

Behebung von Verbindungsproblemen mit dem Sourcefire Benutzer-Agent

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Verbindungsprobleme](#)

[Diagnoseprotokollierung](#)

[Active Directory-Prüfung für Benutzer-Agent](#)

[Benutzer-Agent fragt Active Directory-Server ab](#)

[Vom Agent gemeldete Anzahl \(#\) an das Defense Center](#)

Einleitung

Der Sourcefire-Benutzeragent überwacht Microsoft Active Directory-Server und meldet sich über LDAP authentifizierte Anmeldungen und Abmeldungen an. Das FireSIGHT-System integriert diese Datensätze in die Informationen, die es durch direkte Überwachung des Netzwerkverkehrs durch verwaltete Geräte sammelt. Beim Arbeiten mit dem Sourcefire-Benutzeragenten können technische Probleme auftreten. Dieses Dokument enthält Tipps zur Behebung verschiedener Probleme mit dem Sourcefire-Benutzer-Agent.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in FireSIGHT Management Center, Sourcefire User Agent und Active Directory verfügen.

Tip: Weitere Informationen zu den Schritten für die Installation und Deinstallation von Sourcefire User Agent finden Sie in [diesem Dokument](#).

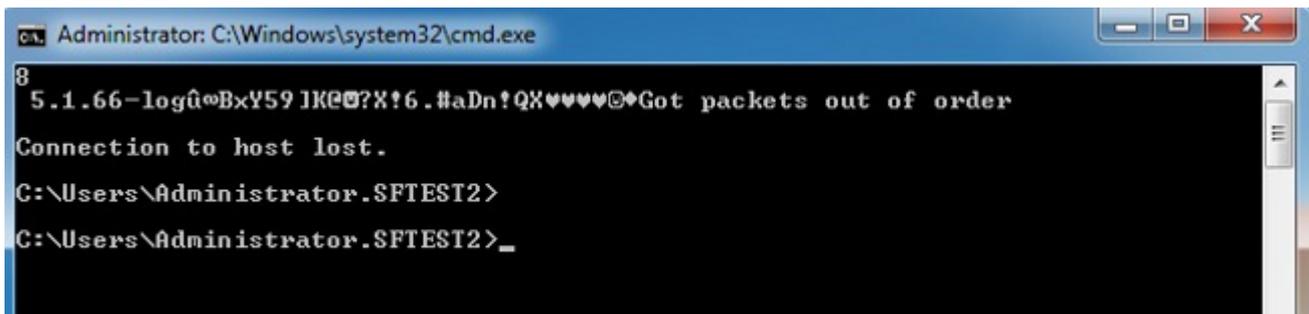
Verbindungsprobleme

1. Überprüfen Sie, ob der Benutzer-Agent zum FireSIGHT Management Center hinzugefügt wurde. Um dies zu überprüfen, navigieren Sie zu **Policies > Users > User Agent**, und überprüfen Sie, ob die IP-Adresse des konfigurierten User Agent-Hosts korrekt ist.
2. Vergewissern Sie sich, dass Port 3306 geöffnet ist, und warten Sie. Es gibt keine Firewalls oder andere Netzwerkgeräte, die die Kommunikation des Benutzer-Agenten mit dem

Defense Center unterbinden.

3. Port 3306 ist erst dann geöffnet, wenn ein Benutzer-Agent-Eintrag im FireSIGHT Management Center konfiguriert wurde.
4. Wenn auf einem Benutzer-Agent-Host Telnet installiert ist, können Sie die Verbindung überprüfen, indem Sie Telnet vom Benutzer-Agent-Host zum FireSIGHT Management Center senden. Es wird 5.1.66-log gefolgt von einer Zeichenfolge von ASCII-Zeichen angezeigt. Drücken Sie wiederholt **STRG+C**, um die Verbindung zu trennen.

Hinweis: Es wird erwartet, dass die Meldung Got packages out of order (Pakete außerhalb der Bestellung erhalten) angezeigt wird.



```
Administrator: C:\Windows\system32\cmd.exe
8
5.1.66-log@BxY59JK@?X!6.#aDn!QX♥♥♥♥@+Got packages out of order
Connection to host lost.
C:\Users\Administrator.SFTEST2>
C:\Users\Administrator.SFTEST2>_
```

Wenn der Benutzer-Agent beim Herstellen einer Verbindung oder bei der Authentifizierung von Active Directory-Server(n) Fehler generiert, kann es zu einem Netzwerk- oder Benutzerkontoberechtigungsproblem kommen. Stellen Sie sicher, dass in Ihrer Umgebung keine Netzwerkverbindungsprobleme auftreten, und konfigurieren Sie den Benutzer-Agenten vorübergehend so, dass er ein Domänenadministratorkonto für die Authentifizierung bei den Active Directory-Servern zum Testen verwendet.

Diagnoseprotokollierung

Um eine allgemeine Fehlerbehebung für den Benutzer-Agenten durchzuführen, aktivieren Sie im GUI-Client des Benutzer-Agenten das Kontrollkästchen **Log to local event log (Im lokalen Ereignisprotokoll protokollieren)**, und klicken Sie auf **Save**. Dadurch werden nützliche Betriebsmeldungen in das Anwendungsereignisprotokoll des Benutzer-Agenten-Hosts eingegeben. Sie können bestätigen, dass das Polling des Benutzer-Agents erfolgreich abgeschlossen wurde, indem Sie nach den folgenden Ereignissen suchen, um die folgende Reihenfolge einzuhalten:

Hinweis: Die folgenden Screenshots stammen aus der Microsoft Event Viewer auf dem Host, auf dem der Benutzer-Agent ausgeführt wird.

Active Directory-Prüfung für Benutzer-Agent

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:

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

Benutzer-Agent fragt Active Directory-Server ab

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:

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

Vom Agent gemeldete Anzahl (#) an das Defense Center

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.