Tareas del administrador de sesión ASR5x00 - Descripción de la función, de la caída, de las operaciones de recupero, y de los registros de la caída

Contenido

Introducción

Este documento describe y explica la confiabilidad del software, la disponibilidad del servicio, y las características de la Conmutación por falla para las 5x00 Series del router de los servicios de la agregación de Cisco (ASR). Presenta la definición para una caída del software en ASR5x00 y los efectos de la caída del software. El artículo continúa establecer eso incluso en caso de las caídas del software inesperadas, cómo el ASR5x00 puede entregar la meta de la disponibilidad debido de la “portador-clase” a la elasticidad inherente del software y a la Disponibilidad de las características. El suscriptor móvil debe nunca tener que pensar en la Disponibilidad del servicio. La meta de Cisco no es ninguna pérdida de la sesión debido a ningunas solas fallas de hardware o de software, que incluyan la pérdida de un sistema completo, es decir - exprese la confiabilidad del grado. Las características de la confiabilidad del software en ASR5x00 se apuntan para poder alcanzar las metas para la disponibilidad del servicio de la “portador-clase” incluso en caso de que los errores imprevistos pudieron ocurrir en la red de un operador.

Arquitectura de software: Diseñado para la elasticidad

El ASR5x00 tiene una colección de tareas del software distribuidas a través del indicador luminoso LED amarillo de la placa muestra gravedad menor de los servicios de paquetes (PSC) o del indicador luminoso LED amarillo de la placa muestra gravedad menor de proceso de datos (DPC) y los indicadores luminosos LED amarillo de la placa muestra gravedad menor (MIO) del indicador luminoso LED amarillo de la placa muestra gravedad menor (SMC) o de la Administración y de la entrada-salida de la administración del sistema que se diseñan para

realizar una variedad de funciones específicas.

Por ejemplo, la tarea del administrador de sesión es responsable de manejar las sesiones para un conjunto de los suscriptores y llevar a cabo los servicios en línea tales como peer a peer (P2P), Deep Packet Inspection (DPI), y así sucesivamente, en el tráfico de usuarios. La tarea del administrador del Authentication, Authorization, and Accounting (AAA) es responsable de la generación de eventos de la factura para registrar el uso del tráfico del suscriptor y así sucesivamente. El administrador de sesión y funcionamiento de las tareas del administrador AAA en el indicador luminoso LED amarillo de la placa muestra gravedad menor PSC/DPC.

El indicador luminoso LED amarillo de la placa muestra gravedad menor SMC/MIO es reservado para el mantenimiento y operación (O&M) y la plataforma relacionaron las tareas. El sistema ASR5x00 se divide en compartimientos virtualmente en diversos subsistemas del software tales como el subsistema de la sesión para procesar las sesiones del suscriptor y el subsistema VPN que es responsable de la asignación de la dirección IP, encaminamiento, y así sucesivamente. Cada subsistema tiene una tarea del regulador que supervise la salud del subsistema que controla. El funcionamiento de las tareas del regulador en el indicador luminoso LED amarillo de la placa muestra gravedad menor SMC/MIO. Emparejan juntos al administrador de sesión y las tareas del administrador AAA para manejar la sesión de un suscriptor para el control, el tráfico de datos, y los fines de facturación. Cuando la recuperación de la sesión se habilita en el sistema, cada tarea del administrador de sesión sostiene el estado de su conjunto de los estados del suscriptor con una tarea del administrador del par AAA de ser recuperado en caso de caída del administrador de sesión.

¿Cuál es una caída?

