Windows 上の FireAMP キャッシュと履歴ファイルの削除

目次

概要

このドキュメントでは、FireAMP for Endpoints でデータベース ファイルを削除する必要があるいくつかのシナリオを紹介し、必要に応じてそれらを削除する正しい手順について説明します。 FireAMP for Endpoints は、最近のファイルの検出と廃棄のレコードをデータベース ファイルに保持します。 特定のケースでは、シスコ サポート エンジニアが問題のトラブルシューティングのために一部のデータベース ファイルの削除を依頼する場合があります。

> **警告**： データベース ファイルはシスコ テクニカル サポートから指示された場合にだけ削除するようにしてください。

キャッシュと履歴のデータベース ファイル

目的

キャッシュ データベース ファイルは、既知のファイルの廃棄を保持します。 履歴データベース ファイルは、ソース ファイル名と SHA256 の値とともにすべての FireAMP ファイルの検出を追跡します。

ブロック リストをポリシーに追加してコネクタを更新しても、指定されたファイルの動作は直ちには変更されません。 これは、悪意がないファイルであることがキャッシュ時点ですでに特定されているためです。 したがって、ファイルの動作はブロック リストによって変更または上書きされません。 廃棄は、キャッシュがポリシー内の時刻に従って期限切れになり、新しい検索が最初はリストに対して、次にクラウドに対して実行されたときに、変更されます。

削除の理由

ディレクトリから履歴データベース ファイルとキャッシュ データベース ファイルを削除すると、FireAMP サービスの再起動時に新しく作り直されます。 特定のケースでは、FireAMP ディレクトリからこれらのファイルを削除しなければならない場合があります。 たとえば、特定のファイルの単純なカスタム検出やアプリケーション ブロック リストをテストする場合です。

データベースが破損して、データベース内の検出を開いたり表示することができなくなる可能性があります。 また、システムのデータベースが破損した場合は、FireAMP Connector サービス内でコネクタの起動不能やシステム全体のパフォーマンスの低下などのエラーが発生する可能性があります。 このようなケースでは、コネクタから履歴ファイルを消去することにより、破損が原因のパフォーマンス関連の問題を回避し、診断用の新しいログをキャプチャすることができます。

データベース ファイルの特定

Microsoft Windows で、これらのファイルは C:\Program Files\Sourcefire\fireAMP か C:\Program Files\Cisco\AMP に一般的にあります。

