

AWS Kinesis FirehoseからHECを介してSplunk Cloudのイベントを取り込めません。

適用性

SplunkクラウドHEC接続

説明

次のエラーが表示されます。

```
"If you have a proxy (ELB or other) between Kinesis Firehose and the HEC node, you must
```

調査

識別方法：

1) AWSで次のようなエラーが発生する場合があります。

```
{
  "deliveryStreamARN": "arn:aws:firehose:ap-southeast-2:406119630047:deliverystream/wageri",
  "destination": "https://http-inputs-ack-xxxx.splunkcloud.com/services/collector/raw",
  "deliveryStreamVersionId": 1,
  "message": "If you have a proxy (ELB or other) between Kinesis Firehose and the HEC node",
  "expiration to support HEC ACKs.",
  "errorCode": "Splunk.ProxyWithoutStickySessions",
  "processor": "arn:aws:lambda:ap-southeast-2:406119630047:function:paism-log-processor"
}
```

2)次のコマンドを使用してHECトークンにテストイベントを送信しようとすると、エラーが発生します

```
{"text":"Data channel is missing","code":10}
```

```
curl -k "https://http-inputs-<stack-id>.splunkcloud.com/services/collector" -H "Authorization: {"event": "Hello, world!", "sourcetype": "manual"}"
```

解決方法

修正方法：

これを修正するには、Settings » Data Inputs » HTTP Event Collectorにアクセスしてインデクサの確認を無効にしてから、問題のあるトークンの「edit」をクリックし、「Enable indexer acknowledgement」のチェックを外して「Save」をクリックします。

{ "text": "Data channel is missing", "code": 10 } エラーが表示される場合 また、AWS Kinesis Firehoseからイベントを送信するのではなく、curlコマンドを使用して、インデクサの確認応答を有効のままにしておきたい場合は、次のようにコマンドにチャンネルを追加します。

```
curl https://http-inputs-<stack-id>.splunkcloud.com/services/collector?channel=FE0ECFAD-BD274822-96AA-4DA6-90EC-18940FB2414C" -d '{"event": "Hello, world!", "sourcetype": "manual"}'
```

関連リンク

Splunkのドキュメント：

[チャンネルとデータの送信について](#)

[HTTPイベントコレクタインデクサの確認応答について](#)

Splunkの解答：

[Splunk LightのHTTPイベントコレクタを使用すると「Data channel is missing \(データチャンネルが見つかりません \) 」というエラーが表示されるのはなぜですか。](#)

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。