Dépannez les problèmes de connectivité avec l'agent d'utilisateur de Sourcefire

Contenu

Introduction

Serveurs de Microsoft Active Directory de moniteurs d'agent d'utilisateur de Sourcefire et procédures de connexion et déconnexions d'état authentifiées par l'intermédiaire du LDAP. Le système de FireSIGHT intègre ces enregistrements avec les informations qu'il collecte par l'intermédiaire de l'observation directe du trafic réseau par des périphériques gérés. Quand vous fonctionnez avec l'agent d'utilisateur de Sourcefire, vous pouvez éprouver des problèmes techniques. Ce document fournit des conseils pour dépanner de diverses questions avec l'agent d'utilisateur de Sourcefire.

Conditions préalables

Cisco recommande que vous ayez la connaissance au centre de Gestion de FireSIGHT, à l'agent d'utilisateur de Sourcefire, et au Répertoire actif.

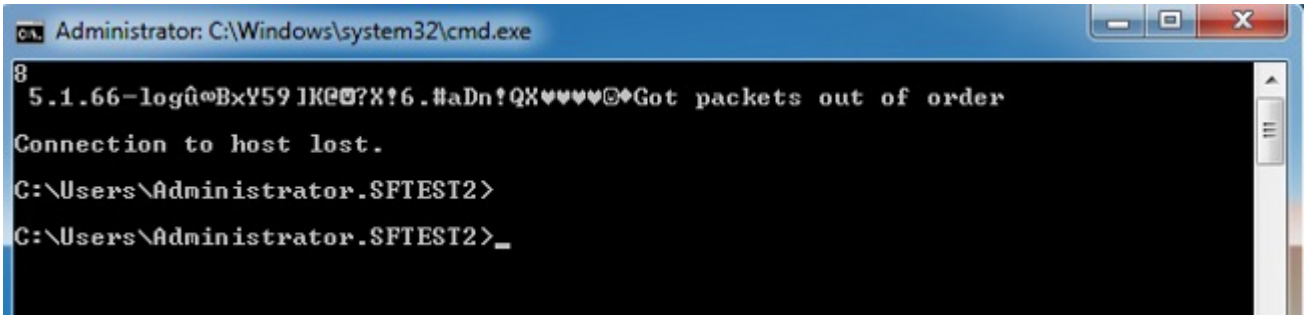
> **Conseil** : Afin de se renseigner plus sur les étapes d'installation et d'uninstallation de l'agent d'utilisateur de Sourcefire, lisez ce document.

Problèmes de connectivité

1. Vérifiez que l'agent d'utilisateur est ajouté au centre de Gestion de FireSIGHT. Pour vérifier cela, naviguez vers des **stratégies > des utilisateurs > l'agent d'utilisateur** et vérifiez que l'adresse IP de l'hôte configuré d'agent d'utilisateur est correcte.
2. Confirmez que le port 3306 est ouvert et écoute. Il n'y a aucun Pare-feu ou d'autres périphériques de réseau arrêtant l'agent d'utilisateur de la communication avec le centre de

la défense.
3. Le port 3306 ne sera pas ouvert jusqu'à ce qu'une entrée d'agent d'utilisateur ait été configurée au centre de Gestion de FireSIGHT.
4. Si un hôte d'agent d'utilisateur a le telnet installé, vous pouvez vérifier la connexion par telneting de l'hôte d'agent d'utilisateur au centre de Gestion de FireSIGHT. Vous verrez `5.1.66-log` suivi d'une chaîne des caractères ASCII. Presse **CTRL+C** à plusieurs reprises à déconnecter.

Note: L'apparence du message `en panne de paquets Got` est prévue.



