Pesquise defeitos problemas de conectividade com agente de usuário de Sourcefire

Índice

Introdução

Server do microsoft ative directory dos monitores do agente de usuário de Sourcefire e inícios de uma sessão e fazer logoff do relatório autenticados através do LDAP. O sistema de FireSIGHT integra estes registros com a informação que recolhe através da observação direta do tráfego de rede por dispositivos gerenciado. Quando você está trabalhando com o agente de usuário de Sourcefire, você pode experimentar questões técnica. Este documento fornece pontas para pesquisar defeitos várias edições com o agente de usuário de Sourcefire.

Pré-requisitos

Cisco recomenda que você tem o conhecimento no centro de gerenciamento de FireSIGHT, no agente de usuário de Sourcefire, e no diretório ativo.

> Dica: A fim aprender mais sobre as etapas da instalação e da desinstalação do agente de usuário de Sourcefire, leia este documento.

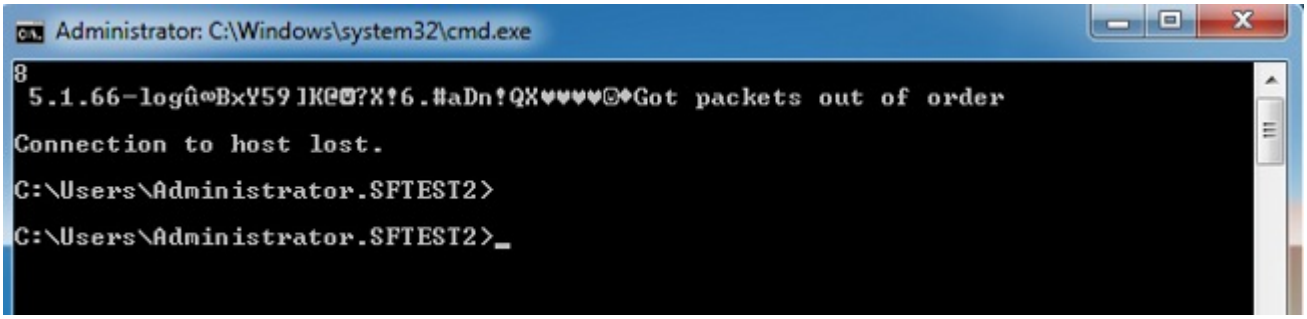
Problemas de conectividade

1. Verifique que o agente de usuário está adicionado ao centro de gerenciamento de FireSIGHT. Para verificar isso, navegue às **políticas > aos usuários > ao agente de usuário** e verifique que o endereço IP de Um ou Mais Servidores Cisco ICM NT do host configurado do agente de usuário está correto.
2. Confirme que a porta 3306 é aberta e escutando. Não há nenhum Firewall ou outros

dispositivos de rede que param o agente de usuário da comunicação com o centro da defesa.

3. A porta 3306 não estará aberta até que uma entrada do agente de usuário esteja configurada no centro de gerenciamento de FireSIGHT.
4. Se um host do agente de usuário tem o telnet instalado, você pode verificar a conexão telneting do host do agente de usuário ao centro de gerenciamento de FireSIGHT. Você verá `5.1.66-log` seguido por uma corda de caracteres ASCII. Pressione o **CTRL+C** repetidamente para desligar.

Nota: A aparência de `pacotes Got` mensagem `fora de serviço` é esperada.



