

# AAAAccSrvUnreachable および AAAAuthSrvUnreachable トラップのトラブルシューティング

## 内容

### [概要](#)

[トラップトリガー](#)

[aaamgrプロセスアプローチで連続した障害](#)

[キープアライブアプローチ](#)

[トラブルシューティングコマンド/アプローチ](#)

[RADIUS設定の基本](#)

[show task resources facility aaaamgr all](#)

[show radius counters {all |サーバー](#)

[show session subsystem facility {aaamgr | sessmgr} {all |インスタンス](#)

[ping](#)

[traceroute](#)

[radius test instance x auth {radius group](#)

[radius test instance x accounting {radius group](#)

[show radius info \[radius group](#)

[monitor subscriber](#)

[パケットキャプチャ](#)

[修正](#)

[最終例](#)

[関連するシスコ サポート コミュニティ ディスカッション](#)

Remote Authentication Dial-In User Service(RADIUS)SNMPAAAAccSrvUnreachable

AAAAuthSrvUnreachable 2

RESULTRADIUS//

LABIP

RADIUS2//

## **aaamgr**

aaamgraaamgrradiusradiusaaamgrsessmgraaamgrshow task resourcesaaamgr1radiusaaamgr

show radius countersAccess-Request Current Consecutive Failures in a mgrshow radius  
accounting (or authentication) servers detailRADIUSActiveNot Responding1SNMP RADIUS

```
[source]PDSN> show radius accounting servers detail
Friday November 28 23:23:34 UTC 2008
```

```
+-----Type:          (A) - Authentication      (a) - Accounting
|                    (C) - Charging          (c) - Charging Accounting
|                    (M) - Mediation         (m) - Mediation Accounting
|
|+-----Preference:  (P) - Primary          (S) - Secondary
||
||+----State:        (A) - Active            (N) - Not Responding
|||                 (D) - Down              (W) - Waiting Accounting-On
|||                 (I) - Initializing      (w) - Waiting Accounting-Off
|||                 (a) - Active Pending    (U) - Unknown
|||
|||+--Admin          (E) - Enabled          (D) - Disabled
|||  Status:
|||  |
|||  |+--Admin
|||  | status        (O) - Overridden      (.) - Not Overridden
|||  | Overridden:
|||  |
vvvvv IP              PORT GROUP
-----
PNE. 198.51.100.1    1813 default
```

Event History:

```
2008-Nov-28+23:18:36      Active
2008-Nov-28+23:18:57      Not Responding
2008-Nov-28+23:19:12      Active
2008-Nov-28+23:19:30      Not Responding
2008-Nov-28+23:19:36      Active
2008-Nov-28+23:20:57      Not Responding
2008-Nov-28+23:21:12      Active
2008-Nov-28+23:22:31      Not Responding
2008-Nov-28+23:22:36      Active
2008-Nov-28+23:23:30      Not Responding
```

このカウンタがリセットされずに設定された値 ( デフォルト=4 ) に達した場合は、設定可能な値に従います。(カッコ[]はオプションの修飾子を示すために使用され、この場合はトラブルシューティングのアカウンティングをキャプチャします ( アカウンティングが指定されていない場合は認証がデフォルトです ) )。

```
radius [accounting] detect-dead-server consecutive-failures 4
```

次に、このサーバは、設定された期間 ( 分 ) の「ダウン」とマークされます。

```
radius [accounting] deadtime 10
```

SNMPトラップとログもトリガーされます。たとえば、認証とアカウンティングの場合は次のようになります。

```
Fri Jan 30 06:17:19 2009 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 172.28.221.178
Fri Jan 30 06:22:19 2009 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
172.28.221.178

Fri Nov 28 21:59:12 2008 Internal trap notification 42 (AAAAccSvrUnreachable) server 6 ip
address 172.28.221.178
```

Fri Nov 28 22:28:29 2008 Internal trap notification 43 (AAAAccSvrReachable) server 6 ip address 172.28.221.178

```
2008-Nov-28+21:59:12.899 [radius-acct 24006 warning] [8/0/518 <aaamgr:231> aaamgr_config.c:1060]
[context: source, contextID: 2] [software internal security config user critical-info] Server
172.28.221.178:1813 unreachable
```

```
2008-Nov-28+22:28:29.280 [radius-acct 24007 info] [8/0/518 <aaamgr:231> aaamgr_config.c:1068]
[context: source, contextID: 2] [software internal security config user critical-info] Server
172.28.221.178:1813 reachable
```

トラップは、到達不能なサーバを示します。パターンに注意してください。たとえば、あるサーバまたは別のサーバまたはすべてのサーバで発生しているか、またバウンスの頻度は何か、頻繁に発生しているか、それとも頻繁に発生しているか。

また、このトラップがトリガーされるために必要なのは1つのaaamgrが失敗することだけなので、このトラップに関する注意すべき部分は、問題の範囲を示さないことです。これは非常に広範囲または非常に小さい可能性があります。これはオペレータが判断し、それを理解するためのアプローチがこの記事で説明されています。

show snmp trap statisticsは、古いトラップが削除されてから長い時間が経過しても、ブートアップ後にトリガーされた回数を報告します。次の例は、到達不能なアカウンティングの問題を示しています。

```
[source]PDSN> show snmp trap statistics | grep -i aaa
Wednesday September 10 08:38:19 UTC 2014
```

Trap Name	#Gen	#Disc	Disable	Last Generated
-----				
AAAAccSvrUnreachable	833	0	0	2014:09:10:08:36:54
AAAAccSvrReachable	839	0	0	2014:09:10:08:37:00

上記の例で報告されているaaamgrは#231です。これは、システム管理カード(SMC)上にあるASR 5000上の管理aaamgrです。この出力で欺かれているのは、個々のaaamgrまたはaaamgrsで到達可能性の問題が発生した場合、ログで報告されるインスタンス番号が管理aaamgrインスタンスであり、問題が発生した特定のインスタンスではないということです。これは、多くのインスタンスで到達可能性の問題が発生している場合は、ロギングが即座に完了するため、管理インスタンスで一般的に報告されています。この情報を知らなかった場合は、騙されます。トラブルシューティングのセクションでは、障害が発生しているaaamgrを判別する方法について詳しく説明します。一部のバージョンのStarOS 17およびv18+以降では、接続に問題がある対応するaaamgrインスタンス番号 (SNMPトラップで報告) が特定のID(Cisco CDETS CSCum84773)のログに報告されるように、この動作が変更されていますこの現象が報告されます。

管理aaamgrは最大sessmgrインスタンス番号+ 1なので、ASR 5500ではデータ処理カード(DPC)が385、またはDPC 2が1153になります。

同様に、管理aaamgrは、オペレータ/管理者ログインの処理と、RADIUSサーバ自体から開始される許可要求の変更の処理を担当します。

続けて、「show radius accounting (またはauthentication) servers detail」コマンドは、トラップ/ログに対応する状態変更のタイムスタンプを「Down」に示します(注意: Not Responding defined earlyはタイムアウトを取得する単一のaaamgrですが、Downは設定ごとに十分な連続タイムアウトを取得してDownをトリガーする単一のaaamgrです)

```
vvvvv IP          PORT GROUP
-----
asDE. 172.28.221.178 1813 default
```

```
Event History:
2008-Nov-28+21:59:12      Down
2008-Nov-28+22:28:29      Active
2008-Nov-28+22:28:57      Not Responding
2008-Nov-28+22:32:12      Down
2008-Nov-28+23:01:57      Active
2008-Nov-28+23:02:12      Not Responding
2008-Nov-28+23:05:12      Down
2008-Nov-28+23:19:29      Active
2008-Nov-28+23:19:57      Not Responding
2008-Nov-28+23:22:12      Down
```

設定されているサーバが1つだけの場合は、マークダウンされません。これは、コールセットアップを正常に行うには重要です。

注意すべき点は、detect-dead-server config行に「response-timeout」という別のパラメータを設定できることです。指定した場合、サーバは、連続する障害と応答タイムアウトの条件の両方が満たされている場合にのみマークダウンされます。response-timeoutは、特定のサーバに送信されたすべての要求に対してNO応答が受信される時間を指定します。(このタイマーは、応答を受信すると継続的にリセットされることに注意してください)。この状態は、サーバまたはネットワーク接続が完全にダウンした場合に発生し、部分的に侵害または低下した場合に発生します。

この使用例は、トラフィックのバーストによって連続した障害がトリガーされますが、その結果としてサーバが即座にダウンするようにマークするというシナリオではありません。むしろ、サーバは、応答が受信されない特定の時間が経過した後にのみマークダウンされ、実際のサーバの到達不能を表します。

radiusステートマシンの変更を制御する方法は、すべてのaaamgrプロセスを調べ、失敗した再試行の状態をトリガーする方法を見つけることに依存します。この方法は、ある程度の障害のランダム性に左右されるため、障害を検出するための理想的なアルゴリズムではない可能性があります。しかし、他のすべての人が正常に動作している間に壊れているaaamgrを見つけるのは特に良いです。

## キープアライブアプローチ

RADIUSサーバの到達可能性を検出するもう1つの方法は、ダミーキープアライブテストメッセージを使用することです。これには、ライブトラフィックを監視する代わりに、偽のRADIUSメッセージを絶えず送信することが含まれます。この方法のもう1つの利点は、常にアクティブであることです。AAAAMGRアプローチで連続した障害が発生した場合は、RADIUSトラフィックが送信されない時間帯があるため、その時間帯に問題が存在するかどうかを知る方法がないため、試行が開始されると検出が遅延されます。また、サーバがマークダウンされると、これらのキープアライブは送信され続け、サーバをできる限り早くマークアップできます。このアプローチの欠点は、テストメッセージに管理aaamgrインスタンスを使用するため、問題が発生している可能性がある特定のaaamgrインスタンスに関連する問題が欠落することです。

このアプローチに関連するさまざまな設定を次に示します。

```
radius (accounting) detect-dead-server keepalive
radius (accounting) keepalive interval 30
```

```
radius (accounting) keepalive retries 3
radius (accounting) keepalive timeout 3
radius (accounting) keepalive consecutive-response 1
radius (accounting) keepalive username Test-Username
radius keepalive encrypted password 2ec59b3188f07d9b49f5ea4cc44d9586
radius (accounting) keepalive calling-station-id 0000000000000000
radius keepalive valid-response access-accept
```

コマンド「radius (accounting) detect-dead-server keepalive」は、aamgrアプローチで連続した障害が発生する代わりに、キープアライブアプローチをオンにします。上記の例では、システムはユーザ名Test-UsernameとパスワードTest-Usernameを30秒ごとにテストメッセージを送信し、応答がない場合は3秒ごとに再試行し、最大3回の再試行を行った後にサーバがダウンします。最初の応答を受け取ると、再びバックアップをマークします。

