删除Windows上的FireAMP缓存和历史记录文件

目录

简介

用于缓存和历史记录的数据库文件

- 目的
- 删除原因
- 识别数据库文件

删除数据库文件的过程

- 步骤 1：停止FireAMP连接器服务
  - 用户界面
  - 服务控制台
  - 命令提示符
- 步骤 2：删除所需的数据库文件
  - 缓存数据库文件
  - 历史记录数据库文件
- 步骤 3：启动FireAMP连接器服务

简介

本文档提供一些需要删除面向终端的FireAMP中的数据库文件的方案，并介绍在必要时删除这些文件的正确过程。面向终端的FireAMP在数据库文件中维护其最新文件检测和处置的记录。在某些情况下，Cisco支持工程师可能会要求您删除一些数据库文件以排除故障。

> 警告：只有在Cisco技术支持指示的情况下才能删除数据库文件。

用于缓存和历史记录的数据库文件

目的

高速缓存数据库文件维护文件的已知性质。历史记录数据库文件跟踪所有FireAMP文件检测，以及源文件名和SHA256值。

向策略添加阻止列表并更新连接器时，给定文件的行为不会立即更改。这是因为缓存已识别出该文件不是恶意文件。因此，阻止列表不会更改或覆盖它。当缓存在策略中的每段时间过期且执行新查找时，性质会更改 — 首先根据列表执行查找，然后根据云执行查找。

删除原因

如果从目录中删除历史记录数据库和缓存数据库文件，则在FireAMP服务重新启动时重新创建它们。在某些情况下，可能需要将这些文件从FireAMP目录中删除。例如，如果要测试给定文件的简单自定义检测或应用阻止列表。

数据库可能会损坏，这会使您无法打开或查看数据库中的检测项。或者，如果系统上的数据库已损坏，则可能导致FireAMP连接器服务出错，例如无法启动连接器或整体系统性能下降。在这些情况下，您可能希望从连接器清除历史记录文件，以便避免性能相关问题损坏并能够捕获新日志以供诊断。

识别数据库文件

在Microsoft Windows上，这些文件通常位于C:\Program Files\Sourcefire\fireAMP或C:\Program Files\Cisco\AMP。

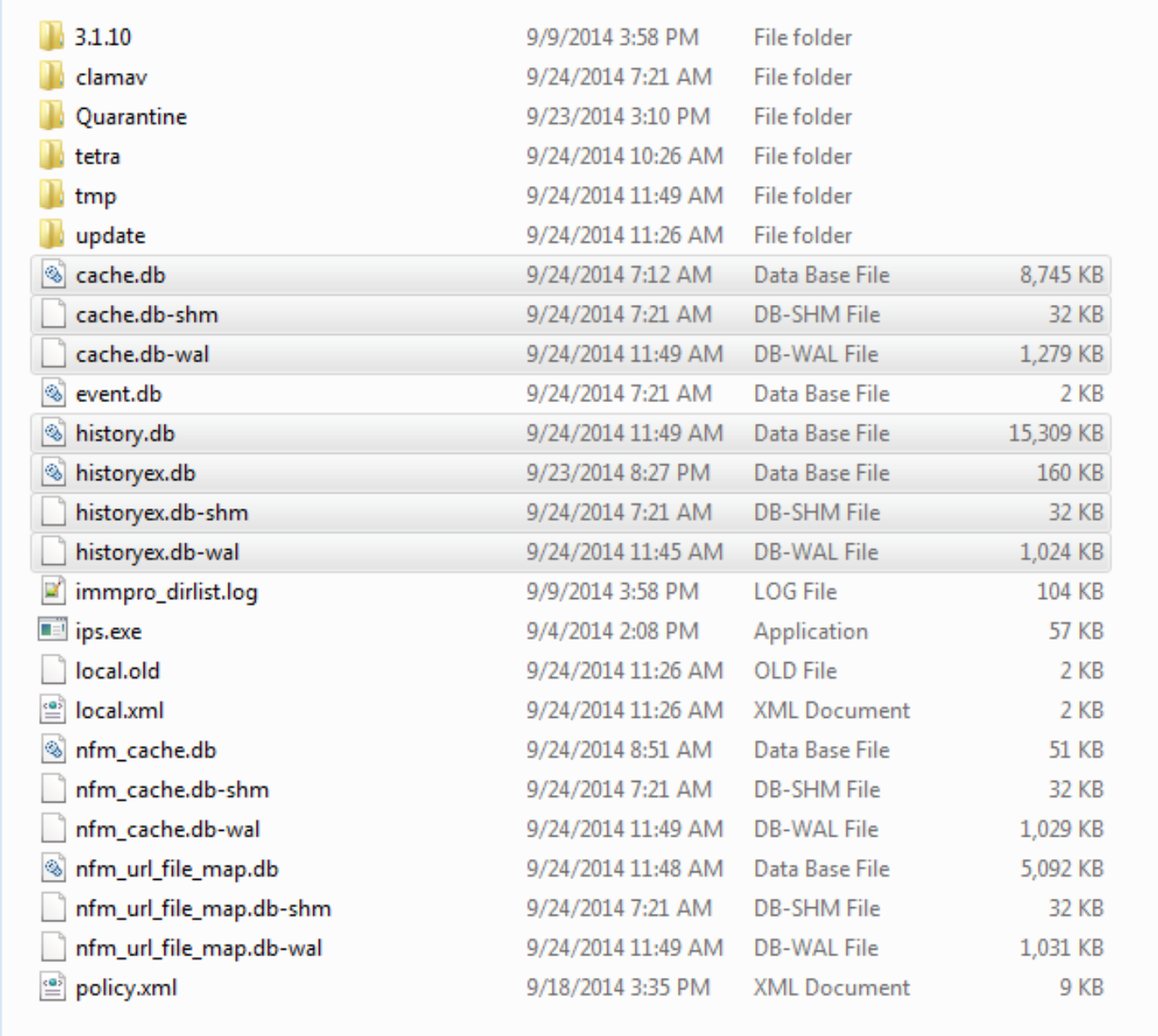
缓存数据库文件的名称为：

```
cache.db
cache.db-shm
cache.db-wal
```

