

Fehlerbehebung bei sicheren Endgeräten - Orbitale Protokolle füllen sich mit Fehlern - CSCwh73163

Inhalt

[Einleitung](#)

[Beispiel](#)

[Ursache](#)

[Lösung/Lösungen](#)

Einleitung

Orbitale Protokolle auf Endpunkten können viele Fehlereinträge enthalten, z. B.:

- Fehler beim Abrufen der Instanzmetadaten vom Metadatendienst.
- Fehler bei 3 Versuchen zum Abrufen eines IMDSv2-Tokens

Diese Fehlerprotokolle können über einen längeren Zeitraum die Orbitalprotokolle der betroffenen Endpunkte überladen und füllen.

Beispiel

```
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
```

Dieses Problem wird derzeit unter [CSCwh73163](#) verfolgt.

Ursache

Am 21.08.2023 aktualisierte Orbital osquery für Version 1.31 von 5.5.1 auf 5.8.2.

Osquery 5.6.0 hat 2 neue Tabellen hinzugefügt, um Informationen über [AWS EC2-Instanzen](#) bereitzustellen: `ec2_instance_metadaten` und `ec2_instance_tags`. Bei Abfragen dieser Tabellen für Endpunkte, die sich nicht auf AWS EC2-Instanzen befinden, werden ähnliche Fehler wie die aufgeführten angezeigt. (Weitere Informationen finden Sie im [osquery-Projektfehler](#)). Wenn Sie versuchen, diese Tabellen für Nicht-AWS EC2-Instanzen abzufragen, wird die Abfrage ebenfalls angehalten und schließlich beendet. Diese Zeitüberschreitung kann 5 Minuten oder länger dauern.

Device Insights, das mit Orbital integriert werden kann, um bessere Informationen über Endpunkte bereitzustellen, stellt eine On-Demand-Abfrage für jeden Endpunkt bereit, die diese neuen Tabellen enthält, unabhängig davon, ob sich der Endpunkt in einer AWS EC2-Instanz befindet oder nicht. Dies führt dazu, dass die aufgeführten Fehler und deren Abfragen einen längeren Zeitraum in Anspruch nehmen.

Wenn ein Kunde benutzerdefinierte Abfragen verwendet, die die neuen EC2-Tabellen in einer Nicht-AWS-Instanz betreffen, treten ähnliche Fehler und Zeitüberschreitungen auf.

Lösung/Lösungen

Das Device Insights-Team entfernt die Abfragen, die auf die AWS EC2-Tabellen am 22. November 2023 abzielen.

Alle benutzerdefinierten Abfragen, die die Tabellen `ec2_instance_metadata` und `ec2_instance_tags` verwenden, dürfen nur für AWS EC2-Instanzen ausgeführt werden.

Abfragen dieser Tabellen nicht auf EC2-Endpunkten ohne AWS.

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.