

ASR5x00系列：由于HTTP流数量巨大，SESSMGR警告状态

目录

[简介](#)

[问题](#)

[故障排除](#)

[解决方案](#)

简介

本文档介绍由于大量HTTP流而进入WARN状态的sessmgr问题。此问题在思科集成多业务路由器(ASR)5x00上报告。

问题

Sessmgr状态为WARN且内存使用率较高。

```
***** 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
```

这些错误日志在进程中生成。由于此错误日志，不会影响用户。根据设计，一旦呼叫从处于WARN状态的sessmgr被拒绝，系统将尝试在不同的会话中，呼叫将通过。

```
[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
```

故障排除

捕获show support details输出并检查命令输出以进一步排除故障。

内存问题与sessmgr处理的流量有关。可以看到具有高内存消耗和高流量的会话管理器之间的关联。

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

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

对于受影响的会话（以及对于一个未受影响的会话），收集这些命令输出，其中x是Sessmgr实例。

```
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
```

检查未优化的规则和规则定义组是否占用大量内存。

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

最高内存消耗是基于命令输出的这些功能造成的。

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

您还可以检查呼叫线路所获得的最大HTTP流数

```
***** 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

您可以断定，分配的HTTP会话数量巨大，这可能是由于HTTP流量过大。此外，还有1044671491个Callline，它们一次的HTTP流量大10000。这会导致内存使用率较高。

解决方案

您有CLI来限制每个用户的流数

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

思科建议在所有受影响的规则库下将跨应用的流限制配置为5000，在这些规则库中可以看到大量HTTP流量。

以下是配置命令的步骤

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

有关此命令的详细信息。

流 跨应用限制

此命令允许您限制每个用户/APN发送到规则库的并发流总数，而不考虑流类型，或根据会话控制功能下的协议类型限制流。

产品:

ACS

权限:

安全管理员、管理员

模式:

```
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)#
```

语法

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

如果之前已配置，则从当前规则库中删除跨应用的流限制配置。

流 跨应用限制

为规则库指定跨所有应用的最大流数。

limit必须是介于1和4000000000之间的整数。

默认:无限制

非TCP限制

指定非TCP类型流的最大限制。

limit必须是介于1和4000000000之间的整数。

默认:无限制

TCP限制

指定TCP流的最大限制。

limit必须是介于1和4000000000之间的整数。

默认:无限制

使用率:

使用此命令可限制规则库允许的流总数，而不考虑流类型，或根据协议(非TCP (无连接) 或 TCP (面向连接))限制流。

如果用户尝试超出这些限制，系统会丢弃新流的数据包。此命令的此限制处理对于UDP、TCP、ICMP和一些豁免流具有以下方面：

- UDP/ICMP:系统在更新计数器并从流数计数中删除计数器之前等待流超时。
- TCP:在TCP流结束后，系统会等待一段较短的时间，以适应从一端重新传输任何丢失的数据包。TCP流已结束，但仍处于等待期，因此对此限制处理可免除超时。
- 豁免流：在ACS计费操作配置模式(ACS Charging Action Configuration Mode)设置为no时，系

统免除**flow limit-for-flow-type**命令指定的所有其他流。

示例：

此命令定义规则库的200000流最大数量：

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