历史记录数据库文件的名称为：

```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

此屏幕截图显示了Windows文件资源管理器上的文件：



3.1.10	9/9/2014 3:58 PM	File folder	
clamav	9/24/2014 7:21 AM	File folder	
Quarantine	9/23/2014 3:10 PM	File folder	
tetra	9/24/2014 10:26 AM	File folder	
tmp	9/24/2014 11:49 AM	File folder	
update	9/24/2014 11:26 AM	File folder	
cache.db	9/24/2014 7:12 AM	Data Base File	8,745 KB
cache.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
cache.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,279 KB
event.db	9/24/2014 7:21 AM	Data Base File	2 KB
history.db	9/24/2014 11:49 AM	Data Base File	15,309 KB
historyex.db	9/23/2014 8:27 PM	Data Base File	160 KB
historyex.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
historyex.db-wal	9/24/2014 11:45 AM	DB-WAL File	1,024 KB
immpro_dirlist.log	9/9/2014 3:58 PM	LOG File	104 KB
ips.exe	9/4/2014 2:08 PM	Application	57 KB
local.old	9/24/2014 11:26 AM	OLD File	2 KB
local.xml	9/24/2014 11:26 AM	XML Document	2 KB
nfm_cache.db	9/24/2014 8:51 AM	Data Base File	51 KB
nfm_cache.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
nfm_cache.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,029 KB