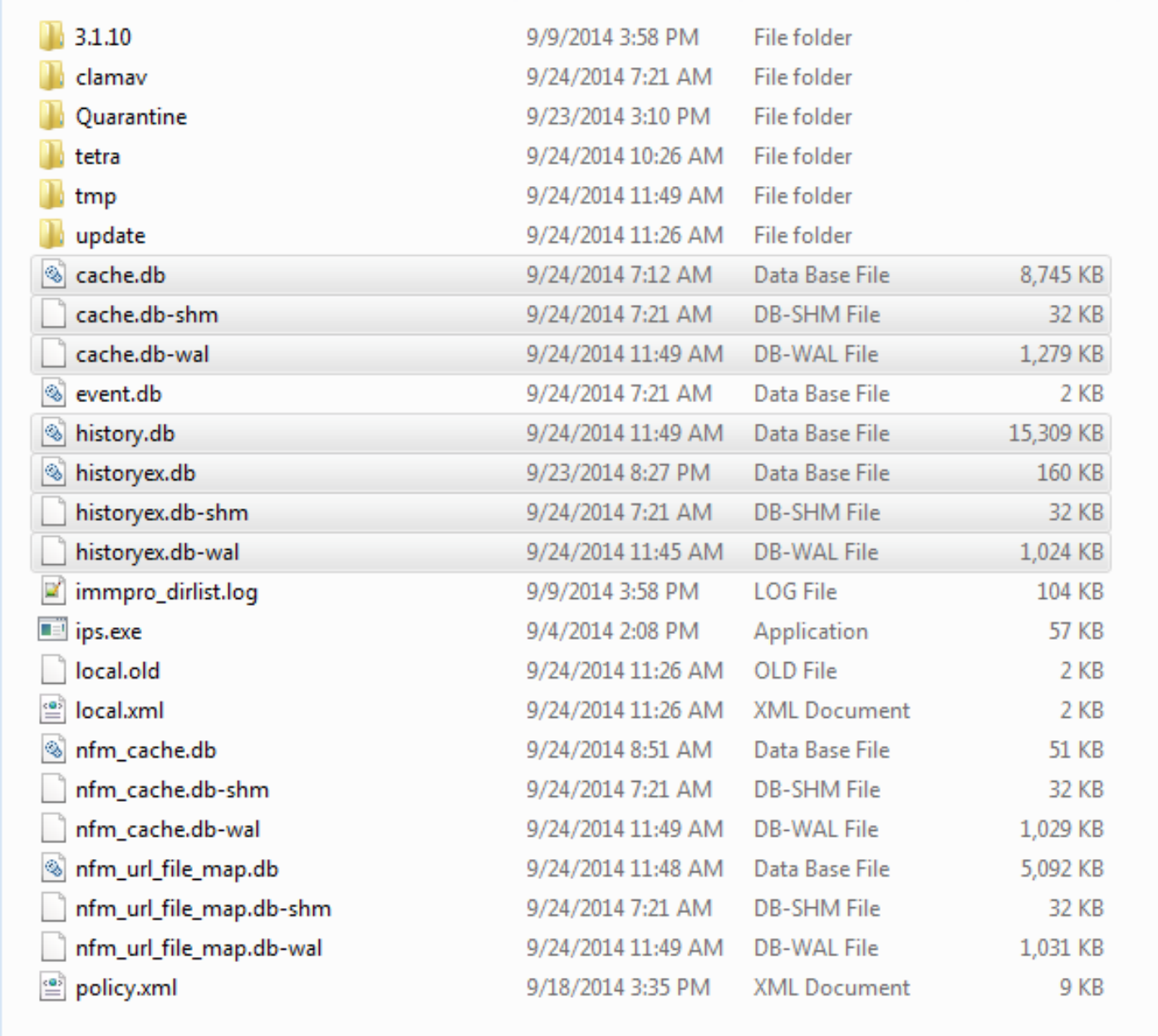
キャッシュ データベース ファイルの名前は次のとおりです。

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

履歴データベース ファイルの名前は次のとおりです。

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

このスクリーンショットは、Windows エクスプローラ上のファイルを示しています。



