDaemon.exe"

Startup type: Automatic (Delayed Start)

この設定では、AMPコネクタの前にRosettaStoneDaemonサービスが開始されるのを防ぎます。

ステップ5:[Apply]をクリックします。



## コマンドラインでプロセスを遅延させる

PowerShell/CMDでは、次のコマンドを使用できます。

ステップ1:PowerShell/CMDを管理者として実行します。

ステップ2 : 次のコマンドを実行します。

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

注: 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
```

このセクションでは、遅延させるプロセスのRosettaStoneDaemonアプリケーション名を置き換

えることができます。

**注意：**コネクタバージョン7.0.5以降では、このバグのソリューションがすでに実装されています。この回避策は、7.0.5以降のコネクタバージョンを対象としています。