nfm_url_file_map.db	9/24/2014 11:48 AM	Data Base File	5,092 KB
nfm_url_file_map.db-shm	9/24/2014 7:21 AM	DB-SHM File	32 KB
nfm_url_file_map.db-wal	9/24/2014 11:49 AM	DB-WAL File	1,031 KB
policy.xml	9/18/2014 3:35 PM	XML Document	9 KB

删除数据库文件的过程

步骤 1：停止FireAMP连接器服务

您可以通过多种方式停止FireAMP连接器服务：

- FireAMP连接器服务的用户界面(UI)
- Windows服务控制台
- 管理员的命令提示符

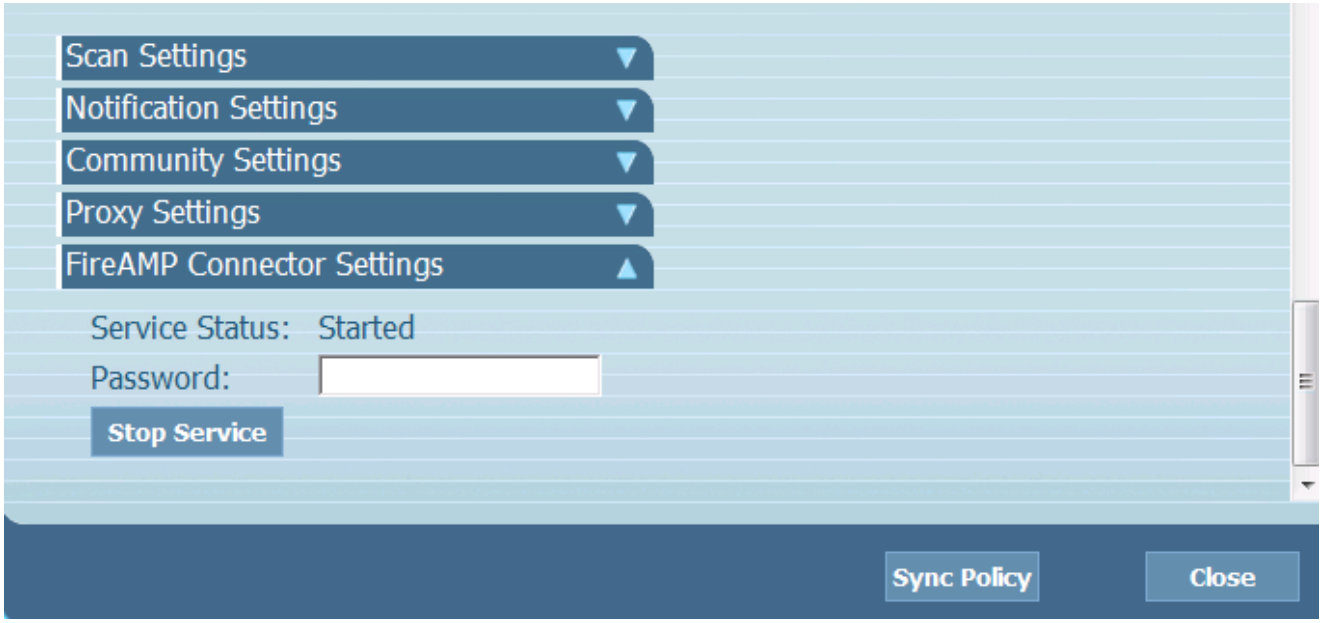
用户界面

注意：如果启用了连接器保护，则必须使用UI以停止FireAMP连接器服务。

---

a. 从托盘中打开UI，然后单击Settings。

b. 滚动到底部，展开FireAMP Connector Settings。
c. 在Password字段中，输入连接器保护密码。单击Stop Service。

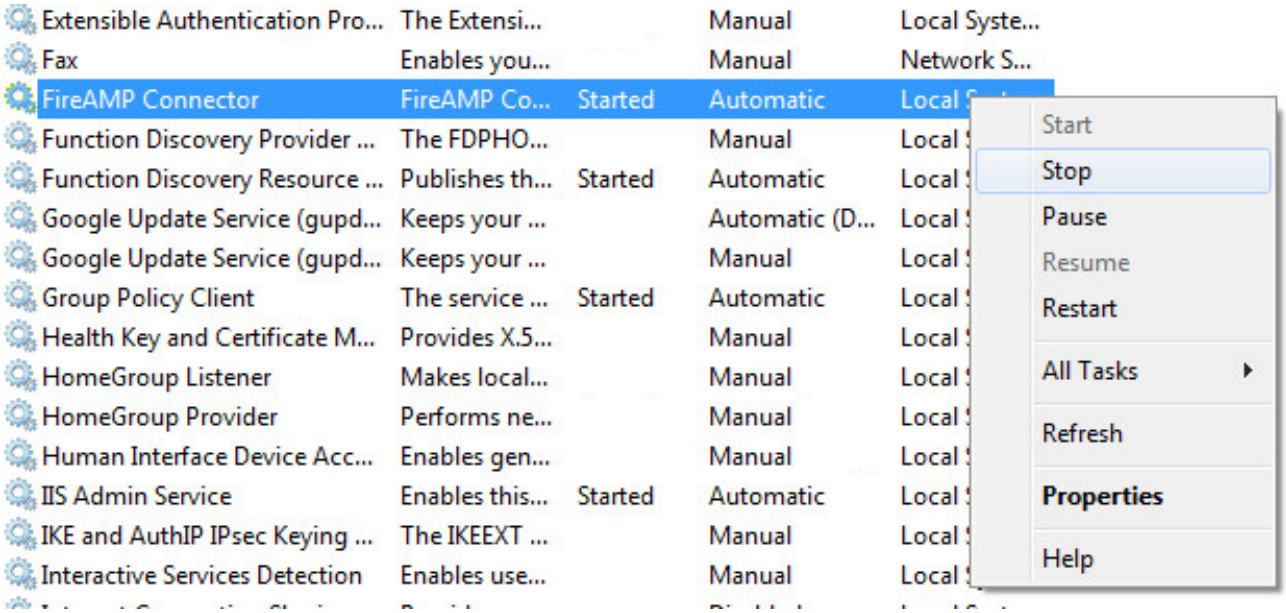


服务控制台

注意：要在“服务”控制台中停止和启动服务，您需要具有管理员权限。

要从服务控制台停止FireAMP连接器服务，请完成以下步骤：

a. 导航到开始菜单。
b. 输入services.msc并按Enter。将打开“服务”控制台。
c. 选择FireAMP Connector服务，然后右键单击服务名称。
d. 选择Stop以停止服务。

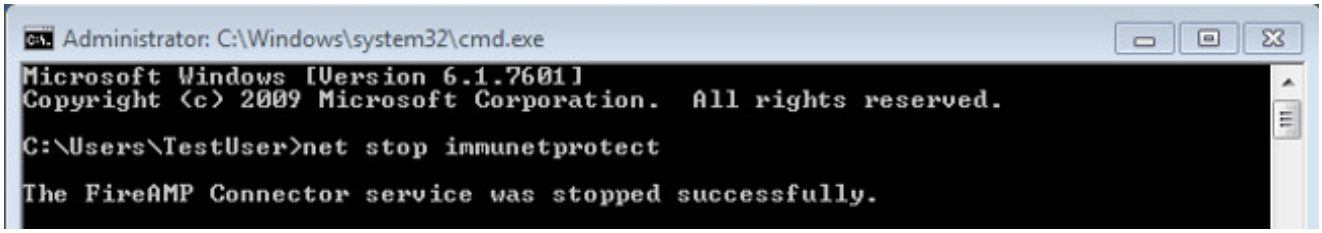


命令提示符

要从管理员的命令提示符停止FireAMP连接器服务，请完成以下步骤：

a. 导航到开始菜单。
b. 输入cmd.exe并按Enter。将会打开命令提示符窗口。
c. 输入net stop immunetprotect命令。如果您有5.0.1版或更高版本，请输入wmic service，其中“name like 'immunetprotect%'”call startservice命令。

此屏幕截图显示成功停止的服务的示例：



步骤 2：删除所需的数据库文件

缓存数据库文件

停止服务后，您可以删除以下三个缓存文件：

警告：如果不删除所有相关的缓存数据库文件，可能会对重新创建的数据库造成缓存问题。因此，服务可能无法启动或者您可能遇到服务性能下降的情况。

