# Solucionar problemas de conectividad con el agente de usuario de Sourcefire

## Contenido



## Introducción

El agente de usuario de Sourcefire supervisa los servidores de Microsoft Active Directory e informa de inicios de sesión y cierres de sesión autenticados mediante LDAP. El sistema FireSIGHT integra estos registros con la información que recopila a través de la observación directa del tráfico de red por parte de los dispositivos gestionados. Cuando trabaje con el agente de usuario de Sourcefire, puede experimentar problemas técnicos. Este documento proporciona consejos para resolver varios problemas con el Agente de usuario de Sourcefire.

## Prerequisites

Cisco recomienda tener conocimientos sobre FireSIGHT Management Center, el agente de usuario de Sourcefire y Active Directory.

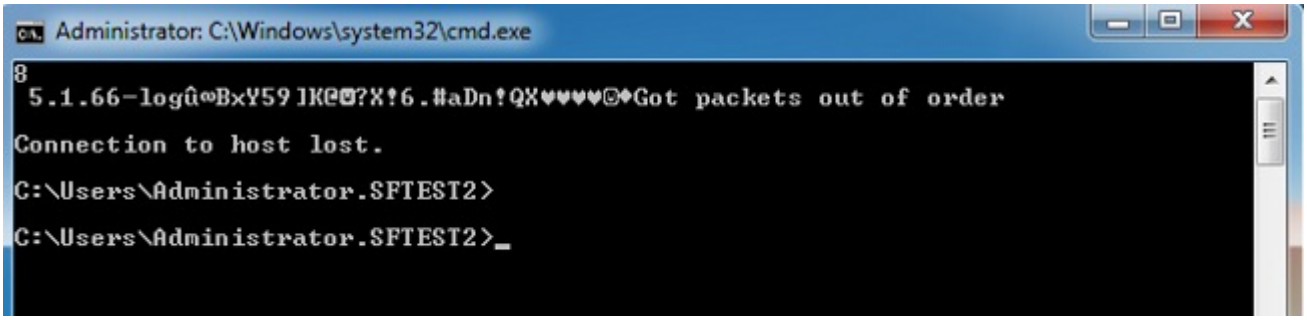
> **Sugerencia**: Para obtener más información sobre los pasos de instalación y desinstalación del agente de usuario de Sourcefire, lea este documento.

## Inconvenientes de conectividad

1. Compruebe que el agente de usuario se ha agregado a FireSIGHT Management Center. Para verificarlo, navegue hasta **Políticas > Usuarios > Agente de usuario** y verifique que la dirección IP del host del Agente de usuario configurado sea correcta.
2. Confirme que el puerto 3306 esté abierto y escuchando. No hay firewalls ni otros dispositivos de red que impidan que el agente de usuario se comunique con el centro de defensa.

3. El puerto 3306 no se abrirá hasta que se haya configurado una entrada de agente de usuario en FireSIGHT Management Center.
4. Si un host de agente de usuario tiene telnet instalado, puede verificar la conexión mediante telnet desde el host de agente de usuario a FireSIGHT Management Center. Verá 5.1.66-log seguido de una cadena de caracteres ASCII. Presione **CTRL+C** repetidamente para desconectar.

