Connectiviteitsproblemen oplossen met Sourcefire User Agent

Inhoud

Inleiding

Sourcefire User Agent bewaakt Microsoft Active Directory-servers en rapporteert logins en logins die zijn geverifieerd via LDAP. Het FireSIGHT System integreert deze records met de informatie die het verzamelt via directe netwerkverkeerswaarneming door beheerde apparaten. Wanneer u met de Sourcefire User Agent werkt, kunt u technische problemen ondervinden. Dit document bevat tips voor het oplossen van verschillende problemen met de Sourcefire User Agent.

Voorwaarden

Cisco raadt u aan kennis te hebben van FireSIGHT Management Center, Sourcefire User Agent en Active Directory.

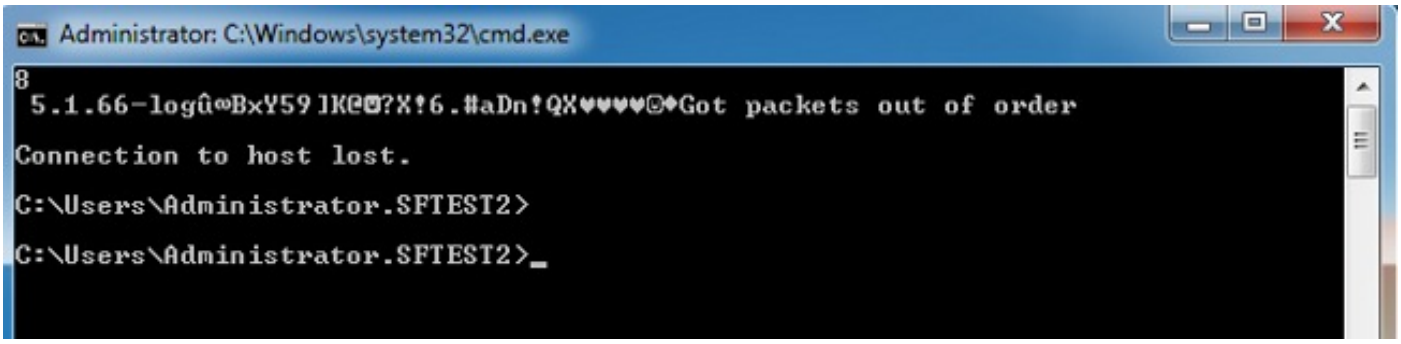
> Tip: Lees dit document om meer te weten te komen over de installatie- en verwijderingsstappen van de Sourcefire User Agent.

Connectiviteitsproblemen

1. Controleer of de User Agent is toegevoegd aan het FireSIGHT Management Center. Om te verifiëren dat, navigeer naar Beleid > Gebruikers > User Agent en controleer dat het IP-adres van de geconfigureerde User Agent-host correct is.
2. Bevestig dat Port 306 open is en luistert. Er zijn geen firewalls of andere netwerkapparaten die de User Agent verhinderen te communiceren met het Defense Center.
3. Port 3306 wordt pas geopend nadat een User Agent-vermelding op het FireSIGHT Management Center is geconfigureerd.
4. Als een User Agent-host Telnet heeft geïnstalleerd, kunt u de verbinding verifiëren door de

User Agent-host te telneteren naar het FireSIGHT Management Center. U ziet 5.1.66-log gevolgd door een reeks ASCII-tekens. Druk herhaaldelijk op CTRL+C om de verbinding te verbreken.

Opmerking: het bericht Got packets out of order wordt verwacht.



