Solución de problemas de trampas AAAAccSrvUnreachable y AAAAuthSrvUnreachable

Contenido

Introducción

Este artículo trata sobre cómo resolver problemas de trampas SNMP AAAAccSrvUnreachable y AAAAuthSrvUnreachable, que se activan debido a problemas de alcance con un servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) utilizado para autenticar suscriptores (o operadores que inician sesión en el nodo, pero eso no es lo que se está discutiendo aquí). Hay dos enfoques que se pueden utilizar para determinar cuándo se activará cualquiera de estas trampas. En este artículo se explica qué condiciones activan estas trampas y qué enfoques de resolución de problemas y recopilación de datos se pueden tomar para determinar la causa raíz y resolverlas. También se analizan algunas posibles medidas correctivas que pueden considerarse.

Tenga en cuenta que el RESULTADO de la inaccesibilidad será fallas de llamada o fallas de contabilización, del mismo modo que si las respuestas de RADIUS son rechazos en lugar de aceptaciones. Aunque la tasa de éxito/fallo (autenticación) se mide independientemente del tiempo de espera/alcance (hay trampas y alarmas para esto) y ciertamente puede ser analizada por derecho propio, el enfoque de este artículo estará en el problema de alcance y no en el problema de rechazo.

El ejemplo de salida del LAB y las entradas reales se utilizan en todo momento para ayudar a llevar a cabo las discusiones. Lo que parece ser direcciones IP públicas en este artículo son

direcciones **falsas**.

Activadores de trampa

Hay dos modelos/algoritmos/enfoques diferentes entre los que elegir para determinar el estado de un servidor RADIUS y cuándo probar un servidor diferente si se producen fallas:

Errores consecutivos en un enfoque de proceso de administración

El enfoque original y el que utilizan con más frecuencia los operadores implica el seguimiento del número de fallos que se han producido en una fila para un proceso de administración determinado. Un proceso aamgr es responsable de todo el procesamiento e intercambio de mensajes radius con un servidor radius, y muchos procesos aamgr existirán en un chasis, cada uno de ellos vinculado con procesos sessmgr (que son los principales procesos responsables del control de llamadas). (Ver todos los procesos aamgr con el comando "show task resources") Por lo tanto, un proceso aamgr en particular procesará los mensajes de RADIUS para muchas llamadas, no sólo una sola llamada, y este algoritmo implica el seguimiento de cuántas veces en una fila un proceso aamgr en particular ha fallado en obtener una respuesta a la misma solicitud que ha tenido que volver a enviar: un "tiempo de espera de solicitud de acceso" como se informa en "show radius counters".

El contador respectivo "Access-Request Current Consecutive Failure in a mgr", también de "show radius counters" se incrementa cuando esto ocurre, y el comando "show radius accounting (o authentication) servers detail" indica las marcas de tiempo del cambio de estado de radius de Activo a No Respondiendo (pero no se genera ninguna trampa o registros SNMP para una sola falla). Este es un ejemplo para la contabilidad de RADIUS:

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

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

Event History:
2008-Nov-28+23:18:36       Active
2008-Nov-28+23:18:57       Not Responding
```

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

Si este contador alcanza el valor configurado (Default = 4) sin ser reiniciado, por configurable: (tenga en cuenta que los corchetes [ ] se utilizan para indicar calificadores opcionales y, en estos casos, captura la contabilidad de resolución de problemas (la autenticación es el valor predeterminado si no se especifica la contabilidad)

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

A continuación, este servidor se marca como "Abajo" durante el período (minutos) configurado:

radius [accounting] deadtime 10

También se activa una trampa y registros SNMP, por ejemplo, para la autenticación y/o contabilidad 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
```

Las trampas indican el servidor inalcanzable. Tenga en cuenta cualquier patrón. Por ejemplo, ¿ocurre con un servidor u otro o con todos los servidores, y cuál es la frecuencia de rebote? ¿Se está produciendo de forma continua u ocasional?

