إزالة ذاكرة التخزين المؤقت لـ FireAMP وملفات المحفوظات على Windows

المحتويات

المقدمة

يقدم هذا المستند بعض السيناريوهات التي تتطلب إزالة ملفات قاعدة البيانات في FireAMP لنقاط النهاية ويصف الإجراء المناسب لإزالتها عند الضرورة. يحتفظ FireAMP for Endpoints بسجل لآخر عمليات الكشف عن الملفات والتصرف فيها في ملفات قاعدة البيانات. في حالات معينة، قد يطلب منك مهندس دعم Cisco إزالة بعض ملفات قاعدة البيانات لاستكشاف أخطاء إحدى المشاكل وإصلاحها.

تحذير: يمكنك إزالة ملف قاعدة بيانات فقط إذا تم توجيهه بواسطة دعم Cisco الفني.

ملفات قاعدة البيانات الخاصة بالذاكرة المؤقتة والمحفوظات

الغرض

تحافظ ملفات قاعدة بيانات التخزين المؤقت على عمليات التوزيع المعروفة للملفات. تقوم ملفات قاعدة بيانات المحفوظات بتعقب كل عمليات الكشف عن ملفات FireAMP، بالإضافة إلى أسماء الملفات المصدر وقيم SHA256.

عند إضافة قائمة حظر إلى نهج وتحديث الموصل، لا يتغير سلوك الملف المحدد فورا. وذلك لأن ذاكرة التخزين المؤقت قد حددت بالفعل أن الملف غير ضار. على هذا النحو، لن يتم تغييره أو تجاوزه من قبل قائمة الحظر الخاصة بك. يتغير المصير النهائي عند انتهاء صلاحية ذاكرة التخزين المؤقت في كل وقت من النهج ويتم إجراء بحث جديد - أولا مقابل قوائمك ثم بعد ذلك مقابل مجموعة النظراء.

أسباب الازالة

إذا تمت إزالة ملفات قاعدة بيانات المحفوظات وقاعدة بيانات ذاكرة التخزين المؤقت من دليل، فإنه يتم إعادة إنشائها

مرة أخرى عند إعادة تشغيل خدمة FireAMP. في حالات معينة، قد يكون من الضروري إزالة هذه الملفات من دليل FireAMP. على سبيل المثال، إذا كنت تريد إختبار كشف مخصص بسيط أو قائمة حظر تطبيق لملف معين.

من المحتمل أن تصبح قاعدة البيانات تالفة، مما يؤدي إلى تعذر فتح عمليات الكشف في قاعدة بيانات أو عرضها. بدلا من ذلك، إذا كانت قاعدة البيانات تالفة على نظام ما، فقد يؤدي ذلك إلى حدوث أخطاء داخل خدمة "موصل FireAMP" مثل عدم القدرة على بدء الموصل أو انخفاض أداء النظام الإجمالي. في هذه الحالات، قد ترغب في مسح ملفات المحفوظات من الموصل بحيث يمكنك تجنب المشاكل المتعلقة بالأداء من الفساد والتمكن من التقاط سجلات جديدة للتشخيص.

التعرف على ملفات قاعدة البيانات

في Microsoft Windows، توجد هذه الملفات عادة في C:\Program Files\Sourcefire\fireAMP أو C:\Program Files\Cisco\AMP.

