Le splunk n'extrait pas les millisecondes des événements

Applicabilité

Splunk Cloud Splunk Enterprise

Description

Le Splunk extrait jusqu'à secondes et ignore les événements de millisecondes lorsque les événements les contiennent. Cet arrondissement entraîne un tri des journaux dans les recherches Splunk qui ne correspond pas à l'ordre temporel de génération des journaux, ce qui peut être problématique pour les rapports et certaines utilisations d'événements.

Enquête

Les éléments suivants peuvent être reproduits pour aider à diagnostiquer l'erreur dans l'extraction :

1. props.conf a été correctement configuré pour extraire les millisecondes, par exemple :

   ```
   TIME_FORMAT =%Y%m%dT%H:%M:%S.%9N%Z
   ```

2. Les événements sont ingérés à l'aide de HEC (HTTP Event Collector).
3. Le point de terminaison utilisé pour envoyer les événements est /collector/event :

   ```
   https://host_name/services/collector/event
   ```

Résolution

Changez le point de terminaison, de event à raw :

```
https://host_name/services/collector/raw
```

Liens connexes

Réponses du Splunk :

Définition de l'horodatage pour entrée hec

Documentation sur le Splunk :

Analyse des événements bruts
Formater les événements pour le collecteur d'événements HTTP : Analyse des événements bruts

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.