安全なエンドポイントのトラブルシューティング：オービタルのログがエラーでいっぱいになる – CSCwh73163

内容

はじめに

エンドポイントのオービタルログには、次のような多くのエラーエントリが含まれる場合があります。

- メタデータサービスからインスタンスメタデータを取得できませんでした
- IMDSv2トークンの取得に3回失敗しました

これらのエラーログは、長時間にわたって、影響を受けるエンドポイント上のOrbital口グを散らかし、いっぱいにする可能性があります。

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
```

この問題は、現在CSCwh73163で追跡中です。

根本原因

2023-08-21で、Orbitalはosqueryをリリース1.31用に5.5.1から5.8.2にアップグレードしました。

Osquery 5.6.0では、AWS EC2インスタンスに関する情報を提供するために、ec2_instance_metadataとec2_instance_tagsの2つの新しいテーブルが追加されました。AWS EC2インスタンス以外のエンドポイントに対して、これらのテーブルでクエリを実行しようとすると、リストされているエラーと同様のエラーが表示されます。(詳細は、osqueryプロジェクトのバグを参照してください)。 AWS EC2以外のインスタンスでこれらのテーブルをクエリしようとすると、クエリが一時停止し、最終的にタイムアウトします。このタイムアウトには5分以上か

かる場合があります。

Device InsightsはOrbitalと統合してエンドポイントに関するより詳細な情報を提供し、エンドポイントがAWS EC2インスタンスにあるかどうかにかかわらず、エンドポイントごとにオンデマンドのクエリを提供して、これらの新しいテーブルを含めます。この結果、エラーが表示され、そのクエリの完了に長時間かかります。

さらに、AWS以外のインスタンスで新しいEC2テーブルに関するカスタムクエリを使用すると、同様のエラーとタイムアウトが発生します。

回避策とソリューション

Device Insightsチームは、2023年11月22日にAWS EC2テーブルを対象とするクエリを削除します。

ec2_instance_metadataテーブルとec2_instance_tagsテーブルを使用するカスタムクエリは、AWS EC2インスタンスに対してのみ実行する必要があります。

AWS EC2以外のエンドポイントでは、これらのテーブルをクエリしないでください。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。