排除ISE情景可視性Elasticsearch損壞和Ghost端點問題

目錄

問題

思科身份服務引擎(ISE)3.2中的情景可視性在嘗試訪問功能時顯示Elasticsearch異常和「所有碎片失敗」錯誤。此外，終端顯示為虛影條目，其中手動新增MAC地址會返回「終端已存在」，但裝置在GUI或搜尋功能中不可見。此損壞阻止新裝置成功進行身份驗證，導致它們使用預設拒絕策略失敗，因為它們無法分配到身份組，從而有效地阻止終端登入。

環境

- 思科身分識別服務引擎(ISE)版本3.2
- ISE監控、故障排除和可見性元件
- 彈性搜尋索引系統
- 情景可視性功能
- ISE索引引擎服務正在運行，但功能已損壞

解析

1.檢查ISE應用程式狀態以確認索引引擎服務狀態：

<#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
```

附註：預期輸出顯示ISE索引引擎為「正在運行」，儘管功能錯誤仍然存在。

2.根據已記錄的Elasticsearch和上下文可視性損壞問題的標準恢複方法執行上下文可視性重置和重新同步過程。此過程包括重置損壞的索引、清除虛影端點和重建端點可見性資料。請參閱

重新同步上下文可見性文檔。

3.完成重置和重新同步過程後，驗證：

- 訪問情景可視性時不再發生Elasticsearch異常
- 從系統中清除Ghost終結點
- 新端點可以登入並成功進行身份驗證
- 不再出現「Endpoint already exists」錯誤衝突
- 終端可視性在GUI和搜尋功能中恢復

4.確認新裝置可以正確接入網路，分配給適當的身份組，並在沒有接收預設拒絕策略的情況下進行身份驗證

原因

根本原因是ISE情景可視性Elasticsearch索引系統中的損壞。此損壞顯示為「所有碎片失敗」異常，並建立資料庫不一致，從而導致Ghost終結點條目。索引損壞會阻止對身份組的正確端點可見性和分配，從而導致新裝置的身份驗證失敗。

相關內容

- 重置身份服務引擎(ISE)情景可視性
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。