Tenga en cuenta también que todo lo que hace falta para que se active esta trampa es que uno de los administradores falle, por lo que la parte complicada de esta trampa es que no indica el alcance del problema. Podría ser muy extenso o muy minoir - que depende del operador determinar, y los enfoques para entender que se discuten en este artículo.

show snmp trap statistics informará el número de veces que se ha disparado desde el inicio, incluso si las trampas más antiguas se han eliminado desde hace mucho tiempo. Este ejemplo muestra un problema de contabilidad inalcanzable:

```
[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
```

Tenga en cuenta que el aaamgr informado en el ejemplo anterior es #231. Se trata del administrador de administración de ASR 5000 que reside en la tarjeta de administración del sistema (SMC). Lo que es engañoso en este resultado es que cuando un administrador o un amamgrs individual experimenta problemas de alcance, el número de instancia informado en los registros es la instancia de administración de aamgr y no las instancias particulares que experimentan el problema. Esto se debe al hecho de que si muchos casos experimentan problemas de accesibilidad, el registro se llenaría rápidamente si se informara de ellos como tales, por lo que el diseño ha sido informar genéricamente sobre la instancia de administración, que si no se sabe esto, ciertamente sería engañoso. En la sección de resolución de problemas se proporcionarán más detalles sobre cómo determinar qué administradores fallan. A partir de algunas versiones de StarOS 17 y v18+, este comportamiento se ha cambiado de modo que el número de instancia de administrador correspondiente con problemas de conectividad (según se informa en trampas SNMP) se informe en los registros con la ID determinada (Cisco CDETS CSCum84773), aunque sólo se informa de la primera aparición de este hecho (en varios casos).

El administrador de aamgr es el número máximo de instancia de sessmgr + 1, y así en un ASR 5500 es 385 para la tarjeta de procesamiento de datos (DPC) o 1153 (para DPC 2).

Como cliente adicional, la administración de aamgr es responsable de gestionar los inicios de sesión de operador/administrador, así como de gestionar los cambios en las solicitudes de autorización iniciadas desde los propios servidores RADIUS.

Continuando, el comando "show radius accounting (o authentication) servers detail" indicará las marcas de tiempo de los cambios de estado en Down que corresponden a las trampas/registros (recordatorio: No responder definido anteriormente es sólo un único administrador que obtiene un tiempo de espera, mientras que Down es un único administrador que obtiene suficientes tiempos de espera consecutivos por configuración para activar Down)

```
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
```

Si sólo hay un servidor configurado, no se demarca, ya que sería esencial para una configuración correcta de la llamada.

Vale la pena mencionar que hay otro parámetro que se puede configurar en la línea de configuración detect-dead-server llamada "response-timeout". Cuando se especifica, un servidor se marca solamente cuando se cumplen las condiciones consecutivas de fallas y de tiempo de espera de respuesta. El tiempo de espera de respuesta especifica un período de tiempo durante el cual NO se reciben respuestas a TODAS las solicitudes enviadas a un servidor determinado. (Tenga en cuenta que este temporizador se restablecería continuamente a medida que se reciban las respuestas.) Esta condición se esperaría cuando un servidor o la conexión de red están completamente inactivos, frente a parcialmente comprometidos o degradados.

El caso práctico para esto sería un escenario en el que una ráfaga de tráfico provoca que se activen los fallos consecutivos, pero no se desea marcar un servidor inmediatamente como resultado. Por el contrario, el servidor solo se demarca después de que transcurra un período de tiempo específico en el que no se recibe ninguna respuesta, lo que representa de forma efectiva la verdadera falta de disponibilidad del servidor.

Este método que se acaba de discutir sobre el control de los cambios en las máquinas de estado de RADIUS depende de observar todos los procesos de administración y encontrar uno que active la condición de los reintentos fallidos. Este método está sujeto en cierto grado a alguna aleatoriedad de fallas, por lo que puede no ser el algoritmo ideal para detectar fallas. Pero es especialmente bueno encontrar a los administradores que están rotos mientras que todos los demás están funcionando bien.

Enfoque Keepalive

Otro método para detectar el alcance del servidor RADIUS es utilizar mensajes de prueba de keepalive ficticios. Esto implica el envío constante de mensajes de radio falsos en lugar de monitorear el tráfico en vivo. Otra ventaja de este método es que siempre está activo, frente a los fallos consecutivos en un enfoque de administración, donde podría haber periodos en los que no se envía tráfico de radio, por lo que no hay manera de saber si existe un problema durante esos tiempos, lo que resulta en una detección retardada cuando los intentos comienzan a ocurrir. Además, cuando se marca un servidor, estas señales de mantenimiento se siguen enviando para que el servidor pueda ser marcado lo antes posible. La desventaja de este enfoque es que se pierden los problemas que están vinculados a instancias de administración específicas que pueden estar experimentando problemas porque utiliza la instancia de administración de aaamgr para los mensajes de prueba.

