Risoluzione dei problemi di autenticazione VPN e RADIUS ISE 3.4

Sommario

Problema

Nelle implementazioni ISE 3.4 Patch 4 si verificano errori di autenticazione in caso di interruzione di un'attività su un nodo di amministrazione secondario (SAN). Anche le richieste di autenticazione dirette al PAN (Primary Policy Administration Node) hanno esito negativo, causando interruzioni delle connessioni VPN ASA e delle autenticazioni RADIUS. Il nodo SAN viene visualizzato come disconnesso nel dashboard di implementazione ISE e i registri indicano gli errori relativi a EAP/TLS e i problemi di tracciamento delle sessioni.

Ambiente

- Cisco Identity Services Engine (ISE)
- Dispositivi di accesso alla rete (NAD): Include dispositivi Meraki e/o firewall ASA
- Topologia: Implementazione ISE a più nodi con SAN e PAN

Risoluzione

1.- Rimuovere tutte le persone dal nodo SAN tramite l'interfaccia di amministrazione di Cisco ISE selezionando Amministrazione > Sistema > Distribuzione. In questo modo vengono interrotti i tentativi di autenticazione per il nodo non riuscito e viene consentito ai nodi non interessati di riprendere l'elaborazione.

 Nota: Dopo la rimozione dell'utente, il nodo SAN continua a essere visualizzato come

---

disconnesso (X rossa) nel dashboard di distribuzione.

2.- Forzare manualmente il firewall ASA a considerare il nodo SAN come NON RIUSCITO, impedendo che ulteriori tentativi di autenticazione vengano indirizzati alla SAN non disponibile. Questa azione viene eseguita sulla configurazione ASA, garantendo il failover sui nodi operativi ISE.

3.- Esaminare l'implementazione ISE per una corretta sincronizzazione e monitorare le metriche dello stato, incluso l'utilizzo di CPU, memoria e dischi.

4.- Verificare che i servizi di autenticazione siano operativi controllando che le nuove richieste Dot1x e RADIUS vengano elaborate dai nodi ISE non interessati.

5.- Raccogliere i registri DEBUG e le acquisizioni dei pacchetti durante gli errori di autenticazione per analizzare i tempi di negoziazione EAP/TLS e i ripristini delle sessioni.

6.- Continuare il monitoraggio delle metriche dello stato del sistema ISE e del comportamento di autenticazione dopo gli eventi di failover della SAN.

7.- Convalidare il comportamento del failover Meraki RADIUS, notando che ISE non supporta i pacchetti RADIUS "Status-Server" per il rilevamento della disponibilità del server.

Messaggi log di esempio

```
Accounting start was received for non-existing session
```

```
Error getting peer certificate from SSL Connection
```

```
packet for this endpoint 58-6D-67-XX-XX-XX is being processed right now so drop the new EAP session
```

```
Long step latency ;2=57290
```

```
Endpoint 58-6D-67-XX-XX-XX abandoned EAP session xxxxxxxxx/552628443/4183334 and started EAP session
```

Causa

La causa principale è un'interruzione del nodo SAN causata da un errore del collegamento ISP, che causa incoerenze nel tracciamento delle sessioni ed errori di negoziazione EAP/TLS tra i nodi supplicant, NAD e ISE. Inoltre, i dispositivi Meraki si basano sui pacchetti RADIUS "Status-Server" per il rilevamento del failover, che Cisco ISE non supporta, consentendo di continuare i tentativi di autenticazione sul nodo SAN guasto.

Contenuto correlato

- Procedura: Integrazione di Meraki Networks con ISE
- Configurazione della VPN ad accesso remoto con autenticazione RADIUS su ISE e Mapping Criteri di gruppo
- 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).