

La strophe du moniteur ne fonctionne pas comme prévu.

Applicabilité

Splunk Enterprise

Description

Lorsque vous essayez de surveiller des fichiers dont les noms ne changent pas mais dont le contenu ne change pas, Splunk ne fonctionne pas comme prévu, par exemple :

```
[monitor:///path/reports]
index = splunk_test
initCrcLength = 4096
ignoreOlderThan = 1d
disabled = 0
sourcetype = DiskUsage
```

Enquête

Le Splunk indexe les données en fonction du contexte d'horodatage dans le fichier et non au moment où le fichier est réellement généré, car le fichier capture des informations de date/heure en fonction des détails d'hôte de ce fuseau horaire particulier.

Résolution

Définissez « DATETIME_CONFIG = CURRENT » dans le fichier props.conf, car les nouveaux journaux qui sont indexés auront l'heure actuelle dans l'horodatage, qui est probablement l'heure à laquelle le fichier a été créé, le redirecteur surveillera le fichier et le transmettra presque instantanément.

Exemple :

```
$SPLUNK_HOME/etc/system/local/props.conf
[source:../mylogs/*.log]
```

```
DATETIME_CONFIG = CURRENT
```

Liens connexes

Documentation Splunk

Configuration de l'extraction des horodatages :

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Propsconf?utm_source=answers&utm_medium=question&utm_term=props.conf&utm_campaign=refdoc#Timestamp_extraction_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.