

A entrada de conexão DB parou de enviar eventos ao indexador, mas outras entradas de conexão DB estão funcionando bem

Aplicabilidade

Splunk Enterprise Splunk DB Connect

Descrição

A entrada de conexão DB parou de enviar eventos ao indexador, mas outras entradas de conexão DB estão funcionando bem

Investigação

Como identificar:

Verifique os logs `db_connect ( index=_internal sourcetype=dbx*)` para mensagens semelhantes ao exemplo abaixo:

```
2018-10-01 12:07:33.885 +0100 INFO c.s.dbx.server.task.listeners.JobMetricsListener - ac
db_read_time=91 hec_record_process_time=826 format_hec_success_count=1000 status=FAILED
is_jmx_monitoring=false start_time=2018-10-01_12:07:27 end_time=2018-10-12_01:07:30 dura
....
2018-10-01 12:07:33.885 +0100 [QuartzScheduler_Worker-27] INFO org.easybatch.core.job.Ba
.....
at com.splunk.dbx.server.dbinput.recordwriter.HecEventWriter.writeRecords(HecEventWriter
at com.splunk.dbx.server.dbinput.recordwriter.HttpEventCollector.uploadEvents(HttpEventC
at com.splunk.dbx.server.dbinput.recordwriter.HttpEventCollector.uploadEventBatch(HttpEv
java.io (https://java.io) .IOException: HTTP Error 400: Bad Request
2018-10-01 12:07:33.885 +0100 [QuartzScheduler_Worker-27] ERROR org.easybatch.core.job.B
```

Resolução

Causado pelo seguinte bug :

DBX-4614 - Entradas DBX 3.1.3 lançando "Erro HTTP 400: Erro "Solicitação Inválida" quando um campo grande é encontrado

Que é uma duplicata de :

SPL-156315 [Regression] Após a atualização para 7.x, os eventos HEC maiores que 512KB são descartados com erros de análise, resultando na redução do throughput da indexação

Se você tentar enviar um evento para HEC que seja > 512KB, o evento será descartado. Se o DBX estiver enviando o evento via HEC e atingir esse limite, ele continuará tentando enviar o evento e falhará, significando que nenhum evento adicional será indexado, a menos que o evento seja ignorado manualmente ou uma substring da coluna seja enviada.

Esse problema é corrigido no Splunk 7.0.5 e acima, 7.1.3 e acima, e 7.2.0 e acima, aumentando o tamanho máximo do evento HEC padrão de 512K para 5MB. Uma nova opção de configuração `maxEventSize` também foi adicionada a `inputs.conf` para permitir o aumento desse valor, se necessário:

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf#http:_28HTTP_Event_Collector.2

```
maxEventSize = <positive integer>[KB|MB|GB]
* The maximum size of a single HEC (HTTP Event Collector) event.
* HEC disregards and triggers a parsing error for events whose size is
greater than 'maxEventSize'.
* Default: 5MB.
```

Links relacionados

Documentação do Splunk

[http: \(Coletor de Eventos HTTP\)](#)

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf#http:_28HTTP_Event_Collector.2

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.