# 排除故障与Sourcefire用户代理的连通性问题

## 目录



## 简介

Sourcefire用户代理监视器Microsoft Active Directory服务器和通过LDAP和注销验证的报告登录。通过直接网络流量观察收集由受管理设备的FireSIGHT系统集成与信息的这些记录。当您工作与Sourcefire用户代理时，您可以遇到技术问题。本文提供提示排除故障与Sourcefire用户代理的多种问题。

## 先决条件

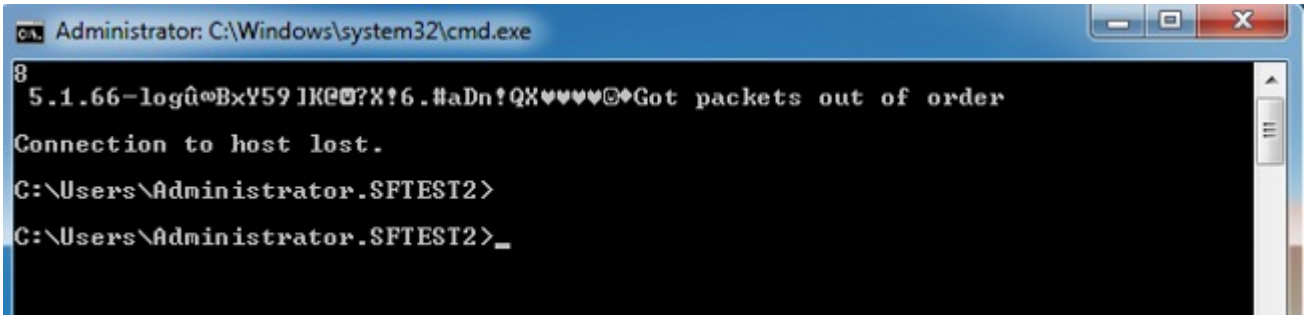
思科建议您有在FireSIGHT管理中心、Sourcefire用户代理和活动目录的知识。

> **提示**：为了得知更多Sourcefire用户代理的安装和卸载步骤，请读本文。

## 连接问题

1. 验证用户代理被添加到FireSIGHT管理中心。要验证那，请导航对**策略> Users >用户代理**并且验证已配置的用户代理主机的IP地址正确。
2. 确认波尔特3306是开放和侦听。没有终止用户代理的防火墙或其他网络设备从通信与防御中心。
3. 波尔特3306不会是开放的，直到用户代理条目在FireSIGHT管理中心配置。
4. 如果用户代理主机有安装的telnet，您能通过telneting验证连接从用户代理主机到FireSIGHT管理中心。 您将看到ASCII字符字符串跟随的5.1.66 `LOG`。 重复普雷斯**CTRL+C**断开连接。

