FireAMP缓存和历史文件的删除在Windows

目录

简介

本文提供在终端的FireAMP要求数据库文件删除的一些方案并且描述适当程序当必要时删除他们。终端的FireAMP保持其最近文件检测和处理记录在数据库文件。在某些情况下， Cisco技术支持工程师也许要求您删除某些数据库文件为了排除故障问题。

> 警告：您能删除数据库文件，只有当提示由思科技术支持。

缓存和历史记录的数据库文件

目的

缓存数据库文件维护文件的已知处理。历史记录数据库文件与源文件名称和SHA256值一起跟踪所有FireAMP文件检测。

当您添加一块列表到策略并且更新连接器时，一个给的文件的行为不立即更改。这是因为缓存已经识别文件不是有恶意的。同样地，它不会由您的块列表更改也不会改写。处理更改，当缓存每在您的策略时的时间超时，并且新的查找执行-首先您的列表和随后网云。

删除的原因

如果历史记录数据库和缓存数据库文件从目录删除，他们是被再创的新鲜的，当FireAMP服务重新启动。在某些情况下从FireAMP目录删除这些文件也许是必要的。例如，如果要为一个给的文件测试简单自定义检测或应用程序块列表。

很可能，数据库可能变得损坏，使您无法打开或查看在数据库的检测。或者，如果数据库是损坏在

系统它在FireAMP连接器服务内能造成错误例如无法开始整个系统性能的连接器或下降。在这些实例您也许要清除从连接器的历史文件，以便您可以避免从损坏的性能相关问题和能获取诊断的新建的日志。

识别数据库文件

在Microsoft Windows上，这些文件典型地查找在C:\Program Files\Sourcefire\fireAMP或C:\Program Files\Cisco\AMP。

