Verwijdering van de FireAMP-bestanden en de historie-bestanden op Windows

Inhoud

Inleiding

Dit document bevat een aantal scenario's die een verwijdering van gegevensbestanden in FireAMP voor endpoints vereisen en een geschikte procedure om deze indien nodig te verwijderen. FireAMP for Endpoints houdt een register bij van de recente bestandsdetecties en -bepalingen in databases. In bepaalde gevallen kan een Cisco Support Engineer u vragen om een aantal van de databases te verwijderen om een probleem op te lossen.

> **Waarschuwing**: U kunt een databases alleen verwijderen als u hiervoor instructies hebt gekregen van Cisco Technical Support.

Databasesbestanden voor cache en geschiedenis

doel

De cache database bestanden behouden de bekende disposities voor bestanden. De historiebestanden volgen alle FireAMP bestanddetectie, samen met bronbestandsnamen en SHA256-waarden.

Wanneer u een bloklijst aan een beleid toevoegt en de connector bijwerkt, verandert het gedrag voor een bepaald bestand niet direct. Dit komt doordat de cache al heeft geïdentificeerd dat het bestand niet kwaadaardig is. Als zodanig wordt de lijst niet gewijzigd of overschreven door de lijst met geblokkeerde bestanden. De dispositie verandert wanneer het cache per het tijdstip in uw beleid is verlopen en een nieuwe raadpleging wordt uitgevoerd - eerst tegen uw lijsten en daarna

tegen de cloud.

Redenen voor verwijdering

Als de geschiedenis database en cache database bestanden uit een folder worden verwijderd, worden ze opnieuw gecreëerd wanneer de FireAMP service opnieuw start. In bepaalde gevallen kan het nodig zijn om deze bestanden uit de FireAMP-map te verwijderen. Bijvoorbeeld, als u een eenvoudige douanedetectie of een toepassingsbloklijst voor een bepaald bestand wilt testen.

Het is mogelijk dat een database corrupt wordt, waardoor u de detecties in een database niet kunt openen of bekijken. Als de database daarentegen corrupt is op een systeem, kan deze fouten veroorzaken in de FireAMP-connector, zoals het onvermogen om de connector te starten of de algehele systeemprestaties achteruit te gaan. In deze gevallen kunt u de historie-bestanden van de connector wissen, zodat u prestatiegerelateerde problemen van corruptie kunt voorkomen en u nieuwe logbestanden voor diagnose kunt opnemen.

De databases identificeren

Op Microsoft Windows bevinden deze bestanden zich doorgaans op C:\Program Files\Sourcefire\fireAMP or C:\Program Files\Cisco\AMP.

