

在Splunk中觀察到來自Kubernetes的通過HEC攝取的重複日誌記錄

適用性

Splunk企業版Kubernetes

說明

HEC資料沒有按預期進行索引，它跨多台伺服器為特定索引建立重複項，該索引具有來自Kubernetes的特定源

調查

1. 首先在Splunk SH GUI中使用下面的命令檢查HEC令牌狀態。

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

2. 如果源錯誤地標籤了多個源型別，則可能會出現重複項。請檢查源或源型別是否配置錯誤。

```
index=  
  
| stats count by source ,sourcetype
```

3. 確認重複事件是否多次出現。

```
index=
```

```
| stats count by _time, source, host | where count > 1
```

4. 在 Splunk GUI 中導航到設定>資料輸入> HTTP事件收集器，檢查Splunk中的HEC輸入設定。 確保沒有為同一源或應用程式定義兩次HEC輸入。

5. 檢查Splunk內部日誌，查詢與HEC攝入相關的可能表明配置錯誤或問題的任何錯誤或警告。

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

解析

- 對於Kubernetes源，命令「stats count by _raw ...欄位N，其中計數> 1"的重複檢測方法不可靠，因為這是由於沒有任何唯一欄位（如事件ID等）的事件。因此，在Splunk GUI中選中時，所有事件似乎都是重複的。除非原始資料中包含相對唯一的欄位，如kubernetes.docker_id或kubernetes.pod_id，並且從源端檢查重複項。

- 由於存在多個負載均衡器，因此發生了重複操作。確保正確配置了負載平衡，以將資料定向到正確的索引器，因為不正確的設定可能會導致同一資料被設定為多個索引器，並且會導致重複。

相關連結

[如何查詢重複事件](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。