Tareas del administrador de sesiones ASR5x00: descripción de funciones, fallos, operaciones de recuperación y registros de fallos

Contenido

Introducción

Este documento describe y explica la confiabilidad del software, la disponibilidad del servicio y las funciones de conmutación por fallas para Cisco Aggregation Services Router (ASR) 5x00 Series. Presenta la definición para un desperfecto del software en ASR5x00 y los efectos del desperfecto del software. El artículo continúa estableciendo que incluso en caso de caídas inesperadas del software, cómo ASR5x00 puede ofrecer el objetivo de disponibilidad de "clase operador" debido a las características inherentes de resistencia y disponibilidad del software. El suscriptor móvil nunca debería tener que pensar en la disponibilidad del servicio. El objetivo de Cisco es no perder sesiones debido a fallos de hardware o software únicos, que incluyen la pérdida de un sistema completo, en otras palabras: fiabilidad de calidad de voz. Las funciones de confiabilidad del software en ASR5x00 están diseñadas para alcanzar los objetivos de disponibilidad del servicio "de clase operador" incluso en casos en los que se puedan producir fallas imprevistas en la red de un operador.

Arquitectura del software: Diseñado para la resistencia

El ASR5x00 tiene una colección de tareas de software distribuidas a través de las tarjetas Packet Services Card (PSC) o Data Processing Card (DPC) y System Management Card (SMC) o Management and I/O (MIO) que están diseñadas para realizar una variedad de funciones específicas.

Por ejemplo, la tarea de administrador de sesiones es responsable de gestionar las sesiones de un conjunto de suscriptores y de realizar servicios en línea como Peer-to-peer (P2P), Inspección profunda de paquetes (DPI), etc., en el tráfico de usuarios. La tarea de administrador de

autenticación, autorización y contabilidad (AAA) es responsable de la generación de eventos de facturación para registrar el uso del tráfico del suscriptor, etc. Las tareas del administrador de sesiones y del administrador AAA se ejecutan en la tarjeta PSC/DPC.

La tarjeta SMC/MIO está reservada para operaciones y mantenimiento (O&M) y tareas relacionadas con la plataforma. El sistema ASR5x00 está virtualmente compartimentado en diferentes subsistemas de software como el subsistema de sesión para procesar sesiones de suscriptores y el subsistema VPN que es responsable de la asignación de direcciones IP, ruteo, etc. Cada subsistema tiene una tarea de controlador que supervisa el estado del subsistema que controla. Las tareas del controlador se ejecutan en la tarjeta SMC/MIO. Las tareas de administrador de sesión y de administrador AAA se emparejan para manejar la sesión de un suscriptor con fines de control, tráfico de datos y facturación. Cuando se habilita la recuperación de sesión en el sistema, cada tarea del administrador de sesión realiza una copia de seguridad del estado de su conjunto de estados del suscriptor con una tarea de administrador AAA de peer que se recuperará en caso de que se produzca un desperfecto en el administrador de sesión.

¿Qué es un accidente?

Una tarea en el ASR5x00 puede potencialmente colapsar si encuentra una condición de falla durante el funcionamiento normal. Una falla o falla de software en el ASR5x00 se define como una salida *inesperada* o la terminación de una tarea en el sistema. Se puede producir una caída si el código de software intenta acceder a las áreas de memoria que están prohibidas (como las estructuras de datos dañadas), encuentra una condición en el código que no se espera (como una transición de estado no válida), etc. También se puede activar un desperfecto si la tarea deja de responder a la tarea del monitor del sistema y el monitor intenta matar y reiniciar la tarea. Un evento de desperfecto también puede activarse explícitamente (a diferencia de lo inesperado) en el sistema cuando una tarea se ve obligada a volcar su estado actual por un comando CLI o por el monitor del sistema para analizar el estado de la tarea. Un evento de crash esperado también puede ocurrir cuando las tareas del controlador del sistema se reinician para corregir potencialmente una situación con una tarea del administrador que falla repetidamente.