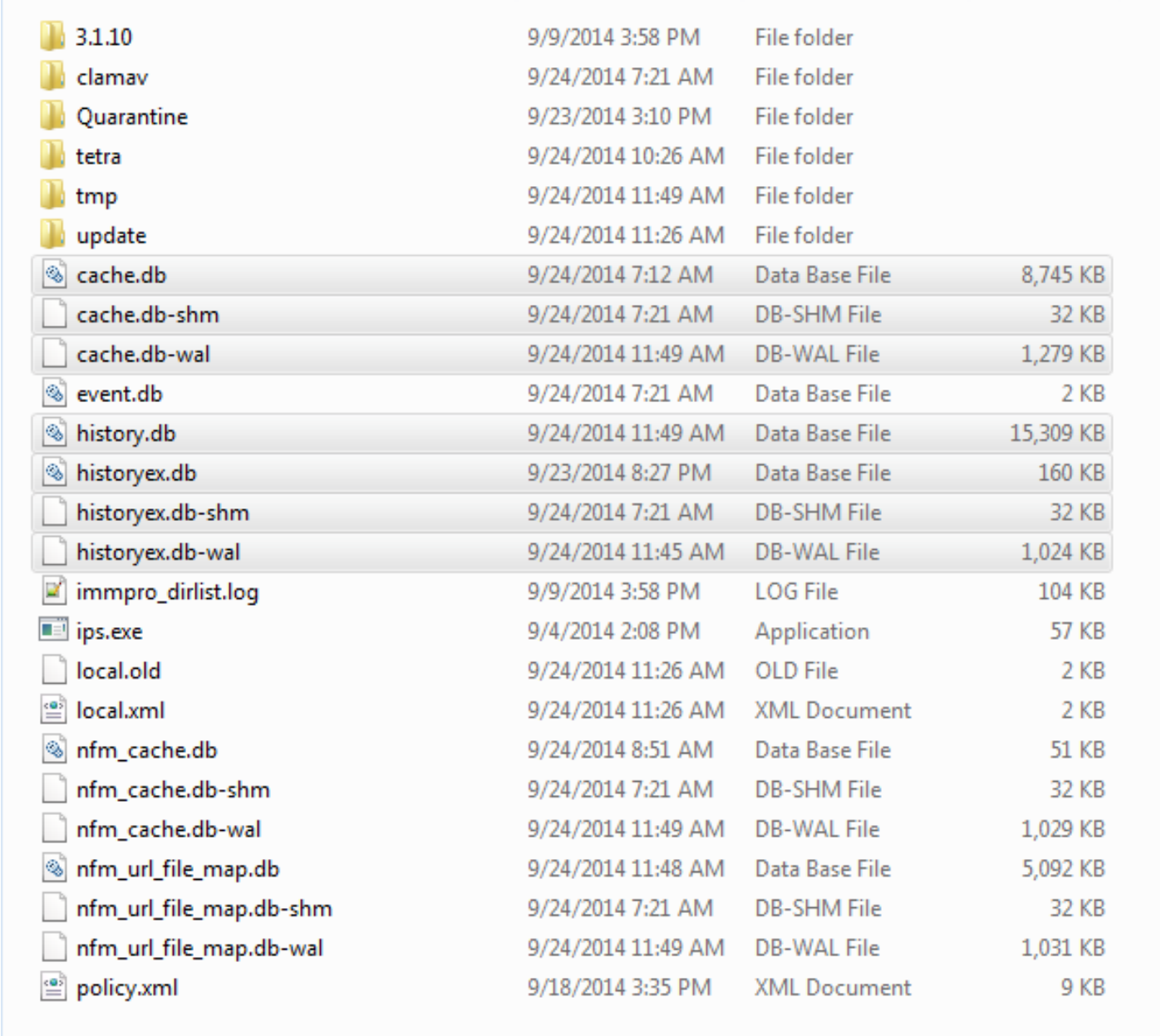
De naam van de cache database bestanden is:

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

De naam van de bestanden met historische databases is:

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

Dit screenshot toont de bestanden in 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

Procedure om databases te verwijderen

Stap 1: Stop de FirePOWER-connector

U kunt de FirePOWER-connector op verschillende manieren stopzetten:

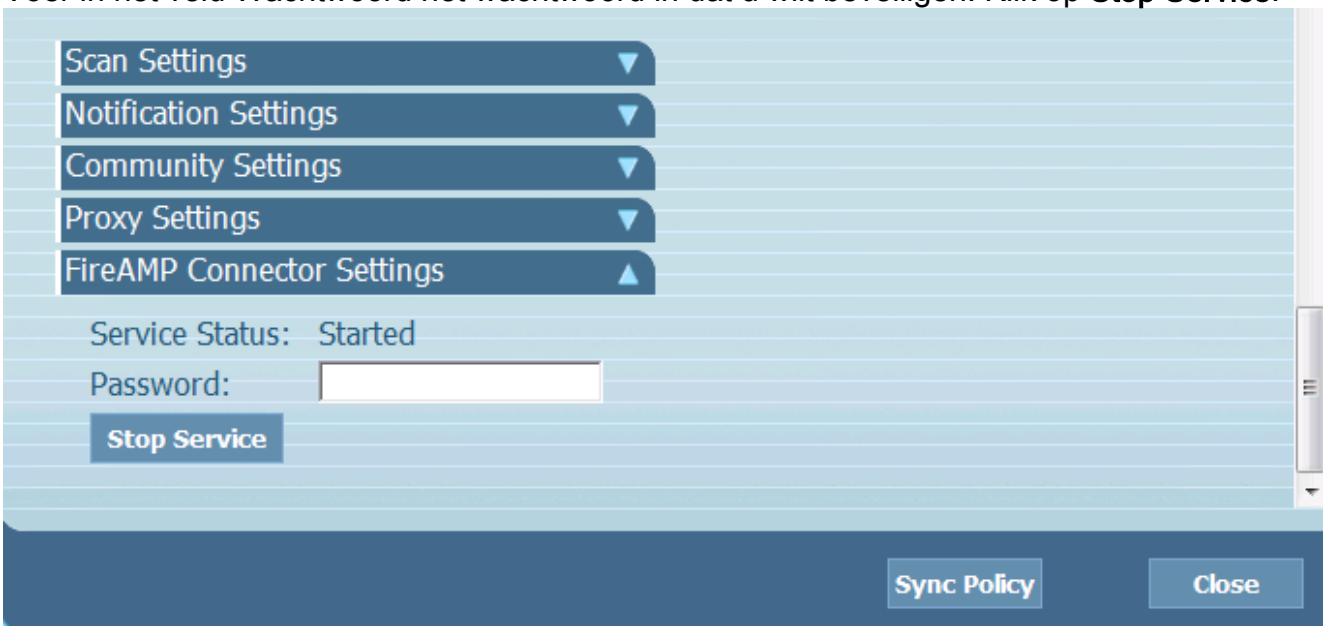
- Gebruikersinterface (UI) van de FireAMP-connector
- Windows-servicesconsole
- opdrachtmelding van de beheerder

