

Universal Forwarder avec utilisation CPU élevée lorsque Splunk_TA_microsoft-IIS est installé.

Applicabilité

Splunk Enterprise Universal Forwarder

Description

Le problème a été isolé au TA, lorsque la désactivation de Splunk_TA_microsoft-IIS fait passer l'utilisation du CPU de ~10% à ~70%.

Enquête

Comment l'identifier :

a. Le redirecteur universel possède les applications suivantes :

- Nom du système d'exploitation Microsoft Windows Server 2008 R2 Entreprise
- Version 6.1.7601 Service Pack 1 Build 7601
- Splunk Universal Forwarder 7.2.0
- Splunk_TA_windows 5.0.0
- Splunk_TA_microsoft-IIS 1.0.1

b. La configuration de Splunk_TA_microsoft-IIS est la suivante :

```
[monitor://C:\inetpub\logs\LogFiles\...\*.log]
disabled = false
sourcetype = ms:iis:auto
index = iis[monitor://D:\inetpub\logs\LogFiles\...\*.log]
disabled = false
sourcetype = ms:iis:auto
index = iis[monitor://D:\inetpub\logs\logfiles\...\*.log]
disabled = false
sourcetype = ms:iis:auto
index = iis[monitor://D:\IISLogs\...\*.log]
disabled = false
```

```
sourcetype = ms:iis:auto  
index = iis
```

- c. Après avoir activé le module complémentaire Splunk_TA_microsoft-IIS avec la configuration ci-dessus, l'utilisation du processeur passe à 70 %.
- d. Les entrées deux et trois pointent vers le même emplacement, la seule différence étant la sensibilité à la casse pour le chemin ignoré dans Windows.

Résolution

Comment le réparer :

Traverses de dossiers "..." sont bien connus pour voler un tas de ressources CPU.

La documentation officielle du module complémentaire Splunk_TA_microsoft-IIS recommande une entrée à une entrée :

[Configurez les entrées à l'aide des fichiers de configuration](#)

Pour résoudre le problème, remplacez toutes les 4 entrées par une traversée de dossier vers une entrée unique (récursive implicite égale true) :

```
[monitor://C:\inetpub\logs\LogFiles]  
whitelist = \.log$|\.LOG$  
disabled = false  
sourcetype = ms:iis:auto
```

Après la modification de \$HOME_SPLUNK/etc/apps/Splunk_TA_microsoft-IIS/local/inputs.conf et le redémarrage de Splunk, l'utilisation du CPU restera normale (~10%).

Liens connexes

[Configurez les entrées à l'aide des fichiers de configuration](#)

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.