Una tarea en el ASR5x00 puede potencialmente causar un crash si encuentra una condición de falla durante el funcionamiento normal. Un incidente de la caída o del software en el ASR5x00 se define para ser una salida o una terminación *inesperada de una* tarea en el sistema. Una caída puede suceder si el código del software intenta a las áreas de memoria de acceso se prohíben que (por ejemplo las estructuras de datos corrompidas), encuentra una condición en el código que no se espera (por ejemplo una transición de estado inválida), y así sucesivamente. Una caída puede también ser accionada si la tarea llega a ser insensible system monitor (Monitor del sistema) a la tarea y el monitor intenta matar y recomenzar a la tarea. Un evento de la caída se puede también accionar explícitamente (en comparación con inesperado) en el sistema cuando una tarea es forzada para vaciar a su estado actual por un comando CLI o por system monitor (Monitor del sistema) para analizar el estado de la tarea. Un evento previsto de la caída puede también suceder cuando las tareas del controlador del sistema se recomienzan para potencialmente correctos una situación con una tarea del administrador que falle en varias ocasiones.

Efectos de una caída del administrador de sesión

Bajo funcionamiento normal, una tarea del administrador de sesión maneja un conjunto de las sesiones del suscriptor y de tráfico de datos asociado para las sesiones junto con una tarea de mirada del administrador AAA que maneje la factura para esas sesiones del suscriptor. Cuando ocurre una caída del administrador de sesión deja de existir en el sistema. Si la recuperación de la sesión se habilita en el sistema, una tarea espera del administrador de sesión se hace para llegar a ser activa en el mismo indicador luminoso LED amarillo de la placa muestra gravedad

menor PSC/DPC. Esta nueva tarea del administrador de sesión reinstala las sesiones del suscriptor mientras que comunica con la tarea del administrador del par AAA. La operación de recupero se extiende a partir de 50 milisegundos a algunos segundos dependientes sobre el número de sesiones que eran activas en el administrador de sesión a la hora de la caída y en conjunto carga de la CPU en el indicador luminoso LED amarillo de la placa muestra gravedad menor y así sucesivamente. No hay pérdida en las sesiones del suscriptor que fueron establecidas ya en el administrador de sesión original en esta operación. Cualquier sesión del suscriptor que estuviera en curso de establecimiento a la hora de la caída también será probablemente restablecido debido a las retransmisiones del protocolo y así sucesivamente. Cualquier paquete de datos que estuviera en la transición a través del sistema a la hora de la caída puede asumido para ser asociado a una pérdida de la red por las entidades de comunicación de la conexión de red y será retransmitido y la conexión serán llevados encendido por el nuevo administrador de sesión. La información de facturación para las sesiones llevadas por el administrador de sesión será preservada en el administrador del par AAA.

¿Cuándo debe el operador conseguir en cuestión?

Cuando ocurre una caída del administrador de sesión, el Procedimiento de recuperación sucede como descrito previamente y el resto del sistema sigue siendo inafectado por este evento. Una caída en un administrador de sesión no afecta a los otros administradores de sesión. Como dirección al operador, si las tareas del administrador de sesión múltiple *en el mismo desperfecto de placa PSC/DPC* simultáneamente o en el plazo de 10 minutos de uno a, allí pudieron ser pérdida de sesiones pues el sistema no pudo poder comenzar a los nuevos administradores de sesión rápidamente bastante para tomar el lugar de las tareas causadas un crash. Esto corresponde a un escenario doble del incidente donde la pérdida de sesiones puede ocurrir. Cuando la recuperación no es posible, recomienzan y está listo al administrador de sesión simplemente para validar las nuevas sesiones.

Cuando un administrador de sesión dado causa un crash en varias ocasiones (por ejemplo ella encuentra la misma condición de falla repetidamente), la tarea del regulador de la sesión toma la nota y se recomienza en un intento por restablecer el subsistema. Si la tarea del regulador de la sesión no puede estabilizar el subsistema de la sesión y se recomienza continuamente encima en este esfuerzo, el siguiente paso en la escalada está para que el sistema cambie a un indicador luminoso LED amarillo de la placa muestra gravedad menor espera SMC/MIO. En el evento improbable que no hay indicador luminoso LED amarillo de la placa muestra gravedad menor espera SMC/MIO o si encuentran a un error en la operación del intercambio, el sistema se reinicia.