上記の設定の認証要求/応答の例を次に示します。

```
<<<<OUTBOUND 17:50:12:657 Eventid:23901(6)
```

```
RADIUS AUTHENTICATION Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1812 (142) PDU-
dict=starent-vsai
Code: 1 (Access-Request)
Id: 16
Length: 142
Authenticator: 51 6D B2 7D 6A C6 9A 96 0C AB 44 19 66 2C 12 0A
  User-Name = Test-Username
  User-Password = B7 23 1F D1 86 46 4D 7F 8F E0 2A EF 17 A1 F3 BF
  Calling-Station-Id = 0000000000000000
  Service-Type = Framed
  Framed-Protocol = PPP
  NAS-IP-Address = 192.168.50.151
  Acct-Session-Id = 00000000
  NAS-Port-Type = HRPD
  3GPP2-MIP-HA-Address = 255.255.255.255
  3GPP2-Correlation-Id = 00000000
  NAS-Port = 4294967295
  Called-Station-ID = 00
```

```
INBOUND>>>> 17:50:12:676 Eventid:23900(6)
```

```
RADIUS AUTHENTICATION Rx PDU, from 192.168.50.200:1812 to 192.168.50.151:32783 (34) PDU-
dict=starent-vsai
Code: 2 (Access-Accept)
Id: 16
Length: 34
Authenticator: 21 99 F4 4C F8 5D F8 28 99 C6 B8 D9 F9 9F 42 70
  User-Password = testpassword
```

同じSNMPトラップを使用して、aaamgrアプローチの連続した障害と同様に、unreachable/downおよびreachable/up radiusの状態を示します。

```
Fri Feb 27 17:54:55 2009 Internal trap notification 39 (AAAAuthSvrUnreachable) server 1 ip
address 192.168.50.200
Fri Feb 27 17:57:04 2009 Internal trap notification 40 (AAAAuthSvrReachable) server 1 ip address
192.168.50.200
```

「show radius counters all」には、認証およびアカウントINGのキープアライブ要求を追跡するためのセクションがあります。認証カウンタは次のとおりです。

## Server-specific Keepalive Auth Counters

```
-----
```

Keepalive Access-Request Sent:	33
Keepalive Access-Request Retried:	3
Keepalive Access-Request Timeouts:	4
Keepalive Access-Accept Received:	29
Keepalive Access-Reject Received:	0
Keepalive Access-Response Bad Authenticator Received:	0
Keepalive Access-Response Malformed Received:	0
Keepalive Access-Response Malformed Attribute Received:	0
Keepalive Access-Response Unknown Type Received:	0
Keepalive Access-Response Dropped:	0

## トラブルシューティングコマンド/アプローチ

AAA Unreachableトラップのトリガーについて説明したので、次のステップは、影響を判別し、根本原因を突き止めるために使用するさまざまなトラブルシューティングコマンドを理解することです。到達不能は非常に広範な用語です。ネットワーク、サーバ、またはASRでの到達不能の場所については説明しません。たとえば、要求が最初に送信されたかどうかはわかりますか。サーバは要求を受信しましたか。要求に応答しましたか。応答はASRに戻ったか、もし応答があれば内部パス（フロー）で処理またはドロップされたか。このセクションでは、これらの質問に答える方法について説明します。

### RADIUS設定の基本

最初に、RADIUSの設定に関する基本的な知識が必要です。RADIUSの設定のほとんどは特別な名前のグループに属しており、すべてのコンテキストには次のように設定できるデフォルトグループがあります。多くの場合、設定にはデフォルトグループの1つのグループだけが含まれます。

```
[local]CSE2# config
[local]CSE2(config)# context aaa_ctx
[aaa_ctx]ASR5000(config-ctx)# aaa group default
[aaa_ctx]ASR5000(config-aaa-group)#
```

特定の名前付きaaaグループが使用されている場合、たとえば、次のような文がサブスクライバプロファイルまたはアプリケーションポイント名(APN)で設定されています。

```
subscriber name <subscriber name>
  aaa group <group name>
```

注：システムは最初に、サブスクライバに割り当てられている特定のaaaグループをチェックし、次にaaa group defaultをチェックして、特定のグループで定義されていない追加の設定を確認します。

さまざまなaaaグループ設定のすべての設定テーブルに割り当てられたすべての値を集約する便利なコマンドを次に示します。これにより、デフォルト値を含むすべての設定を手動で確認しなくても簡単に確認でき、特定の設定を想定する際に間違いを犯さないように役立つ場合があります。次のコマンドは、すべてのコンテキストでレポートされます。

```
show aaa group all
show aaa group name <group name>
```

最も重要な設定は、radiusアクセスサーバとアカウントングサーバ自体です。以下が一例です

。

```
radius server 209.165.201.1 key testtesttesttest port 1645 priority 1 max-rate 5
radius server 209.165.201.2 key testtesttesttest port 1645 priority 2 max-rate 5
radius accounting server 209.165.201.1 key testtesttesttest port 1646 priority 1
radius accounting server 209.165.201.2 key testtesttesttest port 1646 priority 2
```

1秒あたりのサーバに送信される要求の数を制限するmax-rate機能に注意してください

また、NASのIPアドレスも定義する必要があります。NASのIPアドレスは、RADIUS要求の送信元のインターフェイス上のIPアドレスであり、応答を受信します。定義されていない場合、要求は送信されず、サブスクライバトレースをモニタしても明らかなエラーが発生しない可能性があります ( RADIUS要求が送信されず、理由が表示されない )。

```
radius attribute nas-ip-address address 10.211.41.129
```

認証とアカウントングの両方が同じサーバで処理されることが多いため、RADIUSサーバの認証トラフィックとアカウントングトラフィックを区別するために異なるポート番号が使用されることに注意してください。ASR5K側では、UDP送信元ポート番号が指定されておらず、シャーシによってaamgrベースで選択されます ( 詳細は後述 )。

通常、冗長性を確保するために、複数のアクセスサーバとアカウントングサーバが指定されます。ラウンドロビンまたは優先順位付けされた順序を設定できます。

```
radius [accounting] algorithm {first-server | round-robin}
```

first-serverオプションを指定すると、すべての要求が最も低い番号の優先度でサーバに送信されます。再試行の失敗が発生した場合、またはさらに悪い場合にのみ、サーバがマークダウンされ、次の優先度が試行されたサーバになります。詳細は以下をご覧ください。

RADIUS ( アカウントングまたはアクセス ) 要求が送信されると、応答が必要です。タイムアウト期間内 ( 秒 ) に応答が受信されなかった場合 :

```
radius [accounting] timeout 3
```

要求は指定された回数までに再送信されます。

```
radius [accounting] max-retries 5
```

つまり、要求は、試行されている特定のRADIUSサーバで放棄されるまで、max-retries + 1回の合計を送信できます。この時点で、次のRADIUSサーバに同じシーケンスを順に試行します。各サーバが応答なしでmax-retries + 1回試行された場合、その時点までに他に失敗の理由がないと仮定して、コールは拒否されます。

同様に、すべてのサーバにタイムアウトが発生して認証とアカウントングが失敗した場合でも、ユーザがアクセスできる設定は可能ですが、商用の導入では実現できない可能性があります。

```
radius allow [accounting] authentication-down
```

また、設定されたすべてのサーバ間の特定の要求の送信総数を制限できる構成モジュールがあり、これらはデフォルトで無効になっています。

radius [accounting] max-transmissions 256

たとえば、これが設定されている場合は= 1です。セカンダリサーバが存在する場合でも、特定のサブスクリバセットアップに対して1回しか試行されないため、試行されることはありません。

## show task resources facility aaaamgr all

各aaamgrプロセスは、関連するsessmgrプロセス（コール全体の処理を担当）とペアになり、「機能」します。また、異なるPacket Services Card(PSC)またはData Processing Card(DPC)に配置されますが、同じインスタンスIDを使用します。また、この出力例では、ASR 5000用のシステム管理カード(SMC)で実行されている特別なaaamgrインスタンス231（またはASR 5500用の管理入力出力カード）は、加入者要求を処理しませんが、radius testコマンドに使用されます（後述）。CLIログイン処理。

このスニペットでは、PSC 13にあるaaamgr 107が、PSC 1にあるペアのsessmgr 107のすべてのRADIUS処理を処理します。aaamgr 107の到達可能性の問題は、sessmgr 107のコールに影響しません。

cpu	facility	task		cputime		memory		files		sessions		status
		inst	used	allc	used	alloc	used	allc	used	allc	S	
1/0	sessmgr	107	1.6%	100%	119.6M	155.0M	26	500	83	6600	I	good
13/1	aaamgr	107	0.3%	94%	30.8M	77.0M	18	500	--	--	-	good
8/0	aaamgr	231	0.1%	30%	11.6M	25.0M	19	500	--	--	-	good

次の例では、aaamgr 92に関する問題が、セッション数に関して他のsessmgrsと比較した場合に容易に見られるように、ペアのsessmgrに影響を及ぼしていることに注意してください。

cpu	facility	task		cputime		memory		files		sessions		status
		inst	used	allc	used	alloc	used	allc	used	allc	S	
12/0	sessmgr	92	1.2%	100%	451.5M	1220M	43	500	643	21120	I	good
16/0	aaamgr	92	0.0%	95%	119.0M	315.0M	20	500	--	--	-	good
12/0	sessmgr	95	6.9%	100%	477.3M	1220M	41	500	2626	21120	I	good
12/0	sessmgr	105	7.7%	100%	600.5M	1220M	45	500	2626	21120	I	good
12/0	sessmgr	126	3.4%	100%	483.0M	1220M	44	500	2625	21120	I	good
12/0	sessmgr	131	8.1%	100%	491.7M	1220M	45	500	2627	21120	I	good

## show radius counters { {all | server <server IP>} [instance <aamgr #>] |概要}

よく知られているコマンドの数は、「show radius counters」の種類です

このコマンドは、RADIUSの問題のトラブルシューティングに役立つ多数のカウンタを報告します。「show radius counters all」コマンドは、成功と失敗をサーバベースで追跡する際に非常に重要です。このコマンドを構成するさまざまなカウンタの意味を理解することが重要です。これは明らかではないことがあります。コマンドはコンテキストに応じて実行されるため、aaaグループが定義されているコンテキストと同じコンテキストで実行する必要があります。

特記事項：モニタされていない期間では、カウンタ値やカウンタ間の関係から結論を引き出すことは困難です。正確な結論を出すには、最も適切なアプローチは、トラブルシューティング中の問題が発生している間にカウンタをリセットして監視することです。

次の出力では、"Access-Request Sent" = 1、"Access-Request Retried" = 3に注意してください。したがって、特定のRADIUSサーバに対する新しい要求は1回だけカウントされ、すべての再試行は個別にカウントされます。この場合、合計3 + 1 = 4のアクセス要求が送信されます。カウンタ



