

L'entrée de connexion DB a arrêté d'envoyer des événements à l'indexeur mais les autres entrées de connexion DB fonctionnent correctement

Applicabilité

Splunk Enterprise Splunk DB Connect

Description

L'entrée de connexion DB a arrêté d'envoyer des événements à l'indexeur mais les autres entrées de connexion DB fonctionnent correctement

Enquête

Comment identifier :

Vérifiez les journaux db_connect (index=_internal sourcetype=dbx*) pour les messages similaires à l'exemple ci-dessous :

```
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
```

Résolution

Causé par le bogue suivant :

DBX-4614 - Entrées DBX 3.1.3 lançant "Erreur HTTP 400 : Erreur « Requête incorrecte » lorsque la longueur du champ est importante

Lequel est un doublon de :

SPL-156315 [Régression] Après la mise à niveau vers 7.x, les événements HEC supérieurs à 512 Ko sont abandonnés avec des erreurs d'analyse, ce qui entraîne une dégradation du débit d'indexation

Si vous essayez d'envoyer un événement à HEC qui est > 512KB alors l'événement est abandonné. Si DBX envoie l'événement via HEC et atteint cette limite, il continuera à essayer d'envoyer l'événement et échouera, ce qui signifie qu'aucun autre événement ne sera indexé, à moins que l'événement ne soit manuellement ignoré ou qu'une sous-chaîne de la colonne ne soit envoyée à la place.

Ce problème est corrigé dans Splunk 7.0.5 et versions ultérieures, 7.1.3 et versions ultérieures, et 7.2.0 et versions ultérieures en augmentant la taille maximale par défaut des événements HEC de 512K à 5MB. Une nouvelle option de configuration maxEventSize a également été ajoutée à input.conf pour permettre d'augmenter cette valeur si nécessaire :

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.
```

Liens connexes

Documentation Splunk

http : (Collecteur d'événements HTTP)

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

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.