

Solucionar problemas de corrupção de pesquisa elástica de visibilidade de contexto do ISE e de endpoint fantasma

Contents

Problema

A Visibilidade de Contexto no Cisco Identity Services Engine (ISE) 3.2 exibe uma exceção Elasticsearch com erro "todos os fragmentos falharam" ao tentar acessar o recurso. Além disso, os endpoints aparecem como entradas fantasma em que a adição de um endereço MAC retorna manualmente "Endpoint already exists" (O endpoint já existe), mas o dispositivo não fica visível na GUI ou na funcionalidade de pesquisa. Essa corrupção impede que novos dispositivos sejam autenticados com êxito, fazendo com que eles falhem com as políticas de negação padrão, pois não podem ser atribuídos a grupos de identidade, bloqueando efetivamente a integração do endpoint.

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.2
- Componentes de monitoramento, solução de problemas e visibilidade do ISE
- Sistema de indexação Elasticsearch
- Recurso de visibilidade de contexto
- Serviço do Mecanismo de Indexação do ISE em execução, mas com falha funcional

Resolução

1. Verifique o status do aplicativo ISE para confirmar o status do serviço do mecanismo de

indexação:

<#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: A saída esperada mostra o Mecanismo de indexação do ISE como "Em execução" apesar da persistência de erros funcionais.

2. Execute o procedimento de redefinição e ressincronização de Visibilidade de Contexto de acordo com o método de recuperação padrão documentado para problemas de corrompimento de Elasticsearch e Visibilidade de Contexto. Esse processo envolve a redefinição de índices corrompidos, a limpeza de pontos de extremidade fantasmas e a reconstrução de dados de visibilidade do ponto de extremidade. Consulte a seção

Documentação [de visibilidade de contexto de ressincronização](#).

3. Após concluir o processo de redefinição e ressincronização, verifique se:

- As exceções de pesquisa elástica não ocorrem mais ao acessar a Visibilidade de contexto
- Os pontos de extremidade fantasmas são removidos do sistema
- Novos endpoints podem ser integrados e autenticados com êxito
- O conflito falso "Ponto de Extremidade já existe" não aparece mais
- A visibilidade do endpoint é restaurada na GUI e na funcionalidade de pesquisa

4. Confirme se os novos dispositivos podem ser integrados corretamente à rede, atribuídos aos grupos de identidade apropriados e autenticados sem receber políticas de negação padrão

Causa

A causa principal é a corrupção no sistema de indexação Elasticsearch do ISE Context Visibility. Essa corrupção se manifesta como exceções de "todos os fragmentos falharam" e cria inconsistências de banco de dados que resultam em entradas de ponto de extremidade fantasma. A corrupção da indexação impede a visibilidade e a atribuição adequadas do endpoint aos grupos de identidade, causando falhas de autenticação para novos dispositivos.

Conteúdo relacionado

- [Redefinir a visibilidade de contexto do Identity Services Engine \(ISE\)](#)
- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.