由于内存不足而导致SSH身份验证失败

目录

[简介](#)

[问题](#)

[解决方案](#)

简介

本文档介绍Cisco IOS®路由器上的问题，当Secure Shell(SSH)连接到路由器时有时会因在SSH调试中报告的用户身份验证失败而发生故障。即使输入的用户凭证正确，并且相同的凭证能对Telnet正常工作，也会出现此问题。

注意：为了使SSH和Telnet之间的行为保持一致，已归档了Cisco Bug ID CSCum19502。

问题

请注意，在这些调试中，即使启用了“debug aaa authentication”，也不会打印身份验证、授权和记帐(AAA)调试，以显示实际调用了AAA并返回了故障。

<#root>

```
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，在尝试使用SSH时也会看到此处显示的syslog，但它不会始终如一地被打印：

```
*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的内存不足。当AAA无法分配内存以为传入SSH会话创建唯一ID(UID)时，即使未尝试AAA，也会报告与AAA身份验证失败相同的故障。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，会出现此情况，默认情况下，该阈值设置为总内存的3%，可以使用show aaa memory命令进行检查。此问题通常出现在汇聚服务路由器(ASR)1001平台上，在该平台上，路由器上的内存有限，如果大量使用控制平面（如完全边界网关协议[BGP]表），内存可能会耗尽。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会剩余1.1 GB。一旦内存耗尽，AAA不能再为UID分配内存，SSH将无法工作。

考虑来自两个ASR的以下内存数据：

<#root>

```
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上为3.51%(40860008 / 1160982064 * 100)，刚好高于身份验证低内存阈值。

此问题很难识别，因为当由于内存不足而发生此错误时，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依赖于路由处理器(RP)上可用的处理器内存的原始量，而是依赖于总内存的百分比。因此，如果出现这种情况，并且未报告malloc故障，则在show memory summary命令输出中似乎仍有大量处理器内存显示为可用内存。

> 注意：Cisco Bug ID CSCuj50368已归档以便使SSH错误消息更加明确地显示身份验证失败的真实原因。

要验证这是否确实有问题，一种方法是查看AAA内存统计信息：

<#root>

```
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 Unique ID Failure”计数随着每次失败的SSH尝试而增加，则问题是由内存不足情况引起的。

为了对此问题进行故障排除，应采取标准的ASR 1000内存故障排除步骤以查明原因。有关如何排除ASR上的内存问题的详细信息，请参阅内存使用率概述。

解决方案

要解决此问题，应采取标准的路由器内存故障排除步骤。这些步骤可确定问题是否由正常使用引起，在这种情况下，可能需要进行平台/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和常见内存故障排除技术。

对于没有Cisco Bug ID CSCum19502的修复程序的版本，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：aaa memory threshold命令允许您将阈值至少降低到1%。但是，虽然这提供了到路由器的SSH临时方法，但可能会导致其他问题，例如允许处理器内存使用率在管理员收到警报之前降低非常低。这可能会导致更重要的进程（例如消耗大量内存的BGP）不再工作。因此，应谨慎使用此功能。

如前所述，路由器不会泄漏内存，只是对启用的功能超订用是完全合理的。在这种情况下，可能需要进行平台/内存升级。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。