排除Sourcefire使用者代理的連線問題

目錄

簡介

Sourcefire使用者代理監視Microsoft Active Directory伺服器，並報告通過LDAP驗證的登入和註銷。FireSIGHT系統將這些記錄與其通過受管裝置的直接網路流量觀察收集的資訊相整合。使用Sourcefire使用者代理時，可能會遇到技術問題。本文檔提供用於診斷Sourcefire使用者代理的各種問題的提示。

必要條件

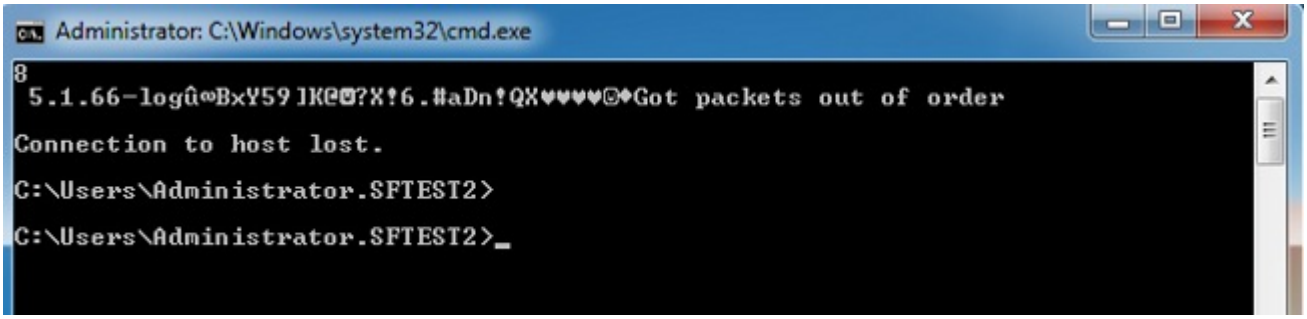
思科建議您瞭解FireSIGHT管理中心、Sourcefire使用者代理和Active Directory的相關知識。

> **提示**：要瞭解有關Sourcefire使用者代理的安裝和解除安裝步驟的詳細資訊，請閱讀此文檔。

連線問題

1. 驗證使用者代理是否已新增到FireSIGHT管理中心。要驗證這一點，請導航到**Policies > Users > User Agent**，然後驗證已配置的使用者代理主機的IP地址是否正確。
2. 確認埠3306已開啟且正在監聽。沒有防火牆或其他網路裝置阻止使用者代理與防禦中心通訊。
3. 在FireSIGHT管理中心上配置使用者代理條目之前，埠3306不會開啟。
4. 如果使用者代理主機已安裝telnet，則可以通過從使用者代理主機通過telnet連線到FireSIGHT管理中心來驗證連線。 您會看到5.1.66-log，後跟一串ASCII字元。 重複按**CTRL+C**以斷開連線。

> **注意**：應該出現Got packets out of order消息。



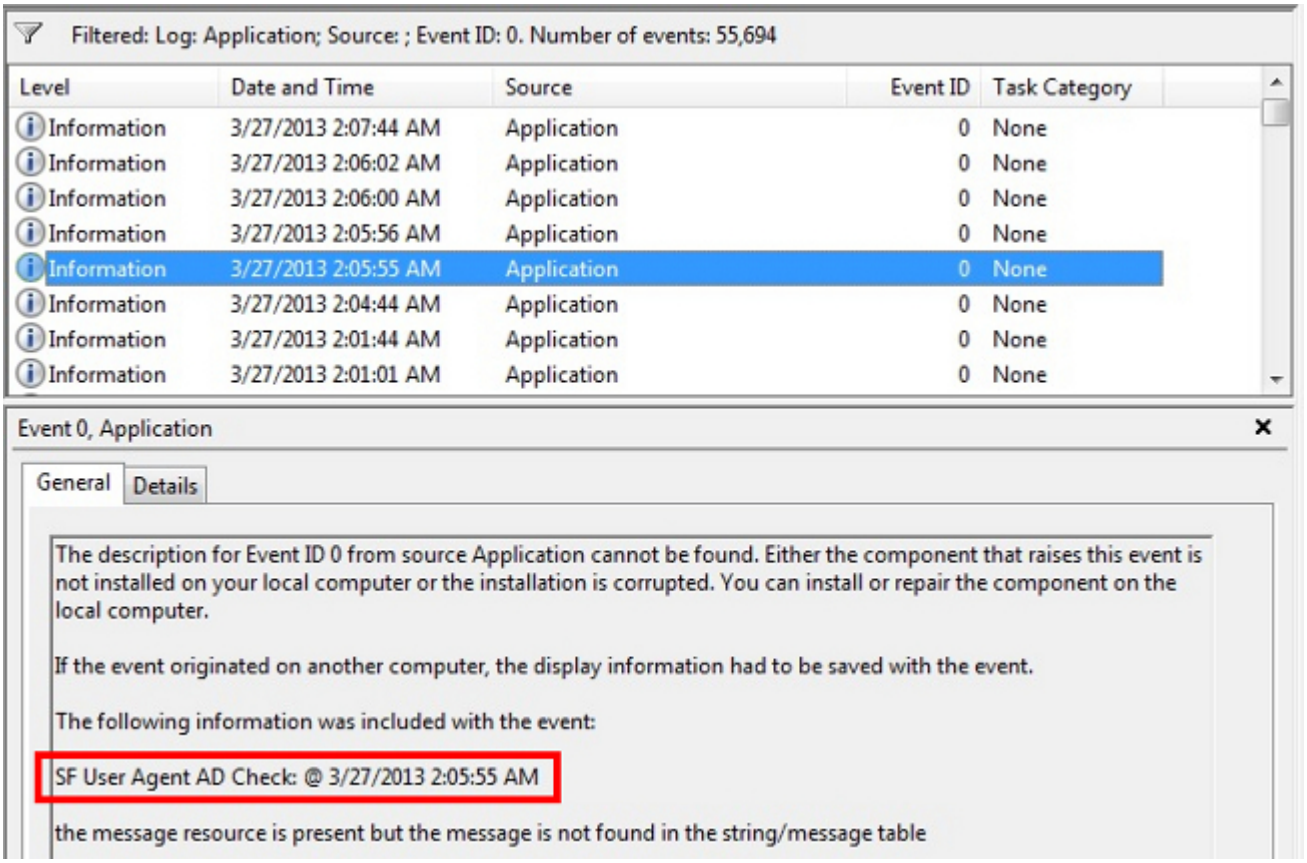
如果使用者代理在連線到Active Directory伺服器或對其進行身份驗證時生成錯誤，則可能存在網路或使用者帳戶許可權問題。 確認您的環境中不存在網路連線問題，並臨時配置使用者代理以使用域管理員帳戶對Active Directory伺服器進行身份驗證，以便在可能的情況下進行測試。

