# ISEコンテキストの可視性の弾性検索の破損とゴーストエンドポイントの問題のトラブルシューティング

## 内容

## お問い合わせ内容

Cisco Identity Services Engine(ISE)3.2のコンテキスト可視性では、機能にアクセスしようとすると、「all shards failed」エラーを伴うElasticsearch例外が表示されます。また、エンドポイントはゴーストエントリとして表示され、MACアドレスを手動で追加すると「Endpoint already exists」と返されますが、GUIまたは検索機能ではデバイスは表示されません。この破損により、新しいデバイスの認証が成功せず、IDグループに割り当てることができないため、デフォルトの拒否ポリシーで失敗し、エンドポイントのオンボーディングが実質的にブロックされます。

## 環境

- Cisco Identity Services Engine(ISE)バージョン3.2
- ISEモニタリング、トラブルシューティング、および可視性のコンポーネント
- エラスティックサーチインデックスシステム
- コンテキスト表示機能
- ISEインデックスエンジンサービスは実行中ですが、機能が低下しています

## 解決策

1. ISEアプリケーションステータスを確認して、インデックスエンジンサービスのステータスを確認します。

<#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
```

---

注：機能エラーが続いているにもかかわらず、予想される出力には、ISEインデックスエンジンが「実行中」と表示されます。

---

2. ElasticsearchとContext Visibilityの破損の問題に対して、文書化されている標準的な回復方法に従って、Context Visibilityのリセットおよび再同期手順を実行します。このプロセスには、破損したインデックスのリセット、ゴーストエンドポイントのクリア、およびエンドポイントの可視性データの再構築が含まれます。詳細については、

Context Visibilityドキュメントの再同期

3. リセットおよび再同期プロセスが完了したら、次のことを確認します。

- コンテキストの可視性へのアクセス時にElasticsearch例外が発生しなくなりました
- ゴーストエンドポイントがシステムから消去されます
- 新しいエンドポイントをオンボーディングし、正常に認証できる
- 「エンドポイントはすでに存在します」という誤った競合が表示されなくなりました
- エンドポイントの可視性は、GUIおよび検索機能で復元されます。

4. 新しいデバイスがネットワークに適切にオンボーディングされ、適切なアイデンティティグループに割り当てられ、デフォルトの拒否ポリシーを受信せずに認証できることを確認します。

## 原因

根本原因は、ISE Context Visibility Elasticsearchインデックスシステム内の破損です。この破損は「すべてのシャードが失敗しました」という例外として現れ、ゴーストエンドポイントエントリを引き起こすデータベースの不整合を引き起こします。インデックスの破損により、IDグループへのエンドポイントの適切な可視性と割り当てが妨げられ、新しいデバイスの認証エラーが発生します。

## 関連コンテンツ

- Identity Services Engine(ISE)コンテキストの可視性のリセット
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。