

Risoluzione dei problemi relativi agli errori dei percorsi EGTP

Sommario

[Introduzione](#)

[Panoramica](#)

[Possibili cause degli errori dei percorsi EGTP](#)

[Registri necessari](#)

[Comandi per la risoluzione dei problemi](#)

[Scenario/Motivi in breve](#)

[Problema di raggiungibilità - Problemi di connettività di rete](#)

[Riavvia modifiche valori contatore](#)

[Richiesta traffico in entrata elevato - Congestione rete](#)

[Soluzione](#)

[Soluzione alternativa](#)

[Modifiche alla configurazione](#)

[Registri di debug](#)

Introduzione

In questo documento viene descritto come risolvere i problemi relativi agli errori dei percorsi EGTP.

Panoramica

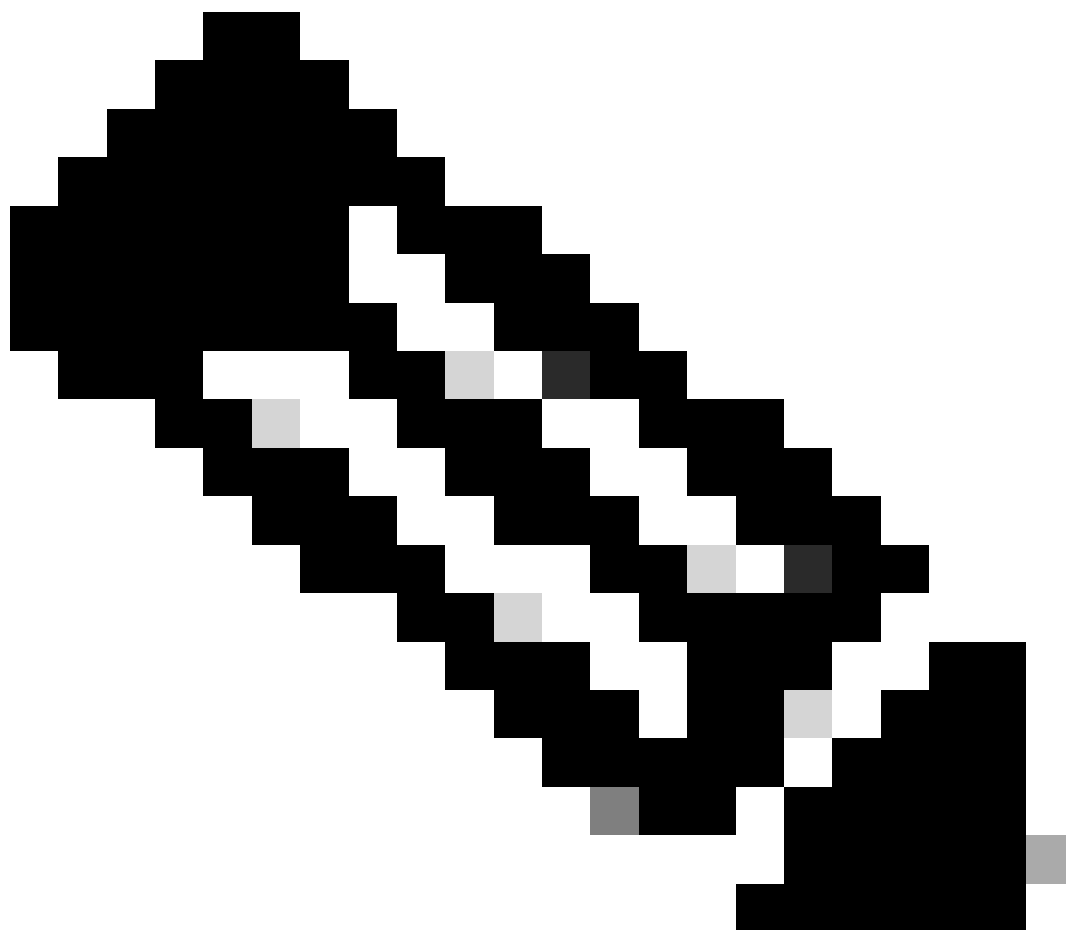
Gli errori di percorso EGTP (Evolved GPRS Tunneling Protocol) fanno riferimento a problemi con il percorso di comunicazione tra i nodi GTP di una rete mobile. Il GTP è un protocollo utilizzato per il trasporto di dati utente e di messaggi di segnalazione tra diversi elementi della rete.

Possibili cause degli errori dei percorsi EGTP

1. Problema di raggiungibilità - Problemi di connettività di rete
2. Riavviare le modifiche dei valori dei contatori
3. Richiesta di traffico in ingresso elevato - Congestione della rete
4. Problema di configurazione in termini di DSCP/QOS e così via
5. Nessun abbonato/sessione sul collegamento EGTPC

Registri necessari

1. SSD/syslog circa l'ora problematica che copre l'intervallo temporale almeno due ore prima dell'inizio del problema fino all'ora corrente.
 2. Conferma della raggiungibilità con i log, ossia ping e traceroute per il percorso per cui si sono verificati errori di percorso.
 3. Controllo della configurazione tra nodi problematici e non problematici.
 4. È necessario verificare se si è verificato un aumento improvviso del traffico o un aumento del rifiuto sulla stessa strada.
 5. Bulkstats durante orari problematici che coprono l'arco temporale almeno 2-3 giorni prima del rilascio.
-



Nota: a seconda del tipo di problema, è possibile che siano necessari i registri menzionati in precedenza. Non tutti i registri sono sempre necessari.

