Troubleshooting de AAAAccSrvUnreachable e AAAAuthSrvUnreachable traps

Contents

Introduction

Este artigo discute como solucionar problemas de armadilhas SNMP AAAAAccSrvUnreachable e AAAAAuthSrvUnreachable, que são disparadas devido a problemas de acessibilidade com um servidor RADIUS (Remote Authentication Dial-In User Service) usado para autenticar assinantes (ou operadores fazendo login no nó, mas não é isso que está sendo discutido aqui). Há duas abordagens que podem ser usadas para determinar quando uma dessas armadilhas disparará. Este artigo explicará quais condições disparam essas armadilhas e quais abordagens de solução de problemas e coleta de dados podem ser tomadas para determinar a causa raiz e resolvê-las. Também discute algumas possíveis etapas de correção que podem ser consideradas.

Observe que o RESULTADO de inalcançabilidade será falhas de chamada ou falhas de contabilidade, o mesmo que se as respostas do raio forem rejeições em vez de aceitações. Embora a taxa de sucesso/falha (autenticação) seja medida independentemente do tempo limite/alcançabilidade (há armadilhas e alarmes para isso) e possa certamente ser analisada por direito próprio, o foco deste artigo estará no problema de alcançabilidade e não no problema de rejeição.

A saída de exemplo do LAB e os tíquetes reais são usados em toda parte para ajudar a conduzir as discussões. O que parece ser endereços IP públicos neste artigo são endereços **falsos**.

Disparadores de armadilhas

Há dois modelos/algoritmos/abordagens diferentes a escolher para determinar o status de um servidor radius e quando tentar um servidor diferente se houver falhas:

Falhas consecutivas em uma abordagem de processo aaamgr

A abordagem original e a mais frequentemente utilizada pelos operadores envolve o acompanhamento do número de falhas que ocorreram numa linha para um determinado processo aaamgr. Um processo aaamgr é responsável por todo o processamento e troca de mensagens radius com um servidor radius, e muitos processos aaamgr existirão em um chassi, cada um emparelhado com processos sessmgr (que são os principais processos responsáveis pelo controle de chamadas). (Exibir todos os processos do aaamgr com o comando "show task resources") Um processo específico do aaamgr processará mensagens de raio para muitas chamadas, não apenas uma única chamada, e esse algoritmo envolve o rastreamento de quantas vezes em uma linha um processo específico do aaamgr não conseguiu obter uma resposta para a mesma solicitação que teve de reenviar - um "Tempo Limite de Solicitação de Acesso" como relatado em "show radius counters".

O respectivo contador "Access-Request Current Consecutive Failures in a mgr", também de "show radius counters", é incrementado quando isso ocorre, e o comando "show radius accounting (ou authentication) servers detail" indica os timestamps da alteração de estado do raio de Ative para Not Responding (mas nenhum trap ou registro SNMP são gerados para apenas uma falha). Aqui está um exemplo de relatório de raio:

```
[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
```

Se este contador atingir o valor configurado (Padrão = 4) sem nunca ser redefinido, por configurável: (observe que os colchetes [ ] são usados para indicar o qualificador opcional e, nesses casos, captura a contabilidade de solução de problemas (a autenticação é o padrão se a contabilidade não for especificada)

radius [accounting] detect-dead-server consecutivas-failure 4

Em seguida, este servidor está marcado como "Inativo" para o período (minutos) configurado:

radius [accounting] tempo de inatividade 10

Uma interceptação e registros SNMP também são disparados, por exemplo, para autenticação e/ou contabilização respectivamente:

```
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
```

As armadilhas indicam o servidor que está inacessível. Anote qualquer padrão. Por exemplo, isso está acontecendo com um servidor ou outro ou com todos os servidores, e qual é a frequência de devolução - isso está acontecendo contínua ou ocasionalmente?

