Résolution des problèmes de connectivité avec Sourcefire User Agent

Table des matières

Introduction

Sourcefire User Agent surveille les serveurs Microsoft Active Directory et signale les connexions et déconnexions authentifiées via LDAP. FireSIGHT System intègre ces enregistrements aux informations collectées via l'observation directe du trafic réseau par les périphériques gérés. Lorsque vous travaillez avec l'agent utilisateur Sourcefire, vous pouvez rencontrer des problèmes techniques. Ce document fournit des conseils pour dépanner divers problèmes avec l'agent utilisateur Sourcefire.

Conditions préalables

Cisco recommande que vous ayez des connaissances sur FireSIGHT Management Center, Sourcefire User Agent et Active Directory.

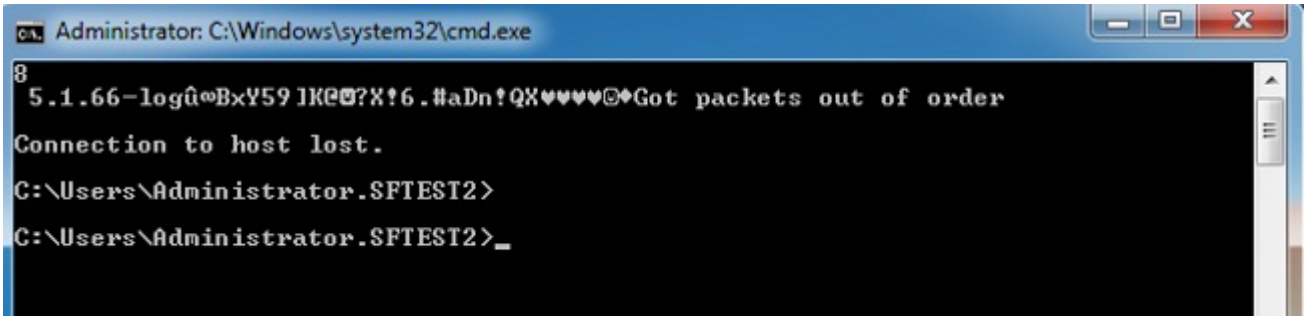
> **Conseil** : pour en savoir plus sur les étapes d'installation et de désinstallation de l'agent utilisateur Sourcefire, lisez ce document.

Problèmes de connectivité

1. Vérifiez que l'agent utilisateur est ajouté à FireSIGHT Management Center. Pour vérifier cela, accédez à **Policies > Users > User Agent** et vérifiez que l'adresse IP de l'hôte User Agent configuré est correcte.
2. Vérifiez que le port 3306 est ouvert et en écoute. Aucun pare-feu ou autre périphérique réseau n'empêche l'agent utilisateur de communiquer avec le Centre de défense.

3. Le port 3306 ne sera pas ouvert tant qu'une entrée User Agent n'aura pas été configurée sur FireSIGHT Management Center.
4. Si un hôte Agent utilisateur est équipé de la fonction Telnet, vous pouvez vérifier la connexion en vous connectant par Telnet à partir de l'hôte Agent utilisateur à FireSIGHT Management Center. Vous verrez 5.1.66-log suivi d'une chaîne de caractères ASCII. Appuyez sur **CTRL+C** à plusieurs reprises pour vous déconnecter.

   Remarque : le message Got packets out of order est attendu.



