Attività di ASR5x00 Session Manager - Descrizione della funzione, arresto anomalo, operazioni di ripristino e registri di arresto anomalo

Sommario

Introduzione

Questo documento descrive e spiega l'affidabilità del software, la disponibilità dei servizi e le funzionalità di failover per Cisco Aggregation Services Router (ASR) serie 5x00. Presenta la definizione di un crash del software su ASR5x00 e gli effetti del crash del software. L'articolo prosegue affermando che, anche in caso di arresto anomalo del software, ASR5x00 è in grado di fornire l'obiettivo di una disponibilità di "classe portante" grazie alle caratteristiche di resilienza e disponibilità del software. L'abbonato alla telefonia mobile non dovrebbe mai pensare alla disponibilità del servizio. L'obiettivo di Cisco è evitare la perdita di sessioni a causa di guasti hardware o software singoli, che includono la perdita di un sistema completo, in altre parole - affidabilità di livello voce. Le funzionalità di affidabilità software di ASR5x00 sono progettate per raggiungere gli obiettivi di disponibilità del servizio di "classe carrier" anche nei casi in cui si possano verificare errori imprevisti nella rete di un operatore.

Architettura software: Progettato per la resilienza

ASR5x00 dispone di una raccolta di attività software distribuite tra le schede Packet Services Card (PSC) o Data Processing Card (DPC) e System Management Card (SMC) o Management and I/O (MIO) progettate per eseguire una varietà di funzioni specifiche.

Ad esempio, il task di gestione delle sessioni è responsabile della gestione delle sessioni per un set di sottoscrittori e dell'esecuzione di servizi in linea, quali Peer-to-peer (P2P), Deep Packet Inspection (DPI) e così via, sul traffico degli utenti. L'attività di gestione autenticazione,

autorizzazione e accounting (AAA) è responsabile della generazione degli eventi di fatturazione per registrare l'utilizzo del traffico degli utenti e così via. Le attività del responsabile della sessione e del responsabile AAA vengono eseguite sulla scheda PSC/DPC.

La scheda SMC/MIO è riservata per le attività di funzionamento e manutenzione (O&M) e relative alla piattaforma. Il sistema ASR5x00 è virtualmente suddiviso in diversi sottosistemi software, come il sottosistema di sessione per l'elaborazione delle sessioni degli abbonati e il sottosistema VPN responsabile dell'assegnazione degli indirizzi IP, del routing e così via. Ogni sottosistema è dotato di un'attività di controllo che controlla lo stato del sottosistema controllato. Le operazioni del controller vengono eseguite sulla scheda SMC/MIO. Le attività del gestore della sessione e del gestore AAA vengono accoppiate per gestire la sessione di un destinatario predefinito a scopo di controllo, traffico di dati e fatturazione. Quando il ripristino della sessione è abilitato nel sistema, ogni task di session manager esegue il backup dello stato del proprio set di stati del sottoscrittore con un task di peer AAA manager da ripristinare in caso di arresto anomalo di session manager.

Cos'è un incidente?

Un'attività nell'ASR5x00 potrebbe bloccarsi se si verifica una condizione di errore durante il normale funzionamento. Un arresto anomalo o un errore software nell'ASR5x00 è definito come un'uscita *imprevista* o la terminazione di un'operazione nel sistema. Un arresto anomalo del sistema può verificarsi se il codice software tenta di accedere ad aree di memoria non consentite, ad esempio strutture di dati danneggiate, rileva una condizione imprevista nel codice, ad esempio una transizione di stato non valida e così via. Un arresto anomalo può inoltre essere attivato se l'attività non risponde all'attività di monitoraggio del sistema e il monitoraggio tenta di terminare e riavviare l'attività. Un evento di arresto anomalo può anche essere attivato in modo esplicito (e non imprevisto) nel sistema quando un'operazione è costretta a eseguire il dump dello stato corrente da un comando CLI o dal monitor di sistema per analizzare lo stato dell'operazione. Un evento di arresto anomalo previsto può inoltre verificarsi quando le attività del controller di sistema vengono riavviate per correggere potenzialmente una situazione con un'attività del manager che si interrompe ripetutamente.

