Problemas de conectividad del Troubleshooting con el agente de usuario de Sourcefire

Contenido

Introducción

El agente de usuario de Sourcefire monitorea los servidores del Microsoft Active Directory y los logines y los cierres de sesión del informe autenticados vía el LDAP. El sistema de FireSIGHT integra estos expedientes con la información que recoge vía la observación directa del tráfico de la red por los dispositivos administrados. Cuando usted está trabajando con el agente de usuario de Sourcefire, usted puede experimentar los problemas técnicos. Este documento proporciona las extremidades para resolver problemas los diversos problemas con el agente de usuario de Sourcefire.

Prerequisites

Cisco recomienda que usted tiene conocimiento en el centro de administración de FireSIGHT, el agente de usuario de Sourcefire, y el Active Directory.

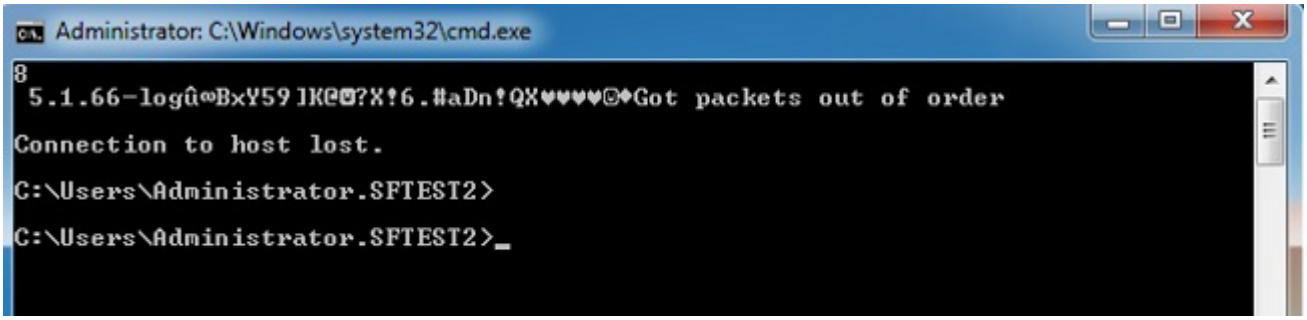
> **Tip**: Para aprender más sobre los pasos de la instalación y de la desinstalación del agente de usuario de Sourcefire, lea este documento.

Problemas de conectividad

1. Verifique que el agente de usuario esté agregado al centro de administración de FireSIGHT. Para verificar eso, navegue a las **directivas > Users > agente de usuario** y verifique que la dirección IP del host configurado del agente de usuario está correcta.
2. Confirme que el puerto 3306 es abierto y que escucha. No hay Firewall u otros dispositivos de red que paran el agente de usuario de la comunicación con el centro de la defensa.

3. El puerto 3306 no estará abierto hasta que una entrada del agente de usuario se haya configurado en el centro de administración de FireSIGHT.
4. Si un host del agente de usuario tiene telnet instalado, usted puede verificar la conexión telneting del host del agente de usuario al centro de administración de FireSIGHT. Usted verá `5.1.66-log` seguido por una cadena de caracteres ASCII. Presione el **CTRL+C** en varias ocasiones para desconectar.

Note: El aspecto de los `paquetes Got` mensaje `fuera de servicio` se espera.