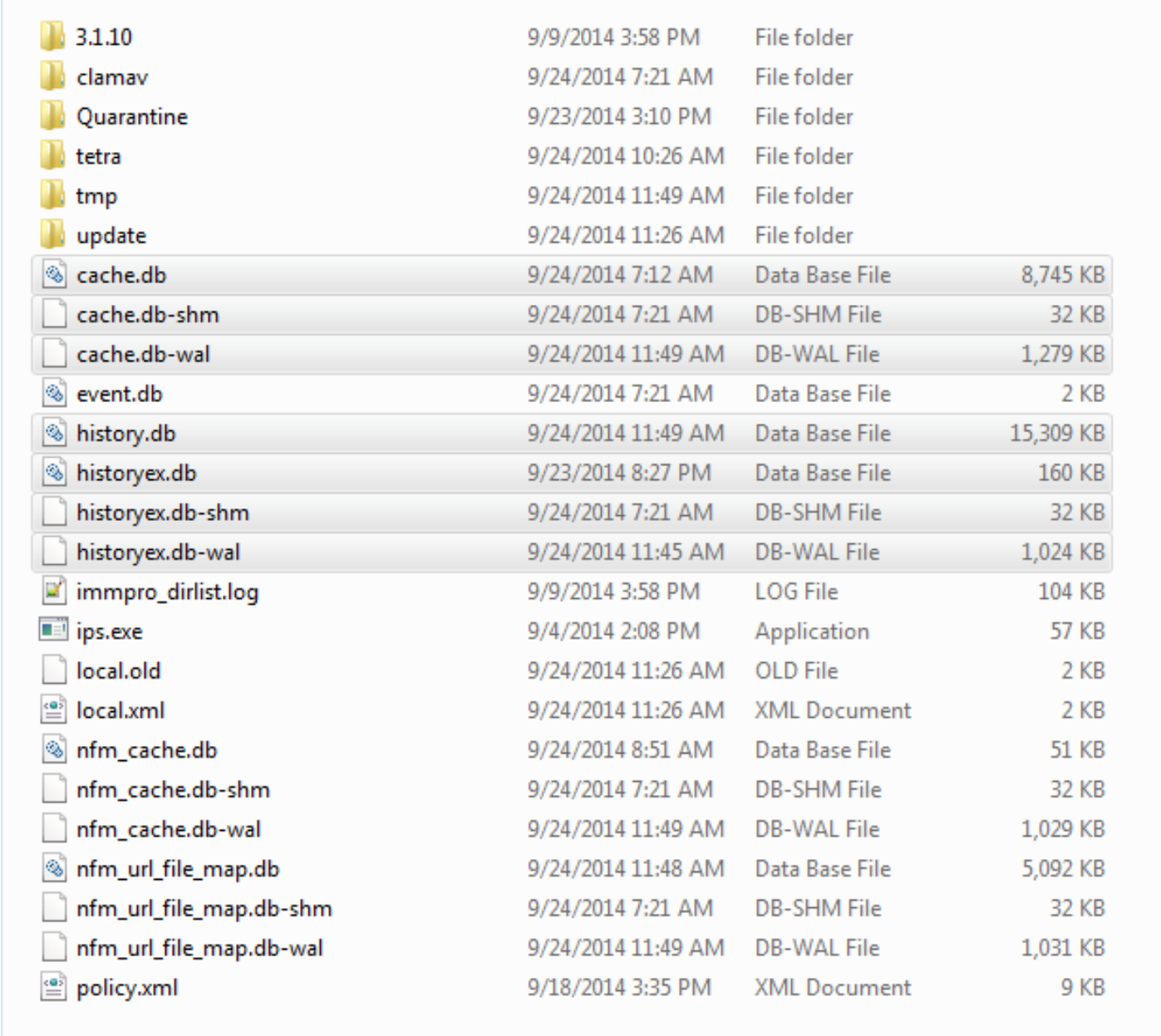
缓存数据库文件的名称是：

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

历史记录数据库文件的名称是：

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

此屏幕画面显示在Windows文件Explorer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

删除数据库文件的步骤

步骤 1：终止FireAMP连接器服务

您能终止FireAMP连接器服务多种方式：

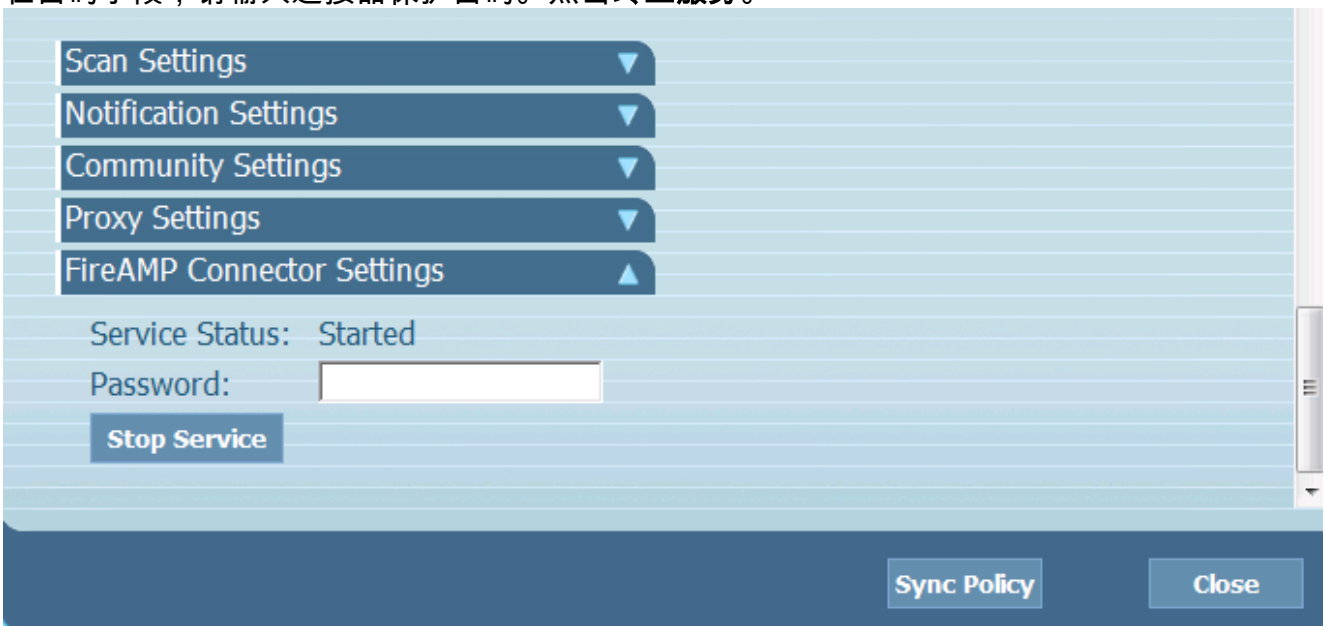
- 用户界面(UI) FireAMP连接器服务
- Windows服务控制台
- 管理员的prompt命令

