أستكشاف أخطاء الاتصال وإصلاحها مع وكيل مستخدم Sourcefire

المحتويات

المقدمة

يقوم "عامل مستخدم Sourcefire" بمراقبة خوادم Microsoft Active Directory والإبلاغ عن عمليات تسجيل الدخول والسحب التي تمت مصادقتها عبر LDAP. يقوم نظام FireSIGHT بدمج هذه السجلات مع المعلومات التي يجمعها من خلال مراقبة حركة مرور الشبكة المباشرة بواسطة الأجهزة المدارة. عند العمل مع "وكيل مستخدم Sourcefire"، قد تواجه مشكلات فنية. يزود هذا وثيقة طرف أن يتحرى مختلف إصدار مع Sourcefire مستعمل عامل.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة ب FireSIGHT Management Center، و Sourcefire User Agent، و Active Directory.

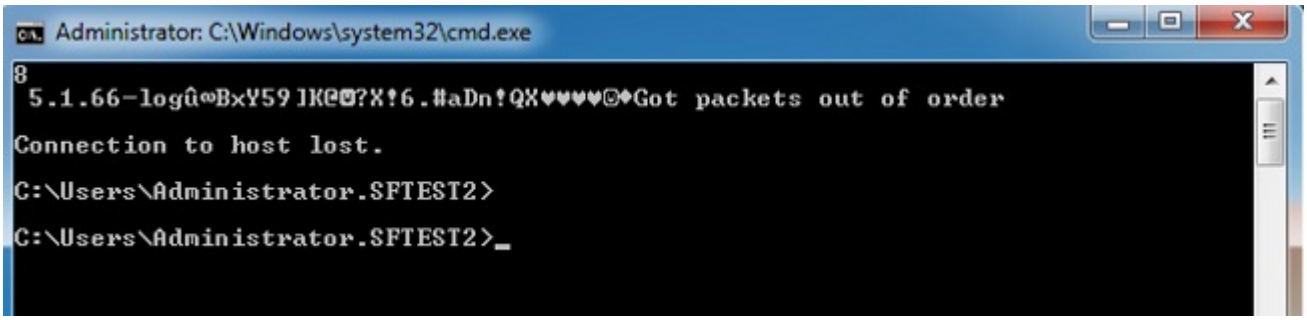
تلميح: لمعرفة المزيد حول خطوات التثبيت وإلغاء التثبيت الخاصة بواجهة مستخدم Sourcefire، اقرأ هذا المستند.

مشكلات الاتصال

1. تحقق من إضافة "عامل المستخدم" إلى "مركز إدارة FireSIGHT". للتحقق من ذلك، انتقل إلى **السياسات > المستخدمون > وكيل المستخدم** وتحقق من صحة عنوان IP الخاص بمضيف وكيل المستخدم الذي تم تكوينه.
2. تأكد من أن المنفذ 3306 مفتوح ومستمع. لا توجد أي جدران حماية أو أجهزة شبكة أخرى تمنع وكيل المستخدم من الاتصال بمركز الدفاع.
3. لن يتم فتح المنفذ 3306 حتى يتم تكوين إدخال "وكيل المستخدم" على "مركز إدارة FireSIGHT".
4. إذا تم تثبيت مضيف "وكيل المستخدم" على برنامج Telnet، فيمكنك التحقق من الاتصال من خلال الاتصال من

مضيف "وكيل المستخدم" إلى مركز إدارة FireSIGHT. سيظهر لديك log-5.1.66 متبوعا بسلسلة من حروف ASCII. اضغط على **Ctrl+C** بشكل متكرر لقطع الاتصال.

ملاحظة: من المتوقع ظهور رسالة الحصول على الحزم خارج الترتيب.



