O Splunk não está extraindo milissegundos dos eventos

Aplicabilidade

Splunk Cloud Splunk Enterprise

Descrição

O Splunk extrai até os segundos e ignora os eventos de milissegundo quando os eventos os contêm. Esse arredondamento resulta em uma classificação dos logs nas pesquisas de Splunk que não corresponde à ordem de tempo da geração dos logs, o que pode ser problemático para relatórios e alguns usos de eventos.

Investigação

Os seguintes itens podem ser reproduzidos para ajudar a diagnosticar o erro na extração:

1. props.conf foi configurado corretamente para extrair os milissegundos, por exemplo:

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

2. Os eventos são ingeridos usando HEC (HTTP Event Collector).
3. O ponto de extremidade usado para enviar os eventos é /collector/event:

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

Resolução

Altere o endpoint, de event para raw:

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

Links relacionados

Respostas de Splunk:

Definindo carimbo de data/hora para entrada hec

Documentação do Splunk:

Análise de evento bruto
Formatar eventos para o Coletor de Eventos HTTP: Análise de evento bruto

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.