أستكشاف أخطاء نقطة النهاية الآمنة التي عُلقت في العزل باستخدام أساليب الاسترداد وإصلاحها

المحتويات

المقدمة

يصف هذا المستند عملية إسترداد نقطة نهاية مع تثبيت موصل نقطة النهاية الآمنة من وضع العزل.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Secure Endpoint Connector
- وحدة التحكم في نقطة النهاية الآمنة
- ميزة عزل نقطة النهاية

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Secure Endpoint Console، الإصدار v5.4.2021092321
- Secure Endpoint Connector، الإصدار v7.4.5.20701

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت

شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يكون الإجراء الموضح في هذا المستند مفيدا في الحالات التي يكون فيها جهاز نقطة النهاية عالقا في هذه الحالة ولا يمكن تعطيل وضع العزل.

عزل نقطة النهاية هي ميزة تتيح لك حظر نشاط الشبكة (IN و OUT) على كمبيوتر Windows لمنع التهديدات مثل تصفية البيانات ونشر البرامج الضارة. وهو متوفر على إصدارات 64 بت من Windows التي تدعم الإصدار 7.0.5 والإصدارات الأحدث من الموصل.

تؤثر جلسات عزل نقطة النهاية على الاتصال بين موصل Windows وسحابة Cisco. هناك نفس مستوى الحماية والإمكانية الرؤية على نقاط النهاية الخاصة بك كما كان قبل الجلسة. يمكنك تكوين قوائم السماح بعزل IP للعناوين التي تجنب قيام الموصل بحظر عناوين IP المعنية أثناء تنشيط جلسة عزل نقطة النهاية النشطة. يمكنك مراجعة معلومات أكثر تفصيلا حول ميزة "عزل نقطة النهاية" هنا.

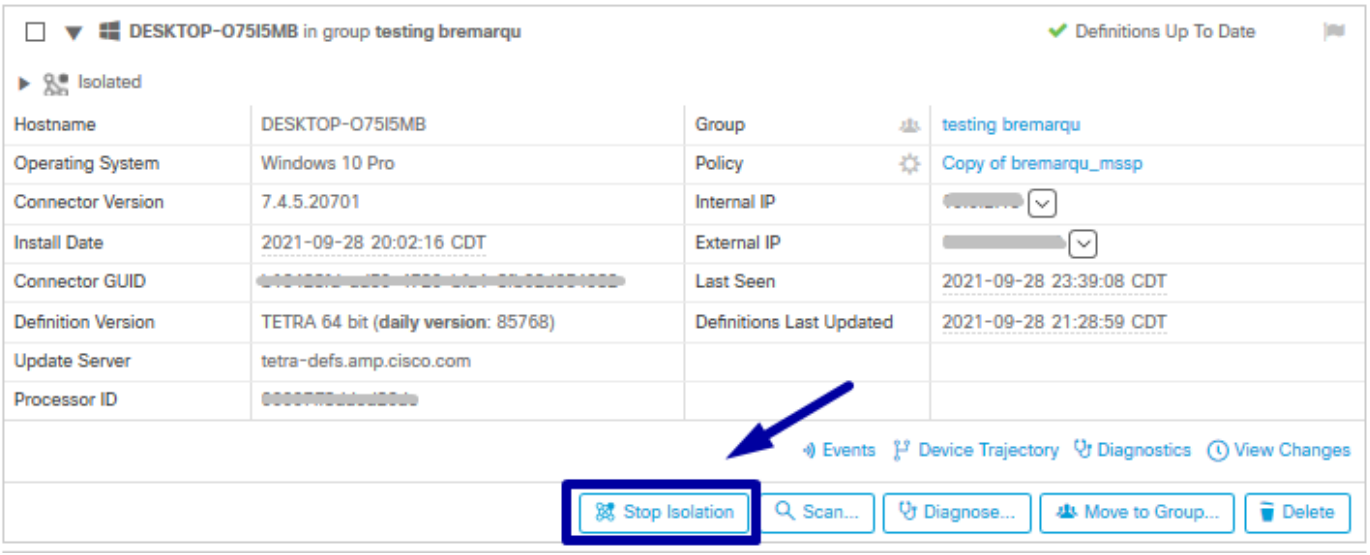
إيقاف العزل

بمجرد أن ترغب في إيقاف عزل نقطة النهاية على كمبيوتر ما، يمكنك اتباع هذه الخطوات السريعة من خلال وحدة تحكم نقطة النهاية الآمنة أو سطر الأوامر.