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

データベース ファイルの削除手順

ステップ 1： FireAMP Connector サービスの停止

FireAMP Connector サービスはさまざまな方法で停止することができます。

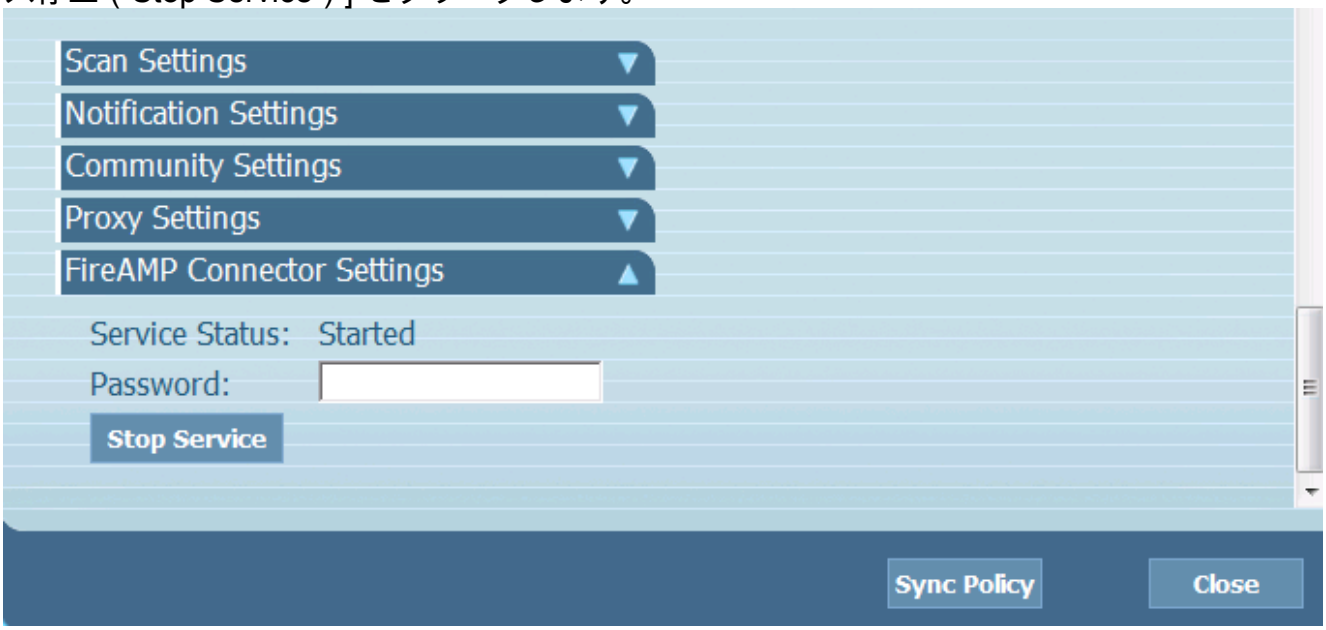
- FireAMP Connector サービスのユーザ インターフェイス (UI)
- Windows サービス コンソール
- 管理者のコマンド プロンプト

