

攝入的事件丟失 — 解決Splunk中的時間戳分析問題：WinHostMon的案例研究

適用性

Splunk企業版

說明

從WinHostMon監視磁碟資料時，發現事件時間戳(_time)和接入時間戳(_indextime)有顯著差異。某些事件的_time設定為過去很久的日期，從而導致索引延遲和誤導搜尋結果。

之所以會出現此問題，是因為'FreeSpaceKB'欄位中的數值被誤解為紀元時間，因為props.conf中的預設'DATETIME_CONFIG=\etc\datetime.xml'設定。

調查

症狀：

- 「index=windows sourcetype=WinHostMon」的搜尋結果完全未返回結果。
- 搜尋同一SPL的所有時間都顯示「_time」和「_indextime」之間存在較大的延遲。
- 儘管攝取或索引過程沒有任何問題，但過去曾出現「_time」事件。
- 即使在同一台伺服器上發生了接收和索引，該問題仍然存在。

主要發現：

- 拆分內部日誌發現事件接收正常：

```
INFO ExecProcessor [4664 ExecProcessorSchedulerThread] - message from ""C:\Program Files\Splunk\
```

- 此日誌確認了事件的正確接收，但搜尋顯示的「_time」值不正確。
- 對原始事件日誌的檢查顯示欄位'FreeSpaceKB=1607839214'，與2020年12月13日的紀元時間相對應。
- 對props.conf檔案的分析顯示DATETIME_CONFIG指向「\etc\datetime.xml」，從而使Splunk錯誤地將「FreeSpaceKB」解釋為時間戳。

解析

1.更新的配置：

- 已修改WinHostMon源型別的props.conf:

```
[WinHostMon]
DATETIME_CONFIG = CURRENT
```

該更改指示Splunk使用接收時間(_indextime)作為事件的時間戳，而不是解析原始資料中的時間戳。

2.驗證步驟：

- 重新啟動Splunk以應用更新的配置。
- 重新索引測試資料以驗證修復。
- 觀察到事件現在有與_indextime對齊的精確_time值。

要點

- 始終驗證Splunk遇到索引延遲或時間戳異常時如何解析時間戳。
- 當事件缺少有效的時間戳欄位或數字欄位可能被錯誤解釋時，使用「DATETIME_CONFIG = CURRENT」。

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）。