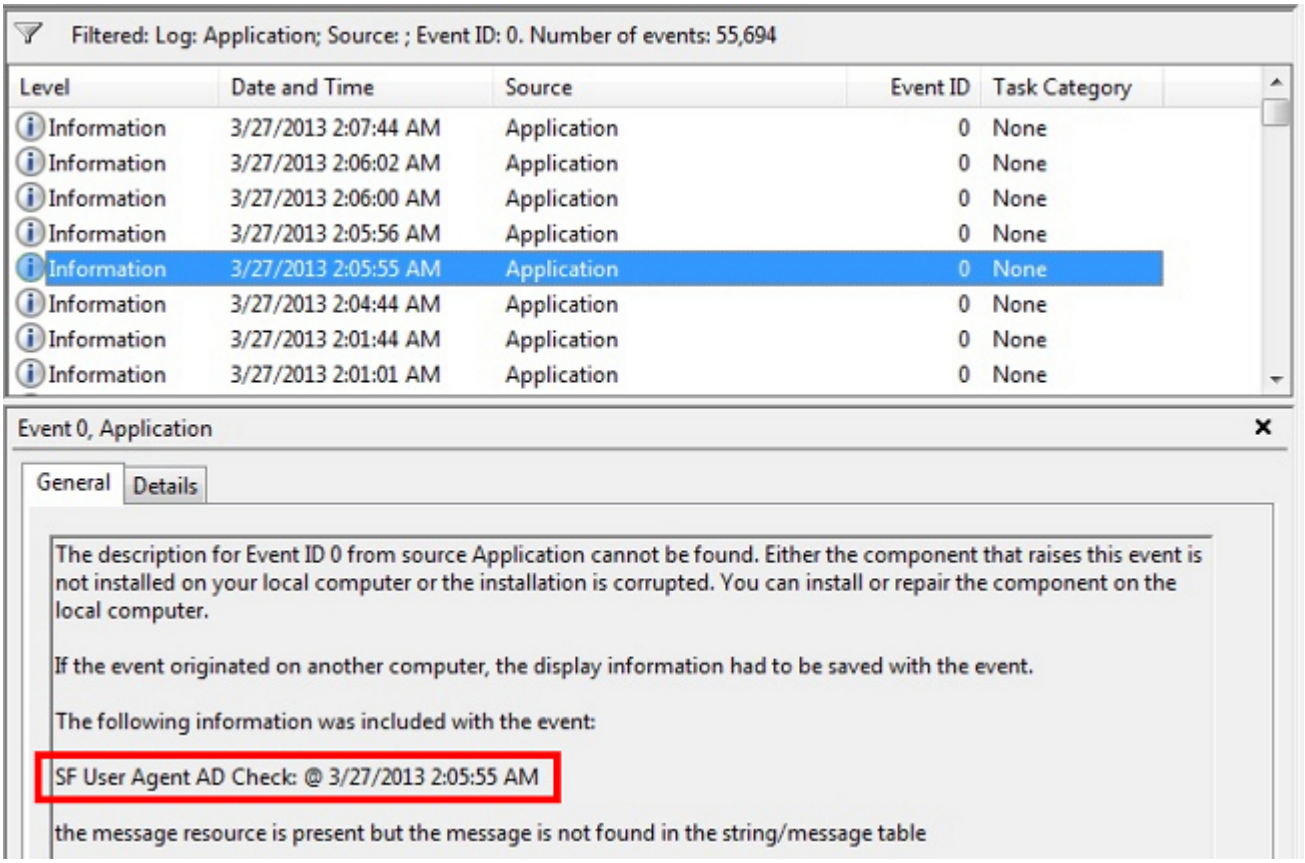
إذا قام "عامل المستخدم" بإنشاء أخطاء عند الاتصال بخادم (خوادم) Active Directory أو المصادقة عليه، فقد تكون هناك مشكلة في إذن الشبكة أو حساب المستخدم. تحقق من عدم وجود مشاكل في اتصال الشبكة في بيئتك وقم بتكوين "وكيل المستخدم" مؤقتا لاستخدام حساب مسؤول المجال للمصادقة على خوادم Active Directory للاختبار إذا أمكن.