Los administradores de sesión también mantienen las estadísticas para cada nombre del Punto de acceso (APN), los servicios, los functionalites, y así sucesivamente que serán perdidos permanentemente cuando ocurre una caída. Por lo tanto una entidad externa que recoge los bulkstats observará periódicamente una inmersión en las estadísticas cuando ocurren una o más caídas. Esto puede manifestar como inmersión en una representación gráfica de las estadísticas drenada sobre un eje del tiempo.

> **Note**: Un chasis típico poblado con PSC 7-14 o 4-10 indicadores luminosos LED amarillo de la placa muestra gravedad menor DPC tiene sobre los administradores de sesión del 120-160, dependientes sobre el número de indicadores luminosos LED amarillo de la placa muestra gravedad menor PSC/DPC, y una sola caída dará lugar a la pérdida de cerca de $1/40^{th}$ o de $1/80^{th}$ de las estadísticas. Cuando un administrador de sesión espera asume el control, comienza a acumular las estadísticas otra vez a partir de la cero.

¿Cómo saber si ocurrió una caída?

Una caída accionará un evento del SNMP trap a una estación de Monitoreo de red, tal como el servicio del monitoreo de evento (EMS) y por los eventos de syslog. Las caídas que han ocurrido en el sistema se pueden también observar con el **comando list de la caída de la demostración**. Observe que este las listas de comandos inesperadas y los eventos previstos de la caída según lo descrito anterior. Estos eventos de dos tipos de caída pueden ser distinguidos mediante una encabezado que describa cada caída.

Una caída de la tarea seguida por la recuperación de la sesión exitosa es indicada por este mensaje del registro:

```
"Death notification of task <name>/<instance id> on <card#>/<cpu#> sent to parent
task <parent name>/<instance id> with failover of <task name>/<instance id>
on <card#>/<cpu#>"
```

Una caída de la tarea que no podría recuperarse es indicada por este mensaje del registro:

```
"Death notification of task <name>/<instance id> on <card#>/<cpu#> sent to parent
task <parent name>/<instance id>"
```

En resumen, con la recuperación de la sesión habilitada, en la mayoría de los casos las caídas no serán notadas porque no tienen ningún impacto del suscriptor. Uno tiene que ingresar el comando CLI, o la mirada en los registros o la notificación SNMP para detectar cualquier acontecimiento de las caídas.

