Sourcefire User Agent に伴う接続問題のトラブルシューティング

目次

概要

Sourcefire User Agent は、Microsoft Active Directory サーバを監視して、LDAP 経由で認証されたログインとログオフを報告します。 FireSIGHT System は、管理対象デバイスによる直接ネットワーク トラフィック監視を介して収集した情報とこれらのレコードを統合します。 Sourcefire User Agent の操作中に、技術的な問題が発生することがあります。 このドキュメントでは、Sourcefire User Agent に伴うさまざまな問題をトラブルシューティングするためのヒントを提供します。

前提条件

FireSIGHT Management Center、Sourcefire User Agent、および Active Directory に精通している必要があります。

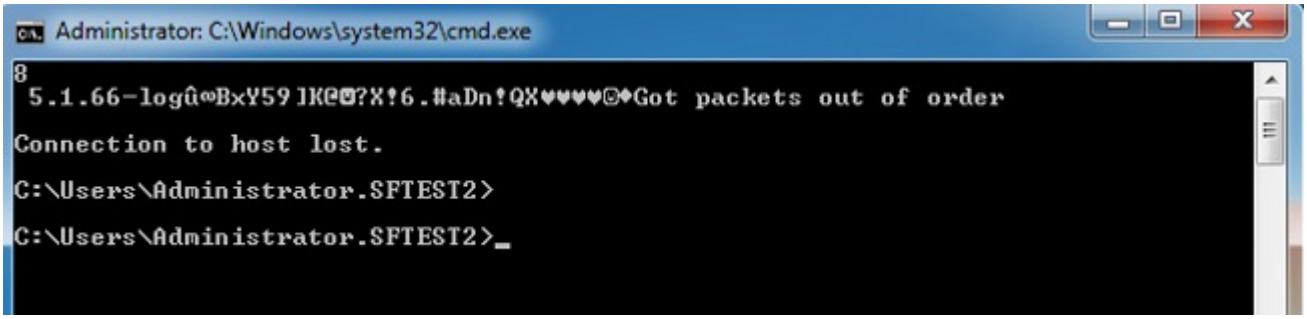
> **ヒント**： Sourcefire User Agent のインストール手順とアンインストール手順の詳細については、[このリンク先のドキュメント](#)を参照してください。

接続性の問題

1. User Agent が FireSIGHT Management Center に追加されていることを確認します。 これを確認するには、[Policies] > [Users] > [User Agent] に移動して、設定された User Agent ホストの IP アドレスが正しいことを確認します。
2. ポート 3306 が開いており、リッスンしていることを確認します。 User Agent と Defense Center 間の通信を阻害しているファイアウォールまたは他のネットワーク デバイスは存在

しません。
3. FireSIGHT Management Center で User Agent エントリが設定されるまで、ポート 3306 は開かれません。
4. User Agent ホストに Telnet がインストールされている場合は、User Agent ホストから FireSIGHT Management Center に Telnet を実行することによって、接続を確認できます。 5.1.66-log という文字列およびそれに続く ASCII 文字列が表示されます。 接続解除するには、**CTRL+C** を繰り返し押します。