إيقاف جلسة عمل العزل من وحدة التحكم

لإيقاف جلسة عزل واستعادة كل حركة مرور الشبكة إلى نقطة نهاية.

الخطوة 1. في وحدة التحكم، انتقل إلى **الإدارة > أجهزة الكمبيوتر**.
الخطوة 2. حدد مكان الكمبيوتر الذي تريد إيقاف عزله وانقر لعرض التفاصيل.
الخطوة 3. انقر زر **إيقاف العزل**، كما هو موضح في الصورة.



الخطوة 4. أدخل أي تعليقات حول سبب إيقاف ميزة العزل على نقطة النهاية.

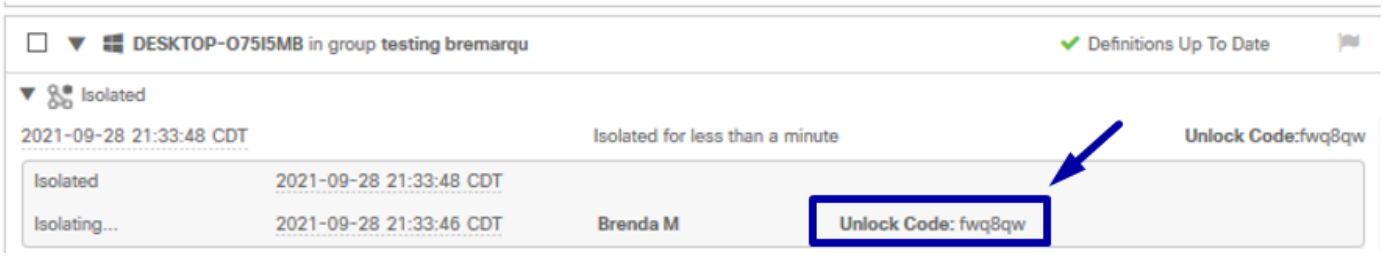
إيقاف جلسة العزل من سطر الأوامر

إذا فقدت نقطة نهاية معزولة إتصالها بسحابة Cisco، وتعجز عن إيقاف جلسة عمل العزل من وحدة التحكم. في هذه الحالات، أنت يستطيع أوقفت الجلسة محليا من الأمر خط مع ال unlock رمز.

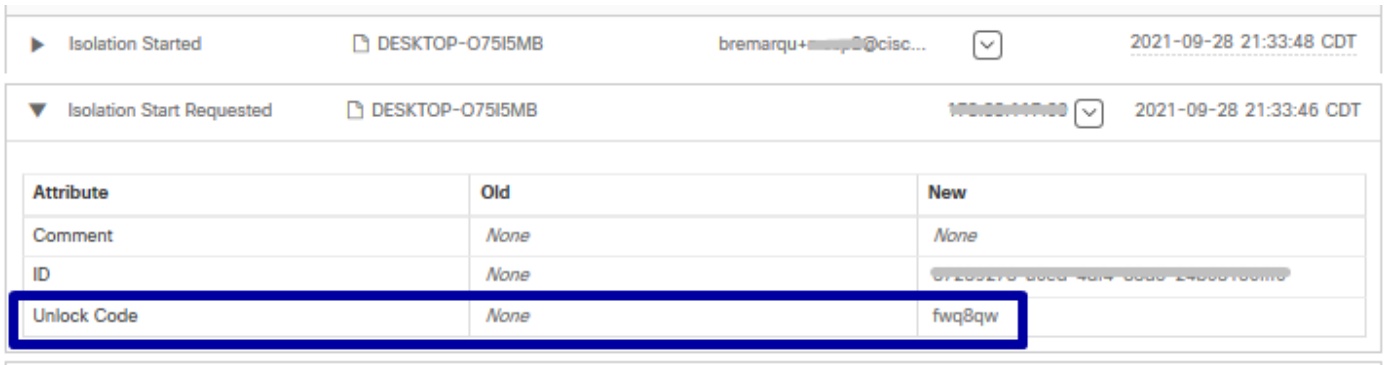
الخطوة 1. في وحدة التحكم، انتقل إلى **الإدارة > أجهزة الكمبيوتر**.