Por ejemplo:

```
 ******** show crash list *******
Tuesday May 26 05:54:14 BDT 2015
=== ==================== ======== ========== =============== ======================
# Time Process Card/CPU/ SW HW_SER_NUM
PID VERSION MIO / Crash Card
=== ==================== ======== ========== =============== ======================

1 2015-May-07+11:49:25 sessmgr 04/0/09564 17.2.1 SAD171600WS/SAD172200MH
2 2015-May-13+17:40:16 sessmgr 09/1/05832 17.2.1 SAD171600WS/SAD173300G1
3 2015-May-23+09:06:48 sessmgr 03/1/31883 17.2.1 SAD171600WS/SAD1709009P
4 2015-May-25+15:58:59 sessmgr 09/1/16963 17.2.1 SAD171600WS/SAD173300G1
5 2015-May-26+01:15:15 sessmgr 04/0/09296 17.2.1 SAD171600WS/SAD172200MH

 ******** show snmp trap history verbose *******
Fri May 22 19:43:10 2015 Internal trap notification 1099 (ManagerRestart) facility
sessmgr instance 204 card 9 cpu 1
Fri May 22 19:43:29 2015 Internal trap notification 73 (ManagerFailure) facility
sessmgr instance 204 card 9 cpu 1
Fri May 22 19:43:29 2015 Internal trap notification 150 (TaskFailed) facility
sessmgr instance 204 on card 9 cpu 1
Fri May 22 19:43:29 2015 Internal trap notification 151 (TaskRestart) facility
sessmgr instance 204 on card 9 cpu 1
Fri May 22 19:43:30 2015 Internal trap notification 183 (SessMgrRecoveryComplete)
Slot Number 9 Cpu Number 1 fetched from aaa mgr 1755 prior to audit 1755 passed
audit 1754 calls recovered 1754 all call lines 1754 time elapsed ms 1108.
Fri May 22 19:43:32 2015 Internal trap notification 1099 (ManagerRestart) facility
sessmgr instance 204 card 9 cpu 1
```

```
Fri May 22 19:44:49 2015 Internal trap notification 73 (ManagerFailure) facility
sessmgr instance 236 card 7 cpu 0
Fri May 22 19:44:49 2015 Internal trap notification 150 (TaskFailed) facility
sessmgr instance 236 on card 7 cpu 0
Fri May 22 19:44:49 2015 Internal trap notification 151 (TaskRestart) facility
sessmgr instance 236 on card 7 cpu 0
Fri May 22 19:44:51 2015 Internal trap notification 183 (SessMgrRecoveryComplete)
Slot Number 7 Cpu Number 0 fetched from aaa mgr 1741 prior to audit 1741 passed audit
1737 calls recovered 1737 all call lines 1737 time elapsed ms 1047.
Fri May 22 19:44:53 2015 Internal trap notification 1099 (ManagerRestart) facility
sessmgr instance 236 card 7 cpu 0
Fri May 22 19:50:04 2015 Internal trap notification 73 (ManagerFailure) facility
sessmgr instance 221 card 2 cpu 1
: Fri May 22 19:50:04 2015 Internal trap notification 150 (TaskFailed) facility
sessmgr instance 221 on card 2 cpu 1
Fri May 22 19:50:04 2015 Internal trap notification 151 (TaskRestart) facility
sessmgr instance 221 on card 2 cpu 1
Fri May 22 19:50:05 2015 Internal trap notification 183 (SessMgrRecoveryComplete)
Slot Number 2 Cpu Number 1 fetched from aaa mgr 1755 prior to audit 1755 passed
audit 1749 calls recovered 1750 all call lines 1750 time elapsed ms 1036.

 ******** show snmp trap history verbose *******
Fri May 22 19:43:10 2015 Internal trap notification 1099 (ManagerRestart) facility
sessmgr instance 204 card 9 cpu 1
Fri May 22 19:43:29 2015 Internal trap notification 73 (ManagerFailure) facility
sessmgr instance 204 card 9 cpu 1
Fri May 22 19:43:29 2015 Internal trap notification 150 (TaskFailed) facility
