Échec de l'authentification SSH dû à des conditions de mémoire insuffisante

Table des matières

Introduction

Problème

Solution

Introduction

Ce document décrit le problème sur un routeur Cisco IOS® lorsque Secure Shell (SSH) vers le routeur échoue parfois avec un échec d'authentification d'utilisateur signalé dans les débogages SSH. Ce problème se produit même si les informations d'identification de l'utilisateur saisies sont correctes et que les mêmes informations fonctionnent correctement pour Telnet.

> Remarque : L'ID de bogue Cisco CSCum19502 a été classé afin de rendre le comportement entre SSH et Telnet cohérent.

Problème

Notez dans ces débogages que même si « debug aaa authentication » est activé, il n'y a aucun débogage d'authentification, d'autorisation et de comptabilité (AAA) imprimé pour montrer que AAA est réellement appelé et renvoie l'échec.

<#root>

```
Router#
```

show debug

```
General OS:
  AAA Authentication debugging is on
SSH:
  Incoming SSH debugging is on
  ssh detail messages debugging is on
Router#
*Sep 30 20:28:57.172: SSH2 2: MAC compared for #8 :ok
*Sep 30 20:28:57.172: SSH2 2: input: padlength 15 bytes
*Sep 30 20:28:57.172: SSH2 2: Using method =
keyboard-interactive
*Sep 30 20:28:57.172: SSH2: password authentication failed
for cisco
*Sep 30 20:28:59.172: SSH2 2: send:packet of  length 64
(length also includes padlen of 14)
*Sep 30 20:28:59.172: SSH2 2: computed MAC for sequence
```

```
no.#8 type 51
*Sep 30 20:29:01.751: SSH2 2: ssh_receive: 144 bytes received
*Sep 30 20:29:01.751: SSH2 2: input: total packet length of
128 bytes
*Sep 30 20:29:01.751: SSH2 2: partial packet length(block size)
16 bytes,needed 112 bytes,
```

Parfois, le syslog affiché ici est également observé lorsque SSH est tenté, mais il n'est pas imprimé de manière cohérente :

```
*Sep 30 20:23:27.598: %AAA-3-ACCT_LOW_MEM_UID_FAIL: AAA unable to create UID for incoming
calls due to insufficient processor memory
```

La cause principale du problème est une mémoire insuffisante sur le routeur. Lorsque AAA ne parvient pas à allouer de la mémoire pour créer l'ID unique (UID) pour la session SSH entrante, il signale le même échec qu'un échec d'authentification AAA même si AAA n'est pas tenté. Cette condition se produit quand la mémoire libre du processeur tombe en dessous du AAA "Authentication low-memory threshold", qui par défaut est défini à 3% de la mémoire totale et peut être vérifié avec la commande show aaa memory. Ce problème est souvent rencontré sur une plate-forme ASR (Aggregation Services Router) 1001 où la mémoire du routeur est limitée et peut être épuisée en cas d'utilisation importante du plan de contrôle, comme une table BGP (Border Gateway Protocol) complète. Sur l'ASR 1001, 4 Go de DRAM sont installés, mais après le démarrage de tous les autres processeurs et processeurs Linux, Cisco IOS récupère les 1,1 Go restants. Une fois que la mémoire est épuisée au point qu'AAA ne peut plus allouer de mémoire pour l'UID, SSH ne fonctionne plus.

Considérez les données de mémoire de deux ASR :

<#root>

```
SSH Not Working:
----------------
ASR1#
```

show memory summary

```
                Head       Total(b)     Used(b)      Free(b)   Lowest(b)  Largest(b)
Processor  7FE150387010  1160982064  1146067400     14914664    14225352    13918620
lsmpi_io  7FE14FB7E1A8      6295128     6294304          824         824         412

SSH Working:
------------
ASR2#
```

show memory summary

```
                Head       Total(b)     Used(b)      Free(b)   Lowest(b)  Largest(b)
Processor  7FFB6ACB0010  1160982064  1120122056     40860008    29163912    24132068
lsmpi_io  7FFB6A4A71A8      6295128     6294304          824         824         412
```

D'après un calcul simple, sur l'ASR hors service, le pourcentage de mémoire libre est de 1,28 % (14914664 / 1160982064 * 100) de la mémoire totale disponible. Sur l'ASR de travail, il est de 3,51 % (40860008 / 1160982064 * 100), ce qui est juste au-dessus du seuil de mémoire faible d'authentification.

