Splunkがイベントからミリ秒を抽出しない

適用性

SplunkクラウドSplunk Enterprise

説明

Splunkは、イベントにミリ秒のイベントが含まれている場合、その秒までの時間を抽出して無視します。この丸めは、Splunk検索のログを並べ替える際にログの生成順序に対応しない結果となり、レポートや一部のイベントで問題が発生する可能性があります。

調査

抽出中のエラーの診断に役立つように、次の内容を再現できます。

1. props.confは、次のように、ミリ秒を抽出するように適切に設定されました。

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

2. イベントはHEC(HTTP Event Collector)を使用して取り込まれます。
3. イベントの送信に使用されるエンドポイントは/collector/eventです。

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

解決方法

エンドポイントを eventから rawに変更します。

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

関連リンク

Splunkの回答：

hec入力のタイムスタンプの定義

Splunkのドキュメント：

生のイベント解析
HTTPイベントコレクタのフォーマットイベント：生イベントの解析

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。