Efectos de un Desperfecto del Administrador de Sesión

En el funcionamiento normal, una tarea de administrador de sesión gestiona un conjunto de sesiones de suscriptor y el tráfico de datos asociado para las sesiones junto con una tarea de administrador AAA de peering que gestiona la facturación para esas sesiones de suscriptor. Cuando se produce un desperfecto del administrador de sesiones, deja de existir en el sistema. Si la recuperación de sesión está habilitada en el sistema, se realiza una tarea de administrador de sesión en espera para activarse en la misma tarjeta PSC/DPC. Esta nueva tarea del administrador de sesión restablece las sesiones del suscriptor cuando se comunica con la tarea del administrador AAA del peer. La operación de recuperación varía de 50 a unos segundos dependiendo del número de sesiones que estuvieron activas en el administrador de sesión en el momento del desperfecto y de la carga total de la CPU en la tarjeta, etc. No hay pérdidas en las sesiones de suscriptores que ya se establecieron en el administrador de sesión original en esta operación. Cualquier sesión de suscriptor que estaba en proceso de establecimiento en el momento del desperfecto también probablemente será restaurada debido a las retransmisiones de protocolo y así sucesivamente. Los paquetes de datos que se encontraban en transición a través del sistema en el momento del desperfecto pueden suponer que están asociados a una pérdida de red por parte de las entidades comunicadoras de la conexión de red y serán

retransmitidos y la conexión será llevada a cabo por el nuevo administrador de sesión. La información de facturación de las sesiones que lleva a cabo el administrador de sesión se conservará en el administrador AAA del peer.

¿Cuándo debería preocuparse el operador?

Cuando se produce un desperfecto en el administrador de sesiones, el procedimiento de recuperación se produce como se describió anteriormente y el resto del sistema no se ve afectado por este evento. Un desperfecto en un administrador de sesión no afecta a los otros administradores de sesión. Como guía para el operador, si varias tareas del administrador de sesión *en la misma tarjeta PSC/DPC* se bloquean simultáneamente o dentro de los 10 minutos uno del otro, podría haber pérdida de sesiones ya que el sistema podría no ser capaz de iniciar nuevos administradores de sesión lo suficientemente rápido como para reemplazar las tareas dañadas. Esto corresponde a un escenario de doble falla en el que se puede producir una pérdida de sesiones. Cuando la recuperación no es factible, el administrador de sesión simplemente se reinicia y está listo para aceptar nuevas sesiones.

Cuando un administrador de sesión determinado se bloquea repetidamente (como cuando se encuentra con la misma condición de falla una y otra vez), la tarea del controlador de sesión toma nota y se reinicia en un intento de restaurar el subsistema. Si la tarea del controlador de sesión no puede estabilizar el subsistema de sesión y se reinicia continuamente en este esfuerzo, el siguiente paso en la escalada es que el sistema pase a una tarjeta SMC/MIO en espera. En el caso poco probable de que no haya una tarjeta SMC/MIO en espera o si se produce un error en la operación de switchover, el sistema se reinicia.

Los administradores de sesiones también mantienen estadísticas para cada nombre de punto de acceso (APN), servicios, funciones, etc. que se perderán de forma permanente cuando se produzca un desperfecto. Por lo tanto, una entidad externa que recopile los bulkstats periódicamente observará un descenso en las estadísticas cuando se produzcan uno o más desperfectos. Esto se puede manifestar como un salto en una representación gráfica de las estadísticas dibujadas sobre un eje de tiempo.

> **Nota:** Un chasis típico con 7-14 tarjetas PSC o 4-10 tarjetas DPC tiene aproximadamente 120-160 administradores de sesiones, según el número de tarjetas PSC/DPC, y un solo desperfecto resultará en la pérdida de aproximadamente 1/40^{o} o 1/80^{o} de las estadísticas. Cuando un administrador de sesión en espera asume el control, comienza a acumular las estadísticas nuevamente desde cero.

¿Cómo saber si se produjo un desperfecto?

Un desperfecto desencadenará un evento de trampa SNMP en una estación de supervisión de red, como el Servicio de supervisión de eventos (EMS) y los eventos syslog. Los desperfectos que han ocurrido en el sistema también se pueden observar con el comando **show crash list**. Tenga en cuenta que este comando enumera los eventos de desperfecto tanto inesperados como esperados, como se ha descrito anteriormente. Estos dos tipos de eventos de desperfecto se pueden distinguir mediante un encabezado que describe cada desperfecto.