「Access-Request Timeouts」 = 1に注意してください。1つのタイムアウトは、すべての再試行が失敗した場合にのみ発生します。この場合、3回の再試行で応答がない場合は、1回のタイムアウトになります(4ではありません)。これは、成功するか、すべての試行が失敗するまで、設定されたすべてのサーバで発生します。したがって、サーバごとに個別に追跡されるカウンタに注意してください。この例を次に示します。

```
radius max-retries 3
radius server 192.168.50.200 encrypted key 01abd002c82b4a2c port 1812 priority 1
radius server 192.168.50.250 encrypted key 01abd002c82b4a2c port 1812 priority 2

[destination]CSE2# show radius counters all

Server-specific Authentication Counters
-----
Authentication server address 192.168.50.200, port 1812:
  Access-Request Sent: 1
  Access-Request with DMU Attributes Sent: 0
  Access-Request Pending: 0
  Access-Request Retried: 3
  Access-Request with DMU Attributes Retried: 0
  Access-Challenge Received: 0
  Access-Accept Received: 0
  Access-Reject Received: 0
  Access-Reject Received with DMU Attributes: 0
  Access-Request Timeouts: 1
  Access-Request Current Consecutive Failures in a mgr: 1
  Access-Request Response Bad Authenticator Received: 0
  Access-Request Response Malformed Received: 0
  Access-Request Response Malformed Attribute Received: 0
  Access-Request Response Unknown Type Received: 0
  Access-Request Response Dropped: 0
  Access-Request Response Last Round Trip Time: 0.0 ms
  Access-Request Response Average Round Trip Time: 0.0 ms
Current Access-Request Queued: 0 ... Authentication server address 192.168.50.250, port 1812:
Access-Request Sent: 1 Access-Request with DMU Attributes Sent: 0 Access-Request Pending: 0
Access-Request Retried: 3 Access-Request with DMU Attributes Retried: 0 Access-Challenge
Received: 0 Access-Accept Received: 0 Access-Reject Received: 0 Access-Reject Received with DMU
Attributes: 0 Access-Request Timeouts: 1 Access-Request Current Consecutive Failures in a mgr: 1
Access-Request Response Bad Authenticator Received: 0 Access-Request Response Malformed
Received: 0 Access-Request Response Malformed Attribute Received: 0 Access-Request Response
Unknown Type Received: 0 Access-Request Response Dropped: 0 Access-Request Response Last Round
Trip Time: 0.0 ms Access-Request Response Average Round Trip Time: 0.0 ms
Current Access-Request Queued: 0
```

タイムアウトは失敗としてカウントされないことに注意してください。タイムアウトが発生した場合、受信したAccess-Acceptと受信したAccess-Rejectの数は、Access-Request Sentに加算されません。

これらのカウンタの分析は、完全に単純ではない可能性があります。たとえば、モバイルIP(MIP)プロトコルの場合、認証に失敗するため、MIP登録応答(RRP)は送信されず、モバイルはMIP RRPを受信していないため、新しいMIP登録要求(RRQ)を開始し続ける可能性があります。新しいMIP RRQが発行されるたびに、PDSNは新しい認証要求を送信します。この要求は、それ自体が一連の再試行を行うことができます。これは、パケットトレースの先頭にあるIdフィールドで確認できます。これは、一連の再試行ごとに一意です。その結果、Sent、Retried、およびTimeoutのカウンタは、受信したコールの数に対して予想をはるかに上回る可能性があります。これらの余分な再試行を最小限に抑えるために有効にできるオプションがあり、外部エージェント(FA)(ただしホームエージェント(HA)サービスでは設定できません。"authentication mn-aaa <6選択肢はこちら> optimize-retries"

その他の有用なカウンタ :

「Access-Request Response Dropped」 : 認証要求への応答を待っている間にコールのセットアップが失敗すると発生します。

「Access-Request Response Last Round Trip Time」 : エンドポイント間の遅延を示します。ただし、遅延の発生場所は明らかではありません。

「Access-Request Current Consecutive Failures in a mgr」は、AAA Unreachableトラップのトリガーに関する最初のセクションで説明した内容に関連しています。連続するタイムアウトの数が最も多いアラームを表します。

「Current Access/Accounting-Request Queued」は、応答されていない要求とキューに残っている要求を示します ( アカウンティングは、認証が行わない間、キューの構築を無期限に許可します )

AAA Unreachableが報告される最も一般的なシナリオは、アクセスタイムアウトや応答ドロップが発生しているのに、アクセスレスポンスが要求に対応していないことです。

専用技術サポートモードにアクセスできる場合は、aaamgrインスタンスレベルでさらに調査を行い、特定のaaamgrsが全体の「悪い」カウンタの増加の原因であるかどうかを判断できます。たとえば、特定のPSC/DPCに配置されているaaamgrsや、問題のある単一のaaamgrやランダムなaaamgrsを探します - パターンを探します。すべてまたはほとんどのaaamgrsに問題がある場合、根本原因がシャーシの外部にあるか、またはシャーシ上で大規模であることを示す可能性が高くなります。その場合、一般的なヘルスチェックを行う必要があります。

アカウンティング用の特定のaaamgrに関する問題を示す出力例を次に示します。(この問題は、特定のaaamgrインスタンス(114)ポートからのトラフィックをブロックしていたASR5KとRADIUSサーバ間のファイアウォールの不具合であることが判明しました)。3週間の間に受信された応答はわずか48個ですが、10万件以上のタイムアウトが発生しています ( 再送信は含まれません )。

```
[source]PDSN> show radius counters server 209.165.201.1 instance 114 | grep -E "Accounting-Request Sent|Accounting-Response Received|Accounting-Request Timeouts"
Wednesday October 01 18:12:24 UTC 2014
  Accounting-Request Sent:                14306189
  Accounting-Response Received:          14299843
  Accounting-Request Timeouts:           6342
```

```
[source]PDSN> show radius counters server 209.165.201.1 instance 114 | grep -E "Accounting server address|Accounting-Request Sent|Accounting-Response Received|Accounting-Request Timeouts"
Wednesday October 22 20:26:35 UTC 2014
  Accounting server address 209.165.201.1, port 1646:
  Accounting-Request Sent:                15105872
  Accounting-Response Received:          14299891
  Accounting-Request Timeouts:           158989
```

```
[source]PDSN> show radius counters server 209.165.201.1 instance 114 | grep Accounting
Wednesday October 22 20:33:09 UTC 2014
  Per-Context RADIUS Accounting Counters
  Accounting Response
  Server-specific Accounting Counters
  Accounting server address 209.165.201.1, port 1646:
  Accounting-Request Sent:                15106321
  Accounting-Start Sent:                  7950140
  Accounting-Stop Sent:                   7156129
  Accounting-Interim Sent:                 52
  Accounting-On Sent:                      0
  Accounting-Off Sent:                     0
  Accounting-Request Pending:              3
  Accounting-Request Retried:              283713
```

```

Accounting-Start Retried:                279341
Accounting-Stop Retried:                 4372
Accounting-Interim Retried:              0
Accounting-On Retried:                   0
Accounting-Off Retried:                  0
Accounting-Response Received:            14299891
Accounting-Request Timeouts:             159000
Accounting-Request Current Consecutive Failures in a mgr: 11
Accounting-Response Bad Response Received: 0
Accounting-Response Malformed Received:  0
Accounting-Response Unknown Type Received: 0
Accounting-Response Dropped:             21
Accounting-Response Last Round Trip Time: 52.5 ms
Accounting-Response Average Round Trip Time: 49.0 ms
Accounting Total G1 (Acct-Output-Octets): 4870358614798
Accounting Total G2 (Acct-Input-Octets):  714140547011
Current Accounting-Request Queued:       17821

```

最後に、どのカウンタが増加しているか、どのサーバに対して、どの速度で増加しているかを判断します。

**show session subsystem facility {aaamgr | sessmgr} {all | instance <instance #>}**

このコマンドから得られるすべての余分な出力を調べることは、この記事の範囲外ですが、いくつかの例を見る価値があります。他のトラブルシューティングと同様に、良いと思われる出力と悪いaaamgrインスタンスの出力を比較すると、報告される値の明らかな違いが明らかになります。これは、要求の総数、失敗/成功率、認証のキャンセルなどに反映されます。現在の状態のクラウド化された画像を提供する可能性のある履歴を削除するには、必ずセッションサブシステムをクリアしてください（1つのインスタンスはクリアできず、すべてクリアする必要があります）。アカウントングに失敗する単一のaaamgrに関して前述の同じ問題を引き続き実行すると、異なるsessmgrインスタンス36を除き、同じ問題を持つ別のノードからの出力が表示されます。一方、インスタンス37からの出力は、動作中のaaamgrの例として示されています。

```

[source]PDSN> show session subsystem facility aaamgr instance 36
Wednesday September 10 08:51:18 UTC 2014

```

```

AAAMgr: Instance 36
39947440 Total aaa requests                17985 Current aaa requests
24614090 Total aaa auth requests          0 Current aaa auth requests
    0 Total aaa auth probes                0 Current aaa auth probes
    0 Total aaa aggregation requests
    0 Current aaa aggregation requests
    0 Total aaa auth keepalive              0 Current aaa auth keepalive
15171628 Total aaa acct requests          17985 Current aaa acct requests
    0 Total aaa acct keepalive              0 Current aaa acct keepalive
20689536 Total aaa auth success            1322489 Total aaa auth failure
    86719 Total aaa auth purged             1016 Total aaa auth cancelled
    0 Total auth keepalive success          0 Total auth keepalive failure
    0 Total auth keepalive purged
    0 Total aaa aggregation success requests
    0 Total aaa aggregation failure requests
    0 Total aaa aggregation purged requests
15237 Total aaa auth DMU challenged
17985/70600 aaa request (used/max)
    14 Total diameter auth responses dropped
6960270 Total Diameter auth requests      0 Current Diameter auth requests
    23995 Total Diameter auth requests retried
    52 Total Diameter auth requests dropped
9306676 Total radius auth requests        0 Current radius auth requests
    0 Total radius auth requests retried
    988 Total radius auth responses dropped
    13 Total local auth requests            0 Current local auth requests

