Fehlerbehebung bei S11-KPI-Degradation

Inhalt

Einleitung

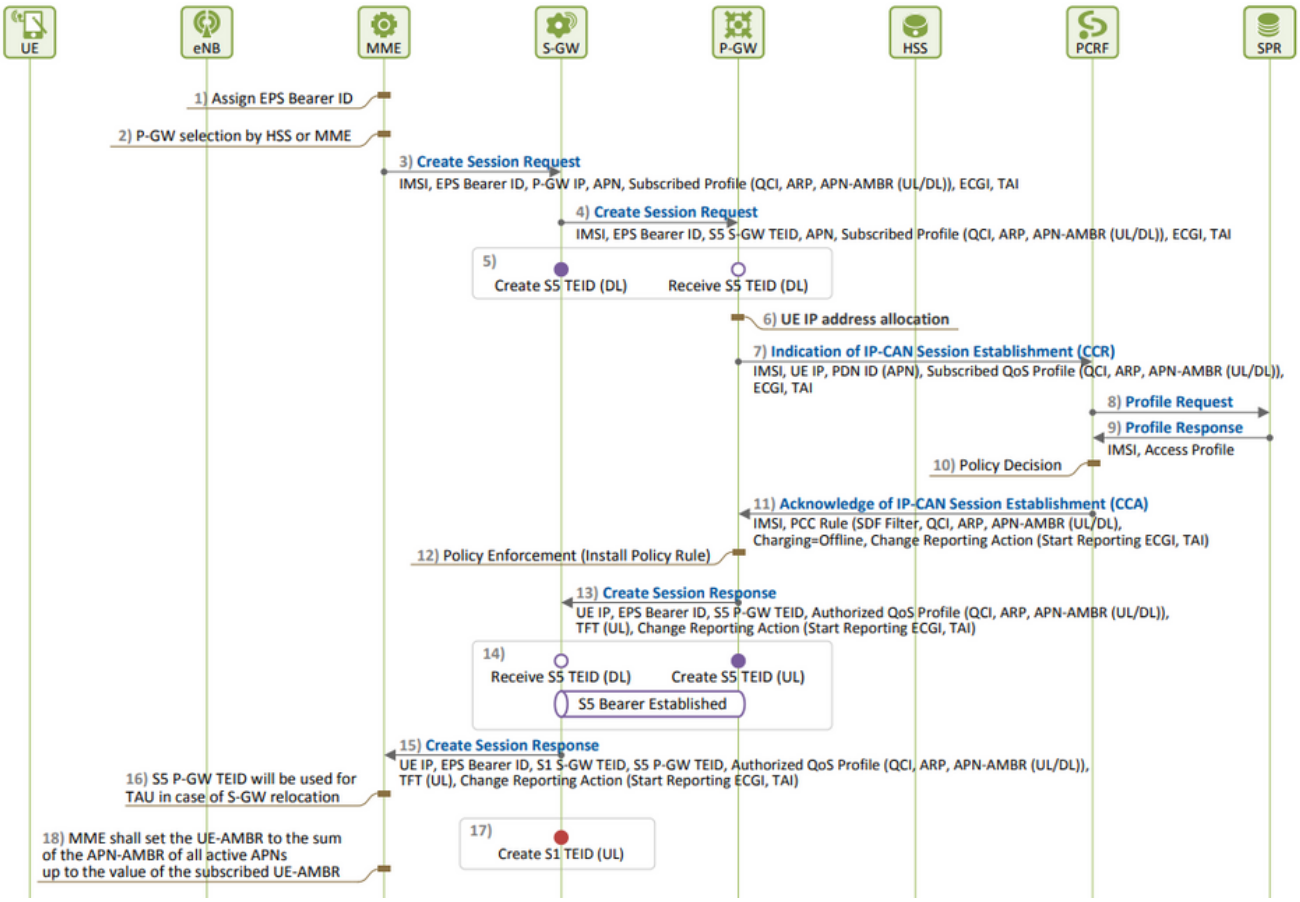
In diesem Dokument wird die Behebung von Problemen mit S11-Leistungskennzahlen (Key Performance Indicators, KPI) beschrieben.

Überblick

S11 ist die Schnittstelle, die die Mobility Management Entity (MME) und das Serving Gateway (SGW) in einem LTE-Netzwerk (Long Term Evolution) verbindet. Die Schnittstelle verwendet Gn oder GPRS Tunneling Protocol-Control (GTP-C).

