Fallo de autenticación SSH debido a condiciones de memoria bajas

Contenido

Introducción

Este documento describe el problema en un router Cisco IOS® cuando Secure Shell (SSH) al router a veces falla con una falla de autenticación de usuario informada en las depuraciones SSH. Este problema ocurre aunque las credenciales de usuario introducidas sean correctas y las mismas credenciales funcionen correctamente para Telnet.

> **Nota:** Se ha registrado el ID de bug Cisco CSCum19502 para hacer que el comportamiento entre SSH y Telnet sea consistente.

Problema

Tenga en cuenta en estas depuraciones que, aunque "debug aaa authentication" esté habilitada, no se están imprimiendo depuraciones de autenticación, autorización y contabilidad (AAA) para mostrar que se invoca AAA realmente y devuelve la falla.

```
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,
```

A veces el syslog mostrado aquí también se observa cuando se intenta SSH, pero no se imprime consistentemente:

```
*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 causa raíz del problema son las condiciones de memoria baja en el router. Cuando AAA no puede asignar memoria para crear el ID único (UID) para la sesión SSH entrante, informa del mismo error que una falla de autenticación AAA aunque no se intente AAA. Esta condición ocurre cuando la memoria libre del procesador cae por debajo del "umbral de memoria baja de autenticación" AAA, que de forma predeterminada se establece en 3% de la memoria total y se puede verificar con el comando **show aaa memory**. Este problema se observa a menudo en una plataforma 1001 de router de servicios de agregación (ASR) donde hay memoria limitada en el router que se puede agotar con un uso intensivo del plano de control, como una tabla completa de protocolo de gateway fronterizo (BGP). En el ASR 1001 hay 4 GB de DRAM instalada, pero después de que todas las otras CPU y los procesadores Linux arranquen, Cisco IOS obtiene 1,1 GB restante. Una vez que se agota la memoria hasta el punto de que AAA ya no puede asignar memoria para UID, SSH no funciona.

Considere estos datos de memoria de dos 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
```

A partir de un simple cálculo, en el ASR que no funciona, el porcentaje de memoria libre es del 1,28% (14914664 / 1160982064 * 100) de la memoria disponible total. En el ASR en funcionamiento es del 3,51% (40860008 / 1160982064 * 100), que está justo por encima del umbral de memoria baja de autenticación.

Este problema es difícil de identificar porque el mensaje %AAA-3-ACCT_LOW_MEM_UID_FAIL a menudo no se imprime cuando se produce este error debido a la condición de memoria baja. Además, la forma en que AAA calcula el umbral de memoria no depende de la cantidad de memoria sin procesar disponible en el procesador de routing (RP), sino más bien de un porcentaje de la memoria total. Por lo tanto, parece que todavía puede haber mucha memoria del procesador mostrada como libre en el resultado del **comando show memory summary** cuando esto ocurre sin que se notifiquen fallas malloc.

> **Nota:** Se ha registrado el ID de bug Cisco CSCuj50368 para hacer que los mensajes de error SSH sean más explícitos sobre la verdadera razón de la falla de autenticación.

Una manera de verificar si este es realmente el problema es ver las estadísticas de memoria 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 el conteo "Falla de ID única AAA" aumenta con cada intento fallido de SSH, el problema es causado por esta condición de memoria baja.

Para resolver este problema, se deben tomar los pasos estándar de troubleshooting de la memoria ASR 1000 para aislar la causa. Para obtener más información sobre cómo resolver problemas de memoria en el ASR, vea Descripción General del Uso de la Memoria.

Solución

Para resolver este problema, se deben tomar los pasos estándar de troubleshooting de la memoria del router. Los pasos aíslan si el problema se debe al uso normal, en cuyo caso se podría justificar una actualización de la plataforma/memoria; o una pérdida de memoria en la que se requiera supervisión adicional de memoria y resolución de problemas. Consulte Detector de fugas de memoria y técnicas comunes de resolución de problemas de memoria para obtener más detalles.

Para las versiones que no tienen la corrección del Id. de error de Cisco CSCum19502 , la solución alternativa más obvia es habilitar el acceso Telnet o de la consola al router, ya que sólo SSH se ve afectado por este umbral.

> **Consejo:** El comando **aaa memory threshold** le permite reducir los valores de umbral a un mínimo de 1%. Sin embargo, mientras esto proporciona una manera temporal de SSH al router, puede llevar a otras implicaciones como la asignación de utilización de la memoria del procesador para caer realmente bajo antes de que los administradores sean alertados. Esto podría hacer que los procesos más importantes, como BGP que utiliza grandes cantidades de memoria, dejen de funcionar. Por lo tanto, esto es algo que debería usarse con precaución.

Como se ha explicado anteriormente, es completamente verosímil que el router no pierda memoria sino que simplemente esté sobresuscrito para las funciones habilitadas. En este caso, puede estar justificada una actualización de la plataforma/memoria.