Observe também que tudo o que é preciso para que essa armadilha seja disparada é que um aaamgr falhe, então a parte difícil dessa armadilha é que ela não indica a extensão do problema. Pode ser muito extenso ou muito minúsculo - depende do operador determinar e as abordagens para descobrir isso são discutidas neste artigo.

show snmp trap statistics relatará o número de vezes que ele disparou desde a inicialização, mesmo que as armadilhas mais antigas tenham sido excluídas há muito tempo. Este exemplo mostra um problema inalcançável de contabilidade:

```
[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
```

Observe que o aaamgr relatado no exemplo acima é #231. Este é o aaamgr de gerenciamento no ASR 5000 que reside no SMC (System Management Card, placa de gerenciamento do sistema). O que está enganando nesta saída é que quando um aaamgr ou aaamgrs individual experimentam problemas de alcançabilidade, o número de instância relatado nos registros é a instância do aaamgr de gerenciamento e não as instâncias específicas que estão enfrentando o problema. Isso se deve ao fato de que, se muitas instâncias estiverem enfrentando problemas de acessibilidade, então o registro será preenchido rapidamente se todos forem relatados como tal, e, portanto, o projeto tem sido reportar genericamente sobre a instância de gerenciamento, que, se não soubéssemos disso, certamente estaria enganando. Na seção de solução de problemas serão fornecidos mais detalhes sobre como determinar que aaamgr(s) está(ão) falhando. Começando em algumas versões do StarOS 17 e v18+, esse comportamento foi alterado de modo que o número de instância correspondente com problemas de conectividade (conforme relatado em interceptações SNMP) é relatado nos registros com a id específica (Cisco CDETS CSCum84773), embora ainda seja relatada apenas a primeira ocorrência (em vários amgrs aaple) desse evento.

O aaamgr de gerenciamento é o número máximo de instância do sessmgr + 1, e assim em um ASR 5500 é 385 para o DPC (Data Processing Card) ou 1153 (para DPC 2).

Como sinônimo, o gerente aaamgr é responsável por manipular logins de operador/administrador, bem como por tratar de alterações de solicitações de autorização iniciadas a partir dos próprios servidores RADIUS.

Continuando, o comando "show radius accounting (ou authentication) servers detail" indicará os timestamps das alterações de estado para Down que correspondem às armadilhas/logs (lembrete: Não responder definido anteriormente é apenas um único aaamgr obtendo um tempo limite, enquanto Down é um único aaamgr obtendo tempos limite consecutivos suficientes por configuração para disparar para baixo)

```
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
```

Se houver apenas um servidor configurado, ele não será marcado como inativo, pois isso seria essencial para uma configuração de chamada bem-sucedida.

Vale mencionar que há outro parâmetro que pode ser configurado na linha de configuração do servidor detect-dead chamado "response-timeout". Quando especificado, um servidor é marcado como inativo somente quando as condições consecutivas de falhas e tempo limite de resposta

são atendidas. O tempo limite de resposta especifica um período em que NÃO são recebidas respostas a TODAS as solicitações enviadas a um servidor específico. Observe que esse temporizador será redefinido continuamente à medida que as respostas forem recebidas. Essa condição seria esperada quando um servidor ou a conexão de rede estiver completamente inoperante, em vez de parcialmente comprometida/degradada.

O caso de uso para isso seria um cenário em que uma intermitência no tráfego faz com que as falhas consecutivas sejam disparadas, mas marcar um servidor imediatamente como resultado não é desejado. Em vez disso, o servidor só é marcado como inativo depois de um período de tempo específico em que nenhuma resposta é recebida, representando efetivamente a inacessibilidade real do servidor.

Esse método discutido sobre o controle de alterações de máquina de estado RADIUS depende da análise de todos os processos do aaamgr e da localização de um que dispara a condição de tentativas com falha. Esse método está sujeito até certo ponto a alguma aleatoriedade de falhas e, portanto, pode não ser o algoritmo ideal para detectar falhas. Mas é especialmente bom encontrar aaamgr(s) quebrado(s) enquanto todos os outros estão funcionando bem.

Abordagem de manutenção de atividade

Outro método de detecção da acessibilidade do servidor radius é o uso de mensagens de teste de keepalive fictícias. Isso envolve o envio constante de mensagens de raio falsas em vez de monitorar o tráfego ao vivo. Outra vantagem desse método é que ele está sempre ativo em comparação com as falhas consecutivas em uma abordagem aaamgr, em que pode haver períodos em que nenhum tráfego de raio é enviado, e portanto não há como saber se um problema existe durante esses períodos, resultando em detecção atrasada quando as tentativas começam a ocorrer. Além disso, quando um servidor é marcado como inativo, essas manutenções de atividade continuam a ser enviadas para que o servidor possa ser marcado assim que possível. A desvantagem dessa abordagem é que ela perde problemas vinculados a instâncias específicas do aaamgr que podem estar tendo problemas porque usa a instância do aaaamgr de gerenciamento para as mensagens de teste.