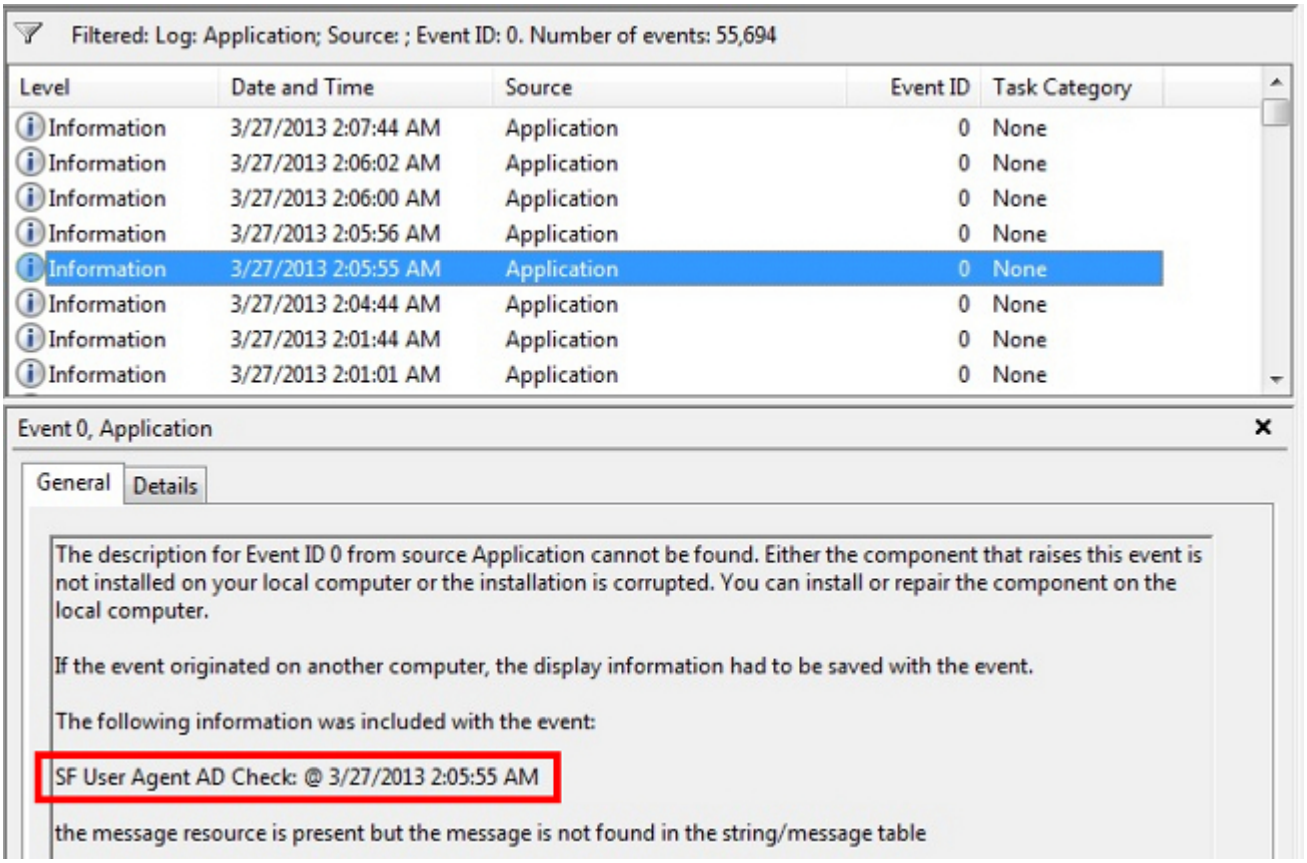
Se o agente de usuário gerencie erros ao conectar ou ao autenticar aos server do diretório ativo pode haver uma edição da permissão da rede ou da conta de usuário. Verifique que não há nenhuma questão de conectividade de rede em seu ambiente e configurar temporariamente o agente de usuário para usar um domínio admin esclarecem a autenticação aos servidores ative directory para testar se possível.