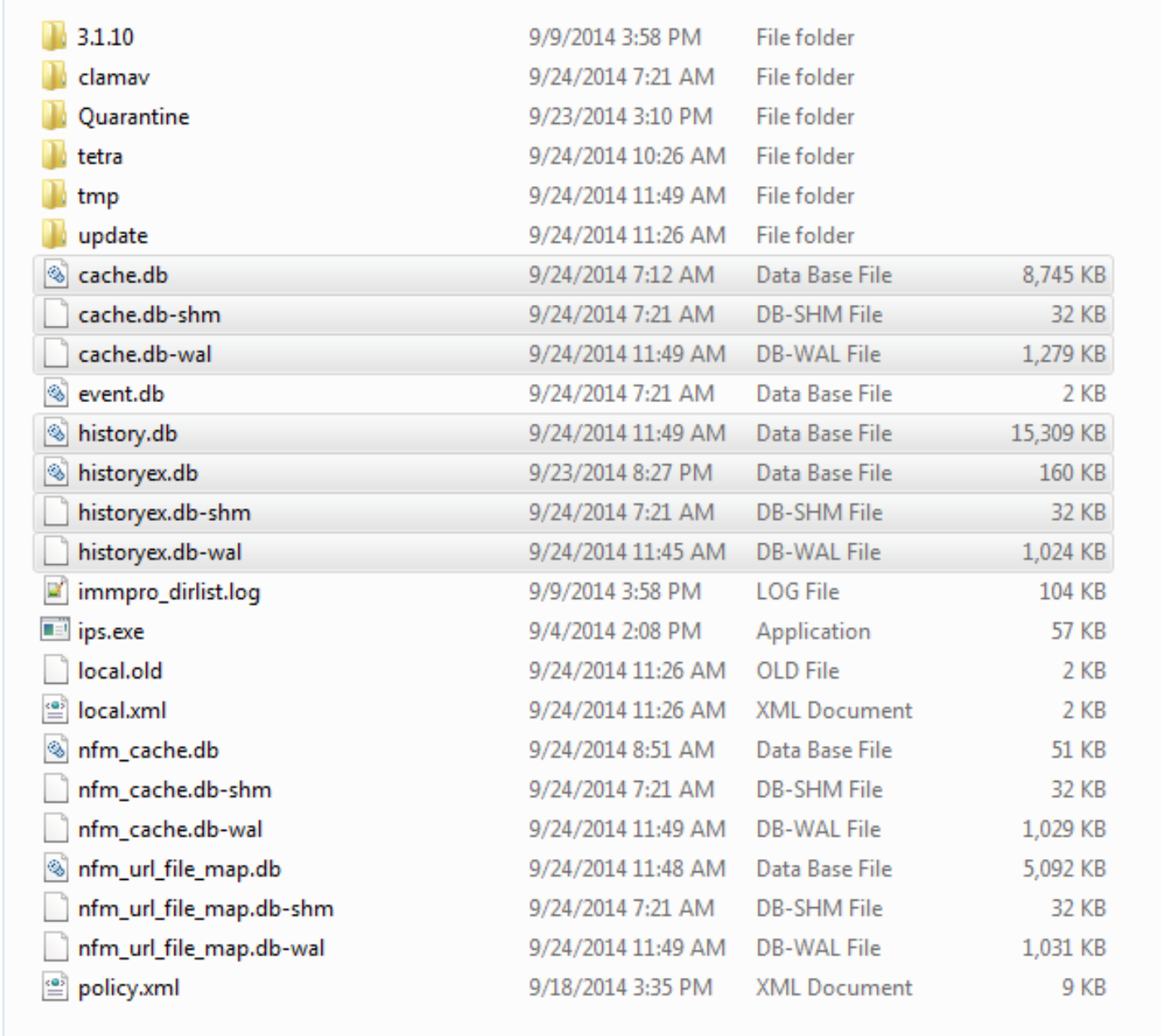
اسم ملفات قاعدة بيانات التخزين المؤقت هو:

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

اسم ملفات قاعدة بيانات المحفوظات هو:

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

توضح لقطة الشاشة هذه الملفات الموجودة على "مستكشف ملفات Windows":



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

إجراء إزالة ملفات قاعدة البيانات

الخطوة 1: إيقاف خدمة موصل FireAMP

يمكنك إيقاف خدمة موصل FireAMP بطرق مختلفة:

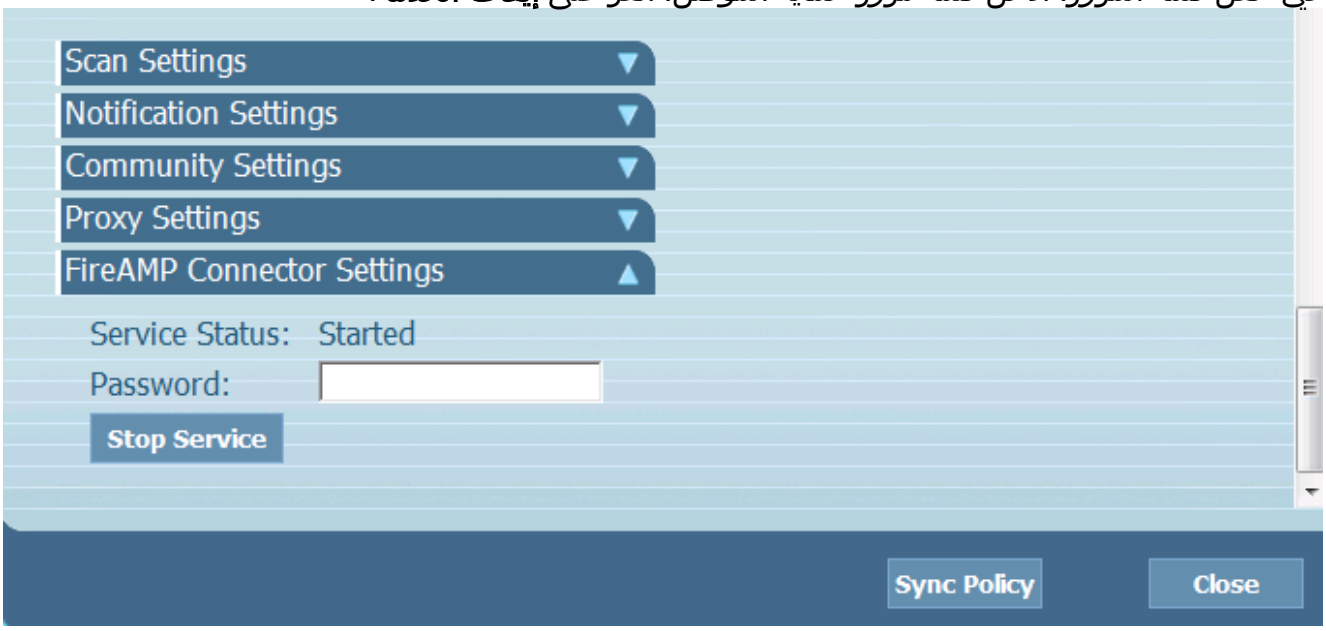
- واجهة المستخدم (UI) الخاصة بخدمة موصل FireAMP
- وحدة التحكم في خدمات Windows
- موجه أوامر المسؤول

