Splunk non estrae millisecondi dagli eventi

Applicabilità

Splunk Cloud Splunk Enterprise

Descrizione

Splunk estrae fino ai secondi e ignora gli eventi dei millisecondi quando questi li contengono. Questo arrotondamento determina un ordinamento dei registri nelle ricerche Splunk che non corrisponde all'ordine temporale di generazione dei registri, che potrebbe essere problematico per i report e alcuni utilizzi di eventi.

Indagine

Per diagnosticare l'errore durante l'estrazione, è possibile riprodurre quanto segue:

1. props.conf è stato configurato correttamente per estrarre i millisecondi, ad esempio:

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

2. Gli eventi vengono acquisiti mediante HEC(HTTP Event Collector).
3. L'endpoint utilizzato per inviare gli eventi è /collector/event:

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

Risoluzione

Modificare l'endpoint, da event a raw:

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

Collegamenti correlati

Risposte Splunk:

[Definizione del timestamp per l'input hec]

Documentazione Splunk:

Analisi evento non elaborato
[Formatta eventi per Raccolta eventi HTTP: Analisi evento non elaborato]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).