Meldungen in der S11-Schnittstelle

- Sitzungsanfrage/Antwort erstellen
- Sitzungsanfrage/Antwort ändern
- Sitzungsanfrage/Antwort löschen



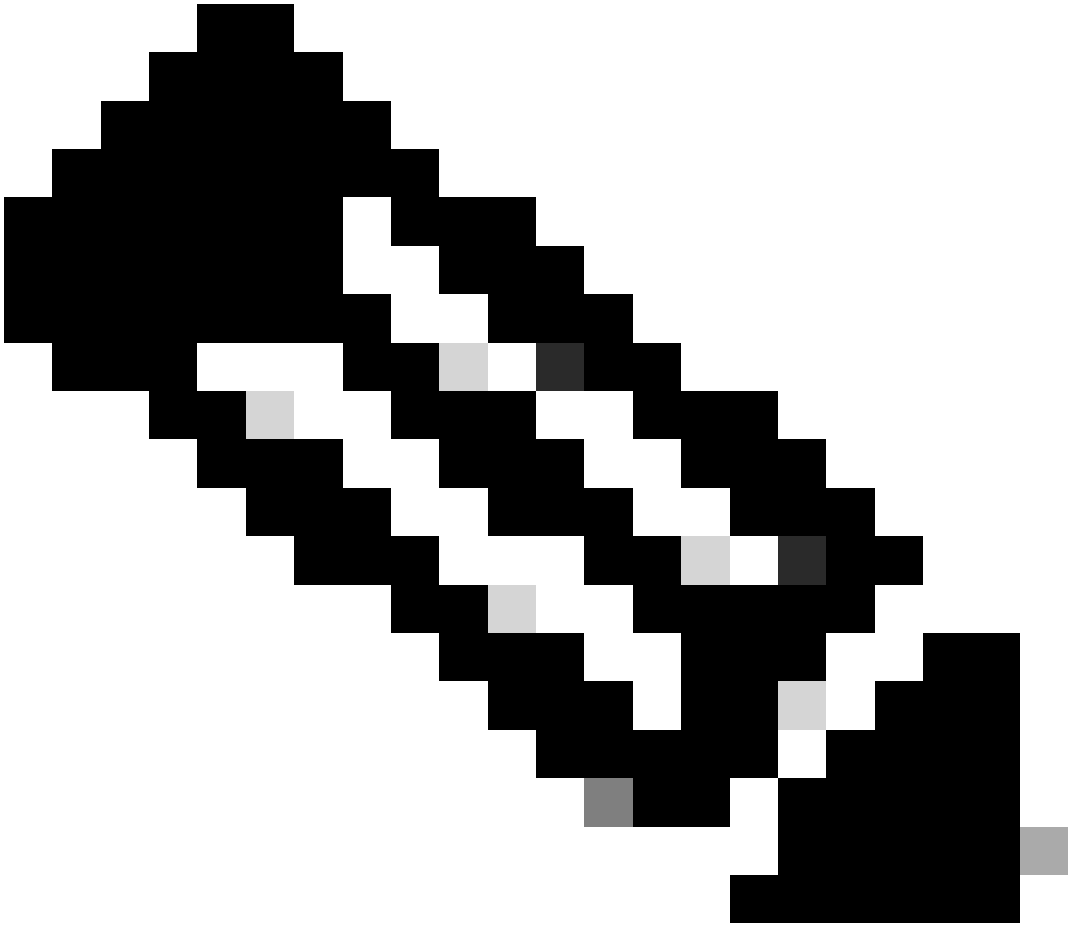
Einrichtung von EPS-Sitzungen:

- Eine Verschlechterung der S11-Kennzahlen wird beobachtet, wenn Sie mehr Ablehnungen von Create Session Requests (CSR) sehen als bei den CSR-Versuchen, die die Ursache sein müssen.

Sie können die Formel kennen, die verwendet wird, um den KPI zu messen, und sich alle Zähler notieren, die in der Formel enthalten sind, und den genauen Zähler bestimmen, der für den Abbau verantwortlich ist.

```
S11 ASR (SPGW)  = ((tun-sent-cresessrespaccept+ggsn_tun-sent-cresessrespdeniedUserAuthFailed+tun-sent-c

PDN Connectivity Success Rate (MME) : ((%esmevent-pdncon-success%) + (%esm-msgtx-pdncon-rej%))*) / (%es
```



Hinweis: Die Formel kann je nach Art der Messung variieren.