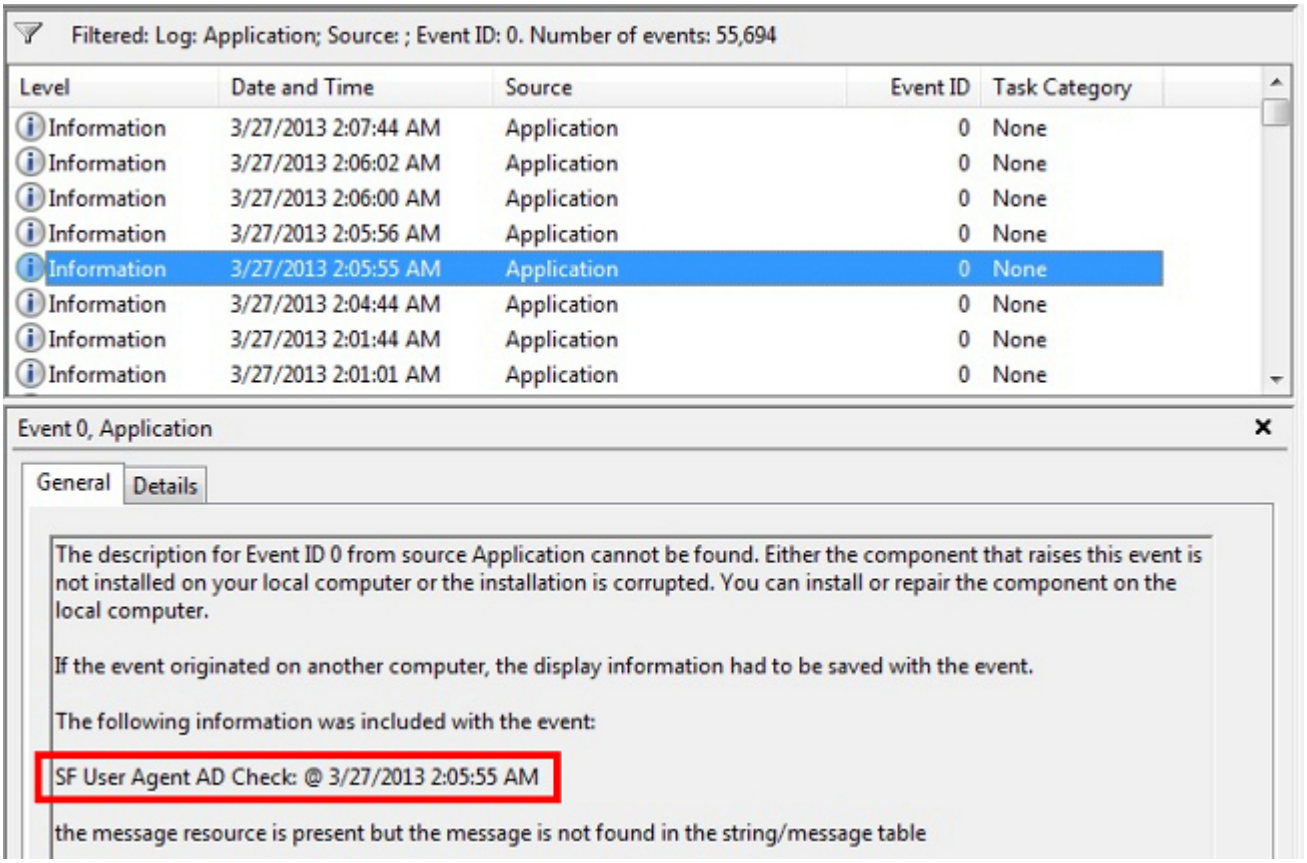
Si l'agent d'utilisateur génère des erreurs en se connectant ou en authentifiant aux serveurs de Répertoire actif il peut y a une question d'autorisation de réseau ou de compte utilisateur. Vérifiez qu'il n'y a aucune question de connexion réseau dans votre environnement et configurez temporairement l'agent d'utilisateur pour utiliser un admin de domaine expliquent l'authentification aux serveurs de Répertoire actif pour tester si possible.

