Удаление кэша FireAMP и файлов истории на Windows

Содержание

Введение

Этот документ предоставляет некоторые сценарии, которые требуют удаления файлов базы данных в FireAMP для Оконечных точек, и описывает соответствующую процедуру для удаления их при необходимости. FireAMP для Оконечных точек поддерживает запись своих обнаружений последнего файла и расположений в файлах базы данных. В определенных случаях специалист службы технической поддержки Cisco мог бы попросить, чтобы вы удалили некоторые файлы базы данных, для решения проблемы.

> **% Warning:** Можно удалить файл базы данных только если проинструктированный технической поддержкой Cisco.

Файлы базы данных для кэша и истории

Цель

Файлы базы данных кэша поддерживают известные расположения для файлов. Файлы базы данных истории отслеживают все обнаружения файла FireAMP, наряду с названиями исходного файла и значениями SHA256.

Когда вы добавляете черный список к политике и обновляете разъём, поведение для данного файла сразу не изменяется. Это вызвано тем, что кэш уже определил это, файл не является злонамеренным. Также, это не будет изменено или отвергнуто вашим черным списком. Расположение изменяется, когда кэш истекается во время в вашей политике, и новый поиск выполнен - сначала против ваших списков и впоследствии против облака.

Причины для удаления

Если база данных истории и файлы базы данных кэша удалены из каталога, они воссозданы новые, когда сервис FireAMP перезапускает. В определенных случаях могло бы быть необходимо удалить эти файлы из каталога FireAMP. Например, если вы хотите протестировать простое пользовательское обнаружение или список блока приложений для данного файла.

Возможно, что база данных могла стать поврежденной, который представляет вас неспособный открыть или просмотреть обнаружения в базе данных. Также, если база данных повреждена в системе, она может вызвать ошибки в сервисе Разъёма FireAMP, такие как неспособность запустить разъём или ухудшение общей производительности системы. В этих экземплярах вы могли бы хотеть очистить файлы истории от разъёма так, чтобы можно было избежать связанных с производительностью проблема от повреждения и быть в состоянии перехватить новые журналы для диагноза.

Определите файлы базы данных

На Microsoft Windows эти файлы, как правило, располагаются в C:\Program Files\Sourcefire\fireAMP.

