禁用和启用AMP连接器服务

目录

简介 <u>背景信息</u> <u>在Microsoft Windows上管理AMP连接器服务</u> <u>控制面板</u> <u>命令提示符</u> <u>使用用户界面停止服务</u> <u>管理OSX上的AMP连接器服务</u> <u>在Linux(RHEL 6)上管理AMP连接器服务</u> <u>在Linux(RHEL 7)上管理AMP连接器服务</u> 相关信息

简介

本文档介绍禁用和启用AMP连接器服务的各种方法。

背景信息

进行故障排除时,您需要禁用AMP连接器服务。您需要这样做的原因有几个:

- •删除损坏的数据库或日志文件。
- •由于错误、安装损坏或安装不完整而卸载AMP连接器。
- 替换policy.xml文件(用于高级故障排除目的)。

在Microsoft Windows上管理AMP连接器服务

控制面板

可通过控制面板禁用AMP连接器。要通过控制面板禁用连接器,请完成以下步骤:

- 1. 选择**开始>控制面板**。
- 2. 在"控制面板"中,单击**系统和安全**,然后单击管理工具。
- 3. 双击Services。
- 4. 在Services窗口中,向下滚动并找到Cisco AMP for Endpoints Connector服务。

| Services | | | | | - 0 | × |
|--------------------|-----------------------------------|---------------------------------|--------------|---------|--------------|-----------|
| File Action View | Help | | | | | |
| 🗢 🄿 🔲 🗔 🖸 | à 🗟 🛛 📷 🕨 🔳 🕪 👘 | | | | | |
| 🔍 Services (Local) | Q Services (Local) | | | | | |
| | Cisco AMP for Endpoints Connector | Name | Description | Status | Startup Type | Log Or ^ |
| | 6.3.1 | 🖏 Capability Access Manager | Provides fac | Running | Manual | Local S |
| | Stop the service | CaptureService_35edb | OneCore Ca | | Manual | Local S |
| | Pause the service | Certificate Propagation | Copies user | | Manual (Trig | Local S |
| | Restart the service | 🖏 Cisco AMP for Endpoints C | Cisco AMP | Running | Automatic | Local S |
| | | 🖏 Cisco Security Connector M | Cisco Securi | Running | Automatic | Local S |
| | Description: | Q Client License Service (ClipS | Provides inf | Running | Manual (Trig | Local S |
| | Cisco AMP for Endpoints Connector | CNG Key Isolation | The CNG ke | Running | Manual (Trig | Local S |
| | 6.3.1 | 🖏 COM+ Event System | Supports Sy | Running | Automatic | Local S |
| | | COM+ System Application | Manages th | Running | Manual | Local S |
| | | 🖏 Computer Browser | Maintains a | Running | Manual (Trig | Local S |
| | | 🖏 ConfigMgr Task Sequence | ConfigMgr | | Manual | Local S |
| | | Configuration Manager Re | Provides th | | Disabled | Local S |
| | | Connected Devices Platfor | This service | Running | Automatic (D | Local S |
| | | Connected Devices Platfor | This user se | Running | Automatic | Local S |
| | | 🖏 Connected User Experience | The Connec | Running | Automatic | Local S |
| | | 🖏 Contact Data_35edb | Indexes con | Running | Manual | Local S |
| | | CoreMessaging | Manages co | Running | Automatic | Local S |
| | | Credential Manager | Provides se | Running | Manual | Local S Y |
| | | < | | | | > |
| | Extended Standard | | | | | |

5. 左键点击**面向终端的思科AMP思科AMP的终端连接器**,然后点击左侧服务名称下的**停止**。

| File Action View | Help | | | | | |
|------------------|---|--|--|--|---|--|
| (+ +) 🔃 🖾 | 2 🗟 🛛 🖬 🕨 🖬 🕪 | | | | | |
| Services (Local) | Services (Local) | | | | | |
| | Cisco AMP for Endpoints Connector 6.3.1 Start the service | Name Capability Access Manager CaptureService_35edb Certificate Propagation | Description Provides fac OneCore Ca Copies user | Status Running | Startup Type Manual Manual Manual (Trig | Log Or ^ Local S Local S Local S |
| | Description: Cisco AMP for Endpoints Connector 6.3.1 | Cisco AMP for Endpoints C Cisco Security Connector M Client License Service (ClipS CNG Key Isolation COM+ Event System COM+ System Application Computer Browser ConfigMgr Task Sequence | Cisco AMP Cisco Securi Provides inf The CNG ke Supports Sy Manages th Maintains a ConfigMgr | Running Running Running Running Running Running | Automatic Automatic Manual (Trig Automatic Manual Manual Manual (Trig Manual | Local S Local S Local S Local S Local S Local S Local S Local S |
| | | Configuration Manager Re Connected Devices Platfor Connected Devices Platfor Connected User Experience Contact Data_35edb CoreMessaging | Provides th This service This user se The Connec Indexes con Manages co | Running Running Running Running Running | Disabled Automatic (D Automatic Automatic Manual Automatic Manual | Local S Local S Local S Local S Local S Local S |
| | | < | Provides se | Kunning | Manual | > |