Se connecter diagnostique

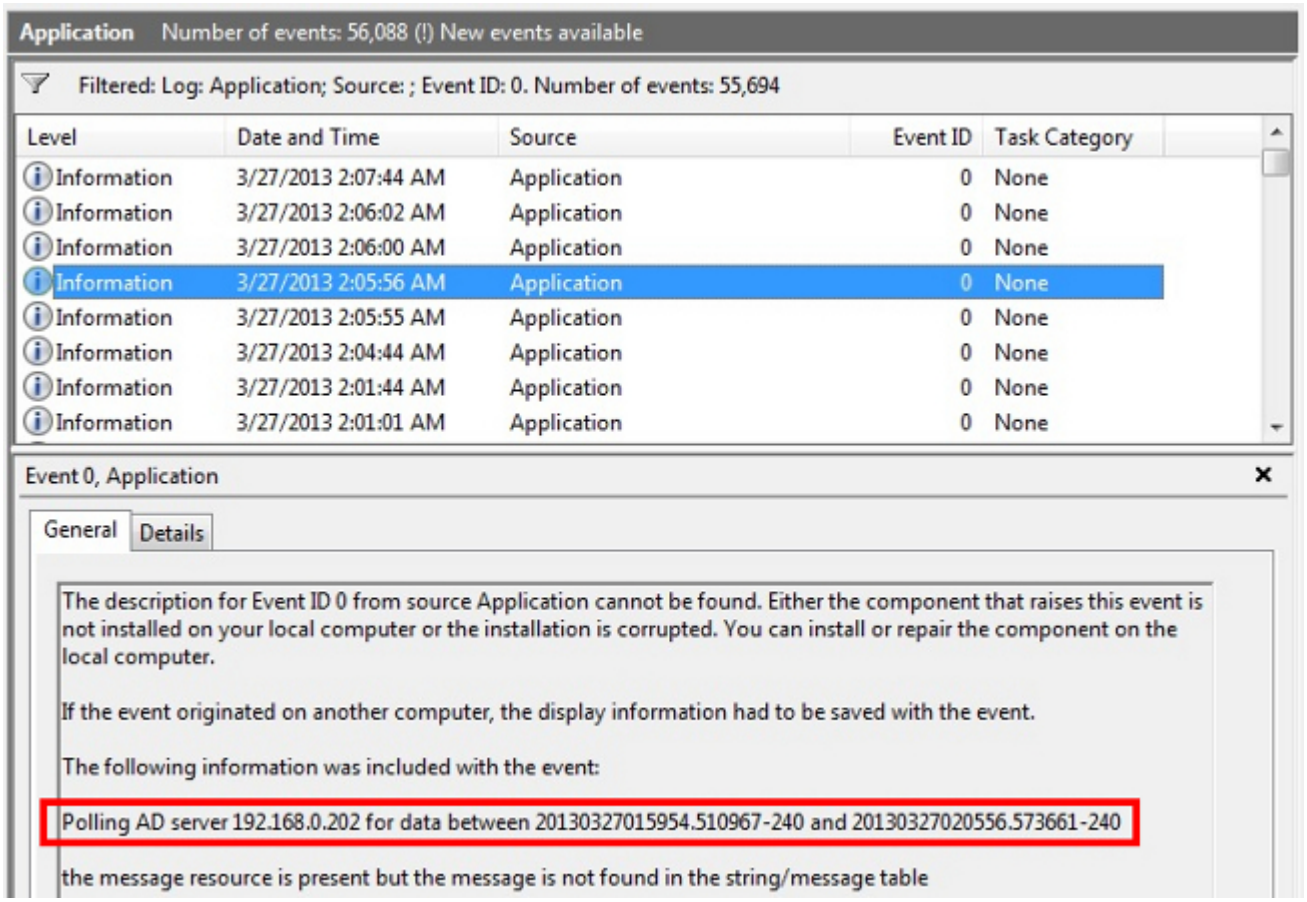
Pour le dépannage général de l'agent d'utilisateur, du **log de** contrôle au **journal d'événements locaux** dans le client GUI d'agent d'utilisateur et la **sauvegarde de** clic. Ceci cause les messages opérationnels utiles d'être entrés dans le journal d'événements d'application hôte d'agent d'utilisateur. Vous pouvez confirmer que l'interrogation d'agent d'utilisateur se termine avec succès en recherchant les événements suivants, dans la commande :

Note: Les captures d'écran ci-dessous sont du Microsoft Event Viewer sur l'hôte qui exécute l'agent d'utilisateur.