```

8500275 Total pseudo auth requests 0 Current pseudo auth requests  
8578 Total null-username auth requests (rejected)  
0 Total aggregation responses dropped  
15073834 Total aaa acct completed 79763 Total aaa acct purged <== If issue started  
recently, this may not have yet started incrementing  
0 Total acct keepalive success 0 Total acct keepalive timeout  
0 Total acct keepalive purged  
4 CLI Test aaa acct purged  
0 IP Interface down aaa acct purged  
0 No Radius Server found aaa acct purged  
0 No Response aaa acct purged  
14441090 Total acct sess alloc  
14422811 Total acct sess delete  
18279 Current acct sessions  
0 Auth No Wait Suppressed  
0 Aggr No Wait Suppressed  
0 Disc No Wait Suppressed  
0 Start No Wait Suppressed  
0 Interim No Wait Suppressed  
0 Stop No Wait Suppressed  
0 Acct OnOff Custom14  
0 Acct OnOff Custom67  
0 Acct OnOff  
0 Recovery Str Suppressed  
0 Recovery Stop Suppressed  
0 Med Chrg Gtpp Suppressed  
0 Med Chrg Radius Suppressed  
0 Radius Probe Trigger  
0 Recovery Stop Acct Session Suppressed  
46 Total aaa acct cancelled  
0 Total Diameter acct requests 0 Current Diameter acct requests  
0 Total Diameter acct requests retried  
0 Total diameter acct requests dropped  
0 Total diameter acct responses dropped  
0 Total diameter acct cancelled  
0 Total diameter acct purged  
15171628 Total radius acct requests 17985 Current radius acct requests  
46 Total radius acct cancelled  
79763 Total radius acct purged  
11173 Total radius acct requests retried  
49 Total radius acct responses dropped  
0 Total radius sec acct requests 0 Current radius sec acct requests  
0 Total radius sec acct cancelled  
0 Total radius sec acct purged  
0 Total radius sec acct requests retried  
0 Total gtpp acct requests 0 Current gtpp acct requests  
0 Total gtpp acct cancelled 0 Total gtpp acct purged  
0 Total gtpp sec acct requests 0 Total gtpp sec acct purged  
0 Total null acct requests 0 Current null acct requests  
16218236 Total aaa acct sessions 21473 Current aaa acct sessions  
8439 Total aaa acct archived 2 Current aaa acct archived  
21473 Current recovery archives 4724 Current valid recovery records  
1 Total aaa sockets opened 1 Current aaa sockets opened  
1 Total aaa requests pend socket opened  
0 Current aaa requests pend socket open  
133227 Total radius requests pend server max-outstanding  
17982 Current radius requests pend server max-outstanding  
0 Total radius auth req queued server max-rate  
0 Max radius auth req queued server max-rate  
0 Current radius auth req queued server max-rate  
0 Total radius acct req queued server max-rate  
0 Max radius acct req queued server max-rate  
0 Current radius acct req queued server max-rate  
0 Total radius chrg auth req queued server max-rate

```

0 Max radius charg auth req queued server max-rate
0 Current radius charg auth req queued server max-rate
0 Total radius charg acct req queued server max-rate
0 Max radius charg acct req queued server max-rate
0 Current radius charg acct req queued server max-rate
0 Total aaa radius coa requests      0 Total aaa radius dm requests
0 Total aaa radius coa acks          0 Total aaa radius dm acks
0 Total aaa radius coa naks          0 Total aaa radius dm naks
0 Total radius charg auth            0 Current radius charg auth
0 Total radius charg auth success    0 Total radius charg auth failure
0 Total radius charg auth purged     0 Total radius charg auth cancelled
0 Total radius charg acct            0 Current radius charg acct
0 Total radius charg acct success    0 Total radius charg acct purged
0 Total radius charg acct cancelled
0 Total gtpv charg                   0 Current gtpv charg
0 Total gtpv charg success            0 Total gtpv charg failure
0 Total gtpv charg cancelled         0 Total gtpv charg purged
0 Total gtpv sec charg               0 Total gtpv sec charg purged
161722 Total prepaid online requests  0 Current prepaid online requests
141220 Total prepaid online success   20392 Current prepaid online failure
0 Total prepaid online retried       102 Total prepaid online cancelled
8 Current prepaid online purged

```

...

```

[source]PDSN> show session subsystem facility aaamgr instance 37
Wednesday September 10 08:51:28 UTC 2014

```

```

AAAMgr: Instance 37
39571859 Total aaa requests           0 Current aaa requests
24368622 Total aaa auth requests      0 Current aaa auth requests
0 Total aaa auth probes               0 Current aaa auth probes
0 Total aaa aggregation requests
0 Current aaa aggregation requests
0 Total aaa auth keepalive            0 Current aaa auth keepalive
15043217 Total aaa acct requests      0 Current aaa acct requests
0 Total aaa acct keepalive            0 Current aaa acct keepalive
20482618 Total aaa auth success       1309507 Total aaa auth failure
85331 Total aaa auth purged           968 Total aaa auth cancelled
0 Total auth keepalive success        0 Total auth keepalive failure
0 Total auth keepalive purged
0 Total aaa aggregation success requests
0 Total aaa aggregation failure requests
0 Total aaa aggregation purged requests
15167 Total aaa auth DMU challenged
1/70600 aaa request (used/max)
41 Total diameter auth responses dropped
6883765 Total Diameter auth requests  0 Current Diameter auth requests
23761 Total Diameter auth requests retried
37 Total Diameter auth requests dropped
9216203 Total radius auth requests    0 Current radius auth requests
0 Total radius auth requests retried
927 Total radius auth responses dropped
15 Total local auth requests          0 Current local auth requests
8420022 Total pseudo auth requests    0 Current pseudo auth requests
8637 Total null-username auth requests (rejected)
0 Total aggregation responses dropped
15043177 Total aaa acct completed      0 Total aaa acct purged
0 Total acct keepalive success        0 Total acct keepalive timeout
0 Total acct keepalive purged
0 CLI Test aaa acct purged
0 IP Interface down aaa acct purged
0 No Radius Server found aaa acct purged
0 No Response aaa acct purged
14358245 Total acct sess alloc

```

```

14356293 Total acct sess delete
 1952 Current acct sessions
    0 Auth No Wait Suppressed
    0 Aggr No Wait Suppressed
    0 Disc No Wait Suppressed
    0 Start No Wait Suppressed
    0 Interim No Wait Suppressed
    0 Stop No Wait Suppressed
    0 Acct OnOff Custom14
    0 Acct OnOff Custom67
    0 Acct OnOff
    0 Recovery Str Suppressed
    0 Recovery Stop Suppressed
    0 Med Chrg Gtpp Suppressed
    0 Med Chrg Radius Suppressed
    0 Radius Probe Trigger
    0 Recovery Stop Acct Session Suppressed
 40 Total aaa acct cancelled
    0 Total Diameter acct requests      0 Current Diameter acct requests
    0 Total Diameter acct requests retried
    0 Total diameter acct requests dropped
    0 Total diameter acct responses dropped
    0 Total diameter acct cancelled
    0 Total diameter acct purged
15043217 Total radius acct requests      0 Current radius acct requests
 40 Total radius acct cancelled
    0 Total radius acct purged
 476 Total radius acct requests retried
 37 Total radius acct responses dropped
    0 Total radius sec acct requests      0 Current radius sec acct requests
    0 Total radius sec acct cancelled
    0 Total radius sec acct purged
    0 Total radius sec acct requests retried
    0 Total gtpp acct requests      0 Current gtpp acct requests
    0 Total gtpp acct cancelled      0 Total gtpp acct purged
    0 Total gtpp sec acct requests      0 Total gtpp sec acct purged
    0 Total null acct requests      0 Current null acct requests
16057760 Total aaa acct sessions      4253 Current aaa acct sessions
 14 Total aaa acct archived      0 Current aaa acct archived
 4253 Current recovery archives      4249 Current valid recovery records
    1 Total aaa sockets opened      1 Current aaa sockets opened
    1 Total aaa requests pend socket opened
    0 Current aaa requests pend socket open
29266 Total radius requests pend server max-outstanding
    0 Current radius requests pend server max-outstanding
    0 Total radius auth req queued server max-rate
    0 Max radius auth req queued server max-rate
    0 Current radius auth req queued server max-rate
    0 Total radius acct req queued server max-rate
    0 Max radius acct req queued server max-rate
    0 Current radius acct req queued server max-rate
    0 Total radius charg auth req queued server max-rate
    0 Max radius charg auth req queued server max-rate
    0 Current radius charg auth req queued server max-rate
    0 Total radius charg acct req queued server max-rate
    0 Max radius charg acct req queued server max-rate
    0 Current radius charg acct req queued server max-rate
    0 Total aaa radius coa requests      0 Total aaa radius dm requests
    0 Total aaa radius coa acks      0 Total aaa radius dm acks
    0 Total aaa radius coa naks      0 Total aaa radius dm naks
    0 Total radius charg auth      0 Current radius charg auth
    0 Total radius charg auth success      0 Total radius charg auth failure
    0 Total radius charg auth purged      0 Total radius charg auth cancelled
    0 Total radius charg acct      0 Current radius charg acct

```

```
0 Total radius charg acct success      0 Total radius charg acct purged
0 Total radius charg acct cancelled
0 Total gtpg charg                      0 Current gtpg charg
0 Total gtpg charg success              0 Total gtpg charg failure
0 Total gtpg charg cancelled           0 Total gtpg charg purged
0 Total gtpg sec charg                 0 Total gtpg sec charg purged
160020 Total prepaid online requests    0 Current prepaid online requests
139352 Total prepaid online success    20551 Current prepaid online failure
...
```

```
[source]PDSN> show session subsystem facility aaamgr instance 36
Wednesday September 10 09:12:13 UTC 2014
```

```
AAAMgr: Instance 36
```

```
39949892 Total aaa requests              17980 Current aaa requests
24615615 Total aaa auth requests         0 Current aaa auth requests
0 Total aaa auth probes                 0 Current aaa auth probes
0 Total aaa aggregation requests
0 Current aaa aggregation requests
0 Total aaa auth keepalive              0 Current aaa auth keepalive
15172543 Total aaa acct requests          17980 Current aaa acct requests
0 Total aaa acct keepalive              0 Current aaa acct keepalive
20690768 Total aaa auth success          1322655 Total aaa auth failure
86728 Total aaa auth purged              1016 Total aaa auth cancelled
0 Total auth keepalive success          0 Total auth keepalive failure
0 Total auth keepalive purged
0 Total aaa aggregation success requests
0 Total aaa aggregation failure requests
0 Total aaa aggregation purged requests
15242 Total aaa auth DMU challenged
17981/70600 aaa request (used/max)
14 Total diameter auth responses dropped
6960574 Total Diameter auth requests     0 Current Diameter auth requests
23999 Total Diameter auth requests retried
52 Total Diameter auth requests dropped
9307349 Total radius auth requests       0 Current radius auth requests
0 Total radius auth requests retried
988 Total radius auth responses dropped
13 Total local auth requests             0 Current local auth requests
8500835 Total pseudo auth requests        0 Current pseudo auth requests
8578 Total null-username auth requests (rejected)
0 Total aggregation responses dropped
15074358 Total aaa acct completed         80159 Total aaa acct purged
0 Total acct keepalive success           0 Total acct keepalive timeout
0 Total acct keepalive purged
4 CLI Test aaa acct purged
0 IP Interface down aaa acct purged
0 No Radius Server found aaa acct purged
0 No Response aaa acct purged
14441768 Total acct sess alloc
14423455 Total acct sess delete
18313 Current acct sessions
0 Auth No Wait Suppressed
0 Aggr No Wait Suppressed
0 Disc No Wait Suppressed
0 Start No Wait Suppressed
0 Interim No Wait Suppressed
0 Stop No Wait Suppressed
0 Acct OnOff Custom14
0 Acct OnOff Custom67
0 Acct OnOff
```

```

0 Recovery Str Suppressed
0 Recovery Stop Suppressed
0 Med Chrg Gtpp Suppressed
0 Med Chrg Radius Suppressed
0 Radius Probe Trigger
0 Recovery Stop Acct Session Suppressed
46 Total aaa acct cancelled
0 Total Diameter acct requests          0 Current Diameter acct requests
0 Total Diameter acct requests retried
0 Total diameter acct requests dropped
0 Total diameter acct responses dropped
0 Total diameter acct cancelled
0 Total diameter acct purged
15172543 Total radius acct requests      17980 Current radius acct requests
46 Total radius acct cancelled
80159 Total radius acct purged
11317 Total radius acct requests retried
49 Total radius acct responses dropped
0 Total radius sec acct requests        0 Current radius sec acct requests
0 Total radius sec acct cancelled
0 Total radius sec acct purged
0 Total radius sec acct requests retried
0 Total gtpp acct requests              0 Current gtpp acct requests
0 Total gtpp acct cancelled            0 Total gtpp acct purged
0 Total gtpp sec acct requests         0 Total gtpp sec acct purged
0 Total null acct requests             0 Current null acct requests
16219251 Total aaa acct sessions        21515 Current aaa acct sessions
8496 Total aaa acct archived           0 Current aaa acct archived
21515 Current recovery archives        4785 Current valid recovery records
1 Total aaa sockets opened             1 Current aaa sockets opened
1 Total aaa requests pend socket opened
0 Current aaa requests pend socket open
133639 Total radius requests pend server max-outstanding
17977 Current radius requests pend server max-outstanding
...

