安全终端故障排除 — 轨道日志错误满载 — CSCwh73163

目录

简介

终端上的轨道日志可能包含许多错误条目，例如：

- 无法从元数据服务获取实例元数据
- 检索IMDSv2令牌的3次尝试失败

这些错误日志经过较长时间可能会杂乱无章并填充受影响终端上的轨道日志。

示例

```
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上当前正在跟踪此问题

根本原因

在2023-08-21上，Orbital将osquery从5.5.1升级到5.8.2，版本1.31。

Osquery 5.6.0添加了2个新表，以提供有关AWS EC2实例的信息:ec2_instance_metadata和ec2_instance_tags。当对这些表中未在AWS EC2实例上的终端尝试查询时，会显示与所列错误类似的错误。(有关详细信息，请参阅osquery project bug)。 尝试在非AWS EC2实例上查询这些表也会导致查询暂停并最终超时。此超时可能需要5分钟或更长时间。

Device Insights与Orbital集成以提供关于终端的更佳信息，可为每个包含这些新表的终端提供按需查询，无论终端是否位于AWS EC2实例上。这会导致所列的错误及其查询需要较长时间才能完成。

此外，如果客户在非AWS实例上使用涉及新EC2表的自定义查询，则会遇到类似的错误和超时。

解决方法/解决方案

Device Insights团队正在删除以2023年11月22日AWS EC2表为目标的查询。

任何使用ec2_instance_metadata和ec2_instance_tags表的自定义查询都必须仅针对AWS EC2实例执行。

请勿在非AWS EC2终端上查询这些表。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。