Troubleshoot of Initial Attach Success Rate Degradation in ePDG

Contents

Introduction

This document describes the issues related to Initial Attach Success Rate (ASR) degradation in Evolved Packet Data Gateway (ePDG).

Overview

The Initial ASR is a vital metric that indicates the success rate of the total number of session setup attempts.

The formula for the Key Performance Indication (KPI) contains the total number of the ePDG session setup attempts and the total number of ePDG session setup successes. If the number of successful attempts decreases, then the whole KPI degrades.

Basic Prechecks

For ePDG functionality, Internet Protocol Security (IPsec) is the process that takes care of IPsec transactions. So, for any ePDG case, some of the prechecks are to be followed before you proceed to troubleshoot the issue.

1. Check the DPC card status as ipsecmgr runs on these cards. DPC cards must be in an active state (except standby cards).

```
show card table
```

2. Check the status of resources for each like **sessmgr/ipsecmgr** in order to review if any abnormal pattern of traffic flow is observed in terms of the number of sessions per **sessmgr/ipsecmgr** of each card or if these processes are in warn/over state. For example, in this output, you see **ipsecmgr** is in over state as shown here.

```
[local]abc# show task resources | grep -v good
Thursday January 19 19:41:15 UTC 2023
                    task   cputime        memory     files      sessions
 cpu facility      inst  used  allc   used  alloc used allc  used  allc S status
---------------------- ----------- ------------- --------- ------------- ------
 3/0 ipsecmgr       261 0.28%   75% 383.4M 300.0M  196 1500    30  6000 -   over
```

```
 3/0 ipsecmgr       262 0.23%   75% 378.0M 300.0M  185 1500    28  6000 -   over
 3/0 ipsecmgr       263 0.46%   75% 382.7M 300.0M  197 1500    30  6000 -   over
 3/0 ipsecmgr       264 0.22%   75% 383.7M 300.0M  212 1500    27  6000 -   over
....
```

Here is an example of sessmgrs running on cards 4 and 5 having uneven distribution of sessions:

```
[local]xyx# show task resources max | grep -i sess
Monday February 17 21:52:38 UTC 2023
                   task   cputime        memory     files      sessions
4/0 sessmgr         45   12%  100% 429.9M  2.00G  129  500  4260 26000 I   good
 4/0 sessmgr         48   12%  100% 428.8M  2.00G  129  500  4267 26000 I   good
 4/0 sessmgr         49   12%  100% 428.5M  2.00G  129  500  4274 26000 I   good
 4/0 sessmgr         52   12%  100% 428.3M  2.00G  129  500  4258 26000 I   good
 5/0 sessmgr       5002 2.34%   50% 87.46M 190.0M   89  500    --    -- S   good
 5/0 sessmgr          2   12%  100% 458.5M  2.00G  107  500  9279 26000 I   good
 5/0 sessmgr          3   13%  100% 459.9M  2.00G  106  500  9281 26000 I   good
```

3. Check crypto statistics if there is any drop at IPsec level:

```
show crypto managers detail     ----------------- this command shows statistics per ipsec so we can chec
show crypto statistics ikev2    ----------------- this command shows overall ikev2 statistics for EPDGs
```

> **Note**: Prechecks are important because sometimes issues are found at the card level where the IPsec/sessmgr of a particular card is not able to take user sessions/traffic and you can clearly see drops at the IPsec level in the statistics mentioned previously.

Logs Required

Few points to ask to troubleshoot the issue better:

- Since when the issue is seen (referring to the exact date and time of the starting of the issue)
- Were there any changes made in the network or any configuration changes?
- Formulas used for ASR in ePDG
- How many ePDGs are there in the affected circle and among them is the issue observed in all ePDGs or one specific EPD

Here are the logs to be collected:

- Show Support Details (SSD) from the node before the time the issue start, during the issue and after the issue (if the issue is not occurring anymore).
- Syslogs for 1 week before the issue (for comparative study), covering the time of the issue and after the issue (if the issue is not occurring anymore).
- Simple Network Management Protocol (SNMP) traps for 1 week before the issue (for comparative study), covering the time of the issue and after the issue (if the issue is not occurring anymore).
- Bulkstats 1 week before the issue (for comparative study), covering the time of the issue and after the

issue (if the issue is not occurring anymore).

- Monsub is to be collected as per these options:

```
monitor subscriber with options S, X, A, Y, 19, 33, 34, 35, 26, 37, 40, 50, 88, 89. Collect traces at ve
```

- 3 SSD at an interval of 30-45 minutes to find the reason for rejection.

Note: Disconnect-reason 519 to 533 are for ePDG session reject.

