

nullqueue正規表現が期待どおりに動作しない

適用性

Splunkエンタープライズ

説明

この「特定のイベントを保持し、残りを破棄する」パターンを実装するユースケースがいくつかあります。

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific_events

インデクサで、次のようにヌルキュー変換が定義されているケースに遭遇しました。この正規表現がすべてのイベントと一致することを確認しました。次に、保持するイベントのサブセットと一致し、<INDEX>インデックスに送信します。

Transforms:

```
[YYY]
REGEX = .*LogName=Security.*
DEST_KEY = queue
FORMAT = nullQueue[XXX]
REGEX=(?msi)^EventCode=(<NUMBERS IN A REGEX>)
DEST_KEY = _MetaData:Index
FORMAT = <INDEX>
```

プロパティ :

```
[WinEventLog:Security]
TRANSFORMS-set=YYY, XXX
```

これは機能しませんでした。<INDEX>には何もなかった。それから、YYY regexを「REGEX=」に変更したら問題なく動作しました。ただし、実際にすべてのイベントと一致する場合は、「」よりも詳細な正規表現を使用して正規表現を使用できます。

調査

ユーザの会議をドキュメントと比較すると、すべての作業ダイアグラムが総合テストから始まっていることがわかりました。キャッチャルから複数の抽出を行うことで、キャッチャルを適切に配置した状態で粒度を調整できます。

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific_events

解決方法

最初にnullqueue変換を行うプロップとトランスフォーメーションを、「。」以外の正規表現で設定します。次に、より具体的な正規表現といくつかのインデックスを持つ別の変換を行い、データがそのインデックスに送られることを期待します。

Transforms:

```
[XXX]
REGEX = .
DEST_KEY = queue
FORMAT = nullQueue[YYY]
REGEX=(?msi)^EventCode=(<NUMBERS IN A REGEX>)
DEST_KEY = _MetaData:Index
FORMAT = <INDEX>[ZZZ]
REGEX= <LOG NAME REGEX>
DEST_KEY = _MetaData:Index
FORMAT = <DIFFERENT INDEX>
```

プロパティ :

```
[WinEventLog:Security]
TRANSFORMS-set=XXX, YYY, ZZZ
```

関連リンク

Splunkドキュメント

特定のイベントを保持し、残りは破棄する :

https://docs.splunk.com/Documentation/SplunkCloud/6.6.3/Forwarding/Routeandfilterdatad#Keep_specific_events

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。