

Doppelte Protokollierung von Kubernetes über HEC-Aufnahme in Splunk beobachtet

Geltungsbereich

Splunk Enterprise Kubernetes

Beschreibung

HEC-Daten werden nicht wie erwartet indexiert, und es werden Duplikate auf mehreren Servern für einen bestimmten Index erstellt, der eine bestimmte Quelle von Kubernetes hat.

Untersuchung

1. Überprüfen Sie zuerst den HEC-Tokenstatus mit dem folgenden Befehl in der Splunk SH-GUI.

```
|rest /services/data/inputs/http/http  
| table name, token , disabled
```

2. Duplikate können entstehen, wenn die Quelle mehrere Quelltypen falsch markiert. Überprüfen Sie also, ob die Quelltexte falsch konfiguriert sind.

```
index=<index_name> | stats count by source ,sourcetype
```

3. Bestätigen Sie, ob doppelte Ereignisse mehr als einmal eintreffen.

```
index=<index_name> | stats count by _time, source, host | where count > 1
```

4. Überprüfen Sie die HEC-Eingabeeinstellungen in Splunk, indem Sie in der Splunk-GUI zu Settings > Data Inputs > HTTP Event Collector navigieren. Stellen Sie sicher, dass keine HEC-Eingabe zweimal für dieselbe Quelle oder Anwendung definiert ist.

5. Überprüfen Sie die internen Splunk-Protokolle auf Fehler oder Warnungen im Zusammenhang mit der HEC-Aufnahme, die auf Fehlkonfigurationen oder Probleme hinweisen können.

```
index=_internal spource*splunkd.log* component-HttpEventCollector*
```

Auflösung

- Für die Kubernetes-Quelle wird der Befehl "stats count by _raw ...field N where count > 1" Methode zur Erkennung von Duplikaten ist unzuverlässig, da dies auf Ereignisse zurückzuführen ist, die keine eindeutigen Felder wie Event ID usw. aufweisen. Es scheint also, dass alle Ereignisse Duplikate sind, wenn sie in der Splunk-GUI überprüft werden. Es sei denn, ein relativ eindeutiges Feld wie kubernetes.docker_id oder kubernetes.pod_id ist in den Rohdaten enthalten und überprüft die Duplikate vom Quellende aus.
- Die Duplikate wurden erstellt, da mehrere Load Balancer vorhanden waren. Stellen Sie sicher, dass der Lastenausgleich ordnungsgemäß konfiguriert ist, um die Daten an die richtigen Indexer weiterzuleiten, da falsche Einstellungen dazu führen können, dass dieselben Daten auf mehrere Indexer festgelegt werden, und dass dies zu Duplikaten führt.

Verwandte Links

[Wie finde ich doppelte Ereignisse?](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.