```

また、show task resourcesを実行して、すべてのセッション間で不均等なセッション数（使用済みカラム）をチェックする必要があります。見つかった場合は、このコマンドを使用して、これらのセッションのペアaaamgrsを確認し、行外のフィールドがあるかどうかを確認します。問題がRADIUSによるものである場合は、何かを見つける良い機会があります。

前のセクションのshow task resourcesの例では、sessmgr 92のセッションカウントが大幅に低く、aamgr 92とペアになっています。show session subsystemの出力は、max-outstandingおよびaaa auth purgedカウンタの合計が大幅に増加していることを示しています。grep機能は、シャーシやメモ帳++などの強力な検索エディタでライブで使用して、データを迅速に分析できます。このコマンドを複数回実行して、どの値が上昇しているか、または上昇したままかを確認します。

```

[Ingress]PGW# show session subsystem facility aaamgr all
Tuesday January 10 04:42:29 UTC 2012
4695 Total aaa auth purged
4673 Total radius auth requests        16 Current radius auth requests
4167 Total radius requests pend server max-outstanding
76 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"
Tuesday January 10 04:51:00 UTC 2012
4773 Total radius requests pend server max-outstanding
67 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"
Tuesday January 10 04:56:10 UTC 2012
5124 Total radius requests pend server max-outstanding

```



```
81 Current radius requests pend server max-outstanding
```

```
[Ingress]PGW# show session subsystem facility aaamgr instance 92
```

```
Tuesday January 10 04:57:03 UTC 2012
```

```
5869 Total aaa auth purged
5843 Total radius auth requests      12 Current radius auth requests
5170 Total radius requests pend server max-outstanding
71 Current radius requests pend server max-outstanding
```

```
[Ingress]PGW# show session subsystem facility aaamgr instance 92
```

```
Tuesday January 10 05:10:05 UTC 2012
```

```
6849 Total aaa auth purged
6819 Total radius auth requests      6 Current radius auth requests
5981 Total radius requests pend server max-outstanding
68 Current radius requests pend server max-outstanding
```

```
[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"
```

```
Tuesday January 10 05:44:22 UTC 2012
```

```
71 Total radius requests pend server max-outstanding
0 Current radius requests pend server max-outstanding
61 Total radius requests pend server max-outstanding
0 Current radius requests pend server max-outstanding
```

```
7364 Total radius requests pend server max-outstanding  <== instance #92
68 Current radius requests pend server max-outstanding
```

```
89 Total radius requests pend server max-outstanding
0 Current radius requests pend server max-outstanding
74 Total radius requests pend server max-outstanding
0 Current radius requests pend server max-outstanding
```

```
[Ingress]PGW#radius test instance 92 auth server 65.175.1.10 port 1645 test test
```

```
Tuesday January 10 06:13:38 UTC 2012
```

```
Authentication from authentication server 65.175.1.10, port 1645
```

```
Communication Failure: No response received
```

## ping

## traceroute

ICMP pingは、基本的な接続をテストして、AAAサーバに到達できるかどうかを確認します。ネットワークによってはsrcキーワードを使用してpingを送信する必要があり、値を持つためにはAAAコンテキストからpingを実行する必要があります。サーバへのpingが失敗した場合は、コンテキスト内のネクストホップアドレスを含む中間要素にpingを実行し、pingが失敗した場合にネクストホップアドレスへのARPエントリがあることを確認します。tracerouteは、ルーティングの問題にも役立ちます。

```
[source]CSE2# ping 192.168.50.200
```

```
PING 192.168.50.200 (192.168.50.200) 56(84) bytes of data.
```

```
64 bytes from 192.168.50.200: icmp_seq=1 ttl=64 time=0.411 ms
```

```
64 bytes from 192.168.50.200: icmp_seq=2 ttl=64 time=0.350 ms
```

```
64 bytes from 192.168.50.200: icmp_seq=3 ttl=64 time=0.353 ms
```

```
64 bytes from 192.168.50.200: icmp_seq=4 ttl=64 time=0.321 ms
```

```
64 bytes from 192.168.50.200: icmp_seq=5 ttl=64 time=0.354 ms
```

```
--- 192.168.50.200 ping statistics ---
```

```
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
```

```
rtt min/avg/max/mdev = 0.321/0.357/0.411/0.037 ms
```

**radius test instance x auth {radius group <group> | all | server <IP> port <port>}**

<username> <password>

radius test instance x accounting {radius group <group name> | all | server <IP> port <port>}

テクニカルサポートテストコマンドにアクセスすると、特定のアラームが任意のRADIUSサーバに到達できるかどうかをテストできます。基本的なRADIUS接続テストでは、特定のaamgrインスタンスに関係なく、特定のインスタンス#を指定せずに、デフォルトで管理インスタンスを使用する汎用バージョンのコマンドを使用します。これが失敗した場合、特定のインスタンスに関係なく、より広範な問題を示す可能性があります。

このコマンドは、基本的な認証要求またはアカウントिंगの開始要求と停止要求を送信し、応答を待ちます。認証には、任意のユーザ名とパスワードを使用します。この場合は、reject応答が必要で、RADIUSが設計どおりに動作していることを確認します。あるいは、既知の動作ユーザ名とパスワードを使用して、accept応答を受信します

次に、モニタプロトコルからの出力例を示し、ラボシャーシでコマンドの認証バージョンを実行します。

```
[source]CSE2# radius test authentication server 192.168.50.200 port 1812 test test
```

```
Authentication from authentication server 192.168.50.200, port 1812
Authentication Success: Access-Accept received
Round-trip time for response was 12.3 ms
```

```
<<<<OUTBOUND 14:53:49:202 Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1812 (58) PDU-
dict=starent-vsai
Code: 1 (Access-Request)
Id: 5
Length: 58
Authenticator: 56 97 57 9C 51 EF A4 08 20 E1 14 89 40 DE 0B 62
  User-Name = test
  User-Password = 49 B0 92 4D DC 64 49 BA B0 0E 18 36 3F B6 1B 37
  NAS-IP-Address = 192.168.50.151
  NAS-Identifier = source
```

```
INBOUND>>>> 14:53:49:214 Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 192.168.50.200:1812 to 192.168.50.151:32783 (34) PDU-
dict=starent-vsai
Code: 2 (Access-Accept)
Id: 5
Length: 34
Authenticator: D7 94 1F 18 CA FE B4 27 17 75 5C 99 9F A8 61 78
  User-Password = testpassword
```

ライブシャーシの例を次に示します。

```
<<<<OUTBOUND 12:45:49:869 Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 10.209.28.200:33156 to 209.165.201.1:1645 (72) PDU-
dict=customl50
Code: 1 (Access-Request)
Id: 6
Length: 72
Authenticator: 67 C2 2B 3E 29 5E A5 28 2D FB 85 CA 0E 9F A4 17
  User-Name = test
  User-Password = 8D 95 3B 31 99 E2 6A 24 1F 81 13 00 3C 73 BC 53
  NAS-IP-Address = 10.209.28.200
  NAS-Identifier = source
  3GPP2-Session-Term-Capability = Both_Dynamic_Auth_And_Reg_Revocation_in_MIP
```

```
INBOUND>>>> 12:45:49:968 Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 209.165.201.1:1645 to 10.209.28.200:33156 (50) PDU-
dict=custom150
Code: 3 (Access-Reject)
Id: 6
Length: 50
Authenticator: 99 2E EC DA ED AD 18 A9 86 D4 93 52 57 4C 2F 84
    Reply-Message = Invalid username or password
```

次に、コマンドのアカウントिंगバージョンを実行した場合の出力例を示します。パスワードは不要です。

```
[source]CSE2# radius test accounting server 192.168.50.200 port 1813 test
RADIUS Start to accounting server 192.168.50.200, port 1813
Accounting Success: response received
Round-trip time for response was 7.9 ms
```

```
RADIUS Stop to accounting server 192.168.50.200, port 1813
Accounting Success: response received
Round-trip time for response was 15.4 ms
```

```
<<<<OUTBOUND 15:23:14:974 Eventid:24901(6)
RADIUS ACCOUNTING Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1813 (62) PDU-
dict=starent-vsai
Code: 4 (Accounting-Request)
Id: 8
Length: 62
Authenticator: DA 0F A8 11 7B FE 4B 1A 56 EB 0D 49 8C 17 BD F6
    User-Name = test
    NAS-IP-Address = 192.168.50.151
    Acct-Status-Type = Start
    Acct-Session-Id = 00000000
    NAS-Identifier = source
    Acct-Session-Time = 0
```

```
INBOUND>>>> 15:23:14:981 Eventid:24900(6) RADIUS ACCOUNTING Rx PDU, from 192.168.50.200:1813 to
192.168.50.151:32783 (20) PDU-dict=starent-vsai Code: 5 (Accounting-Response) Id: 8 Length: 20
Authenticator: 05 E2 82 29 45 FC BC D6 6C 48 63 AA 14 9D 47 5B <<<<OUTBOUND 15:23:14:983
Eventid:24901(6) RADIUS ACCOUNTING Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1813 (62)
PDU-dict=starent-vsai Code: 4 (Accounting-Request) Id: 9 Length: 62 Authenticator: 29 DB F1 0B
EC CE 68 DB C7 4D 60 E4 7F A2 D0 3A User-Name = test NAS-IP-Address = 192.168.50.151 Acct-
Status-Type = Stop Acct-Session-Id = 00000000 NAS-Identifier = source Acct-Session-Time = 0
INBOUND>>>> 15:23:14:998 Eventid:24900(6) RADIUS ACCOUNTING Rx PDU, from 192.168.50.200:1813 to
192.168.50.151:32783 (20) PDU-dict=starent-vsai Code: 5 (Accounting-Response) Id: 9 Length: 20
Authenticator: D8 3D EF 67 EA 75 E0 31 A5 31 7F E8 7E 69 73 DC
```

次の出力は、特定のRADIUSアカウントングサーバへの接続が切断されている前述の同じaamgrインスタンス36に対するものです。

```
[source]PDSN> radius test instance 36 accounting all test
Wednesday September 10 10:06:29 UTC 2014
```

```
RADIUS Start to accounting server 209.165.201.1, port 1646
Accounting Success: response received
Round-trip time for response was 51.2 ms
```

```
RADIUS Stop to accounting server 209.165.201.1, port 1646
Accounting Success: response received
Round-trip time for response was 46.2 ms
```

```
RADIUS Start to accounting server 209.165.201.2, port 1646
Accounting Success: response received
Round-trip time for response was 89.3 ms
```

```
RADIUS Stop to accounting server 209.165.201.2, port 1646
Accounting Success: response received
Round-trip time for response was 87.8 ms
```

```
RADIUS Start to accounting server 209.165.201.3, port 1646
Communication Failure: no response received
```

```
RADIUS Stop to accounting server 209.165.201.3, port 1646
Communication Failure: no response received
```

```
RADIUS Start to accounting server 209.165.201.4, port 1646
Accounting Success: response received
Round-trip time for response was 81.6 ms
```

```
RADIUS Stop to accounting server 209.165.201.4, port 1646
Accounting Success: response received
Round-trip time for response was 77.1 ms
```

```
RADIUS Start to accounting server 209.165.201.5, port 1646
Accounting Success: response received
Round-trip time for response was 46.7 ms
```

```
RADIUS Stop to accounting server 209.165.201.5, port 1646
Accounting Success: response received
Round-trip time for response was 46.7 ms
```

```
RADIUS Start to accounting server 209.165.201.6, port 1646
Accounting Success: response received
Round-trip time for response was 79.6 ms
```

```
RADIUS Stop to accounting server 209.165.201.6, port 1646
Accounting Success: response received
Round-trip time for response was 10113.0 ms
```

