# ISE Context Visibility(상황 가시성)Elasticsearch Corruption(Elasticsearch 손상) 및 Ghost Endpoint(고스트 엔드포인트) 문제 해결

## 목차

## 문제

Cisco ISE(Identity Services Engine) 3.2의 컨텍스트 가시성은 기능에 액세스하려고 할 때 "모든 샤드가 실패했습니다" 오류가 있는 Elasticsearch 예외를 표시합니다. 또한 엔드포인트는 MAC 주소를 수동으로 추가하면 "엔드포인트가 이미 있음"이 반환되지만 디바이스가 GUI 또는 검색 기능에 표시되지 않는 고스트 항목으로 표시됩니다. 이러한 손상으로 인해 새 디바이스가 성공적으로 인증되지 못하므로 ID 그룹에 할당할 수 없으므로 기본 거부 정책에서 실패하여 엔드포인트 온보딩을 효과적으로 차단할 수 있습니다.

## 환경

- Cisco ISE(Identity Services Engine) 버전 3.2
- ISE 모니터링, 문제 해결 및 가시성 구성 요소
- Elasticsearch 인덱싱 시스템
- 컨텍스트 가시성 기능
- ISE 인덱싱 엔진 서비스가 실행 중이지만 기능이 손상됨

## 해결

1. ISE 애플리케이션 상태를 확인하여 인덱싱 엔진 서비스 상태를 확인합니다.

<#root>

**show application status ise**

```
ISE PROCESS NAME                       STATE            PROCESS ID

--------------------------------------------------------------------

Database Listener                      running          4278
Database Server                        running          128 PROCESSES
Application Server                     running          22343
Profiler Database                      running          12130

ISE Indexing Engine                    running          23867


AD Connector                           running          40415
M&T Session Database                   running          18502
M&T Log Processor                      running          22838
Certificate Authority Service          running          36578
EST Service                            running          53105
SXP Engine Service                     disabled
TC-NAC Service                         disabled
PassiveID WMI Service                  running          37050
PassiveID Syslog Service               running          37938
PassiveID API Service                  running          38666
PassiveID Agent Service                running          39356
PassiveID Endpoint Service             running          39737
PassiveID SPAN Service                 running          40239
DHCP Server (dhcpd)                    disabled
DNS Server (named)                     disabled
ISE Messaging Service                  running          8760
ISE API Gateway Database Service       running          11076
ISE API Gateway Service                running          17461
ISE pxGrid Direct Service              running          50936
Segmentation Policy Service            disabled
REST Auth Service                      disabled
SSE Connector                          disabled
Hermes (pxGrid Cloud Agent)            disabled
McTrust (Meraki Sync Service)          disabled
MFA (Duo Sync Service)                 disabled
ISE Node Exporter                      disabled
ISE Prometheus Service                 disabled
ISE Grafana Service                    disabled
ISE MNT LogAnalytics Elasticsearch     disabled
ISE Logstash Service                   disabled
ISE Kibana Service                     disabled
ISE Native IPSec Service               running          47108
MFC Profiler                           running          57620
```

---

참고: 필요한 출력은 작동 오류가 지속되는 경우에도 ISE 인덱싱 엔진을 "실행 중"으로 표시합니다.

---

2. Elasticsearch 및 Context Visibility 손상 문제에 대한 문서화된 표준 복구 방법에 따라 Context

Visibility 재설정 및 재동기화 절차를 실행합니다. 이 프로세스에는 손상된 인덱스를 재설정하고, 고스트 엔드포인트를 지우고, 엔드포인트 가시성 데이터를 재구축하는 작업이 포함됩니다. 다음을 참조하십시오.

Context Visibility 설명서를 재동기화합니다.

3. 재설정 및 재동기화 프로세스를 완료한 후 다음을 확인합니다.

- Context Visibility에 액세스할 때 더 이상 Elasticsearch 예외가 발생하지 않습니다.
- 고스트 엔드포인트가 시스템에서 지워집니다.
- 새 엔드포인트를 온보딩하고 성공적으로 인증할 수 있음
- "Endpoint already exists(엔드포인트가 이미 있음)" 잘못된 충돌이 더 이상 나타나지 않습니다
- GUI 및 검색 기능에서 엔드포인트 가시성 복원

4. 새 디바이스를 네트워크에 올바르게 온보딩하고 적절한 ID 그룹에 할당하며 기본 거부 정책을 받지 않고 인증할 수 있는지 확인합니다

## 원인

근본 원인은 ISE Context Visibility Elasticsearch 인덱싱 시스템 내의 손상입니다. 이 손상은 "모든 샤드 실패" 예외로 표시되고 데이터베이스 불일치가 발생하여 유령 엔드포인트 항목이 생성됩니다. 인덱싱 손상은 ID 그룹에 대한 적절한 엔드포인트 가시성 및 할당을 방지하여 새 디바이스에 대한 인증 실패를 유발합니다.

## 관련 콘텐츠

- ISE(Identity Services Engine) 상황 가시성 재설정
- Cisco 기술 지원 및 다운로드

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.