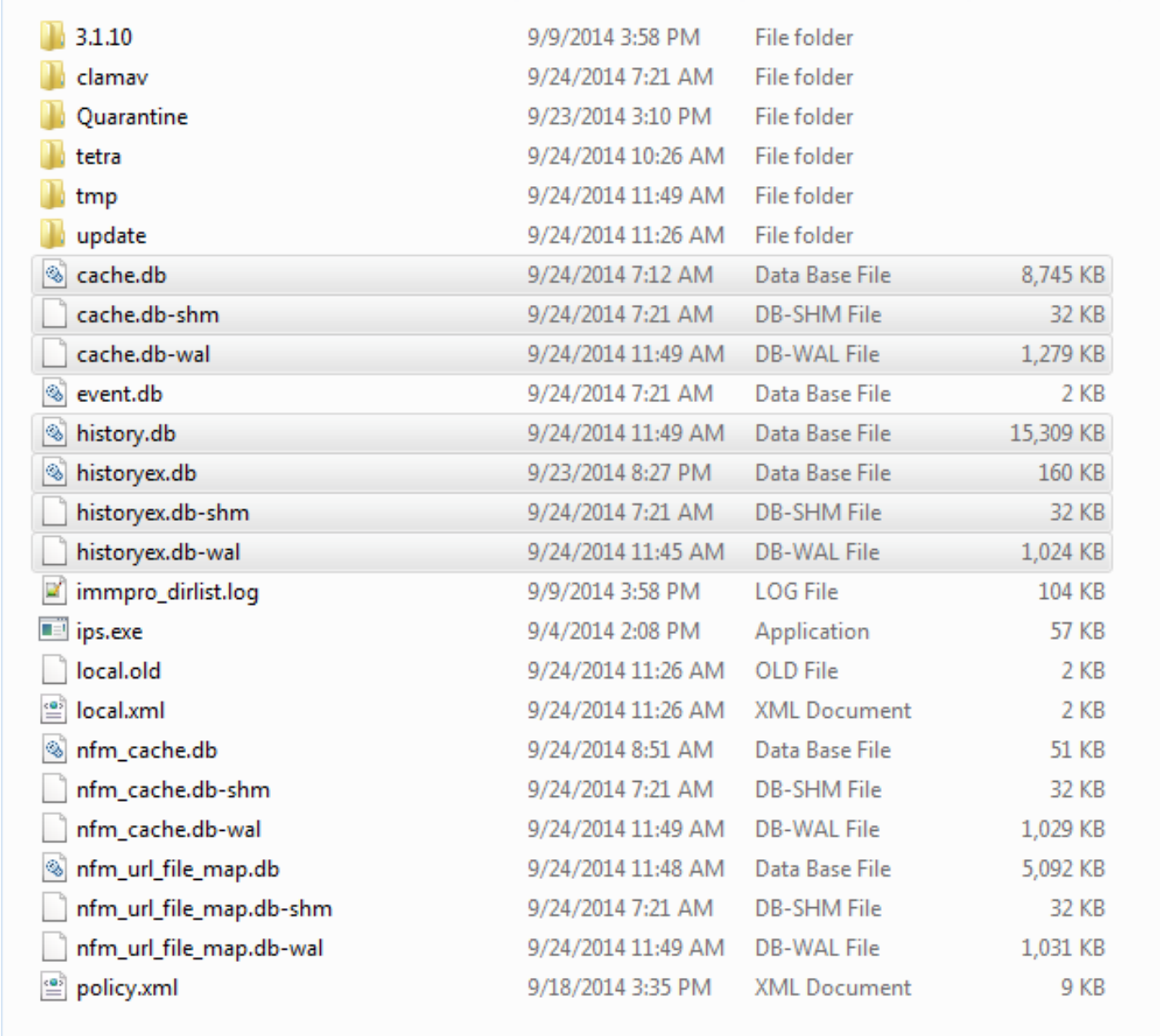
Название файлов базы данных кэша:

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

Название файлов базы данных истории:

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

Этот снимок экрана показывает файлы на Windows File Explorer:



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

Процедура для удаления файлов базы данных

Шаг 1: Остановите сервис разъёма FireAMP

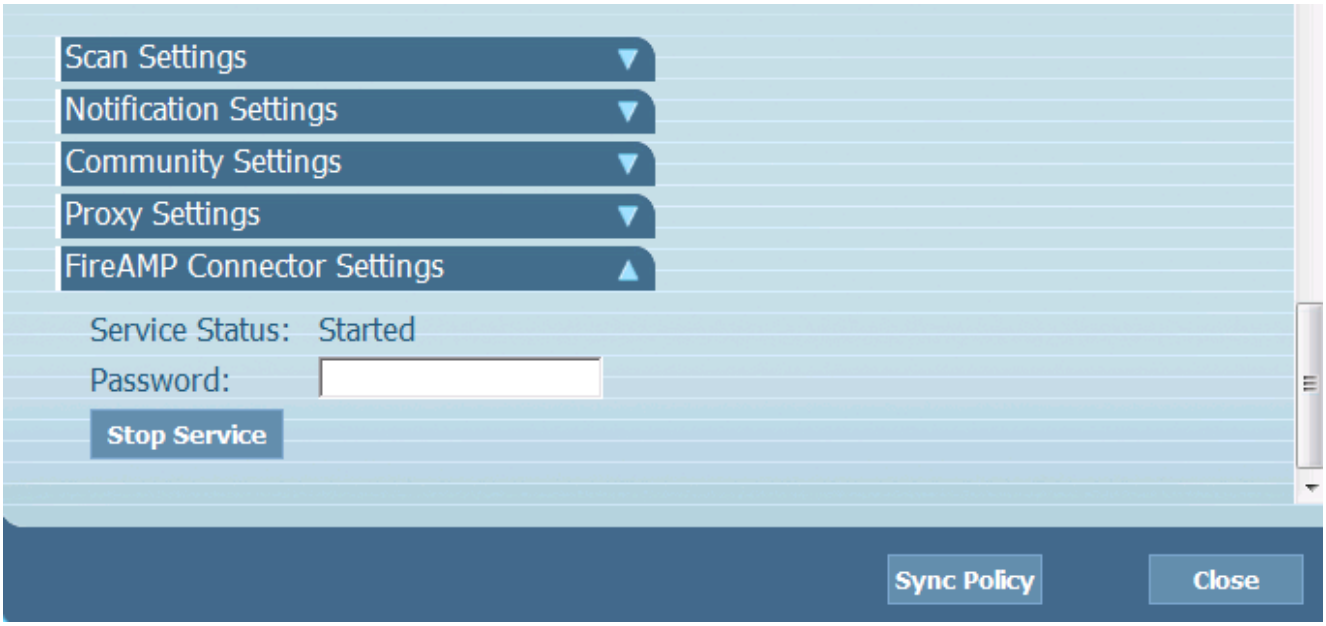
Можно остановить различные способы сервиса Разъёма FireAMP:

- Интерфейс пользователя (UI) сервиса Разъёма FireAMP
- Консоль Windows Services
- Командная строка администратора

Пользовательский интерфейс

> **Примечание:** Если вам включили защиту разъёма, необходимо использовать UI для остановки сервиса Разъёма FireAMP.

1. Откройте UI от лотка и нажмите **Settings**.
2. Перейдите к нижней части и разверните **Параметры настройки Разъёма FireAMP**.
3. В Поле Password введите пароль защиты разъёма. Нажмите **Stop Service**.

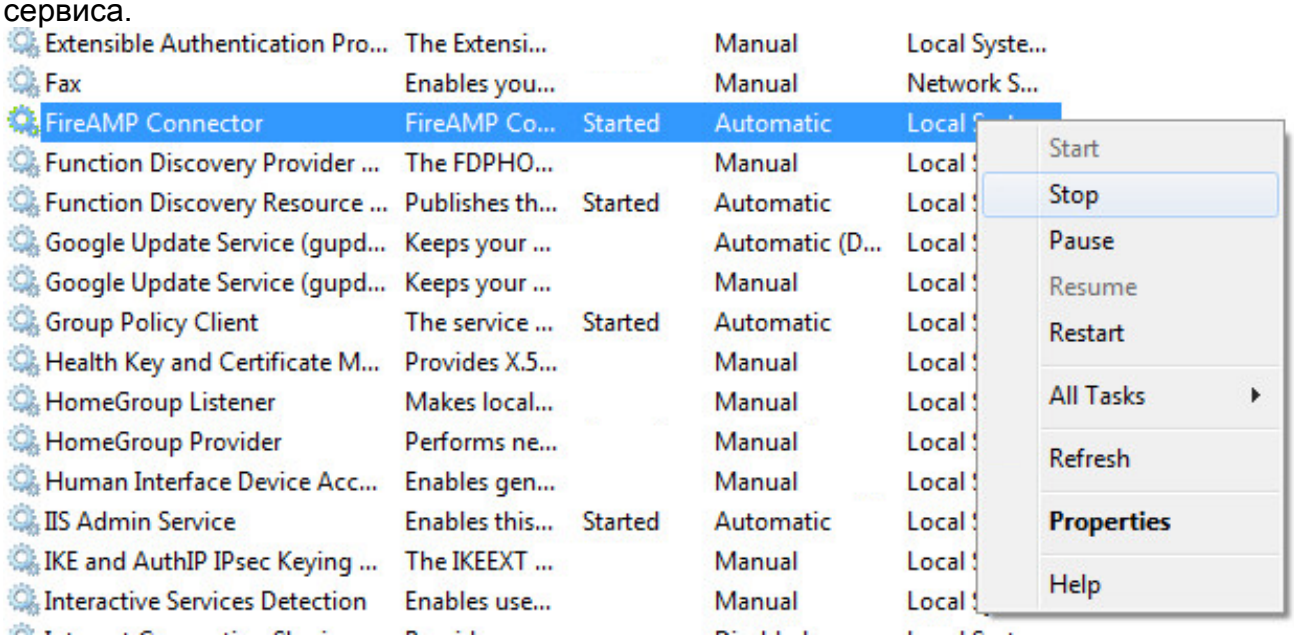


Консоль сервисов

Примечание: Чтобы остановить и запустить сервисы в консоли Сервисов, вам нужны Администраторские привилегии.