用户界面

Note:如果有连接器保护启用您必须使用UI为了终止FireAMP连接器服务。

1. 打开从盘的UI并且点击**设置**。
2. 移动到底部并且展开**FireAMP连接器设置**。

3. 在密码字段，请输入连接器保护密码。点击**终止服务**。

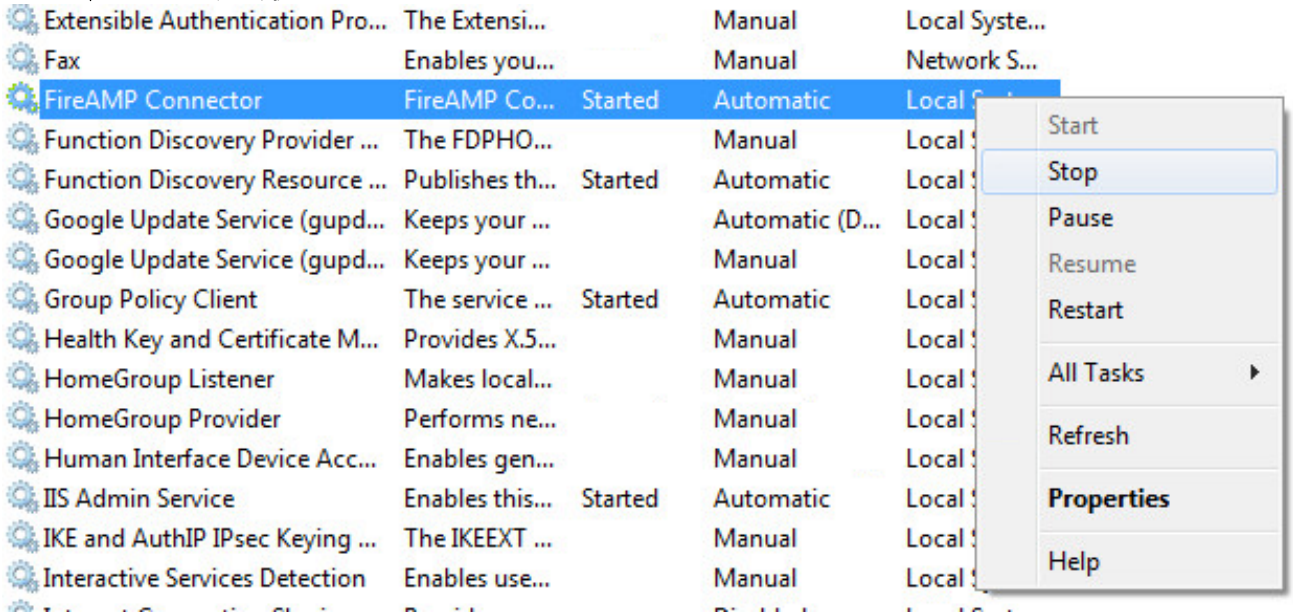


服务控制台

Note:为了终止和开始在服务控制台的服务您需要管理员权限。

为了从服务控制台终止FireAMP连接器服务，请完成这些步骤：

1. 导航对**开始菜单**。
2. 输入**services.msc并且**按回车。服务控制台打开。
3. 选择**FireAMP连接器**服务并且用鼠标右键单击服务名称。
4. 选择**终止**为了终止服务。

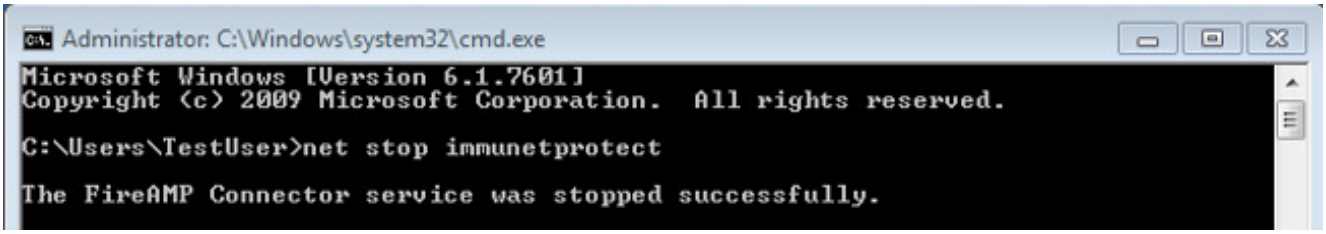


Prompt命令

为了从管理员的prompt命令终止FireAMP连接器服务，请完成这些步骤：

1. 导航对**开始菜单**。

2. 输入**cmd.exe并且**按回车。**A命令**提示窗口打开。
3. 输入**net stop immunetprotect**命令。如果有版本5.0.1或以上，请加入**“名称类似‘immunetprotect%’”呼叫startservice**发出命令的**wmic服务**。 此屏幕画面显示顺利地被终止的服务的示例
：



