

역할을 통해 객체 및 이벤트를 삭제할 수 있는 유효 권한

적용 가능성

스플링크 고공

설명

사용자가 아티팩트 및 이벤트만 삭제할 수 있도록 특정 권한을 설정하는 방법을 알아봅니다.

조사

단계 재현:

AS 관리자:

1. ADMINISTRATION(관리) -> USER MANAGEMENT(사용자 관리) -> ROLES AND PERMISSIONS(역할 및 권한) -> Select "CSOC Orchestration Engineer(CSOC 오케스트레이션 엔지니어)" 역할로 이동합니다.
2. 기본 권한 탭에서 이벤트 삭제, 편집 및 보기를 선택하거나 사용으로 설정합니다
3. LABEL PERMISSIONS(레이블 권한) 탭에서 사용자가 객체 및 이벤트를 삭제할 수 있게 할 각 레이블에 대해 DELETE, EDIT 및 VIEW를 선택/활성화합니다.
4. 변경사항을 저장합니다
5. 내 명명 계정 사용자로 로그인하고 삭제 권한이 있는 레이블로 이벤트를 생성합니다.
6. 값이 몇 개 포함된 객체를 추가합니다.
7. 이제 방금 생성한 동일한 객체를 삭제하려고 시도하면 삭제 버튼이 회색으로 표시됩니다.
8. 이제 방금 생성한 바로 그 이벤트를 삭제하려고 시도하면 DELETE 버튼이 회색으로 표시됩니다

역할 권한에 누락된 항목이 있는 것 같습니다.

설명서가 상세하지 않아서 어떤 것이 빠졌는지 설명이 안 됩니다.

문제 해결:

1. 브라우저를 새로 고치려고 했습니다.
2. 동일한 권한을 사용하여 새 역할의 새 로컬 계정을 만들려고 했습니다.
 - TEST1이라는 새 로컬 계정을 만들었습니다.

- 그런 다음 CSOC ORCHESTRATOR 역할을 TEST1 사용자에게 추가했으며 사용자는 아티팩트 또는 이벤트를 삭제할 수 없습니다.
- TEST1ROLE이라는 새 역할을 만들었습니다.
- TEST1ROLE의 권한을 CSOC ORCHESTRATOR 역할과 정확히 동일하게 설정합니다.
- 사용자가 아티팩트 및 이벤트를 삭제할 수 있었습니다.
- TEST1 사용자 역할을 다시 CSOC ORCHESTRATOR로 변경했으며 사용자는 아티팩트 또는 이벤트를 삭제할 수 없습니다.
- 따라서 어떤 이유에서든 기존 CSOC ORCHESTRATOR 역할의 구문 분석/시행 문제에 대한 힌트를 제공합니다.

3. 두 역할에 대한 rest API를 확인하려면

```
https://<phantom_ip>/rest/role/<TEST1ROLE_ID>
https://<phantom_ip>/rest/role/<CSOC_ORCHESTRATOR_ID>
```

Role ID를 가져오려면 해당 특정 역할 컨피그레이션으로 이동한 다음 URL에서 URL 경로의 끝에 있는 정수를 찾는 것이 가장 쉽습니다. 역할 ID입니다.

그렇지 않으면 `https://<phantom_ip>/rest/role`과 함께 모든 Role을 나열할 수 있습니다. 여기서 각 Role의 JSON 파일에서 ID를 찾을 수 있습니다.

JSON 파일 컨피그레이션에 차이가 있는지 확인합니다.

4. CSOC Orchestrator Role JSON 출력이 더 큰 것 같습니다.

5. 테넌트 nabCERT CSOC가 삭제를 거부하는 CSOC Orchestrator Role에 컨피그레이션이 있습니다. 이것은 사용자가 삭제를 허용하지 않는 문제입니다.

```
{
  "execute": "deny",
  "name": "tenant",
  "extra": "nabCERT CSOC",
  "edit": "allow",
  "object_id": 1,
  "role": 8,
  "content_type": 20,
  "delete": "deny",
  "id": 66,
  "view": "allow"
}
```

해결

CSOC 오케스트레이션 엔지니어 역할을 변경하여 nabCERT CSOC 역할 거부를 허용합니다.

```
{
  "execute": "deny",
  "name": "tenant",
  "extra": "nabCERT CSOC",
  "edit": "allow",
  "object_id": 1,
  "role": 8,
  "content_type": 20,
  "delete": "allow",
  "id": 66,
  "view": "allow"
}
```

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.