## **show radius info [radius group <group name>] instance { X }**

このコマンドは、設定されたNAS IPアドレスがRADIUSサーバに接続するために使用するネットワークプロセッサユニット(NPU)フローIDとUDPポートを報告します。これは、出力のaaa group defaultセクションで報告されます。特定のaamgrインスタンス#を持つパケットキャプチャのRADIUSパケットと一致する必要がある場合は、ポート番号が役に立ちます (NPUフローは複雑で、この記事では説明していませんが、サポートエンジニアが詳しく調査できるエンティティに注意してください)。また、サーバへの未処理の要求も追跡します。この記事で使用している同じ問題の例では、特定のRADIUSサーバ<==> NAS IP/UDPポートペアだけが強調表示されているとおり失敗しています。

```
[source]PDSN> show radius info radius group all instance 114
Wednesday October 01 11:39:15 UTC 2014
```

```
Context source:
```

```
-----
AAAMGR instance 114:  cb-list-en: 1 AAA Group:  aaa-roamingprovider.com
-----
```

```
Authentication servers:
```

-----  
Primary authentication server address 209.165.201.1, port 1645  
state Active  
priority 1  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0  
Secondary authentication server address 209.165.201.2, port 1645  
state Active  
priority 2  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

Accounting servers:

-----  
Primary accounting server address 209.165.201.1, port 1646  
state Active  
priority 1  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0  
Secondary accounting server address 209.165.201.2, port 1646  
state Active  
priority 2  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

AAAMGR instance 114: cb-list-en: 1 AAA Group: aaa-maingroup.com

-----  
Authentication servers:

-----  
Primary authentication server address 209.165.201.3, port 1645  
state Active  
priority 1  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0  
Secondary authentication server address 209.165.201.4, port 1645  
state Active  
priority 2  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

Accounting servers:

-----  
Primary accounting server address 209.165.201.3, port 1646  
state Down  
priority 1  
requests outstanding 3  
max requests outstanding 3  
consecutive failures 7  
dead time expires in 146 seconds  
Secondary accounting server address 209.165.201.4, port 1646  
state Active  
priority 2  
requests outstanding 0  
max requests outstanding 3  
consecutive failures 0

AAAMGR instance 114: cb-list-en: 1 AAA Group: default

```
socket number: 388550648
socket state: ready
local ip address: 10.210.21.234
local udp port: 25808
flow id: 20425379
use med interface: yes
VRF context ID: 2
```

Authentication servers:

```
-----
Primary authentication server address 209.165.201.5, port 1645
state Active
priority 1
requests outstanding 0
max requests outstanding 3
consecutive failures 0
Secondary authentication server address 209.165.201.6, port 1645
state Not Responding
priority 2
requests outstanding 0
max requests outstanding 3
consecutive failures 0
```

Accounting servers:

```
-----
Primary accounting server address 209.165.201.5, port 1646
state Active
priority 1
requests outstanding 0
max requests outstanding 3
consecutive failures 0
Secondary accounting server address 209.165.201.6, port 1646
state Active
priority 2
requests outstanding 0
max requests outstanding 3
consecutive failures 0
```

[source]PDSN>

## monitor subscriber

モニタサブスクライバを使用して、認証が少なくとも試行されているかどうか、およびモニタされているコールに対して応答が処理されているかどうかを判別できます。Sessmgr Sender Infoのオプション「S」をオンにします。このオプションは、問題のメッセージを処理しているsessmgrまたはaamgrインスタンス番号を効果的にレポートします。HAでのMIPコールの例を次に示します sessmgr / aamgrインスタンス132に接続しています。

Incoming Call:

```
-----
MSID/IMSI      :                               Callid      : 2719afb2
IMEI           : n/a                          MSISDN     : n/a
Username       : 6667067222@cisco.com        SessionType : ha-mobile-ip
Status         : Active                       Service Name: HAService
Src Context    : source
-----
```

\*\*\* Sender Info (ON ) \*\*\*

Thursday June 11 2015

INBOUND>>>> From sessmgr:132 sessmgr\_ha.c:861 (Callid 2719afb2) 15:42:35:742 Eventid:26000(3)

MIP Rx PDU, from 203.0.113.11:434 to 203.0.113.1:434 (190)

Message Type: 0x01 (Registration Request)

Flags: 0x02  
Lifetime: 0x1C20  
Home Address: 0.0.0.0  
Home Agent Address: 255.255.255.255

Thursday June 11 2015

```
<<<<OUTBOUND From aaamgr:132 aaamgr_radius.c:367 (Callid 2719afb2) 15:42:35:743
Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 203.0.113.1:59933 to 209.165.201.3:1645 (301) PDU-
dict=custom9
Code: 1 (Access-Request)
Id: 12
Length: 301
```

Thursday June 11 2015

```
INBOUND>>>> From aaamgr:132 aaamgr_radius.c:1999 (Callid 2719afb2) 15:42:35:915
Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 209.165.201.3:1645 to 203.0.113.1:59933 (156) PDU-
dict=custom9
Code: 2 (Access-Accept)
Id: 12
```

Thursday June 11 2015

```
<<<<OUTBOUND From sessmgr:132 mipha_fsm.c:6617 (Callid 2719afb2) 15:42:36:265 Eventid:26001(3)
MIP Tx PDU, from 203.0.113.1:434 to 203.0.113.11:434 (112)
Message Type: 0x03 (Registration Reply)
Code: 0x00 (Accepted)
Lifetime: 0x1C20
Home Address: 10.229.6.167
```

この記事の最後にも失敗例があります。

## パケット キャプチャ

到達可能性の問題が発生している原因を特定するためにASRに関する情報が十分でない場合があります。この場合、パケットキャプチャが必要になります。個々のサブスクライバの問題をトラブルシューティングする場合、トレース内の各パケットを簡単に特定できます。それ以外の場合は、特定のaaamgrインスタンス# <==> RADIUSサーバペアのいずれかの端で使用されているUDPポートを知っておくと、問題が特定のポート/aamgrインスタンスに関連付けられている場合に役立ちます。ネットワーク内の複数の場所でキャプチャを試みると、パケットがドロップされる場所を判別する必要がある場合があります。この記事で分析した問題は、ASRとRADIUSサーバの間の転送パスの適切な場所でパケットキャプチャを行い、問題を解決するためのブレークスルーとなっていました。

## 修正

この最後のセクションでは、RADIUS接続の問題を修復するためのアイデアをいくつか示します。これらは特定の順序ではなく、単にトラブルシューティングプロセスで考慮すべきリストです。

RADIUSサーバに過負荷が発生している場合は、「radius (accounting) max-outstanding」に設定された値 (デフォルトは256) を使用して負荷を軽減できます。これにより、特定のaamgrプロセスの未処理 (未応答) 要求の数が制限されます。制限に達すると、ログに次のように表示されます。「Failed to assign message id for radius authentication server x.x.x.x:1812」

特定のサーバにレート制限RADIUSメッセージを送信すると、各サーバ設定行のレート制限キーワードを使用して負荷を軽減することもできます。

接続の問題ではなく、アカウントングトラフィックの増加の問題である場合があります。これはRADIUSパーシーの問題ではなく、より多くのアカウントングの開始と停止を引き起こすppp再ネゴシエーションの増加などの別のエリアを指します。したがって、RADIUS以外のトラブ

ルシューティングを行って、観察されている症状の原因またはトリガーを見つける必要がある場合があります。

トラブルシューティングプロセス中に、何らかの理由でRADIUS認証サーバまたはアカウントングサーバをライブサーバのリストから削除すると決定された場合は、サービスを再開する必要があるまでサーバを無期限に停止する(non-config)コマンドがあります。これは、手動で設定から削除する方法よりも明確な方法です。

```
{ | enable} radius [accounting] server x.x.x.x
```

```
[source]CSE2# show radius authentication servers detail
```

```
+-----Type:          (A) - Authentication      (a) - Accounting
|                   (C) - Charging          (c) - Charging Accounting
|                   (M) - Mediation          (m) - Mediation Accounting
|
|+-----Preference: (P) - Primary          (S) - Secondary
||
||+----State:        (A) - Active          (N) - Not Responding
|||                 (D) - Down              (W) - Waiting Accounting-On
|||                 (I) - Initializing      (w) - Waiting Accounting-Off
|||                 (a) - Active Pending    (U) - Unknown
|||
|||+---Admin         (E) - Enabled          (D) - Disabled
|||  Status:
|||
|||+--Admin
|||  status          (O) - Overridden      (.) - Not Overridden
|||  Overridden:
|||
vvvvv IP              PORT GROUP
-----
APNDO 192.168.50.200 1812 default
```

PSCまたはDPCの移行またはラインカードの切り替えにより、NPUフローに関する問題の原因であるnpumgrを含め、移行によりカード上のプロセスが再起動されるため、問題が解決される場合があります。

しかし、前述のaaamgr 92の例を使用した興味深い展開では、PSCの移行が行われた時点でAAA Unreachable障害が実際に開始されています。これは、PSC移行が完了してPSC 11をスタンバイにしたときにNPUフローが失われたためにトリガーされました。1時間後にアクティブ化された時点で、フローの損失の実際の影響がamgr 92に対して開始されました。このような問題は、テクニカルサポートの支援を受けずにトラブルシューティングするのが非常に困難です。

```
[Ingressc]PGW# show rct stat
```

```
RCT stats Details (Last 6 Actions)
```

Action	Type	From	To	Start Time	Duration
Migration	Planned	11	16	2012-Jan-09+16:27:38.135	36.048 sec
Migration	Planned	3	11	2012-Jan-09+17:28:57.413	48.739 sec

```
Mon Jan 09 17:31:11 2012 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3
```

```
Mon Jan 09 17:31:16 2012 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3
```



この問題は、ポートの切り替えによって一時的に解決され、aamgr 92のNPUフローが欠落しているPSCカードがアクティブなラインカードに接続されなくなります。

```
Tue Jan 10 06:52:17 2012 Internal trap notification 93 (CardStandby) card 27
Tue Jan 10 06:52:17 2012 Internal trap notification 1024 (PortDown) card 27 port 1 ifindex
453050375port type 10G Ethernet
Tue Jan 10 06:52:17 2012 Internal trap notification 55 (CardActive) card 28
Tue Jan 10 06:52:17 2012 Internal trap notification 1025 (PortUp) card 28 port 1 ifindex
469827588port type 10G Ethernet
```