sessmgr instance 204 on card 9 cpu 1
Fri May 22 19:43:29 2015 Internal trap notification 151 (TaskRestart) facility
sessmgr instance 204 on card 9 cpu 1
Fri May 22 19:43:30 2015 Internal trap notification 183 (SessMgrRecoveryComplete)
Slot Number 9 Cpu Number 1 fetched from aaa mgr 1755 prior to audit 1755 passed
audit 1754 calls recovered 1754 all call lines 1754 time elapsed ms 1108.
Fri May 22 19:43:32 2015 Internal trap notification 1099 (ManagerRestart) facility
sessmgr instance 204 card 9 cpu 1
Fri May 22 19:44:49 2015 Internal trap notification 73 (ManagerFailure) facility
sessmgr instance 236 card 7 cpu 0
Fri May 22 19:44:49 2015 Internal trap notification 150 (TaskFailed) facility
sessmgr instance 236 on card 7 cpu 0
Fri May 22 19:44:49 2015 Internal trap notification 151 (TaskRestart) facility
sessmgr instance 236 on card 7 cpu 0
Fri May 22 19:44:51 2015 Internal trap notification 183 (SessMgrRecoveryComplete)
Slot Number 7 Cpu Number 0 fetched from aaa mgr 1741 prior to audit 1741 passed
audit 1737 calls recovered 1737 all call lines 1737 time elapsed ms 1047.
Fri May 22 19:44:53 2015 Internal trap notification 1099 (ManagerRestart) facility
sessmgr instance 236 card 7 cpu 0
Fri May 22 19:50:04 2015 Internal trap notification 73 (ManagerFailure) facility
sessmgr instance 221 card 2 cpu 1
: Fri May 22 19:50:04 2015 Internal trap notification 150 (TaskFailed) facility
sessmgr instance 221 on card 2 cpu 1
Fri May 22 19:50:04 2015 Internal trap notification 151 (TaskRestart) facility
sessmgr instance 221 on card 2 cpu 1
Fri May 22 19:50:05 2015 Internal trap notification 183 (SessMgrRecoveryComplete
) Slot Number 2 Cpu Number 1 fetched from aaa mgr 1755 prior to audit 1755 passed
audit 1749 calls recovered 1750 all call lines 1750 time elapsed ms 1036.

 ******** show logs  *******
2015-May-25+23:15:53.123 [sitmain 4022 info] [3/1/4850 <sitmain:31> sittask.c:4762]
[software internal system critical-info syslog] Readdress requested for facility
sessmgr instance 5635 to instance 114
2015-May-25+23:15:53.122 [sitmain 4027 critical] [3/1/4850 <sitmain:31>
crash_mini.c:908] [software internal system callhome-crash] Process Crash Info:
time 2015-May-25+17:15:52(hex time 556358c8) card 03 cpu 01 pid 27118 procname
```

```
sessmgr crash_details
Assertion failure at acs/acsmgr/analyzer/ip/acs_ip_reasm.c:2970
Function: acsmgr_deallocate_ipv4_frag_chain_entry()
Expression: status == SN_STATUS_SUCCESS
Proclet: sessmgr (f=87000,i=114)
Process: card=3 cpu=1 arch=X pid=27118 cpu=~17% argv0=sessmgr
Crash time: 2015-May-25+17:15:52 UTC
Recent errno: 11 Resource temporarily unavailable
Stack (11032@0xffffb000):
[ffffe430/X] __kernel_vsyscall() sp=0xffffbd28
[0af1de1f/X] sn_assert() sp=0xffffbd68
[0891e137/X] acsmgr_deallocate_ipv4_frag_chain_entry() sp=0xffffbde8
[08952314/X] acsmgr_ip_frag_chain_destroy() sp=0xffffbee8
[089d87d1/X] acsmgr_process_tcp_packet() sp=0xffffc568
[089da270/X] acs_process_tcp_packet_normal_path() sp=0xffffc5b8
[089da3fd/X] acs_tcp_analyzer() sp=0xffffc638
[0892fb39/X] do_acsmgr_process_packet() sp=0xffffc668
[08940045/X] acs_ip_lean_path() sp=0xffffc6b8
[0887e309/X] acsmgr_data_receive_merge_mode() sp=0xffffc9d8