Ce problème est difficile à identifier, car le message %AAA-3-ACCT_LOW_MEM_UID_FAIL n'est souvent pas imprimé lorsque cette erreur se produit en raison d'une mémoire insuffisante. De plus, la façon dont AAA calcule le seuil de mémoire ne dépend pas de la quantité brute de mémoire processeur disponible sur le processeur de routage (RP), mais plutôt d'un pourcentage de la mémoire totale. Par conséquent, il peut y avoir encore apparemment beaucoup de mémoire de processeur affichée comme libre dans le résultat de la commande show memory summary quand cela se produit sans aucune défaillance de malloc rapportée.

> Remarque : L'ID de bogue Cisco CSCuj50368 a été classé afin de rendre les messages d'erreur SSH plus explicites sur la vraie raison de l'échec de l'authentification.

Une façon de vérifier si c'est bien le problème est de regarder les statistiques de la mémoire AAA :

<#root>

```
Router#
show aaa memory

  Allocator-Name                 In-use/Allocated            Count
--------------------------------------------------------------------------------
  AAA AttrL Hdr             :          0/65888      (  0%) [      0] Chunk
  AAA AttrL Sub             :          0/65888      (  0%) [      0] Chunk
  AAA DB Elt Chun           :        544/65888      (  0%) [      4] Chunk
  AAA Unique Id Hash Table  :       8196/8288       ( 98%) [      1]
  AAA chunk                 :          0/16936      (  0%) [      0] Chunk
  AAA chunk                 :          0/16936      (  0%) [      0] Chunk
  AAA Interface Struct      :       1600/1968       ( 81%) [      4]

Total allocated: 0.230 Mb, 236 Kb, 241792 bytes


AAA Low Memory Statistics:
__________________________
  Authentication low-memory threshold      : 3%
  Accounting low-memory threshold          : 2%


  AAA Unique ID Failure                    : 96
  Local server  Packet dropped             : 0
  CoA  Packet dropped                      : 0
  PoD  Packet dropped                      :
```

Si le compte « AAA Unique ID Failure » s'incrémente à chaque tentative SSH ayant échoué, le problème est causé par cette condition de mémoire insuffisante.

Afin de résoudre ce problème, des étapes de dépannage de mémoire ASR 1000 standard doivent être prises afin d'isoler la cause. Pour plus d'informations sur la façon de dépanner des problèmes de mémoire sur l'ASR, consultez Vue d'ensemble de l'utilisation de la mémoire.

Solution

Afin de résoudre ce problème, des étapes de dépannage de mémoire de routeur standard doivent être effectuées. Les étapes permettent de déterminer si le problème est dû à une utilisation normale, auquel cas une mise à niveau de la plate-forme/mémoire peut être justifiée ; ou d'une fuite de mémoire pour laquelle une surveillance et un dépannage supplémentaires de la mémoire peuvent s'avérer nécessaires. Voir Détecteur de fuite de mémoire et techniques courantes de dépannage de la mémoire pour plus de détails.

Pour les versions qui n'ont pas le correctif de l'ID de bogue Cisco CSCum19502 , la solution de contournement la plus évidente est d'activer l'accès Telnet ou console au routeur, puisque seul SSH est affecté par ce seuil.

> Conseil : La commande aaa memory threshold vous permet de réduire les valeurs de seuil à un minimum de 1 %. Cependant, bien que cela fournisse un moyen temporaire de SSH vers le routeur, cela peut entraîner d'autres implications telles que la possibilité que l'utilisation de la mémoire du processeur soit très faible avant que les administrateurs ne soient alertés. Cela peut entraîner le non-fonctionnement de processus plus importants, tels que le protocole BGP qui utilise de grandes quantités de mémoire. C'est donc une chose qui doit être utilisée avec prudence.

Comme expliqué précédemment, il est tout à fait plausible que le routeur ne fuit pas de mémoire, mais soit simplement surabonné pour les fonctionnalités activées. Dans ce cas, une mise à niveau de la plate-forme/mémoire peut être garantie.

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.