

数据库连接输入停止向索引器发送事件，但其他数据库连接输入运行正常

适用范围

Splunk Enterprise Splunk DB连接

描述

数据库连接输入停止向索引器发送事件，但其他数据库连接输入运行正常

调查

如何识别:

检查db_connect日志(index=_internal sourcetype=dbx*)，用于类似于以下示例的消息：

```
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
```

分辨率

由以下Bug导致：

DBX-4614 - DBX 3.1.3输入引出“HTTP错误400:遇到大字段长度时出现“错误请求”错误

是的副本：

SPL-156315 [Regression]升级到7.x后，会丢弃大于512KB的HEC事件，并出现解析错误，从而导致索引吞吐量下降

如果您尝试向HEC（大于512KB）发送事件，则事件将被丢弃。如果DBX通过HEC发送事件并达到此限制，它将继续尝试发送事件并失败，这意味着除非手动跳过该事件或改为发送该列的子字符串，否则不会再对事件编制索引。

通过将默认最大HEC事件大小从512K增加到5MB，此问题在Splunk 7.0.5及更高版本、7.1.3及更高版本以及7.2.0及更高版本中得到修复。还向inputs.conf中添加了一个新的配置选项maxEventSize，以允许根据需要增加此值：

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf#http:_28HTTP_Event_Collector.28

```
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.
```

相关链接

Splunk文档

http: (HTTP事件收集器)

https://docs.splunk.com/Documentation/Splunk/latest/Admin/Inputsconf#http:_28HTTP_Event_Collector.28

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。