Для остановки сервиса Разъёма FireAMP от консоли Сервисов выполните эти шаги:

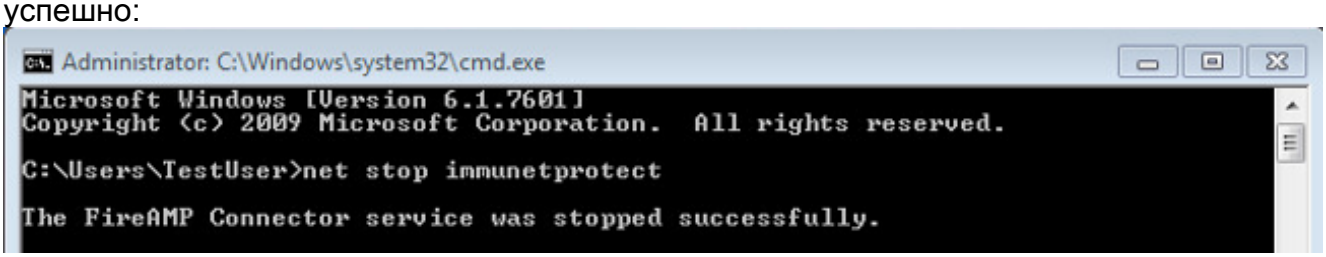
1. Перейдите к **меню Пуск**.
2. Введите **services.msc** и нажмите **Enter**. Консоль Сервисов открывается.
3. Выберите сервис **Разъёма FireAMP** и щелкните правой кнопкой мыши имя сервиса.
4. Выберите **Stop** для остановки сервиса.



Командная строка

Для остановки сервиса Разъёма FireAMP от командной строки администратора выполните эти шаги:

1. Перейдите к **меню Пуск**.
2. Введите **cmd.exe** и нажмите **Enter**. Окно командной строки открывается.
3. Введите **сетевую остановку immunetprotect** команда.Этот снимок экрана показывает, что пример сервиса остановился
   успешно:



Шаг 2: Удалите требуемые файлы базы данных

Файлы базы данных кэша

Как только сервис остановлен, можно удалить эти три файла кэша:

> **% Warning:** Если вы не удаляете все связанные файлы базы данных кэша, это может создать кэширующиеся проблемы с воссозданной базой данных. Также, сервис мог бы быть не в состоянии запускаться, или вы могли бы испытать ухудшенную производительность от сервиса.

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

Файлы базы данных истории

Как только сервис остановлен, удалите эти файлы базы данных истории:

