Contenido

Introducción

Este artículo discute cómo resolver problemas el SNMP traps AAAAccSrvUnreachable y AAAAuthSrvUnreachable, que son accionado debido a los problemas del accesibilidad con un servidor del Remote Authentication Dial-In User Service (RADIUS) usado para autenticar los suscriptores (o los operadores la registración en el nodo, sino a ése no es qué se está discutiendo aquí). Hay dos acercamientos que se pueden utilizar para determinar cuando cualquiera de estos desvíos accionará. Este artículo explicará qué condiciones accionan estos desvíos y qué métodos de Troubleshooting y obtención de datos se puede tomar para determinar la causa raíz y para solucionarlos. También discute algunos pasos potenciales de la corrección que puedan ser considerados.

Observe que el RESULTADO del unreachability será averiado fallas de llamada o errores de las estadísticas, lo mismo como si las respuestas del radio sean rechazos en vez de las aceptaciones. Mientras que la tarifa del éxito/del error (autenticación) se mide independientemente del descanso/del accesibilidad (hay desvíos y alarmas para esto) y se puede analizar ciertamente por derecho propio, el foco de este artículo estará en el problema de accesibilidad y no el problema del rechazo.

Utilizan a la salida de ejemplo del LABORATORIO y de los boletos reales en todas partes para ayudar a subrayar las discusiones. Qué aparece ser los IP Address públicos en este artículo son direccionamientos **falsos**.

Activadores del desvío

Hay dos diversos modelos/algoritmos/acercamientos a elegir de determinar el estatus de un servidor de RADIUS y cuándo intentar un diverso servidor si están ocurriendo los incidentes:

Errores consecutivos en un acercamiento del proceso del aaamgr

El acercamiento original y el utilizaron por los operadores implica más a menudo el no perder de vista del número de errores que han ocurrido en fila para un proceso determinado del aaamgr. Un proceso del aaamgr es responsable de todo el proceso e intercambio de mensaje de RADIUS con un servidor de RADIUS, y mucho el proceso del aaamgr existirá en un chasis, cada uno emparejada con los procesos del sessmgr (que son procesos principales responsables del Control de llamadas). (Vea todos los procesos del aaamgr con “el comando de los recursos de la tarea de la demostración”) el proceso determinado del aaamgr A por lo tanto procesará los mensajes de RADIUS para muchas llamadas, no apenas una sola llamada, y este algoritmo implica el seguir de cuántas veces en fila no ha podido un proceso determinado del aaamgr conseguir a una respuesta a la misma petición que ha tenido que volver a enviar - un “descanso del pedido de acceso” como se explica en “los contadores del radio de la demostración”.

El contrario respectivo los “errores consecutivos actuales del pedido de acceso en un mgr”, también “los contadores del radio de la demostración” se incrementa cuando ocurre éste, y “del comando del detalle de los servidores de las estadísticas del radio de la demostración (o autenticación)” indica los grupos fecha/hora del cambio de estado del radio del Active a la respuesta (solamente a ningún SNMP trap o registros se generan para apenas un error). Aquí está un ejemplo para las estadísticas del radio:

Si este contador alcanza el valor configurado (valor por defecto = 4) sin nunca el reajuste, por configurable: (observe los corchetes que el [] se utiliza para indicar al calificador opcional y en estas capturas de los casos que resuelven problemas las estadísticas (la autenticación es el valor por defecto si considera no se especifica)

consecutivo-errores 4 del detectar-muerto-servidor del [accounting] del radio

Entonces este servidor es marcado “abajo” para el período (minutos) configurado:

deadtime 10 del [accounting] del radio

Un SNMP trap y los registros se acciona también, por ejemplo, para la autenticación y/o considerar respectivamente:

Los desvíos indican el servidor que es inalcanzable. Tome la nota de cualquier modelo. ¿Por ejemplo, está sucediendo con un servidor u otro o todos los servidores, y cuál es la frecuencia de despedir - es que sucede continuamente o de vez en cuando?

También observe que todo lo que toma para que este desvío sea accionado está para que un aaamgr falle, y así que la parte difícil sobre este desvío es que no indica el fragmento del problema. Podría ser muy extenso o mismo el minoir - que incumben hasta el operador a determinar, y se acerca a figurar eso hacia fuera se discute en este artículo.

las estadísticas del desvío SNMP de la demostración señalarán la cantidad de veces que ha accionado desde el bootup, incluso si se han borrado los desvíos más viejos hace mucho tiempo. Este ejemplo muestra a estadísticas el problema inalcanzable:

Observe que el aaamgr señalado en el ejemplo antedicho es #231. Éste es el aaamgr de la Administración en el ASR 5000 que reside en el indicador luminoso LED amarillo de la placa muestra gravedad menor de la administración del sistema (SMC). Qué está engañando en esta salida es que cuando un aaamgr individual o los aaamgrs experimenta los problemas del accesibilidad, el número del caso señalado en los registros es el caso del aaamgr de la Administración y no el caso particular que experimentan el problema. Esto es debido al hecho de que si muchos casos están experimentando accesibilidad publica, después el registro se llenaría rápidamente si todos fueran señalados como tal, y así que el diseño ha sido señalar genéricamente sobre el caso de la Administración, que si uno no conociera esto, estaría engañando ciertamente. En los detalles posteriores de la sección de Troubleshooting será proporcionado en cómo determinar que Comenzando en algunas versiones de StarOS 17 y v18+, se ha cambiado este comportamiento para señalar el número correspondiente del caso del aaamgr que tiene problemas de conectividad (como se explica en el SNMP traps) en los registros con la identificación determinada (Cisco CDETS CSCum84773), aunque todavía solamente el primer acontecimiento (a través de los aaamgrs múltiples) de esto que sucede está señalado.

El aaamgr de la Administración es el número máximo del caso del sessmgr + 1, y así sucesivamente un ASR 5500 es 385 para el indicador luminoso LED amarillo de la placa muestra gravedad menor de proceso de datos (DPC) o 1153 (para DPC 2).

Como sidenote, el aaamgr de la Administración es responsable de manejar el operador/los logines del administrador así como manejando el cambio de los pedidos de autorización iniciados de los servidores de RADIUS ellos mismos.

La continuación, “el comando del detalle de los servidores de las estadísticas del radio de la demostración (o autenticación)” indicará los grupos fecha/hora de los cambios de estado para tragar que corresponde a los desvíos/a los registros (recordatorio: Está respondiendo definido anterior es solamente un solo aaamgr que consigue un descanso, mientras que abajo un solo aaamgr que consigue bastantes descansos consecutivos por la configuración para accionar abajo)

Si hay solamente un servidor configurado, después no se marca abajo, como que sería crítico para la configuración de llamada satisfactoria.

¿Digno de mencionar es que hay otro parámetro que se puede configurar en la línea de los config del detectar-muerto-servidor llamada? respuesta-descanso?. Cuando está especificado, un servidor se marca abajo de solamente cuando cumplen a los errores y las condiciones consecutivos ambas del respuesta-descanso. El respuesta-descanso especifica un período de tiempo en que no se recibe NINGUNAS respuestas A TODAS LAS peticiones enviadas a un servidor determinado. (Nota que este temporizador sería reajustado continuamente pues se reciben las respuestas.) Esta condición sería esperada cuando un servidor o la conexión de red está totalmente abajo, contra comprometido parcialmente/degradado.

El caso del uso para esto sería un escenario donde una explosión en el tráfico causa los errores consecutivos accionar, pero el marcado de un servidor abajo como consecuencia no se desea inmediatamente. Bastante, el servidor es se marque solamente abajo después de que un período de tiempo específico pase adonde no se recibe ningunas respuestas, representando con eficacia el O.N.U-accesibilidad verdadero del servidor.

Este método apenas discutido de controlar los cambios de la máquina de estado del radio es

dependiente en la mirada de todos los procesos del aaamgr y encontrar uno que accione la condición de las recomprobaciones falladas. Este método es conforme a un cierto grado a una cierta aleatoriedad de los errores, y así que puede no ser el algoritmo ideal a detectar los errores. Pero es especialmente bueno en el hallazgo

Acercamiento del keepalive

Otro método de detectar el accesibilidad del servidor de RADIUS está utilizando los mensajes de prueba simulados del keepalive. Esto implica el envío constante de los mensajes de RADIUS falsos en vez del tráfico real de la supervisión. Otra ventaja de este método es que es siempre activa, contra con los errores consecutivos en un acercamiento del aaamgr, donde podría haber los períodos donde no se envía ningún tráfico de RADIUS, y tan no hay manera de saber si un problema existe durante esas épocas, dando por resultado la detección retrasada cuando las tentativas comienzan a ocurrir. También cuando un servidor se marca abajo, este Keepalives continúa siendo enviado para poder marcar el servidor encima de cuanto antes. La desventaja a este acercamiento es que falta los problemas que se atan a los casos específicos del aaamgr que pueden experimentar los problemas porque utilizan el caso del aaaamgr de la Administración para los mensajes de prueba.

Aquí están los diversos configurables relevantes a este acercamiento:

El comando? ¿keepalive del detectar-muerto-servidor del radio (estadísticas)? gira el acercamiento señal de mantenimiento en vez de los errores consecutivos en un acercamiento del aaamgr. En el ejemplo anterior, el sistema envía un mensaje de prueba con el Prueba-nombre de usuario del nombre de usuario y el Prueba-nombre de usuario de la contraseña cada 30 segundos, y revisa cada 3 segundos si no se recibe ninguna respuesta, y revisa hasta 3 veces, después de lo cual marca el servidor abajo. Una vez que consigue su primera respuesta, la marca de reserva otra vez.

