Solução de problemas de endpoint seguro - registros orbitais preenchendo com erros - CSCwh73163

Contents

Introdução

Logs orbitais em endpoints podem conter muitas entradas de erro, como:

- Falha ao obter metadados de instância do serviço de metadados
- Falha em 3 tentativas de recuperar um token IMDSv2

Esses registros de erros, durante um longo período de tempo, podem sobrecarregar e preencher os registros orbitais nos endpoints afetados.

Exemplo

```
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
```

Este problema está sendo rastreado no CSCwh73163

Causa raiz

Em 21 de agosto de 2023, a Orbital atualizou o osquery de 5.5.1 para 5.8.2 para a versão 1.31.

O Osquery 5.6.0 adicionou 2 novas tabelas para fornecer informações sobre instâncias AWS EC2: ec2_instance_metadata e ec2_instance_tags. Quando há tentativas de consultas nessas tabelas para pontos de extremidade que não estejam em instâncias AWS EC2, erros semelhantes aos listados são exibidos. (Consulte o bug do projeto osquery para obter mais detalhes). A tentativa de consultar essas tabelas em instâncias EC2 não-AWS também faz com que a consulta seja pausada e eventualmente exceda o tempo limite. Esse tempo limite pode levar 5 minutos ou mais.

O Device Insights, que se integra à Orbital para fornecer melhores informações sobre endpoints, fornece uma consulta sob demanda por endpoint que inclui essas novas tabelas, independentemente de o endpoint estar localizado em uma instância AWS EC2 ou não. Isso faz com que os erros listados e suas consultas levem um longo período de tempo para serem concluídas.

Além disso, se um cliente usa consultas personalizadas envolvendo as novas tabelas EC2 em uma instância não AWS, ele encontra erros e tempos limite semelhantes.

Solução alternativa/soluções

A equipe do Device Insights está removendo as consultas direcionadas para as tabelas AWS EC2 em 22 de novembro de 2023.

Quaisquer consultas personalizadas usando as tabelas ec2_instance_metadata e ec2_instance_tags devem ser executadas somente em instâncias AWS EC2.

Não consulte essas tabelas em pontos de extremidade EC2 não-AWS.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.