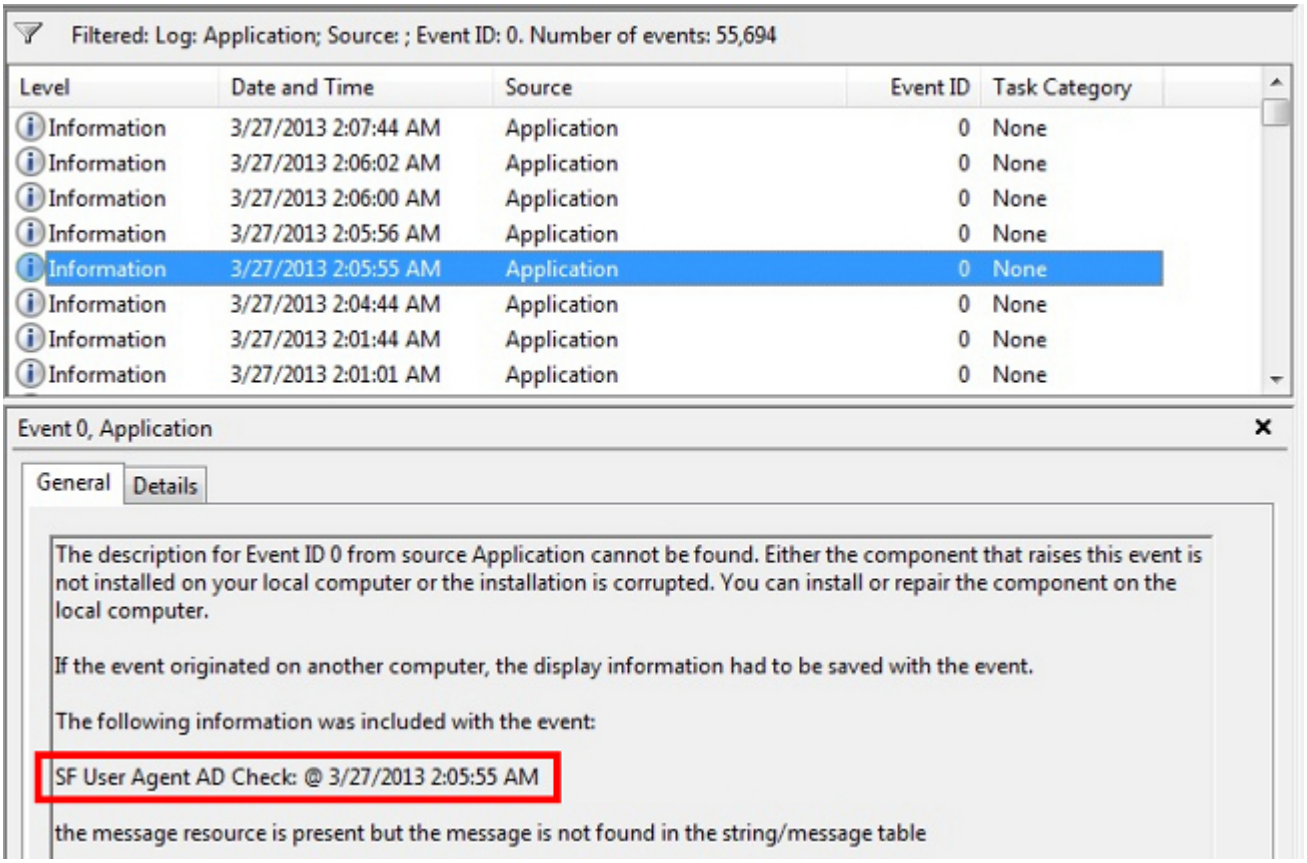
Si l'agent utilisateur génère des erreurs lors de la connexion ou de l'authentification au(x) serveur(s) Active Directory, il peut y avoir un problème d'autorisation de compte d'utilisateur ou de réseau. Vérifiez qu'il n'y a aucun problème de connectivité réseau dans votre environnement et configurez temporairement l'agent utilisateur pour qu'il utilise un compte d'administrateur de domaine pour l'authentification aux serveurs Active Directory afin de les tester si possible.

