思科安全終端 — 軌道日誌滿含錯誤 — CSCwh73163

目錄

問題

端點上的軌道日誌可能包含許多錯誤條目，例如：

- 無法從後設資料服務獲取例項後設資料
- 檢索IMDSv2令牌的3次嘗試失敗

這些錯誤日誌經過較長的時間可能會雜亂和填充受影響終端上的軌道日誌。

範例

```
Error 1: {"level":"error","component":"osqueryd","time":"2023-09-10T15:05:50Z","message":"Failed to get
Error 2: {"level":"error","component":"osqueryd","time":"2023-09-10T15:07:29Z","message":"Failed 3 atte
```

CSCwh73163上當前正在跟蹤此問題

根本原因

在2023-08-21年，軌道公司將軌道從5.5.1升級為5.8.2，以便發行版本1.31。

Osquery 5.6.0新增了2個新表，以提供有關AWS EC2例項的資訊：ec2_instance_metadata和ec2_instance_tags。當嘗試對這些表進行查詢以查詢不在AWS EC2例項上的端點時，將顯示類似於上面列出的錯誤。(有關詳細資訊，請參閱osquery project bug)。嘗試在非AWS EC2例項上查詢這些表也會導致查詢暫停並最終超時。此超時可能需要5分鐘或更長時間。

Device Insights與Orbital整合以提供關於終端的更佳資訊，可為每個包含這些新表的終端提供按需查詢，無論該終端是否位於AWS EC2例項上。這會導致上面列出的錯誤及其查詢需要較長的時間才能完成。

此外，如果客戶在非AWS例項上使用涉及新EC2表的自定義查詢，他們將遇到類似的錯誤和超時。

因應措施/解決方案

Device Insights團隊將於2023年11月22日刪除針對AWS EC2表的查詢。

使用ec2_instance_metadata和ec2_instance_tags表的任何自定義查詢應僅針對AWS EC2例項執行。

請勿在非AWS EC2終端上查詢這些表。

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）。