A continuación se indican los diversos parámetros de configuración relevantes para este enfoque:

```
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
```

El comando "radius (accounting) detect-dead-server keepalive" activa el enfoque "keep-alive" en lugar de las fallas consecutivas en un enfoque de aaamgr. En el ejemplo anterior, el sistema envía un mensaje de prueba con el nombre de usuario Test-Username y la contraseña Test-Username cada 30 segundos, y lo reintenta cada 3 segundos si no se recibe respuesta, y lo reintenta hasta 3 veces, después de lo cual marca el servidor inactivo. Una vez que obtiene su

primera respuesta, la marca de nuevo.

A continuación se muestra un ejemplo de solicitud/respuesta de autenticación para la configuración anterior:

```
<<<<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
```

Las mismas trampas SNMP se utilizan para significar los estados de radio inalcanzable/descendente y alcanzable/ascendente como con las fallas consecutivas en un enfoque de aamgr:

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

"show radius counters all" tiene una sección para realizar un seguimiento de las solicitudes de keepalive para autenticación y contabilidad también - aquí están los contadores de autenticación:

```
   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
```

Resolución de problemas de comandos/enfoques

Ahora que se ha explicado el disparador de trampas AAA inalcanzables, el siguiente paso es entender los diversos comandos de troubleshooting que se utilizan para determinar el impacto e intentar averiguar la causa raíz. La inaccesibilidad es un término muy amplio. No explica dónde se encuentra la inaccesibilidad: en la red, en el servidor o en el ASR. Por ejemplo, ¿se sabe si las solicitudes se enviaron siquiera en primer lugar? ¿El servidor recibió las solicitudes? ¿Respondió a las solicitudes? ¿Las respuestas volvieron a llegar al ASR y, en caso afirmativo, se procesaron o se descartaron en la ruta interna (es decir, los flujos)? En esta sección se intenta abordar cómo responder a estas preguntas.

Aspectos básicos de la configuración de Radius

Primero, hay algunos conceptos básicos con los que uno debe estar familiarizado con respecto a la configuración RADIUS. La mayor parte de la configuración para RADIUS está en un grupo con nombre específico, y todos los contextos tienen un grupo predeterminado que se puede configurar de la siguiente manera. Muchas veces las configuraciones tendrán sólo un grupo, el grupo predeterminado.

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

Si se utilizan grupos aaa con nombre específicos, se señalan con la siguiente instrucción configurada en un perfil del suscriptor o en el nombre del punto de aplicación (APN) (en función de la tecnología de control de llamadas), por ejemplo:

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

Nota: El sistema verifica primero el grupo aaa específico asignado al suscriptor y, a continuación, verifica el valor predeterminado del grupo aaa para las configuraciones adicionales no definidas en el grupo específico.

Estos son comandos útiles que resumen todos los valores asignados a todos los configurables en las diversas configuraciones de grupo aaa. Esto permite ver rápidamente todos los valores configurables, incluidos los valores predeterminados, sin tener que examinar la configuración manualmente y, posiblemente, ayuda a evitar errores al asumir ciertas configuraciones. Estos comandos informan en todos los contextos:

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

Lo más importante que se puede configurar es, por supuesto, los propios servidores de acceso y contabilidad radius. Aquí tiene un ejemplo:

```
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 la función max-rate que limita el número de solicitudes enviadas al servidor por administrador por segundo

Además, también es necesario definir la dirección IP de NAS, que es la dirección IP en una interfaz en el contexto desde el cual se envían las solicitudes de RADIUS y se reciben las respuestas. Si no se define, las solicitudes no se envían y los seguimientos de los suscriptores de supervisión no pueden publicar un error obvio (no se envían solicitudes radius ni se indica el motivo).

radius attribute nas-ip-address address dirección 10.211.41.129

Tenga en cuenta que, debido a que la autenticación y la contabilización suelen ser manejadas por el mismo servidor, se utiliza un número de puerto diferente para diferenciar el tráfico de autenticación frente al tráfico de contabilización en el servidor RADIUS. Para el lado ASR5K, el número de puerto de origen UDP NO se especifica y el chasis lo elige de forma similar (más en esto más adelante).
Normalmente, se especifican varios servidores de acceso y contabilidad para fines de redundancia. Se puede configurar un ordenamiento cíclico o un orden de prioridad:

algoritmo {first-server de RADIUS [accounting] | ordenamiento cíclico}

La opción de primer servidor da como resultado que TODAS las solicitudes se envíen al servidor con la prioridad más baja numerada. Sólo cuando se producen errores de reintento o, peor aún, se demarca un servidor, se intenta el servidor con la siguiente prioridad. Más sobre esto a continuación.

Cuando se envía una solicitud de RADIUS (contabilidad o acceso), se espera una respuesta. Cuando no se recibe una respuesta dentro del período de tiempo de espera (segundos):

radius [accounting] timeout 3

La solicitud se envía hasta el número de veces especificado:

radius [accounting] max-retries 5

Esto significa que una solicitud puede enviarse un total de reintentos máximos + 1 veces hasta que se detenga en el servidor RADIUS concreto que se está probando. En este punto, intenta la misma secuencia al siguiente servidor RADIUS en orden. Si se ha intentado cada uno de los servidores con reintentos máximos + 1 veces sin respuesta, se rechaza la llamada, suponiendo que no haya otra razón para la falla hasta ese momento.

Como usuario adicional, hay configurables que permiten a los usuarios tener acceso incluso si la autenticación y la contabilidad fallan debido a los tiempos de espera de todos los servidores, aunque una implementación comercial probablemente no implementaría esto:

RADIUS allow [accounting] authentication-down

Además, hay configurables que pueden limitar el número total absoluto de transmisiones de una

solicitud determinada a través de todos los servidores configurados, y éstas están desactivadas de forma predeterminada:

radius [accounting] max-transmission 256

Por ejemplo, si esto se configura = 1, entonces incluso si hay un servidor secundario, nunca se intenta porque sólo se intenta un intento de configuración específica de un suscriptor.

show Task Resources Facility aaamgr all

Cada proceso de aamgr se empareja con un proceso de sessmgr asociado (responsable de la gestión general de llamadas) y funciona con él, y se encuentra en una tarjeta de servicios de paquetes (PSC) o una tarjeta de procesamiento de datos (DPC) diferentes, pero con la misma ID de instancia. También en este ejemplo, observe la instancia especial de aamgr 231 que se ejecuta en la tarjeta de administración del sistema (SMC) para ASR 5000 (o tarjeta de salida de entrada de administración para ASR 5500 (MIO)) que NO procesa las solicitudes de suscriptores pero se utiliza para los comandos de prueba de radius (consulte la sección posterior para obtener más detalles al respecto) Y para el procesamiento de inicio de inicio de sesión de operador CLI.

En este fragmento, aamgr 107 ubicado en PSC 13 es responsable de manejar todo el procesamiento RADIUS para el sessmgr 107 emparejado ubicado en PSC 1. Los problemas de disponibilidad para aamgr 107 afectan a las llamadas en 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
```

En el siguiente ejemplo, observe que los problemas con aamgr 92 están afectando al sessmgr emparejado como se puede ver fácilmente en comparación con otros sessmgrs con respecto a los recuentos de sesiones:

```
                   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 #>] | summary}

El comando número uno con el que debe estar familiarizado son las variedades de "show radius counters"

Este comando reporta muchos contadores útiles para resolver problemas de RADIUS. El comando "show radius counters all" es muy valioso para hacer un seguimiento de los éxitos y las fallas en el servidor, y es importante entender el significado de los diversos contadores que componen este comando, ya que puede que no sea obvio. El comando es sensible al contexto y

por lo tanto debe ejecutarse en el mismo contexto donde se definen los grupos aaa.

Nota importante: Durante un período de tiempo no supervisado, es difícil extraer conclusiones de los valores de los contadores o de las relaciones entre los contadores. Para llegar a conclusiones precisas, el mejor enfoque es restablecer los contadores y supervisarlos durante un período de tiempo en el que se produce el problema.

En el siguiente resultado, observe "Access-Request Sent" = 1, mientras que "Access-Request Retried" = 3. Por lo tanto, cualquier nueva solicitud dada a un servidor RADIUS en particular se cuenta sólo una vez y todos los reintentos se cuentan por separado. En este caso, se trata de un total de 3 + 1 = 4 solicitudes de acceso enviadas. Observe el contador "Tiempo de espera de solicitud de acceso" = 1. Un único tiempo de espera se produce solamente cuando TODOS los reintentos fallan, por lo que en este caso, 3 reintentos sin respuesta dan como resultado 1 tiempo de espera (no 4). Esto sucede en todos los servidores configurados hasta que se produce el éxito o todos los intentos han fallado. Por lo tanto, preste atención a los contadores que se siguen para cada servidor por separado. A continuación se muestra un ejemplo de esto, donde:

```
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
```

Tenga en cuenta también que los tiempos de espera NO se cuentan como fallos, por lo que el número de Access-Accept recibidos y Access-Reject recibidos no se sumará a Access-Request Sent (Solicitud de acceso enviada) si hay algún tiempo de espera.

Es posible que el análisis de estos contadores no sea completamente sencillo. Por ejemplo, para

el protocolo Mobile IP (MIP), dado que las autenticaciones fallan, no se envía ninguna respuesta de registro de MIP (RRP) y el móvil puede continuar iniciando nuevas solicitudes de registro de MIP (RRQ) porque no ha recibido un RRP de MIP. Cada nuevo RRQ MIP hace que el PDSN envíe una nueva solicitud de autenticación que puede tener su propia serie de reintentos. Esto se puede ver en el campo Id de la parte superior de un seguimiento de paquetes; es único para cada conjunto de reintentos. El resultado es que los contadores de Enviados, Retirados y Tiempo de Espera pueden ser mucho mayores de lo esperado para el número de llamadas recibidas. Hay una opción que se puede habilitar para minimizar estos reintentos adicionales y se puede establecer en el servicio Foreign Agent (FA) (pero no en Home Agent (HA)): "authentication mn-aaa <6 choice here> optimice-retries"

Otros contadores útiles:

"Respuesta de solicitud de acceso descartada": se produce si la llamada no se configura mientras se espera la respuesta a las solicitudes de autenticación.

"Tiempo de último viaje de ida y vuelta de respuesta de solicitud de acceso": indica cualquier retraso entre los terminales, aunque obviamente no indicaría dónde podría estar el retraso.

"Access-Request Current Consecutive Failure in a mgr" se relaciona con lo que se discutió en la primera sección sobre los desencadenadores de trampas AAA inalcanzables. Representa los administradores con el mayor número de tiempos de espera consecutivos.

"Current Access/Accounting-Request Queued" (Acceso actual/Solicitud de contabilidad en cola) indica las solicitudes que no se están respondiendo y que permanecen en cola (la contabilización permite una acumulación de cola indefinidamente mientras que la autenticación no lo hace)

El escenario más común que se observa cuando se informa de AAA Unreachable es que también se producen tiempos de espera de acceso y/o caídas de respuesta, mientras que las respuestas de acceso no están a la altura de las solicitudes.

Si se dispone de acceso al modo de soporte técnico privilegiado, se puede realizar una investigación adicional en el nivel de instancia de aamgr para determinar si uno o más tipos específicos son la causa del aumento en los recuentos "malos" generales. Por ejemplo, busque los administradores que se encuentran en un PSC/DPC específico con recuentos altos o quizás un solo administrador o aleatorios que tengan problemas: busque patrones. Si todos o la mayoría de los administradores tienen problemas, existe una mayor probabilidad de que la causa raíz sea externa al chasis O que manifieste una gran escala en el chasis. En tal caso, deben realizarse controles sanitarios generales.

A continuación se muestra un ejemplo de resultado que muestra un problema con un administrador específico para la contabilidad. (El problema resultó ser un error de funcionamiento en un firewall entre el ASR5K y el servidor RADIUS que estaba bloqueando el tráfico de un puerto específico de instancia de administración (114). En un período de tres semanas, solo se han recibido 48 respuestas, pero se han producido más de 100 000 tiempos de espera (y eso no incluye retransmisiones).

```
[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
```

En conclusión, determine qué contadores están aumentando, para qué servidores y a qué velocidad.

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

Si bien está fuera del alcance de este artículo examinar todos los resultados superfluos de este comando, vale la pena mirar un par de ejemplos. Como cualquier otra solución de problemas, la comparación del resultado entre lo que se cree que es bueno o malo, a menudo revela diferencias obvias en los valores notificados. Esto podría reflejarse en el número total de solicitudes, la tasa de fallos/éxito, la autenticación cancelada, etc. Como recordatorio, asegúrese de borrar el subsistema de sesión (una instancia no puede ser despejada, todas deben ser borradas) para eliminar cualquier historial que pueda proporcionar una imagen en nube del estado actual.

Continuando con el mismo problema mencionado anteriormente con respecto a un solo administrador que falla en la contabilización, aquí se muestra el resultado de un nodo diferente con ese mismo problema excepto una instancia de sessmr diferente 36. Observe todos los campos interesantes para el administrador que falla y cómo esos valores aumentan con el tiempo con las dos capturas del comando. Mientras tanto, la salida de la instancia 37 se muestra como un ejemplo de un administrador de trabajo.

