Splunk haalt geen milliseconden uit de gebeurtenissen

toepasbaarheid

Splunk Cloud Splunk Enterprise

Beschrijving

Splunk haalt tot de seconden en negeert de milliseconde gebeurtenissen wanneer de gebeurtenissen ze bevatten. Deze afronding resulteert in een sortering van de logs in de Splunk-zoekopdrachten die niet overeenkomt met de tijdvolgorde van het genereren van de logs, wat problematisch kan zijn voor rapporten en sommige gebeurtenistoepassingen.

onderzoek

Het volgende kan worden gereproduceerd om de fout in de extractie te diagnosticeren:

1. props.conf is goed geconfigureerd om de milliseconden te extraheren, bijvoorbeeld:

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

2. Gebeurtenissen worden ingenomen met HEC (HTTP Event Collector).
3. Het eindpunt dat wordt gebruikt om de gebeurtenissen te verzenden is /verzamelaar/gebeurtenis:

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

resolutie

Wijzig het eindpunt, van gebeurtenis naar onbewerkt:

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

Gerelateerde links

Splunk antwoordt:

Tijdstempel definiëren voor hec-invoer

Splunk-documentatie:

Raw event parsing
Formatteer gebeurtenissen voor HTTP Event Collector: Raw event parsing

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.