Aqui estão os vários configuráveis relevantes para esta abordagem:

```
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 000000000000000
radius keepalive valid-response access-accept
```

O comando "radius (accounting) detect-dead-server keepalive" ativa a abordagem de manutenção de atividade em vez de falhas consecutivas em uma abordagem aaamgr. No exemplo acima, o sistema envia uma mensagem de teste com o nome de usuário Test-Username e a senha Test-Username a cada 30 segundos, e tenta novamente a cada 3 segundos se nenhuma resposta for recebida, e tenta até 3 vezes, após o que marca o servidor inoperante. Quando recebe sua primeira resposta, ele a marca novamente.

Aqui está um exemplo de solicitação/resposta de autenticação para as configurações acima:

```
<<<<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-vsa1
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-vsa1
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
```

As mesmas interceptações SNMP são usadas para significar os estados de raio inalcançável/inacessível e alcançável/ativo como com as falhas consecutivas em uma abordagem aaamgr:

```
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
```

O "show radius counters all" tem uma seção para controlar as solicitações de keepalive para autenticação e tarifação - aqui estão os contadores de autenticação:

```
   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
```

Troubleshooting de comandos/abordagens

Agora que o gatilho para armadilhas não alcançáveis AAA foi explicado, a próxima etapa é entender os vários comandos de solução de problemas a serem usados para determinar o impacto e tentar descobrir a causa raiz. A inacessibilidade é um termo muito amplo. Ele não explica onde está a inacessibilidade - na rede, no servidor ou no ASR. Por exemplo, sabe-se se os pedidos foram enviados em primeiro lugar? O servidor recebeu as solicitações? Respondeu aos pedidos? As respostas retornaram ao ASR e, em caso afirmativo, foram processadas ou descartadas no caminho interno (ou seja, fluxos). Esta seção tenta abordar como responder a essas perguntas.

Princípios básicos da configuração do RADIUS

Primeiro, há alguns conceitos básicos com os quais é preciso conhecer a configuração do RADIUS. A maior parte da configuração do RADIUS está em um grupo especificamente nomeado, e todos os contextos têm um grupo padrão que pode ser configurado da seguinte maneira. Muitas vezes, as configurações terão apenas um grupo, o grupo padrão.

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

Se grupos de aaa com nome específico forem usados, eles serão apontados pela seguinte instrução configurada em um perfil de assinante ou Nome do ponto de aplicativo (APN) (dependendo da tecnologia de controle de chamadas), por exemplo:

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

Note: O sistema primeiro verifica o grupo aaa específico atribuído ao assinante e, em seguida, verifica o padrão do grupo aaa para outros configuráveis não definidos no grupo específico.

Aqui estão comandos úteis que resumem todos os valores atribuídos a todos os configuráveis nas várias configurações de grupo aaa. Isso permite uma visualização rápida de todos os configuráveis, incluindo valores padrão, sem ter que examinar a configuração manualmente e, possivelmente, ajudar a evitar erros ao assumir determinadas configurações. Esses comandos relatam em todos os contextos:

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

O mais importante configurável é, claro, o acesso radius e os próprios servidores de contabilidade. Aqui está um exemplo:

```
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
```

Observe o recurso de taxa máxima que limita o número de solicitações enviadas ao servidor por aaamgr por segundo

Além disso, o endereço IP do NAS também precisa ser definido, que é o endereço IP em uma

interface no contexto do qual as solicitações radius são enviadas e as respostas recebidas. Se não for definido, as solicitações não serão enviadas e os rastreamentos de assinantes monitorados poderão não postar um erro óbvio (nenhuma solicitação de raio enviada e nenhuma indicação de porquê).

radius attribute nas-ip-address address 10.211.41.129

Observe que, como a autenticação e a contabilidade são frequentemente tratadas pelo mesmo servidor, um número de porta diferente é usado para diferenciar a autenticação em relação ao tráfego de contabilidade no servidor RADIUS. Para o lado ASR5K, o número da porta de origem UDP NÃO é especificado e é escolhido pelo chassi em uma base aaamgr (mais adiante).
Normalmente, vários servidores de acesso e tarifação são especificados para fins de redundância. É possível configurar um pedido redondo ou priorizado:

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

A opção do primeiro servidor resulta no envio de TODAS as solicitações ao servidor com a prioridade de número mais baixo. Somente quando ocorrem falhas de nova tentativa, ou pior, um servidor é marcado como inativo, o servidor com a próxima prioridade é tentada. Mais informações sobre isso abaixo.