命令提示符

您也可以使用命令提示符禁用AMP连接器服务。

1.您必须确定正确的服务名称。

2.选择开始>控制面板。

3.在"控制面板"中,单击**系统和安全**,然后单击管理工具。

4.双击Services。

5.在Services窗口中,向下滚动并找到Cisco AMP for Endpoints Connector服务。

6.右键单击此服务,然后单击**属性**。

7.请注意在后续步骤中使用的服务名称。

| Cisco AMP for En | idpoints Connector 6.3.1 Properties (Local Compu 🗙 |
|---|--|
| General Log On | Recovery Dependencies |
| Service name: | CiscoAMP_6.3.1 |
| Display name: | Cisco AMP for Endpoints Connector 6.3.1 |
| Description: | Cisco AMP for Endpoints Connector 6.3.1 |
| Path to executat "C:\Program File | ole: s\Cisco\AMP\6.3.1\sfc.exe'' |
| Startup type: | Automatic 🗸 🗸 |
| Service status: Start You can specify from here. Start parameters | Running Stop Pause Resume the start parameters that apply when you start the service |
| | |
| | OK Cancel Apply |

注意:服务名称根据安装的AMP连接器版本而更改。

8.转到开始菜单并查找cmd.exe文件。

9.右键单击并选择**以管理员身份运行**。

| Program | ns (1 |) | |
|---------|--------|--------------------------------------|---|
| ex. cm | | Open | |
| | ۲ | Run as administrator | |
| | | MediaInfo | |
| | × | Sourcefire + | |
| | | Pin to Taskbar | |
| | | Pin to Start Menu | |
| | м | Scan with Malwarebytes' Anti-Malware | |
| | | Restore previous versions | |
| | | Send to + | |
| | | Cut | |
| | | Сору | |
| | | Delete | |
| | | Open file location | |
| | | Properties | |
| 🔎 See m | ore re | sults | · |
| cmd | | × Shut down + | |

10.在命令提示符下,输入以下命令以停止AMP连接器:



11.或者,您也可以使用wmic命令。



12.要重新启动连接器,请输入以下命令:

C:\Windows\system32> net start CiscoAMP_6.3.1

(OR)

wmic service where name="CiscoAMP_6.3.1" call startservice 13.连接器启动时,将显示此输出。

| Administrator, Command Prompt | - | × |
|---|---|---|
| C:\WINDOWG\system32>net start CiscoAMP_6.3.1 The Cisco AMP for Endpoints Connector 6.3.1 service is starting. The Cisco AMP for Endpoints Connector 6.3.1 service was started successfully. | | ^ |
| C:\NINDONS\system12>_ | | |
| | | |
| | | |
| | | |
| | | |

注意:如果启用了连接器密码保护,**则这些步骤**将不起作用。 使用以下步骤添加保护密码 ,以停止服务。 此命令仅适用于4.3.0版及更高版本的AMP连接器。

14. 输入以下命令:

sfc.exe -k password 将"password"一词替换为策略中设置的实际密码。



注:目录根据安装的Cisco AMP连接器版本而更改。

使用用户界面停止服务

您也可以从用户界面停止受密码保护的服务。

| Scan Settings | • |
|----------------------------|----------|
| Notification Settings | • |
| Community Settings | • |
| Proxy Settings | • |
| FireAMP Connector Settings | A |
| Service Status: Started | |
| Password: | |
| Stop Service | |
| | |
| | |
| | |

管理OSX上的AMP连接器服务

要在OSX上禁用AMP服务,请在终端中输入以下命令:

sudo launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist 要在OSX上启用AMP服务,请在终端中输入以下命令:

sudo launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist

在Linux(RHEL 6)上管理AMP连接器服务

要在Linux上禁用AMP服务,请在终端中输入以下命令:

sudo initctl stop cisco-amp 要在Linux上启用AMP服务,请在终端中输入以下命令:

sudo initctl start cisco-amp

在Linux(RHEL 7)上管理AMP连接器服务

要在Linux上禁用AMP服务,请在终端中输入以下命令:

sudo systemctl stop cisco-amp 要在Linux上启用AMP服务,请在终端中输入以下命令:

sudo systemctl start cisco-amp

相关信息

- AMP连接器安装程序的命令行开关
- <u>技术支持和文档 Cisco Systems</u>

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言,希望全球的用户都能通过各 自的语言得到支持性的内容。

请注意:即使是最好的机器翻译,其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任,并建议您总是参考英文原始文档(已提供 链接)。