واجهة المستخدم

ملاحظة: إذا كانت لديك حماية الموصل ممكنة، فيجب إستخدام واجهة المستخدم لإيقاف خدمة موصل FireAMP.

1. افتح واجهة المستخدم من الدرج وانقر فوق **إعدادات**.

2. قم بالتمرير إلى الأسفل **وقم** بتوسيع **إعدادات موصل FireAMP**.
3. في حقل كلمة المرور، أدخل كلمة مرور حماية الموصل. انقر على **إيقاف الخدمة**.

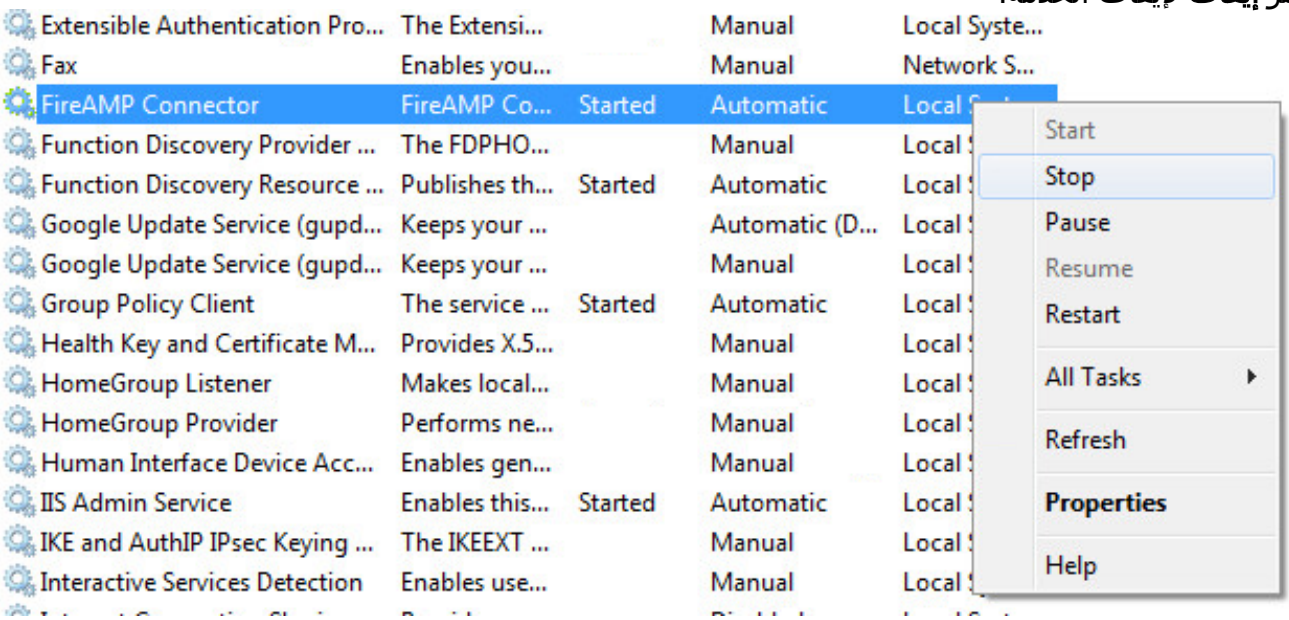


وحدة التحكم في الخدمات

ملاحظة: لإيقاف الخدمات وبدء تشغيلها في وحدة تحكم الخدمات، تحتاج إلى امتيازات المسؤول.

