

L'input DB connect ha interrotto l'invio di eventi all'indicizzatore, ma altri input DB connect funzionano correttamente

Applicabilità

Splunk Enterprise Splunk DB Connect

Descrizione

L'input DB connect ha interrotto l'invio di eventi all'indicizzatore, ma altri input DB connect funzionano correttamente

Indagine

Come identificare :

Controllare i log db_connect (index=_internal sourcetype=dbx*) per messaggi simili a quello riportato di seguito:

```
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
```

Risoluzione

Causata dal seguente bug:

DBX-4614 - Gli input DBX 3.1.3 generano "HTTP Error 400: Errore "Richiesta non valida" quando viene rilevata una lunghezza di campo elevata

Che è un duplicato di:

SPL-156315 [Regressione] Dopo l'aggiornamento a 7.x, gli eventi HEC di dimensioni superiori a 512 KB vengono eliminati con errori di analisi, con conseguente riduzione del throughput di indicizzazione

Se si tenta di inviare un evento a HEC che è > 512KB, l'evento viene eliminato. Se DBX invia l'evento tramite HEC e raggiunge questo limite, continuerà a tentare di inviare l'evento e non riuscirà a indicare che non verranno indicizzati ulteriori eventi a meno che l'evento non venga ignorato manualmente o non venga invece inviata una sottostringa della colonna.

Questo problema viene risolto in Splunk 7.0.5 e versioni successive, 7.1.3 e versioni successive e 7.2.0 e versioni successive, aumentando le dimensioni predefinite degli eventi HEC da 512K a 5 MB. È stata inoltre aggiunta una nuova opzione di configurazione `maxEventSize` a `inputs.conf` per consentire un aumento di questo valore se necessario:

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.
```

Collegamenti correlati

Documentazione relativa a Splunk

`http:` (Raccolta eventi HTTP)

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).