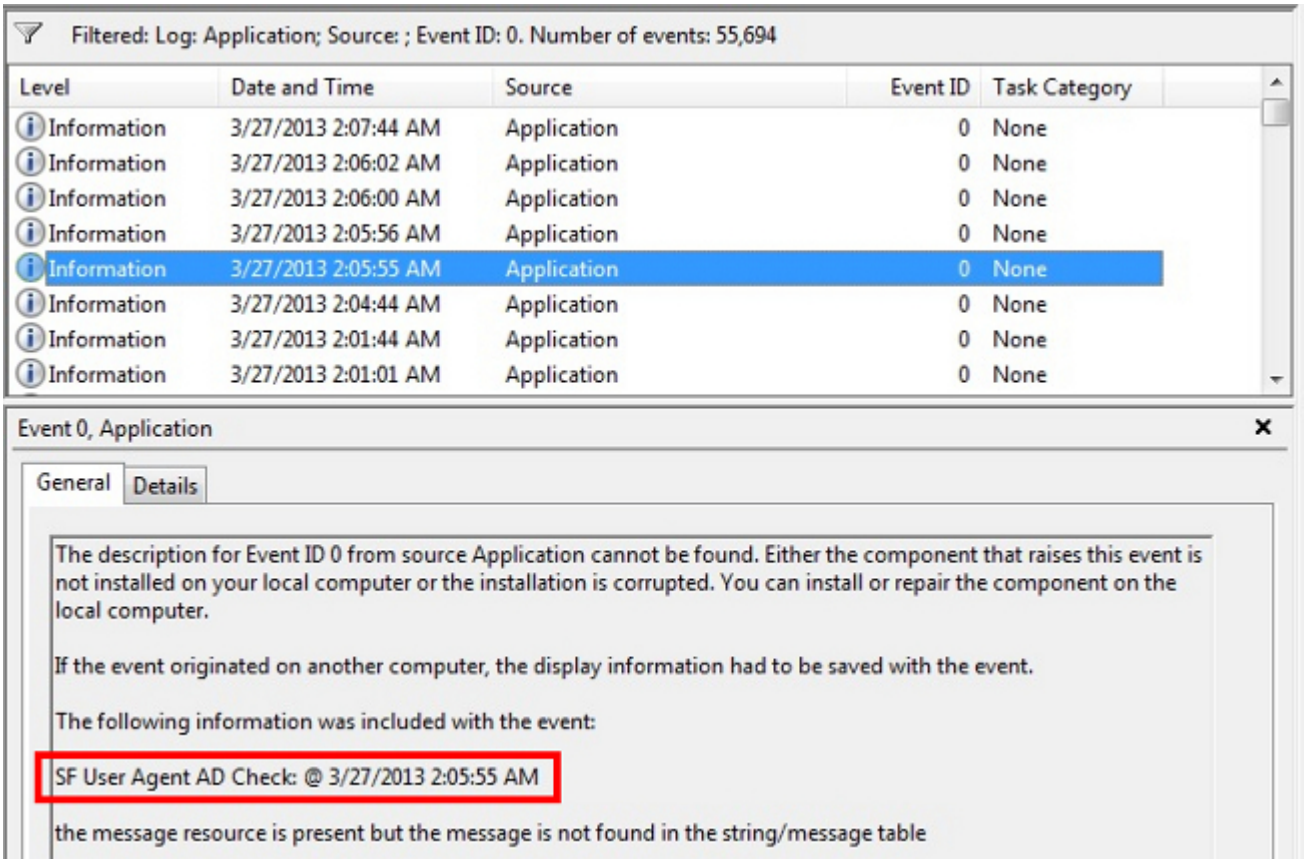
Si el agente de usuario genera los errores al conectar o autenticando a los servidores del Active Directory puede haber un problema del permiso de la red o de la cuenta de usuario. Verifique que no haya problemas de conectividad de red en su entorno y configure temporalmente el agente de usuario para utilizar un dominio admin explican la autenticación a los servidores Active Directory para probar si es posible.