لإيقاف خدمة FireAMP Connector من وحدة تحكم الخدمات، أكمل الخطوات التالية:

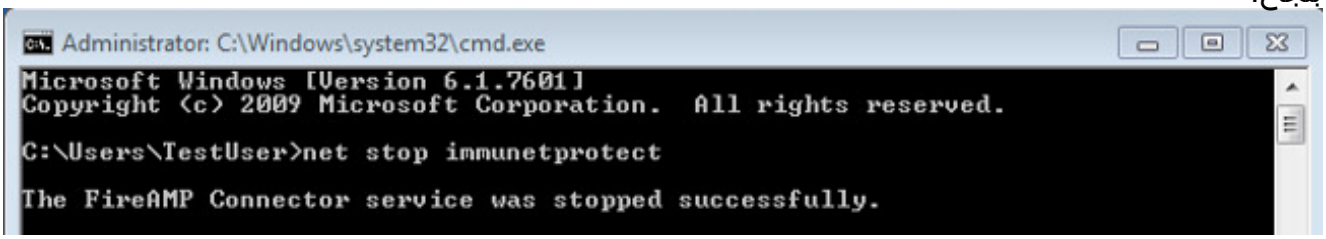
1. انتقل إلى **القائمة ابدأ**.
2. أدخل **services.msc** ثم اضغط على مفتاح **Enter**. يتم فتح وحدة التحكم في الخدمات.
3. حدد خدمة **موصل FireAMP** وانقر بزر الماوس الأيمن فوق اسم الخدمة.
4. أختر **إيقاف** لإيقاف الخدمة.



موجه الأوامر

لإيقاف خدمة FireAMP Connector من موجه أوامر المسؤول، أكمل الخطوات التالية:

1. انتقل إلى **القائمة ابدأ**.
2. أدخل **cmd.exe** واضغط **Enter**. يتم فتح نافذة موجه الأوامر.
3. أدخل الأمر **net stop immunetprotect**. إذا كان لديك الإصدار 5.0.1 أو إصدار أحدث، فأدخل **خدمة WMIC** **حيث** أمر **إستدعاء** **startupService** بدلا **من ذلك** باسم **مثل 'emetprotect٪'**. توضح لقطة الشاشة هذه مثالا على الخدمة التي تم إيقافها بنجاح:



الخطوة 2: حذف ملفات قاعدة البيانات المطلوبة

تخزين ملفات قاعدة البيانات مؤقتا

بمجرد إيقاف الخدمة يمكنك حذف ملفات التخزين المؤقت الثلاثة هذه:

تحذير: إذا لم تقم بحذف كافة ملفات قاعدة بيانات ذاكرة التخزين المؤقت ذات الصلة، فيمكن إنشاء مشاكل التخزين المؤقت لقاعدة البيانات التي تمت إعادة إنشائها. وعلى هذا النحو، قد تفشل الخدمة في بدء التشغيل أو قد تواجه أداء متدنيا من الخدمة.

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

ملفات قاعدة بيانات المحفوظات

بمجرد إيقاف الخدمة، قم بإزالة ملفات قاعدة بيانات المحفوظات هذه:

