Dépannage des échecs d'authentification VPN et RADIUS ISE 3.4

Table des matières

Problème

Les déploiements ISE 3.4 Patch 4 connaissent des échecs d'authentification lorsqu'un noeud d'administration secondaire (SAN) subit une panne. Les demandes d'authentification dirigées vers le noeud PPAN (Primary Policy Administration Node) échouent également, entraînant des interruptions des connexions VPN ASA et des authentifications RADIUS. Le noeud SAN s'affiche comme déconnecté dans le tableau de bord de déploiement ISE et les journaux indiquent les erreurs EAP/TLS et les problèmes de suivi de session.

Environnement

- Cisco Identity Services Engine (ISE)
- Périphériques d'accès réseau (NAD) : Inclut les périphériques Meraki et/ou le pare-feu ASA
- Topologie: Déploiement ISE multinoeud avec SAN et PAN

Résolution

1.- Supprimez toutes les personnalités du noeud SAN via l'interface d'administration de Cisco ISE en sélectionnant Administration > System > Deployment. Cela interrompt les tentatives d'authentification sur le noeud défaillant et permet aux noeuds non affectés de reprendre le traitement.

 Remarque : Une fois la suppression de personnalisation effectuée, le noeud SAN continue à

---

s'afficher comme étant déconnecté (X rouge) dans le tableau de bord de déploiement.

2.- Forcez manuellement le pare-feu ASA à considérer le noeud SAN comme ÉCHOUÉ, ce qui empêchera d'autres tentatives d'authentification d'être dirigées vers le SAN non disponible. Cette action est effectuée sur la configuration ASA, assurant le basculement vers les noeuds ISE opérationnels.

3.- Examiner le déploiement ISE pour une synchronisation appropriée et surveiller les mesures d'intégrité, y compris l'utilisation du processeur, de la mémoire et du disque.

4.- Vérifiez que les services d'authentification sont opérationnels en vérifiant que les nouvelles requêtes Dot1x et RADIUS sont traitées par les noeuds ISE non affectés.

5.- Collecter les journaux DEBUG et les captures de paquets pendant les échecs d'authentification pour analyser la synchronisation de négociation EAP/TLS et les réinitialisations de session.

6.- Continuez à surveiller les mesures d'intégrité du système ISE et le comportement d'authentification après les événements de basculement SAN.

7.- Validez le comportement de basculement de Meraki RADIUS, en notant que ISE ne prend pas en charge les paquets RADIUS « Status-Server » pour la détection de la disponibilité du serveur.

Exemples de messages du journal

```
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
```

Motif

La cause principale est une panne de noeud SAN due à une défaillance de liaison ISP, qui entraîne des incohérences de suivi de session et des erreurs de négociation EAP/TLS entre les noeuds demandeur, NAD et ISE. En outre, les périphériques Meraki dépendent des paquets RADIUS « Status-Server » pour la détection de basculement, ce que Cisco ISE ne prend pas en charge, ce qui entraîne des tentatives d'authentification continues vers le noeud SAN défaillant.

Autres informations utiles

- Comment : Intégration des réseaux Meraki avec ISE
- Configurer le VPN d'accès à distance avec l'authentification RADIUS sur ISE et le mappage de stratégie de groupe
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.