**Nota**: Se espera el aspecto del mensaje Paquetes obtenidos fuera de orden.



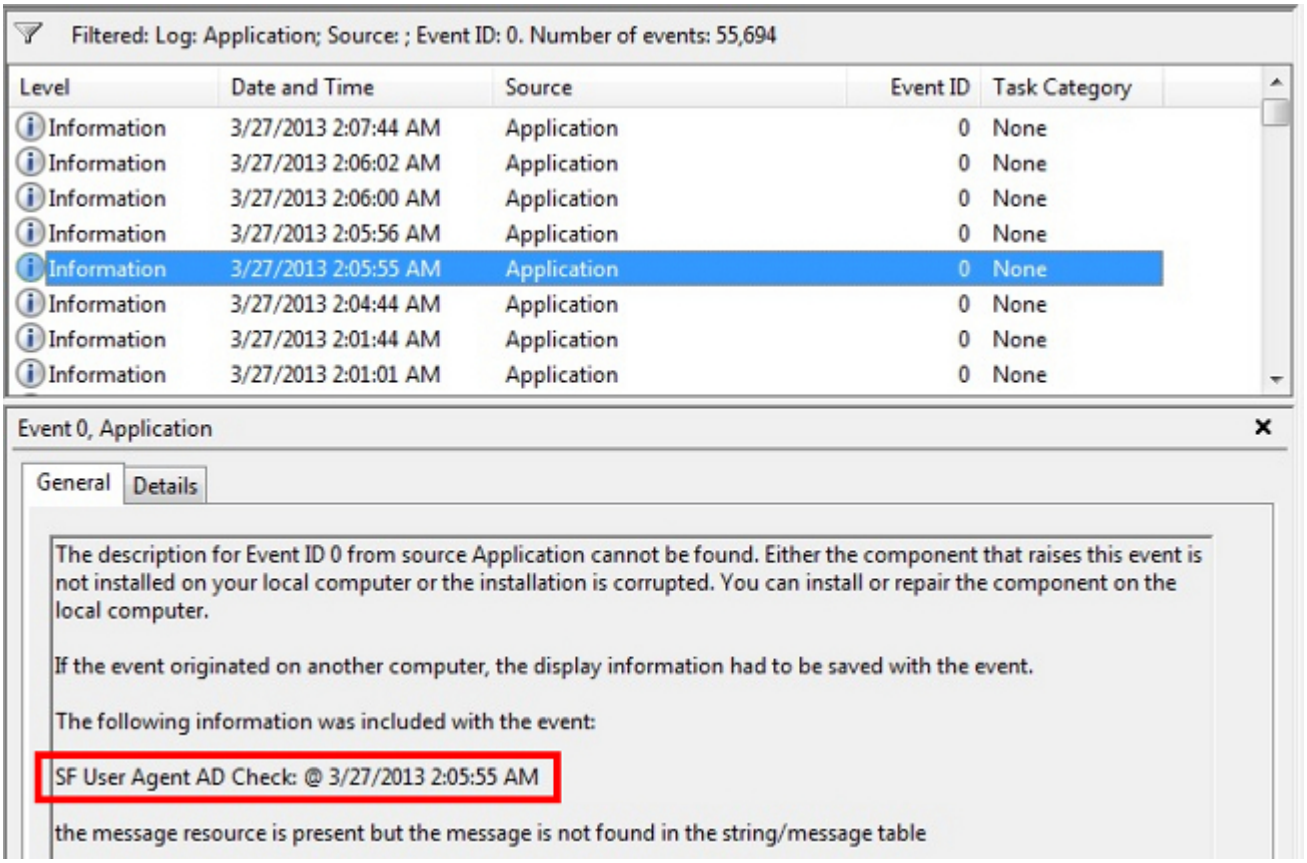

Si el agente de usuario genera errores al conectarse o autenticarse en los servidores de Active Directory, puede haber un problema de permisos de la cuenta de usuario o de la red. Verifique que no haya problemas de conectividad de red en su entorno y configure temporalmente el Agente de usuario para utilizar una cuenta de administrador de dominio para la autenticación a los servidores de Active Directory para realizar pruebas si es posible.