Registro diagnóstico

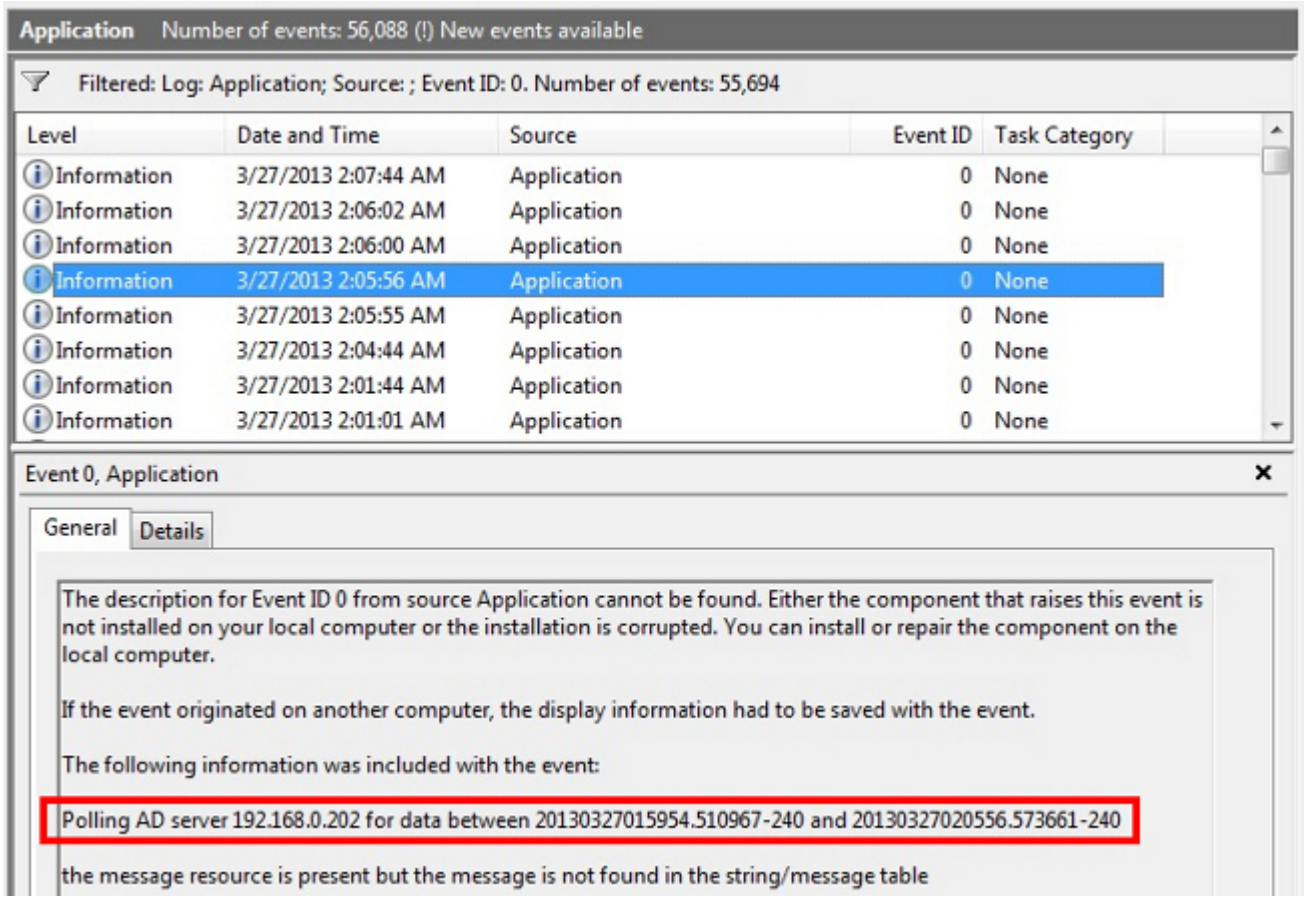
Para o Troubleshooting geral do agente de usuário, verifique o **log ao log de eventos local** dentro do cliente GUI do agente de usuário e clique a **salvaguarda**. Isto faz com que as mensagens operacionais úteis sejam incorporadas ao log de eventos do aplicativo do host do agente de usuário. Você pode confirmar que a votação do agente de usuário está terminando com sucesso procurando pelos seguintes eventos, em ordem:

Nota: Os screenshots abaixo são do Microsoft Event Viewer no host que está executando o agente de usuário.

