排除Sourcefire用户代理的连接问题

目录

简介

Sourcefire用户代理监控Microsoft Active Directory服务器，并报告通过LDAP进行身份验证的登录和注销。FireSIGHT系统将这些记录与其通过受管设备的直接网络流量观察收集的信息相集成。使用Sourcefire用户代理时，可能会遇到技术问题。本文档提供了对Sourcefire用户代理的各种问题进行故障排除的提示。

先决条件

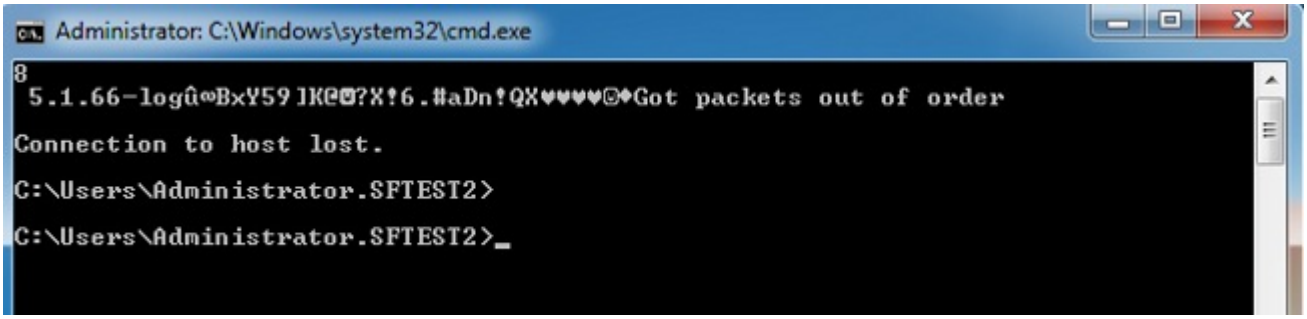
思科建议您具备FireSIGHT管理中心、Sourcefire用户代理和Active Directory的相关知识。

> **提示**：要了解有关Sourcefire用户代理的安装和卸载步骤的详细信息，请阅读此文档。

连接问题

1. 验证用户代理已添加到FireSIGHT管理中心。要验证这一点，请导航到**Policies > Users > User Agent**，并验证已配置的用户代理主机的IP地址是否正确。
2. 确认端口3306已打开并正在侦听。没有防火墙或其他网络设备阻止用户代理与防御中心通信。
3. 在FireSIGHT管理中心上配置用户代理条目之前，端口3306不会打开。
4. 如果用户代理主机已安装telnet，则可以通过从用户代理主机通过telnet连接到FireSIGHT管理中心来验证连接。 您将看到5.1.66-log，后面跟有一串ASCII字符。 重复按**CTRL+C**以断开连接。

> **注意**：预期会出现Got packets out of order消息。



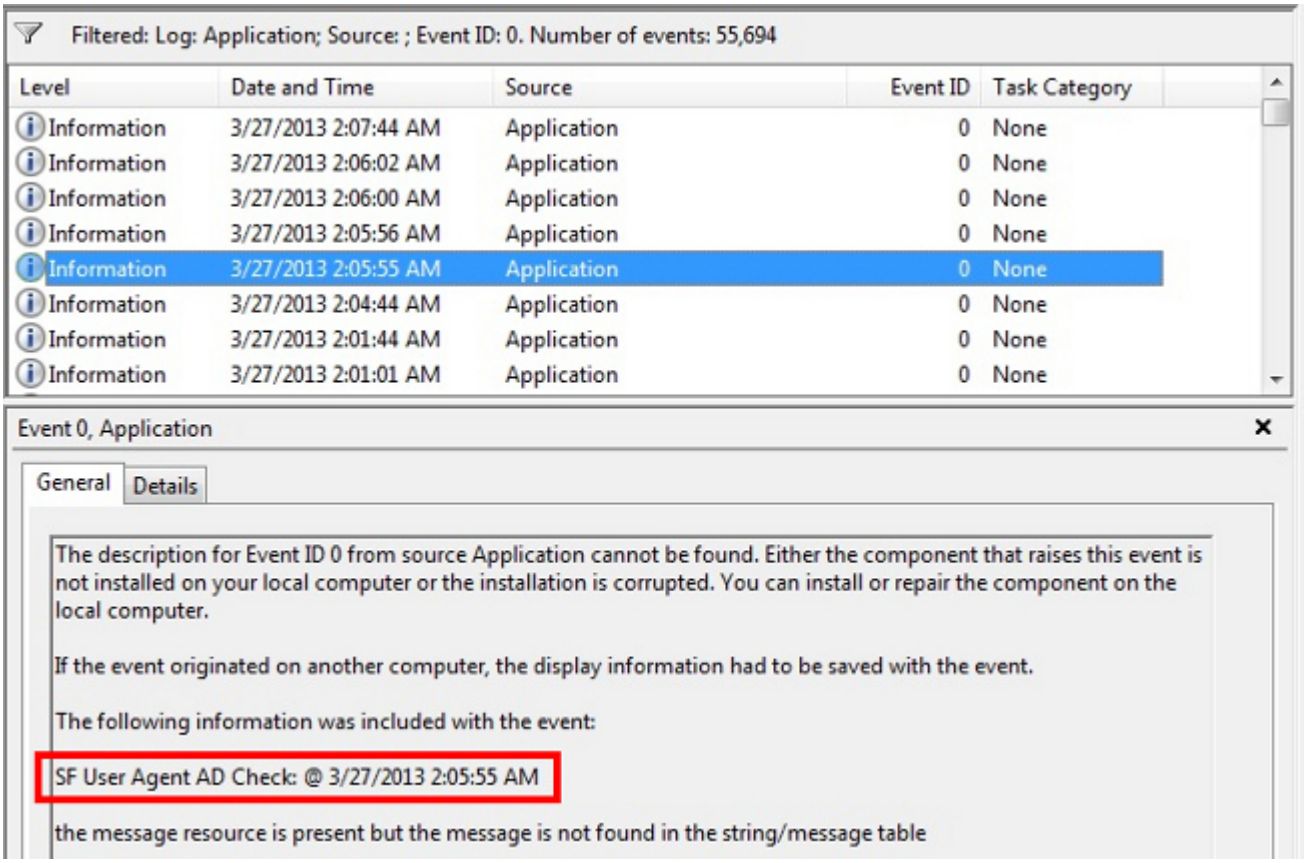
如果用户代理在连接到Active Directory服务器或对其进行身份验证时生成错误，则可能存在网络或用户帐户权限问题。 验证您的环境中不存在网络连接问题，并临时配置用户代理，以使用域管理员帐户对Active Directory服务器进行身份验证，以便在可能的情况下进行测试。