Auf der ersten Ebene erforderliche Protokolle:

- KPI-Trend, der die Verschlechterung darstellt.
- Verwendete KPI-Formel.
- Unformatierte Bulkstat-Zähler und Codetrends vom Anfang des Problems an.
- Erfassen Sie zwei Instanzen von Show Support Details (SSDs) vom Knoten in einem Intervall von 30 Minuten während problematischer Zeiträume.
- Syslogs reichten von zwei Stunden vor dem Abbau bis zur aktuellen Zeit. mon sub/pro traces und logging monitor msid <imsi> .

Reihenfolge der Fehlerbehebung

- Bewerten Sie den KPI-Trend jedes Zählers, der an der S11-KPI-Formel beteiligt ist, durch Analyse der Bulkstats.

- Vergleichen Sie den KPI-Trend bei problematischen Zeitachsen mit unproblematischen Zeitachsen.

- Untersuchen Sie, wie der erkannte problematische Bulkstat-Zähler basierend auf dem Fluss definiert wird, und stellen Sie Muster fest.

- Sammeln Sie Gründe für die Verbindungstrennung vom Knoten durch mehrere Iterationen in Intervallen von 3 bis 5 Minuten.

Sie können das Delta der Ursachen für die Trennung zwischen zwei SSDs analysieren, die zu unterschiedlichen Zeitstempeln erfasst werden. Der Grund für die Verbindungstrennung, der eine deutliche Erhöhung des Delta-Werts anzeigt, kann als Ursache für die Verschlechterung der Kennzahlen betrachtet werden. Eine detaillierte Beschreibung der Ursachen für die Verbindungstrennung finden Sie in der Cisco Statistik- und Zählerreferenz unter: https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21-23/Stat-Count-Reference/21-23-show-comman...

show session disconnect-reasons verbose

5. Überprüfen Sie die egtp-Statistik basierend auf dem Typ des Knotens, für den sie erstellt wurde:

--- SGW end -----

show egtpc statistics interface sgw-ingress path-failure-reasons
show egtpc statistics interface sgw-ingress summary
show egtpc statistics interface sgw-ingress verbose
show egtpc statistics interface sgw-ingress sessmgr-only

show egtpc statistics interface sgw-egress path-failure-reasons
show egtpc statistics interface sgw-egress summary
show egtpc statistics interface sgw-egress verbose
show egtpc statistics interface sgw-egress sessmgr-only

---- PGW end -----

show egtpc statistics interface pgw-ingress path-failure-reasons
show egtpc statistics interface sgw-ingress summary
show egtpc statistics interface sgw-ingress verbose
show egtpc statistics interface sgw-ingress sessmgr-only

--- MME end -----

show egtpc statistics interface mme path-failure-reasons
show egtpc statistics interface mme summary
show egtpc statistics interface mme verbose
show egtpc statistics interface mme sessmgr-only

6. Nachdem Sie den spezifischen Zähler identifiziert haben, der das Problem verursacht, müssen Sie die mon-sub/mon-pro-Anrufnachverfolgungen erfassen, um den spezifischen Anrufverlauf, der die Leistungskennzahlen herabsetzt, weiter zu analysieren und zu identifizieren. Darüber hinaus können Sie externe Tools verwenden, um Wireshark-Traces für eine detailliertere Analyse zu erhalten.

Die Befehle zum Erfassen von Mon-Subtraces sind wie folgt:

monitor subscriber with options 19, 26,33, 34, 35, 49,A,S, X, Y, verbosity +5 during the issue.

mon-pro with options 19, 26,33, 34, 35, 49,A,S, X, Y, verbosity +5 during the issue if no mon-sub is present.