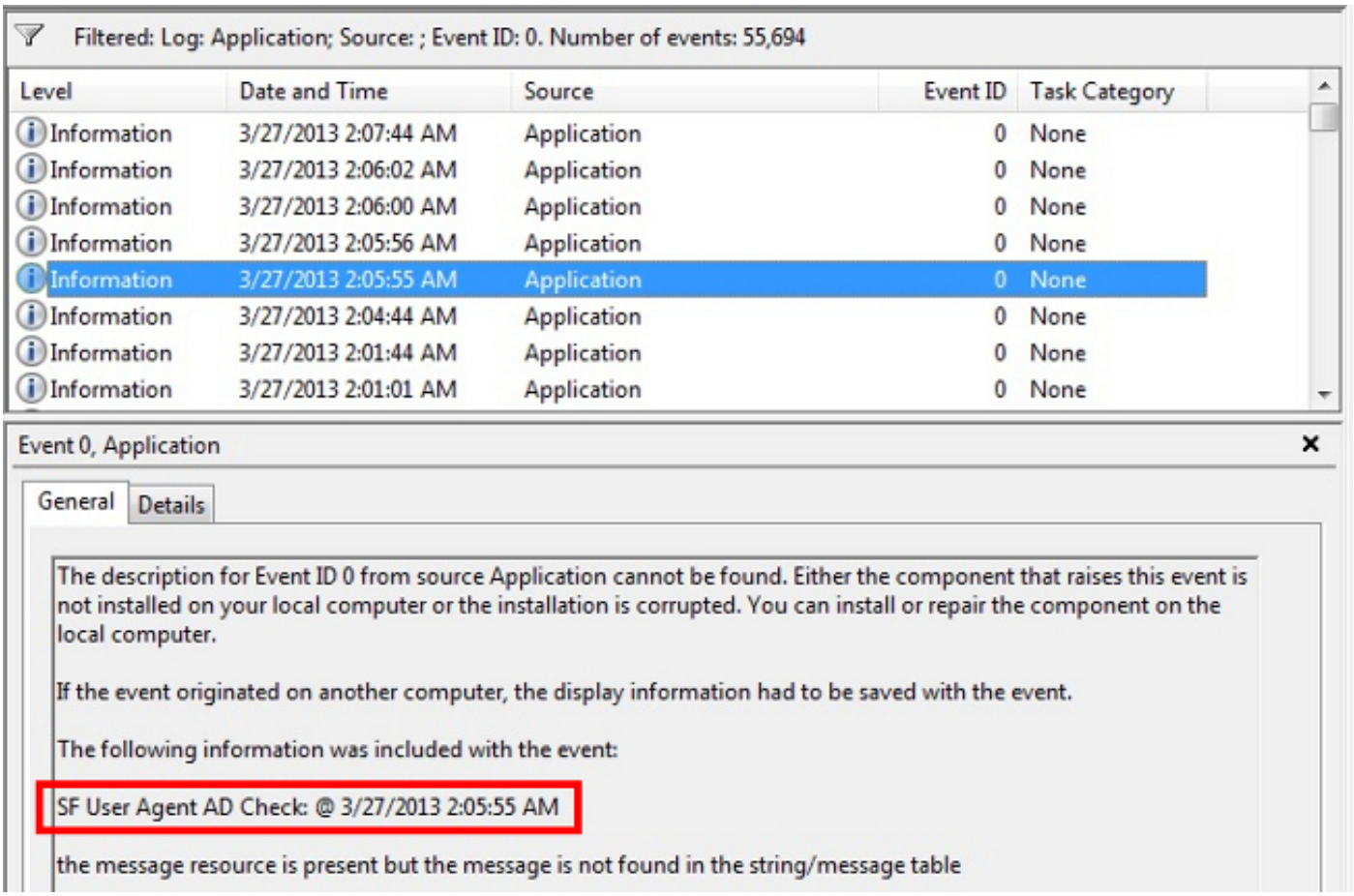
Als de User Agent fouten genereert bij het verbinden met of verifiëren van de Active Directory-server(s), kan er een probleem zijn met de toestemming van een netwerk- of gebruikersaccount. Controleer of er geen problemen zijn met de netwerkverbinding in uw omgeving en stel de User Agent tijdelijk in om een domeinadmin-account te gebruiken voor verificatie naar de Active Directory-servers voor zo mogelijk testen.