Gebruikersinterface

> Opmerking: Als u verbindingsbescherming hebt ingeschakeld, moet u de UI gebruiken om de FireAMP Connector service te stoppen.

1. Open de UI uit het dienblad en klik op **Instellingen**.

2. Scrolt naar de onderkant en breid **FireAMP Connector - instellingen uit**.
3. Voer in het veld Wachtwoord het wachtwoord in dat u wilt beveiligen. Klik op **Stop Service**.

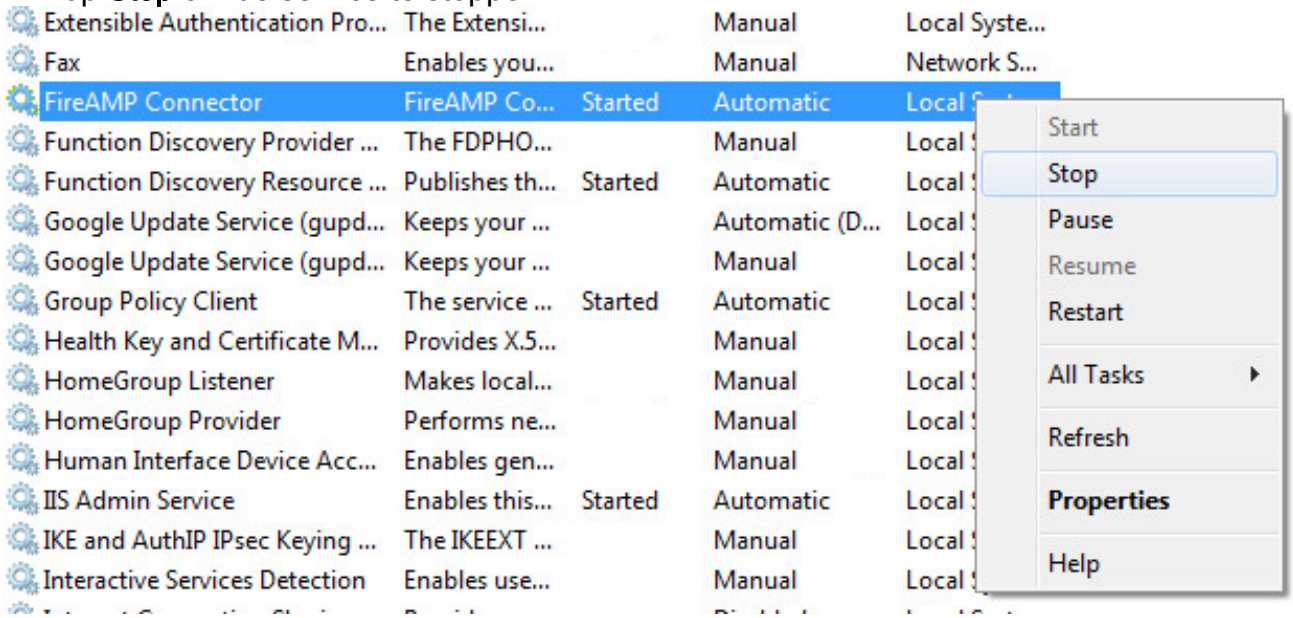


Servicesconsole

> Opmerking: Om de services in de servicesconsole te stoppen en te starten hebt u Administrator-rechten nodig.