# Registros de diagnóstico

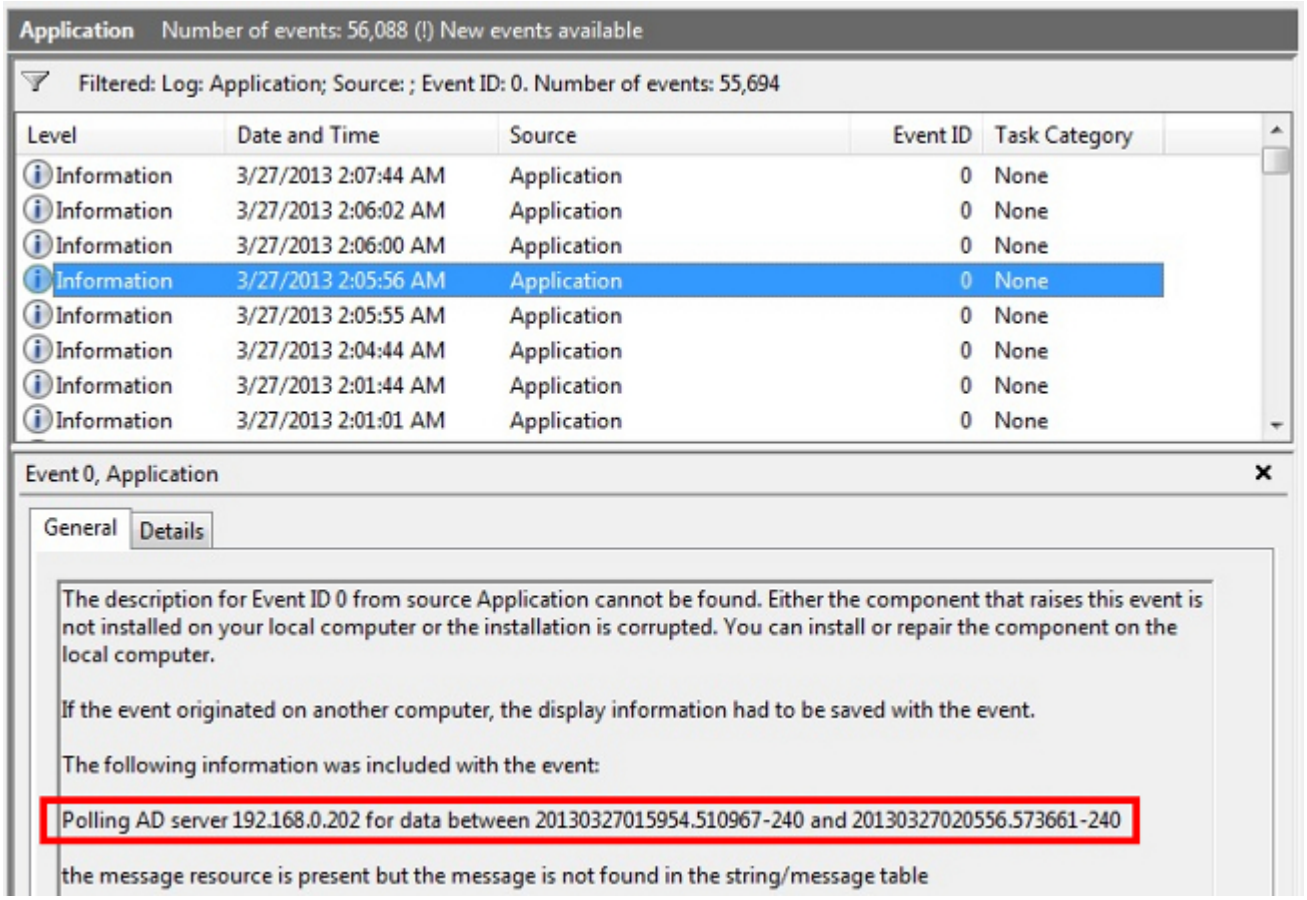
Para la resolución general de problemas del agente de usuario, marque **Log to local event log** dentro del cliente GUI del agente de usuario y haga clic en **Save**. Esto hace que se introduzcan mensajes operativos útiles en el registro de eventos de la aplicación host del agente de usuario. Puede confirmar que el sondeo del agente de usuario se ha completado correctamente buscando los siguientes eventos, por orden:

**Nota**: Las capturas de pantalla siguientes provienen del Visor de eventos de Microsoft en el host que ejecuta el agente de usuario.