```
cache.db
cache.db-shm
cache.db-wal
```

历史记录数据库文件

服务停止后，请删除以下历史记录数据库文件：

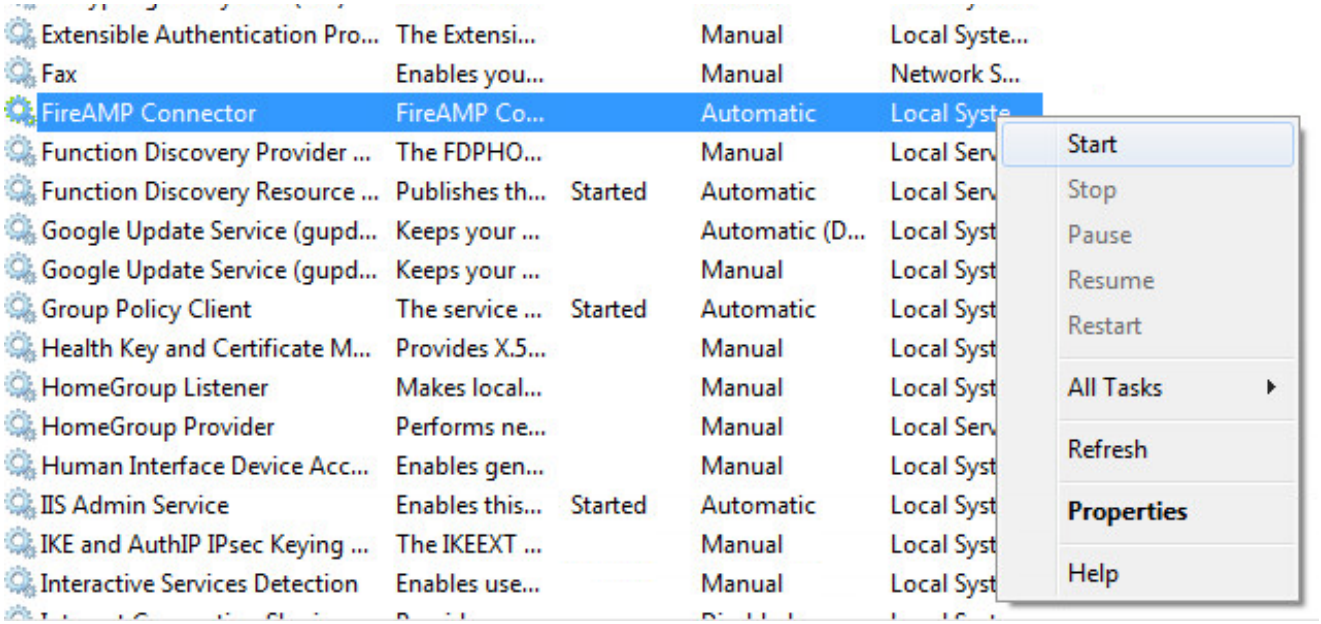
警告：如果不删除所有相关的历史记录数据库文件，可能会对重新创建的数据库产生缓存问题。因此，服务可能无法启动或者您可能遇到服务性能下降的情况。

