メモリの枯渇状態による SSH 認証の失敗

内容

概要

このドキュメントでは、ルータへの Secure Shell（SSH）が失敗し、SSH のデバッグ情報でユーザ認証の失敗が報告されることがあるという、Cisco IOS® ルータでの問題について説明します。この問題は、入力したユーザ クレデンシャルが正しく、同じクレデンシャルが Telnet では正しく機能する場合でも発生します。

> **注**：Cisco Bug ID CSCum19502は、SSHとTelnet間の動作を一貫させるために記載されています。

問題

以下のデバッグ情報で、「debug aaa authentication」が有効であるにもかかわらず、認証、認可、およびアカウンティング（AAA）が実際に実行されて失敗が返されたことを示す AAA デバッグ情報が表示されていないことに注意してください。

```
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,
```

SSH を実行したときに、次に示す syslog が表示されることもありますが、常に出力されるわけではありません。

```
*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
```

問題の根本的な原因は、ルータのメモリ不足状態です。AAA が受信 SSH セッション用の一意の ID（UID）を作成するためのメモリ割り当てに失敗すると、AAA を実行しない場合でも、AAA の認証失敗と同じ失敗を報告します。この状態は、プロセッサの空きメモリが、AAA の「Authentication low-memory threshold」を下回った場合に発生します。この設定は、デフォルトでは全メモリの 3 % に設定され、**show aaa memory command コマンドで確認できます。**この問題は、アグリゲーション サービス ルータ（ASR）1001 プラットフォームでしばしば発生します。このプラットフォームでは、ルータのメモリが限られており、完全な Border Gateway Protocol（BGP）テーブルなど、コントロール プレーンでの使用量が多い場合にメモリが枯渇する可能性があります。ASR 1001には4 GBのDRAMがインストールされていますが、他のすべてのCPUとLinuxプロセッサがブートすると、Cisco IOSは1.1 GBを残します。AAAがメモリを使い果たすと、SSHは動作しません。

2 つの ASR からの次のメモリ データを考えてください。

```
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
```

単純な計算から、正常に動作しない ASR 上での空きメモリのパーセンテージは、全使用可能メモリの 1.28 % です（14914664 / 1160982064 * 100）。正常に動作している ASR では 3.51 %（40860008 / 1160982064 * 100）であり、「Authentication low-memory threshold」を少し上回っています。

この問題の特定は困難です。それは、このエラーが発生しても、メモリ不足状態が原因で、%AAA-3-ACCT_LOW_MEM_UID_FAIL メッセージが表示されないことがあるためです。また、AAA がメモリしきい値を計算する方法は、ルート プロセッサ（RP）で使用できるプロセッサ メモリ量そのものではなく、合計メモリの割合に依存します。そのため、malloc の障害が報告されずにこの問題が発生すると、**show memory summary コマンドの出力でプロセッサ メモリが十分に空いているように見える可能性があります。**

> **注**：Cisco Bug ID CSCuj50368は、SSHエラーメッセージを認証失敗の本当の理由をより明確にするために記載されています。

これが本当の問題かどうかを確認するための 1 つの方法は、AAA のメモリ統計情報を調べることです。

```
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 :
```

「AAA Unique ID Failure」の数が、SSH が失敗するたびに増加している場合は、このメモリ不足状態が問題の原因となっています。

この問題をトラブルシューティングするには、ASR 1000 の標準的なメモリ トラブルシューティング手順を実施し、原因を特定する必要があります。ASR でメモリの問題をトラブルシューティングする方法についての詳細は、「メモリ使用量の概要」を参照してください。

解決方法

この問題をトラブルシューティングするには、ルータの標準的なメモリ トラブルシューティング手順を実行する必要があります。この手順により、問題が通常の使用によるものかどうかが特定されます。その場合には、プラットフォームまたはメモリのアップグレードが有効な場合があります。また、メモリ リークの場合は、さらなるメモリ モニタリングとトラブルシューティングが必要になることもあります。詳細は、「メモリ リーク検出」および共通のメモリのトラブルシューティング テクニックを参照してください。

Cisco Bug ID CSCum19502（登録ユーザ専用）で修正が適用されていないバージョンの場合、最も明白な回避策は、SSHのみがこのスレッショルドの影響を受けるため、Telnetまたはコンソールアクセスを有効にすることです。

> **ヒント**：**aaa memory threshold コマンドを使用すると、しきい値を最小値の 1 % に減らすことができます。**これにより、一時的にルータに SSH で接続できるようになりますが、プロセッサ メモリ使用量の余裕が非常に低くなってから管理者にアラートが通知されるといった、他の影響があります。また、大量のメモリを使用する BGP などの重要なプロセスが動作しなくなることがあります。したがって、この方法は注意して使用する必要があります。

前述のように、最も可能性の高い原因は、ルータでメモリ リークが発生していないものの、有効化された機能に対してオーバーサブスクライブされていることです。その場合には、プラットフォームやメモリのアップグレードが有効な場合があります。