Aquí está un pedido de autenticación/una respuesta del ejemplo para las configuraciones antedichas:

El mismo SNMP traps se utiliza para significar el inalcanzable/abajo y los estados del radio reachable/up como con los errores consecutivos en un acercamiento del aaamgr:

? ¿muestre que el radio contradice todos? ¿tiene una sección para no perder de vista los pedidos del keepalive la autenticación y considerar también? aquí están los contadores de la autenticación:

Comandos de Troubleshooting/acercamientos

Ahora que el activador para los desvíos inalcanzables AAA se ha explicado, el siguiente paso es entender los diversos comandos de Troubleshooting de utilizar para determinar el impacto y para intentar imaginar la causa raíz. Unreachability es un término muy amplio. No explica donde está el unreachability - en la red, en el servidor, o en el ASR. ¿Por ejemplo, se sabe si las peticiones incluso fueron enviadas en el primer lugar? ¿El servidor recibió las peticiones? Respondió a las peticiones. Hizo las respuestas lo hacen de nuevo al ASR y si es así eran ellas procesó o cayó en el trayecto interno (es decir flujos). Esta tentativa de la sección de dirigir cómo contestar a estas

preguntas.

Fundamentos de la configuración de RADIUS

Hay primer algunos fundamentos que uno necesite ser familiares con en lo que respecta a la configuración de RADIUS. La mayor parte de la configuración para el RADIUS está en un grupo específicamente Nombrado, y todos los contextos tienen un grupo predeterminado que pueda ser configurado como sigue. Muchas configuraciones de las épocas tendrán apenas un grupo, el grupo predeterminado.

Si se utilizan los grupos Nombrados específicos aaa, son señalados por a la declaración siguiente configurada en un perfil del suscriptor o un nombre de la punta de la aplicación (APN) (dependiendo de la tecnología del Control de llamadas), por ejemplo:

Nota: Las en primer lugar controles de sistema el grupo específico aaa asignado al suscriptor, y entonces marcan el valor por defecto del grupo aaa para los configurables adicionales no definidos en el grupo específico.

Aquí están los comandos útiles que resumen todos los valores asignados a todos los configurables en las diversas configuraciones de grupo aaa. Esto permite la visión rápida de todos los configurables incluyendo los valores predeterminados sin tener que examinar la configuración manualmente, y ayuda posiblemente a evitar incurrir en equivocaciones al si se asume que ciertas configuraciones. Informe de estos comandos a través de todos los contextos:

El configurable más importante es por supuesto el acceso a RADIUS y los servidores de contabilidad ellos mismos. Aquí tiene un ejemplo:

Observe la característica de la MAX-tarifa que limita el número de peticiones enviadas al servidor por el aaamgr por segundo

Además, la dirección IP NAS también se requiere ser definida, que es la dirección IP en una interfaz en el contexto del cual se envían los pedidos de RADIUS y las respuestas recibidas. Si no definido, las peticiones no se envían y las trazas del suscriptor del monitor pueden no fijar un claro error (ningunos pedidos de RADIUS enviados y ninguna indicación porqué).

direccionamiento 10.211.41.129 del Nas-ip-address del atributo de RADIUS

Observe que porque la autenticación y las estadísticas son manejadas a menudo por el mismo servidor, un diverso número del puerto está utilizado para distinguir la autenticación contra el tráfico de las estadísticas en el servidor de RADIUS. Para el lado ASR5K, el número del puerto de origen UDP no es especificado y es elegido por el chasis sobre una base del aaamgr (más en esto más adelante).

Normalmente especifican el acceso múltiple y a los servidores de contabilidad para los propósitos de la redundancia. Un ordenamiento cíclico o la orden prioritaria puede ser configurado:

algoritmo del [accounting] del radio {primero-servidor | circular}

Los resultados de la opción del primero-servidor en TODAS LAS peticiones que son enviadas al

servidor con la prioridad con el número menor. Solamente cuando ocurren los errores de la recomprobación, o peor, un servidor se marca abajo, es el servidor con la prioridad siguiente intentada. Más en este abajo.

Cuando se envía una petición del radio (las estadísticas o acceso), se espera una contestación. Cuando una contestación no se recibe dentro del período de agotamiento del tiempo de espera (segundos):

descanso 3 del [accounting] del radio

La petición se vuelve a enviar hasta la cantidad de veces especificada:

Reintento máximo 5 del [accounting] del radio

Esto significa que una petición se puede enviar un total de Reintento máximo + las épocas 1 hasta que abandone en el servidor de RADIUS determinado que es intentado. En este momento, intenta la misma secuencia al servidor de RADIUS siguiente en la orden. Si cada uno de los servidores ha sido Reintento máximo intentados + las épocas 1 sin la respuesta, después la llamada se rechaza, asumiendo que no hay otra razón del error hasta esa punta.

