Problembehandlung beim Durchsuchen von Benutzerdaten für bestimmte Web-URLs

Inhalt

Einleitung

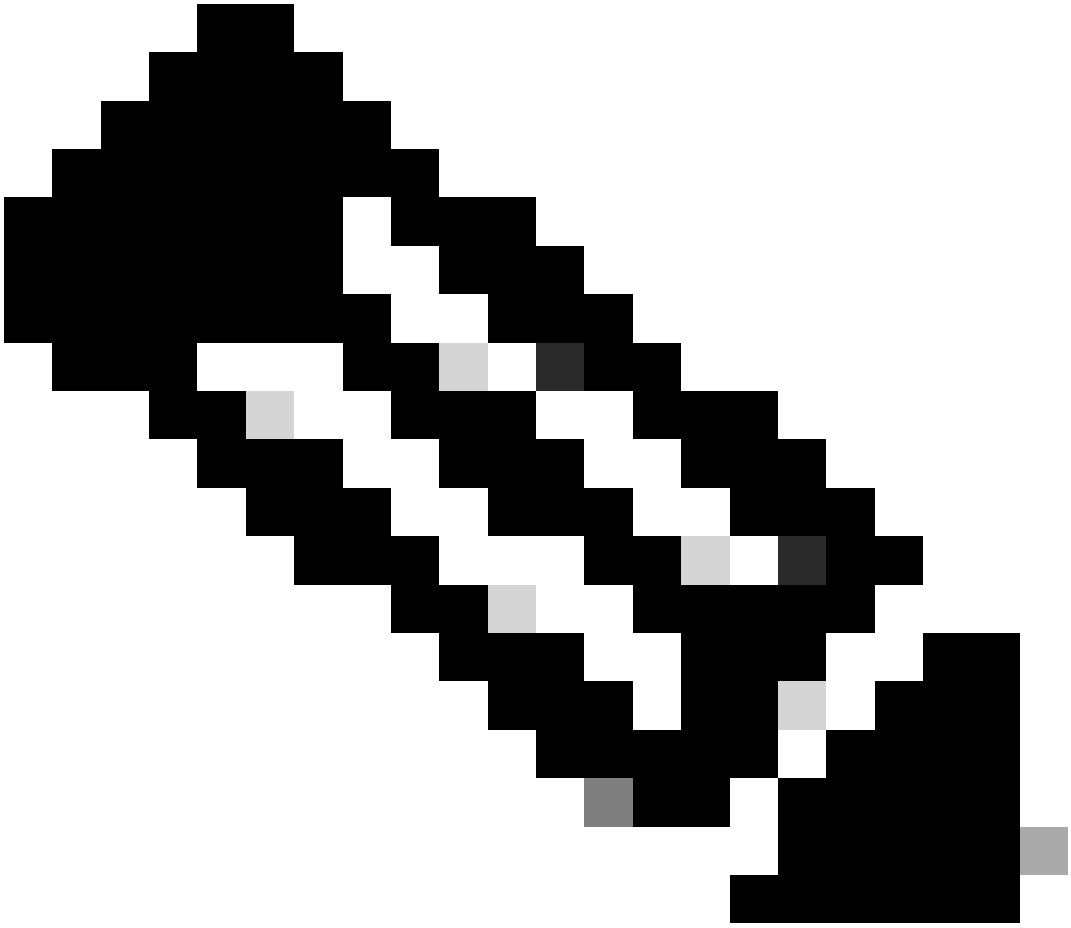
In diesem Dokument werden die Probleme beim Durchsuchen von Benutzerdaten im 4G-Netzwerk für alle Uniform Resource Locators (URLs) beschrieben.

Voraussetzungen

Cisco empfiehlt, dass Sie mit den Funktionen dieser Knoten vertraut sind:

- Serving Packet Data Gateway (SPGW)
- CUPS (Control and User Plane Separation)

Identifizierung der Symptome



Hinweis: Bevor Sie mit dem Testen und der Protokollerfassung beginnen, müssen Sie diese Details überprüfen.

1. Überprüfen Sie, bei welchem Datentyp das Problem auftritt: IPv4/IPv6/IPv4v6

2. Überprüfen Sie, ob das Problem bei einem bestimmten Access Point-Namen (APN) oder allen APNs vorliegt, da das Problem mit einem bestimmten APN in Zusammenhang stehen kann.

3. Überprüfen Sie, ob das Problem bei bestimmten Web-URLs oder mehreren URLs auftritt.

