

# Problemen oplossen Veilig eindpunt - Orbitale logboeken vullen met fouten - CSCwh73163

## Inhoud

---

[Inleiding](#)

[Voorbeeld](#)

[Hoofdoorzaak](#)

[Workaround/oplossingen](#)

---

## Inleiding

Orbitale logs op eindpunten kunnen veel foutmeldingen bevatten, zoals:

- De instantiemetagegevens kunnen niet worden opgehaald uit de metagegevensservice
- Er zijn 3 pogingen mislukt om een IMDSv2-token op te halen

Deze foutlogboeken kunnen na verloop van tijd de Orbital-logboeken op de getroffen eindpunten verstoppert en vullen.

## Voorbeeld

```
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 atter
```

Dit probleem wordt momenteel gevolgd op [CSCwh73163](#)

## Hoofdoorzaak

Op 21-08-2023 verbeterde Orbital osquery van 5.5.1 naar 5.8.2 voor release 1.31.

Osquery 5.6.0 heeft 2 nieuwe tabellen toegevoegd om informatie te geven over [AWS EC2-instanties](#): `ec2_instance_metadata` en `ec2_instance_tags`. Wanneer query's op deze tabellen worden geprobeerd voor eindpunten die niet op AWS EC2-instanties staan, worden fouten weergegeven die vergelijkbaar zijn met de vermelde fouten. (Raadpleeg de [projectbug](#) van [osquery](#) voor meer details). Als u probeert deze tabellen op niet-AWS EC2-instanties te bevragen, wordt de query ook onderbroken en wordt er uiteindelijk een time-out uitgevoerd. Deze time-out kan 5 minuten of langer duren.

Device Insights, dat met Orbital wordt geïntegreerd om betere informatie over eindpunten te

bieden, biedt een on-demand query per eindpunt met deze nieuwe tabellen, ongeacht of het eindpunt zich op een AWS EC2-instantie bevindt of niet. Dit leidt ertoe dat het langer duurt voordat de vermelde fouten en de bijbehorende zoekopdrachten zijn voltooid.

Bovendien, als een klant aangepaste query's gebruikt met betrekking tot de nieuwe EC2-tabellen op een niet-AWS-instantie, komen ze vergelijkbare fouten en time-outs tegen.

## Workaround/oplossingen

Het Device Insights-team verwijdert de zoekopdrachten die zich richten op de AWS EC2-tabellen op 22 november 2023.

Aangepaste query's met de tabellen `ec2_instance_metadata` en `ec2_instance_tags` mogen alleen worden uitgevoerd met AWS EC2-instanties.

Deze tabellen niet opvragen op niet-AWS EC2-eindpunten.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.