Registro de diagnóstico

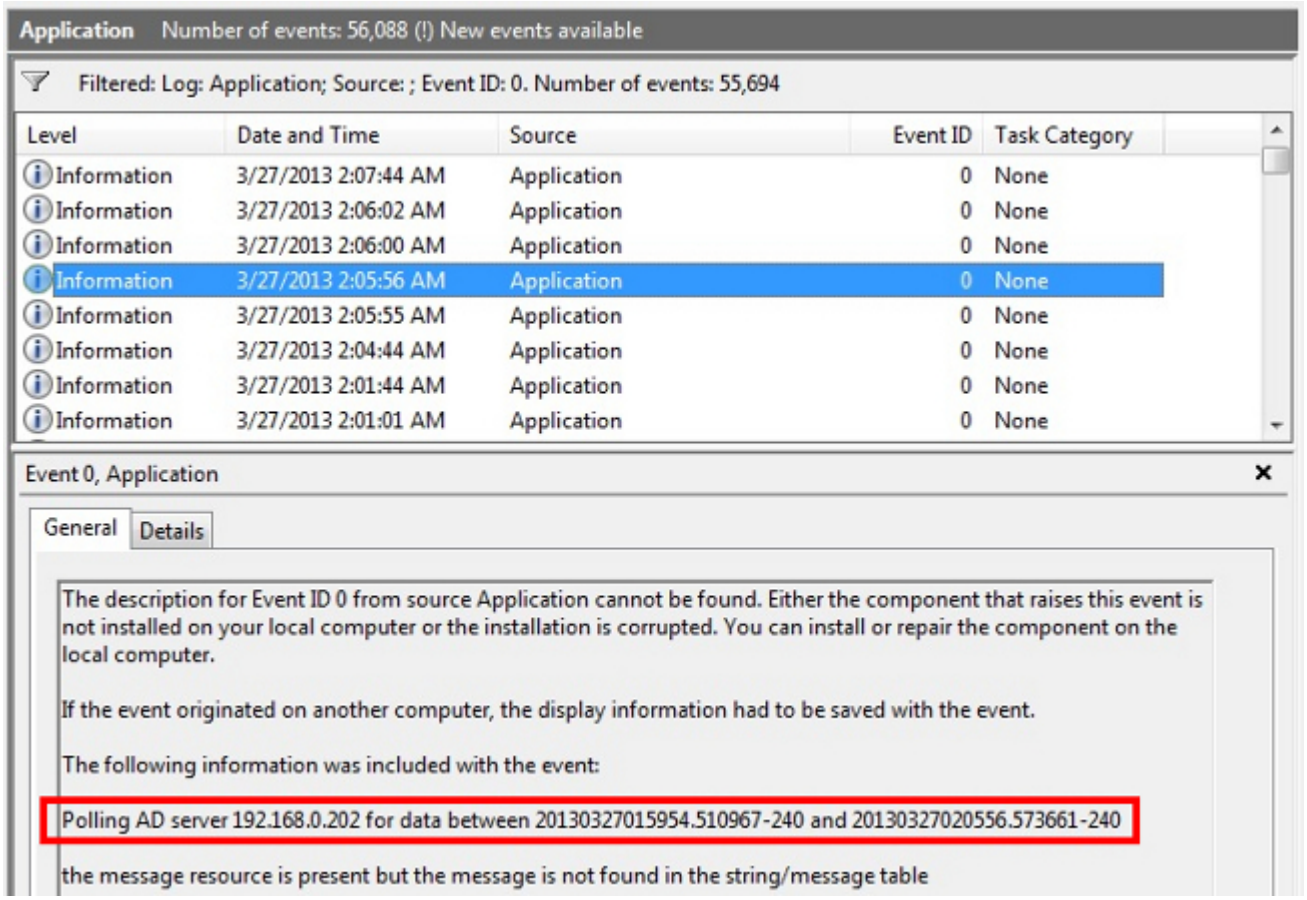
Para el Troubleshooting general del agente de usuario, **registro del** control al **registro de eventos locales** dentro del GUI del cliente del agente de usuario y de la **salvaguardia del** tecleo. Esto hace los mensajes operativos útiles ser ingresada en el registro de eventos de aplicación del host del agente de usuario. Usted puede confirmar que la interrogación del agente de usuario está completando con éxito buscando para los eventos siguientes, en la orden:

Note: El screenshots abajo es del Microsoft Event Viewer en el host que está funcionando con el agente de usuario.

