在Winevent log事件時間和Splunk索引時間之間報告的索引延遲

適用性

Splunk企業版

說明

如何識別

首先確認事件時間(_time)和Splunk indextime(_indextime)之間的增量，然後根據受影響的索引和源型別修改以下內容。以下示例是查詢Security channel事件記錄：

```
index=<splunk_index> sourcetype="WinEventLog:Security" host=<splunk_forwarder>
| fields _time, _indextime, host
| eval delay=(_indextime - _time)/60
| timechart avg(delay) by host
```

調查

要驗證的重要事項：

- 索引延遲最初出現於什麼時候？
- 在第一次出現延遲時，部署的位置發生了哪些變化（如果有）？
- 延遲是否隨時間增加（線性）或波動？

確認每秒最大事件數和平均事件數(eps):

```
index=_internal source=*metrics.log* security per_source_thruput host=<splunk_forwarder>
```

```
| timechart max(eps) max(max_age)
```

如果延遲隨時間變化，則高EPS值可能表示資料吞吐量存在瓶頸。

解析

快速修復

此選項僅在希望獲取當前事件而不關心缺少的歷史資料時才適用。對於每個問題轉發器，必須一次執行以下操作：

1. Set `current_only = 1` in `$SPLUNK_HOME\etc\system\local\inputs.conf`:

   ```
   [WinEventLog://Security]
   current_only = 1
   ```

2. 阻止轉發器
3. 重新命名過時的檢查點檔案：

   ```
   ren "C:\Program Files\SplunkUniversalForwarder\var\lib\splunk\modinput\WinEventLog\Securit
   ```

4. 啟動轉發器
5. 確保生成新的安全檢查點檔案
6. 確認檢查點和安全日誌彼此有數百個事件
7. 重新命名`$SPLUNK_HOME\etc\system\local\inputs.conf`檔案，將`current_only=1`設定恢復為預設設定。
8. 重新啟動Splunk
9. 搜尋以確認資料正在接收

為什麼執行常規UF重新引導可能無濟於事

重新啟動UF會強制它重新讀取檢查點並短暫地清空記憶體緩衝區。由於事件生成速率超過了處理/吞吐量限制，轉發器將在重新啟動後的幾分鐘內立即重新開始累積延遲。

長期解決方案

快速修複方案要求對每個受影響的UF進行手動干預，這在大型部署中通常是不可行的（並且一些管理員沒有命令列訪問UF）。除此之外，超額準備金很有可能再次落後。您的最佳選擇可能是提供長期解決方案。由於每個環境都不同，因此不能將任何簡單設定應用於每個場景。但是，此知識庫中的建議應適用於許多使用案例。本文中的所有配置建議都要求在UF上重新啟動Splunk才能生效，從而確保部署伺服器上的自定義應用已選中「重新啟動Splunkd」。

先嘗試此操作(limits.conf)

開啟maxKBps

在調整以下選項之前，請檢視`limits.conf/[thruput]maxKBps`。UF的預設設定為256KB/s，這限制轉發器每天的網路傳輸總量為~22 GB。繁忙的生成安全日誌的伺服器很容易產生超過256 KB/s的流量，因此轉發器實際上無法跟上。

所以，首先：在`limits.conf`中將此值設定為0（無限制）以取消網路頻寬限制：

```
[thruput]
maxKBps = 0
```

由於大多數通用轉發器正在給部署伺服器回呼電話，最佳實踐是通過部署應用設定此配置，以便所有轉發器一次接收此配置（如果可能，首先在測試環境中，然後進入生產環境）。 如果測試環境不可用，則另一個選擇是部署到包含小組UF和監控器的「測試」伺服器類中，然後再將其應用到所有位置。這同樣適用於此知識庫文章中提供的所有建議。