Quando uma solicitação radius (accounting ou access) é enviada, uma resposta é esperada. Quando uma resposta não é recebida dentro do período de tempo limite (segundos):

radius [accounting] timeout 3

A solicitação é enviada novamente até o número de vezes especificado:

radius [accounting] max-retries 5

Isso significa que uma solicitação pode receber um total de máx-retries + 1 vezes até que desista do servidor radius específico que está sendo tentado. Nesse ponto, ele tenta a mesma sequência para o próximo servidor radius na ordem. Se cada um dos servidores tiver tentado max-retries + 1 vezes sem resposta, a chamada será rejeitada, supondo que não haja outra razão para falha até esse ponto.

Como sinônimo, há configuráveis que permitem que os usuários tenham acesso mesmo se a autenticação e a contabilidade falharem devido a intervalos para todos os servidores, embora uma implantação comercial provavelmente não implementaria isso:

radius allow [accounting] authentication-down

Além disso, há configuráveis que podem limitar o número total absoluto de transmissões de uma solicitação específica em todos os servidores configurados, e esses são desativados por padrão:

radius [accounting] max-transmissions 256

Por exemplo, se for definido como = 1, mesmo que haja um servidor secundário, ele nunca será tentado porque apenas uma tentativa de configuração de um assinante específico é tentada.

show task resources facility aaamgr all

Cada processo aaamgr é emparelhado e "trabalha para" um processo associado do sessmgr (responsável pelo tratamento geral de chamadas) e está localizado em um diferente Packet Services Card (PSC) ou Data Processing Card (DPC), mas usando o mesmo ID de instância. Também neste exemplo de saída observe a instância especial do aaamgr 231 em execução no SMC (System Management Card) para ASR 5000 (ou placa de entrada de gerenciamento para ASR 5500 (MIO)) que NÃO processa solicitações de assinantes, mas é usada para comandos de teste de raio (consulte a seção posterior para obter mais detalhes sobre isso) E para o processamento de login CLI do operador.

Neste trecho, o aaamgr 107, localizado em PSC 13, é responsável pelo tratamento de todo o processamento de RADIUS para o sessmgr 107 emparelhado localizado em PSC 1. Os problemas de acessibilidade para o aaamgr 107 afetam as chamadas no sessmgr 107.

```
                  task   cputime       memory     files     sessions
cpu facility     inst used allc   used alloc used allc used allc S status
----------------------- --------- ------------ --------- ------------ -----
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
```

No exemplo a seguir, observe que os problemas com o aaamgr 92 estão afetando o sessmgr emgr emparelhado tão facilmente visto quando comparado a outros sessmgrs com relação às contagens de sessão:

```
                   task   cputime        memory     files      sessions
cpu facility      inst used allc   used  alloc used allc  used  allc S status
----------------------- --------- ------------ --------- ------------ ------
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 <aaamgr #>] | resumo}

O comando número um com o qual se familiarizar são as variedades de "show radius counters"

Esse comando reporta vários contadores úteis para a solução de problemas de raio. O comando "show radius counters all" é muito valioso para rastrear o sucesso e as falhas em uma base de servidor, e é importante entender o significado dos vários contadores que compõem esse comando, pois ele pode não ser óbvio. O comando é sensível ao contexto e, portanto, deve ser executado no mesmo contexto em que os grupos aaa estão definidos.

Nota importante: Durante um período de tempo não monitorado, é difícil tirar conclusões dos contravalores ou das relações entre os contadores. Para tirar conclusões precisas, a melhor abordagem é redefinir os contadores e monitorá-los durante um período em que o problema que está sendo solucionado está ocorrendo.

Na saída a seguir, observe "Access-Request Sent" = 1, enquanto "Access-Request Retried" = 3. Portanto, qualquer nova solicitação a um determinado servidor radius é contada apenas uma vez, e todas as novas tentativas são contadas separadamente. Nesse caso, é um total de 3 + 1 = 4 solicitações de acesso enviadas. Observe o contador "Access-Request Timeouts" = 1. Um único tempo limite ocorre somente quando TODAS as novas tentativas falham, portanto, nesse caso, 3 novas tentativas sem uma resposta resultam em 1 Tempo limite (não 4). Isso acontece em todos

os servidores configurados até que haja sucesso ou todas as tentativas tenham falhado. Preste atenção aos contadores que são rastreados para cada servidor separadamente. Aqui está um exemplo disso, onde:

```
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
```

Observe também que os tempos limite NÃO são contados como falhas, o resultado é que o número de Access-Accept recebido e Access-Reject recebidos não serão adicionados à Solicitação de Acesso Enviada se houver algum tempo limite.

A análise desses contadores pode não ser completamente direta. Por exemplo, para o protocolo de IP Móvel (MIP), como as autenticações estão falhando, não há Resposta de Registro de MIP (RRP) sendo enviada e o celular pode continuar iniciando novas Solicitações de Registro de MIP (RRQ) porque não recebeu um RRP de MIP. Cada novo MIP RRQ faz com que o PDSN envie uma nova solicitação de Autenticação que pode ter sua própria série de novas tentativas. Isso pode ser visto no campo Id na parte superior de um rastreamento de pacote - é exclusivo para cada conjunto de novas tentativas. O resultado é que os contadores para Enviado, Retentado e Tempo Limite podem ser muito superiores ao esperado para o número de chamadas recebidas. Há uma opção que pode ser habilitada para minimizar essas novas tentativas extras e ela pode ser definida no serviço Agente Externo (FA) (mas não no Agente Doméstico (HA)): "authentication mn-aaa <6 options here> otimize-retries"

Alguns outros contadores úteis:

"Resposta de solicitação de acesso ignorada" - ocorre se a chamada não é configurada enquanto espera respostas para solicitações de autenticação.

"Access-Request Response Last Round Trip Time" (Resposta à solicitação de acesso em tempo de viagem da última rodada) - indica qualquer atraso entre os endpoints, embora obviamente não indique onde o atraso pode estar.

"Falha Consecutiva Atual de Solicitação de Acesso em um gerente" refere-se ao que foi discutido na primeira seção sobre disparadores para armadilhas AAA Inalcançáveis. Representa o(s) aaamgr(s) com a maior contagem de intervalos consecutivos.

"Acesso Atual/Solicitação de Contabilidade na Fila" indica solicitações que não estão sendo respondidas e permanecem na fila (a contabilidade permite uma compilação da fila indefinidamente enquanto a autenticação não o faz)

O cenário mais comum observado quando AAA Inalcançável é relatado é que os tempos limite de acesso e/ou quedas de resposta também estão ocorrendo, enquanto as Respostas de acesso não estão acompanhando as solicitações.

Se estiver disponível acesso ao modo de suporte técnico privilegiado, uma investigação mais detalhada pode ser feita no nível de instância do aaamgr para determinar se uma ou mais aaamgrs específicos são a causa do aumento geral das contagens "ruins". Por exemplo, procure por aaamgrs localizados em um PSC/DPC específico com altas contagens ou talvez um único aaamgr ou aaamgrs aleatórios com problemas - procure padrões. Se todos ou a maioria dos aaamgrs estiverem tendo problemas, há uma maior probabilidade de a causa raiz ser externa ao chassi OU manifestar-se em larga escala no chassi. Nesse caso, devem ser efetuados controlos sanitários gerais.

Aqui está um exemplo de saída que mostra um problema com um aaamgr específico para contabilidade. (O problema acabou sendo um bug em um firewall entre o ASR5K e o servidor RADIUS que estava bloqueando o tráfego de uma porta específica de instância do aaamgr (114).) Em um período de três semanas, apenas 48 respostas foram recebidas, mas mais de 100.000 timeouts ocorreram (e isso não inclui retransmissões).

```
[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
```

Concluindo, determine quais contadores estão aumentando, para quais servidores e em que velocidade.

show session subsistema facility {aaamgr | sessmgr} {all | instância <instance #>}

Embora esteja além do escopo deste artigo para examinar toda a saída supérflua desse comando, alguns exemplos merecem ser vistos. Como qualquer outra solução de problemas, a comparação da saída entre o que se acredita ser bom versus instâncias ruins do aaamgr geralmente revela diferenças óbvias nos valores relatados. Isso pode ser refletido no número total de solicitações, taxa de falha/sucesso, auth cancelada, etc. Como lembrete, certifique-se de limpar o subsistema da sessão (uma instância não pode ser removida, todas devem ser limpas) para eliminar qualquer histórico que possa fornecer uma imagem em nuvem do estado atual.

Continuando com o mesmo problema mencionado anteriormente no que diz respeito a um único aaamgr não responsável pela contabilidade, aqui está a saída de um nó diferente com esse mesmo problema, exceto uma instância de sessmr 36 diferente. Observe todos os campos interessantes para o aaamgr com falha e como esses valores aumentam com o tempo com as duas capturas do comando. Enquanto isso, a saída da instância 37 é mostrada como um exemplo de um aaamgr em funcionamento.