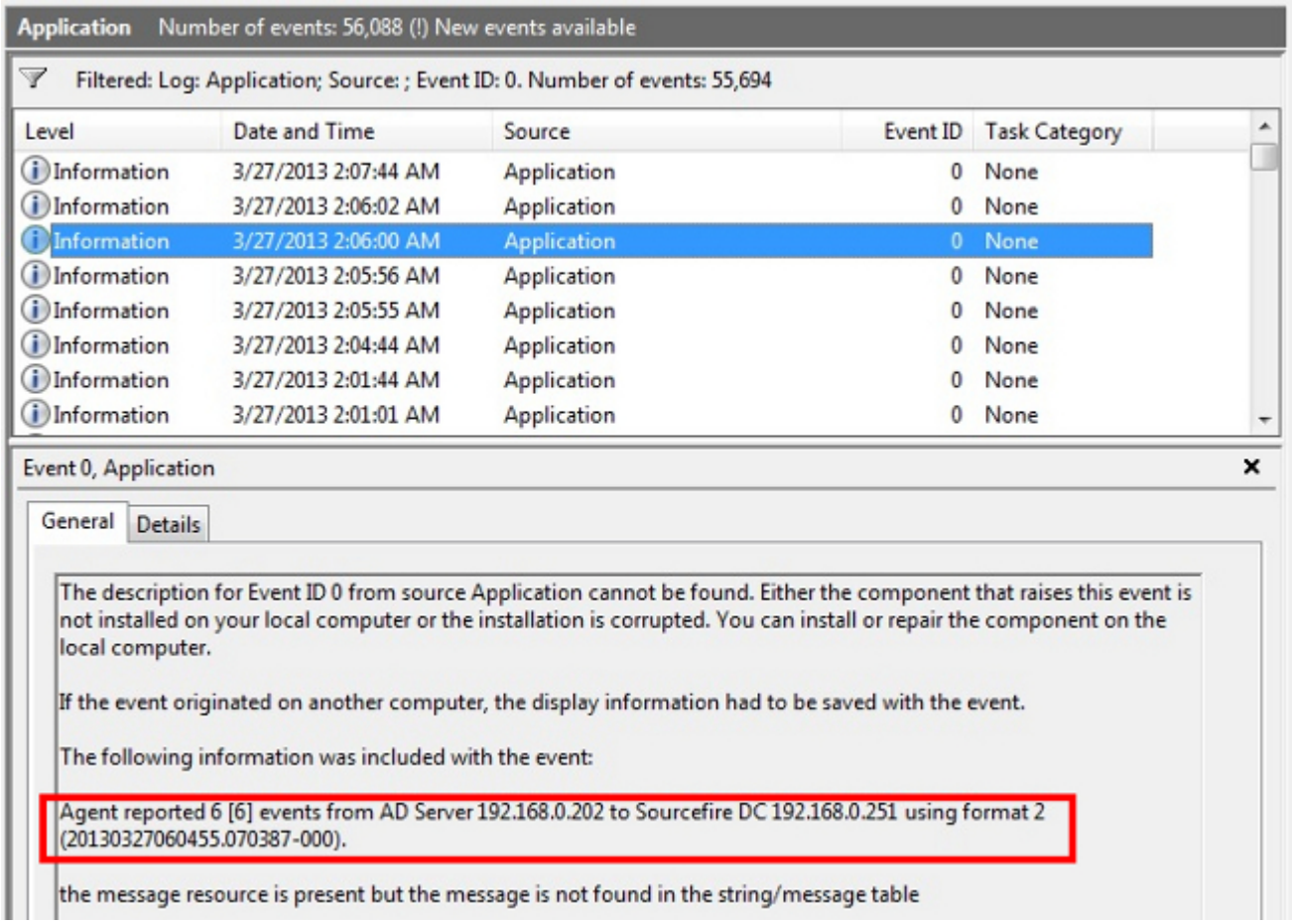
Contrôle de Répertoire actif d'agent d'utilisateur



Serveur de Répertoire actif d'interrogation d'agent d'utilisateur



Événements de nombre signalés par agent (#) au centre de la 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