[0887f323/X] acs_handle_datapath_events_from_sm_interface() sp=0xffffca08
[037c2e1b/X] sessmgr_sef_initiate_data_packet_ind() sp=0xffffca88
[037c2f50/X] sessmgr_pcc_intf_send_data_packet_ind() sp=0xffffcaf8
[061de74a/X] sessmgr_pcc_fwd_packet() sp=0xffffcb58
[0627c6a4/X] sessmgr_ipv4_process_inet_pkt_part2_slow() sp=0xffffcf68
[06318343/X] sessmgr_ipv4_process_inet_pkt_pgw_ggsn() sp=0xffffd378
[0632196c/X] sessmgr_med_ipv4_data_received() sp=0xffffd418
[0633da9a/X] sessmgr_med_data_receive() sp=0xffffd598
[0afb977c/X] sn_epoll_run_events() sp=0xffffd5e8
[0afbdeb8/X] sn_loop_run() sp=0xffffda98
[0ad2b82d/X] main() sp=0xffffdb08

2015-May-25+23:15:53.067 [rct 13038 info] [5/0/7174 <rct:0> rct_task.c:305]
[software internal system critical-info syslog] Death notification of task
sessmgr/114 on 3/1 sent to parent task sessctrl/0 with failover of sessmgr/5635 on 3/1
2015-May-25+23:15:53.065 [evlog 2136 info] [5/0/7170 <evlogd:0> odule_persist.c:3102]
[software internal system critical-info syslog] Evlogd crashlog: Request received to
check the state of persistent crashlog.
2015-May-25+23:15:53.064 [sitmain 4099 info] [3/1/4850 <sitmain:31> crash_mini.c:765]
[software internal system critical-info syslog] have mini core, get evlogd status for
logging crash file 'crashdump-27118'
2015-May-25+23:15:53.064 [sitmain 4017 critical] [3/1/4850 <sitmain:31> sitproc.c:1544]
[software internal system syslog] Process sessmgr pid 27118 died on card 3 cpu 1
signal=6 wstatus=0x86
2015-May-25+23:15:53.048 [sitmain 4074 trace] [5/0/7168 <sitparent:50> crashd.c:1130]
[software internal system critical-info syslog] Crash handler file transfer starting
(type=2 size=0 child_ct=1 core_ct=1 pid=23021)
2015-May-25+23:15:53.047 [system 1001 error] [6/0/9727 <evlogd:1> evlgd_syslogd.c:221]
[software internal system syslog] CPU[3/1]: xmitcore[21648]: Core file transmitted to
card 5 size=663207936 elapsed=0sec:908ms
2015-May-25+23:15:53.047 [system 1001 error] [5/0/7170 <evlogd:0> evlgd_syslogd.c:221]
[software internal system syslog] CPU[3/1]: xmitcore[21648]: Core file transmitted to
card 5 size=663207936 elapsed=0sec:908ms
2015-May-25+23:15:53.047 [sitmain 4080 info] [5/0/7168 <sitparent:50> crashd.c:1091]
[software internal system critical-info syslog] Core file transfer to SPC complete,
received 8363207936/0 bytes

 ******** show session recovery status verbose *******
Tuesday May 26 05:55:26 BDT 2015
Session Recovery Status:
Overall Status : Ready For Recovery
Last Status Update : 8 seconds ago

----sessmgr--- ----aaamgr---- demux
```

```
cpu state active standby active standby active status
---- ------- ------ ------- ------ ------- ------ ------------------------
1/0 Active 24 1 24 1 0 Good
1/1 Active 24 1 24 1 0 Good
2/0 Active 24 1 24 1 0 Good
2/1 Active 24 1 24 1 0 Good
3/0 Active 24 1 24 1 0 Good
3/1 Active 24 1 24 1 0 Good
4/0 Active 24 1 24 1 0 Good
4/1 Active 24 1 24 1 0 Good
5/0 Active 0 0 0 0 14 Good (Demux)
7/0 Active 24 1 24 1 0 Good
7/1 Active 24 1 24 1 0 Good
8/0 Active 24 1 24 1 0 Good
8/1 Active 24 1 24 1 0 Good
9/0 Active 24 1 24 1 0 Good
9/1 Active 24 1 24 1 0 Good
10/0 Standby 0 24 0 24 0 Good
10/1 Standby 0 24 0 24 0 Good
```