Vastlegging diagnoses

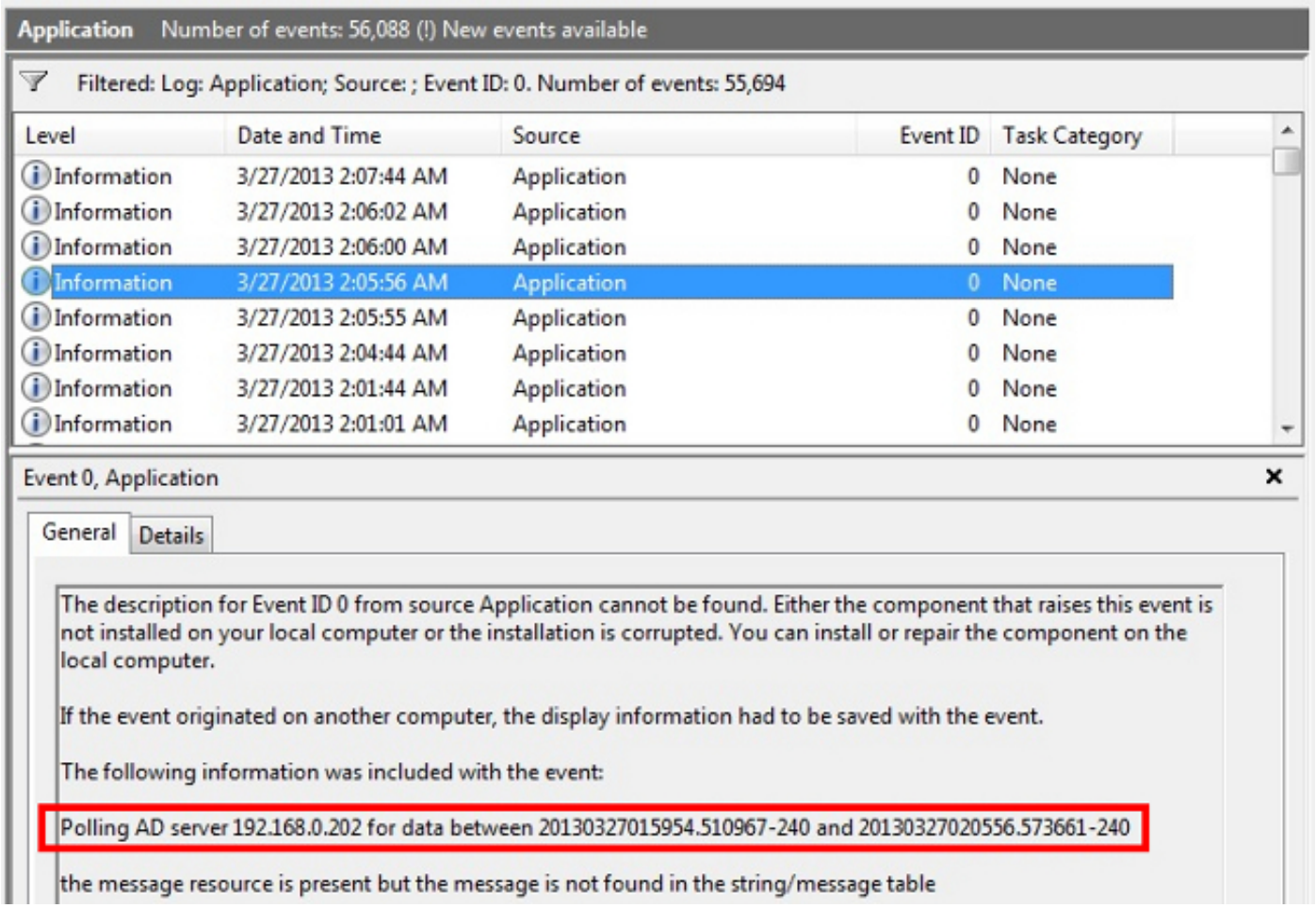
Voor algemene probleemoplossing van de User Agent selecteert u Log in op het lokale gebeurtenissenlogboek binnen de User Agent GUI-client en klikt u op Opslaan. Hierdoor worden nuttige operationele berichten ingevoerd in het gebeurtenissenlogboek van de User Agent-host. U kunt bevestigen dat de opiniepeiling van User Agent met succes wordt afgerond door te zoeken naar de volgende gebeurtenissen, in volgorde:

Opmerking: De screenshots hieronder zijn afkomstig uit de Microsoft Event Viewer op de host waarop de User Agent wordt uitgevoerd.