- You need to compare configurations from the problematic and non-problematic nodes.

```
show configuration

show configuration verbose
```

- Needed to debug logs:

```
logging filter active facility sessmgr level <critical/error>
logging filter active facility ipsec level <critical/error>
logging filter active facility ikev2 level <critical/error>
logging filter active facility epdg level <critical/error>
logging filter active facility diameter level<critical/error>
logging filter active facility egtpc level<critical/error>

logging active ------------------- to enable debug logs
no logging active  --------------- to disable debug logs

Note :: Above mentioned debug logs are taken considering debug logs at the level of critical/error but w

logging filter active facility egtpc level debug
```

- The output of commands that can be useful for troubleshooting:

```
show epdg-service all counters
-> View ePDG service information and statistics

show epdg-service statistics
-> View ePDG service statistics

show epdg-service session all
-> View ePDG service session information

show egtpc statistics interface edpg-egress debug-info
-> View egtpc statistics for  ePD-egress
```

```
show session [ disconnect-reasons | duration | progress | setuptime | subsystem ]
-> iew additional session statistics.

show crypto statistics ikev2
-> View IKEv2 statistics

show diameter aaa-statistics all
->View Diameter AAA server statistics.

show subscribers epdg-only [ [ all ] | [ callid call_id ]]
-> View a list of ePDG subscribers currently accessing the system.

show subscribers epdg-service service_name [ [ all ] | [ callid call_id ]]
 ->View a list of ePDG subscribers currently accessing the system per ePDG service.

show crypto managers summary ipsec-sa-stats
---Need to collect with some iterations to check ipsec associations stats
```

> **Warning**: When you are asked to collect logs like debug logs, logging monitor, mon-sub, and mon pro, always collect in the maintenance window and always monitor the load on the CPU.

Analysis

This is the example of a formula for the ePDG Initial Attach Sessions Success Rate:

```
Initial Attach Sessions Success Rate ==((totsetupsuccess / totsetupattempt )*100)
```

From the Statistics and Counters Reference - Bulkstatistic Descriptions, you can find the counters that are used in the formula to know their meaning.

```
epdg totsetup-attempt- Total number of epdg session setup attempts. Increments upon receiving IKE_AUTH (

epdg totsetup-success Total number of epdg session setup success. Increments upon successful IPv4/IPv6/D
```

From the SSD, you can see the output show crash list to see if there are any continuous/high number of crashes that lead to the KPI dip.

From the SSD, you can check show license info and show resource output to see if the license is not expired or the session count is within the limit.

```
******** show resources *******
Wednesday December 07 16:58:25 IST 2022
 EPDG Service:
    In Use              : 1118147
    Max Used            : 1450339 ( Tuesday November 29 00:06:00 IST 2022 )
    Limit               : 1600000
```

```
    License Status      : Within Acceptable Limits  >>>>>
```

From the output of the command `show epdg-service statistics` , the failure reason which is incremented can be checked.

```
******** show epdg-service statistics *******
Session Disconnect reason:
  Remote disconnect:          580994781   Admin disconnect:           168301
  Idle timeout:               0           Absolute timeout:           0
  Long duration timeout:      0           Session setup timeout:      169445470
  No resource:                185148      Auth failure:               7634409
  Flow add failure:           0           Invalid dest-context:       0
  Source address violation:   42803       LMA Revocations(non-HO):    0
  Duplicate Request:          19973167    Addr assign failure:        0
  LTE/Other handoff:          1310701444  Miscellaneous reasons:      456928065
  MIP-reg-timeout  :          0           Invalid-APN  :              0
  ICSR Procedure   :          0           Local PGW Res. Failed :     10424
  Invalid QCI :               0           UE Redirected :             0
  Roaming Mandatory :         0           Invalid IMEI :              3
```

From the problematic traces, the reason for rejections can be found and can be compared with the non-problematic trace for any discrepancy.

Some of the scenarios that you can get from traces:

In Case-1 (diameter-no-subscription), after analyzing the traces, it is observed that a Diameter EAP request is sent to the AAA server. However, the response received indicates a failure with the Cause Code **DIAMETER_ERROR_USER_NO_APN_SUBSCRIPTION**. As a result, the Serving Packet Data Gateway (SPGW) registers the same failure with the disconnect reason `diameter-no-subscription`. This behavior is considered normal for a user without a subscription, as they are rejected by the authentication, authorization, and accounting (AAA) server at the time of the process.

> **Note**: Get the APN subscription checked at AAA/HSS for the test number and if possible arrange online testing for the same.

In Case-2 (Session-setup-timeout), upon analyzing the traces, it is observed that the session setup is being rejected with the disconnect reason `Session-setup-timeout`. Further investigation revealed that the ePDG is sending an `EGTP_CREATE_SESSION_REQUEST` to the SPGW, but it is not receiving any response for the same. It can be observed that three consecutive requests are sent without receiving any response.

```
Solution : In such cases mostly need to check why SPGW is not sending any response towards EPDG because
```

In Case-3, a request with a specific Access Point Name (APN) is being sent to the PGW, but it is being rejected with the Cause Code **EGTP_CAUSE_USER_AUTHENTICATION_FAILED**.

```
Solution : Here the issue can be either at HSS or EPDG itself need to check the authentication parameter
```

To investigate all the mentioned cases, it is necessary to capture debug logs for a more detailed analysis. These logs are examined according to the 3GPP standard, and based on the findings, an appropriate action plan or workaround can be determined. It is important to note that the course of action can vary depending on the specific scenario.