   **注意**：`got`外观消息预计。



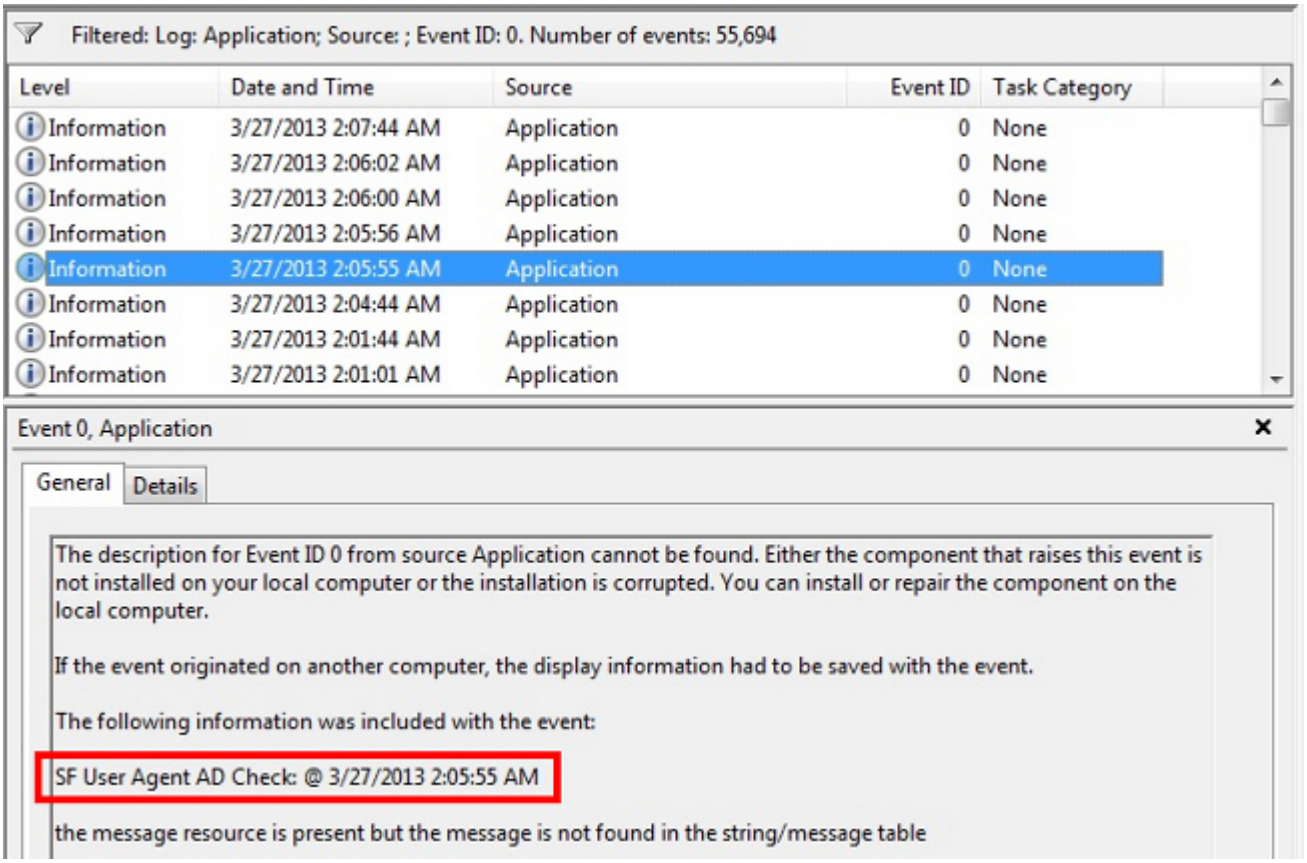

如果用户代理生成错误，当连接或验证对活动目录服务器时可能有网络或用户帐户权限问题。 验证没有在您的环境的网络连通性问题若可能和临时地配置用户代理使用验证的一个域管理帐户到激活目录服务器测试的。

# 诊断记录

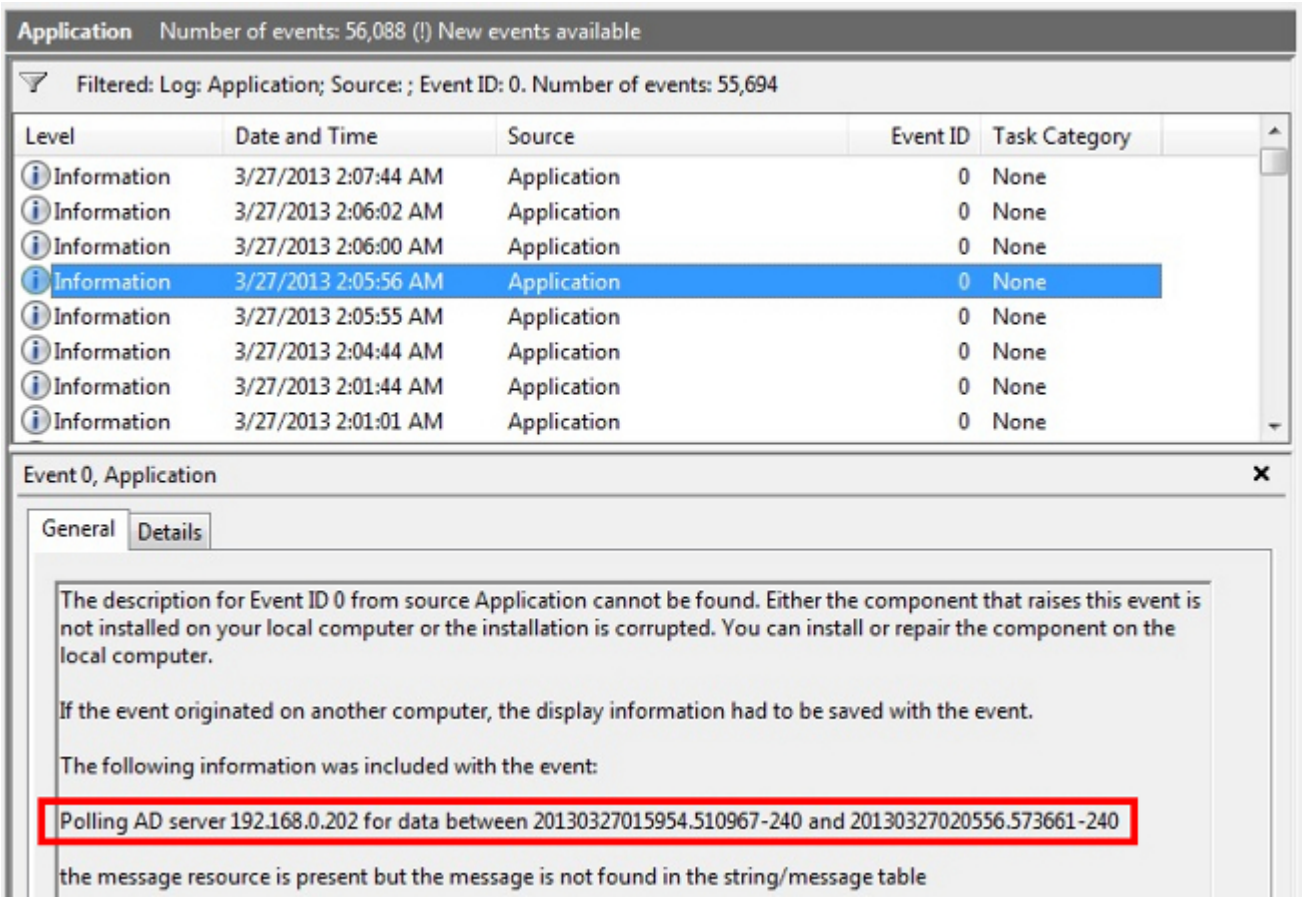
对于用户代理的通用故障排除，请检查**日志对**在用户代理GUI客户端内的**本地事件日志**并且点击**“Save”**。 这在用户代理主机应用事件日志造成有用的作战文电被输入。 您能按顺序确认用户代理?顺利地完成通过搜索以下事件， ：