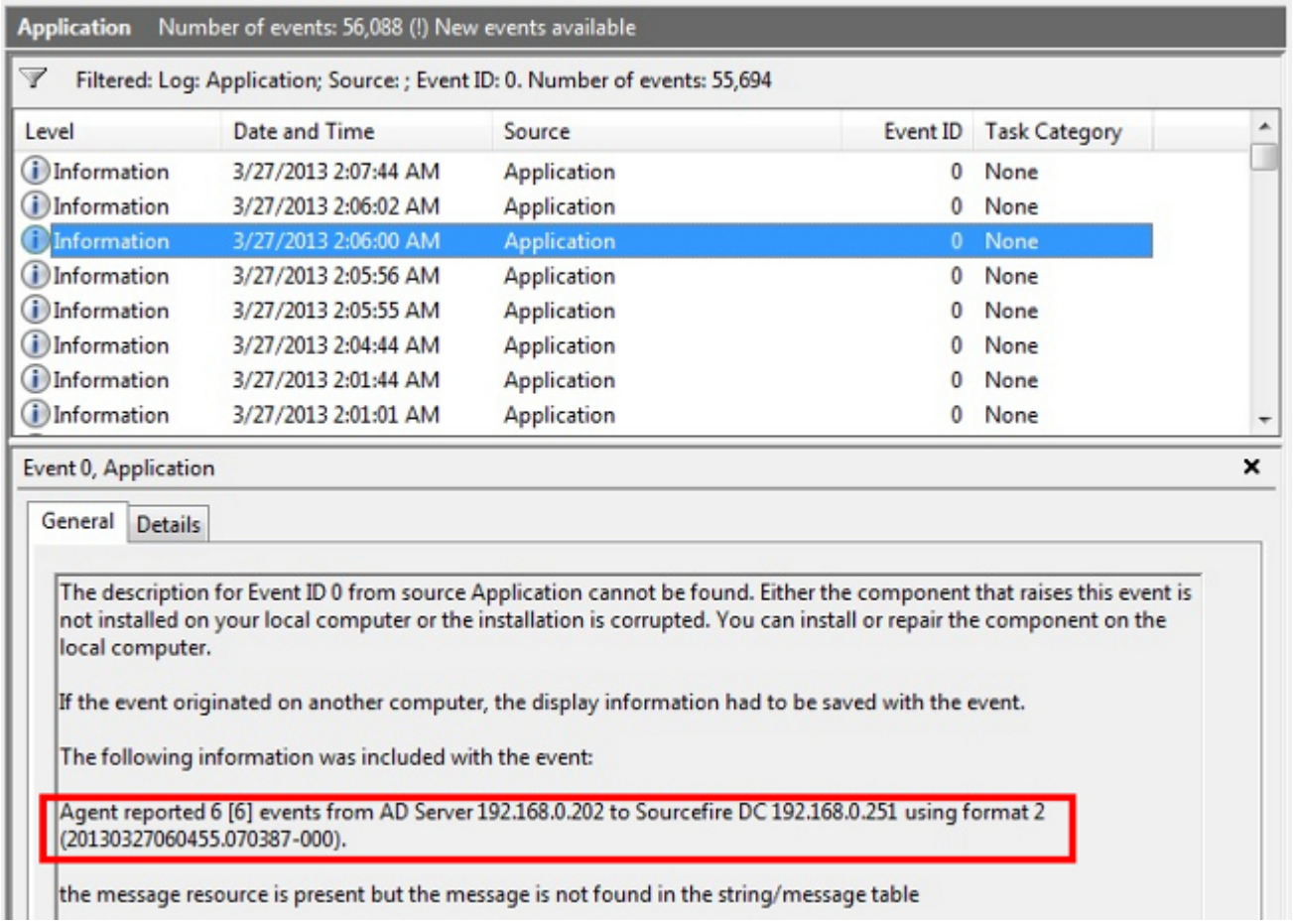
Verificação do diretório ativo do agente de usuário



Servidor ative directory da votação do agente de usuário



Eventos relatados agente do número (#) ao centro da 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