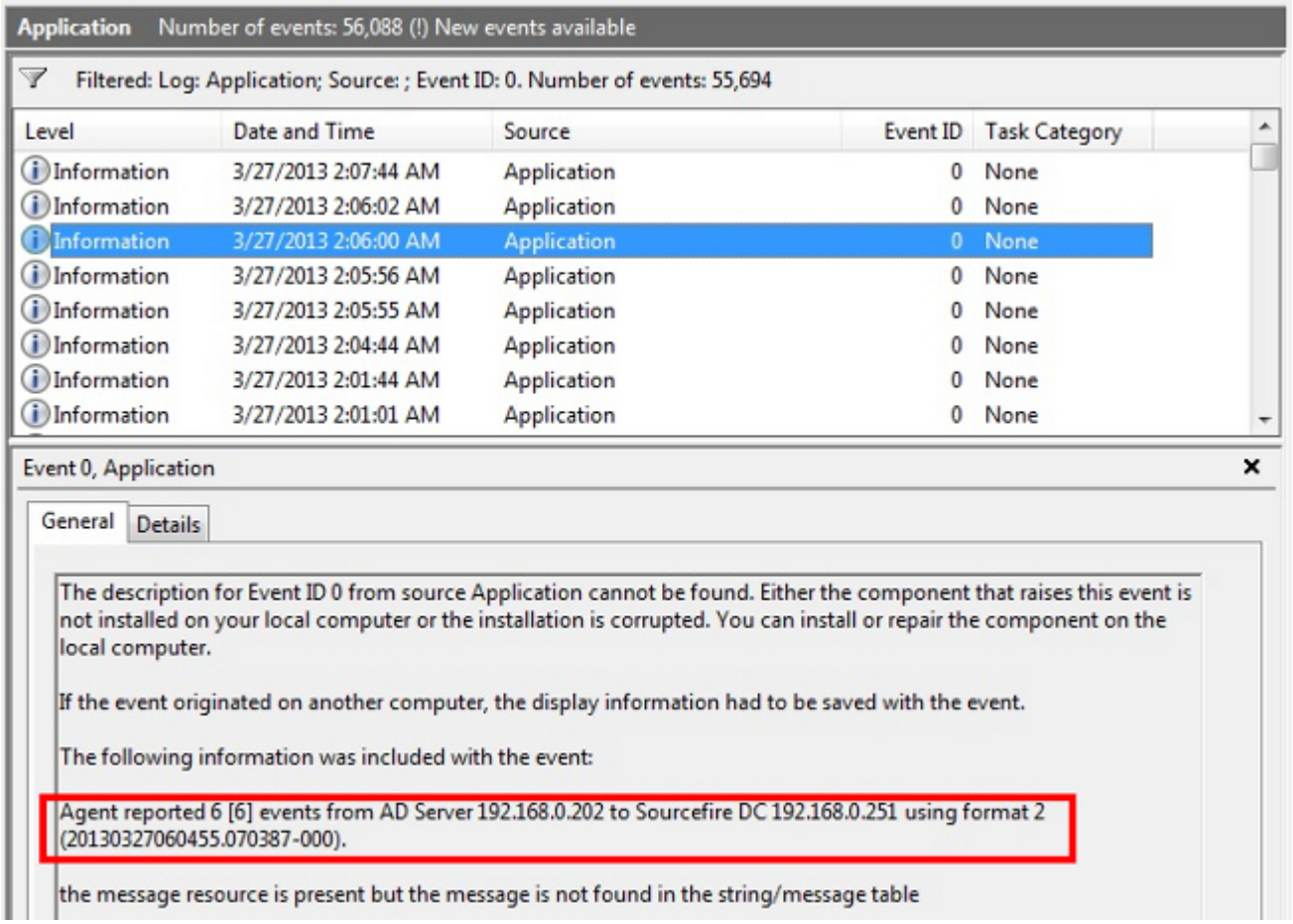
Control del Active Directory del agente de usuario



Servidor Active Directory de la interrogación del agente de usuario



Eventos señalados agente del número (#) al centro de la defensa


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