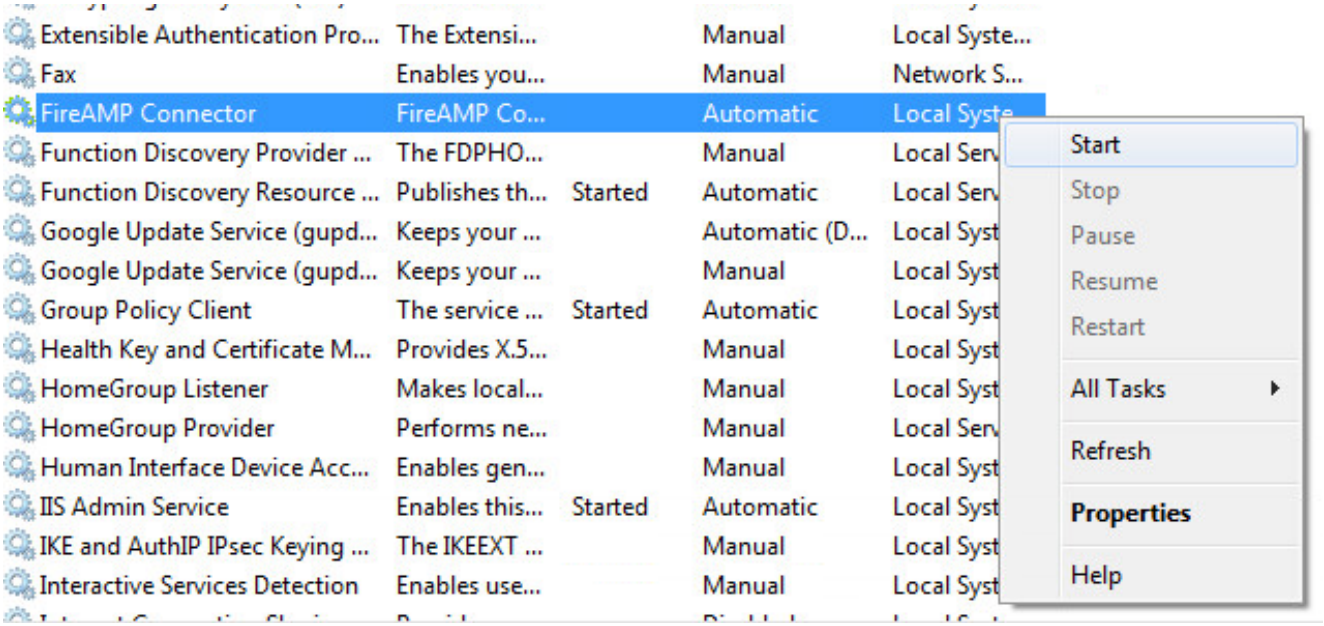
تحذير: إذا لم تقم بحذف كافة ملفات قاعدة بيانات المحفوظات ذات الصلة، فيمكن إنشاء مشاكل التخزين المؤقت لقاعدة البيانات التي تمت إعادة إنشائها. وعلى هذا النحو، قد تفشل الخدمة في بدء التشغيل أو قد تواجه أداء متدنيا من الخدمة.

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

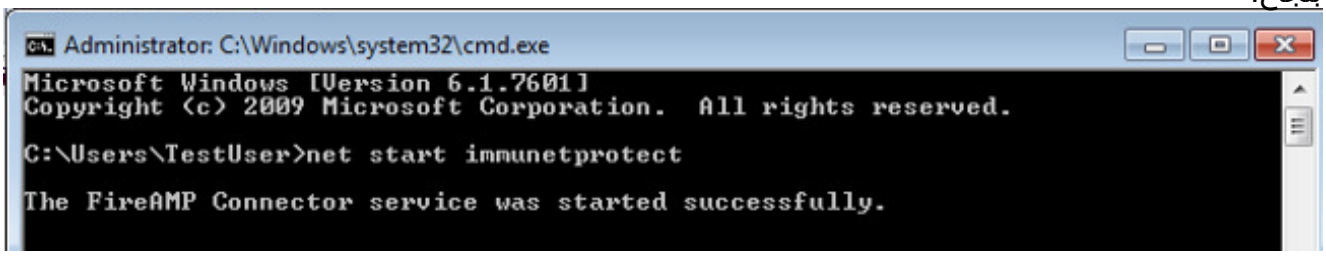
الخطوة 3: بدء تشغيل خدمة موصل FireAMP

لبدء تشغيل خدمة موصل FireAMP، أكمل الخطوات التالية:

1. انتقل إلى **القائمة ابدأ**.
2. أدخل **services.msc** ثم اضغط على مفتاح **Enter**. يتم فتح وحدة التحكم في الخدمات.
3. أختر خدمة **موصل FireAMP** وانقر بزر الماوس الأيمن فوق اسم الخدمة.
4. أختر **بدء** لبدء تشغيل الخدمة.



بدلا من ذلك، في موجه أوامر المسؤول، يمكنك إدخال الأمر **net start immunetprotect**. إذا كان لديك الإصدار 5.0.1 أو إصدار أحدث، فأدخل **خدمة WMIC حيث** أمر **إستدعاء startupService** بدلا **من ذلك** باسم **مثل 'emetprotect٪'**.توضح لقطة الشاشة هذه مثالا للخدمة التي تم بدء تشغيلها بنجاح:



بعد إعادة تشغيل الخدمات، يتم إنشاء مجموعة جديدة من ملفات قاعدة البيانات. يجب أن يوفر لك هذا الآن مثيل جديد لموصل FireAMP يحتوي على القوائم البيضاء الحالية وقوائم المنع والاستبعادات وما إلى ذلك.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).