4. Überprüfen Sie, ob es sich bei der URL um eine Unternehmens-URL bzw. eine Kunden-App-URL oder eine reguläre Service-URL handelt, und prüfen Sie, ob das Problem bei einem bestimmten VPN liegt.

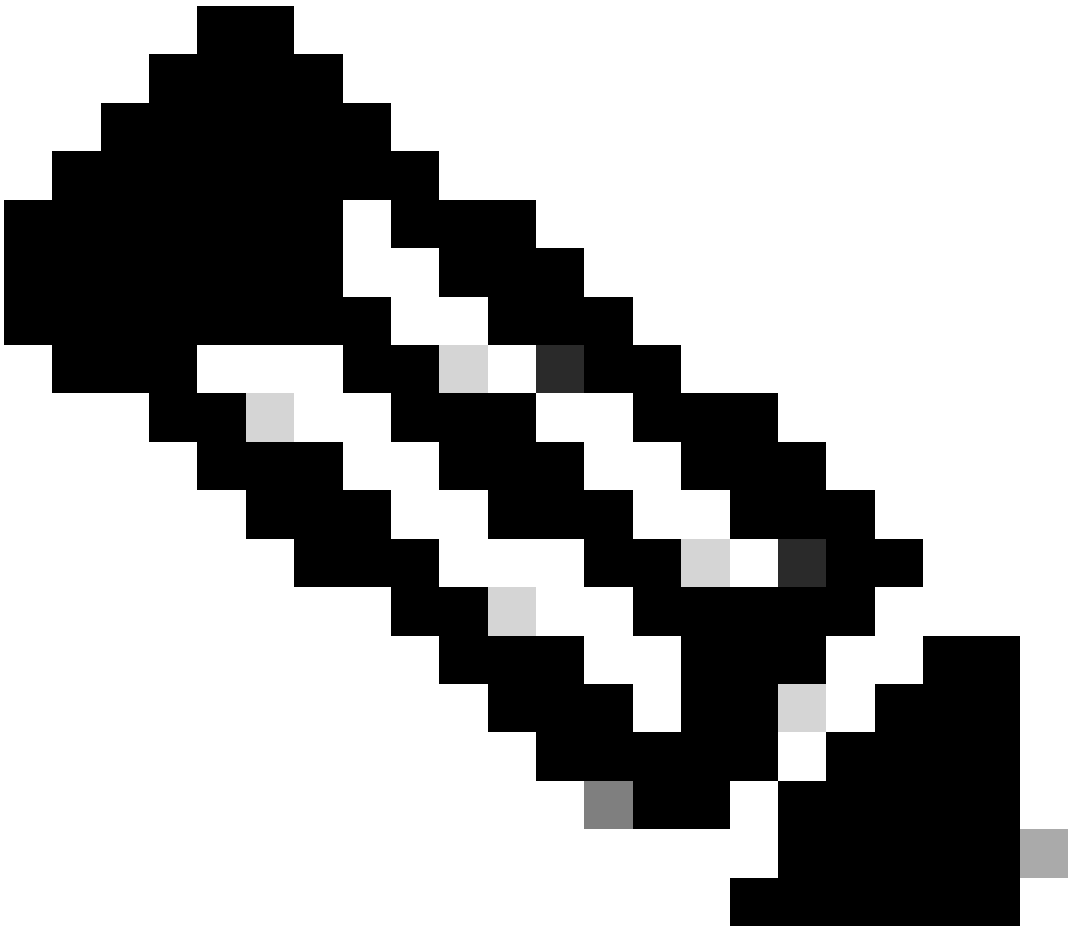
5. Überprüfen Sie, ob das Problem beim Zugriff auf die URL direkt vom Browser oder beim Zugriff auf die Web-App selbst auftritt.

6. Überprüfen Sie, ob das Problem nur gelegentlich auftritt, z. B. nach dem Neustart des Hörers

oder nach dem Aktualisieren der Web-URLs, oder ob es konsistent ist und auch nach dem Neustart des Hörers nicht funktioniert.

7. Überprüfen Sie die beobachtete Ablehnungsursache und für welche Ratinggruppe.

Protokollerfassung/-tests



> Hinweis: Bei diesem Problem müssen Sie eine Online-Fehlerbehebung in Echtzeit mit dem problematischen Benutzer IMSI durchführen, bei dem Sie die Protokolle/Ablaufverfolgungen entsprechend erfassen müssen.

