

# SSH-Authentifizierungsfehler aufgrund von Bedingungen für niedrigen Arbeitsspeicher

## Inhalt

[Einführung](#)

[Problem](#)

[Lösung](#)

## Einführung

In diesem Dokument wird das Problem bei einem Cisco IOS<sup>®</sup>-Router beschrieben, wenn Secure Shell (SSH) zum Router bei einem gemeldeten Fehler bei der Benutzerauthentifizierung im SSH-Debugger ausfällt. Dieses Problem tritt auf, obwohl die eingegebenen Benutzeranmeldeinformationen korrekt sind und dieselben Anmeldeinformationen für Telnet korrekt funktionieren.

**Hinweis:** Die Cisco Bug-ID [CSCum19502](#) wurde gespeichert, um das Verhalten zwischen SSH und Telnet konsistent zu machen.

## Problem

Beachten Sie in diesen Debuggen, dass, obwohl "debug aa authentication" aktiviert ist, keine Debug-Debugger für Authentifizierung, Autorisierung und Abrechnung (AAA) ausgegeben werden, um anzuzeigen, dass AAA tatsächlich aufgerufen wird und den Fehler zurückgibt.

```
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,
```

Manchmal wird das hier abgebildete Syslog auch beobachtet, wenn SSH versucht wird, aber es

wird nicht konsistent gedruckt:

```
*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
```

Die Ursache des Problems sind die niedrigen Speicherbedingungen auf dem Router. Wenn AAA keinen Speicher zuweist, um die eindeutige ID (UID) für die eingehende SSH-Sitzung zu erstellen, meldet sie denselben Fehler wie ein AAA-Authentifizierungsfehler, obwohl AAA nicht versucht wird. Diese Bedingung tritt ein, wenn der freie Speicher des Prozessors unter den AAA-Grenzwert für "Authentication Low Memory" (Authentifizierung niedriger Speicher) fällt, der standardmäßig auf 3 % des gesamten Speichers festgelegt ist und mit dem Befehl **show aa memory** überprüft werden kann. Dieses Problem tritt häufig bei einer Aggregation Services Router (ASR) 1001-Plattform auf, bei der der Router nur über einen begrenzten Speicher verfügt, der bei starker Nutzung der Kontrollebene ausgeschöpft werden kann, z. B. eine vollständige Border Gateway Protocol (BGP)-Tabelle. Auf dem ASR 1001 sind 4 GB DRAM installiert, aber nachdem alle anderen CPUs und Linux-Prozessoren booten, erhält das Cisco IOS die 1,1 GB übrig. Nachdem der Speicher so weit ausgeschöpft ist, dass AAA keinen Speicher mehr für UID zuweisen kann, funktioniert SSH nicht mehr.

Beachten Sie die Speicherdaten von zwei 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
```

Aus einer einfachen Berechnung, auf der nicht funktionierenden ASR ist der Prozentsatz des freien Arbeitsspeichers 1,28% ( $14914664 / 1160982064 * 100$ ) des gesamten verfügbaren Arbeitsspeichers. Auf dem funktionierenden ASR liegt dieser Wert bei 3,51 % ( $40860008 / 1160982064 * 100$ ), der knapp über dem Schwellenwert für die Authentifizierung bei geringem Speicher liegt.

Dieses Problem ist schwer zu identifizieren, da die Meldung %AAA-3-ACCT\_LOW\_MEM\_UID\_FAIL häufig nicht gedruckt wird, wenn dieser Fehler aufgrund des niedrigen Speicherzustands auftritt. Darüber hinaus hängt die AAA-Berechnung der Speicherschwelle nicht von der Rohspeicherkapazität des Routingprozessors (RP) ab, sondern von einem Prozentsatz des Gesamtspeichers. Daher ist es möglich, dass in der Ausgabe des Befehls **show memory summary** immer noch genügend Prozessorspeicher verfügbar ist, wenn keine Malloc-Fehler gemeldet werden.

**Hinweis:** Die Cisco Bug-ID [CSCuj50368](#) wurde gespeichert, um SSH-Fehlermeldungen expliziter auf den wahren Grund für den Authentifizierungsfehler hinzuweisen.

Eine Möglichkeit, zu überprüfen, ob dies tatsächlich das Problem ist, sind die AAA-Speicherstatistiken:

```
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 :
```

Wenn die Anzahl "AAA Unique ID Failure" bei jedem fehlgeschlagenen SSH-Versuch zunimmt, wird das Problem durch diesen niedrigen Speicherzustand verursacht.

Um dieses Problem zu beheben, sollten Sie die standardmäßige ASR 1000-Speicherfehlerbehebung durchführen, um die Ursache zu isolieren. Weitere Informationen zur Behebung von Speicherproblemen im ASR finden Sie unter [Übersicht über die Speicherauslastung](#).

## Lösung

Um dieses Problem zu beheben, müssen die Schritte zur Fehlerbehebung für den Standardspeicher des Routers ausgeführt werden. Bei den Schritten wird isoliert, ob das Problem auf die normale Nutzung zurückzuführen ist. In diesem Fall kann ein Plattform-/Speicher-Upgrade erforderlich sein, oder Speicherlecks, bei denen zusätzliche Speicherüberwachung und Fehlerbehebung erforderlich sein können. Weitere Informationen finden Sie unter [Speicherverlusterkennung](#) und häufige [Verfahren](#) zur [Speicherfehlerbehebung](#).

Bei Versionen, die nicht mit der Behebung der Fehler-ID [CSCum19502 von](#) Cisco beheben, besteht die offensichtlichste Problemumgehung darin, den Telnet- oder Konsolenzugriff auf den Router zu aktivieren, da nur SSH von diesem Grenzwert betroffen ist.

**Tipp:** Mit dem Befehl [aaa memory threshold](#) können Sie die Schwellenwerte auf mindestens 1% reduzieren. Dies stellt zwar eine temporäre Möglichkeit zum SSH-Zugriff auf den Router dar, kann jedoch zu anderen Auswirkungen führen, wie z. B. zu einer Verringerung der Speicherauslastung des Prozessors, bevor Administratoren informiert werden. Dies kann dazu führen, dass wichtigere Prozesse, wie BGP, die große Mengen an Arbeitsspeicher beansprucht, nicht mehr funktionieren. Daher ist dies etwas, das mit Vorsicht angewendet werden sollte.

Wie bereits erläutert, ist es durchaus plausibel, dass der Router nicht den Speicher verlässt,

sondern nur für die aktivierten Funktionen überbelegt ist. In diesem Fall kann ein Plattform-/Speicherupgrade erforderlich sein.