Troubleshoot Connectivity Issues with Sourcefire User Agent

Document ID: 118159

Contributed by Nazmul Rajib and Patrick Owens, Cisco TAC Engineers.

Aug 04, 2014

Contents

Introduction

Sourcefire User Agent monitors Microsoft Active Directory servers and report logins and logoffs authenticated via LDAP. The FireSIGHT System integrates these records with the information it collects via direct network traffic observation by managed devices. When you are working with the Sourcefire User Agent, you may experience technical issues. This document provides tips to troubleshoot various issues with the Sourcefire User Agent.

Prerequisites

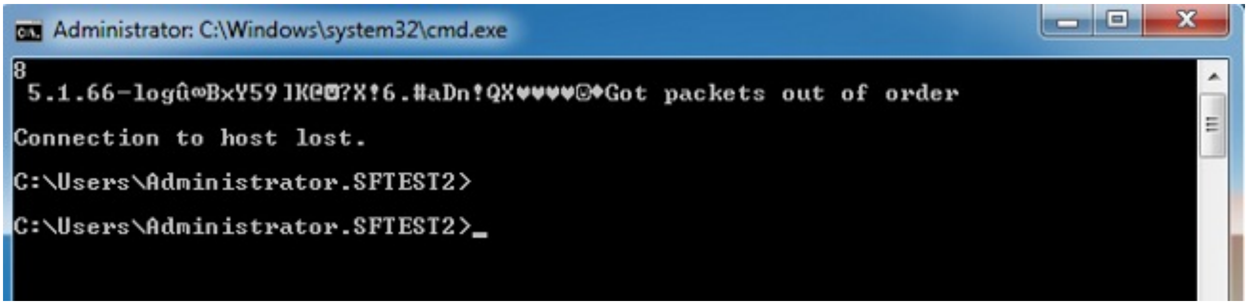
Cisco recommends that you have knowledge on FireSIGHT Management Center, Sourcefire User Agent, and Active Directory.

Tip: In order to learn more about the installation and uninstallation steps of the Sourcefire User Agent, read this document.

Connectivity Issues

1. Verify that the User Agent is added to the FireSIGHT Management Center. To verify that, navigate to ***Policies > Users > User Agent*** and verify that the IP address of configured User Agent host is correct.
2. Confirm that Port 3306 is open and listening. There are no firewalls or other network devices stopping the User Agent from communicating with the Defense Center.
3. Port 3306 will not be open until a User Agent entry has been configured on the FireSIGHT Management Center.
4. If an User Agent host has telnet installed, you can verify the connection by telneting from the User Agent host to the FireSIGHT Management Center. You will see 5.1.66−log followed by a string of ASCII characters. Press ***CTRL+C*** repeatedly to disconnect.

Note: The appearance of Got packets out of order message is expected.



```
8
 5.1.66-logû∞BxY59]K@◙?X!6.#aDn!QX♥♥♥♥☺♦Got packets out of order

Connection to host lost.

C:\Users\Administrator.SFTEST2>

C:\Users\Administrator.SFTEST2>_
```

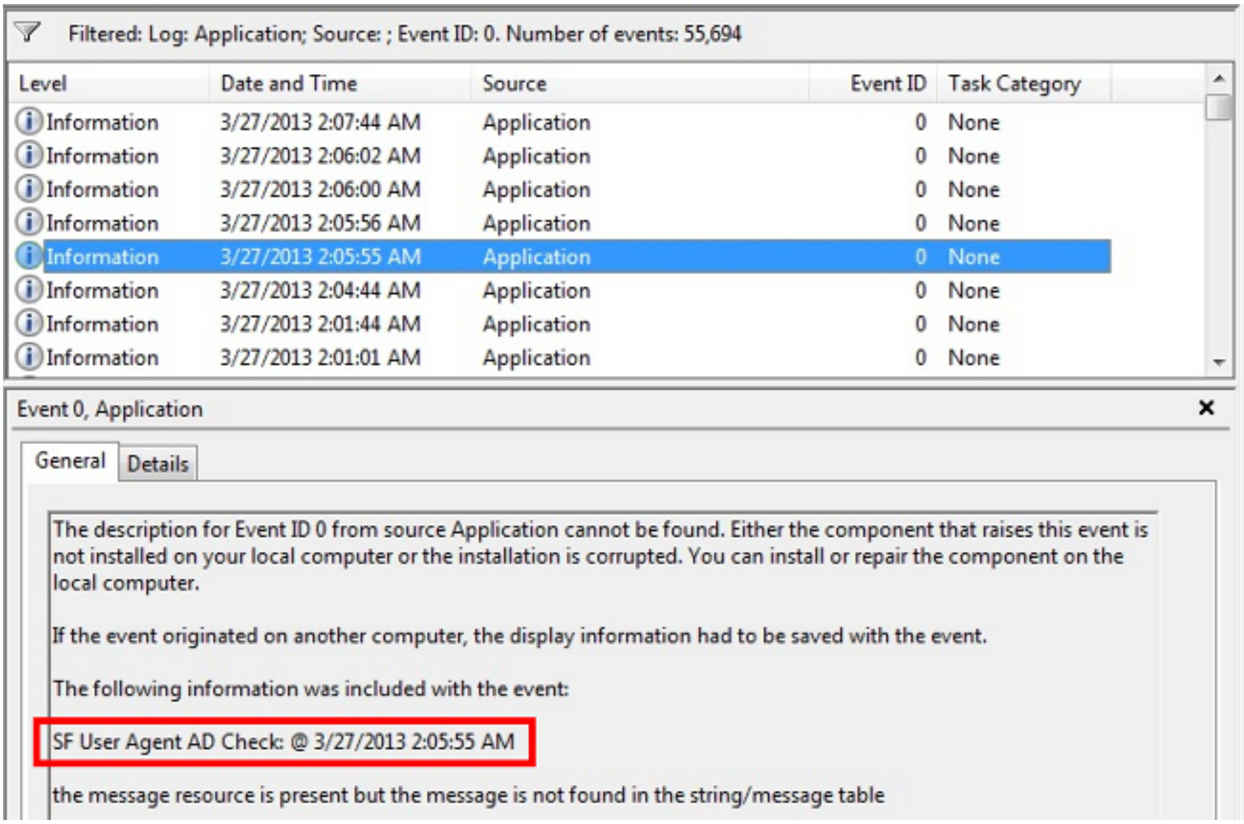
If the User Agent generates errors when connecting or authenticating to the Active Directory Server(s) there may be a network or user account permission issue. Verify that there are no network connectivity issues in your environment and temporarily configure the User Agent to use a domain admin account for authentication to the Active Directory servers for testing if possible.

