보안 엔드포인트 문제 해결 - 오류 가득 채우기 궤도 로그 - CSCwh73163

목차

소개

예

근본 원인

해결 방법/솔루션

소개

엔드포인트의 궤도 로그에는 다음과 같은 많은 오류 항목이 포함될 수 있습니다.

- 메타데이터 서비스에서 인스턴스 메타데이터를 가져오지 못했습니다.
- IMDSv2 토큰 검색을 3회 시도했으나 실패했습니다.

이러한 오류 로그는 장기간에 걸쳐 영향을 받는 엔드포인트의 Orbital 로그를 어수선하게 만들어 채울 수 있습니다.

예

```
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
```

이 문제는 현재 CSCwh에서 추적 중입니다73163

근본 원인

오비탈은 2023-08-21년, 오비탈을 5.5.1에서 5.8.2로 업그레이드하여 1.31 릴리스를 출시했습니다.

Osquery 5.6.0에는 AWS EC2 인스턴스에 대한 정보를 제공하기 위해 2개의 새로운 테이블이 추가되었습니다. ec2_instance_metadata 및 ec2_instance_tags입니다. AWS EC2 인스턴스가 아닌 엔드포인트에 대해 이러한 테이블에서 쿼리를 시도하면 나열된 것과 유사한 오류가 표시됩니다. (자세한 내용은 osquery 프로젝트 버그를 참조하십시오.) 비 AWS EC2 인스턴스에서 이러한 테이블을 쿼리하려고 시도하면 쿼리가 일시 중지되고 결국 시간 초과됩니다. 이 시간 제한은 5분 이상 걸릴 수 있습니다.

Orbital과 통합하여 엔드포인트에 대한 더 나은 정보를 제공하는 Device Insights는 엔드포인트가 AWS EC2 인스턴스에 위치하는지 여부에 관계없이 엔드포인트당 온디맨드 쿼리를 제공합니다. 이

렇게 하면 나열된 오류와 해당 쿼리를 완료하는 데 오랜 시간이 걸립니다.

또한 고객이 비 AWS 인스턴스에서 새 EC2 테이블과 관련된 사용자 지정 쿼리를 사용할 경우 유사한 오류와 시간 초과가 발생합니다.

해결 방법/솔루션

Device Insights 팀은 2023년 11월 22일 AWS EC2 테이블을 대상으로 하는 쿼리를 제거하고 있습니다.

ec2_instance_metadata 및 ec2_instance_tags 테이블을 사용하는 사용자 지정 쿼리는 AWS EC2 인스턴스에 대해서만 실행해야 합니다.

비 AWS EC2 엔드포인트에서 이러한 테이블을 쿼리하지 마십시오.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.