ユーザ インターフェイス

> **注:** コネクタ保護が有効になっている場合は、UI を使用して FireAMP Connector サービスを停止する必要があります。

1. トレイから UI を開いて、[設定 (Settings)] をクリックします。

2. 一番下までスクロールして、[FireAMP Connector設定（FireAMP Connector Settings）] を展開します。
3. [パスワード（Password）] フィールドに、コネクタ保護パスワードを入力します。 [サービス停止（Stop Service）] をクリックします。

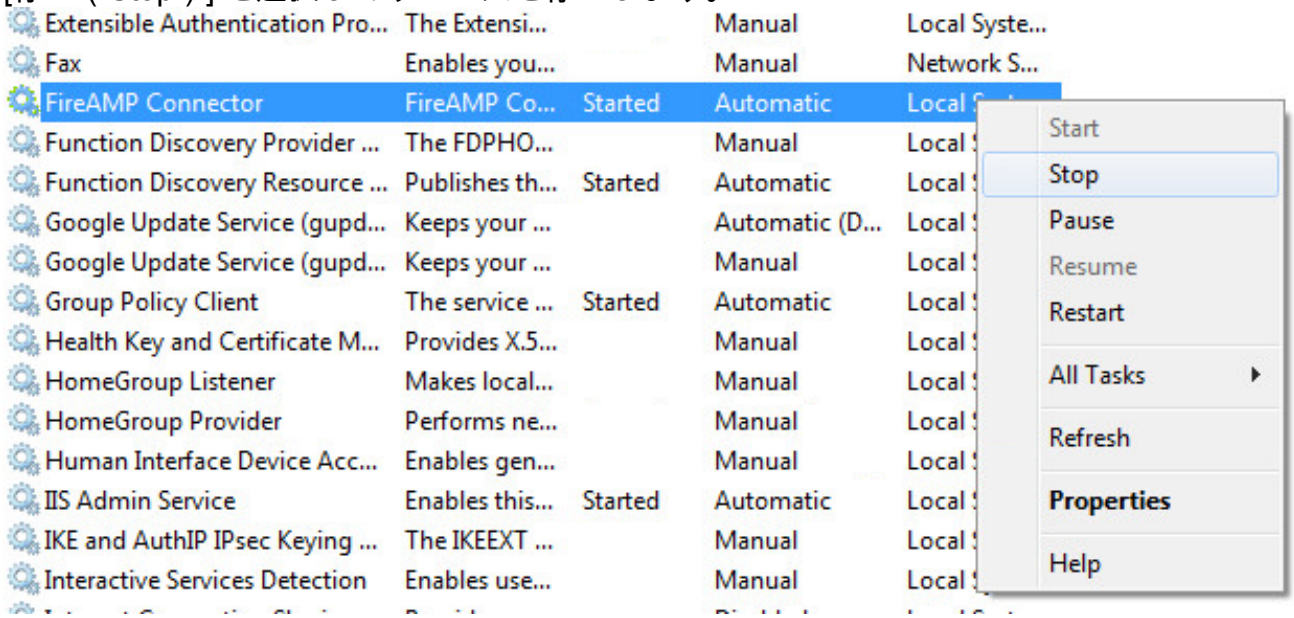


サービス コンソール

注: サービス コンソールでサービスを停止して開始するには、管理者権限が必要です。

サービス コンソールから FireAMP Connector サービスを停止するには、次の手順を実行します。

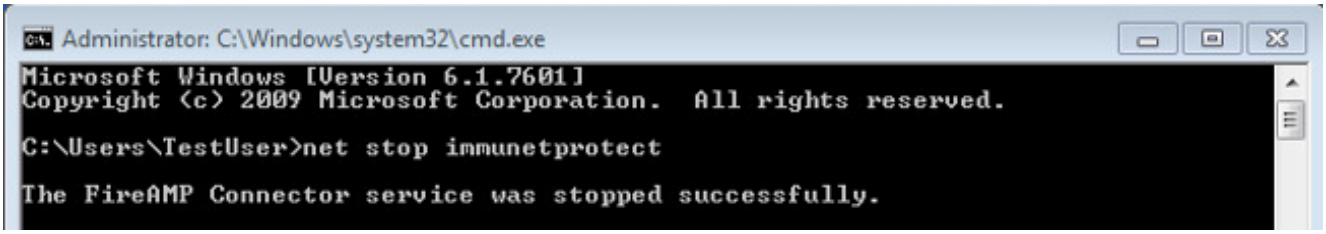
1. [スタート（Start）] メニューに移動します。
2. 「**services.msc**」と入力して、**Enter** キーを押します。 サービス コンソールが開きます。
3. [FireAMP Connector] サービスを選択して、サービス名を右クリックします。
4. [停止（Stop）] を選択してサービスを停止します。



コマンド プロンプト

管理者のコマンド プロンプトから FireAMP Connector サービスを停止するには、次の手順を実行します。

1. [スタート（Start）] メニューに移動します。
2. 「**cmd.exe**」と入力して、**Enter** キーを押します。 コマンド プロンプト ウィンドウが開きます。
3. **net stop immunetprotect** コマンドを入力します。 バージョン 5.0.1 または それ 以降がある場合、**immunetprotect%」」コール startservice 「のような「が名前**代りに命じる **wmic サービスを**入力して下さい。 このスクリーンショットは、正常に停止されたサービスの例を示しています。



ステップ 2： 必要なデータベース ファイルの削除

キャッシュ データベース ファイル

サービスが停止したら、次の 3 つのキャッシュ ファイルを削除できます。

> **警告**： 関連するキャッシュ データベース ファイルのすべてを削除しなかった場合は、再作成されたデータベースのキャッシング問題が発生する可能性があります。 その場合は、サービスが開始しないか、サービスのパフォーマンスが低下する可能性があります。

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

履歴データベース ファイル

サービスが停止したら、次の履歴データベース ファイルを削除します。

> **警告**： 関連する履歴データベース ファイルのすべてを削除しなかった場合は、再作成されたデータベースのキャッシング問題が発生する可能性があります。 その場合は、サービスが開始しないか、サービスのパフォーマンスが低下する可能性があります。

