Échec d'authentification de SSH dû aux états de taille mémoire basse

Contenu

[Introduction](#)
[Problème](#)
[Solution](#)

Introduction

Ce document décrit la question sur un routeur de Cisco IOS® quand le Protocole Secure Shell (SSH) au routeur échoue parfois avec une panne signalée d'authentification de l'utilisateur dans le SSH met au point. Cette question se produit quoique les identifiants utilisateurs écrits soient corrects et les mêmes qualifications fonctionnent correctement pour le telnet.

> Remarque: L'ID de bogue Cisco CSCum19502 a été classé afin de faire le comportement entre le SSH et le telnet cohérents.

Problème

L'avis dans ces derniers met au point que quoique le « debug aaa authentication » soit activé, il n'y a aucun Authentification, autorisation et comptabilité (AAA) met au point être imprimé au show aaa est appelé réellement et renvoie la panne.

```
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 quand le SSH est tenté, mais il n'obtient pas imprimé uniformément :

```
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,
```

L'origine du problème est des états de taille mémoire basse sur le routeur. Quand l'AAA n'alloue pas la mémoire pour créer l'identificateur unique (UID) pour la session entrante de SSH, elle signale la même panne qu'un échec d'authentification d'AAA quoique l'AAA ne soit pas tenté. Cette condition se produit quand la mémoire disponible de processeur tombe au-dessous de l'AAA « seuil de low-memory d'authentification », qui par défaut est placée à 3% de toute la mémoire et peut être vérifiée avec la commande de **mémoire de show aaa**. Ce problème est souvent vu sur une plate-forme 1001 du routeur de services d'agrégation (ASR) où il y a mémoire limitée sur le routeur qui peut être épuisé avec l'utilisation lourde d'avion de contrôle, telle qu'une pleine table de Protocole BGP (Border Gateway Protocol). Sur l'ASR 1001 il y a de 4GB de mémoire vive dynamique installés, mais le démarrage après tous les autres processeurs de CPU et de Linux Cisco IOS obtient le 1.1 Go laissé plus de. Une fois que la mémoire est épuisée au point que l'AAA peut plus n'allouer la mémoire pour l'UID, le SSH ne fonctionne pas.

Considérez ces 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
```

D'un calcul simple, sur l'ASR non-travaillant le pourcentage de la mémoire disponible est 1.28% (14914664/1160982064 * 100) de la mémoire disponible totale. Sur l'ASR fonctionnant il est 3.51% (40860008/1160982064 * 100), qui est juste au-dessus du seuil de low-memory d'authentification.

Il est difficile l'identifier ce problème parce que le message %AAA-3-ACCT_LOW_MEM_UID_FAIL souvent n'obtient pas imprimé quand cette erreur se produit en raison de l'état de taille mémoire basse. D'ailleurs, la manière que l'AAA calcule le seuil de mémoire ne dépend pas de la quantité crue de mémoire du processeur disponible sur le processeur d'artère (RP), mais plutôt d'un

pourcentage de toute la mémoire. Par conséquent, il pourrait encore y avoir apparemment d'abondance de mémoire du processeur affichée comme libre dans la **sortie de commande récapitulative de show memory** quand ceci se produit sans des défaillances d'allocation mémoire signalées.

> Remarque: L'ID de bogue Cisco **CSCuj50368** a été classé afin de rendre des messages d'erreur de SSH plus explicites au sujet du motif réel pour l'échec d'authentification.

Une manière à de vérifier si c'est en effet le problème est de regarder les statistiques de mémoire d'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 compte « de panne d'identificateur unique d'AAA » incrémente avec chaque tentative défectueuse de SSH, le problème est provoqué par par cet état de taille mémoire basse.

Afin de dépanner cette question, les étapes de dépannage standard de la mémoire ASR 1000 devraient être commande rentrée pour isoler la cause. Pour plus d'informations sur la façon dépanner des questions de mémoire sur l'ASR, voir l'aperçu d'utilisation de mémoire.

Solution

Afin de dépanner cette question, des étapes de dépannage standard de mémoire de routeur devraient être prises. L'isolat d'étapes si le problème est dû à l'utilisation normale, dans ce cas une mise à jour de plate-forme/mémoire pourrait être justifiée ; ou une fuite de mémoire où la surveillance et le dépannage supplémentaires de mémoire pourraient être exigés. Voir le Memory Leak Detector et les techniques de dépannage communes de mémoire pour plus de détails.

Pour les versions qui n'ont pas la difficulté de l'ID de bogue Cisco CSCum19502, le contournement le plus évident est d'activer le telnet ou l'accès de console au routeur, puisque seulement le SSH est affecté par ce seuil.

Conseil : La commande de **seuil de mémoire d'AAA** te permet pour ramener les valeurs seuil à un minimum de 1%. Cependant, alors que ceci fournit une manière provisoire au SSH au routeur, il peut mener à d'autres implications telles que l'indemnité d'utilisation de mémoire du processeur pour relâcher vraiment bas avant que des admins soient alertés. Ceci pourrait faire pour ne fonctionner plus des processus plus importants, tels que le BGP qui épuise un grand nombre de mémoire. Par conséquent c'est quelque chose qui devrait être utilisé avec prudence.

Comme expliqué plus tôt, il est complètement plausible que le routeur ne coule pas la mémoire mais est simplement oversubscribed pour les caractéristiques activées. Dans ce cas une mise à jour de plate-forme/mémoire pourrait être justifiée.