Voltooi de volgende stappen om de FireAMP Connector vanuit de servicesconsole te stoppen:

1. Navigeer naar het **menu Start**.
2. Voer **services.msc in** en druk op **Voer in**. De servicesconsole wordt geopend.
3. Selecteer de **FirePOWER-**connector en klik met de rechtermuisknop op de servicenaam.
4. Klik op **Stop** om de service te stoppen.

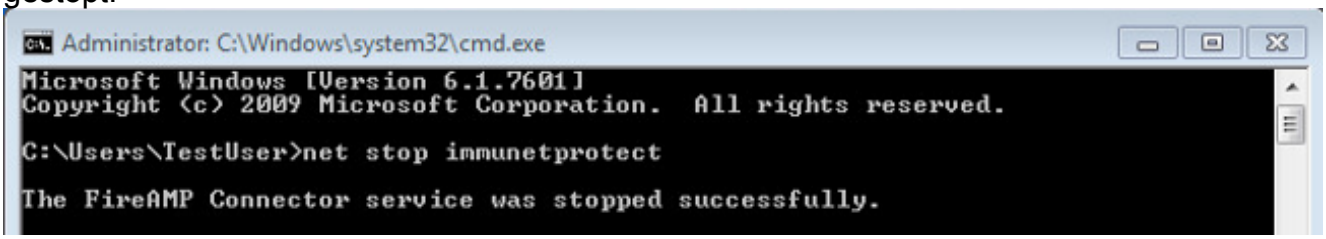


Opdrachtmelding

Voltooi de volgende stappen om de FireAMP Connector vanuit de opdrachtmelding van een

beheerder te stoppen:

1. Navigeer naar het **menu Start**.
2. Voer **cmd.exe in** en druk op **ENTER**. Er wordt een venster met de opdrachtmelding geopend.
3. Typ de opdracht **Stop immunetprotection**. Indien u versie 5.0.1 of hoger heeft, dient u de **wmic-service in te** voeren **waarbij "naam als 'immunetprotection%'" de** opdracht **startservice** inplaats daarvan **belt**. Dit screenshot toont een voorbeeld van de service die is gestopt:



Stap 2: De gewenste databases verwijderen

Databasesopieën

Nadat de service is stopgezet, kunt u deze drie cache bestanden verwijderen:

> **Waarschuwing**: Als u niet alle verwante cache-bestanden verwijdert, kan het caching-problemen met de herkende database creëren. Als u dit wel doet, kan de service niet starten of u kunt bij de service minder goed werken.

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

Databasestbestanden

Nadat de service is gestopt, verwijdert u deze bestanden uit de historie van de database:

> **Waarschuwing**: Als u niet alle verwante historie-gegevensbestanden verwijdert, kunt u caching-kwesties maken met de herkende database. Als u dit wel doet, kan de service niet starten of u kunt bij de service minder goed werken.

