排除ISE情景可视性Elasticsearch损坏和Ghost终端问题

目录

问题

在尝试访问功能时，思科身份服务引擎(ISE)3.2中的情景可视性显示Elasticsearch异常和“所有分片失败”错误。此外，终端显示为ghost条目，其中手动添加MAC地址会返回“终端已存在”，但设备在GUI或搜索功能中不可见。此损坏会阻止新设备成功进行身份验证，导致它们使用默认拒绝策略失败，因为它们无法分配到身份组，从而有效阻止终端登录。

环境

- 思科身份服务引擎(ISE)版本3.2
- ISE监控、故障排除和可见性组件
- 弹性搜索索引系统
- 情景可视性功能
- ISE索引引擎服务正在运行，但功能受损

分辨率

1.检查ISE应用程序状态以确认索引引擎服务状态：

<#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
```

注意：预期输出显示ISE索引引擎为“Running”，尽管功能错误仍然存在。

2.根据Elasticsearch和情景可视性损坏问题的书面标准恢复方法执行情景可视性重置和重新同步过程。此过程包括重置损坏的索引、清除虚构端点和重建端点可视性数据。请参阅

重新同步情景可视性文档。

3.完成重置和重新同步过程后，请验证：

- 访问情景可视性时不再发生Elasticsearch异常
- 从系统中清除Ghost终端
- 新终端可以注册并成功通过身份验证
- 不再出现“Endpoint already exists”错误冲突
- 终端可视性在GUI和搜索功能中恢复

4.确认新设备可以正确连接到网络，分配到适当的身份组，并在不接收默认拒绝策略的情况下进行身份验证

原因

根本原因是ISE情景可视性Elasticsearch索引系统中的损坏。此损坏显示为“所有分片失败”异常，并造成数据库不一致，从而导致Ghost终端条目。索引损坏会阻止对身份组的正确终端可视性和分配，从而导致新设备的身份验证失败。

相关内容

- 重置身份服务引擎(ISE)情景可视性
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。