Bevor Sie mit dem Testen und der Protokollsammlung fortfahren:

```
Flush the subscriber from the node and also clear browsing history/database from testing user handset s

clear subscriber imsi <IMSI number>  ----------------- to be executed in the node to clear the subscri
```

1. Beginnen Sie mit dem Test mit einem PDP-Typ wie IPv4, bei dem Sie das Problem sehen.
2. Aktivieren Sie diese Debug-Protokolle, und protokollieren Sie die putty-Sitzung. Stellen Sie sicher, dass die Sitzung nicht beendet werden darf (drücken Sie alle paar Minuten die Tabulatortaste, damit die Sitzung nicht beendet wird).

<#root>

On SPGW:

```
logging filter active facility sessmgr level debug
logging filter active facility acsmgr level debug
logging filter active facility npumgr-acl level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active   ---------------- to enable the logging

after 5 mins
no logging active ---------------- to disable the logging
```

On CP:

```
logging filter active facility sessmgr level debug
logging filter active facility sxdemux level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active ---------------- to enable the logging

after 5 mins
no logging active ---------------- to disable the logging
```

On UP:

```
logging filter active facility sessmgr level debug
logging filter active facility sxdemux level debug
logging filter active facility npumgr-acl level debug
logging filter active facility firewall level debug
logging filter active facility vpn level debug
logging filter active facility vpnmgr level debug
logging active ---------------- to enable the logging
no logging active ---------------- to disable the logging

Note :: These logging has to be enabled for short time depending on the CPU utilization because it
increase the utilization so while enabling logging need to keep a watch on CPU
```

3. Navigieren Sie in den Konfigurationsmodus, und aktivieren Sie dann die Protokollierungsüberwachung für den Abonnenten.

```
config
logging monitor msid <imsi>
end
```

4. Öffnen Sie ein anderes Terminal, protokollieren Sie die Kitt-Sitzung und starten Sie die Überwachung Abonnent mit Verbosity 5 und aktivieren Sie diese Optionen:

<#root>

SPGW:

```
Press + for times then it collects the logs verbosity 5 logs then select next options
+++++
X, A, Y, 19, 33, 34, 35, 22, 26, 75
Once option 75 is pressed then select 3,4,8 then press esc
```

CUPS::

on CP:

```
monitor subscriber imsi <IMSI> +++++        S, X,A,Y,56,26,33,34,19,37,35,88,89
```

on UP:

```
monitor subscriber imsi <IMSI> +++++        S,X,A,Y,56,26,33,34,19,37,35,88,89
```

5. Fügen Sie den Abonnenten und durchsuchen Sie die URL kontinuierlich für 3 bis 5 Minuten und während des Durchsuchens führen Sie diese Befehle mehrmals und protokollieren Sie die putty-Sitzung für die gleiche.

<#root>

ON SPGW/SAEGW:

```
show subscriber full imsi <>
show active-charging session full imsi <>
show subscriber pgw-only full imsi <>
show subscriber sgw-only full imsi <>
show subscribers data-rate summary imsi <>
show ims-authorization sessions full imsi <>
show subscribers debug-info msid <>
```

On CP node:

```
Show subscriber full imsi <imsi>
Show active-charging session full imsi <imsi>
show subscribers pgw-only full imsi <>
show subscribers sgw-only full imsi <>
show session subsystem facility sessmgr instance <> verbose
show logs
```

On UP node:

```
show sub user-plane-only full callid  <>
show sub user-plane-only callid <> urr full all
show sub user-plane-only callid <> far full all
show sub user-plane-only callid <> pdr full all
show subscribers user-plane-only callid <> far all
show subscribers user-plane-only callid <> far
show subs data-rate call <callid>
show subscribers user-plane-only flows
show user-plane-service statistics all
show user-plane-service statistic rulebase name <rulebase_name>
```

6. Nach 5 Minuten Durchsuchen, führen Sie die no logging active in der anderen Terminal, das in Schritt 3 geöffnet wird.

7. Deaktivieren Sie den Protokollmonitor für den Abonnenten.

Config
no logging monitor msid <imsi>
end

8. Stoppen Sie das Mon-U-Boot nicht und lassen Sie es laufen, bis Sie mit dem Sammeln der Nummernspuren fertig sind, aber behalten Sie die CPU im Auge.

9. Führen Sie diesen Befehl aus, um die Anrufer-ID des Teilnehmers abzurufen und die Putty-Sitzung auch dafür zu protokollieren.

Show subscriber full imsi <imsi>. -à get the call id
show logs callid <call_id>
show logs

Wenn die Anrufer-ID vorhanden ist, wird deutlich, dass die Protokolle der Teilnehmersitzungen gesammelt wurden. Wenn dies nicht der Fall ist, müssen Sie sie erneut ausführen.