```
[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 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 gtpp charg                    0 Current gtpp charg
       0 Total gtpp charg success            0 Total gtpp charg failure
       0 Total gtpp charg cancelled          0 Total gtpp charg purged
       0 Total gtpp sec charg                0 Total gtpp 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 gtpp charg                    0 Current gtpp charg
       0 Total gtpp charg success            0 Total gtpp charg failure
       0 Total gtpp charg cancelled          0 Total gtpp charg purged
       0 Total gtpp sec charg                0 Total gtpp 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
...
```

Também é necessário executar o comando show task resources para verificar se há contagens de sessão desiguais (coluna usada) entre todos os parâmetros. Se algum for encontrado, verifique os aaamgrs emparelhados para os sessmrs com este comando para ver se há algum campo fora de linha - se o problema é devido ao RADIUS então há uma boa chance de encontrar algo.

No exemplo de show task resources em uma seção anterior, houve uma contagem de sessão significativamente mais baixa no sessmgr 92, que foi emparelhada com aaamgr 92. A saída do subsistema show session mostra um aumento significativo no total de contadores max-notados e aaa auth purged e no número de contadores L max-notados atuais elevados. É possível usar o recurso grep ao vivo no chassi e/ou no Bloco de Notas++ ou em outro editor de pesquisa potente para analisar dados rapidamente. Execute o comando várias vezes para ver quais valores estão aumentando ou permanecendo elevados:

```
[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

Um Ping ICMP testa a conectividade básica para ver se o servidor AAA pode ser alcançado ou não. O ping pode precisar ser originado com a palavra-chave src dependendo da rede e precisa ser feito do contexto AAA para ter valor. Se o ping para o servidor falhar, tente fazer ping nos elementos intermediários incluindo o endereço do próximo salto no contexto, confirmando que há uma entrada ARP para o endereço do próximo salto se o ping falhar. O traceroute também pode ajudar com problemas de roteamento.

```
[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> | todos | server <IP> port <port>} <username> <password>

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

Com acesso aos comandos do Teste de suporte técnico, é possível testar ainda mais se um aaamgr específico consegue alcançar qualquer servidor RADIUS. Para um teste básico de conectividade RADIUS, independente de qualquer instância específica do aaamgr, use a versão genérica desse comando que não especifica nenhum número de instância específico, mas usa a instância de gerenciamento por padrão. Se isso falhar, poderá apontar para uma questão mais ampla, independentemente de casos específicos.

Este comando envia uma solicitação de autenticação básica ou uma **inicialização** e **parada de** relatório e espera uma resposta. Para autenticação, use qualquer nome de usuário e senha, caso em que uma resposta de rejeição seria esperada, confirmando que o RADIUS está funcionando como projetado, ou que um nome de usuário/senha de trabalho conhecido pode ser usado, caso em que uma resposta de aceitação deve ser recebida

Aqui está um exemplo de saída do protocolo de monitor e a execução da versão de autenticação do comando em um chassi de laboratório:

```
[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-vsa1
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-vsa1
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
```

Aqui está um exemplo de um chassi ao vivo:

```
<<<<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=custom150
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
```

Aqui está um exemplo de saída da execução da versão contábil do comando. Não é necessária uma senha.