步骤 2：删除需要的数据库文件

缓存数据库文件

一旦服务被终止您能删除这三个缓存文件：

> 警告：如果不删除所有相关缓存数据库文件它能创建与被重建的数据库的高速缓冲存储问题。同样地，服务也许不能开始或您也许体验从服务的下降的性能。

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

历史记录数据库文件

一旦服务被终止，请删除这些历史记录数据库文件：

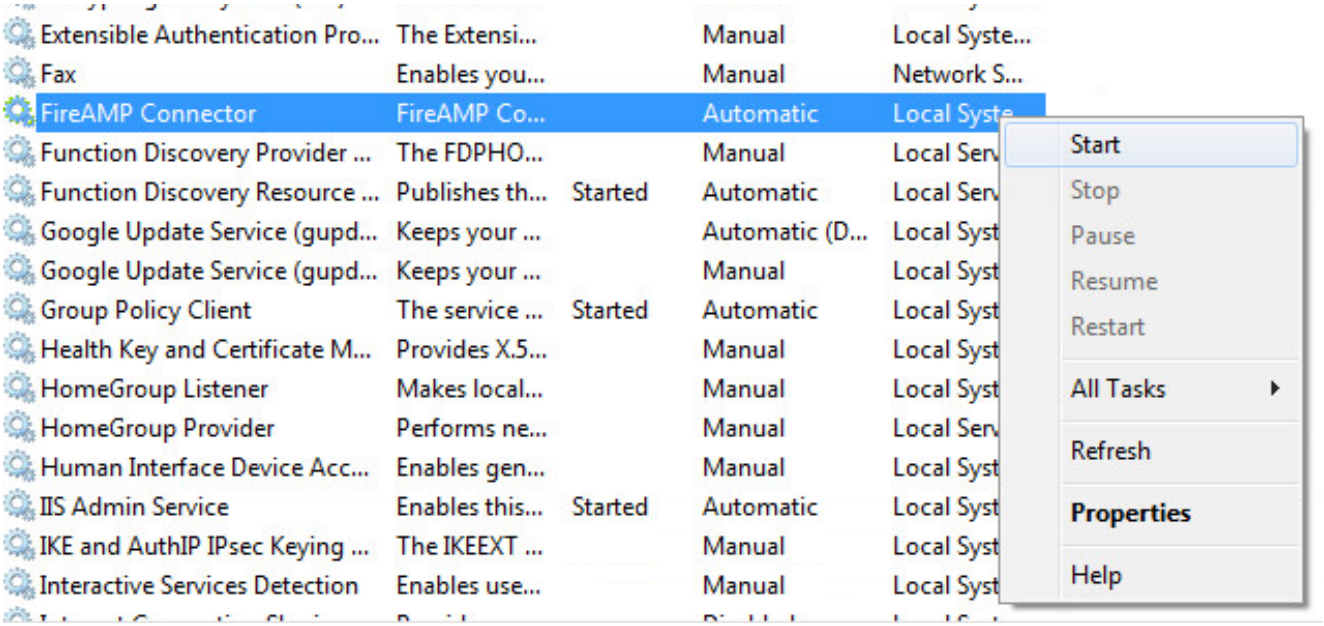
> 警告：如果不删除所有相关历史记录数据库文件它能创建与被重建的数据库的高速缓冲存储问题。同样地，服务也许不能开始或您也许体验从服务的下降的性能。

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

步骤 3：开始FireAMP连接器服务

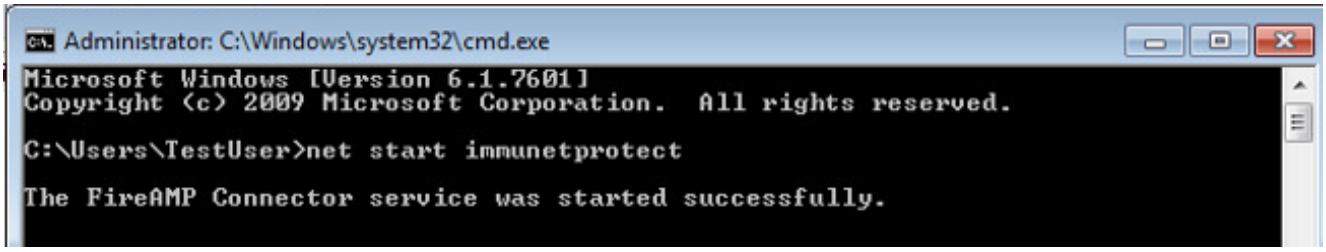
为了开始FireAMP连接器服务，请完成这些步骤：

1. 导航对**开始菜单**。
2. 输入**services.msc并且**按回车。服务控制台打开。
3. 选择**FireAMP连接器**服务并且用鼠标右键单击服务名称。
4. 选择**开始**为了开始服务。



或者，在管理员的prompt命令您能输入**net start immunetprotect**命令。如果有版本5.0.1或以上，请加入**"名称类似'immunetprotect%'"呼叫startservice**发出命令的**wmic服务**。此屏幕画面显示顺利地开始的服务的示例

：



在您重新启动新的一套数据库文件创建的服务后。这应该当前提供您FireAMP连接器的一个新实例有当前白色列表的，块列表，排除，等等。