

Invoer voor DB-verbinding is gestopt met het verzenden van gebeurtenissen naar de indexeerder, maar andere ingangen voor DB-verbinding werken prima

toepasbaarheid

Splunk Enterprise Splunk DB Connect

Beschrijving

Invoer voor DB-verbinding is gestopt met het verzenden van gebeurtenissen naar de indexeerder, maar andere ingangen voor DB-verbinding werken prima

onderzoek

Hoe te identificeren:

Controleer de db_connect-logboeken (index=_internal sourceType=DBX*) voor berichten die lijken op het onderstaande voorbeeld:

```
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
```

resolutie

Veroorzaakt door de volgende bug:

DBX-4614 - DBX 3.1.3-ingangen die de fout "HTTP-fout 400: slecht verzoek" weergeven wanneer een grote veldlengte wordt aangetroffen

Dit is een duplicaat van:

SPL-156315 [Regressie] Na de upgrade naar 7.x worden HEC-gebeurtenissen groter dan 512KB verlaagd met parseringsfouten, wat resulteert in een degradatie van de indexeringsdoorvoer

Als u probeert een gebeurtenis naar HEC te sturen die > 512KB is, wordt de gebeurtenis verwijderd. Als DBX de gebeurtenis via HEC verzendt en deze limiet bereikt, blijft het proberen de gebeurtenis te verzenden en mislukt, wat betekent dat er geen verdere gebeurtenissen worden geïndexeerd, tenzij de gebeurtenis handmatig wordt overgeslagen of een subtekenreeks van de kolom wordt verzonden.

Dit probleem is verholpen in Splunk 7.0.5 en hoger, 7.1.3 en hoger en 7.2.0 en hoger door de standaard maximale HEC-gebeurtenisgrootte te verhogen van 512K naar 5MB. Er is ook een nieuwe configuratieoptie `maxEventSize` toegevoegd aan `inputs.conf` om deze indien nodig te verhogen:

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.
```

Gerelateerde links

Splunk-documentatie

[http: \(HTTP \(evenementenverzamelaar\)\)](#)

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.