```
[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-vsa1
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-vsa1 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-vsa1 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-vsa1 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
```

A saída a seguir é para a mesma instância 36 do aaamgr que acabou de ser mencionada onde a conectividade com um servidor de contabilidade RADIUS específico é interrompida:

```
[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 | todos}

Esse comando relata o ID de fluxo da NPU (Network Processor Unit, unidade de processador de rede) e a porta UDP usadas pelo endereço IP NAS configurado para se conectar a servidores RADIUS. Isso é relatado na seção padrão do grupo aaa da saída. Certamente, o número da porta pode ser útil se for necessário combinar pacotes RADIUS em uma captura de pacote com um número de instância específica do aaamgr. (Observe que os fluxos de NPU são complicados e

não algo discutido neste artigo, mas uma entidade que um engenheiro de suporte poderia investigar mais a fundo.) Ele também rastreia solicitações pendentes para o servidor. No mesmo exemplo de problema usado neste artigo, apenas um par de portas IP / UDP de servidor RADIUS **<==>** NAS falhou conforme destacado.

```
[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>
```

assinante de monitor

O assinante do monitor pode ser usado para determinar se a autenticação está pelo menos sendo tentada e se uma resposta está sendo processada para as chamadas monitoradas. Ative a opção 'S', que significa Sessmgr Sender Info (Informações do remetente do Sessmgr) - gerando relatórios eficazes sobre o número de instância do sessmgr ou aaamgr que está tratando a mensagem em questão. Aqui está um exemplo de uma chamada MIP em um HA anexando às

instâncias do sessmgr / aaamgr 132.

```
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
```

Há um exemplo de falha no final deste artigo também.

Captura do pacote

Às vezes, não há informações suficientes no ASR para determinar por que problemas de acessibilidade estão ocorrendo, caso em que uma captura de pacote será necessária. Ao solucionar problemas de assinantes individuais, a identificação dos respectivos pacotes em um rastreamento deve ser fácil. Caso contrário, saber que a porta UDP está sendo usada em uma das extremidades de uma determinada instância do aaamgr # **<=>>** par de servidores RADIUS pode ser útil se o problema estiver ligado a portas/instâncias específicas do aaamgr. Tentar capturar em vários lugares da rede pode ser necessário para determinar onde os pacotes estão sendo descartados. No problema analisado em todo este artigo, foi uma captura de pacotes no lugar certo no caminho de transporte entre o ASR e o servidor RADIUS que foi a ruptura na solução do problema.

Correções

Esta última seção oferece algumas ideias para corrigir problemas de conectividade RADIUS. Eles não são apresentados em nenhuma ordem específica, mas simplesmente uma lista a ser considerada no processo de solução de problemas.

Se o servidor RADIUS estiver sendo sobrecarregado, a carga poderá ser diminuída através do valor (padrão 256) configurado para "radius (accounting) max-pending", que define um limite no número de solicitações pendentes (não atendidas) para qualquer processo aaamgr. Se o limite for atingido, os registros podem indicar o seguinte: "Falha ao atribuir ID de mensagem para o servidor de autenticação radius x.x.x.x:1812".

As mensagens RADIUS de limitação de taxa para servidores específicos também podem ajudar a reduzir a carga através da palavra-chave rate-limit para as respectivas linhas de configuração de servidor.

Às vezes, não é um problema de conectividade, mas de aumento do tráfego contábil, o que não é um problema com o RADIUS, mas aponta para outra área, como o aumento das renegociações de ppp, que estão causando mais iniciações e paradas de contabilidade. Assim, pode ser necessário solucionar problemas fora do RADIUS para encontrar uma causa ou um gatilho para os sintomas que estão sendo observados.

Se, durante o processo de solução de problemas, tiver sido decidido remover um servidor de autenticação radius ou tarifação da lista de servidores ao vivo por qualquer motivo, há um comando (não-config) que tirará um servidor do serviço indefinidamente até que seja desejado colocá-lo novamente em serviço. Esta é uma abordagem mais limpa do que ter que removê-la da configuração manualmente:

```
{disable | 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
```

A migração de PSC ou DPC ou a comutação da placa de linha podem, muitas vezes, resolver problemas devido ao fato de a migração resultar na reinicialização dos processos na placa, incluindo o bombeador que tem sido a causa de problemas de tempos em tempos no que diz

respeito aos fluxos de NPU.