Este mensaje de registro indica un desperfecto de la tarea seguido de una recuperación de la

sesión exitosa:

```
"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#>"
```

Este mensaje de registro indica un desperfecto de tarea que no pudo recuperarse:

```
"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 activada, en la mayoría de los casos no se notarán los desperfectos porque no tienen impacto en el suscriptor. Uno debe ingresar el comando CLI, o mirar los registros o la notificación SNMP para detectar cualquier ocurrencia de 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 de registro de fallos

Los registros de desperfectos registran toda la información posible que se relaciona con un desperfecto del software (vaciado completo del núcleo). Debido a su tamaño, no se pueden almacenar en la memoria del sistema. Por lo tanto, estos registros sólo se generan si el sistema se configura con una URL que apunta a un dispositivo local o un servidor de red donde se puede almacenar el registro.

El registro de desperfectos es un repositorio persistente de información de eventos de desperfecto. Cada evento está numerado y contiene texto asociado a una CPU (minicore), una unidad de procesamiento de red (NPU) o una caída del kernel. Los eventos registrados se registran en registros de longitud fija y se almacenan en /flash/crashlog2.

Siempre que se produce un desperfecto, esta información de desperfecto se almacena:

1. El registro de eventos se almacena en el archivo /flash/crashlog2 (el registro de fallos).
2. El archivo minicore, NPU o vaciado de kernel asociado se almacena en el directorio /flash/crsh2.
3. Un vaciado de memoria completo se almacena en un directorio configurado por el usuario.

Sincronización de eventos de caída y minicores entre tarjetas de administración

El crashlog es exclusivo para cada una de las tarjetas de administración, por lo que si ocurre un desperfecto cuando la tarjeta "8" está activa, se registrará en la tarjeta "8". Un switchover posterior ya no mostraría el desperfecto en el registro. Para recuperar este desperfecto, se debe volver a realizar un switch a la tarjeta "8". El registro de eventos de desperfecto y los vaciados son exclusivos de las tarjetas de administración activas y en espera, por lo que si se produce un desperfecto en una tarjeta activa, el registro de eventos de desperfecto y los vaciados relacionados se almacenarán solamente en una tarjeta activa. Esta información de desperfecto no está disponible en la tarjeta en espera. Siempre que la conmutación de las tarjetas debido a un desperfecto en la tarjeta activa, y la información de desperfecto ya no se muestra en la tarjeta que toma el control, la información de desperfecto se puede recuperar solamente de la tarjeta activa actual. Para recuperar la lista de desperfectos de la otra tarjeta, se requiere una conmutación de nuevo. Para evitar este switchover y obtener la información del desperfecto de la tarjeta standby, se requiere la sincronización entre dos tarjetas de administración y el mantenimiento de la última información del desperfecto.

El evento de desperfecto que llega será enviado al SMC/MIO en espera y guardado en el archivo crashlog en espera de la misma manera. Minicore, NPU, o los vaciados de kernel en la memoria flash de SMC/MIO activo deben sincronizarse con SMC/MIO en espera con el comando **rsync**. Cuando se elimina una entrada de crashlog o la lista completa a través del comando CLI, se debe borrar tanto en SMC/MIO activos como en espera. No hay impacto en la memoria. Toda la actividad de sincronización relacionada con el desperfecto será realizada por el evlogd de la tarjeta SMC/MIO en espera, ya que el evlogd en espera está menos cargado y la tarjeta en espera tiene suficiente espacio para la actividad de sincronización. Por lo tanto, el rendimiento del sistema no se verá afectado.

Comandos

Estos comandos se pueden utilizar para resolver 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
```

Los corefiles se generan después de una caída. Normalmente, los operadores los almacenan en un servidor externo. El nombre del archivo de puntuación suele parecerse a crash-<Cardnum>-<CPU Num>-<Hex timestamp>-coree.gcrash-09-00-5593a1b8-core.

Siempre que se produce un desperfecto, esta información de desperfecto se almacena:

- El registro de eventos se almacena en el archivo /flash/crashlog2 (el registro de fallos).
- El archivo minicore, NPU o vaciado de kernel asociado se almacena en el directorio /flash/crsh2.

Summary

Todo el software ASR5x00 está diseñado para manejar las condiciones/eventos previstos y las condiciones/eventos imprevistos. Mientras Cisco se esfuerza por tener un software perfecto, inevitablemente existirán errores y se producirán desperfectos. Por eso la función de recuperación de sesión es tan importante. Los esfuerzos de Cisco por la perfección minimizarán los casos de desperfectos, y la recuperación de la sesión permitirá que las sesiones continúen después de un desperfecto. No obstante, es importante que Cisco siga esforzándose por conseguir un software perfecto. Un menor número de caídas reducirá la probabilidad de que se produzcan múltiples caídas simultáneamente. Mientras que la recuperación de la sesión cura sin problemas un solo desperfecto, la recuperación de varios desperfectos simultáneos se ha diseñado un poco diferente. Los operadores rara vez (o nunca) deben experimentar múltiples caídas simultáneas, pero si se producen, el ASR5x00 está diseñado para recuperar la integridad del sistema como la prioridad más alta, posiblemente a expensas de algunas sesiones de suscriptores.