其他選項

如果開啟轉發器的推力不能完全解決問題，請考慮以下事項：

特定於`inputs.conf/[WinEventLog://Security]`

選項#1 — 更改批大小

預設情況下，Splunk以小批捕獲事件（10個事件），並頻繁更新磁碟上的檢查點檔案。在繁忙的主機上，檢查點檔案上的磁碟I/O會成為主要的阻塞點。設定batch_size = 500、將磁碟同步延遲到600秒(checkpointInterval = 600)，以及設定suppress_checkpoint = true會顯著增加splunk-winevtlog.exe的EPS（每秒事件數）吞吐量。

```
batch_size = 500
suppress_checkpoint = true
checkpointInterval = 600
```

選項#2 — 使用renderXML減少API呼叫數

預設情況下，Splunk為事件中的每個欄位發出API呼叫。相反，啟用renderXml將針對每個事件發出API呼叫，從而可能提高效能：以XML顯示Windows事件日誌事件

```
renderXml = true
```

選項#3 — 篩選抑制哪些欄位以減少資料負載

此選項對原始速度有效，但請確保它滿足稽核要求（如果適用）。

這些設定會在傳送前從原始事件中去除報頭欄位，以減少位元組大小和API呈現呼叫。如果其SIEM、CIM模型或合規性儀表板依賴Keywords（例如，稽核成功/失敗）、TaskCategory或Opcode，則刪除這些欄位將中斷這些檢測。

```
suppress_sourcename = true
suppress_keywords = true
suppress_type = true
suppress_task = true
suppress_opcode = true
```

選項#4 — 在輸入模式中啟用FormatMessage()API

evtFormatMessage()是大多數Windows部署中的預設API，與以前的FormatMessage()API相比，該部署具有更高的處理開銷。還原到舊的API可能會緩解索引延遲。

如果**renderXml = true**，則不要設定此項。傳統FormatMessage() API在解析經典純文字檔案多行日誌(renderXml = false)時只更快，因為它繞過了繁重的evtFormatMessage() DLL字串查詢。使用renderXml = true時，Splunk已經以結構化格式直接從現代EVTX API(EvtRender)讀取，而不呼叫消息格式化DLL。

```
use_old_eventlog_api = true
```

增加UF接收管道(server.conf)

預設情況下，轉發器運行單個解析和接收管道。對於攝入大量事件卷的多核機器，可以增加流水線集以允許並行處理。控制轉發器從本地Windows API讀取資料、打包資料並將其推入網路所使用的內部執行緒數。

在UF上，與索引器或重轉發器相比，將攝入管道1增加到2的資源佔用空間非常輕便，因為UF僅執行輕量讀取、批處理和網路輸出（沒有正規表示式轉換、欄位提取或到磁碟的索引）。

如果Windows伺服器至少具有4個CPU核心和8 GB RAM，則設定parallelIngestionPipelines = 2通常是安全的，這將大大有助於清除大量事件積壓並防止未來延遲。當UF被捕獲時，CPU使用率可能會增加，但是一旦攝入恢復正常水準，CPU使用率將再次下降。

```
[general]
parallelIngestionPipelines = 2
```

Outputs.conf隊列大小

如果將輸入批處理調整為500，請考慮確保TCP輸出隊列具有足夠的記憶體緩衝區，以便網路層不會阻止輸入工作進程：

```
[tcpout:myindexers]
maxQueueSize = 50MB
```

檢查Windows Defender/防病毒排除

安全終結點代理（例如Defender、CrowdStrike、Carbon Black）可以主動檢查`splunk-winevtlog.exe`，並鎖定`$SPLUNK_HOME\var\lib\splunk\modinput\WinEventLog\`目錄。請確保在即時檔案系統檢查中排除整個$SPLUNK_HOME目錄和`splunk-winevtlog.exe`。

域控制器相關性/網路路由：

如果問題UF在域控制器上運行或處理高Active Directory流量，請確保沒有本地防火牆或網路速率限制將Splunk TCP埠(預設`9997`)限制在接收層（HF或索引器）。

相關連結

- Splunk文檔：
  - 使用Splunk Enterprise監視Windows事件日誌資料
  - 通用轉發器的高級配置
  - 規範檔案：server.conf、inputs.conf、outputs.conf
- Splunk知識庫文章
  - 排除來自UF或HF的延遲日誌故障
  - UF未將安全日誌傳送到Splunk
- Splunk Lantern文章：效能調整轉發層

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）。