Como sidenote, hay los configurables que permiten para que los usuarios tengan acceso incluso si la autenticación y las estadísticas fallan debido a los descansos a todos los servidores, aunque un despliegue comercial no implementaría probablemente esto:

el radio permite la autenticación-abajo del [accounting]

También, hay los configurables que pueden limitar el número total absoluto de transmisiones de una petición determinada a través de todos los servidores configurados, y éstos se inhabilitan por abandono:

MAX-transmisiones 256 del [accounting] del radio

Por ejemplo si esto se fija = 1, después incluso si hay servidor secundario, nunca se intenta porque solamente una tentativa para una configuración específica del suscriptor se intenta nunca.

muestre a recursos de la tarea el aaamgr todo del recurso

Cada proceso del aaamgr se empareja con y “trabaja para” un proceso asociado del sessmgr (responsable del manejo de llamadas total) y está situado en un diverso indicador luminoso LED amarillo de la placa muestra gravedad menor de los servicios de paquetes (PSC) o el indicador luminoso LED amarillo de la placa muestra gravedad menor de proceso de datos (DPC) solamente usar la misma instancia ID. También en esta nota de la salida de ejemplo el caso especial 231 del aaamgr que se ejecuta en el indicador luminoso LED amarillo de la placa muestra gravedad menor de la administración del sistema (SMC) para ASR 5000 (o el Input Output Card de la Administración para ASR 5500 (MIO)) cuál no procesa las peticiones del suscriptor pero consigue utilizado para los comandos test del radio (véase la sección posterior para más detalle en eso) Y para el operador CLI para iniciar sesión el proceso.

En este snippet, el aaamgr 107 situado en PSC 13 es responsable de dirigir todo el RADIUS que procesa para el sessmgr emparejado 107 situado en los problemas de accesibilidad PSC 1. para las llamadas de las influencias del aaamgr 107 en el sessmgr 107.

En el siguiente ejemplo, observe que los problemas con el aaamgr 92 están afectando al sessmgr emparejado según lo considerado fácilmente cuando está comparado a otros sessmgrs en cuanto a las cuentas de sesiones:

muestre los contadores del radio {{todos | [instance <aaamgr ->] del <server IP> del servidor} | resumen}

El comando del número uno de ser familiar con es variedades “de contadores del radio de la demostración”

Este los comandos informa apoyan muchos contadores útiles para resolver problemas los problemas del radio. El “radio de la demostración contradice todo el” comando tiene mucho valor en el éxito y fracaso de seguimiento sobre una base del servidor, y es importante entender el significado de los diversos contadores que componen este comando, pues puede no ser obvio. El comando es sensible al contexto y así que se debe ejecutar en el mismo contexto en donde se definen los grupos aaa.

NOTA IMPORTANTE: Durante un período de tiempo no controlado, es difícil extraer cualquier conclusión de los valores de contador o de las relaciones entre los contadores. Para hacer las conclusiones exactas, el mejor acercamiento es reajustar los contadores y monitorearlos durante un período de tiempo cuando está ocurriendo el problema que es resuelto problemas.

En el producto siguiente, observe el “pedido de acceso enviado” = 1, mientras que el “pedido de acceso revisó” = 3. Así pues, cualquier nueva petición dada a un servidor de RADIUS determinado se cuenta solamente una vez, y todas las recomprobaciones se cuentan por separado. En este caso, ésa es un total de 3 + 1 = 4 peticiones del acceso enviadas. Observe los “descansos contrarios” = 1. del pedido de acceso. Un solo descanso ocurre solamente cuando TODAS LAS recomprobaciones fallan, tan en este caso, 3 recomprobaciones sin un resultado de la respuesta en 1 descanso (no 4). Esto sucede a través de todos los servidores configurados hasta que haya éxito, o todas las tentativas han fallado. Preste tan la atención a los contadores que se siguen para cada servidor por separado. Aquí está un ejemplo de esto, donde:

Observe también que los descansos no están contados como errores, el resultado que es que el número de access-accept recibido y el Access-Reject recibido no equivaldrán hasta el pedido de acceso enviado si hay algunos descansos.

El análisis de estos contadores puede no ser totalmente directo. Por ejemplo para el protocolo del IP móvil (MIPS), como las autenticaciones están fallando, allí no es ninguna contestación del registro MIPS (RRP) que es enviada, y el móvil puede continuar iniciando los nuevos pedidos de inscripción MIPS (RRQ) porque no ha recibido un RRP MIPS. Cada nueva MIPS RRQ hace el PDSN enviar un nuevo pedido de autenticación que sí mismo pueda tener su propia serie de recomprobaciones. ¿Esto se puede ver en el campo identificación en la cima de una traza del paquete? es único para cada conjunto de las recomprobaciones. El resultado es que los contadores para Sent, revisados, y el descanso pueden ser mucho más altos que esperados para el número de llamadas recibidas. Hay una opción que se puede habilitar para minimizar estas recomprobaciones adicionales, y puede ser fijada en el agente extranjero (FA) (pero no en el Home Agent (HA)) servicio: ¿? ¿optimizar-Retries del here> de las opciones <6 de la autenticación manganeso-AAA?

