Dépannage des échecs d'authentification ISE TACACS+ en raison d'une surcharge du système

Table des matières

Problème

Les authentifications TACACS+ (Terminal Access Controller Access-Control System Plus) de Cisco ISE (Identity Services Engine) cessent de fonctionner par intermittence et entraînent le retour des connexions des périphériques réseau aux utilisateurs locaux au lieu de l'authentification TACACS+. Pendant les pannes, les raisons de l'échec de la requête « TACACS+ a été abandonnée en raison d'une surcharge du système » s'affichent dans les journaux en direct. Les échecs d'authentification se produisent sans qu'aucune modification de configuration ne soit apportée à ISE pour TACACS+ ou aux périphériques réseau concernant la configuration TACACS+.

Environnement

- Correctif 7 de Cisco Identity Services Engine (ISE) version 3.3
- Déploiement ISE distribué avec PSN spécifiques pour l'administration des périphériques
- Service d'authentification TACACS+ pour l'accès administratif
- Configuration de la cible Syslog TCP (Transmission Control Protocol)

Résolution

L'activation des débogages runtime-AAA sur le noeud de service de stratégie (PSN) pendant le problème et l'examen de port-server.log révèlent des valeurs ContextN extrêmement élevées

indiquant que le traitement sur le PSN est sauvegardé :

```
ContextCounter,2026-05-05 12:17:08,442,DEBUG,0x7f42bead0700,ContextN incremented, number=113687,Context
```

AcsLoggerReactorThread et TCPSyslogReactorThread sont les pools de threads qui sont élevés et provoquent la sauvegarde :

```
EventHandler,2026-05-05 12:17:10,461,DEBUG,0x7f42bead0700,Passed event to the next thread pool name=Acs
EventHandler,2026-05-05 12:17:12,859,DEBUG,0x7f429b6d0700,Passed event to the next thread pool name=TCP
```

Les connexions TACACS+ sont abandonnées en raison de la limite d'espace atteinte :

```
TCPListener,2026-05-05 12:17:08,804,DEBUG,0x7f429b4cf700,NIL-CONTEXT,Hit space limit. Dropping request!
```

Toutes les cibles Syslog TCP activées sous Administration > System > Logging > Remote Logging Targets avec le paramètre « Buffer Messages When Server Down » activé dans la configuration ne doivent pas être inaccessibles pendant des périodes prolongées en raison du défaut Cisco CSCwt35414. Si l'accessibilité ne peut pas être garantie, une version fixe d'ISE doit être installée ou la fonctionnalité « Buffer Messages When Server Down » doit être désélectionnée sur la cible Syslog TCP pour empêcher ce comportement.

Motif

La cause première a été identifiée comme étant le défaut Cisco CSCwt35414. Ce défaut provoque le blocage du traitement d'authentification sur le PSN chaque fois que la mémoire tampon configurée sur la cible Syslog TCP devient pleine. Les journaux sont écrits dans la mémoire tampon lorsque la cible Syslog TCP est inaccessible ou ne répond pas pour être envoyée une fois qu'elle répond à nouveau, mais si la cible est inaccessible pendant de longues périodes avec un trafic important sur le PSN, la mémoire tampon se remplit et le traitement de l'authentification est affecté.

Autres informations utiles

- Défaut Cisco CSCwt35414
- Paramètres des cibles de journalisation distantes

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.