```
[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
...
```

También se deben ejecutar show task resources para comprobar si hay recuentos de sesiones desiguales (columna usada) entre todos los sessmgrs. Si se encuentra alguno, verifique los indicadores emparejados para esos sessmrs con este comando para ver si hay campos que están fuera de línea - si el problema se debe a RADIUS entonces hay una buena oportunidad de

encontrar algo.

En el ejemplo de recursos de tareas show de una sección anterior, hubo un conteo de sesiones significativamente menor en sessmgr 92 que se emparejó con aamgr 92. El resultado del subsistema show session muestra un aumento significativo en los contadores purgados total max-extraordinario y aaa auth, y los contadores actuales máximos sobresalientes elevados. Se puede utilizar la función grep en vivo en el chasis y/o Notepad++ u otro potente editor de búsqueda para analizar rápidamente los datos. Ejecute el comando varias veces para ver qué valores están aumentando o siguen siendo 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

Un ping ICMP prueba la conectividad básica para ver si se puede alcanzar o no el servidor AAA. Es posible que el ping deba originarse con la palabra clave src dependiendo de la red y que se deba hacer desde el contexto AAA para tener valor. Si falla el ping al servidor, intente hacer ping a los elementos intermediarios, incluida la dirección del siguiente salto en el contexto, confirmando que hay una entrada ARP a la dirección del siguiente salto si falla el ping. Traceroute también puede ayudar con los problemas de ruteo.

```
[source]CSE2# ping 192.168.50.200
PING 192.168.50.200 (192.168.50.200) 56(84) bytes of data.
64 bytes from 192.168.50.200: icmp_seq=1 ttl=64 time=0.411 ms
64 bytes from 192.168.50.200: icmp_seq=2 ttl=64 time=0.350 ms
64 bytes from 192.168.50.200: icmp_seq=3 ttl=64 time=0.353 ms
64 bytes from 192.168.50.200: icmp_seq=4 ttl=64 time=0.321 ms
64 bytes from 192.168.50.200: icmp_seq=5 ttl=64 time=0.354 ms

--- 192.168.50.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.321/0.357/0.411/0.037 ms
```

RADIUS Test instance x auth {radius group <group> | all | server <IP> port <port>} <username> <password>

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

Con el acceso a los comandos Tech Support Test, se puede probar más a fondo si un administrador específico puede alcanzar cualquier servidor RADIUS. Para una prueba de conectividad RADIUS básica, independientemente de cualquier instancia de aamgr específica, utilice la versión genérica de este comando que no especifica ningún número de instancia específico pero utiliza la instancia de administración de forma predeterminada. Si esto falla, entonces puede apuntar a un problema más amplio independientemente de instancias específicas.

Este comando envía una solicitud de autenticación básica o **solicitudes de inicio** de contabilización y **detención** y espera una respuesta. Para la autenticación, utilice cualquier nombre de usuario y contraseña, en cuyo caso se esperaría una respuesta de rechazo, confirmando que RADIUS funciona como está diseñado, o se podría utilizar un nombre de usuario/contraseña que funcione, en cuyo caso se debería recibir una respuesta de aceptación

A continuación se muestra un ejemplo de salida del protocolo monitor y de la ejecución de la versión de autenticación del comando en un chasis de laboratorio:

```
[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
```

Este es un ejemplo de un chasis activo:

```
<<<<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
```

A continuación se muestra un ejemplo de salida de la ejecución de la versión de contabilidad del comando. No se necesita una contraseña.