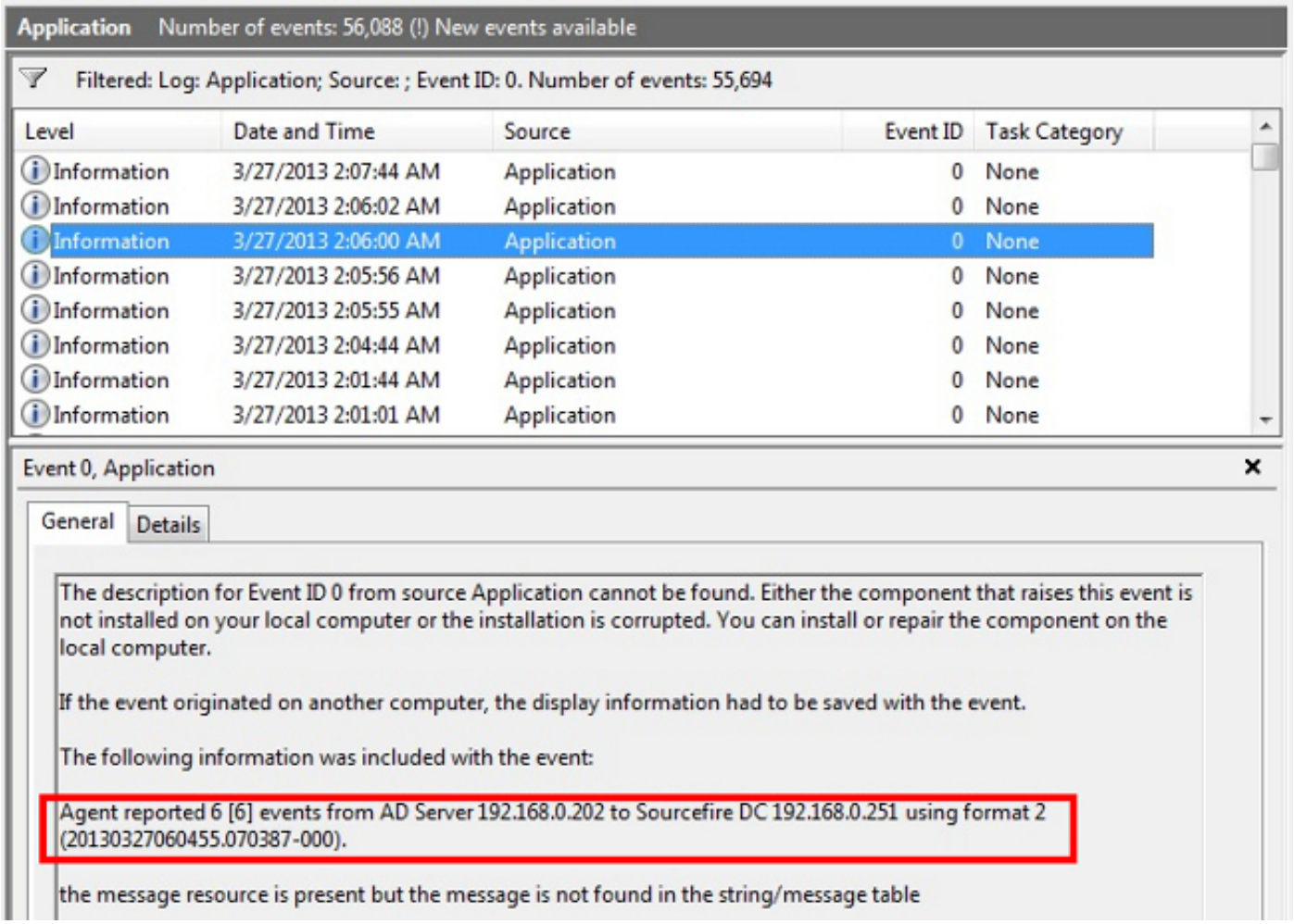
Active Directory-controle van User Agent



User Agent Polling Active Directory-server



Gebeurtenissen van Agent met nummer (#) naar het 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
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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.