Échec de l'authentification SSH en raison de conditions de mémoire insuffisantes

Contenu

Introduction

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

> **Note**: 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, aucun débogage AAA (Authentication, Authorization, and Accounting) n'est imprimé pour indiquer que AAA est effectivement appelé et retourne l'échec.

```
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 présenté ici est également observé lors de la tentative de SSH, 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 première du problème est le manque de mémoire sur le routeur. Quand AAA ne parvient pas à allouer de la mémoire pour créer l'ID unique (UID) pour la session SSH entrante, il signale la même erreur qu'une erreur d'authentification AAA même si AAA n'est pas tenté. Cette condition se produit lorsque la mémoire libre du processeur tombe en dessous du seuil de mémoire faible de l'authentification AAA, qui par défaut est défini à 3% de la mémoire totale et peut être vérifiée avec la commande **show aaa memory**. Ce problème est souvent observé sur une plate-forme ASR (Aggregation Services Router) 1001 où il y a une mémoire limitée sur le routeur qui peut être épuisée avec une utilisation intensive du plan de contrôle, comme une table BGP (Border Gateway Protocol) complète. Sur l'ASR 1001, 4 Go de DRAM sont installés, mais après que tous les autres processeurs et processeurs Linux démarrent, Cisco IOS obtient le 1,1 Go restant. Une fois la mémoire épuisée au point que AAA ne peut plus allouer de mémoire pour UID, SSH ne fonctionne plus.

Considérez les données de mémoire de deux ASR :

```
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
```

Àpartir d'un calcul simple, sur le ASR non fonctionnel, 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), qui est juste au-dessus du seuil de faible mémoire 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 condition de mémoire insuffisante. De plus, la manière 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 toujours y avoir une quantité suffisante de mémoire du processeur affichée comme libre dans la sortie de **la commande show memory summary** lorsque cela se produit sans défaillance de malloc signalée.

> **Note**: L'ID de bogue Cisco CSCuj50368 a été enregistré afin de rendre les messages d'erreur SSH plus explicites sur la véritable raison de l'échec de l'authentification.

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

```
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 nombre d'échecs d'ID unique AAA s'incrémente avec chaque échec de tentative SSH, 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 résolution 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 standard de dépannage de la mémoire du routeur doivent être prises. Les étapes permettent de déterminer si le problème est dû à une utilisation normale, auquel cas une mise à niveau de la plate-forme/de la mémoire peut être justifiée ; ou une fuite de mémoire où une surveillance et un dépannage supplémentaires de la mémoire peuvent être nécessaires. Pour plus d'informations, consultez Memory Leak Detector et les techniques courantes de dépannage de la mémoire.

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

> **Astuce** : 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 au routeur, cela peut entraîner d'autres conséquences, comme la réduction de l'utilisation de la mémoire du processeur à un niveau très bas avant que les administrateurs ne soient avertis. Cela pourrait entraîner la fin du fonctionnement de processus plus importants, tels que BGP qui consomme une grande quantité de mémoire. C'est pourquoi il convient de l'utiliser avec prudence.

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