

Não é possível incluir eventos na nuvem Splunk por meio de HEC da AWS Kinesis Firehose.

Aplicabilidade

conexão Splunk Cloud HEC

Descrição

O erro exibido é:

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

Investigação

Como identificá-lo:

1) Você pode obter um erro como o abaixo no AWS:

```
{
  "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) Se tentar enviar um evento de teste para o token HEC usando o comando abaixo, você receberá o erro

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

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

Resolução

Como corrigi-lo:

Para corrigi-lo, desative as confirmações do indexador acessando Configurações "Entradas de dados" Coletor de eventos HTTP, clique em "editar" no token com o problema e desmarque "Habilitar confirmação do indexador" e clique em "Salvar"

Se o erro `{\"text\": \"O canal de dados está ausente\", \"code\": 10}` e não enviando os eventos da AWS Kinesis Firehose, mas usando o comando curl e você deseja manter as confirmações do indexador habilitadas, em seguida, basta adicionar um canal ao comando, por exemplo:

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

Links relacionados

Documentação do Splunk:

[Sobre canais e envio de dados](#)

[Sobre a Confirmação do Indexador do Coletor de Eventos HTTP](#)

Resposta Splunk:

[Por que estou recebendo o erro "Data channel is missing" \(Canal de dados ausente\) usando o coletor de eventos HTTP com luz de tronco?](#)

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.