Arquitectura del registro de la caída

Los registros de la caída registran toda la información posible que pertenecen a una caída del software (vaciado de memoria completo). Debido a su tamaño, no pueden ser salvados en memoria del sistema. Por lo tanto, estos registros se generan solamente si el sistema se configura con un URL que señale a un dispositivo local o a un servidor de red donde el registro puede ser salvado.

El registro de la caída es un repositorio persistente de la Información del evento de la caída. Cada evento se numera y contiene el texto asociado a un CPU (minicore), a la unidad de procesamiento de la red (NPU), o a la caída del corazón. Los eventos registrados se registran en los expedientes de la longitud fija y se salvan en /flash/crashlog2.

Siempre que ocurra una caída, se salva esta información del desperfecto:

1. El expediente del evento se salva en el archivo de /flash/crashlog2 (el registro de la caída).
2. El minicore, el NPU, o el archivo de volcado asociado del corazón se salva en el directorio de /flash/crsh2.
3. Un vaciado de memoria completo se salva en un directorio del usuario configurado.

Sincronización de los eventos y de Minicores de la caída entre las placas de administración

El crashlog es único a cada uno de las placas de administración, así que si ocurre una caída cuando el indicador luminoso LED amarillo de la placa muestra gravedad menor el "8" es activo será el indicador luminoso LED amarillo de la placa muestra gravedad menor abierto una sesión el "8". Un Switchover subsiguiente visualizaría no más la caída en el registro. Para extraer esta caída, un Switch detrás encima para cardar el "8" tiene que ser hecho. El registro de acontecimientos y los volcados de la caída son únicos a las placas de administración activas y espera, así que si una caída ocurre en una placa activa entonces el registro de acontecimientos de la caída y los volcados relacionados serán salvados en una placa activa solamente. Esta información del desperfecto no está disponible en la placa de reserva. Siempre que el intercambio de los indicadores luminosos LED amarillo de la placa muestra gravedad menor debido a una caída en la placa activa, y la información del desperfecto se visualice no más en el indicador

luminoso LED amarillo de la placa muestra gravedad menor que asume el control, la información del desperfecto se puede extraer solamente de la placa activa actual. Para extraer la lista de la caída del otro indicador luminoso LED amarillo de la placa muestra gravedad menor, un intercambio se requiere otra vez. Para evitar este intercambio y obtener la información del desperfecto de la placa de reserva, la sincronización entre dos placas de administración y el mantenimiento de la información del desperfecto más reciente se requiere.

El evento de llegada de la caída será enviado al SMC/MIO espera y guardado en el archivo del crashlog del recurso seguro de la manera similar. Minicore, NPU, o los volcados del corazón en el flash de SMC/MIO activo necesita ser sincronizado a SMC/MMIO espera con el comando del **rsync**. Cuando una entrada del crashlog o la lista entera se borra a través del comando CLI, debe ser borrada en SMC activos y espera/MIOs. No hay impacto en la memoria. Toda la actividad relacionada caída de la sincronización será hecha por el evlogd del indicador luminoso LED amarillo de la placa muestra gravedad menor espera SMC/MIO, pues el evlogd espera se carga menos y la placa de reserva tiene bastante sitio para la actividad de la sincronización. Por lo tanto el funcionamiento del sistema no será afectado.

Comandos

Estos comandos se pueden utilizar para resolver problemas los problemas:

```
#show support details

#show crash list

#show logs

#show snmp trap history verbose

#show session recovery status verbose

#show task resources facility sessmgr instance <>

#show task resources facility sessmgr all
```

Corefiles se genera después de una caída. Los operadores los salvan generalmente en un servidor externo. El nombre corefile parece generalmente el crash-<Cardnum>-<CPU Num>-<Hex timestamp>-coree.gcrash-09-00-5593a1b8-core.

Siempre que ocurra una caída, se salva esta información del desperfecto:

- El expediente del evento se salva en el archivo de /flash/crashlog2 (el registro de la caída).
- El minicore, el NPU, o el archivo de volcado asociado del corazón se salva en el directorio de /flash/crsh2.

Resumen

Todo el software ASR5x00 se diseña para manejar las condiciones previstas/los eventos y las condiciones/los eventos imprevistos. Mientras que Cisco se esfuerza tener software perfecto, los errores existirán inevitable y las caídas serán posibles. Por eso la función de recuperación de la sesión es tan importante. Cisco se esfuerza para la perfección minimizará los acontecimientos de las caídas, y la recuperación de la sesión permitirá que las sesiones continúen después de una

caída. No obstante, es importante que Cisco continúa esforzándose alcanzar el software perfecto. Menos caídas reducirán la probabilidad de las caídas múltiples que suceden simultáneamente. Mientras que el seamlessly de la recuperación de la sesión cura una sola caída, la recuperación de las caídas simultáneas múltiples se diseña un bit diferentemente. Los operadores deben raramente (o nunca) experimentar las caídas simultáneas múltiples, pero si tal era ocurrir, el ASR5x00 se diseña para recuperar la integridad del sistema como la prioridad más alta, posiblemente en el sacrificio de algunas sesiones del suscriptor.