الخطوة 2. حدد مكان الكمبيوتر الذي تريد إيقاف عزله وانقر لعرض التفاصيل.

الخطوة 3. لاحظ **فك تأمين الرمز**، كما هو موضح في الصورة.



الخطوة 4. يمكنك أيضا العثور على **فك قفل الرمز** إذا قمت بالتنقل إلى **الحساب > سجل التدقيق**، كما هو موضح في الصورة.



الخطوة 5. على الكمبيوتر المعزول، افتح موجه أوامر بامتيازات المسؤول.

الخطوة 6. انتقل إلى الدليل الذي تم تثبيت الموصل فيه (C:\Program Files\Cisco\AMP\[رقم الإصدار]) وقم بتشغيل الأمر **sfc.exe -n [إلغاء تأمين الرمز]** كما هو موضح في الصورة.

```
sfc.exe -n [unlock code]
```

```
C:\Program Files\Cisco\AMP\7.4.5.20701>sfc.exe -n fwq8qw

C:\Program Files\Cisco\AMP\7.4.5.20701>
```

> **تحذير**: إذا تم إدخال رمز إلغاء التأمين بشكل غير صحيح 5 مرات، فمن الضروري الانتظار لمدة 30 دقيقة قبل إجراء محاولة إلغاء تأمين أخرى.

أستكشاف أخطاء الاسترداد وإصلاحها

في حالة استنفاد كافة المسارات ولا تزال غير قادر على إسترداد نقطة نهاية معزولة من وحدة تحكم نقطة النهاية الآمنة أو محليا باستخدام رمز إلغاء التأمين؛ يمكنك إسترداد

نقطة النهاية المعزولة باستخدام أسالیب إستردادالطوارئ.

إستعادة أسلوب العزل من سطر الأوامر

في الحالات التي يكون فيها جهاز نقطة النهاية الخاص بك عالقا في العزل والا يمكن تعطيل العزل عبر وحدة تحكم نقطة النهاية الآمنة أو باستخدام رمز إلغاء التأمين، يمكنك اتباع هذه الخطوات.

الخطوة 1. قم بإيقاف خدمة Connector عبر واجهة مستخدم الموصل أو **خدمات Windows**.

الخطوة 2. حدد موقع خدمة موصل نقطة النهاية الآمنة وأوقف الخدمة.

الخطوة 3. على الكمبيوتر المعزول، افتح موجه أوامر بامتيازات المسؤول.

الخطوة 4. قم بتشغيل الأمر **reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f** كما هو موضح في الصورة.