Diagnostic Logging

For general troubleshooting of the User Agent, check ***Log to local event log*** within the User Agent GUI client and click ***Save***. This causes useful operational messages to be entered in the User Agent host Application event log. You can confirm that User Agent polling is completing successfully by searching for the following events, in order:

Note: The screenshots below are from the Microsoft Event Viewer on the host that is running the User Agent.

User Agent Active Directory Check


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

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.

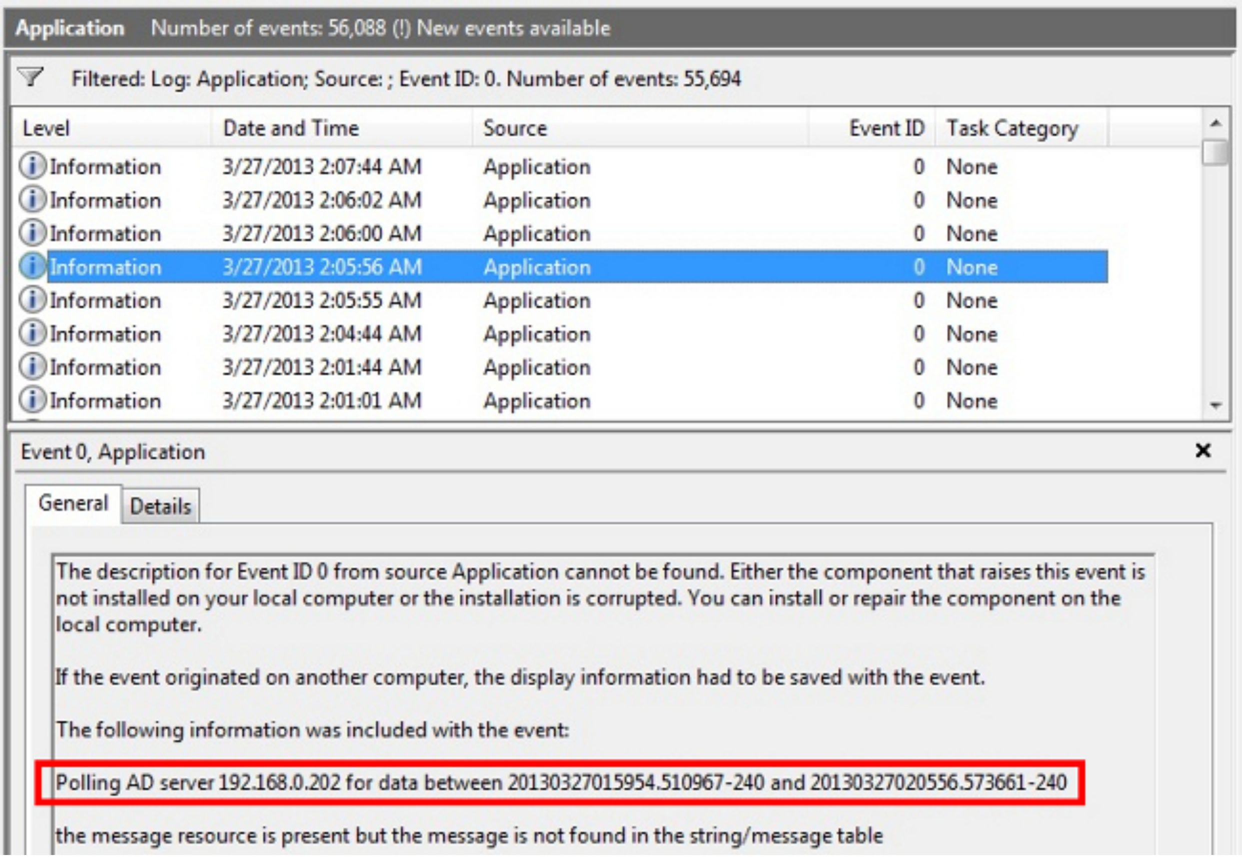
If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

