Risoluzione dei problemi relativi alla visibilità del contesto ISE per Elasticsearch Corruption e Ghost Endpoint

Sommario

Problema

Durante il tentativo di accesso alla funzionalità, in Cisco Identity Services Engine (ISE) 3.2 viene visualizzata un'eccezione Elasticsearch con l'errore "all shards failed" (tutte le condivisioni non riuscite). Inoltre, gli endpoint vengono visualizzati come voci ghost, in cui l'aggiunta manuale di un indirizzo MAC restituisce "Endpoint già esistente" ma il dispositivo non è visibile nella GUI o nella funzionalità di ricerca. Il danneggiamento impedisce ai nuovi dispositivi di eseguire correttamente l'autenticazione, provocando il mancato rispetto dei criteri di negazione predefiniti in quanto non possono essere assegnati a gruppi di identità e bloccando di fatto l'onboarding dell'endpoint.

Ambiente

- Cisco Identity Services Engine (ISE) versione 3.2
- Componenti ISE Monitoring, Troubleshooting e Visibility
- Sistema di indicizzazione Elasticsearch
- Funzione Visibilità contesto
- Servizio Motore di indicizzazione ISE in esecuzione, ma con problemi di funzionalità

Risoluzione

1. Controllare lo stato dell'applicazione ISE per confermare lo stato del servizio del motore di indicizzazione:

<#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
```

Nota: L'output previsto visualizza il motore di indicizzazione ISE come "in esecuzione" nonostante il persistere di errori funzionali.

---

2. Eseguire la procedura di reimpostazione e risincronizzazione della visibilità del contesto in base al metodo di ripristino standard documentato per i problemi di danneggiamento di Elasticsearch e della visibilità del contesto. Questo processo include la reimpostazione degli indici danneggiati, la cancellazione degli endpoint fantasma e la ricostruzione dei dati di visibilità degli endpoint. Per ulteriori informazioni, fare riferimento al

Documentazione relativa alla visibilità del contesto di risincronizzazione.

3. Dopo aver completato il processo di reimpostazione e risincronizzazione, verificare che:

- Le eccezioni Elasticsearch non si verificano più quando si accede a Visibilità contesto
- Gli endpoint fantasma vengono cancellati dal sistema
- È possibile caricare e autenticare nuovi endpoint
- Il conflitto falso "Endpoint già esistente" non viene più visualizzato
- La visibilità degli endpoint viene ripristinata dalla GUI e dalla funzionalità di ricerca

4. Confermare che i nuovi dispositivi possano essere collegati correttamente alla rete, assegnati ai gruppi di identità appropriati e autenticati senza ricevere le policy di negazione predefinite

Causa

La causa principale è il danneggiamento all'interno del sistema di indicizzazione di ISE Context Visibility Elasticsearch. Questo danneggiamento si manifesta come eccezioni "tutte le condivisioni non riuscite" e crea incoerenze nel database che generano voci di endpoint fantasma. Il danneggiamento dell'indicizzazione impedisce la corretta visibilità degli endpoint e l'assegnazione ai gruppi di identità, causando errori di autenticazione per i nuovi dispositivi.

Contenuto correlato

- Ripristino della visibilità del contesto di Identity Services Engine (ISE)
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).