Dépannage du point d'extrémité sécurisé - Journaux orbitaux remplis d'erreurs - CSCwh73163

Table des matières

Introduction

- Exemple

Cause première

Solution de contournement/solutions

Introduction

Les journaux orbitaux sur les terminaux peuvent contenir de nombreuses entrées d'erreur, telles que :

- Impossible d'obtenir les métadonnées d'instance du service de métadonnées
- Échec de 3 tentatives de récupération d'un jeton IMDSv2

Ces journaux d'erreurs, sur une longue période, peuvent encombrer et remplir les journaux orbitaux sur les terminaux affectés.

Exemple

```
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
```

Ce problème est actuellement suivi sur CSCwh73163

Cause première

Le 21 décembre 2023, Orbital a mis à niveau osquery de 5.5.1 à 5.8.2 pour la version 1.31.

Osquery 5.6.0 a ajouté 2 nouveaux tableaux pour fournir des informations sur les instances AWS EC2 : ec2_instance_metadata et ec2_instance_tags. Lorsque des requêtes sont tentées sur ces tables pour des points de terminaison qui ne se trouvent pas sur des instances AWS EC2, des erreurs similaires à celles répertoriées s'affichent. (Référez-vous au bogue du projet osquery pour plus de détails). La tentative d'interrogation de ces tables sur des instances EC2 non-AWS entraîne également la suspension de l'interrogation et éventuellement le dépassement du délai

d'attente. Ce délai d'attente peut durer 5 minutes ou plus.

Device Insights, qui s'intègre à Orbital pour fournir de meilleures informations sur les terminaux, fournit une requête à la demande par terminal qui inclut ces nouvelles tables, que le terminal soit situé sur une instance AWS EC2 ou non. Il en résulte que les erreurs répertoriées et leurs requêtes prennent un temps considérable à se terminer.

En outre, si un client utilise des requêtes personnalisées impliquant les nouvelles tables EC2 sur une instance non-AWS, il rencontre des erreurs et des délais d'attente similaires.

Solution de contournement/solutions

L'équipe Device Insights supprime les requêtes qui ciblent les tables AWS EC2 le 22 novembre 2023.

Toutes les requêtes personnalisées utilisant les tables ec2_instance_metadata et ec2_instance_tags doivent être exécutées uniquement sur les instances AWS EC2.

N'interrogez pas ces tables sur des points de terminaison EC2 non-AWS.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.