診斷日誌記錄

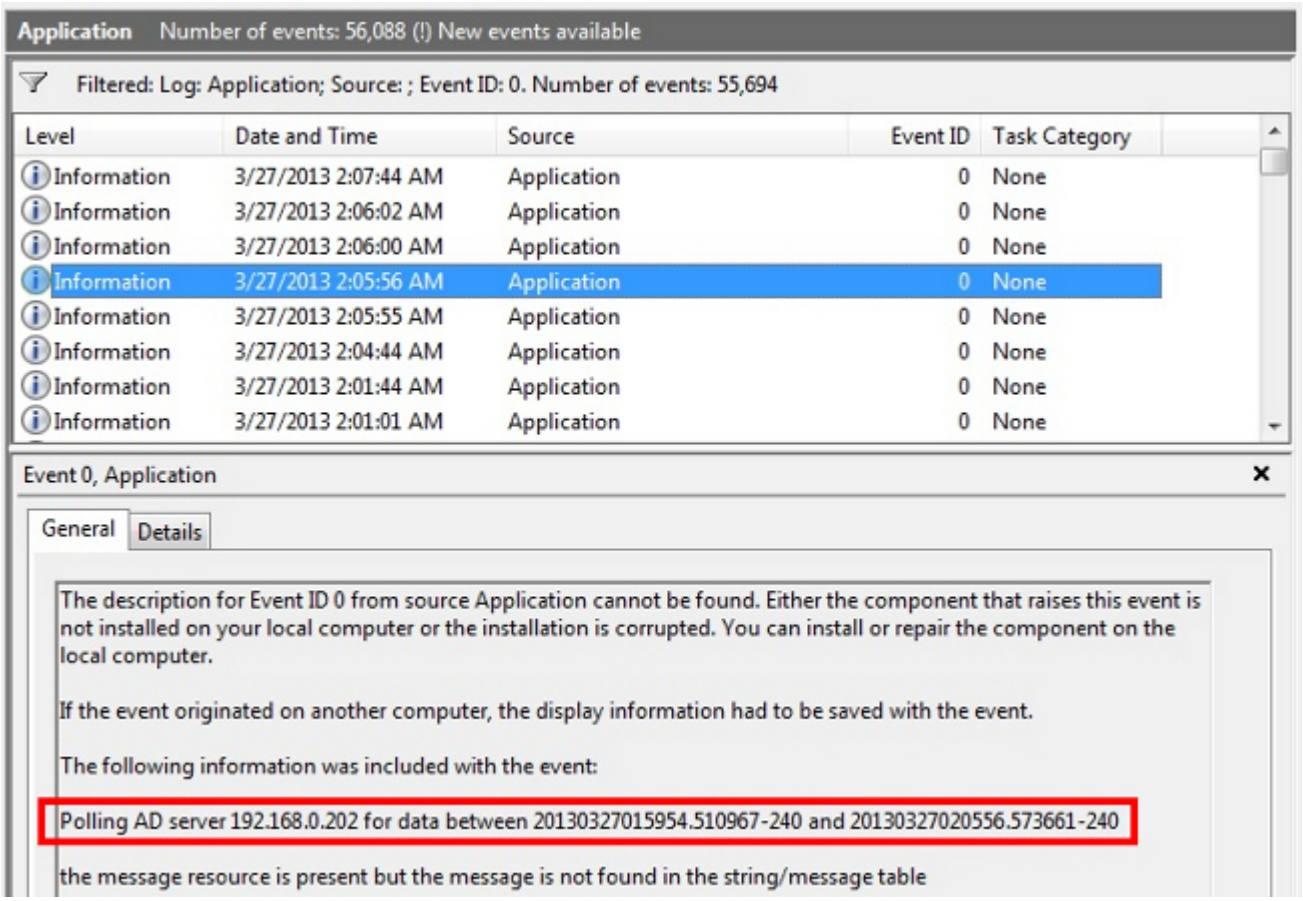
有關使用者代理的常規故障排除，請在使用者代理GUI客戶端中選中**Log to local event log**，然後按一下**Save**。 這會導致在使用者代理主機應用程式事件日誌中輸入有用的操作消息。 您可以通過按順序搜尋以下事件來確認使用者代理輪詢是否成功完成：