Algunos otros contadores útiles:

“Respuesta del pedido de acceso caída” - ocurre si la llamada no puede poner mientras que

espera las respuestas a los pedidos de autenticación.

“Round Trip Time del último de la respuesta del pedido de acceso” - indica cualquier retardo entre los puntos finales, aunque no indicaría obviamente donde el retardo pudo estar.

Los “errores consecutivos actuales del pedido de acceso en un mgr” se relacionan con qué fue discutida en la primera sección en los activadores para los desvíos inalcanzables AAA. Representa

El “acceso/la Estadística-petición actuales hecha cola” indica las peticiones a las cuales no se están respondiendo y permaneciendo en la cola (las estadísticas permiten una acumulación de la cola indefinidamente mientras que no lo hace la autenticación)

La mayoría del escenario frecuente visto cuando el AAA inalcanzable está señalado es que están ocurriendo los descansos del acceso y/o los descensos de la respuesta también, mientras que las respuestas del acceso no están continuando con las peticiones.

Si el acceso al modo priviledged del Soporte técnico está disponible, después la investigación adicional puede ser hecha en el caso del aaamgr llano para determinar si uno o más aaamgrs específicos son la causa del aumento en las “malas” cuentas totales. Por ejemplo, busque los aaamgrs que están situados en un PSC/DPC específico que tiene los conteos altos o quizá un solo aaamgr o los aaamgrs al azar que tienen problemas - busque los modelos. Si todos o la mayoría de los aaamgrs están teniendo problemas, después hay probabilidad creciente que la causa raíz es externo al chasis O manifestación en grande en el chasis. Los controles de saludes generales se deben hacer en ese caso.

Aquí está la salida de ejemplo que muestra un problema con un aaamgr específico para considerar. (El problema resultó ser un bug en un Firewall entre el ASR5K y el servidor de RADIUS que bloqueaba el tráfico puertos específico) del caso del aaamgr (de los 114). ¿Durante un período de tres semanas, se han recibido solamente 48 respuestas, con todo sobre 100,000 descansos han ocurrido (y ese doesn? t incluye retransmite).

En conclusión, determine que los contadores están incrementando, para los cuales los servidores, y a qué velocidad.

muestre el recurso del subsistema de la sesión {aaamgr | sessmgr} {todo | #> del <instance del caso}

Mientras que está fuera del alcance de este artículo para examinar toda la salida superflua de este comando, los ejemplos de un par valen el mirar. Como cualquier otro troubleshooting, comparar la salida entre qué se cree para ser buena contra los malos casos del aaamgr revela a menudo las diferencias obvias en los valores señalados. Esto se podía reflejar en el número total de peticiones, de error/de índice de éxito, de auth cancelados, de etc. Como recordatorio, esté seguro de borrar el subsistema de la sesión (un caso no se puede borrar, ellos debe ser borrado todo) para eliminar cualquier historial que podría potencialmente proporcionar una imagen nublada del estado actual.

La continuación con el mismo problema mencionado anterior en cuanto a un solo aaamgr que falla para considerar, aquí se hace salir de un diverso nodo con ese mismo problema excepto un diverso caso 36 del sessmr. Observe todos los campos interesantes para el aaamgr que falla y cómo esos valores aumentan en un cierto plazo con las dos capturas del comando. Mientras tanto haga salir del caso 37 se muestra como ejemplo de un aaamgr de trabajo.

Uno debe también funcionar con a los recursos de la tarea de la demostración para marcar para saber si hay cualquier cuenta de sesiones desigual (columna usada) entre todos los sessmgrs. Si se encuentran ningunos, marque los aaamgrs emparejados para esos sessmrs con este comando de ver si hay algunos campos que estén fuera de línea - si el problema es debido al RADIUS

entonces allí es una buena ocasión de encontrar algo.