诊断日志

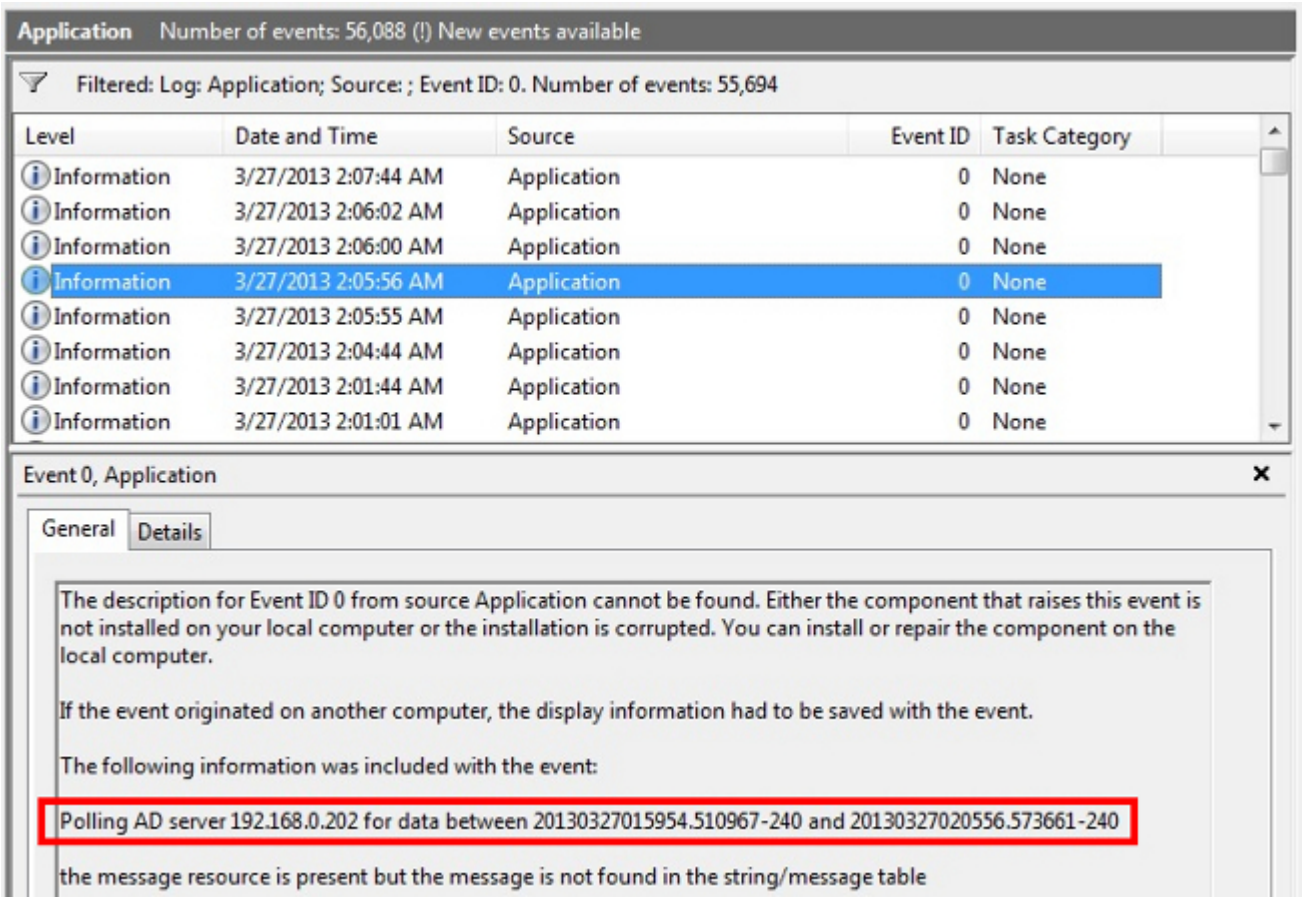
对于用户代理的一般故障排除，请在用户代理GUI客户端中选中**Log to local event log**，然后单击**Save**。 这会导致在用户代理主机应用程序事件日志中输入有用的操作消息。 您可以通过按顺序搜索以下事件来确认用户代理轮询是否成功完成：