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
```

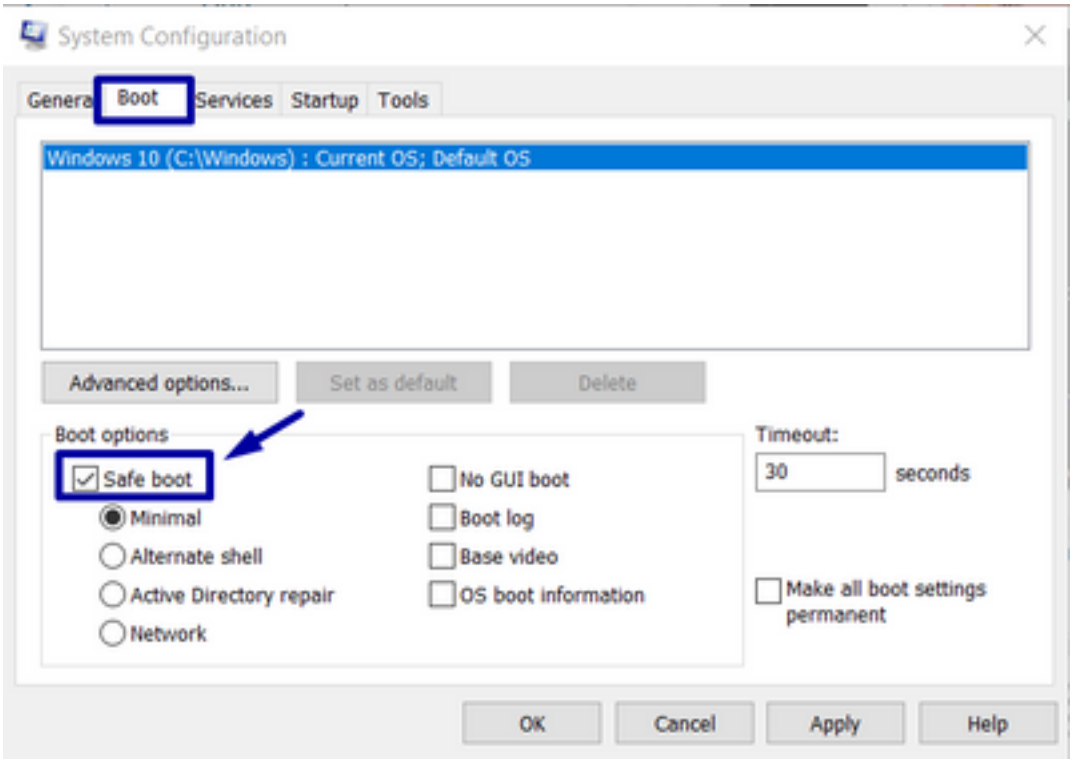
```
C:\Windows\system32>reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\Immunet Protect" /v "unlock_code" /f
The operation completed successfully.