最後の障害トラップ：

```
Tue Jan 10 06:53:11 2012 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address
209.165.201.3
```

```
[Ingress]PGW# radius test instance 93 authen server 209.165.201.3 port 1645 test test
Tuesday January 10 07:18:22 UTC 2012
```

```
Authentication from authentication server 209.165.201.3, port 1645
Authentication Failure: Access-Reject received
Round-trip time for response was 38.0 ms
```

```
[Ingress]PGW# show session subsystem facility aaamgr instance 92
Tuesday January 10 07:39:47 UTC 2012
 12294 Total aaa auth purged
 14209 Total radius auth requests          0 Current radius auth requests
 9494 Total radius requests pend server max-outstanding
 0 Current radius requests pend server max-outstanding
```

同様に、「スタック」した特定のaamgrsを再起動すると、問題が解決する場合があります。ただし、これはテクニカルサポートが制限付きテクニカルサポートコマンドを含むため、テクニカルサポートが行うべき課題です。前述のshow task resourcesセクションで紹介したaamgr 92の例では、これは試行されましたが、これは助かりませんでした。これは、根本原因がaamgr 92ではなく、aamgr 92が必要とするNPUフローがないためです ( aamgrの問題ではなくNPUの問題でした )。次に、この試みの関連する出力を示します。プロセスidとタスクインスタンス番号92の関連付けを表示するには、「show task table」を実行します。

```
5 2012-Jan-10+06:20:53 aaamgr 16/0/04722 12.0(40466) PLB27085474/PLB38098237
```

```
[Ingress]PGW# show crash number 5
***** CRASH #05 *****
Build: 12.0(40466)
Fatal Signal 6: Aborted
PC: [b7eb6b90/X] __poll()
Note: User-initiated state dump w/core.
```

```
***** show task table *****
      task
cpu facility      inst      pid pri      parent
-----
      facility      inst      pid
-----
16/0 aaamgr          92      4722  0      sessctrl          0      2887
```

## 最終例

ここでは、この記事で説明されているトラブルシューティングのコマンドとアプローチの多くを集約する、実際のネットワークの停止の最終的な例を示します。このノードは、3G MIP、4G Long Term Evolution(LTE)およびEvolved High Rate Packet Data(eHRPD)コールタイプを処理することに注意してください。

## show snmp trap history

トラップだけで、開始点が顧客から19:25 UTCとして報告された値と一致していることを確認できません。別に、プライマリサーバ209.165.201.3の**AAAAuthSvrUnreachable**トラップは数時間が経過するまで発生しません(理由は不明ですが、注意が必要です。しかし、そのサーバに対するアカウントは即座に開始されました)

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3
Sun Dec 29 19:32:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.3
Sun Dec 29 19:33:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.3
Sun Dec 29 19:34:13 2013 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address
209.165.201.3
Sun Dec 29 19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.3
Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.3
Sun Dec 29 19:38:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 6 ip
address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```

## show task resources

この出力は、DPC 8/1でのコールの数がはるかに少ないことを示しています。これ以上の分析がなければ、DPC 8に問題があることを示唆し、スタンバイDPCに移行するオプションを提案できます。ただし、実際のサブスクリバの影響を確認することが重要です。これらのシナリオでは、通常、サブスクリバは後続の試行で正常に接続するため、サブスクリバにとって影響が大きすぎず、ユーザプレーンの停止も発生していないとプロバイダーに報告しません(障害の内容によって可能)。

7/1	sessmgr	230	27%	100%	586.2M	2.49G	43	500	4123	35200	I	good
7/1	aaamgr	237	0.9%	95%	143.9M	640.0M	22	500	--	--	-	good
7/1	sessmgr	243	22%	100%	588.1M	2.49G	42	500	4118	35200	I	good
7/1	sessmgr	258	19%	100%	592.8M	2.49G	43	500	4122	35200	I	good
7/1	aaamgr	268	0.9%	95%	143.5M	640.0M	22	500	--	--	-	good
7/1	sessmgr	269	23%	100%	586.7M	2.49G	43	500	4115	35200	I	good
7/1	aaamgr	274	0.4%	95%	144.9M	640.0M	22	500	--	--	-	good
7/1	sessmgr	276	30%	100%	587.9M	2.49G	43	500	4123	35200	I	good
7/1	aaamgr	285	1.0%	95%	142.7M	640.0M	22	500	--	--	-	good
7/1	aaamgr	286	0.8%	95%	143.8M	640.0M	22	500	--	--	-	good
7/1	sessmgr	290	28%	100%	588.2M	2.49G	41	500	4115	35200	I	good
8/0	sessmgr	177	23%	100%	588.7M	2.49G	48	500	4179	35200	I	good
8/0	sessmgr	193	24%	100%	591.3M	2.49G	44	500	4173	35200	I	good
8/0	aaamgr	208	0.9%	95%	143.8M	640.0M	22	500	--	--	-	good

8/0	sessmgr	211	23%	100%	592.1M	2.49G	45	500	4173	35200	I	good
8/0	sessmgr	221	27%	100%	589.2M	2.49G	44	500	4178	35200	I	good
8/0	aaamgr	222	0.9%	95%	142.0M	640.0M	22	500	--	--	-	good
8/0	sessmgr	225	25%	100%	592.0M	2.49G	43	500	4177	35200	I	good
8/0	aaamgr	238	0.9%	95%	140.0M	640.0M	22	500	--	--	-	good
8/0	aaamgr	243	1.0%	95%	144.9M	640.0M	22	500	--	--	-	good
8/0	sessmgr	244	31%	100%	593.3M	2.49G	43	500	4177	35200	I	good
8/0	aaamgr	246	0.9%	95%	138.5M	640.0M	22	500	--	--	-	good
8/0	aaamgr	248	0.9%	95%	141.4M	640.0M	22	500	--	--	-	good
8/0	aaamgr	258	0.9%	95%	138.3M	640.0M	22	500	--	--	-	good
8/0	aaamgr	259	0.8%	95%	139.2M	640.0M	22	500	--	--	-	good
8/0	aaamgr	260	0.8%	95%	142.9M	640.0M	22	500	--	--	-	good
8/0	aaamgr	262	0.9%	95%	145.0M	640.0M	22	500	--	--	-	good
8/0	aaamgr	264	0.9%	95%	143.4M	640.0M	22	500	--	--	-	good
8/0	sessmgr	270	24%	100%	592.2M	2.49G	44	500	4171	35200	I	good
8/0	sessmgr	277	20%	100%	593.7M	2.49G	43	500	4176	35200	I	good
8/0	sessmgr	288	23%	100%	591.9M	2.49G	43	500	4177	35200	I	good
8/0	sessmgr	296	24%	100%	593.0M	2.49G	42	500	4170	35200	I	good
8/1	sessmgr	186	2.0%	100%	568.3M	2.49G	48	500	1701	35200	I	good
8/1	sessmgr	192	2.0%	100%	571.1M	2.49G	46	500	1700	35200	I	good
8/1	aaamgr	200	1.0%	95%	147.3M	640.0M	22	500	--	--	-	good
8/1	sessmgr	210	2.1%	100%	567.1M	2.49G	46	500	1707	35200	I	good
8/1	aaamgr	216	0.9%	95%	144.6M	640.0M	22	500	--	--	-	good
8/1	sessmgr	217	2.0%	100%	567.7M	2.49G	45	500	1697	35200	I	good
8/1	sessmgr	231	2.2%	100%	565.7M	2.49G	45	500	1705	35200	I	good
8/1	sessmgr	240	2.0%	100%	569.8M	2.49G	45	500	1702	35200	I	good
8/1	aaamgr	242	0.9%	95%	148.5M	640.0M	22	500	--	--	-	good
8/1	sessmgr	252	1.8%	100%	566.5M	2.49G	44	500	1704	35200	I	good
8/1	aaamgr	261	0.9%	95%	142.0M	640.0M	22	500	--	--	-	good
8/1	aaamgr	263	1.0%	95%	144.1M	640.0M	22	500	--	--	-	good
8/1	aaamgr	265	1.0%	95%	146.4M	640.0M	22	500	--	--	-	good
8/1	aaamgr	267	1.0%	95%	144.4M	640.0M	22	500	--	--	-	good
8/1	aaamgr	269	1.0%	95%	143.8M	640.0M	22	500	--	--	-	good
8/1	sessmgr	274	1.9%	100%	570.5M	2.49G	44	500	1704	35200	I	good
8/1	sessmgr	283	2.0%	100%	570.0M	2.49G	44	500	1708	35200	I	good
8/1	sessmgr	292	2.1%	100%	567.6M	2.49G	44	500	1703	35200	I	good
9/0	sessmgr	1	30%	100%	587.2M	2.49G	48	500	4161	35200	I	good
9/0	diamproxy	1	5.2%	90%	37.74M	250.0M	420	1000	--	--	-	good
9/0	sessmgr	14	25%	100%	587.4M	2.49G	48	500	4156	35200	I	good
9/0	sessmgr	21	20%	100%	591.5M	2.49G	47	500	4156	35200	I	good
9/0	sessmgr	34	23%	100%	586.5M	2.49G	48	500	4155	35200	I	good
9/0	aaamgr	44	0.9%	95%	145.1M	640.0M	21	500	--	--	-	good
9/0	sessmgr	46	29%	100%	592.1M	2.49G	48	500	4157	35200	I	good

## monitor subscriber

DPC 9/1のsessmgr 242に対する認証要求に対する応答がないコールセットアップが捕捉されました。この場合、ペアのaaamgrがDPC 8/1に存在し、8/1のAAA到達不能による3G障害が確認されます。209.165.201.3この時点では、そのサーバの応答を処理する際に問題がないという意味ではありません（上に示すように、トラップは開始するが数時間後）。

8/1	aaamgr	242	0.9%	95%	148.5M	640.0M	22	500	--	--	-	good
9/1	sessmgr	242	20%	100%	589.7M	2.49G	43	500	4167	35200	I	good

-----  
Incoming Call:  
-----

MSID/IMSI	:	Callid	:	4537287a
IMEI	:	MSISDN	:	n/a
Username	:	SessionType	:	ha-mobile-ip

Status : Active Service Name: HAService  
Src Context : Ingress

-----  
INBOUND>>>> From sessmgr:242 sessmgr\_ha.c:880 (Callid 4537287a) 23:18:19:099 Eventid:26000(3)  
MIP Rx PDU, from 203.0.113.1:434 to 203.0.113.3:434 (190)  
Message Type: 0x01 (Registration Request)

<<<<OUTBOUND From aaamgr:242 aaamgr\_radius.c:370 (Callid 4537287a) 23:18:19:100  
Eventid:23901(6)  
RADIUS AUTHENTICATION Tx PDU, from 203.0.113.3:27856 to 209.165.201.3:1645 (301) PDU-  
dict=custom9  
Code: 1 (Access-Request)  
Id: 195  
Length: 301  
Authenticator: CD 59 0C 6D 37 2C 5D 19 FB 60 F3 35 23 BB 61 6B  
User-Name = 6664600074@cisco.com

INBOUND>>>> From sessmgr:242 mipha\_fsm.c:8438 (Callid 4537287a) 23:18:21:049 Eventid:26000(3)  
MIP Rx PDU, from 203.0.113.1:434 to 203.0.113.3:434 (140)  
Message Type: 0x01 (Registration Request)  
Flags: 0x02  
Lifetime: 0x1C20