注: 「Got packets out of order」というメッセージが表示されるはずです。



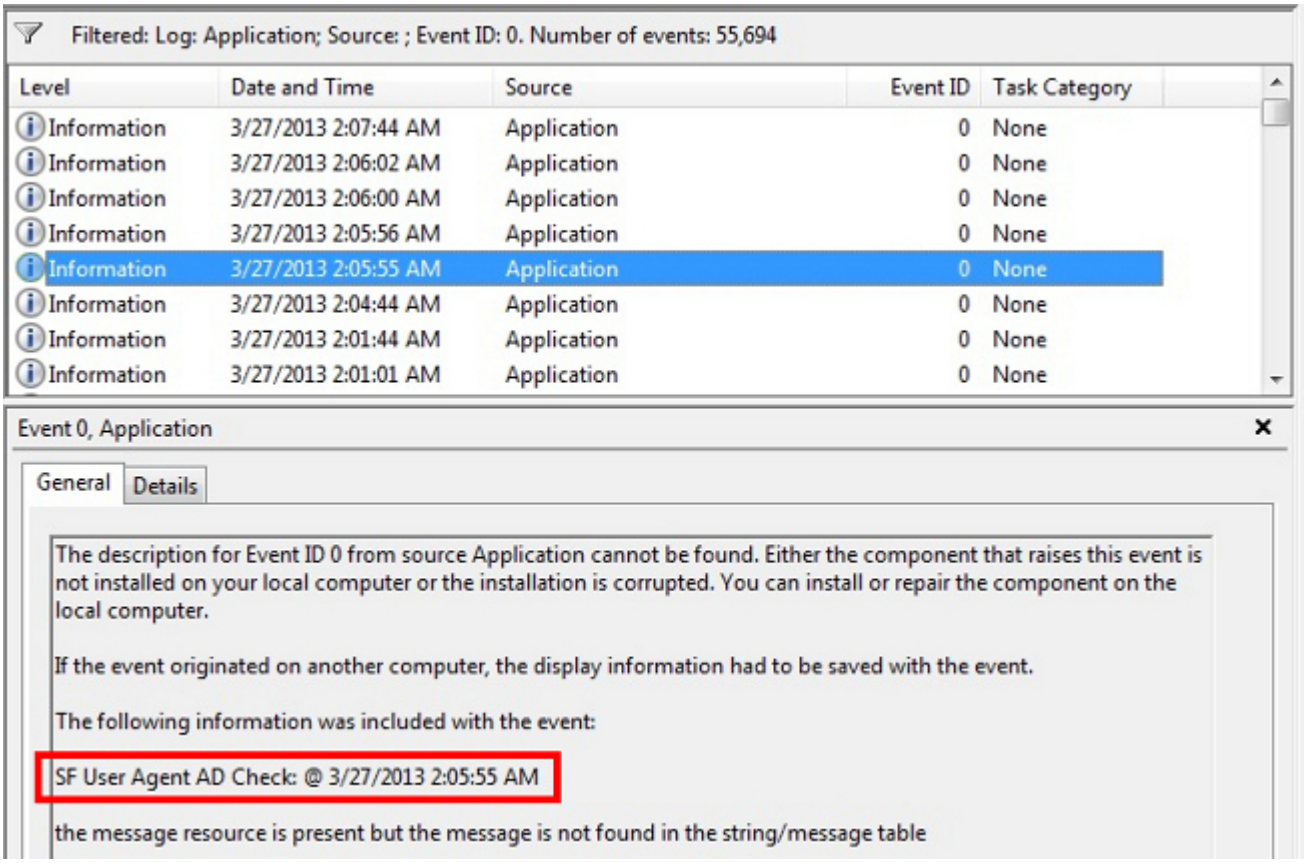
Active Directory サーバに接続中または認証中に User Agent でエラーが発生した場合は、ネットワークまたはユーザ アカウントの権限に問題がある可能性があります。 環境内にネットワーク接続の問題がないことを確認して、可能であれば、Active Directory サーバに対する認証用のドメイン管理者アカウントを使用してテストするように一時的に User Agent を設定します。

