ASR5x00-Serie: Sessmgr WARN-Status aufgrund einer hohen Anzahl von HTTP-Datenflüssen

Inhalt

Einführung

In diesem Dokument wird das Problem beschrieben, dass sessmgr aufgrund der hohen Anzahl von HTTP-Datenflüssen in den WARN-Status wechselt. Dieses Problem wird bei Cisco Aggregated Service Routern (ASR) 5 x 00 gemeldet.

Problem

Der Status "Sessmgr" lautet WARN und hohe Speichernutzung.

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

Diese Fehlerprotokolle werden während des Prozesses generiert. Aufgrund dieses Fehlerprotokolls sind keine Auswirkungen auf den Teilnehmer zu verzeichnen. Sobald der Anruf von Sessmgr abgelehnt wurde, der sich im **WARN-**Zustand befindet, versucht das System, verschiedene Sitzungen abzuhalten, und der Anruf geht durch.

```
[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
```

Fehlerbehebung

Erfassen Sie **die** Ausgabe **der Support-Details**, und prüfen Sie, ob die Befehlsausgaben eine weitere Fehlerbehebung ermöglichen.

Das Speicherproblem hängt mit der Anzahl der Flows zusammen, die der Sessmgr verarbeitet.

Die Korrelation zwischen Sessmgr mit einem hohen Speicherverbrauch und einer hohen Anzahl an Datenflüssen ist erkennbar.

```
 ******** 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!
--------------------------------------------------------------------------------
       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
```

Für betroffene Sessmgrs (und für eine nicht betroffene Sessmgrs) sollten Sie diese Befehlsausgaben erfassen, wobei *x* die Sessmgr-Instanz ist.

```
show messenger proclet facility sessmgr instance <x> heap
show messenger proclet 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 faciltity sessmgr instance <x> max
```

Überprüfen Sie, ob unoptimierte Regeln und Regelgruppen viel Speicher verbrauchen.

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

Die höchste Speicherbelegung ergibt sich aus diesen Funktionen, die auf den Befehlsausgaben basieren.

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

Sie können auch die maximale Anzahl gleichzeitiger HTTP-Datenflüsse überprüfen, die durch Anrufzeilen erreicht werden.

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

Sie können daraus schließen, dass eine große Anzahl von HTTP-Sitzungen zugewiesen wird, was auf den hohen HTTP-Verkehr zurückzuführen sein könnte. Außerdem gibt es fast 1044671491 Calllines, die mehr als 10000 HTTP-Datenflüsse gleichzeitig haben. Dies führt zu einer hohen Speichernutzung.

Lösung

Sie verfügen über die CLI, um die Anzahl der Datenflüsse pro Teilnehmer zu begrenzen.

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

Cisco empfiehlt, **Flow-Limit-Limit-Anwendungen-übergreifend** auf **5000** zu konfigurieren, wie es in allen betroffenen Regeldatenbanken empfohlen wird, in denen eine große Anzahl von HTTP-Datenverkehr zu erkennen ist.

Dies ist die Prozedur zum Konfigurieren des Befehls

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

Weitere Informationen zu diesem Befehl.

Fluss Anwendungsübergreifende Begrenzung

Mit diesem Befehl können Sie die Gesamtanzahl der an eine Regeldatenbank gesendeten

gleichzeitigen Datenflüsse pro Subscriber/APN, unabhängig vom **Flow-**Typ, begrenzen oder Datenflüsse basierend auf dem Protokolltyp unter der Sitzungssteuerungsfunktion begrenzen.

Produkt:

ACS

Berechtigung:

Sicherheitsadministrator, Administrator

Modus:

```
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)#
```

Syntax

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

Wenn die Konfiguration zuvor konfiguriert wurde, löscht die **Flow-Limit-Cross-Applications-**Konfiguration aus der aktuellen Regelebase.

Fluss Grenzwert für Anwendungen

Gibt die maximale Anzahl an Datenflüssen für alle Anwendungen der Regelebase an.

Der Grenzwert muss eine ganze Zahl zwischen 1 und 4000000000 sein.

Standard: Keine Einschränkungen

Nicht-TCP-Grenzwert

Gibt die maximale Grenze für Nicht-TCP-Typflüsse an.

Der Grenzwert muss eine ganze Zahl zwischen 1 und 4000000000 sein.

Standard: Keine Einschränkungen

TCP-Grenzwert

Gibt die maximale Grenze für TCP-Datenflüsse an.

Der Grenzwert muss eine ganze Zahl zwischen 1 und 4000000000 sein.

Standard: Keine Einschränkungen

Verwendung:

Verwenden Sie diesen Befehl, um die Gesamtzahl der für eine Regelebase zulässigen Datenflüsse unabhängig vom **Flow-**Typ zu begrenzen oder Datenflüsse, die auf dem Protokoll basieren, zu beschränken - nicht TCP (verbindungslos) oder TCP (verbindungsorientiert).

Wenn ein Teilnehmer versucht, diese Grenzwerte zu überschreiten, verwirft das System die Pakete des neuen **Datenflusses**. Diese begrenzte Verarbeitung dieses Befehls umfasst die folgenden Aspekte für UDP, TCP, ICMP und einige der ausgenommenen Flows:

- UDP/ICMP: Das System wartet auf das **Flow**-Timeout, bevor es den Zähler aktualisiert und aus der Anzahl der Datenflüsse entfernt.
- TCP: Nachdem ein TCP-**Datenfluss** beendet wurde, wartet das System eine kurze Zeit lang, um die erneute Übertragung eines verpassten Pakets von einem Ende aus zu ermöglichen. TCP-Datenflüsse, die beendet wurden, aber noch in der Wartezeit sind für diese Limit-Verarbeitung ausgenommen.
- Exemptierte Flows: Das System befreit alle anderen Datenflüsse, die mit dem Befehl **flow limit-for-flow-type** im Konfigurationsmodus "ACS Charging Action" auf **no** festgelegt wurden.

Beispiel:

Dieser Befehl definiert die maximale Anzahl von 200000 Datenflüssen für die Regeldatenbank:

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