> **注意**：下面的屏幕画面是从在运行用户代理的主机的微软Event Viewer。

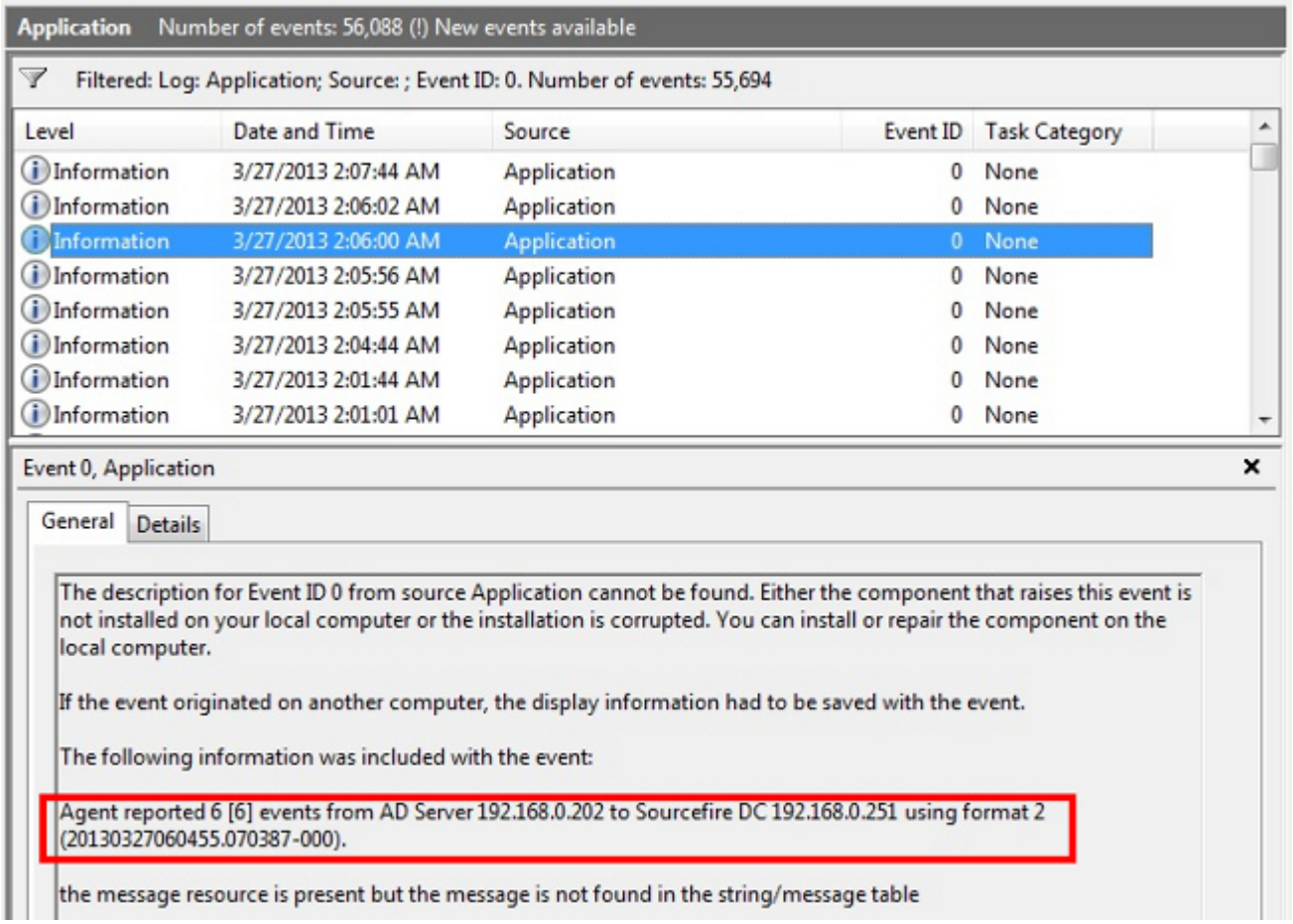
## 用户代理活动目录检查



## 用户代理?激活目录服务器




## 代理程序对防御中心的报告的编号(#)事件


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