注意：以下螢幕截圖來自運行使用者代理的主機上的Microsoft事件檢視器。

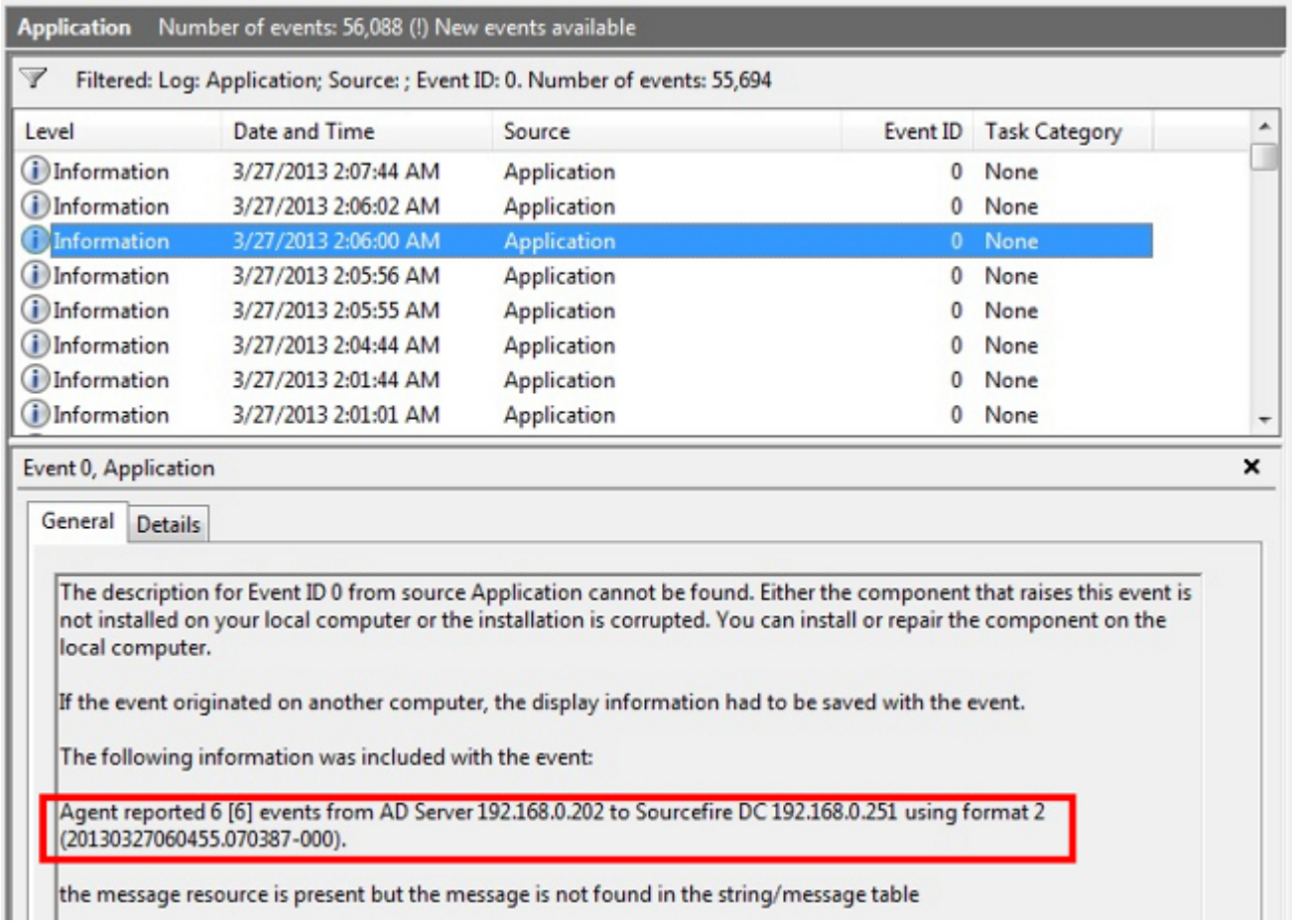
使用者代理Active Directory檢查



使用者代理輪詢Active Directory伺服器



代理向防禦中心報告的數字(#)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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。