Effetti dell'arresto anomalo di una gestione delle sessioni

In condizioni di funzionamento normali, un'attività di gestione delle sessioni gestisce un set di sessioni del sottoscrittore e il traffico di dati associato per le sessioni, insieme a un'attività di gestione AAA di peering che gestisce la fatturazione per tali sessioni del sottoscrittore. Quando si verifica un arresto anomalo di un gestore di sessione, questo cessa di esistere nel sistema. Se il ripristino della sessione è abilitato nel sistema, viene eseguita un'attività di gestione delle sessioni in standby per diventare attiva nella stessa scheda PSC/DPC. Questa nuova attività di gestione delle sessioni reintegra le sessioni del sottoscrittore mentre comunica con l'attività di gestione AAA peer. L'operazione di ripristino varia da 50 msec a pochi secondi a seconda del numero di sessioni attive nel gestore delle sessioni al momento dell'arresto anomalo e del carico complessivo della CPU sulla scheda e così via. Nessuna perdita nelle sessioni sottoscrittore già stabilite nel gestore sessioni originale in questa operazione. È probabile che anche le sessioni degli utenti che erano in fase di definizione al momento dell'arresto anomalo verranno ripristinate a causa di ritrasmissioni del protocollo e così via. Tutti i pacchetti di dati che erano in transizione attraverso il sistema al momento dell'arresto anomalo possono essere associati a una perdita di rete da parte delle entità comunicanti della connessione di rete e verranno ritrasmessi e la connessione verrà eseguita dal nuovo gestore della sessione. Le informazioni di fatturazione per le sessioni eseguite dal

responsabile della sessione verranno conservate nel responsabile AAA peer.

Quando dovrebbe interessare l'operatore?

Quando si verifica un arresto anomalo di un gestore della sessione, la procedura di ripristino viene eseguita come descritto in precedenza e il resto del sistema non viene influenzato da questo evento. Un arresto anomalo di un gestore di sessione non influisce sugli altri gestori di sessione. Come guida per l'operatore, se più attività di gestione della sessione *sulla stessa scheda PSC/DPC* si bloccano contemporaneamente o entro 10 minuti l'una dall'altra, potrebbe verificarsi la perdita di sessioni in quanto il sistema potrebbe non essere in grado di avviare nuovi manager della sessione abbastanza velocemente da sostituire le attività arrestate. Ciò corrisponde a uno scenario di doppio errore in cui può verificarsi la perdita di sessioni. Quando il ripristino non è possibile, il gestore delle sessioni viene semplicemente riavviato ed è pronto ad accettare nuove sessioni.

Quando un determinato gestore di sessione si blocca ripetutamente (ad esempio quando incontra ripetutamente la stessa condizione di errore), l'operazione del controller di sessione prende nota e si riavvia nel tentativo di ripristinare il sottosistema. Se l'attività del controller di sessione non è in grado di stabilizzare il sottosistema di sessione e si riavvia continuamente durante questo tentativo, il passaggio successivo nell'escalation prevede il passaggio del sistema a una scheda SMC/MIO in standby. Nel caso improbabile che non vi sia una scheda SMC/MIO in standby o se si verifica un errore nell'operazione di switchover, il sistema si riavvia da solo.

I gestori delle sessioni gestiscono inoltre le statistiche per ogni nome di punto di accesso (APN, Access Point Name), servizi, funzionalità e così via che andranno definitivamente perduti in caso di arresto anomalo. Di conseguenza, un'entità esterna che raccoglie periodicamente statistiche ausiliarie osserverà un calo nelle statistiche quando si verificano uno o più arresti anomali. Questo può manifestarsi come un dip in una rappresentazione grafica delle statistiche disegnate su un asse temporale.

> **Nota:** In uno chassis tipico con 7-14 schede PSC o 4-10 schede DPC sono presenti circa 120-160 responsabili di sessione, a seconda del numero di schede PSC/DPC, e un singolo guasto causerà la perdita di circa $1/40^{esimo}$ o $1/80^{esimo}$ delle statistiche. Quando un gestore della sessione di standby subentra, ricomincia ad accumulare le statistiche da zero.

Come sapere se si è verificato un incidente?

Un arresto anomalo attiverà un evento trap SNMP per una stazione di monitoraggio di rete, ad esempio il servizio di monitoraggio degli eventi (EMS) e gli eventi syslog. Gli arresti anomali del sistema possono essere osservati anche con il comando **show crash list**. In questo comando vengono elencati gli eventi di arresto anomalo previsti e non previsti, come descritto in precedenza. Questi due tipi di eventi di arresto anomalo possono essere distinti mediante un'intestazione che descrive ciascun arresto anomalo.

Un arresto anomalo dell'attività seguito dal ripristino della sessione è indicato dal seguente messaggio di 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#>"
```

Questo messaggio di log indica un arresto anomalo delle attività che non è stato possibile ripristinare:

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

In sintesi, con il ripristino della sessione abilitato, nella maggior parte dei casi gli arresti anomali non vengono rilevati perché non hanno alcun impatto sul sottoscrittore. È necessario immettere il comando CLI o esaminare i registri o la notifica SNMP per rilevare eventuali arresti anomali.

Ad esempio:

```
 ******** 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
```

Architettura di registrazione degli arresti anomali

I registri degli arresti anomali registrano tutte le possibili informazioni relative a un arresto anomalo del software (full core dump). A causa delle loro dimensioni, non possono essere archiviati nella memoria di sistema. Pertanto, questi log vengono generati solo se il sistema è configurato con un URL che punta a un dispositivo locale o a un server di rete in cui è possibile archiviare il log.

Il registro di arresto anomalo del sistema è un archivio permanente di informazioni sugli eventi di arresto anomalo del sistema. Ogni evento è numerato e contiene testo associato a una CPU (minicore), a un'unità di elaborazione di rete (NPU) o a un arresto anomalo del kernel. Gli eventi registrati vengono registrati in record a lunghezza fissa e memorizzati in /flash/crashlog2.

Quando si verifica un arresto anomalo, vengono archiviate le seguenti informazioni:

1. Il record dell'evento è memorizzato nel file /flash/crashlog2 (il registro di arresto anomalo).
2. Il file di dump associato di minicore, NPU o kernel viene archiviato nella directory /flash/crsh2.
3. Un dump di base completo viene archiviato in una directory configurata dall'utente.

Sincronizzazione di eventi di arresto anomalo e miniature tra le schede di gestione

Il crashlog è specifico di ciascuna scheda di gestione, quindi se si verifica un crash quando la scheda "8" è attiva, verrà registrata sulla scheda "8". Se si passa a un'altra modalità, il crash non verrà più visualizzato nel log. Per recuperare l'arresto anomalo, occorre tornare alla scheda "8". Il registro degli eventi di arresto anomalo e i dump sono specifici delle schede di gestione attive e in standby, quindi se si verifica un arresto anomalo su una scheda attiva, il registro degli eventi di arresto anomalo e i relativi dump verranno memorizzati solo su una scheda attiva. Queste informazioni sull'arresto anomalo non sono disponibili sulla scheda di standby. Ogni volta che le schede vengono sostituite a causa di un arresto anomalo della scheda attiva e le informazioni relative all'arresto anomalo non vengono più visualizzate sulla scheda che subentra, le informazioni relative all'arresto anomalo possono essere recuperate solo dalla scheda attiva corrente. Per recuperare la lista di crash dell'altra scheda, è necessario un altro switchover. Per evitare questo passaggio e ottenere le informazioni relative al guasto dalla scheda di standby, è necessaria la sincronizzazione tra due schede di gestione e la conservazione delle informazioni più recenti relative al guasto.

L'evento di arresto anomalo in arrivo verrà inviato al SMC/MIO in standby e salvato nel file crashlog dello standby nello stesso modo. Minicore, NPU o dump del kernel nella memoria flash di SMC/MIO attivo devono essere sincronizzati con SMC/MMIO in standby con il comando **rsync**. Quando una voce del crashlog o l'intero elenco viene eliminato tramite il comando CLI, deve essere cancellata sia sugli SMC/MIO attivi che su quelli in standby. Nessun impatto sulla memoria. Tutta l'attività di sincronizzazione correlata all'arresto anomalo del sistema verrà eseguita dall'evlog della scheda SMC/MIO in standby, poiché l'evlog in standby è meno caricato e la scheda in standby dispone di spazio sufficiente per l'attività di sincronizzazione. Le prestazioni del sistema non ne risentiranno.

Comandi

Questi comandi possono essere usati per risolvere i problemi:

```
#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
```

I corefile vengono generati dopo un arresto anomalo. In genere gli operatori li memorizzano in un server esterno. Il nome del file principale è in genere simile a crash-<Cardnum>-<Num CPU>-<Timestamp esadecimale>-core.gcrash-09-00-5593a1b8-core.

Quando si verifica un arresto anomalo, vengono archiviate le seguenti informazioni:

- Il record dell'evento è memorizzato nel file /flash/crashlog2 (il registro di arresto anomalo).
- Il file di dump associato di minicore, NPU o kernel viene archiviato nella directory /flash/crsh2.

Riepilogo

Tutto il software ASR5x00 è progettato per gestire sia le condizioni/gli eventi previsti che quelli imprevisti. Mentre Cisco si impegna per avere un software perfetto, inevitabilmente ci saranno degli errori e degli arresti anomali saranno possibili. Ecco perché la funzione di ripristino della sessione è così importante. La ricerca della perfezione da parte di Cisco riduce al minimo il numero di arresti anomali e il ripristino della sessione consente alle sessioni di continuare anche dopo un arresto anomalo. Tuttavia, è importante che Cisco continui a impegnarsi per realizzare il software perfetto. Un numero inferiore di arresti anomali riduce la probabilità di più arresti anomali simultanei. Mentre il ripristino della sessione risolve un singolo guasto, il ripristino da più arresti simultanei è progettato in modo leggermente diverso. Gli operatori devono sperimentare raramente (o mai) più arresti anomali simultanei, ma se dovessero verificarsi, l'ASR5x00 è progettato per ripristinare l'integrità del sistema come priorità massima, probabilmente sacrificando alcune sessioni degli utenti.