En el ejemplo de los recursos de la tarea de la demostración en una sección anterior, había una cuenta de sesiones signficantly más baja en el sessmgr 92 que fue emparejado al aaamgr 92. La salida del aumento importante de las demostraciones del subsistema de la sesión de la demostración en el auth MAX-excepcional y aaa total purgó los contadores, y elevó los contadores MAX-excepcionales actuales. Uno puede utilizar la característica del grep viva en el chasis y/o el Notepad++ o el otro editor potente de la búsqueda para analizar rápidamente los datos. Funcione con los tiempos múltiples del comando para ver qué valores son cada vez mayores o que siguen elevados:

ping

traceroute

Un ping de ICMP prueba la conectividad básica para considerar si el servidor de AAA puede ser alcanzado o no. El ping puede necesitar ser originado con la palabra clave del src dependiendo de la red y de las necesidades de ser hecho del contexto AAA para tener valor. Si el ping al servidor falla, después intente hacer ping los elementos intermediarios incluyendo la dirección del salto siguiente en el contexto, confirmando allí es una entrada ARP a la dirección del salto siguiente si el ping falla. Traceroute puede también ayudar con los problemas de ruteo.

auth del caso x de la prueba del radio {<group> del grupo del radio | todos | <password> del <username> del <port> del puerto del <IP> del servidor}

caso x de la prueba del radio que considera {name> del <group del grupo del radio | todos | <port> del puerto del <IP> del servidor}

Con el acceso a los comandos test del soporte técnico, uno puede probar más lejos si un aaamgr específico puede alcanzar a cualquier servidor de RADIUS. Para una prueba de conectividad del RADIUS básico, la independiente de cualquier caso específico del aaamgr, utiliza la versión genérica de este comando que no especifique ninguna instancia específica # pero utiliza el caso de la Administración por abandono. Si esto falla, después puede señalar a una independiente de un problema más ancho de las instancias específicas.

Este comando envía las peticiones de una petición de la autenticación básica o del **comienzo** y de la **parada de las** estadísticas y espera una respuesta. Para la autenticación, utilice cualquier nombre de usuario y contraseña, en este caso una respuesta del rechazo sería esperada, confirmando que el RADIUS está trabajando según lo diseñado, o un nombre de usuario/una contraseña de trabajo sabidos podría ser utilizado, en este caso se recibiera una respuesta del validar

Aquí está una salida de ejemplo del protocolo y del funcionamiento del monitor la versión de la autenticación del comando en un chasis del laboratorio: Aquí está un ejemplo de un chasis vivo:

Aquí está una salida de ejemplo de funcionar con la versión de las estadísticas del comando. Una contraseña no es necesaria.

El producto siguiente está para el mismo caso 36 del aaamgr apenas mencionado donde está quebrada la Conectividad a un servidor de contabilidad específico RADIUS:

[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC 2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS 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 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 10113.0 ms

muestre el caso del [radius group <group name>] de la información de RADIUS {X | todos}

Este los comandos informa el flujo ID de la unidad del procesador de red (NPU) y puerto UDP utilizaron por la dirección IP configurada NAS para conectar con los servidores de RADIUS. Esto está señalada en la sección del valor por defecto del grupo aaa de la salida. Ciertamente el número del puerto puede ser útil si uno necesita hacer juego los paquetes RADIUS en una captura de paquetes con un caso específico del aaamgr #. (Nota que los flujos NPU son complicados y no algo discutida en este artículo pero una entidad que un ingeniero de servicio técnico podría investigar más lejos.) También sigue las peticiones extraordinarias al servidor. En el mismo problema del ejemplo usado en este artículo, solamente un par de puerto específico del servidor de RADIUS **<==>** NAS IP/UDP había fallado según lo resaltado.

[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC 2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS 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 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 10113.0 ms

suscriptor del monitor

El suscriptor del monitor puede ser utilizado para determinar si la autenticación se intenta por lo menos y si una contestación se está procesando para las llamadas que son monitoreadas. Gire la opción “S” que información del remitente de Sessmgr de la significa - con eficacia señalando sobre el caso del sessmgr o del aaamgr # que está manejando la Mensajería en la pregunta. Aquí está un ejemplo para una llamada MIPS en un HA que asocia a los casos 132 del sessmgr/del aaamgr.

[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC 2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response

receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS 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 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 10113.0 ms

Hay un ejemplo de falla en el extremo de este artículo también.

Captura de paquete

A veces no hay bastante información sobre el ASR para determinar porqué están ocurriendo los problemas del accesibilidad, en este caso una captura de paquetes es necesaria. Cuando resolver problemas al suscriptor individual publica, identificando los paquetes respectivos en una traza debe ser fácil. Si no, conociendo el puerto UDP que era utilizado en cualquier final de un caso determinado del aaamgr **# <==>** los pares del servidor de RADIUS podrían ser útiles si el problema se ata a los puertos específicos/a los casos del aaamgr. Intentar la captura en los lugares múltiples en la red puede ser necesario determinar donde los paquetes están consiguiendo caídos. En el problema que era analizado en este artículo, era una captura de paquetes en apenas el lugar correcto en la trayectoria del transporte entre el ASR y el servidor de RADIUS que era el descubrimiento en solucionar el problema.

Correcciones

Esta última sección ofrece algunas ideas para remediating los problemas de conectividad RADIUS. Éstos no se presentan en ningún orden particular pero una lista de considerar bastante simplemente en el proceso de Troubleshooting.

