

内存不足导致SSH身份验证失败

目录

[简介](#)

[问题](#)

[解决方案](#)

简介

本文档描述Cisco IOS®路由器上的问题，当SSH调试中报告的用户身份验证失败时，路由器的安全外壳(SSH)有时会失败。即使输入的用户凭证正确且相同的凭证对Telnet工作正常，也会发生此问题。

注意：为了使SSH和Telnet之间的行为一致，已提交Cisco Bug ID [CSCum19502](#)。

问题

请注意，在这些调试中，即使启用了“debug aaa authentication”，也没有打印身份验证、授权和记帐(AAA)调试，以显示AAA实际被调用并返回故障。

```
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,
```

有时，尝试SSH时也会观察此处显示的系统日志，但它不会一致打印：

```
*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
```

问题的根本原因是路由器内存不足。当AAA无法分配内存为传入SSH会话创建唯一ID(UID)时，它报告与AAA身份验证失败相同的故障，即使未尝试AAA。当处理器可用内存低于AAA“Authentication

low-memory threshold”（身份验证低内存阈值）时，会发生此情况，该阈值默认设置为总内存的3%，并可使用**show aaa memory**命令进行检查。此问题在聚合服务路由器(ASR)1001平台上经常出现，在该平台上，路由器内存有限，可以通过使用重量控制平面(如全边界网关协议(BGP)表)来耗尽。在ASR 1001上安装了4GB的DRAM，但在所有其他CPU和Linux处理器启动后，Cisco IOS将剩余1.1GB的内存。一旦内存耗尽，AAA无法再为UID分配内存，SSH就无法工作。

考虑两个ASR的此内存数据：

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
```

根据简单计算，在非工作ASR上，可用内存的百分比为总可用内存的1.28%(14914664 / 1160982064 * 100)。在工作ASR上，该值为3.51%(40860008 / 1160982064 * 100)，仅略高于身份验证低内存阈值。

此问题难以识别，因为当由于内存不足而出现此错误时，通常不会打印%AAA-3-ACCT_LOW_MEM_UID_FAIL消息。此外，AAA计算内存阈值的方式不取决于路由处理器(RP)上可用的处理器内存的原始量，而取决于总内存的百分比。因此，如果发生此情况时未报告malloc故障，则show memory summary命令输出中似乎仍会显示大量可用的处理器内存。

注意：为了使SSH错误消息更明确地说明身份验证失败的真实原因，已提交Cisco Bug ID CSCuj50368。

验证这是否确实是问题的一种方法是查看AAA内存统计信息：

```
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 :
```

如果“AAA唯一ID失败”计数随着每次SSH尝试失败而增加，则问题是由此内存不足导致的。

要排除此问题，应执行标准ASR 1000内存故障排除步骤以查明原因。有关如何对ASR上的内存问题进行故障排除的详细信息，请参阅[内存使用概述](#)。

解决方案

要排除此问题，应执行标准路由器内存故障排除步骤。这些步骤将查明问题是否是由于正常使用所致，在这种情况下，可能需要保证平台/内存升级；或内存泄漏，可能需要额外的内存监控和故障排除。有关[详细信息](#)，请参阅[内存泄漏检测](#)器和常见内存故障排除技术。

对于没有Cisco Bug ID [CSCum19502](#)（仅限注册用户）修复的版本，最明显的解决方法是启用对路由器的Telnet或控制台访问，因为只有SSH受此阈值影响。

提示：使用[aaa memory threshold](#)命令可将阈值降至最低1%。但是，虽然这提供了对路由器进行SSH的临时方法，但它可能会导致其他影响，例如在向管理员发出警报之前处理器内存利用率允许极低。这可能导致更重要的进程（如耗用大量内存的BGP）不再工作。因此，应谨慎使用。

如前所述，路由器不泄漏内存，而只是超订用了启用的功能，这完全可信。在这种情况下，可能需要升级平台/内存。