

Risoluzione dei problemi relativi a Secure Endpoint - Registri orbitali con errori - CSCwh73163

Sommario

[Introduzione](#)

[Esempio](#)

[Causa principale](#)

[Soluzioni](#)

Introduzione

I registri orbitali sugli endpoint possono contenere numerose voci di errore, ad esempio:

- Impossibile ottenere i metadati dell'istanza dal servizio metadati
- 3 tentativi non riusciti di recupero di un token IMDSv2

Questi log degli errori, nel tempo esteso, possono ingombrare e riempire i log orbitali sugli endpoint interessati.

Esempio

```
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
```

Il problema è attualmente tracciato su [CSCwh73163](#)

Causa principale

Nel 2023-08-21, Orbital ha aggiornato osquery da 5.5.1 a 5.8.2 per la release 1.31.

Osquery 5.6.0 ha aggiunto 2 nuove tabelle per fornire informazioni sulle [istanze AWS EC2](#): `ec2_instance_metadata` e `ec2_instance_tags`. Quando si tenta di eseguire query su queste tabelle per gli endpoint non su istanze AWS EC2, vengono visualizzati errori simili a quelli elencati. Per ulteriori informazioni, fare riferimento al [bug del progetto osquery](#). Se si tenta di eseguire una query su queste tabelle in istanze di EC2 non AWS, la query verrà sospesa e alla fine si verificherà un timeout. Questo timeout può richiedere 5 minuti o più.

Device Insights, che si integra con Orbital per fornire informazioni migliori sugli endpoint, fornisce una query su richiesta per ogni endpoint che include queste nuove tabelle, indipendentemente dal fatto che l'endpoint si trovi o meno in un'istanza AWS EC2. Di conseguenza, gli errori elencati e le relative query impiegano un periodo di tempo prolungato per il completamento.

Inoltre, se un cliente utilizza query personalizzate che coinvolgono le nuove tabelle EC2 in un'istanza non AWS, si verificano errori e timeout simili.

Soluzioni

Il team di Device Insights sta rimuovendo le query destinate alle tabelle AWS EC2 del 22 novembre 2023.

Le query personalizzate che utilizzano le tabelle `ec2_instance_metadata` e `ec2_instance_tags` devono essere eseguite solo su istanze AWS EC2.

Non eseguire query su queste tabelle in endpoint EC2 non AWS.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).