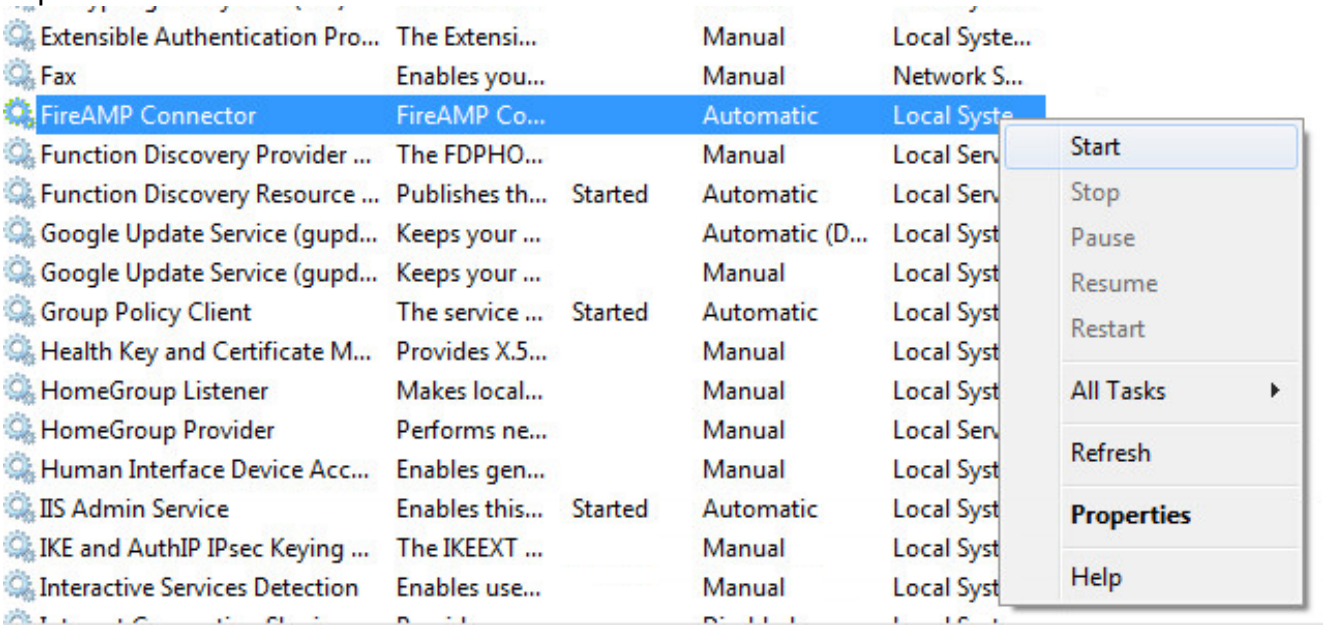
> **% Warning:** Если вы не удаляете все связанные файлы базы данных истории, это может создать кэширующиеся проблемы с воссозданной базой данных. Также, сервис мог бы быть не в состоянии запускаться, или вы могли бы испытать ухудшенную производительность от сервиса.

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

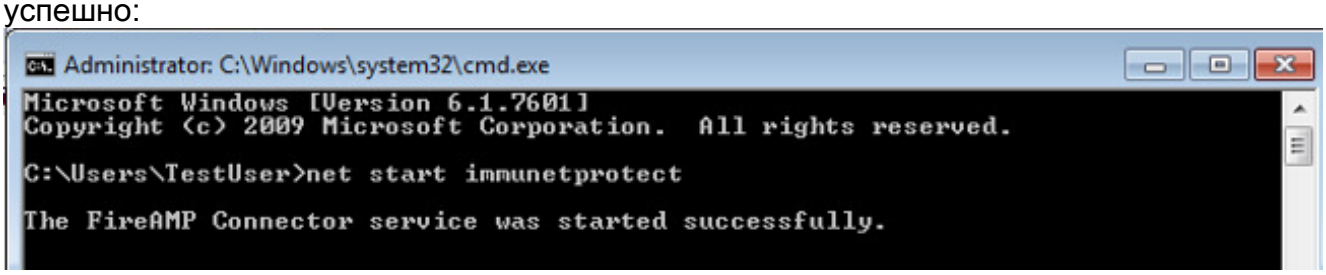
Шаг 3: Запустите сервис разъёма FireAMP

Для начала сервиса Разъёма FireAMP выполните эти шаги:

1. Перейдите к **меню Пуск**.
2. Введите **services.msc** и нажмите **Enter**. Консоль Сервисов открывается.
3. Выберите сервис **Разъёма FireAMP** и щелкните правой кнопкой мыши имя сервиса.
4. Выберите **Start** для начала
   сервиса.



Также на командной строке Администратора можно ввести **сетевой запуск immunetprotect** команда.Этот снимок экрана показывает, что пример сервиса запустился
успешно:



После перезапуска сервисов, новый набор файлов базы данных создан. Это должно теперь предоставить вам новый экземпляр Разъёма FireAMP с текущими белыми списками, черными списками, исключениями, и так далее.