

Solucionar problemas de terminal seguro - Los registros orbitales se llenan de errores - CSCwh73163

Contenido

[Introducción](#)

[Ejemplo:](#)

[Causa raíz](#)

[Solución/soluciones](#)

Introducción

Los registros orbitales en los terminales pueden contener muchas entradas de error, tales como:

- Error al obtener metadatos de instancia del servicio de metadatos
- Fallo 3 intentos de recuperación de un token IMDSv2

Estos registros de errores, a lo largo del tiempo, pueden desordenar y llenar los registros orbitales en los terminales que se ven afectados.

Ejemplo:

```
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 atten...
```

Este problema se está rastreando actualmente en [CSCwh73163](#)

Causa raíz

En 2023-08-21, Orbital actualizó osquery de 5.5.1 a 5.8.2 para la versión 1.31.

Osquery 5.6.0 agregó 2 tablas nuevas para proporcionar información sobre las [instancias de AWS EC2](#): ec2_instance_metadata y ec2_instance_tags. Cuando se intentan realizar consultas en estas tablas para extremos que no están en instancias AWS EC2, se muestran errores similares a los enumerados. (Refiérase al [bug del proyecto osquery](#) para obtener más detalles). Si se intenta consultar estas tablas en instancias EC2 que no son de AWS, también se hace que la consulta se detenga y, finalmente, se agote el tiempo de espera. Este tiempo de espera puede tardar 5 minutos o más.

Device Insights, que se integra con Orbital para proporcionar mejor información sobre los terminales, proporciona una consulta a demanda por terminal que incluye estas nuevas tablas, independientemente de si el terminal se encuentra en una instancia AWS EC2 o no. Esto hace que los errores enumerados y sus consultas tarden mucho tiempo en completarse.

Además, si un cliente utiliza consultas personalizadas que involucran las nuevas tablas EC2 en una instancia que no es de AWS, encuentra errores y tiempos de espera similares.

Solución/soluciones

El equipo de Device Insights eliminará las consultas dirigidas a las tablas AWS EC2 el 22 de noviembre de 2023.

Cualquier consulta personalizada que utilice las tablas `ec2_instance_metadata` y `ec2_instance_tags` sólo se debe ejecutar contra instancias AWS EC2.

No consulte estas tablas en terminales EC2 que no sean AWS.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).