More options can be enabled depending on the protocol or call flow we need to capture specifically

In Fällen, in denen die Erfassung von Ablaufverfolgungen wie mon-sub aufgrund eines minimalen Prozentsatzes der KPI-Verschlechterung nicht möglich ist, müssen Sie stattdessen Debug-Protokolle auf Systemebene erfassen. Dazu gehört das Erfassen von Debug-Protokollen für sessmgr und egptc sowie, falls erforderlich, das Erfassen von Gateway-spezifischen Flows.

logging filter active facility sessmgr level debug
logging filter active facility egtpc level debug
logging filter active facility sgw level debug
logging filter active facility pgw level debug

logging active ---------- to enable
no logging active ---------- to disable

Note :: Debugging logs can increase CPU utilization so need to keep a watch while executing debugging logs

7. Wenn Sie nach der Analyse der Debug-Protokolle die Ursache des Problems ermitteln, können Sie mit der Erfassung der Kerndatei für das jeweilige Ereignis fortfahren, wobei Sie die Fehlerprotokolle beobachten.

logging enable-debug facility sessmgr instance <instance-ID> eventid 11176 line-number 3219 collect-cores 1

For example :: consider we are getting below error log in debug logs which we suspect can be a cause of issue
and we don;t have any call trace

[egtpc 141027 info] [15/0/6045 <sessmgr:93> _handler_func.c:10068] [context: INLAND_PTL_MME01, contextID: 6] [software internal user syslog] [mm

So in this error event

facility :: sessmgr
event ID = 141027
line number = 10068

Warnung: Wenn Sie die Erfassung von Protokollen wie Debug-Protokollen, Protokollierungsüberwachung, Mon-Sub oder Mon-Pro anfordern, ist es wichtig, sicherzustellen, dass diese Protokolle während eines Wartungsfensters erfasst werden. Außerdem ist es wichtig, die CPU-Last während dieser Zeit zu überwachen.

Analyse und Identifizierung von Symptomen

- Prüfen Sie zunächst, ob im System häufige Abstürze von SSD auftreten.

```
show crash list
```

- Überprüfen Sie, ob Lizenzprobleme aufgetreten sind. In einigen Fällen kann die Lizenz am Serving Packet Data Gateway (SPGW) nach Ablauf keine neuen Anrufe mehr annehmen. Dies führt zu fehlgeschlagenen Anrufen und zu einer Verschlechterung oder einem Absinken von S11.

```
show resource info
```

- Überprüfen Sie, ob sich aufgrund einer hohen Arbeitsspeicher- oder CPU-Auslastung mehrere Sessmgr-Instanzen in einem Warn-/Überschreibungsstatus befinden. Wenn solche Instanzen gefunden werden, überprüfen Sie, ob neue Anrufe aufgrund dieser Bedingungen abgelehnt werden.

- Aus den Debug-Protokollen können Sie überprüfen, auf welcher Schnittstelle die Anrufabweisungsfehler aufgetreten sind.

Tritt für einen bestimmten Teilnehmer im Kontext "sgw-egress" eine erhebliche Anzahl von Anrufabweisungsfehlern auf, gefolgt von der Ablehnung desselben Teilnehmers im Kontext "sgw-ingress", kann daraus geschlossen werden, dass die Abweisungen vom Packet Data Gateway (PGW) im S11-Kontext an SGW-> MME gesendet werden. Um das PGW-Ende weiter zu bestätigen und eine Fehlerbehebung durchzuführen, können Sie für diese IMSI jetzt einen Mono-Sub-Befehl eingeben.

```
2022-Nov-26+00:20:51.763 [egtpc 141018 unusual] [7/0/16871 <sessmgr:579> _handler_func.c:3227] [context

2022-Nov-26+00:20:51.763 [egtpc 141018 unusual] [7/0/16871 <sessmgr:579> _handler_func.c:2505] [context
```

- Manchmal kann es mehrere Ablehnungsgründe für das KPI-Dip geben, daher müssen Sie jeden Grund einzeln überprüfen und entsprechend fortfahren.

So kann es beispielsweise bei bestimmten IMSI-Serien (International Mobile Subscriber Identity) für In-Roamer-Abonnenten zuno_resource_available/user_auth_failure Fehlererhöhungen kommen, sodass diese vom PGW überprüft werden müssen. Es kann Gründe geben, z. B. remote peer not responding eine Sitzungsanfrage zu erstellen, die beim SGW ein Timeout erhält, was zu einer Verschlechterung der S11-Kennzahl führen kann. Diese Sitzung zum Erstellen konnte vom SGW alsNo_resource_available in Richtung MME abgelehnt werden. Diese Ablehnungsursachencodes können aus den Überwachungsprotokollprotokollen ermittelt werden, und Sie können die Optionen zum Erstellen von Sitzungsanfragen und zum Erstellen von Sitzungsantworten überprüfen, um die spezifischen IP-Adressen zu identifizieren, von denen diese Ablehnungsursachencodes gesendet werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.