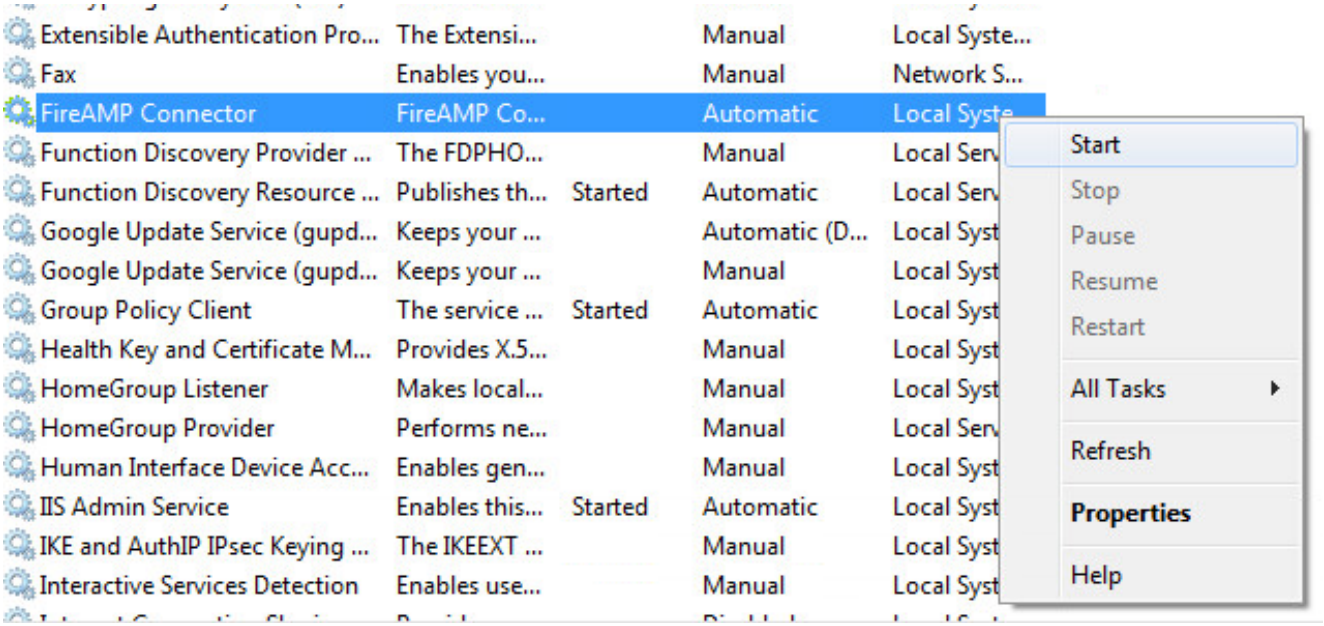
```
history.db
historyex.db
historyex.db-shm
historyex.db-wal
```

Stap 3: Start de FirePOWER-connector

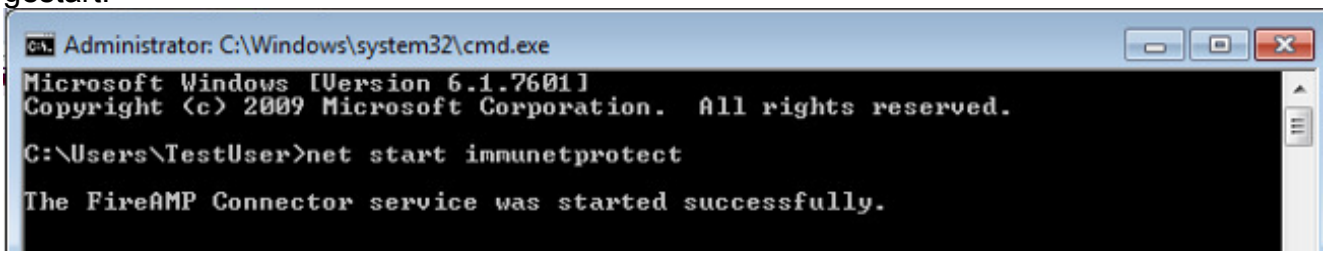
Voltooi de volgende stappen om de FireAMP-connector te starten:

1. Navigeer naar het **menu Start**.
2. Voer **services.msc in** en druk op **Voer in**. De servicesconsole wordt geopend.
3. Kies de FirePOWER-connector en klik met de rechtermuisknop op de servicenaam.

4. Kies **Start** om de service te starten.



U kunt ook de opdracht **immunetProtection** (**netto-start-**beveiliging) **invoeren** in de opdrachtmelding van de beheerder. Indien u versie 5.0.1 of hoger heeft, dient u de **wmic-service in te** voeren **waarbij "naam als 'immunetprotection%'" de** opdracht **startservice** inplaats daarvan **belt**.Dit screenshot toont een voorbeeld van de service die met succes is gestart:



Nadat u de services opnieuw hebt gestart, wordt er een nieuwe set databases aangemaakt. Dit zou u nu van een nieuw exemplaar van de FireAMP Connector moeten voorzien van huidige witte lijsten, bloklijsten, uitsluitingen, etc.