

Сбой из-за аутентификации SSH к состояниям нехватки памяти

Содержание

[Введение](#)

[Проблема](#)

[Решение](#)

Введение

Когда Secure Shell (SSH) к маршрутизатору иногда отказывает с ошибкой аутентификации пользователя, о которой сообщают, в отладках SSH, этот документ описывает проблему на маршрутизаторе Cisco IOS®. Эта проблема происходит даже при том, что введенные учетные данные пользователя корректны, и те же учетные данные работают правильно для Telnet.

Примечание: [CSCum19502](#) идентификатора ошибки Cisco был подан для создания поведения между SSH и Telnet последовательным.

Проблема

Заметьте в этих отладках, что даже при том, что "debug aaa authentication" включен, нет никаких отладок Аутентификации, авторизации и учета (AAA), распечатываемых к show AAA, фактически вызван и возвращает сбой.

```
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,

Иногда системный журнал, показанный здесь, также наблюдается, когда SSH предпринят, но это не становится печатным последовательно:

```
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,
```

Основная причина проблемы является состояниями нехватки памяти на маршрутизаторе. Когда AAA не в состоянии выделять память для создания Уникального идентификатора (UID) для входящего Сеанса SSH, это сообщает о том же сбое как сбой аутентификации AAA (проверка подлинности, авторизация и учет) даже при том, что не предпринят AAA. Это условие происходит, когда доступная память процессора падает ниже AAA "Опознавательный порог нижней области памяти", который по умолчанию установлен к 3% общей памяти и может быть проверен с командой **memory show aaa**. Эта проблема часто замечается на Маршрутизаторе агрегации (ASR) 1001 платформа, где существует ограниченная память на маршрутизаторе, который может быть исчерпан с тяжелым использованием уровня управления, таким как полная таблица Протокола BGP. На ASR 1001 существует 4 ГБ установленного DRAM, но после того, как все другие процессоры CPU и Linux загружаются, Cisco IOS перенесла 1.1 ГБ. Как только память исчерпана до такой степени, что AAA больше не может выделять память для UID, SSH не в состоянии работать.

Рассмотрите эти данные памяти от двух ASR:

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
```

От простого способа расчета на нерабочем ASR процент от доступной памяти составляет 1.28% ($14914664 / 1160982064 * 100$) общей доступной памяти. На рабочем ASR это - 3.51% ($40860008 / 1160982064 * 100$), который является чуть выше опознавательного порога нижней области памяти.

Эту проблему трудно определить, потому что сообщение %AAA-3-ACST_LOW_MEM_UID_FAIL часто не становится печатным, когда эта ошибка происходит из-за состояния нехватки памяти. Кроме того, способ, которым AAA вычисляет порог памяти, не зависит от необработанной суммы памяти процессора, доступной на процессоре маршрута (RP), а скорее проценте от общей памяти. Поэтому могло бы все еще быть по-видимому много памяти процессора, показанной как свободное в выходных данных команды **show memory summary**, когда это происходит без ошибок функции malloc, сообщил.

Примечание: [CSCuj50368](#) идентификатора ошибки Cisco был подан для создания сообщений об ошибках SSH более явными о настоящей причине для ошибки проверки подлинности.

Один путь к проверить, является ли это действительно проблемой, состоит в том, чтобы посмотреть на статистику памяти AAA:

```
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 :
```

Если "инкременты количества" Сбоя Уникального идентификатора AAA с каждой отказавшей попыткой SSH, проблема вызвана этим состоянием нехватки памяти.

Для решения этой проблемы стандартные шаги по устранению неисправностей памяти должны быть предприняты для изоляции причины. Для получения дополнительной информации о том, как устранить неполадки проблем памяти на ASR, см. [Обзор Использования памяти](#).

Решение

Для решения этой проблемы стандартные шаги по устранению неисправностей памяти

маршрутизатора должны быть предприняты. Шаги изолируют, является ли проблема из-за стандартного использования, в этом случае платформа/обновление памяти могла бы быть гарантирована; или утечка памяти, где могли бы потребоваться дополнительный мониторинг памяти и устранение проблем. Посмотрите [методики поиска и устранения проблем Детектора](#) и [общей памяти Утечки памяти](#) для получения дополнительной информации.

Для версий, которые не имеют исправления от идентификатора ошибки Cisco [CSCum19502](#), самый очевидный обходной путь должен включать Telnet или консольный доступ к маршрутизатору, так как только на SSH влияет этот порог.

Совет: [Команда threshold памяти aaa](#) позволяет вам уменьшать пороговые значения до минимума 1%. Однако, в то время как это предоставляет временный путь к SSH к маршрутизатору, он может привести к другим результатам, таким как допуск использования памяти процессора для отбрасывания действительно низко, прежде чем будут предупреждены admin. Это могло бы вызвать более важные процессы, такие как BGP, который израсходовал большие количества памяти, чтобы больше не работать. Следовательно это - что-то, что должно использоваться с осторожностью.

Как объяснено ранее, абсолютно вероятно, что маршрутизатор не пропускает память, но просто превышен для активированных опций. В этом случае платформа/обновление памяти могла бы быть гарантирована.