La saturation du contexte RADIUS ISE empêche le noeud de répondre

Table des matières

Problème

Un noeud Cisco Identity Services Engine (ISE) cesse de répondre de façon intermittente aux demandes d'authentification RADIUS, ce qui entraîne le marquage des périphériques réseau comme « RADIUS DEAD ». Le noeud affecté reçoit des requêtes RADIUS (confirmées par les journaux de pare-feu et les captures de paquets) mais ne répond pas. Les symptômes suivants sont observés :

- Messages de retransmission RADIUS sur les périphériques réseau
- Alarmes critiques « Radius Context Allocation Failed » apparaissant dans ISE
- Consigner les messages indiquant « Hit context count limit ». Abandon de la demande !"
- L'interface utilisateur graphique ISE devient inaccessible pendant le problème, même si tous les services sont en cours d'exécution
- Le noeud redémarre temporairement pour résoudre le problème pendant environ 30 minutes avant qu'il ne se reproduise

Les messages d'erreur spécifiques suivants ont été observés :

```
033057: Mar 11 09:33:59.015: RADIUS: Retransmit to (10.0.5.11:1812,1813) for id 1645/127
033058: Mar 11 09:33:59.015: RADIUS: PAC key found while sending request (rctx:0x75EB6A555690)
033059: Mar 11 09:33:59.015: RADIUS: Message Authenticator encoded
033060: Mar 11 09:33:59.015: RADIUS(00000000): Started 4 sec timeout
```

Et dans les journaux ISE :

```
RadiusListener,2026-06-28 23:21:22,149,WARN ,0x7efea2055700,NIL-CONTEXT,Hit context count limit. Droppi
```

Environnement

- Cisco Identity Services Engine (ISE) version 3.5.0.331 (patch 3)
- Noeud servant plusieurs rôles : Noeud d'administration principal (PAN), gestion de session et dépannage (SMNT) et noeud de service de stratégie (PSN)
- Méthodes d'authentification : 802.1X et MAB activés sur les ports de commutation d'accès
- Sources d'identité externes : Intégration de Microsoft Entra ID
- Périphériques réseau configurés avec ISE comme serveur RADIUS pour l'authentification

Résolution

Le problème a été résolu par l'application d'un correctif fourni par Cisco qui répond à une condition d'interblocage dans le processus ISE SessionUpdater. Suivez ces étapes pour mettre en oeuvre la résolution :

Étape 1: Obtention et installation du correctif logiciel

Téléchargez les fichiers de correctifs à partir de Cisco et transférez-les vers votre référentiel de noeuds ISE. Les fichiers de correctifs sont les suivants :

- ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz (fichier d'installation)
- ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz (fichier de restauration)

Étape 2: Application du correctif

Installez le correctif à l’aide de la commande CLI :

```
application install ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

⚠Mise en garde : Possible. Les détails mentionnés ici semblent contenir des procédures ou des commandes qui pourraient avoir un impact significatif si elles étaient exécutées. Veuillez vous assurer que les procédures ou commandes ci-dessus ont été évaluées par un expert ou une unité commerciale avant de les exécuter ou de les recommander.

Étape 3: Vérifier l'installation

Vérifiez l'installation du correctif à l'aide de l'une des commandes suivantes :

```
show logging application hotpatch.log
```

OU:

```
show version
```

Étape 4: Surveiller le système

Après l'installation, surveillez le noeud ISE pendant au moins deux semaines pour vous assurer que le problème ne se reproduit pas. L'installation du correctif nécessite un redémarrage du service. Par conséquent, planifiez l'installation au cours d'une fenêtre de maintenance.

Facultatif: Procédure De Restauration

Si nécessaire, le correctif peut être supprimé à l'aide de la commande rollback :

```
application install ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

Commandes de dépannage pour la surveillance

Pour surveiller l'allocation de contexte RADIUS, utilisez :

```
show logging application prrt-server.log | include ContextN
```

Activez les débogages AAA d'exécution avant tout dépannage ultérieur :

```
debug aaa runtime
```

Motif

La cause première a été identifiée comme une condition d'interblocage dans le processus SessionUpdater ISE. Lorsque des événements de début et d'arrêt de comptabilisation simultanés se sont produits pour la même session, deux threads ont entré un scénario d'attente circulaire :

- Thread-162 : propriétaire cacheLock, attente du verrouillage SessionInfo
- Thread-125 : SessionInfo propriétaire verrouillée, attente de cacheLock

Cette attente circulaire a entraîné des fuites de ContextN et une file d'attente de traitement RADIUS en constante augmentation. L'accumulation de file d'attente a fini par épuiser les contextes RADIUS disponibles, entraînant une latence d'authentification et des périphériques réseau pour marquer le noeud ISE comme RADIUS DEAD.

Le problème est documenté dans le bogue Cisco ayant l'ID CSCwv71473.

Autres informations utiles

- ID de bogue Cisco CSCwv71473
- 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.