Fehlerbehebung durchgeführt

- Senden Sie einen Ping an die IP-Adresse des Web-URL-Servers, und überprüfen Sie, ob Pakete verworfen werden.

ping <URL IP address> ---------- from Gi context
--- ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 12160ms. >.>>>> There are packet drops, now we need to check were it is dropping

2. Führen Sie eine traceroute aus dem GI-Kontext aus, und überprüfen Sie, ob Probleme mit der Erreichbarkeit vorliegen.

traceroute <peer ip address> src <local diameter origin host ip address>

Ex: traceroute 10.52.5.49 src 10.203.144.8

3. Überprüfen Sie die Teilnehmerstatistiken, um zu überprüfen, ob das Paket verloren geht.

<#root>

Show subscriber full imsi <imsi number>

```
input pkts: 455 output pkts: 474
input bytes: 75227 output bytes: 103267
input bytes dropped: 0 output bytes dropped: 0
input pkts dropped: 0 output pkts dropped: 0
input pkts dropped due to lorc : 0 output pkts dropped due to lorc : 0
input bytes dropped due to lorc : 0
in packet dropped suspended state: 0 out packet dropped suspended state: 0
in bytes dropped suspended state: 0 out bytes dropped suspended state: 0
in packet dropped sgw restoration state: 0 out packet dropped sgw restoration state: 0
in bytes dropped sgw restoration state: 0 out bytes dropped sgw restoration state: 0
pk rate from user(bps): 18547 pk rate to user(bps): 25330
ave rate from user(bps): 6182 ave rate to user(bps): 8443
sust rate from user(bps): 5687 sust rate to user(bps): 7768
pk rate from user(pps): 13 pk rate to user(pps): 14
ave rate from user(pps): 4 ave rate to user(pps): 4
sust rate from user(pps): 4 sust rate to user(pps): 4
link online/active percent: 92
ipv4 bad hdr: 0 ipv4 ttl exceeded: 0
ipv4 fragments sent: 0 ipv4 could not fragment: 0
ipv4 input acl drop: 0 ipv4 output acl drop: 0
ipv4 bad length trim: 0
ipv6 input acl drop: 0 ipv6 output acl drop: 0
ipv4 input css down drop: 0 ipv4 output css down drop: 0
ipv4 input css down drop: 0 ipv4 output css down drop: 0
ipv4 output xoff pkts drop: 0 ipv4 output xoff bytes drop: 0
ipv6 output xoff pkts drop: 0 ipv6 output xoff bytes drop: 0
ipv6 input ehrpd-access drop: 0 ipv6 output ehrpd-access drop: 0
input pkts dropped (0 mbr): 0 output pkts dropped (0 mbr): 0
ip source violations: 0 ipv4 output no-flow drop: 0
ipv6 egress filtered: 0
ipv4 proxy-dns redirect: 0 ipv4 proxy-dns pass-thru: 0
ipv4 proxy-dns drop: 0
ipv4 proxy-dns redirect tcp connection: 0
```

```
ipv6 bad hdr: 0 ipv6 bad length trim: 0
ip source violations no acct: 0
ip source violations ignored: 0
dormancy total: 0 handoff total: 0
ipv4 icmp packets dropped: 0
APN AMBR Input Pkts Drop: 0 APN AMBR Output Pkts Drop: 0
APN AMBR Input Bytes Drop: 0 APN AMBR Output Bytes Drop: 0
APN AMBR UE Overload Input Pkts Drop: 0 APN AMBR UE Overload Output Pkts Drop: 0
APN AMBR UE Overload Input Bytes Drop: 0 APN AMBR UE Overload Output Bytes Drop: 0
Access-flows:0
Num Auxiliary A10s:0
```

4. Überprüfen Sie die Anzeige der aktiven Ladeausgabe für die Auswirkungen auf den Teilnehmerdatenverkehr.

Show active-charging session full imsi <imsi num>

PP Dropped Packets: 0
CC Dropped Uplink Packets: 0 CC Dropped Uplink Bytes: 0
CC Dropped Downlink Packets: 0 CC Dropped Downlink Bytes: 0

5. Überprüfen Sie die Ausgabe des Befehls show active loading auf ECS/ACS-Paketverlust, und prüfen Sie, ob Pakete verworfen werden. Überprüfen Sie dann in der Konfiguration, welche Aktion konfiguriert wird.

