XDR 장치 통찰력 및 궤도 통합 문제 해결

목차

소개

이 문서에서는 통합을 구성하고 Device Insights 및 Orbital 통합을 트러블슈팅하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

컨피그레이션에 대해 자세히 알아보려면 여기 통합 모듈 세부 정보.

배경 정보

XDR Device Insights는 조직 내 장치에 대한 통합 보기를 제공하며 Orbital과 같은 통합 데이터 소스의 인벤토리를 통합합니다.

문제 해결

이 섹션에서는 컨피그레이션 트러블슈팅에 사용할 수 있는 정보를 제공합니다.

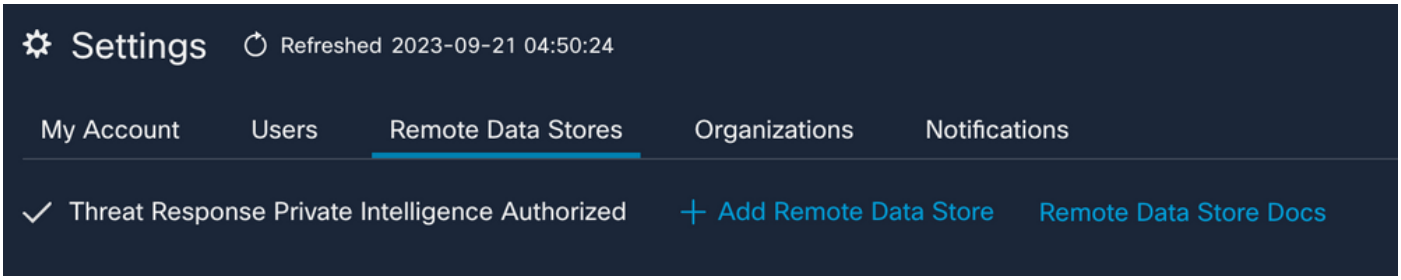
연결

- 소스의 REST API 자격 증명을 사용하여 Postman과 같은 툴을 사용하여 기본 연결을 테스트

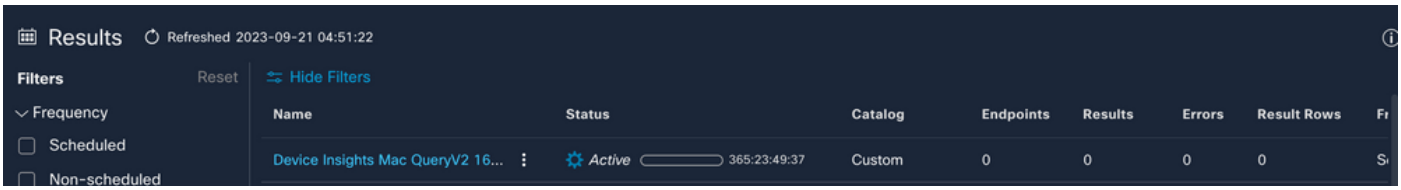
할 수 있습니다.

- 쿼리 결과가 Orbital 에이전트에서 나오기 시작하면 데이터는 원격 데이터 저장소에 게시됩니다.
- Device Insights에 대해 원격 데이터 저장소가 생성되었는지 확인합니다. 계정 설정에서 확인할 수 있습니다.

