

SSH-verificatiestoornis vanwege lage geheugencondities

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

Inleiding

Dit document beschrijft de kwestie op een Cisco IOS[®] router wanneer Secure Shell (SSH) naar de router soms mislukt met een gemelde storing in de SSH-apparaten voor gebruikersverificatie. Dit probleem doet zich voor zelfs al zijn de ingevoerde gebruikersreferenties correct en de zelfde geloofsbrieven werken correct voor Telnet.

Opmerking: Cisco bug-ID [CSCum19502](#) is ingediend om het gedrag tussen SSH en telnet consistent te maken.

Probleem

Merk op dat, ook al is "debug a Authentication" ingeschakeld, er geen detectie-, autorisatie- en accounting (AAA)-debugs worden afgedrukt om AAA daadwerkelijk te laten zien en de mislukking terug te geven.

```
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,
```

Soms wordt ook de hier getoonde syslog waargenomen wanneer SSH wordt geprobeerd, maar deze wordt niet consequent afgedrukt:

```
*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
```

De oorzaak van het probleem is lage geheugenomstandigheden op de router. Wanneer AAA er niet in slaagt het geheugen toe te wijzen om de unieke ID (UID) voor de inkomende SSH-sessie te maken, rapporteert het dezelfde fout als een AAA-echtheidsstoring, ook al wordt AAA niet geprobeerd. Deze conditie doet zich voor wanneer het processorvrije geheugen onder de AAA "Verificatie met laag geheugen" valt, die standaard is ingesteld op 3% van het totale geheugen en kan worden gecontroleerd met de opdracht **weergeven**. Dit probleem wordt vaak gezien op een platform van Aggregation Services Router (ASR) 1001 waar er beperkt geheugen op de router is die met zwaar controlevliegtuig kan worden uitgeput, zoals een tabel met Full Border Gateway Protocol (BGP). Op de ASR 1001 is 4 GB DRAM geïnstalleerd, maar na alle andere CPU's en Linux-processors is Cisco IOS overgebleven van 1,1 GB. Zodra het geheugen is uitgeput tot het punt dat AAA geheugen niet langer kan toewijzen voor UID, werkt SSH niet meer.

Beschouw deze geheugengegevens van twee ASR's:

```
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  
lsmapi_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  
lsmapi_io 7FFB6A4A71A8 6295128 6294304 824 824 412
```

Uit een simpele berekening blijkt dat het percentage vrij geheugen voor de niet-werkende ASR 1,28% ($14914664 / 1160982064 * 100$) van het totale beschikbare geheugen is. Voor de werkende ASR is het 3,51% ($40860008 / 1160982064 * 100$), wat net boven de authenticatiedrempel met weinig geheugen ligt.

Dit probleem is moeilijk te identificeren omdat het bericht %AAA-3-ACCT_LOW_MEM_UID_FAIL vaak niet wordt afgedrukt als deze fout veroorzaakt door de geheugenstoornis. Bovendien is de manier waarop AAA de geheugendrempel berekent niet afhankelijk van de hoeveelheid geheugen van de processor die beschikbaar is bij de routeprocessor (RP), maar eerder van een percentage van het totale geheugen. Daarom is er mogelijk nog steeds een overvloed aan processorgeheugen dat gratis wordt weergegeven in de output van de **samenvatting van het geheugen** van de **show** wanneer dit gebeurt zonder gemelde malloc-fouten.

Opmerking: Cisco bug-ID [CSCuj50368](#) is gedeponereerd om SSH-foutmeldingen explicieter te maken over de werkelijke reden voor de echtheidsfout.

Eén manier om te controleren of dit inderdaad het probleem is, is door te kijken naar de AAA-geheugenstatistieken:

```
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 :
```

Als bij elke mislukte SSH-poging de toename van "AAA unieke ID-fout" is geregistreerd, wordt het probleem veroorzaakt door deze geheugenstoornis.

Om dit probleem op te lossen, moet de standaard ASR 1000 stappen voor het oplossen van problemen worden genomen om de oorzaak te isoleren. Zie [Geheugenoverzicht](#) voor meer informatie over het [oplossen](#) van [geheugenproblemen](#) bij de ASR.

Oplossing

Om dit probleem op te lossen, moeten de standaard stappen voor het oplossen van problemen in het routergeheugen worden genomen. De stappen isoleren of het probleem het gevolg is van normaal gebruik, in welk geval een platform/geheugenupgrade gerechtvaardigd zou kunnen zijn; of een geheugenlek waar extra geheugencontrole en probleemoplossing vereist zijn. Zie [Geheugendetectie](#) en algemene [technieken voor het oplossen van geheugenproblemen](#) voor meer informatie.

Voor versies die de oplossing niet hebben van Cisco bug-ID [CSCum19502](#), is de meest voor de hand liggende bewerking het inschakelen van telnet of de console toegang tot de router, omdat alleen SSH door deze drempel wordt beïnvloed.

Tip: Met de opdracht [Aa memory threshold](#) kunt u de drempelwaarden tot minimaal 1% beperken. Hoewel dit een tijdelijke manier biedt om SSH te gebruiken voor de router, kan dit echter andere implicaties met zich meebrengen, zoals de vergoeding voor het gebruik van het processorgeheugen om echt laag te blijven vooraleer de toediening wordt gewaarschuwd. Dit zou belangrijker processen kunnen veroorzaken, zoals BGP dat grote hoeveelheden geheugen gebruikt, om niet langer te werken. Daarom is voorzichtigheid geboden.

Zoals eerder uitgelegd, is het volledig plausibel dat de router geen geheugen lekt maar net oversubscript is geplaatst voor de enabled-functies. In dit geval is een platform/geheugenupgrade mogelijk geboden.