Troubleshoot ISE Context Visibility Elasticsearch Corruption and Ghost Endpoint Issues

Contents

Issue

Context Visibility in Cisco Identity Services Engine (ISE) 3.2 displays an Elasticsearch exception with "all shards failed" error when attempting to access the feature. Additionally, endpoints appear as ghost entries where adding a MAC address manually returns "Endpoint already exists" but the device is not visible in the GUI or search functionality. This corruption prevents new devices from authenticating successfully, causing them to fail with Default Deny policies because they cannot be assigned to Identity Groups, effectively blocking endpoint onboarding.

Environment

- Cisco Identity Services Engine (ISE) version 3.2
- ISE Monitoring, Troubleshooting and Visibility components
- Elasticsearch indexing system
- Context Visibility feature
- ISE Indexing Engine service running but functionally impaired

Resolution

1. Check the ISE application status to confirm the indexing engine service status:

<#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
```

Note: The expected output shows ISE Indexing Engine as "Running" despite functional errors persisting.

---

2. Execute the Context Visibility reset and resync procedure according to the documented standard recovery method for Elasticsearch and Context Visibility corruption issues. This process involves resetting corrupted indexes, clearing ghost endpoints, and rebuilding endpoint visibility data. Refer to the

Resync Context Visibility documentation.

3. After completing the reset and resynchronization process, verify that:

- Elasticsearch exceptions no longer occur when accessing Context Visibility
- Ghost endpoints are cleared from the system
- New endpoints can be onboarded and authenticated successfully
- The "Endpoint already exists" false conflict no longer appears
- Endpoint visibility is restored in the GUI and search functionality

4. Confirm that new devices can be properly onboarded to the network, assigned to appropriate Identity Groups, and authenticate without receiving Default Deny policies

Cause

The root cause is corruption within the ISE Context Visibility Elasticsearch indexing system. This corruption manifests as "all shards failed" exceptions and creates database inconsistencies that result in ghost endpoint entries. The indexing corruption prevents proper endpoint visibility and assignment to Identity Groups, causing authentication failures for new devices.

Related Content

- Reset Identity Services Engine (ISE) Context Visibility
- Cisco Technical Support & Downloads