```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

步骤 3：启动FireAMP连接器服务

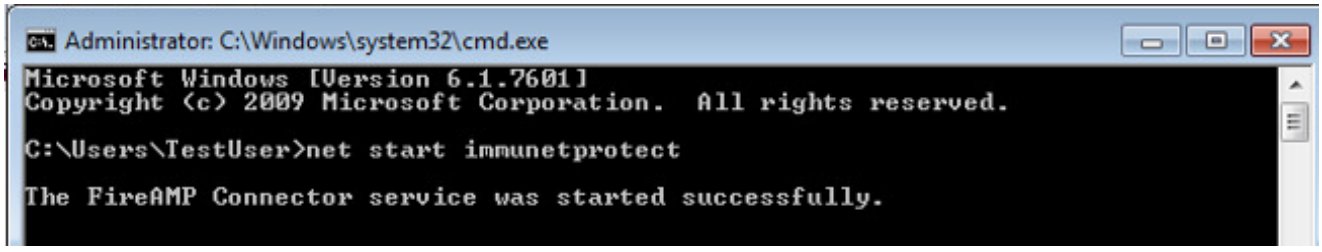
要启动FireAMP连接器服务，请完成以下步骤：

a. 导航到开始菜单。
b. 输入services.msc并按Enter。将打开“服务”控制台。
c. 选择FireAMP Connector服务并右键单击服务名称。
d. 选择Start以启动服务。



或者，在管理员的命令提示符下，您可以输入net start immunetprotect命令。如果您有5.0.1版或更高版本，请输入wmic service，其中“name like 'immunetprotect%'”call startservice命令。

此屏幕截图显示已成功启动的服务示例：



重新启动服务后，将创建一组新的数据库文件。现在，这应该会为您提供一个包含当前白名单、阻止列表、例外项等的新FireAMP连接器实例。

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）。

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）。