

Falla debido de la autenticación SSH a las condiciones de memoria baja

Contenido

[Introducción](#)

[Problema](#)

[Solución](#)

Introducción

Este documento describe el problema en un router del [®] del Cisco IOS cuando el Secure Shell (SSH) al router falla a veces con un error señalado de la autenticación de usuario en los debugs de SSH. Este problema ocurre aunque los credenciales de usuario ingresados están correctos y las mismas credenciales trabajan correctamente para el telnet.

Nota: El Id. de bug Cisco [CSCum19502](#) se ha clasificado para hacer el comportamiento entre SSH y Telnet constantes.

Problema

El aviso en éstos los debugs que aunque “se habilita la autenticación aaa del debug”, no hay debugs del Authentication, Authorization, and Accounting (AAA) que son impresos para mostrar el AAA se invoca y vuelve realmente el error.

```
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,
```

El Syslog mostrado aquí también se observa a veces cuando se intenta SSH, pero no consigue impreso constantemente:

```

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,

```

La causa raíz del problema es condiciones de memoria baja en el router. Cuando el AAA no puede afectar un aparato la memoria para crear el ID único (UID) para la sesión SSH entrante, señala el mismo error que un error de la autenticación AAA aunque el AAA no se intenta. Esta condición ocurre cuando memoria libre del procesador baja debajo del AAA “umbral de memoria baja de la autenticación”, que por abandono se fija hasta el 3% de memoria total y se puede marcar con el **comando memory aaa de la demostración**. Este problema se considera a menudo en una plataforma 1001 del router de los servicios de la agregación (ASR) donde hay memoria limitada en el router que puede ser agotado con el uso pesado del avión del control, tal como una tabla llena del Border Gateway Protocol (BGP). En el ASR 1001 hay 4GB del DRAM instalados, pero después el inicio de todos los otros procesadores CPU y de Linux Cisco IOS consigue los 1.1 GB dejados encima. Una vez que la memoria se agota a la punta que el AAA puede afectar un aparato no más la memoria para el UID, SSH no puede trabajar.

Considere estos datos de la memoria a partir 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 |

De un simple cálculo, en el ASR festivo el porcentaje de memoria libre es 1.28% (14914664/1160982064 * 100) de memoria disponible total. En el ASR de trabajo es 3.51% (40860008/1160982064 * 100), que está apenas sobre el umbral de memoria baja de la autenticación.

Este problema es difícil de identificar porque el mensaje %AAA-3-ACCT_LOW_MEM_UID_FAIL no consigue a menudo impreso cuando ocurre este error debido a la condición de memoria baja. Por otra parte, la manera que el AAA calcula el umbral de la memoria no depende de la cantidad sin procesar de memoria del procesador disponible en el (RP) del Route Processor, sino bastante

de un porcentaje de memoria total. Por lo tanto, pudo todavía haber aparentemente un montón de memoria del procesador mostrado según lo libremente en el **comando show memory summary** hecho salir cuando éste ocurre sin las fallas Malloc señaladas.

Nota: El Id. de bug Cisco [CSCuj50368](#) se ha clasificado para hacer los mensajes de error de SSH más explícitos sobre el motivo real para la falla de autenticación.

Una manera a de verificar si éste es de hecho el problema es mirar las estadísticas de la 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 “la cuenta del error del ID único AAA” incrementa con cada tentativa fallada de SSH, el problema es causado por esta condición de memoria baja.

Para resolver problemas este problema, los pasos de Troubleshooting estándar de la memoria ASR 1000 deben ser orden admitida para aislar la causa. Para más información sobre cómo resolver problemas los problemas de la memoria en el ASR, vea la [descripción del uso de la memoria](#).

Solución

Para resolver problemas este problema, los pasos de Troubleshooting estándar de memoria del router deben ser tomados. El aislante de los pasos si el problema es debido a la utilización normal, en este caso una plataforma/una actualización de memoria pudo ser autorizada; o una fuga de memoria donde la supervisión y el troubleshooting adicionales de la memoria pudieron ser requeridos. Vea el [detector de fuga de memoria](#) y las [técnicas de Troubleshooting](#) comunes de la [memoria](#) para más detalles.

Para las versiones que no tienen el arreglo del Id. de bug Cisco [CSCum19502](#), la solución alternativa más obvia es habilitar Telnet o el acceso a la consola al router, puesto que solamente SSH es afectado por este umbral.

Consejo: [El comando threshold de la memoria aaa](#) permite que usted reduzca los valores de umbral a un mínimo del 1%. Sin embargo, mientras que éste proporciona una manera temporal a SSH al router, puede llevar a otras implicaciones tales como el permiso de utilización de memoria del procesador para caer realmente bajo antes de que se alerten los admins. Esto pudo hacer procesos más importantes, tales como BGP que utiliza encima de una gran cantidad de memoria, para trabajar no más. Por lo tanto éste es algo que se debe utilizar con cautela.

Según lo explicado anterior, es totalmente plausible que el router no se escapa la memoria pero es apenas oversubscribed para las características habilitadas. En este caso una plataforma/una actualización de memoria pudo ser autorizada.