注：以下屏幕截图来自运行用户代理的主机上的Microsoft事件查看器。

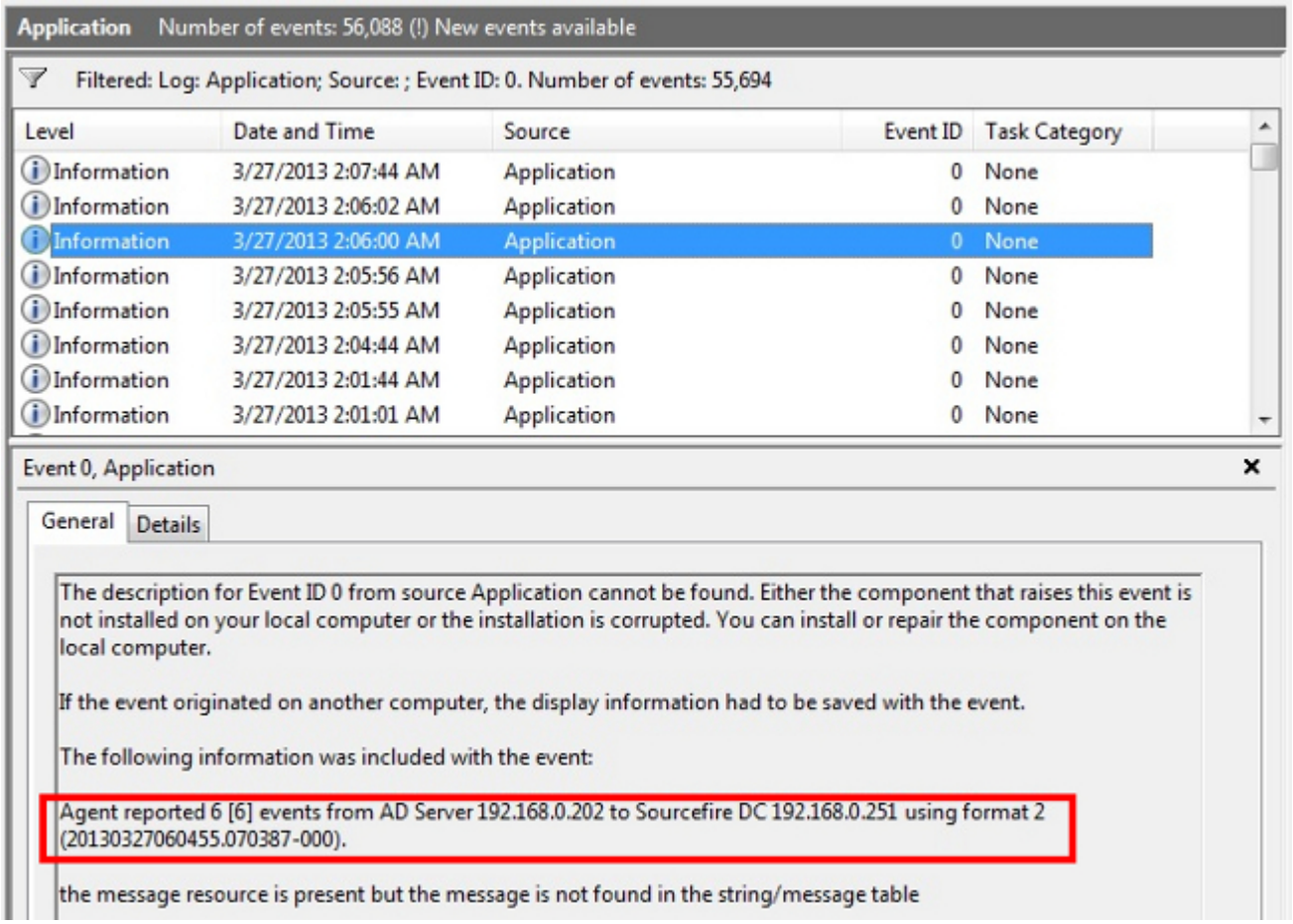
用户代理Active Directory检查



用户代理轮询Active Directory服务器



代理向防御中心报告的编号(#)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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。