Mas em uma reviravolta interessante com o exemplo acima de aaamgr 92, as falhas inalcançáveis da AAA realmente COMEÇARAM quando a migração da PSC foi feita. Isso foi desencadeado devido a um fluxo de NPU que estava faltando quando uma migração de PSC foi concluída, deixando o PSC 11 em standby. Quando ele foi ativado uma hora depois, o impacto real do fluxo ausente começou por aaamgr 92. Problemas como esse são muito difíceis de solucionar sem a assistência do Suporte Técnico.

```
[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
```

O problema foi temporariamente resolvido com um switchover de porta que fez com que a placa PSC que tinha um fluxo de NPU ausente para aaamgr 92 não fosse mais conectada a uma placa de linha ativa.

```
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
```

A última armadilha de falha:

```
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
```

Da mesma forma, reiniciar aaamgrs específicos que ficam "presos" também pode resolver problemas, embora esta seja uma atividade que o Suporte Técnico deve fazer, pois envolve comandos restritos de Suporte Técnico. No exemplo do aaamgr 92 apresentado na seção show task resources anteriormente, isso foi tentado, mas não ajudou porque a causa raiz não era o aaamgr 92, mas sim o fluxo de NPU ausente que o aaamgr 92 precisava (era um problema de

NPU, não um problema de aaamgr). Aqui está o resultado relevante da tentativa. "show task table" é executado para mostrar a associação da id do processo e da instância de tarefa nº 92.

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

Exemplo final

Aqui está um exemplo final de uma interrupção real em uma rede ativa que reúne muitos dos comandos e abordagens de solução de problemas discutidos neste artigo. Observe que esse nó lida com tipos de chamada 3G MIP e 4G Long Term Evolution (LTE) e High Rate Packet Data (eHRPD).

show snmp trap history

Somente pelas armadilhas, pode ser confirmado que o ponto de partida corresponde ao que o cliente relatou como UTC 19:25. À parte, observe que as armadilhas AAAAuthSvrUnreachable para o servidor primário 209.165.201.3 não começaram a acontecer até horas mais tarde (não está claro o porquê, mas é bom notar; mas a **contabilização inalcançável** para esse servidor foi iniciada imediatamente)

```
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

A saída mostra uma contagem muito menor de chamadas no DPC 8/1. Com base nisso, sem nenhuma análise adicional, uma PESSOA PODERIA sugerir que há um problema no DPC 8 e propor a opção de migrar para o DPC em espera. Mas é importante reconhecer o impacto real do assinante - nestes cenários, os assinantes geralmente se conectarão com êxito em uma tentativa subsequente e, portanto, o impacto não é muito significativo para o assinante e provavelmente não relatarão nada para o provedor, supondo que não haja paralisação do plano do usuário também ocorrendo (o que é possível dependendo do que está quebrado).

```
 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
```

assinante de monitor

Uma configuração de chamada foi detectada quando não houve resposta à solicitação de autenticação para o 209.165.201.3 primário para o sessmgr 242 em DPC 9/1, que por acaso tem seu aaamgr emparelhado residindo em DPC 8/1, confirmando falhas 3G devido a AAA inalcançável em 8/1. Também confirma que, embora não tenha havido nenhuma armadilha AAAAuthSrvUnreachable para 209.165.201.3 até esse momento, não significa que não haja um problema para lidar com respostas para esse servidor (como mostrado acima, as armadilhas começam mas horas depois).

```
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        : n/a                       MSISDN      : n/a
Username    : 6664600074@cisco.com      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

O que é interessante é que a contagem de sessões do sessmgr 242 é semelhante a outras sessões em funcionamento. Uma investigação mais profunda mostrou que as chamadas 4G, também hospedadas neste chassi, foram capazes de se conectar e, por isso, compensaram a falta de chamadas 3G Mobile IP que pudessem se conectar. Pode-se determinar que, ao recuar até 8 horas após a interrupção ter sido iniciada, não há chamadas MIP para este sessmgr 242, enquanto que, ao voltar 9 horas antes do início da interrupção, há chamadas conectadas:

```
[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
```

As chamadas LTE e eHRPD mostram uma taxa mais alta para chamadas MIP ao comparar avaliações conectadas a aaamgrs em funcionamento e quebrados:

```
[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 test instance X authentication server

Todos os aaamgrs em 8/1 estão mortos - nenhum comando radius test instance funciona para nenhum desses aaamgrs, mas funciona para aaamgrs em 8/0 e outras placas:

```
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

O comando principal para a solução de problemas de RADIUS mostra muitos intervalos que estão aumentando rapidamente:

```
[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
```

Correção

Durante as janelas de manutenção, uma migração de DPC de 8 a 10 resolveu o problema, as armadilhas AAAAuthSrvUnreachable pararam e o DPC 8 foi configurado como RMA e a causa raiz foi determinada como uma falha de hardware no DPC 8 (os detalhes dessa falha não são importantes para saber para os fins deste artigo).

```
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
```