<<<<OUTBOUND From sessmgr:242 mipha\_fsm.c:6594 (Callid 4537287a) 23:18:22:117 Eventid:26001(3)  
MIP Tx PDU, from 203.0.113.3:434 to 203.0.113.1:434 (104)  
Message Type: 0x03 (Registration Reply)  
Code: 0x83 (Mobile Node Failed Authentication)

\*\*\*CONTROL\*\*\* From sessmgr:242 sessmgr\_func.c:6746 (Callid 4537287a) 23:18:22:144 Eventid:10285  
CALL STATS: <6664600074@cisco.com>, msid <>, Call-Duration(sec): 0  
Disconnect Reason: MIP-auth-failure  
Last Progress State: Authenticating

### show sub [summary] smgr-instance X

興味深いのは、sessmgr 242のセッション数が他の動作中のsessmgrsと似ていることです。さらに詳しく調査したところ、このシャーシでもホストされている4Gコールが接続できたため、3G Mobile IPコールが接続できなかったことが判明しました。停止が開始された後の8時間まで戻ると、このsessmgr 242に対するMIPコールが存在せず、停止が開始される9時間前に戻ると、接続されたコールが存在することが確認できます。

```
[local]PGW# show sub sum smgr-instance 242 connected-time less-than 28800 (8 hours)
Monday December 30 03:38:23 UTC 2013
```

Total Subscribers:	1504		
Active:	1504	Dormant:	0
hsgw-ipv4-ipv6:	0	pgw-pmip-ipv6:	98
pgw-pmip-ipv4:	0	pgw-pmip-ipv4-ipv6:	75
pgw-gtp-ipv6:	700	pgw-gtp-ipv4:	3
pgw-gtp-ipv4-ipv6:	628	sgw-gtp-ipv6:	0
..			
ha-mobile-ip:	0	ggsn-pdp-type-ppp:	0

```
[local]PGW# show sub sum smgr-instance 242 connected-time less-than 32400 (9 hours)
Monday December 30 03:38:54 UTC 2013 ...
ha-mobile-ip: 63 ggsn-pdp-type-ppp: 0
```

### LTEeHRPDaaamgrsessmgrsMIP

```
[local]PGW# show sub sum smgr-instance 272
```

```
Monday December 30 03:57:51 UTC 2013
hsgw-ipv4-ipv6: 0 pgw-pmip-ipv6: 125 pgw-pmip-ipv4: 0 pgw-pmip-ipv4-ipv6: 85 pgw-gtp-ipv6: 1530
pgw-gtp-ipv4-ipv6: 1126
ha-mobile-ip: 1103
```

```
[local]PGW# show sub sum smgr-instance 242
Monday December 30 03:52:35 UTC 2013
hsgw-ipv4-ipv6: 0 pgw-pmip-ipv6: 172 pgw-pmip-ipv4: 0 pgw-pmip-ipv4-ipv6: 115
pgw-gtp-ipv6: 1899
pgw-gtp-ipv4-ipv6: 1348
```

```
ha-mobile-ip: 447
```

## radiusテストインスタンスX認証サーバ

8/1上のすべてのaaamgrsが停止しています。これらのaaamgrsではradius test instanceコマンドは動作しませんが、8/0およびその他のカードではaaamgrsコマンドは動作します。

9/1 sessmgr	242	22%	100%	600.6M	2.49G	41	500	3989	35200	I	good
4/1 sessmgr	20	27%	100%	605.1M	2.49G	47	500	3965	35200	I	good
4/0 sessmgr	27	25%	100%	592.8M	2.49G	46	500	3901	35200	I	good
8/1 aaamgr	242	0.9%	95%	150.6M	640.0M	22	500	--	--	--	good
8/1 aaamgr	20	1.0%	95%	151.9M	640.0M	21	500	--	--	--	good
8/0 aaamgr	27	1.0%	95%	146.4M	640.0M	21	500	--	--	--	good

```
[Ingress]PGW# radius test instance 242 auth server 209.165.201.3 port 1645 test test
Monday December 30 01:03:08 UTC 2013
```

```
Authentication from authentication server 209.165.201.3, port 1645
Communication Failure: No response received
```

```
[Ingress]PGW# radius test instance 20 auth server 209.165.201.3 port 1645 test test
Monday December 30 01:08:45 UTC 2013
```

```
Authentication from authentication server 209.165.201.3, port 1645
Communication Failure: No response received
```

```
[Ingress]PGW# radius test instance 27 auth server 209.165.201.3 port 1645 test test
Monday December 30 01:11:40 UTC 2013
```

```
Authentication from authentication server 209.165.201.3, port 1645
Authentication Failure: Access-Reject received
Round-trip time for response was 16.8 ms
```

## show radius counters all

RADIUSのトラブルシューティングに使用するflagshipコマンドでは、タイムアウトが頻繁に発生し、急速に増加しています。

```
[Ingress]PGW> show radius counters all | grep -E "Authentication server address|Access-Request Timeouts"
```

```
Monday December 30 00:42:24 UTC 2013
```

```
Authentication server address 209.165.201.3, port 1645, group default
Access-Request Timeouts: 400058
Authentication server address 209.165.201.5, port 1645, group default
Access-Request Timeouts: 26479
```

```
[Ingress]PGW> show radius counters all | grep -E "Authentication server address|Access-Request Timeouts"
```

```
Monday December 30 00:45:23 UTC 2013
```

```
Authentication server address 209.165.201.3, port 1645, group default
  Access-Request Timeouts: 400614
Authentication server address 209.165.201.5, port 1645, group default
  Access-Request Timeouts: 26679
```

```
[Ingress]PGW> show radius counters all
Monday December 30 00:39:15 UTC 2013
```

...

```
Authentication server address 209.165.201.3, port 1645, group default
  Access-Request Sent: 233262801
  Access-Request with DMU Attributes Sent: 0
  Access-Request Pending: 22
  Access-Request Retried: 0
  Access-Request with DMU Attributes Retried: 0
  Access-Challenge Received: 0
  Access-Accept Received: 213448486
  Access-Reject Received: 19414836
  Access-Reject Received with DMU Attributes: 0
  Access-Request Timeouts: 399438
  Access-Request Current Consecutive Failures in a mgr: 3
  Access-Request Response Bad Authenticator Received: 16187
  Access-Request Response Malformed Received: 1
  Access-Request Response Malformed Attribute Received: 0
  Access-Request Response Unknown Type Received: 0
  Access-Request Response Dropped: 9039
  Access-Request Response Last Round Trip Time: 267.6 ms
  Access-Request Response Average Round Trip Time: 201.9 ms
  Current Access-Request Queued: 2
```

```
Authentication server address 209.165.201.5, port 1645, group default
  Access-Request Sent: 27731
  Access-Request with DMU Attributes Sent: 0
  Access-Request Pending: 0
  Access-Request Retried: 0
  Access-Request with DMU Attributes Retried: 0
  Access-Challenge Received: 0
  Access-Accept Received: 1390
  Access-Reject Received: 101
  Access-Reject Received with DMU Attributes: 0
  Access-Request Timeouts: 26240
  Access-Request Current Consecutive Failures in a mgr: 13
  Access-Request Response Bad Authenticator Received: 0
  Access-Request Response Malformed Received: 0
  Access-Request Response Malformed Attribute Received: 0
  Access-Request Response Unknown Type Received: 0
  Access-Request Response Dropped: 0
  Access-Request Response Last Round Trip Time: 227.5 ms
  Access-Request Response Average Round Trip Time: 32.3 ms
  Current Access-Request Queued: 0
```

修復

メンテナンスウィンドウ中に、DPCの移行8から10で問題が解決し、AAAAuthSvrUnreachableトラップが停止し、DPC 8がRMA状態になり、根本原因はDPC 8のハードウェア障害であると判断されました (この記事では詳細は不明)。

```
Mon Dec 30 05:58:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip address 209.165.201.3
```

```
Mon Dec 30 05:58:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address 209.165.201.5
```

```
Mon Dec 30 05:58:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
```

209.165.201.5  
Mon Dec 30 05:58:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address 209.165.201.3  
Mon Dec 30 05:59:14 2013 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.5  
Mon Dec 30 06:01:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip address 209.165.201.3  
Mon Dec 30 06:01:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address 209.165.201.3  
  
Mon Dec 30 06:01:28 2013 Internal trap notification 16 (PACMigrateStart) from card 8 to card 10  
Mon Dec 30 06:01:49 2013 Internal trap notification 60 (CardDown) card 8 type Data Processing Card  
Mon Dec 30 06:01:50 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 10 operational status changed to Active  
Mon Dec 30 06:01:50 2013 Internal trap notification 55 (CardActive) card 10 type Data Processing Card  
Mon Dec 30 06:01:50 2013 Internal trap notification 17 (PACMigrateComplete) from card 8 to card 10  
  
Mon Dec 30 06:02:08 2013 Internal trap notification 5 (CardUp) card 8 type Data Processing Card  
Mon Dec 30 06:02:08 2013 Internal trap notification 1502 (EntStateOperEnabled) Card(8) Severity: Warning  
Mon Dec 30 06:02:08 2013 Internal trap notification 93 (CardStandby) card 8 type Data Processing Card  
  
Mon Dec 30 06:08:41 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 08 operational status changed to Offline  
Mon Dec 30 06:08:41 2013 Internal trap notification 60 (CardDown) card 8 type Data Processing Card  
Mon Dec 30 06:08:41 2013 Internal trap notification 1503 (EntStateOperDisabled) Card(8) Severity: Critical  
  
Mon Dec 30 06:09:24 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity Card : 08 Power OFF  
Mon Dec 30 06:09:24 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 08 operational status changed to Empty  
Mon Dec 30 06:09:24 2013 Internal trap notification 7 (CardRemoved) card 8 type Data Processing Card  
Mon Dec 30 06:09:24 2013 Internal trap notification 1507 (CiscoFruRemoved) FRU entity Card : 08 removed  
Mon Dec 30 06:09:24 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity Card : 08 Power OFF  
Mon Dec 30 06:09:50 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity Card : 08 Power ON  
Mon Dec 30 06:09:53 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 08 operational status changed to Offline  
Mon Dec 30 06:09:53 2013 Internal trap notification 8 (CardInserted) card 8 type Data Processing Card  
Mon Dec 30 06:09:53 2013 Internal trap notification 1506 (CiscoFruInserted) FRU entity Card : 08 inserted  
Mon Dec 30 06:10:00 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 08 operational status changed to Booting  
Mon Dec 30 06:11:59 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity Card : 08 operational status changed to Standby  
Mon Dec 30 06:11:59 2013 Internal trap notification 5 (CardUp) card 8 type Data Processing Card  
Mon Dec 30 06:11:59 2013 Internal trap notification 93 (CardStandby) card 8 type Data Processing Card

[local]PGW# show rct stat  
Wednesday January 01 16:47:21 UTC 2014

RCT stats Details (Last 2 Actions)

Action	Type	From	To	Start Time	Duration
Migration	Planned	8	10	2013-Dec-30+06:01:28.323	21.092 sec
Shutdown	N/A	8	0	2013-Dec-30+06:08:41.483	0.048 sec