<#root>

Show active-charging session full imsi <imsi num> or show sub user-plane-only full callid <>

```
 Ruledef Name Pkts-Down Bytes-Down Pkts-Up Bytes-Up Hits Match-Bypassed
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
dns_free_covid 4 428 4 340 8 0
icmpv6 0 0 5 1423 5 0
ip-pkts 479 103670 432 74488 764 429
```

6. Überprüfen Sie, ob die DNS-Auflösung erfolgreich ist oder nicht. Wenn sie erfolgreich ist, liegt kein Problem mit DNS vor.

```
10.60.150.135    GTP <DNS>    Standard query response 0x3a4c AAAA tracking.india.miui.com CNAME tracking-india-miui-com-1-77
42.105.241.29    GTP <DNS>    Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29    GTP <DNS>    Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29    GTP <DNS>    Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29    DNS          Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29    DNS          Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29    DNS          Standard query 0x3984 AAAA www.shcilestamp.com
42.105.241.29    GTP <DNS>    Standard query 0x63bb A www.shcilestamp.com
42.105.241.29    GTP <DNS>    Standard query 0x63bb A www.shcilestamp.com
42.105.241.29    GTP <DNS>    Standard query 0x63bb A www.shcilestamp.com
42.105.241.29    DNS          Standard query 0x63bb A www.shcilestamp.com
42.105.241.29    DNS          Standard query 0x63bb A www.shcilestamp.com
42.105.241.29    DNS          Standard query 0x63bb A www.shcilestamp.com
10.60.150.135    DNS          Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135    DNS          Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135    DNS          Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135    GTP <DNS>    Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135    GTP <DNS>    Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135    GTP <DNS>    Standard query response 0x63bb A www.shcilestamp.com A 121.241.45.21
10.60.150.135    DNS          Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
10.60.150.135    DNS          Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
10.60.150.135    DNS          Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
10.60.150.135    GTP <DNS>    Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
10.60.150.135    GTP <DNS>    Standard query response 0x3984 AAAA www.shcilestamp.com AAAA 64:ff9b::79f1:2d15
```

7. Überprüfen Sie, ob die TCP-Verbindung zwischen der Benutzerausrüstung (UE) und dem Server erfolgreich hergestellt wurde.

8. Wenn in einem dieser Schritte keine Verluste festgestellt werden, liegt kein Problem im Knoten vor.

Paketverlust

1. Überprüfen Sie die Abonnentenveröffentlichungsstatistiken, um festzustellen, ob es zu Paketverlusten kommt, die den hier gezeigten ähneln.

Total Dropped Packets : 132329995
Total Dropped Packet Bytes: 14250717212

Total PP Dropped Packets : 0
Total PP Dropped Packet Bytes: 0

R7Gx Rule-Matching Failure Stats:
Total Dropped Packets : 871921
Total Dropped Packet Bytes : 86859232

P2P random drop stats:
Total Dropped Packets : 0
Total Dropped Packet Bytes : 0

2. Überprüfen Sie den Prozentsatz der Fehler, die in der Ausgabe von Anzeigeabonnenten festgestellt wurden. Wenn das Paket weniger als 1 % verwirft, ist dies höchstwahrscheinlich ein Zufall und hat keine Auswirkungen.

input pkts: 455 output pkts: 474
input bytes: 75227 output bytes: 103267
input bytes dropped: 0 output bytes dropped: 0
input pkts dropped: 0 output pkts dropped: 0

3. Wenn Sie feststellen, dass Pakete in der RX-Bewertungsgruppe und in ITC-Paketen verworfen werden, ist dies höchstwahrscheinlich auf ein Bandbreitenproblem zurückzuführen, und das Abonnentenpaket ist abgelaufen.

ITC Packets Drop: 47235019

4. Auf der Stufe "Enhanced Charging Service (ECS)" (Erweiterte Gebührenerhebung) müssen Sie die ECS-Konfiguration der Definition von Regel-/Gebührenaktionen/Regelbasis überprüfen/überprüfen und feststellen, ob ein Sperrfaktor vorliegt. Auf ECS-Ebene gibt es verschiedene Arten von Tropfen, und je nach Art des Tropfens müssen Sie mit dem nächsten Aktionsplan fortfahren.

5. MTU-Größe für die Paketgröße, die weitergeleitet und nicht verarbeitet wird.

6. Zwischengeschaltete Pfadprobleme, bei denen das Paket verworfen wird, können anhand von TCP-Dump-/Traces auf Benutzerebene identifiziert werden.

Der Aktionsplan für die Rückforderung ist bei dieser Art von Problem nicht identisch, da er je nach Muster der Frage variiert.

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.