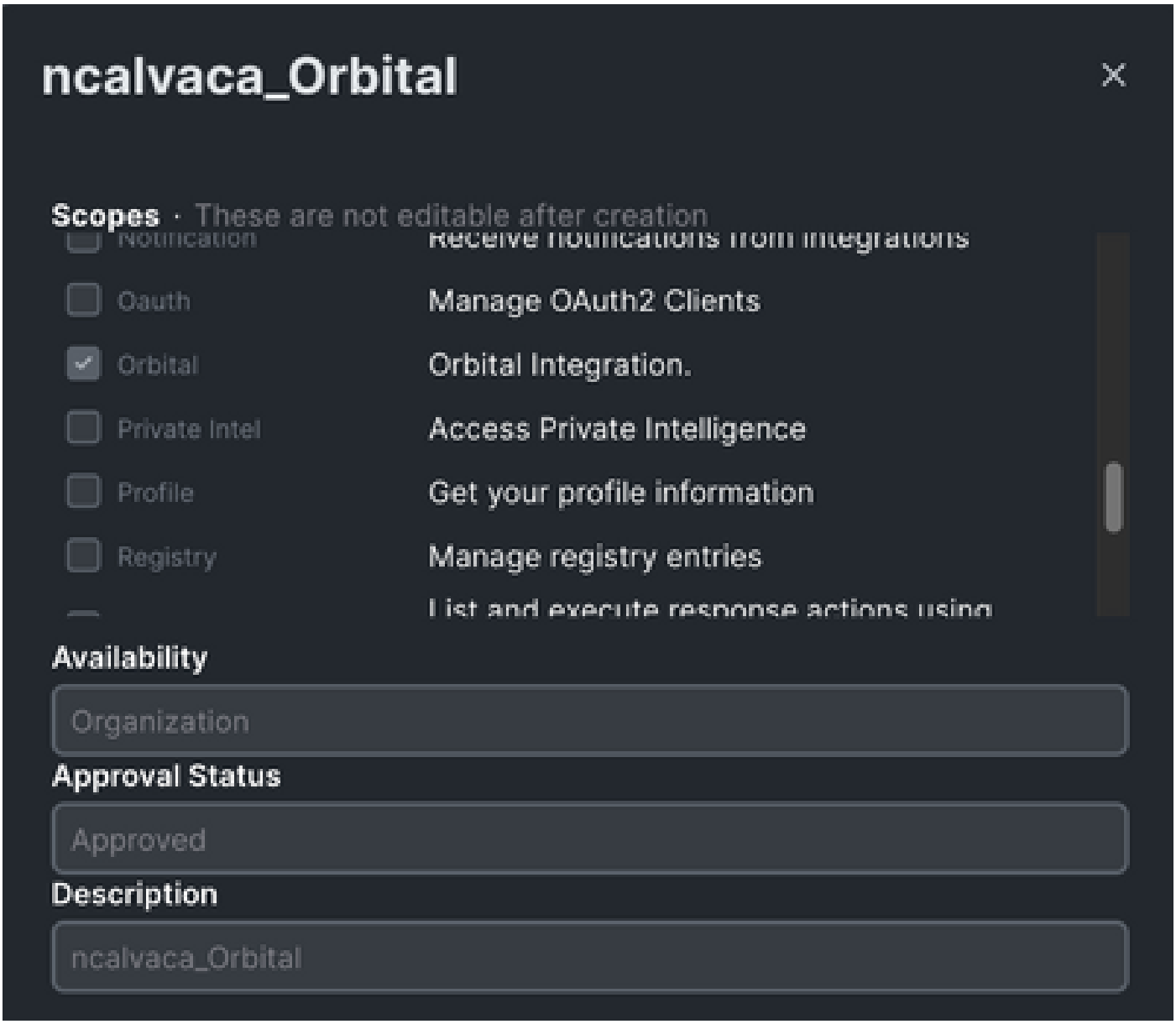
- Remote Data Store 세부 정보 관리자에서 Device Insights 테넌트 ID와 Device Insights URL이 표시되는지 확인합니다. Status는 Authenticated여야 합니다.



- Device Insights에서 만든 작업을 작업 목록에서 보려면 결과 탭으로 이동합니다.



- XDR 포털에서 Administration(관리)으로 이동하여 API Clients(API 클라이언트)를 선택하고 Orbital(오비탈)이 선택되었는지 확인합니다.



- 오류 "엔드포인트에서 응답이 없습니다. 오프라인 상태일 수 있습니다." - 이 오류는 엔드포인트가 꺼져 있거나 Orbital 클라우드와 연결되어 있지 않음을 의미합니다. 올바른 Cisco Secure Endpoint & Malware Analytics Operations의 필수 서버 주소 문서를 참조하여 IP, 포트 및 URL이 허용되는지 확인하십시오.

불일치 수

- 디바이스 수가 일치하지 않으면 Orbital이 버전 1.14 이후 90일 이상 된 엔드포인트의 인벤토리를 유지하지 않으므로 이는 Orbital 커넥터가 설치된 모든 엔드포인트를 포함하며 인벤토리에 활성 엔드포인트만 포함되지 않습니다. 디바이스 인사이트 기능이 활성화되면 모든 엔드포인트에 대해 매일 반복되는 작업이 생성됩니다. 작업이 엔드포인트에서 실행되고 결과 디바이스 정보가 Orbital로 다시 전송되면 XDR은 Orbital에서 해당 디바이스의 존재를 알립니다. 90일 이내에 해당 디바이스에 대한 작업 결과가 수신되지 않으면 디바이스 인사이트의 인벤토리에서 Orbital 엔드포인트가 삭제됩니다.
- 궤도 재설치로 인해 새 GUID가 생성되면 콘솔에 중복이 발생할 수 있습니다.

라이선스

- Secure Endpoint Console에 Orbital에 액세스할 수 있는 적절한 라이센스가 있는지 확인합니다.

Mac 및 Linux 디바이스가 표시되지 않음

- XDR Device Insights에서는 아직 오비탈 소스의 MacOS 및 Linux 디바이스가 지원되지 않습니다.

XDR Device Insights 및 Orbital 통합과 관련하여 문제가 지속되는 경우 이 문서를 참조하여 브라우저에서 HAR 로그를 수집하고 TAC 지원에 문의하여 더 심층적인 분석을 수행하십시오.

관련 정보

- XDR 참조 설명서
- 궤도 트러블슈팅
- 기술 지원 및 문서 – Cisco Systems

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.