Journaux de diagnostic

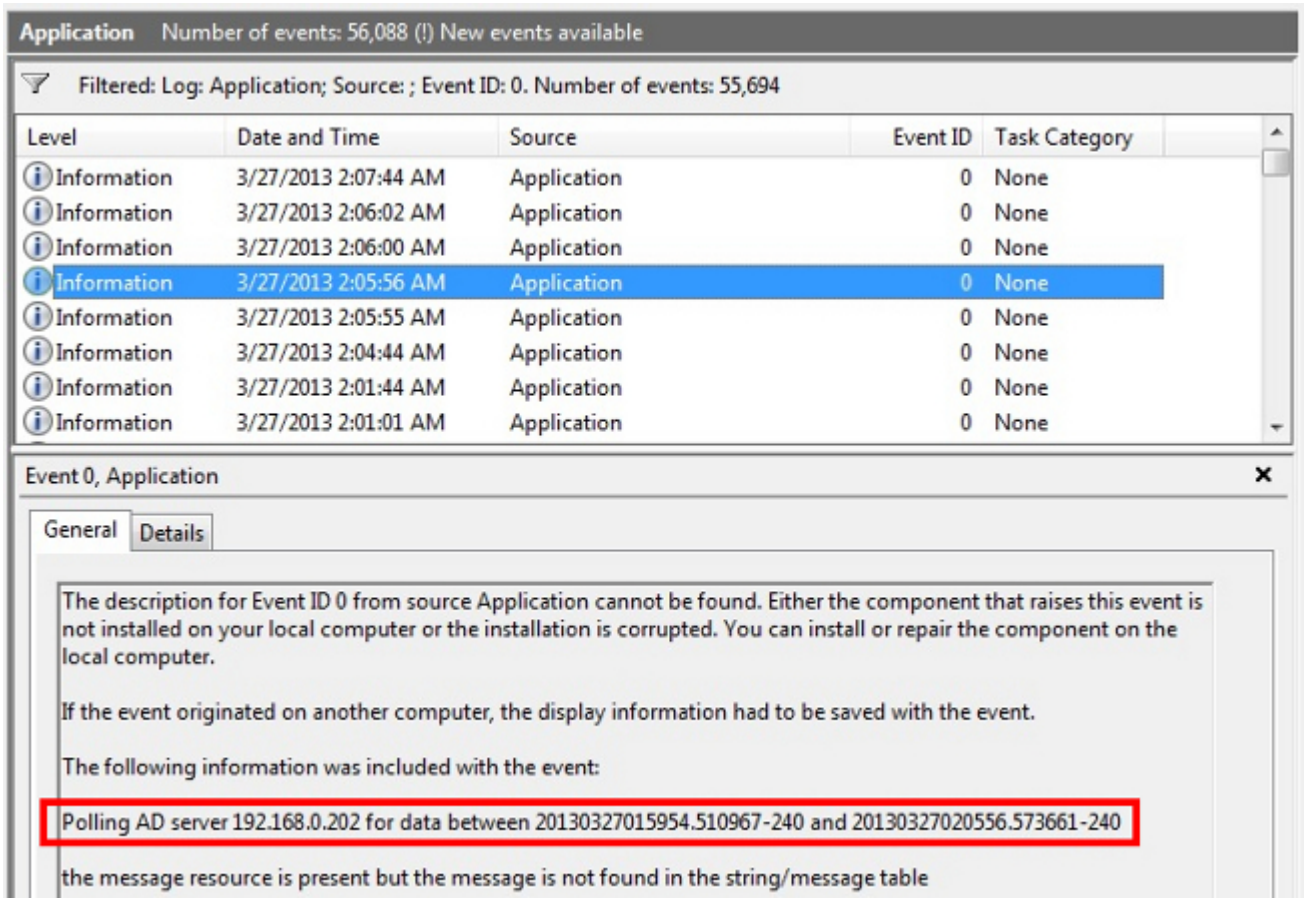
Pour un dépannage général de l'agent utilisateur, vérifiez **Log to local event log** dans le client GUI de l'agent utilisateur et cliquez sur **Save**. Cela entraîne la saisie de messages opérationnels utiles dans le journal des événements de l'application hôte de l'agent utilisateur. Vous pouvez confirmer que l'interrogation de l'agent utilisateur s'est terminée correctement en recherchant les événements suivants, dans l'ordre :

Remarque : les captures d'écran ci-dessous proviennent de l'Observateur d'événements Microsoft sur l'hôte qui exécute l'agent utilisateur.

