

# ASR5x00 シリーズ：膨大な数のHTTPフローによるSessmgr WARN状態

## 内容

[概要](#)

[問題](#)

[トラブルシューティング](#)

[解決方法](#)

## 概要

このドキュメントでは、大量のHTTPフローが原因でsessmgrがWARN状態になる問題について説明します。この問題は、Ciscoアグリゲーションサービスルータ(ASR)5x00で報告されています。

## 問題

SessmgrのステータスはWARNで、メモリ使用率が高い。

```
***** 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
```

これらのエラーログはプロセスで生成されます。このエラーログが原因で、サブスクリバへの影響はありません。設計上、呼び出しがWARN状態のsessmgrから拒否されると、システムは異なるsessmgrで試行し、呼び出しが行われます。

```
[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
```

## トラブルシューティング

show support detailsの出力をキャプチャし、さらにトラブルシューティングを行うためのコマンド出力を確認します。

メモリの問題は、sessmgrが処理するフローの量に関連しています。高いメモリ消費と高いフロー量を有するセッション間の相関を見ることができると。

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

```
-----
```

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

```
-----
```

影響を受けるsessmgrs ( および影響を受けないsessmgrs ) の場合は、次のコマンド出力を収集します。xはSessmgrインスタンスです。

```
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
```

最適化されていないルールとルールのグループが大量のメモリを消費しているかどうかを確認します。

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

最大のメモリ消費は、コマンド出力に基づくこれらの機能によるものです。

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

また、[Max No of Simultaneous HTTP Flows actured by Call lines]をオンにすることもできます

```
***** 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

大量のHTTPセッションが割り当てられており、これはHTTPトラフィックの増加が原因である可能性がありますと結論付けることができます。また、ほぼ1044671491のCalllinesがあり、一度に10000を超えるHTTPフローがあります。これにより、メモリ使用率が高くなります。

## 解決方法

加入者あたりのフロー数を制限するCLIがあります

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

シスコは、大量のHTTPトラフィックが見られる影響を受けるすべてのルールベースでは、推奨されるフロー制限を5000に設定することを推奨します。

次に、コマンドを設定する手順を示します

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

このコマンドの詳細。

### フロー limit-across-applications

このコマンドを使用すると、フロータイプに関係なく、加入者/APNごとにルールベースに送信される同時フローの総数を制限したり、セッション制御機能のプロトコルタイプに基づいてフローを制限したりできます。

Product:

ACS

権限 :

セキュリティ管理者、管理者

## Mode ( モード ) :

```
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)#
```

## 構文

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

以前に設定した場合、は現在のルールベースからフロー制限アプリケーション全体の設定を削除します。

### フロー limit-across-applications limit

ルールベースのすべてのアプリケーションにわたるフローの最大数を指定します。

limitには1 ~ 4000000000の整数を指定してください。

デフォルト：制限なし

### 非TCP制限

非TCPタイプフローの最大制限を指定します。

limitには1 ~ 4000000000の整数を指定してください。

デフォルト：制限なし

### TCP制限

TCPフローの最大制限を指定します。

limitには1 ~ 4000000000の整数を指定してください。

デフォルト：制限なし

## 使用方法 :

このコマンドを使用して、フローの種類に関係なくルールに許可されるフローの総数を制限するか、プロトコルに基づいてフローを制限する(TCP以外 ( 接続なし ) またはTCP ( コネクション型 ) )を使用します。

加入者がこれらの制限を超えようとする、新しいフローのパケットが廃棄されます。このコマンドの制限処理には、UDP、TCP、ICMPおよび一部の除外フローに関する次の側面があります。

- UDP/ICMP:システムは、フローのタイムアウトを待ってから、カウンタを更新し、フローの数から削除します。
- TCP : TCPフローが終了した後、システムは短い時間だけ待機して、一方の端からの欠落したパケットの再送信に対応します。TCPフローは終了しますが、タイムアウトの待機時間は、この制限処理に対して免除されます。
- 除外フロー : ACS Charging Action Configuration Modeでnoに設定されているflow limit-for-flow-typeコマンドで指定された他のすべてのフローが除外されます。

例 :

このコマンドは、ルールベースのフローの最大数を200000に定義します。

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