C:\Windows\system32>
```

الخطوة 5. تشير الرسالة **التي اكتملت العملية بنجاح** إلى اكتمال العملية. (إذا تم عرض رسالة أخرى، كـ "خطأ: تم رفض الوصول"، يجب إيقاف خدمة موصل نقطة النهاية الآمنة قبل تشغيل الأمر).

الخطوة 6. بدء تشغيل خدمة موصل نقطة النهاية الآمنة.

> **تلميح**: إذا تعذر عليك إيقاف خدمة موصل نقطة النهاية الآمنة من واجهة المستخدم للموصل أو خدمات Windows، فيمكنك إجراء تمهيد آمن.

على نقطة النهاية المعزولة، انتقل إلى **تكوين النظام > تحميل > خيارات التمهيد** وحدد **التمهيد الآمن**، كما هو موضح في الصورة.

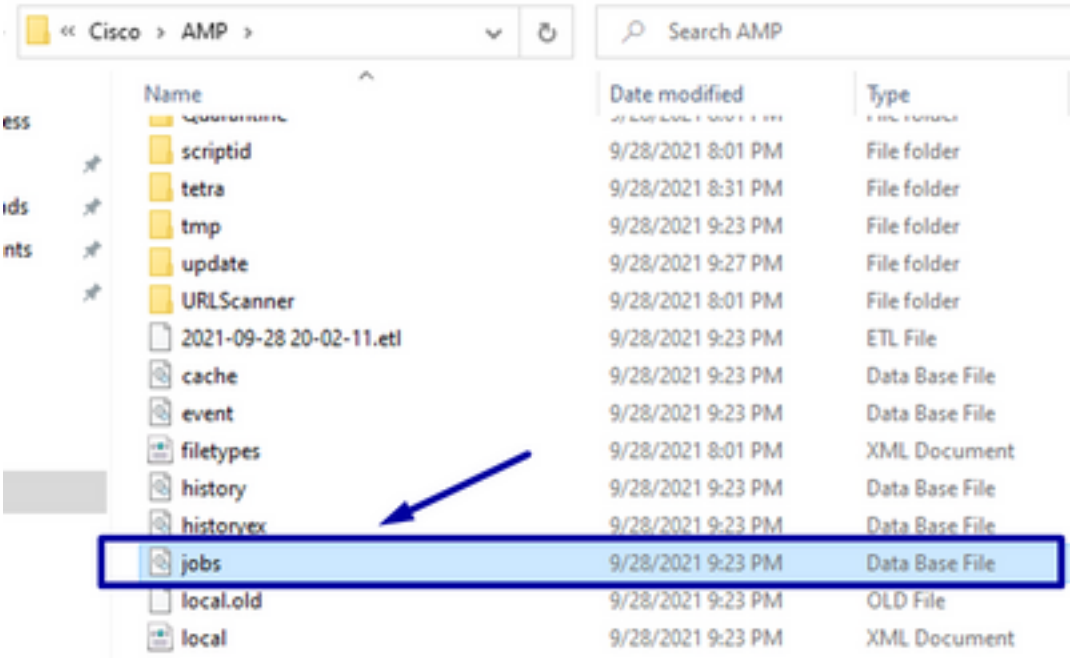


إستعادة أسلوب العزل بدون سطر الأوامر

في حالة توقف جهاز نقطة النهاية في العزل ويتعذر تعطيل العزل عبر وحدة تحكم نقطة النهاية الآمنة أو باستخدام رمز إلغاء التأمين أو حتى إذا تعذر عليك إستخدام سطر الأوامر، يمكنك اتباع الخطوات التالية:

الخطوة 1. قم بإيقاف خدمة Connector عبر واجهة مستخدم الموصل أو **خدمات Windows**.

الخطوة 2. انتقل إلى الدليل الذي تم تثبيت الموصل فيه (C:\Program Files\Cisco\AMP\) واحذف **وظائف** الملف.db، كما هو موضح في الصورة.



3. قم بإعادة تشغيل الكمبيوتر.

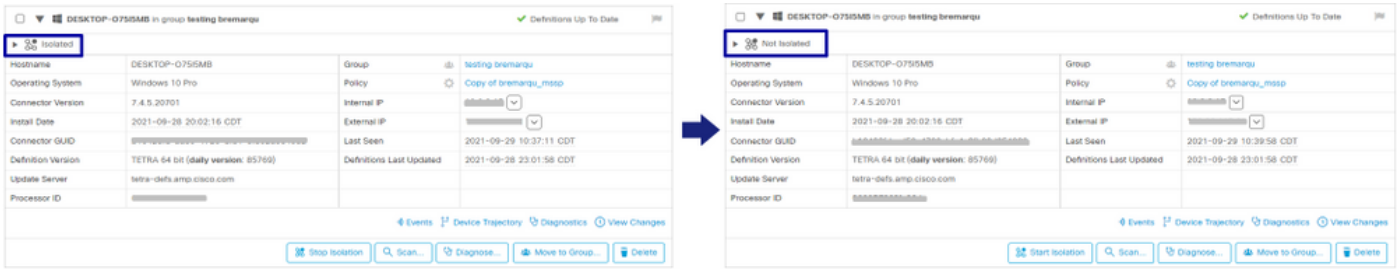
بالإضافة إلى ذلك، إذا رأيت حدث العزل في وحدة التحكم، فيمكنك الانتقال إلى **تفاصيل**

الخطأ لمراجعة رمز الخطأ ووصفه، كما هو موضح في الصورة.

التحقق من الصحة

للتحقق من أن نقطة النهاية قد عادت من العزل أو لم تعد معزولة، يمكنك رؤية واجهة مستخدم موصل نقطة النهاية الآمنة تعرض حالة العزل على أنها **غير معزولة**، كما هو موضح في الصورة.

من وحدة تحكم نقطة النهاية الآمنة، إذا قمت بالتنقل في **الإدارة > أجهزة الكمبيوتر**، وتحديد موقع الكمبيوتر المعني، يمكنك النقر لعرض التفاصيل. تعرض حالة العزل **غير معزولة**، كما هو موضح في الصورة.



معلومات ذات صلة

- دليل مستخدم نقطة النهاية الآمنة
- الدعم التقني والمستندات - Cisco Systems

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).