

Consommation CPU élevée sur Universal Forwarder

Applicabilité

Splunk Enterprise

Description

Une activité inattendue d'un processus hôte Windows traitant les opérations d'E/S d'événement Windows a été observée, qui maintient constamment son utilisation du CPU entre 10 % et 30 %. Les utilisateurs se sont plaints de la dégradation de l'expérience utilisateur des terminaux.

Il est à noter que le processus splunk-PowerShell écrit constamment sur le pipeline PowerShell ouvert.

Enquête

La survenue de ces événements :

```
Event 4103CommandInvocation(Out-Null): "Out-Null"CommandInvocation(Out-Null): "Out-Null"
```

```
Event 4103CommandInvocation(Start-Sleep): "Start-Sleep"ParameterBinding(Start-Sleep): na
```

Ces mises en veille constantes de 200 ms et la journalisation des événements entraînent une consommation élevée du processeur par le service EventLog.

Résolution

Modifiez le code PS1 parent Splunk `$SPLUNK_HOME\bin\splunk-powershell.ps1` sur quelques machines en remplaçant le code suivant :

```
if($disposedNow -eq 0){start-sleep -m 200}
```

Avec une valeur plus élevée, dans notre test : 250000 ms (~4 min)

Après cela, le processeur était stable.

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.