¿Si el servidor de RADIUS está consiguiendo sobrecargado, la carga se podría disminuir vía el valor (256 predeterminado) configurado para? ¿radio (estadísticas) MAX-excepcional? , que establece un límite en el número de pedidos (por contestar) excepcionales cualquier proceso dado del aaamgr. Si se alcanza el límite, los registros pueden indicar esto: ¿? No podido asignar el ID del mensaje para el servidor de autenticación de RADIUS x.x.x.x:1812?.

Los mensajes de RADIUS de la limitación de la tarifa a los servidores específicos pueden también ayudar a reducir la carga vía la palabra clave del tarifa-límite para las líneas de configuración del servidor correspondiente.

No es a veces un problema de la Conectividad sino del tráfico que considera creciente, que no es un problema con el RADIUS persay, solamente de señalar a otra área, tal como renegociaciones crecientes ppp que estén causando más comienzo y paradas de las estadísticas. Tan uno puede necesitar resolver problemas el exterior del RADIUS para encontrar una causa o un activador para los síntomas que son observados.

Si durante el proceso de Troubleshooting se ha decidido para quitar una autenticación de RADIUS o a un servidor de contabilidad de la lista de servidores vivos por la razón que sea, hay el comando a (NON-config) que tomará un Out Of Service del servidor indefinidamente hasta que se desee para ponerlo detrás en el servicio. Esto es un acercamiento más limpio que teniendo

que quitarlo de la configuración manualmente:

```
{neutralización | servidor x.x.x.x del [accounting] del radio del
permiso}
```

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC
2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response
receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1,
port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS
Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-
trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port
1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to
accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop
to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS
Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-
trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port
1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to
accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time
for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting
Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting
server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response
was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response
receivedRound-trip time for response was 10113.0 ms
```

Una migración PSC o DPC o un intercambio del linecard puede los problemas debido a menudo claros al hecho de que la migración dé lugar al reinicio de los procesos en el indicador luminoso LED amarillo de la placa muestra gravedad menor, incluyendo el npumgr que ha sido la causa de los problemas en lo que respecta a NPU fluye de vez en cuando.

Pero en una torsión interesante con el ejemplo ya mencionado del aaamgr 92, los errores inalcanzables AAA COMENZADOS realmente cuando una migración PSC fue hecha. Esto era accionado debido a un NPU fluye falta que iba cuando una migración PSC fue hecha que hacía el recurso seguro PSC 11. Cuando fue hecho active a la hora más adelante, el impacto real del flujo que falta empezó para el aaamgr 92. Los problemas como esto son muy difíciles de resolver problemas sin la ayuda del Soporte técnico.

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC
2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response
receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1,
port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS
Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-
trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port
1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS Start to
accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS Stop
to accounting server 209.165.201.3, port 1646Communication Failure: no response receivedRADIUS
Start to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-
trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port
1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to
accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time
for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting
Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting
server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response
was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response
receivedRound-trip time for response was 10113.0 ms
```

El problema fue resuelto temporalmente con un intercambio del puerto que causó el indicador luminoso LED amarillo de la placa muestra gravedad menor PSC que tenía un NPU que falta fluye para el aaamgr 92 que se conectará no más con un linecard activo.

```
[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC
2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response
```

receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS 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 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 10113.0 ms

El desvío más reciente del error:

[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC 2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS 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 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response was 10113.0 ms

Semejantemente, el recomienzo de los aaamgrs específicos que consiguen “se pegó” puede también resolver los problemas, aunque ésta es una actividad que el Soporte técnico debe hacer puesto que implica los comandos restrictos del soporte técnico. En el ejemplo del aaamgr 92 introducido en los recursos de la tarea de la demostración seccione anterior, esto fue intentado pero no ayudó porque la causa raíz no era el aaamgr 92 pero fluyen bastante los NPU que falta que el aaamgr 92 necesitó (era un problema NPU, no un problema del aaamgr). Aquí está la salida relevante de la tentativa. “la tabla de la tarea de la demostración” se funciona con para mostrar la asociación del identificador de proceso y encargar el caso # 92.

