

# Solucione problemas de conectividade com o agente de usuário do Sourcefire

## Contents

[Introdução](#)

[Pré-requisitos](#)

[Problemas de conectividade](#)

[Registro de diagnóstico](#)

[Verificação do Ative Directory do Agente do Usuário](#)

[Servidor do Ative Directory de Sondagem do Agente do Usuário](#)

[Eventos de Número Relatado \(#\) do Agente para o Centro de Defesa](#)

## Introdução

O Sourcefire User Agent monitora os servidores do Microsoft Active Directory e relata logons e logoffs autenticados via LDAP. O sistema FireSIGHT integra esses registros com as informações coletadas por meio da observação direta do tráfego de rede por dispositivos gerenciados. Ao trabalhar com o Sourcefire User Agent, você poderá ter problemas técnicos. Este documento fornece dicas para solucionar vários problemas com o Sourcefire User Agent.

## Pré-requisitos

A Cisco recomenda que você tenha conhecimento sobre o FireSIGHT Management Center, o Sourcefire User Agent e o Active Directory.

---

Dica: para saber mais sobre as etapas de instalação e desinstalação do Sourcefire User Agent, leia [este documento](#).

---

## Problemas de conectividade

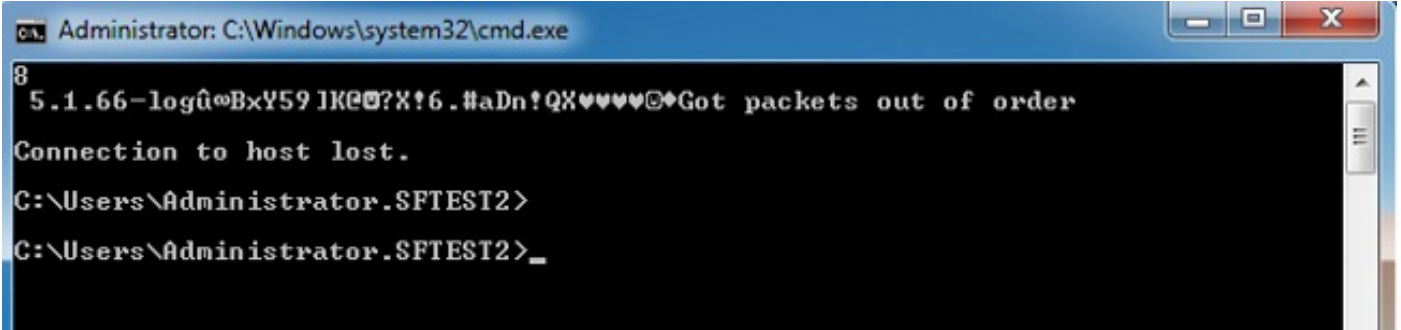
1. Verifique se o agente de usuário foi adicionado ao FireSIGHT Management Center. Para verificar isso, navegue até Políticas > Users > User Agent e verifique se o endereço IP do host do User Agent configurado está correto.
2. Confirme se a porta 3306 está aberta e ouvindo. Não há firewalls ou outros dispositivos de rede impedindo que o agente de usuário se comunique com o Defense Center.
3. A porta 3306 não será aberta até que uma entrada do agente de usuário tenha sido configurada no FireSIGHT Management Center.
4. Se um host do agente de usuário tiver o telnet instalado, você poderá verificar a conexão

por telnet do host do agente de usuário para o FireSIGHT Management Center. Você verá 5.1.66-log seguido por uma sequência de caracteres ASCII. Pressione CTRL+C várias vezes para desconectar.

---

Observação: a aparência da mensagem Got packout of order é esperada.

---



```
Administrator: C:\Windows\system32\cmd.exe
8
5.1.66-log@BxY59IK@?X!6.#aDn!QX♥♥♥♥@Got packets out of order
Connection to host lost.
C:\Users\Administrator.SFTEST2>
C:\Users\Administrator.SFTEST2>_
```

Se o agente de usuário gerar erros ao se conectar ou autenticar no(s) servidor(es) do Active Directory, pode haver um problema de permissão de conta de usuário ou de rede. Verifique se não há problemas de conectividade de rede em seu ambiente e configure temporariamente o Agente do Usuário para usar uma conta de administrador de domínio para autenticação nos servidores do Active Directory para teste, se possível.

## Registro de diagnóstico

Para a solução geral de problemas do agente de usuário, marque Log to local event log no cliente da GUI do agente de usuário e clique em Save. Isso faz com que mensagens operacionais úteis sejam inseridas no log de eventos do Aplicativo host do Agente do Usuário. Você pode confirmar se a pesquisa de agente de usuário está sendo concluída com êxito pesquisando os seguintes eventos, na ordem:

---

Observação: as capturas de tela abaixo são do Visualizador de Eventos da Microsoft no host que está executando o Agente de Usuário.

---

## Verificação do Active Directory do Agente do Usuário

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

Servidor do Ative Diretory de Sondagem do Agente do Usuário

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

Eventos de Número Relatado (#) do Agente para o Centro de Defesa

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

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.