SF User Agent AD Check: @ 3/27/2013 2:05:55 AM

the message resource is present but the message is not found in the string/message table

User Agent Polling Active Directory Server



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

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.

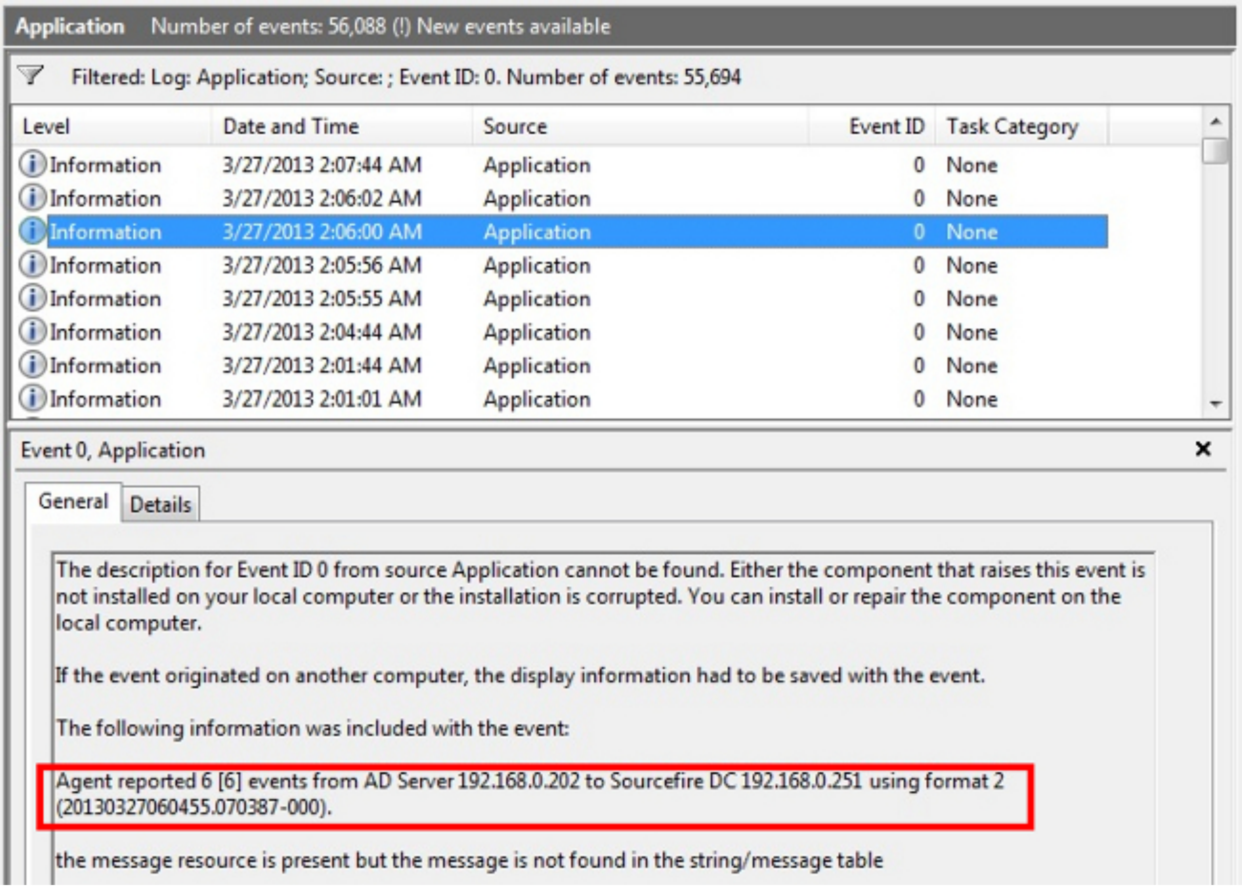
If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

Polling AD server 192.168.0.202 for data between 20130327015954.510967-240 and 20130327020556.573661-240

the message resource is present but the message is not found in the string/message table

Agent Reported Number (#) Events to the Defense Center



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

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