診断ロギング

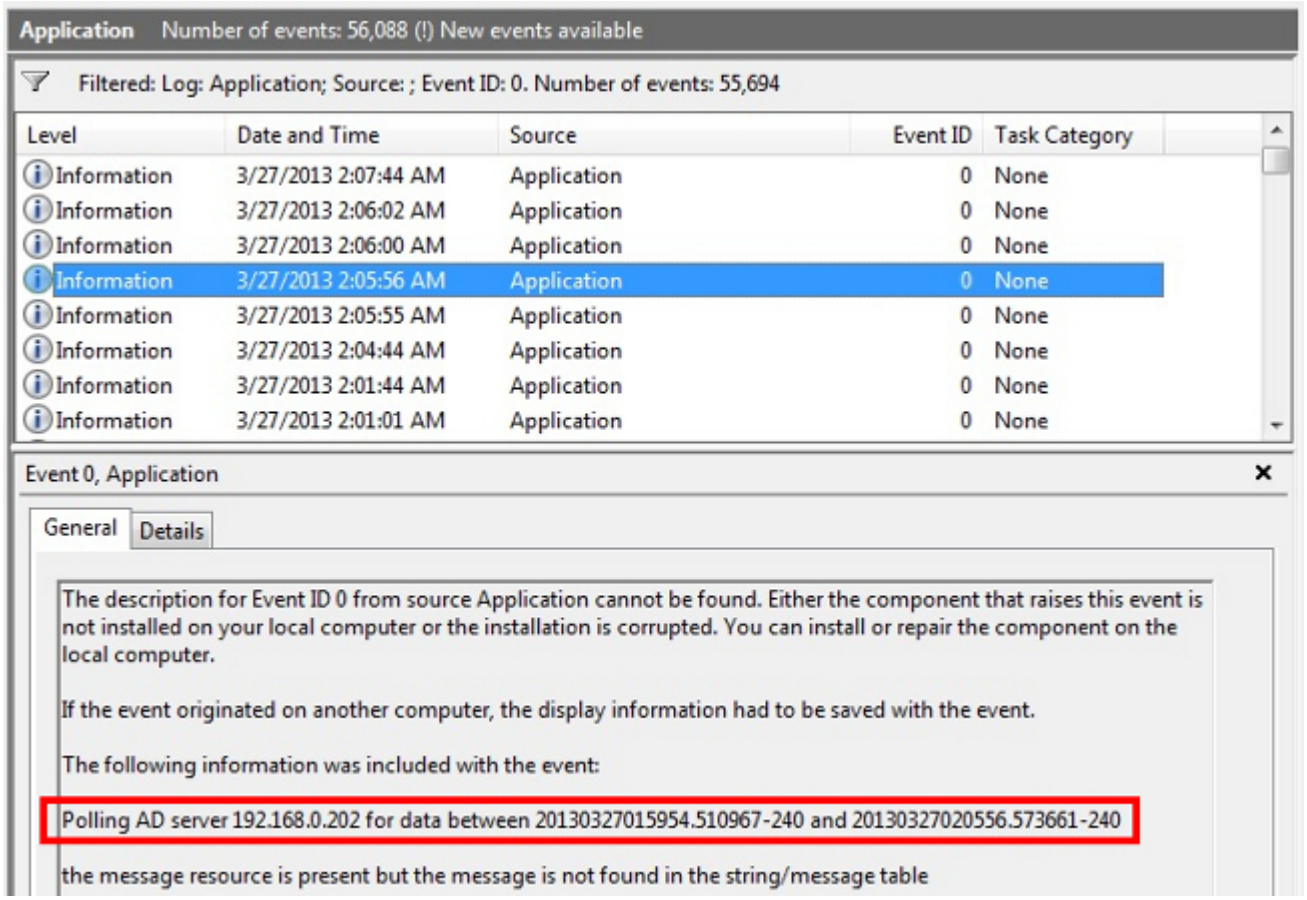
User Agent の一般的なトラブルシューティングでは、User Agent GUI クライアントで [Log to local event log] をオンにして、[Save] をクリックします。 これにより、有益な運用メッセージが User Agent ホスト アプリケーション イベント ログに記録されます。 次のイベントを順に検索することによって、User Agent ポーリングが正常に完了したかどうかを確認できます。

