Contents

Introduction

This document describes the issue on a Cisco IOS® router when Secure Shell (SSH) to the router sometimes fails with a reported user authentication failure in the SSH debugs. This issue occurs even though the user credentials entered are correct and the same credentials work correctly for Telnet.

> **Note**: Cisco bug ID CSCum19502 has been filed in order to make the behavior between SSH and Telnet consistent.

Problem

Notice in these debugs that even though "debug aaa authentication" is enabled, there are no Authentication, Authorization, and Accounting (AAA) debugs being printed to show AAA actually is invoked and returns the failure.

```
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,
```

Sometimes the syslog shown here is also observed when SSH is attempted, but it does not get printed consistently:

```
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,
```

The root cause of the problem is low memory conditions on the router. When AAA fails to allocate memory to create the Unique ID (UID) for the incoming SSH session, it reports the same failure as an AAA authentication failure even though AAA is not attempted. This condition occurs when the processor free memory falls below the AAA "Authentication low-memory threshold", which by default is set to 3% of the total memory and can be checked with the **show aaa memory** command. This problem is often seen on an Aggregation Services Router (ASR) 1001 platform where there is limited memory on the router that can be exhausted with heavy control plane usage, such as a full Border Gateway Protocol (BGP) table. On the ASR 1001 there is 4GB of DRAM installed, but after all of the other CPUs and Linux processors boot Cisco IOS gets the 1.1 GB left over. Once the memory is exhausted to the point that AAA can no longer allocate memory for UID, SSH fails to work.

Consider this memory data from two ASRs:

```
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
```

From a simple calculation, on the nonworking ASR the percentage of free memory is 1.28% (14914664 / 1160982064 * 100) of total available memory. On the working ASR it is 3.51% (40860008 / 1160982064 * 100), which is just above the authentication low-memory threshold.

This problem is difficult to identify because the %AAA-3-ACCT_LOW_MEM_UID_FAIL message often does not get printed when this error occurs due to the low memory condition. Moreover, the way that AAA calculates memory threshold does not depend on the raw amount of processor memory available on the route processor (RP), but rather a percentage of the total memory. Therefore, there might still be seemingly plenty of processor memory shown as free in the **show memory summary command** output when this occurs with no malloc failures reported.

> **Note**: Cisco bug ID **CSCuj50368** has been filed in order to make SSH error messages more explicit about the real reason for the authentication failure.

One way to to verify if this is indeed the problem is to look at the AAA memory statistics:

```
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 :
```

If the "AAA Unique ID Failure" count increments with each failed SSH attempt, the problem is caused by this low memory condition.

In order to troubleshoot this issue, standard ASR 1000 memory troubleshooting steps should be taken in order to isolate the cause. For more information on how to troubleshoot memory issues on the ASR, see Memory Usage Overview.

Solution

In order to troubleshoot this issue, standard router memory troubleshooting steps should be taken. The steps isolate whether the problem is due to normal usage, in which case a platform/memory upgrade might be warranted; or a memory leak where additional memory monitoring and troubleshooting might be required. See Memory Leak Detector and common memory troubleshooting techniques for more details.

For versions that do not have the fix from Cisco bug ID CSCum19502 , the most obvious workaround is to enable Telnet or console access to the router, since only SSH is affected by this threshold.

> **Tip**: The **aaa memory threshold** command allows you to reduce the threshold values to a minimum of 1%. However, while this provides a temporary way to SSH to the router, it can lead to other implications such as the allowance of processor memory utilization to drop really low before admins are alerted. This might cause more important processes, such as BGP that uses up large amounts of memory, to no longer work. Hence this is something that should be used with caution.

As explained earlier, it is completely plausible that the router does not leak memory but is just oversubscribed for the features enabled. In this case a platform/memory upgrade might be warranted.