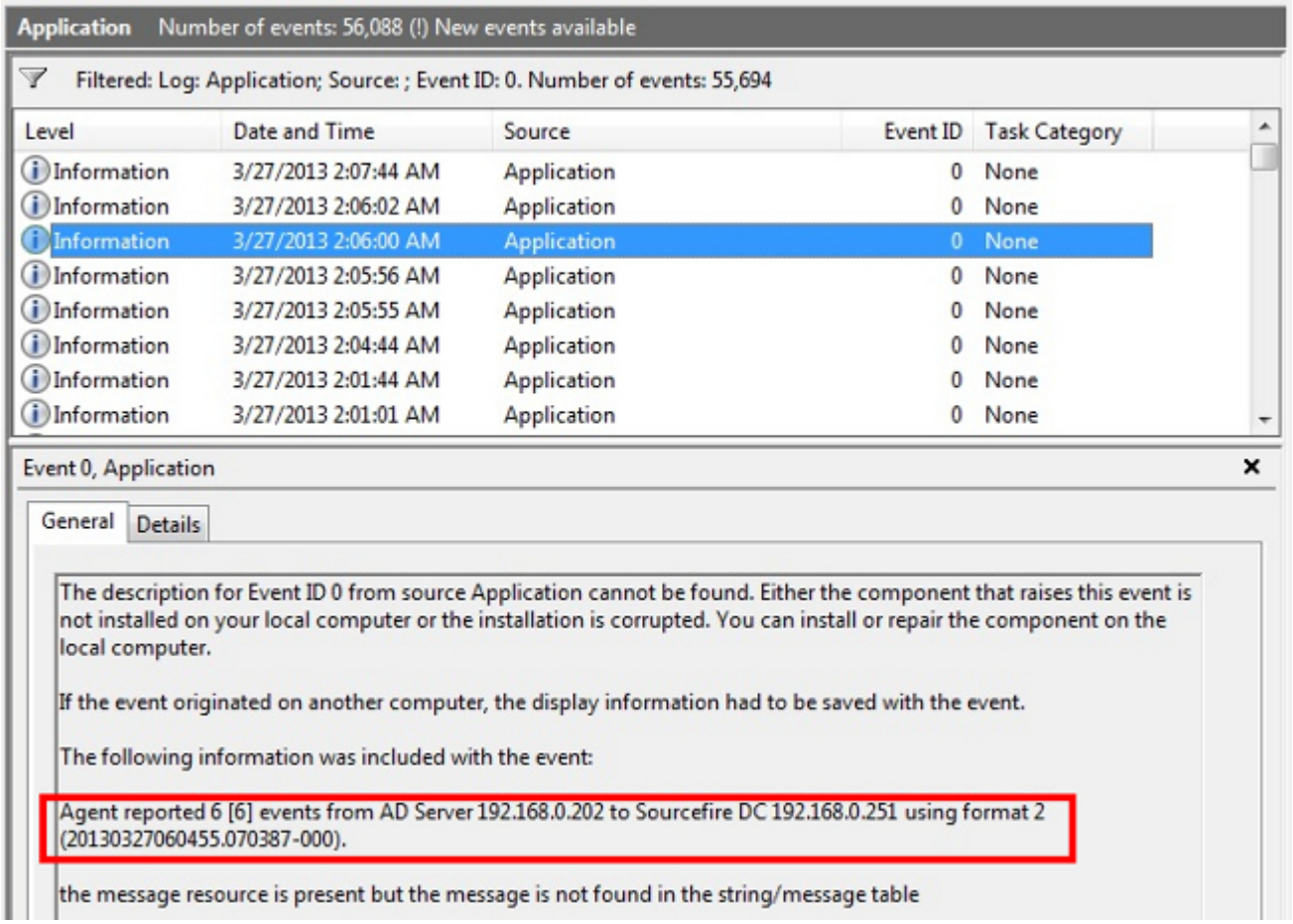
## Comprobación de Active Directory del agente de usuario




## Agente de usuario que consulta al servidor de Active Directory




## El agente notificó los eventos de número (#) al centro de 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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).