```
[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
```

El siguiente resultado es para la misma instancia de aaamgr 36 que se acaba de mencionar donde se interrumpe la conectividad con un servidor de contabilización RADIUS específico:

```
[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 | all}

Este comando informa del ID de flujo de la unidad del procesador de red (NPU) y del puerto UDP que utiliza la dirección IP NAS configurada para conectarse a los servidores RADIUS. Esto se informa en la sección predeterminada del grupo aaa del resultado. Ciertamente, el número de puerto puede ser útil si se necesita hacer coincidir los paquetes RADIUS en una captura de paquetes con un número de instancia específico de un administrador. (Tenga en cuenta que los flujos de NPU son complicados y no se tratan en este artículo, sino una entidad que un ingeniero de soporte podría investigar más.) También realiza un seguimiento de las solicitudes pendientes al servidor. En el mismo problema de ejemplo utilizado a lo largo de este artículo, sólo un par de puertos RADIUS **<=>** NAS IP/UDP específico del servidor RADIUS ha fallado como se destacó.

```
[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>
```

suscriptor de monitor

El suscriptor monitor se puede utilizar para determinar si se intenta al menos la autenticación y si se procesa una respuesta para las llamadas que se supervisan. Active la opción 'S' que significa Información del remitente de Sessmgr: informa de forma efectiva sobre el sessmgr o el número de instancia de aamgr que está manejando el mensaje en cuestión. Este es un ejemplo de una llamada MIP en un HA adjuntar a instancias de 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
```

También hay un ejemplo de falla al final de este artículo.

Captura de paquete

A veces no hay suficiente información sobre el ASR para determinar por qué se producen problemas de alcance, en cuyo caso será necesaria una captura de paquetes. Al resolver problemas de suscriptores individuales, identificar los paquetes respectivos en un seguimiento debe ser fácil. De lo contrario, conocer el puerto UDP que se utiliza en cualquiera de los extremos de un par de servidores RADIUS de instancia de aamgr determinado # **<=>** podría ser útil si el problema está ligado a puertos/instancias de aamgr específicos. Es posible que sea necesario intentar capturar varios lugares de la red para determinar dónde se descartan los paquetes. En el tema que se analiza a lo largo de este artículo, fue una captura de paquetes en el lugar adecuado en la trayectoria de transporte entre el ASR y el servidor RADIUS lo que constituyó la ruptura para resolver el problema.

Remediaciones

Esta última sección ofrece algunas ideas para solucionar los problemas de conectividad RADIUS. Estos no se presentan en un orden concreto, sino simplemente en una lista que se debe tener en cuenta en el proceso de resolución de problemas.

Si el servidor RADIUS se sobrecarga, la carga podría reducirse a través del valor (predeterminado 256) configurado para "radius (accounting) max-pending", que establece un límite en el número de solicitudes pendientes (sin responder) para cualquier proceso de aamgr dado. Si se alcanza el límite, los registros pueden indicar lo siguiente: "No se pudo asignar el id de mensaje para el servidor de autenticación radius x.x.x.x:1812".

Los mensajes RADIUS de limitación de velocidad a servidores específicos también pueden ayudar a reducir la carga a través de la palabra clave rate-limit para las líneas de configuración del servidor respectivo.

A veces no se trata de un problema de conectividad, sino de aumento del tráfico de contabilización, que no es un problema con RADIUS persay, sino que apunta a otro área, como el aumento de las renegociaciones ppp que están causando más inicios y paradas de contabilización. Por lo tanto, es posible que sea necesario resolver problemas fuera de RADIUS para encontrar una causa o un disparador para los síntomas observados.

Si durante el proceso de resolución de problemas se ha decidido quitar un servidor de autenticación o contabilidad radius de la lista de servidores activos por cualquier razón, hay un comando (non-config) que sacará un servidor del servicio indefinidamente hasta que se desee ponerlo de nuevo en servicio. Este es un enfoque más claro que tener que eliminarlo manualmente de la configuración:

```
{inhabilitar | 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
```

Una migración de PSC o DPC o un switchover de tarjeta de línea a menudo pueden despejar problemas debido al hecho de que la migración resulta en el reinicio de los procesos en la tarjeta, incluido el npumgr que ha sido la causa de problemas de vez en cuando con respecto a los flujos de NPU.

Pero en un giro interesante con el mencionado ejemplo de aamgr 92, los fracasos de AAA inalcanzable realmente COMENZARON cuando se hizo una migración de PSC. Esto se activó debido a un flujo de NPU que desapareció cuando se realizó una migración de PSC para hacer PSC 11 en espera. Cuando se hizo activa una hora más tarde, el impacto real del flujo faltante comenzó para aamgr 92. Problemas como este son muy difíciles de resolver sin la asistencia del Soporte 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
```