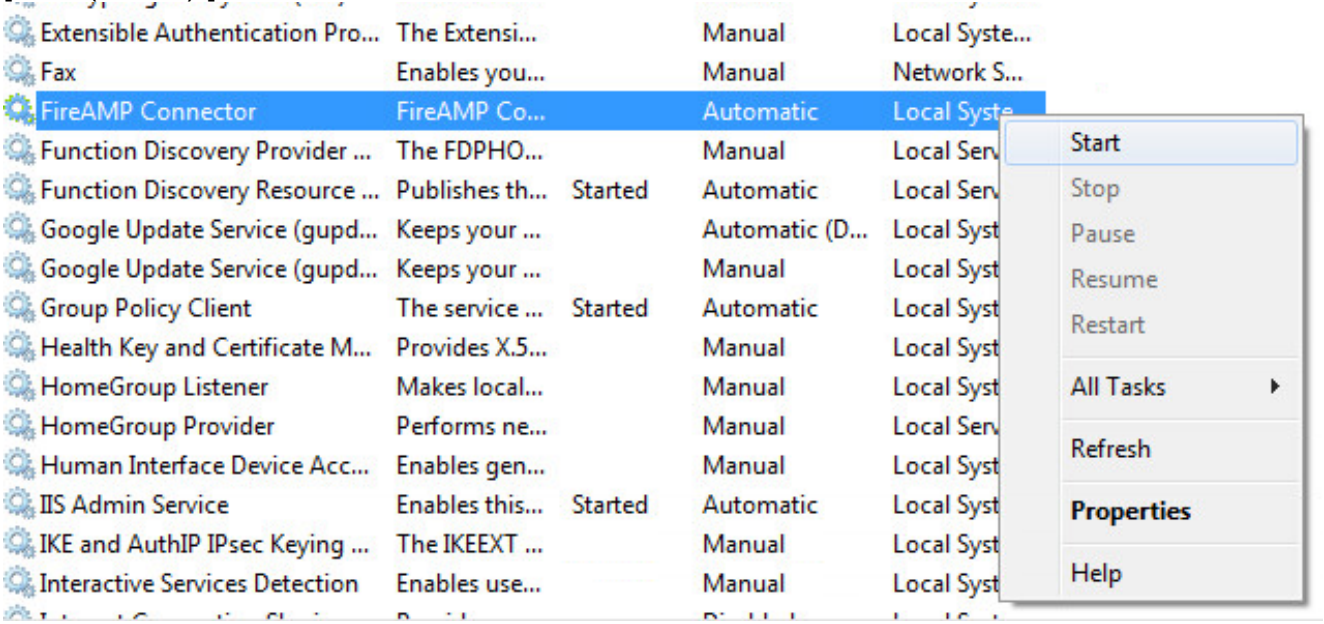
```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

ステップ3： FireAMP Connector サービスの開始

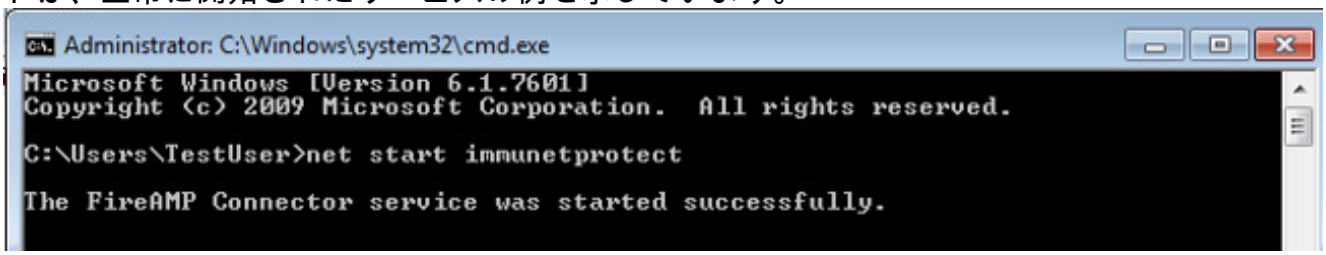
FireAMP Connector サービスを開始するには、次の手順を実行します。

1. [スタート（Start）] メニューに移動します。
2. 「**services.msc**」と入力して、**Enter** キーを押します。 サービス コンソールが開きます。

3. [FireAMP Connector] サービスを選択して、サービス名を右クリックします。
4. [開始 (Start)] を選択してサービスを開始します。



または、管理者のコマンド プロンプトで、net start immunetprotect コマンドを入力します。 バージョン 5.0.1 または それ 以降がある場合、immunetprotect%」」コール startservice「のような「が名前代りに命じる wmic サービスを入力して下さい。このスクリーンショットは、正常に開始されたサービスの例を示しています。



サービスが再起動したら、新しいデータベース ファイルのセットが作成されます。 これで、現在のホワイト リスト、ブロック リスト、除外などを含む FireAMP Connector の新しいインスタンスが表示されるはずです。