注: 次のスクリーンショットは、User Agent を実行しているホスト上の Microsoft イベント ビューアの出力です。

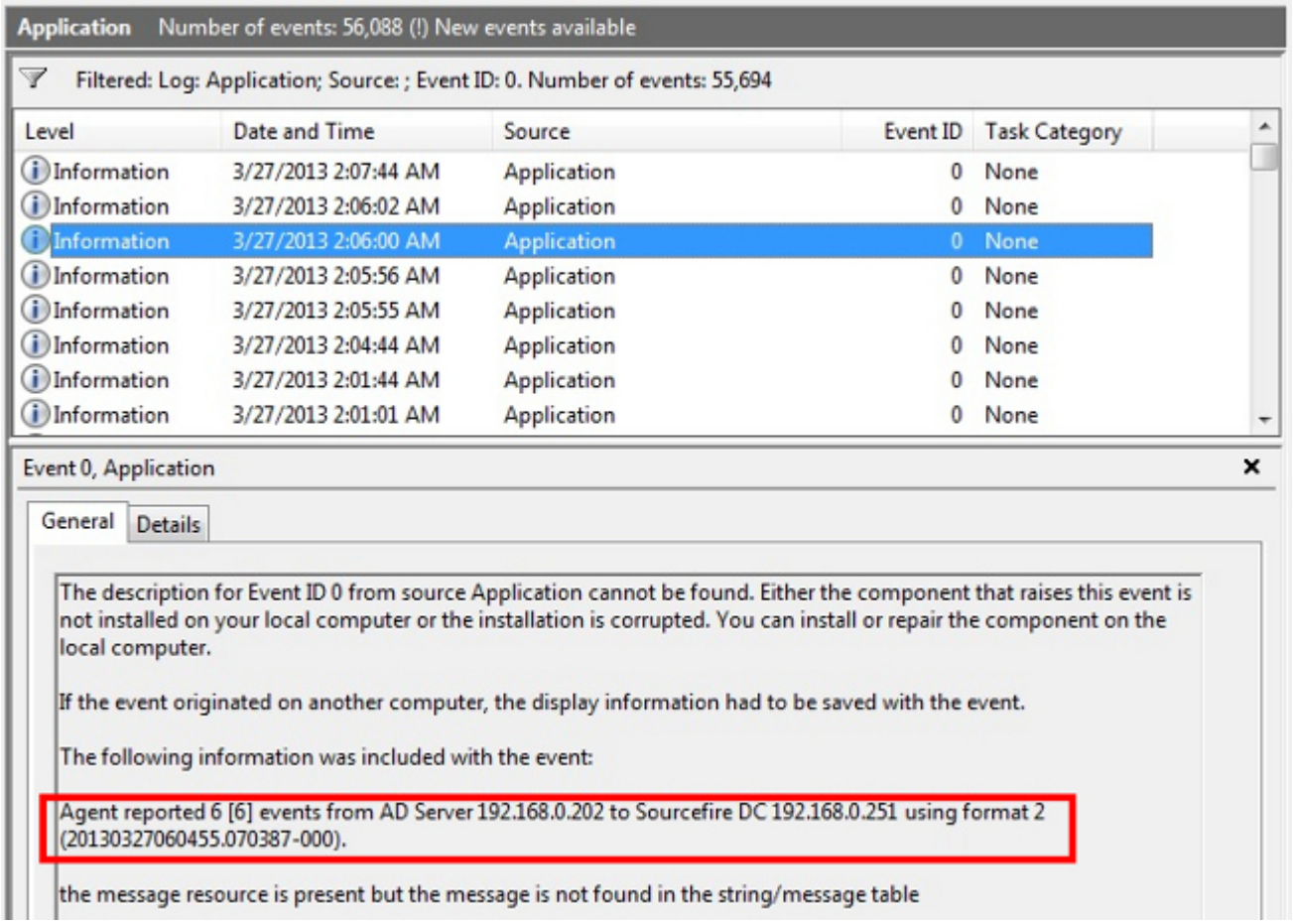
User Agent の Active Directory のチェック



User Agent の Active Directory サーバのポーリング



Agent から Defense Center に報告された番号（＃）イベント


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