

Serie ASR5x00: Sessmgr Avvisa Lo Stato A Causa Dell'Elevato Numero Di Flussi HTTP

Sommario

[Introduzione](#)

[Problema](#)

[Risoluzione dei problemi](#)

[Soluzione](#)

Introduzione

In questo documento viene descritto il problema relativo al passaggio dello stato WARN di sessmgr a causa dell'elevato numero di flussi HTTP. Il problema è segnalato sui Cisco Aggregated Service Router (ASR) 5x00.

Problema

Lo stato di Sessmgr è WARN e l'utilizzo della memoria è elevato.

```
***** show task resources *****
Thursday July 24 17:44:58 IST 2014
      task  cputime      memory      files      sessions
cpu facility  inst used allc   used  alloc used allc  used  allc S status
-----
4/0 sessmgr      3  26% 100%  1.86G  1.86G   34  500  1766 28160 I  warn
```

Questi log degli errori vengono generati nel processo. Non vi è alcun impatto sul sottoscrittore a causa di questo log degli errori. Una volta rifiutata la chiamata da sessmgr in stato **WARN**, il sistema tenta in sessioni diverse e la chiamata viene eseguita.

```
[sessmgr 10018 error] [4/0/6812 <sessmgr:3> sessmgr_func.c:44683] [software internal system
syslog] Sessmgr-3 full (35200 effective number of calls, 1777 calllines in use, 51146 free
flows, 31221 free aaa_sessions, 1777 used-mem-credits, 1777 used-sess-credits, 1948360 mem-
usage, 1945600 mem-limit, 0 ecs-queue-usage, 70400 ecs-queue-limit, 16850 ecs-num-flows, 400000
ecs-max-flows, 2334720 ecs-mem-limit[ecs-flow/mem-values:valid], 0x86 limit-flags) - call
rejected
```

Risoluzione dei problemi

Acquisire l'output **show support details** e verificare la presenza di output del comando per risolvere ulteriormente i problemi.

Il problema di memoria è correlato alla quantità di flussi gestiti da sessmgr. La correlazione può essere rilevata tra un elevato consumo di memoria e un'elevata quantità di flussi di sessmgr.

```
***** debug acsmgr show memory usage *****
Thursday July 24 17:50:06 IST 2014
```

```
-----
!           !           Caches Count           !
Instance Memory !     Flows     ! Callline   Data-Session TCP OOO   !
! Current      Max ! Total    Free   Total   Free   Total   Free!
-----
```

Instance	Memory	Current	Max	Total	Free	Total	Free	Total	Free
1	865.68M	43365	64360	5500	1178	56140	12775	1102	1064
2	852.05M	43879	64767	5500	1178	60150	16271	1102	1067
3	1902.68M	17252	276519	4400	2631	44110	26858	551	541

Per i sessmgr interessati (e per uno non interessato), raccogliere questi output di comando, dove x è l'istanza di Sessmgr.

```
show messenger procllet facility sessmgr instance <x> heap
show messenger procllet facility sessmgr instance <x> system heap
task core facility sessmgr instance <x>
show active-charging flows instance <x>
show profile facility sessmgr active depth 8 head 201
show task resources facility sessmgr instance <x> max
```

Verificare se le regole non ottimizzate e i gruppi di valori di riferimento per le regole richiedono molta memoria.

```
debug acsmgr show rule-optimization-information
debug acsmgr show grp-of-rdef-optimization-information
```

Il maggiore consumo di memoria è dovuto a queste funzioni basate sugli output del comando.

```
acs_http_pkt_inspection()
acsmgr_alloc_buffer()
snx_add_dbufs()
sn_aaa_alloc_session_block()
sgx_imsa_bind_user()
```

È inoltre possibile selezionare il numero massimo di flussi HTTP simultanei raggiunti dalle linee di chiamata

```
***** debug acsmgr show flow-stats max-simultaneous-flows http *****
Thursday July 24 17:50:04 IST 2014
```

Histogram of Max No of Simultaneous HTTP Flows attained by Calllines

No Of Flows	No Of Calllines
1 to 10	964712518
11 to 20	384105002
21 to 40	232987189
41 to 100	148938918
101 to 200	115919586
201 to 500	86729303
501 to 1000	69975385
1001 to 2000	59635906

