Cisco Secure Endpoint - Orbital Logs Filling Up with Errors - CSCwh73163

Contents

Issue

Orbital logs on endpoints can contain many error entries, such as:

- Failed to get instance metadata from the metadata service
- Failed 3 attempts at retrieving an IMDSv2 token

These error logs, over extended time, can clutter and fill up the Orbital logs on endpoints that are impacted.

Example

```
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
```

This issue is currently being tracked on CSCwh73163

Root Cause

On 2023-08-21, Orbital upgraded osquery from 5.5.1 to 5.8.2 for Release 1.31.

Osquery 5.6.0 added 2 new tables to provide information regarding AWS EC2 instances: ec2_instance_metadata and ec2_instance_tags. When queries are attempted on these tables for endpoints not on AWS EC2 instances, errors similar to those listed above will be displayed. (Refer to the osquery project bug for more details). Attempting to query these tables on non-AWS EC2 instances will also cause the query to pause and eventually timeout. This timeout can take 5 minutes or longer.

Device Insights, which integrates with Orbital to provide better information about endpoints, provides an on-demand query per endpoint that includes these new tables, regardless of whether the endpoint is located on an AWS EC2 instance or not. This results in the errors listed above and their queries taking an extended period of time to complete.

Additionally, if a customer uses custom queries involving the new EC2 tables on a non-AWS instance, they will encounter similar errors and timeouts.

Workaround/Solutions

The Device Insights team will be removing the queries that target the AWS EC2 tables on Nov 22, 2023.

Any custom queries using the ec2_instance_metadata and ec2_instance_tags tables should only be executed against AWS EC2 instances only.

Do not query these tables on non-AWS EC2 endpoints.