El problema se resolvió temporalmente con un switchover de puerto que causó que la tarjeta PSC que tenía un flujo NPU faltante para aamgr 92 dejara de estar conectada a una tarjeta de línea activa.

```
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
```

La última trampa de falla:

```
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
```

De manera similar, reiniciar los programas específicos que se quedan "atascados" también puede resolver problemas, aunque esta es una actividad que el Soporte Técnico debería hacer ya que implica comandos de soporte técnico restringidos. En el ejemplo de aamgr 92 introducido anteriormente en la sección show task resources, se intentó pero no se ayudó porque la causa raíz no era de aaamgr 92 sino más bien el flujo NPU faltante que necesitaba aamgr 92 (era un problema de NPU, no un problema de aaamgr). Aquí está el resultado relevante del intento. "show task table" se ejecuta para mostrar la asociación del id de proceso y la instancia de tarea 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
```

Ejemplo final

Este es el último ejemplo de una verdadera interrupción en una red activa que reúne muchos de los comandos y enfoques de resolución de problemas que se tratan en este artículo. Tenga en cuenta que este nodo gestiona los tipos de llamadas 3G MIP y 4G Long Term Evolution (LTE) y High Rate Packet Data (eHRPD) evolucionados.

show snmp trap history

Solo con las trampas, se puede confirmar que el punto de partida coincide con lo que el cliente informó como UTC 19:25. Dejando de lado, tenga en cuenta que las trampas AAAAuthSvrUnreachable para el servidor primario 209.165.201.3 no comenzaron a ocurrir hasta horas después (no está claro por qué, pero es bueno notar; pero la **contabilización inalcanzable** para ese servidor comenzó de inmediato)

```
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

El resultado muestra un conteo mucho menor de llamadas en DPC 8/1. Sobre la base de esto por sí solo, sin ningún análisis adicional, se PODRÍA sugerir que hay un problema en el DPC 8 y proponer la opción de migrar al DPC en espera. Pero es importante reconocer cuál es el impacto real del suscriptor - en estos escenarios, por lo general los suscriptores se conectarán exitosamente en un intento posterior y por lo tanto el impacto no es demasiado significativo para el suscriptor y probablemente no le informarán nada al proveedor, suponiendo que no haya interrupción del plano del usuario también en curso (lo que es posible dependiendo de lo que se ha roto).

```
 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
```

suscriptor de monitor

Se capturó una configuración de llamada en la que no hubo respuesta a la solicitud de autenticación al 209.165.201.3 primario para el sessmgr 242 en el DPC 9/1 que resulta que su administrador emparejado reside en el DPC 8/1, confirmando fallas 3G debido a AAA inalcanzables el 8/1. También confirma que aunque no hubo trampas AAAAuthSrvUnreachable para 209.165.201.3 hasta ese momento, no significa que no haya un problema para manejar las respuestas para ese servidor (como se muestra arriba, las trampas comienzan pero horas después).

```
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

Lo interesante es que el recuento de sesiones para sessmgr 242 es similar al de otros sessmgrs de trabajo. Una investigación más detallada mostró que las llamadas 4G, también alojadas en este chasis, pudieron conectarse, por lo que compensaron la falta de llamadas IP móviles 3G capaces de conectarse. Se puede determinar que, retrocediendo hasta 8 horas después de que se haya iniciado la interrupción, no hay llamadas MIP para este sessmgr 242, mientras que retrocede 9 horas hasta antes de que se inicie la interrupción, hay llamadas 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
```

Las llamadas LTE y eHRPD muestran una mayor proporción de llamadas MIP cuando se comparan los sessmgrs que están conectados a los programas en funcionamiento y rotos:

```
[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
```

servidor de autenticación X de la instancia de prueba de RADIUS

Todos los aamgrs en 8/1 están muertos - no hay comandos de instancia de prueba radius que funcionen para ninguno de esos aamgrs pero sí funcionan para aamgrs en 8/0 y otras tarjetas:

```
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

El comando emblship para la resolución de problemas de RADIUS muestra muchos tiempos de espera que aumentan rápidamente:

```
[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
```

Remediación

Durante las ventanas de mantenimiento, una migración de DPC de 8 a 10 resolvió el problema, las trampas AAAAuthSrvUnreachable se detuvieron y DPC 8 fue RMA'd y se determinó que la causa raíz era una falla de hardware en DPC 8 (los detalles de esa falla no son importantes para los fines de este artículo).

```
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
```