التسجيل التشخيص

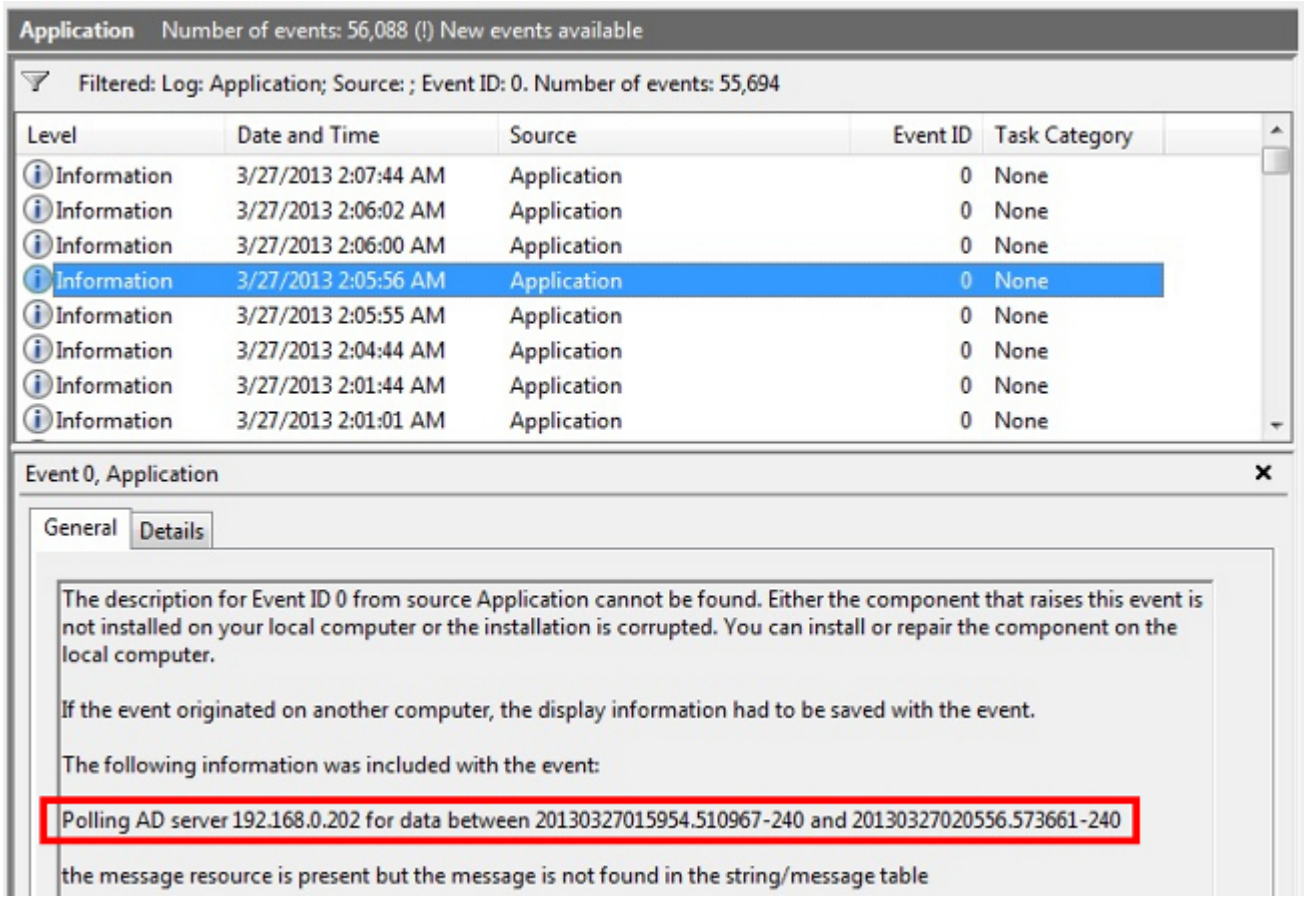
لاستكشاف أخطاء "وكيل المستخدم" وإصلاحها بشكل عام، تحقق من **السجل إلى سجل الأحداث المحلي** داخل عميل واجهة المستخدم الرسومية (GUI) لعامل المستخدم، ثم انقر فوق **حفظ**. وهذا يتسبب في إدخال رسائل عملية مفيدة في سجل أحداث تطبيق مضيف وكيل المستخدم. يمكنك تأكيد إكمال التحقق من "وكيل المستخدم" بنجاح من خلال البحث عن الأحداث التالية، بالترتيب:

ملاحظة: تأتي لقطات الشاشة أدناه من Microsoft Event Viewer على المضيف الذي يقوم بتشغيل "وكيل المستخدم".