2001 to 5000	50743511
5001 to 10000	44566999
> 10000	1044671491

```
***** debug acsmgr show flow-stats cumulative http *****  
Thursday July 24 17:50:03 IST 2014
```

Histogram of Total Cumulative HTTP Flows by Calllines

No Of Flows	No Of Calllines
1 to 10	964712485
11 to 20	384104980
21 to 40	232987175
41 to 100	148938911
101 to 200	115919583
201 to 500	86729297
501 to 1000	69975377
1001 to 2000	59635907
2001 to 5000	50743509
5001 to 10000	44567004
> 10000	1044671452

Si può concludere che il numero di sessioni HTTP allocate è elevato e che ciò potrebbe essere dovuto al traffico HTTP elevato. Sono inoltre presenti quasi 1044671491 linee telefoniche, che hanno più di 10000 flussi HTTP alla volta. Ciò comporta un utilizzo elevato della memoria.

Soluzione

è disponibile la CLI per limitare il numero di flussi per sottoscrittore

```
flow limit-across-applications
```

Cisco consiglia di configurare il **limite di flusso tra le applicazioni su 5000**, come consigliato in tutte le basi regole interessate, in cui è possibile visualizzare un numero elevato di traffico HTTP.

Questa è la procedura per configurare il comando

```
In local context under Global configuration.  
# active-charging service ECS  
(config-acs)# rulebase GOLIVE  
(config-rule-base)# flow limit-across-applications 5000
```

Ulteriori informazioni sul comando.

flusso limite tra le applicazioni

Questo comando consente di limitare il numero totale di flussi simultanei per Sottoscrittore/APN inviati a una base regole indipendentemente dal tipo di **flusso** o di limitare i flussi in base al tipo di protocollo sotto la funzione di controllo della sessione.

Prodotto:

ACS

Privilegio:

Amministratore sicurezza, Amministratore

Modalità:

```
Exec > ACS Configuration> Rulebase Configuration
active-charging service service_name > rulebase rulebase_name

Entering the above command sequence results in the following prompt:

[local]host_name(config-rule-base)#
```

Sintassi

```
flow limit-across-applications { limit | non-tcp limit | tcp limit }no flow limit-across-
applications [ non-tcp | tcp ] no
```

Se è stato configurato in precedenza, elimina la configurazione **flow limit-through-applications** dalla base regole corrente.

flusso limite tra applicazioni

Specifica il numero massimo di flussi tra tutte le applicazioni per la base regole.

limit deve essere un numero intero compreso tra 1 e 400000000.

Predefinito: Nessun limite

limite non tcp

Specifica il limite massimo di flussi di tipo non TCP.

limit deve essere un numero intero compreso tra 1 e 400000000.

Predefinito: Nessun limite

limite tcp

Specifica il limite massimo di flussi TCP.

limit deve essere un numero intero compreso tra 1 e 400000000.

Predefinito: Nessun limite

Utilizzo:

Utilizzare questo comando per limitare il numero totale di flussi consentiti per una base regole

indipendentemente dal tipo di **flusso** o per limitare i flussi in base al protocollo, non TCP (senza connessione) o TCP (orientato alla connessione).

Se un sottoscrittore tenta di superare questi limiti, il sistema scarta i pacchetti del nuovo **flusso**. Questo limite di elaborazione di questo comando prevede i seguenti aspetti per UDP, TCP, ICMP e alcuni flussi esentati:

- UDP/ICMP: Il sistema attende il timeout **del flusso** prima di aggiornare il contatore e rimuoverlo dal conteggio dei flussi.
- TCP: Dopo il termine di un **flusso** TCP, il sistema attende per un breve periodo di tempo per accettare la ritrasmissione di qualsiasi pacchetto perso da un'estremità. I flussi TCP che sono terminati, ma sono ancora in attesa per timeout sono esentati per questa elaborazione limite.
- Flussi esentati: Il sistema esenta tutti gli altri flussi specificati con il comando **flow limit-for-flow-type** nella modalità di configurazione ACS Charging Action impostata su **no**.

Esempio:

Questo comando definisce il numero massimo di 200000 flussi per la base regole:

```
flow limit-across-applications 200000
```