Fehlerbehebung bei Durchmesserverlusten von Nachrichten aufgrund von Max-Outstanding-CCRU-Grenzwert

Inhalt

Einführung

In diesem Dokument werden die Details der Cisco Packet Data Network Gateway (PGW)/Policy and Charging Enforcement Function (PCEF) Syslog-Fehlermeldung bezüglich des Verfalls von Durchmessernachrichten beschrieben und Methoden zur Behebung des Problems vorgeschlagen.

Problem Syslog-Meldung

Im Folgenden sind einige Beispiele für Syslog-Meldungen aufgeführt, die von StarOS generiert werden, wenn die maximale Anzahl ausstehender Nachrichten für ein Credit Control Update Request für einen bestimmten Abonnenten erreicht wird.

```
Nov 18 08:01:44 evlogd: [local-60sec44.282] [ims-authorizatn 98916 error] [1/0/6046 <sessmgr:78>
imsa_sgx.c:1493] [callid 17100da1] [software internal user syslog] [IMSI: 123456789012341,
MSISDN :1234567890] Pending CCR-U equal to Max Outstanding threshold. CCR-U Dropped for :
USAGE_REPORT

Nov 21 07:02:07 evlogd: [local-60sec7.271] [ims-authorizatn 98916 error] [1/1/5983 <sessmgr:31>
imsa_sgx.c:1493] [callid 090fe704] [software internal user syslog] [IMSI: 123456789012342,
MSISDN :1234567891] Pending CCR-U equal to Max Outstanding threshold. CCR-U Dropped for :
USAGE_REPORT

Nov 24 15:17:52 evlogd: [local-60sec52.471] [ims-authorizatn 98916 error] [1/1/5185
<sessmgr:271> imsa_sgx.c:1493] [callid 46f53fd5] [software internal user syslog] [IMSI:
123456789012343, MSISDN :1234567892] Pending CCR-U equal to Max Outstanding threshold. CCR-U
Dropped for : USAGE_REPORT

Nov 22 21:05:58 evlogd: [local-60sec58.422] [ims-authorizatn 98916 error] [3/1/5966 <sessmgr:10>
imsa_sgx.c:1493] [callid 02ce20d8] [software internal user syslog] [IMSI: 123456789012344,
MSISDN :6789012344] Pending CCR-U equal to Max Outstanding threshold. CCR-U Dropped for :
USAGE_REPORT
```

Ursache des Problems

Die Fehlermeldung wird angezeigt, wenn der StarOS PGW/PCEF-Durchmesser IP Multimedia Subsystem (IMS)-Authorization-Service die Grenze für **maximal ausstehende** Cr-u-Diameter-

Nachrichten zur Policy and Charging Rules Function (PCRF) für eine bestimmte Sitzung erreicht. Sobald diese maximale Grenze erreicht ist, beginnt StarOS damit, nachfolgende CCR-U-Nachrichten (Credit Control Request) an PCRF für diese Sitzung zu verwerfen, bis die ausstehenden Nachrichten auf eine Zahl unterhalb der konfigurierten Obergrenze reduziert werden. Die ausstehenden Nachrichten werden entweder durch den Empfang einer Antwort auf eine zuvor ausstehende Nachricht oder durch das Verfallsdatum dieser ausstehenden Nachrichten reduziert.

Fehlerbehebung

Dieses Fehlerprotokoll ist in der Regel ein Hinweis auf die Änderung des Anrufmodells, das eine Konfigurationsoptimierung erfordert, da die Anzahl der ausstehenden CCR-U-Meldungen für eine bestimmte Gx-Sitzung erhöht wird. In diesem Fall wird das IMSI-Protokoll im Protokoll gedruckt. Rufen Sie nach Möglichkeit die historische Paketerfassung dieses Teilnehmers ab, um herauszufinden, warum die Teilnehmersitzung versucht hat, mehr als die konfigurierte ausstehende CCR-U-Sitzung zu initiieren. Suchen Sie außerdem nach der Anzahl der eindeutigen IMSIs, die gedruckt werden, um eine Vorstellung vom Umfang des Problems zu erhalten. Um das Problem vom StarOS-Ende aus zu beheben, gehen Sie zur StarOS-Konfiguration und aktualisieren Sie die Konfiguration für "max-ausstehende-ccr-u" unter diesem IMS Authorization Service basierend auf dem neuen Teilnehmerverhalten oder dem neuen Anrufmodell. Neben dieser Änderung im StarOS muss der Peer Diameter Routing Agent (DRA)/PCRF eine solche Anzahl ausstehender Nachrichten pro Sitzung unterstützen und über die TPS-Kapazität verfügen, um die steigende Anzahl von Nachrichten zu bewältigen, die aufgrund des Anrufmodells und der Konfigurationsänderung verursacht werden können. Wenn mehrere ausstehende CCR-U-Nachrichten vorliegen, kann StarOS diese Nachrichten in einer falschen Reihenfolge beantworten.

Im Folgenden sehen Sie einen Ausschnitt aus der Ausgabe einer SSD-Datei (Show Support Details), die die Anzahl der CCR-U-Ausfälle aufgrund des Grenzwerts für max-ausstehende CCRU anzeigt:

```
******** show ims-authorization policy-control statistics debug-info *******
callid_mismatch          : 0
capi_session_init        : 236157394
capi_session_add         : 236157394
capi_session_update      : 1657200358
capi_session_del         : 235071716
capi_session_gone        : 235067742
capi_session_checkpoint  : 0
capi_session_recover     : 0
capi_config              : 22902
dapi_message_received    : 2492716060
dapi_message_sent        : 2492723514
asr_err                  : 0
ccru_dropped_max_outstanding: 433034
```

Mit diesem StarOS-Befehl können Sie den konfigurierten Wert von maximal ausstehenden CCR-U-Nachrichten ermitteln, die 4 ausstehende CCR-U-Nachrichten anzeigen, die pro Sitzung zulässig sind.

```
# show ims-authorization service name <Your GX service name>
Context: SAMPLE-CONTEXT
IMS Authorization Service name: sampleGx
Service State: Enabled
 Failure Handling: Retry and Terminate Max-Outstanding-CCRU: 4
```

```
Local Policy Service: NA
Host Selection: Table: 1 Algorithm: Round-Robin
```

Dieser Ausschnitt zeigt den Teil der StarOS-Konfiguration, in dem dieser Wert definiert ist.

```
config
  context SAMPLE-CONTEXT
    ims-auth-service sample-gx
    policy-control
    diameter origin endpoint sample-pcrf-ep
    diameter dictionary dpca-custom11
    diameter request-timeout 60 deciseconds msg-type any
    endpoint-peer-select on-host-select-failure
    no event-report-indication
    custom-reauth-trigger none
    diameter host-select table 1 algorithm round-robin
    max-outstanding-ccr-u 4
```

Zugehörige Informationen

- Leitfaden zur StarOS CLI
- Technischer Support und Dokumentation für Cisco Systeme