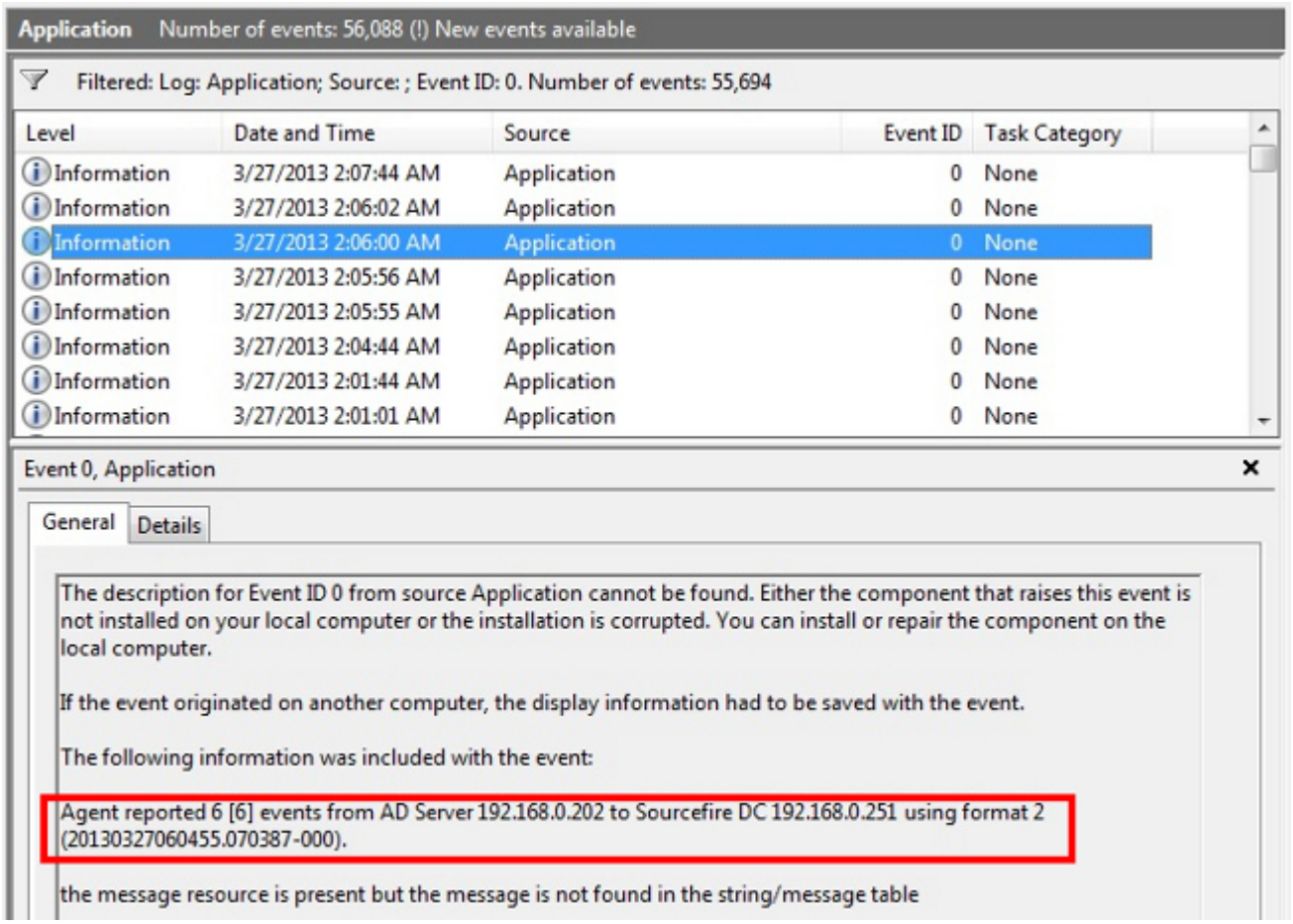
التحقق من خدمة Active Directory الخاصة بوكيل المستخدم



خادم Active Directory لاستطلاع وكيل المستخدم



تم إبلاغ الوكيل عن أحداث الرقم (#) إلى مركز الدفاع


Application Number of events: 56,088 (!) New events available
Filtered: Log: Application; Source: ; Event ID: 0. Number of events: 55,694
Level Date and Time Source Event ID Task Category
Information 3/27/2013 2:07:44 AM Application 0 None
Information 3/27/2013 2:06:02 AM Application 0 None
Information 3/27/2013 2:06:00 AM Application 0 None
Information 3/27/2013 2:05:56 AM Application 0 None
Information 3/27/2013 2:05:55 AM Application 0 None
Information 3/27/2013 2:04:44 AM Application 0 None
Information 3/27/2013 2:01:44 AM Application 0 None
Information 3/27/2013 2:01:01 AM Application 0 None
Event 0, Application
General Details
The description for Event ID 0 from source Application cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.
If the event originated on another computer, the display information had to be saved with the event.
The following information was included with the event:
Agent reported 6 [6] events from AD Server 192.168.0.202 to Sourcefire DC 192.168.0.251 using format 2 (20130327060455.070387-000).
the message resource is present but the message is not found in the string/message table

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).