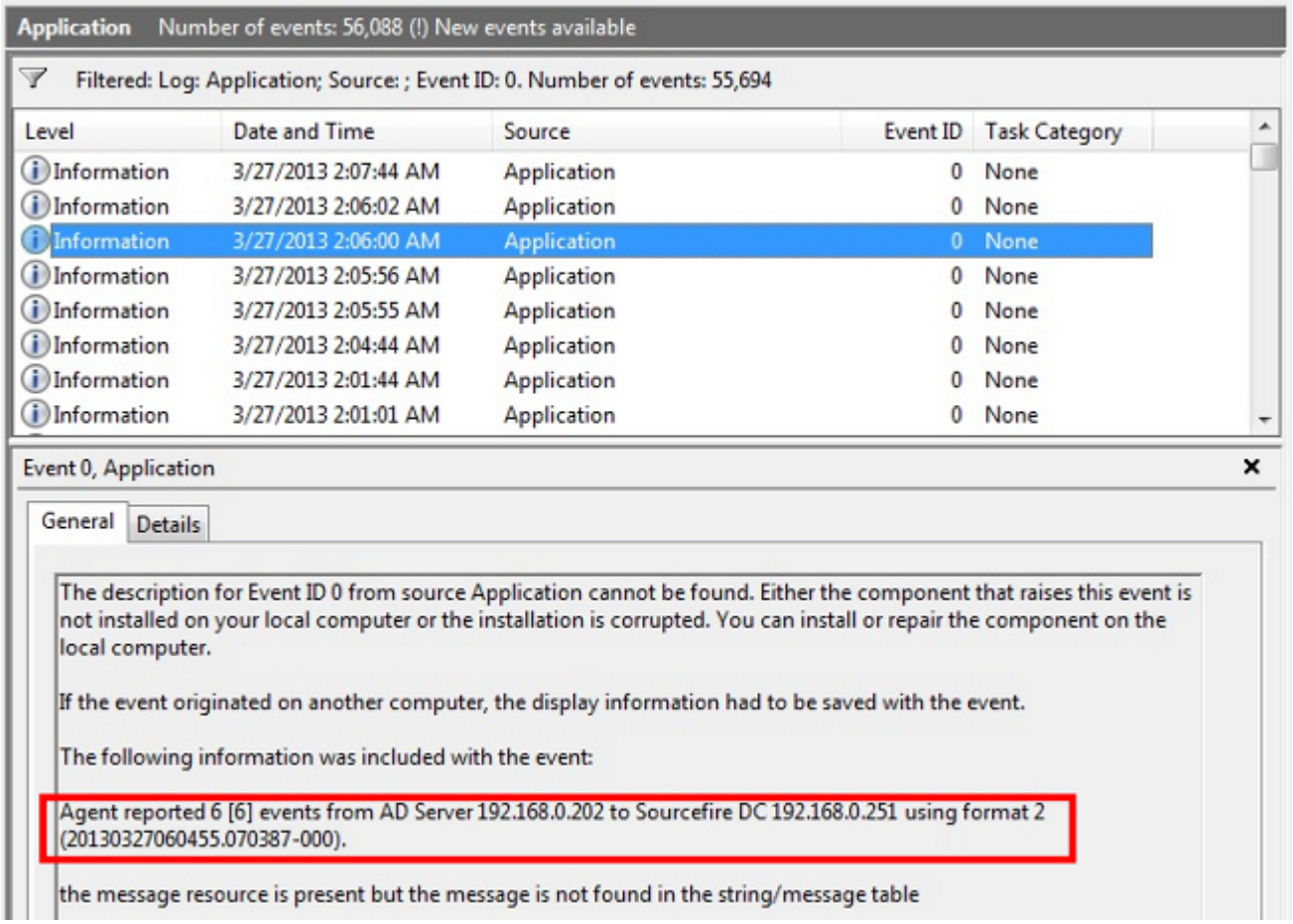
Vérification Active Directory de l'agent utilisateur



Agent utilisateur interrogeant le serveur Active Directory



Nombre d'événements signalés par l'agent (#) au Centre de défense


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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.