[source]PDSN> radius test instance 36 accounting all testWednesday September 10 10:06:29 UTC 2014RADIUS Start to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 51.2 msRADIUS Stop to accounting server 209.165.201.1, port 1646Accounting Success: response receivedRound-trip time for response was 46.2 msRADIUS Start to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 89.3 msRADIUS Stop to accounting server 209.165.201.2, port 1646Accounting Success: response receivedRound-trip time for response was 87.8 msRADIUS 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 1646Accounting Success: response receivedRound-trip time for response was 81.6 msRADIUS Stop to accounting server 209.165.201.4, port 1646Accounting Success: response receivedRound-trip time for response was 77.1 msRADIUS Start to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Stop to accounting server 209.165.201.5, port 1646Accounting Success: response receivedRound-trip time for response was 46.7 msRADIUS Start to accounting server 209.165.201.6, port 1646Accounting Success: response receivedRound-trip time for response

```
was 79.6 msRADIUS Stop to accounting server 209.165.201.6, port 1646Accounting Success: response
receivedRound-trip time for response was 10113.0 ms
```

Ejemplo final

Aquí está un ejemplo final de una caída del sistema real en una red en funcionamiento que tire juntos de muchos de los comandos de Troubleshooting y de los acercamientos discutidos en este artículo. Observe que este nodo dirige 3G MIPS, y la evolución a largo plazo 4G (LTE) y los tipos de llamada desarrollados de los datos del paquete de la alta velocidad (eHRPD).

muestre el historial del desvío SNMP

Por los desvíos solamente, puede ser confirmado que el punto de partida hace juego con lo que señaló el cliente como 19:25 UTC. Como aparte, observe que los desvíos de AAAAuthSvrUnreachable para el servidor primario 209.165.201.3 no comenzaron a suceder hasta las horas más adelante (no claro porqué, pero bueno observar; pero el **considerar inalcanzable a** ese servidor encendido inmediatamente)

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun 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
```

muestre a los recursos de la tarea

La salida muestra una cuenta mucho más baja de las llamadas en DPC 8/1. De acuerdo con este solo, sin cualquier análisis más otro, uno PODRÍA sugerir que hay un problema en DPC 8 y proponer la opción para emigrar al DPC espera. Pero es importante reconocer cuál es el impacto real del suscriptor - en estos escenarios que los suscriptores conectarán típicamente con éxito en una tentativa subsiguiente y por lo tanto el impacto no es demasiado significativo para el suscriptor y no señalarán probablemente cualquier cosa al proveedor, si se asume que no hay caída del sistema del plano del usuario también que continúa (que es posible dependiendo de cuál está quebrado).

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
```

```
2 ip address 209.165.201.3Sun 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
```

suscriptor del monitor

Una configuración de la llamada fue cogida donde no había respuesta al pedido de autenticación a 209.165.201.3 primario para el sessmgr 242 en el DPC 9/1 que sucede tener su aaamgr emparejado que reside en DPC 8/1, confirmando a las fallas debido 3G al AAA inalcanzable en 8/1. También confirma que aunque no había habido ninguna desvíos de AAAAuthSrvUnreachable para 209.165.201.3 hasta esa punta a tiempo, no significa que no hay un problema para manejar las respuestas para ese servidor (como se muestra arriba, los desvíos comienzan solamente las horas más adelante).

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun 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
```

muestre el smgr-caso sub X del [summary]

Cuál es interesante es que la cuenta de sesiones para el sessmgr 242 es similar a otros sessmgrs de trabajo. La investigación adicional mostró que las llamadas 4G, también recibidas en este chasis, podían conectar y así que compensaron la falta de llamadas del IP móvil 3G que podían conectar. Puede ser determinado que volviendo por lo que 8 horas que era después de que la interrupción haya comenzado, no son ninguna llamada MIPS para este sessmgr 242, mientras que va detrás 9 horas a antes de que la interrupción comenzada, allí sea llamadas conectadas:

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
```

```
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun 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
```

El LTE y las llamadas del eHRPD muestran una relación de transformación más alta a las llamadas MIPS al comparar los sessmgrs que están conectados con el trabajo y los aaamgrs rotos:

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun 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
```

servidor de autenticación del caso X de la prueba del radio

¿Todos los aaamgrs en 8/1 están muertos? ningunos comandos del caso de la prueba del radio trabajan para ningunos de esos aaamgrs pero trabajan para los aaamgrs en 8/0 y otros indicadores luminosos LED amarillo de la placa muestra gravedad menor:

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun 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
```

muestre que el radio contradice todos

El comando del buque insignia para resolver problemas el RADIUS muestra las porciones de descansos que estén aumentando quckly:

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun 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
```

Corrección

Durante las ventanas de mantenimiento, una migración 8 a 10 DPC resolvió el problema, los desvíos de AAAAuthSrvUnreachable parados, y el DPC 8 era RMA'd y la causa raíz fue determinada de ser una falla de hardware en DPC 8 (los detalles de ese incidente no son importantes saber con el propósito de este artículo).


```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3Sun Dec 29 19:32:13 2013 Internal trap notification 39
(AAAAuthSvrUnreachable) server 2 ip address 209.165.201.3Sun Dec 29 19:33:05 2013 Internal trap
notification 40 (AAAAuthSvrReachable) server 2 ip address 209.165.201.3Sun Dec 29 19:34:13 2013
Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address 209.165.201.3Sun Dec 29
19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip address
209.165.201.3Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server
2 ip address 209.165.201.3Sun 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
```