Comandi per la risoluzione dei problemi

<#root>

show egtpc peers interface

show egtpc peers path-failure-history

show egtpc statistics path-failure-reasons

show egtp-service all

show egtpc sessions

show egtpc statistics

egtpc test echo gtp-version 2 src-address <source node IP address> peer-address <remote node IP address>

For more details related to above command refer doc as mentioned below

<https://www.cisco.com/c/en/us/support/docs/wireless-mobility/gateway-gprs-support-node-ggsn/119246-tech.html>

Trap SNMP:

Sun Feb 05 03:00:20 2023 Internal trap notification 1112 (EGTPCPathFail) context s11mme, service s11-mme

Tue Jul 09 18:41:36 2019 Internal trap notification 1112 (EGTPCPathFail) context pgw, service s5-s8-sgw

Scenario/Motivi in breve

Problema di raggiungibilità - Problemi di connettività di rete

I problemi di raggiungibilità si verificano quando un problema nel percorso di routing può riguardare l'estremità del router o il firewall tra SGSN/MME e SPGW/GSN.

ping <destination IP>

tracert <destination IP> src <source IP>



Nota: entrambi i comandi per verificare la raggiungibilità devono essere controllati dal contenuto su cui è in esecuzione il servizio EGTP.

Riavvia modifiche valori contatore

Il percorso EGTP gestisce i contatori di riavvio a entrambe le estremità del percorso tra SGSN/MME e GSN/SPGW.



Per informazioni dettagliate su questo tipo di problema, fare riferimento al collegamento

<https://www.cisco.com/c/en/us/support/docs/wireless/asr-5000-series/200026-ASR-5000-Series-Troubleshooting-GTPC-and.html>.

Richiesta traffico in entrata elevato - Congestione rete

Quando si verificano improvvise transazioni ad alto traffico, c'è la possibilità che i pacchetti EGTP Tx e Rx scendano. Controlli di base per confermare lo scenario:

1. È necessario verificare se esiste un utilizzo elevato della CPU per egtpinmgr.

```
Mar 25 14:30:48 10.224.240.132 evlogd: [local-60sec48.142] [resmgr 14907 debug] [6/0/10088 <rmngr:60> _  
Mar 25 14:31:05 10.224.240.132 evlogd: [local-60sec5.707] [resmgr 14907 debug] [6/0/10088 <rmngr:60> _r
```

2. Verificare se la richiesta/risposta echo ha esito negativo (comando condiviso in precedenza).

3. Può verificare se ci sono perdite di pacchetti dalla scheda demux.

Tutto il traffico in entrata EGTP deve passare attraverso lo stesso egtpmgr. Se si osservano errori di percorso in un nodo, è probabile che il volume del traffico in entrata aumenti. Inoltre, è possibile riscontrare un calo del traffico a livello di processo egtpmgr. Anche il processo che si trova nello stesso percorso deve passare attraverso la stessa coda egtpmgr e ottenere l'impatto.

Di seguito viene riportata la procedura per controllare la perdita di pacchetti che deve essere eseguita con più iterazioni

<#root>

```
debug shell card <> cpu 0
```

```
cat /proc/net/boxer
```

```
***** card1-cpu0 /proc/net/boxer *****
```

```
Wednesday March 25 17:34:54 AST 2020
```

```
what                total_used next      refills      hungry  exhausted  system_rate_kbps      system_cr
```

```
bdp_rld             4167990936249KB  094  51064441      292          1  3557021/65000000  7825602KB/793
```

```
what                bhn local          remote          ver            rx      rx_drop          tx
```

total cpu 34	*	*	*	*	3274522	59	60
total cpu 35	*	*	*	*	6330639	46	121
total cpu 46	*	*	*	*	5076520	27	15524
total cpu 47	*	*	*	*	4163101019	83922	133540922

4. È necessario acquisire l'output del profiler CPU egtpinmgr se viene visualizzato un valore elevato di CPU per egtpinmgr.

Se tutte le condizioni di cui sopra sono valide, è possibile verificare la soluzione possibile indicata.

Soluzione

1. Aumentare il timeout dell'eco EGTP - Se 5 secondi non aiutano, è possibile provare 15 o 25. Per sintonizzarlo, è possibile discuterne con il team AS.

2. Diminuire il timeout di salvataggio dei peer - Minore è il valore di timeout, minore è il numero di peer inattivi, quindi è possibile modificare il valore di tempo con questo comando:

```
gtpc peer-salvation min-peers 2000 timeout 24
```

3. protezione da sovraccarico: l'ottimizzazione della protezione da sovraccarico può essere eseguita in base alla tendenza del traffico, perché senza conoscere la frequenza esatta del traffico in entrata prima che egpinmgr affronti il problema, è difficile regolare questo. Inoltre, una regolazione errata può causare ulteriore traffico di segnalazione a causa di cadute invisibili all'utente.

Quindi, per ottimizzare la protezione dall'overload, è possibile raccogliere alcune gocce di pacchetto dalla scheda demux per egtpinmgr e output del profiler della CPU come accennato in precedenza.

4. Nessun sottoscrittore/sessione sul collegamento EGTPC - quando non ci sono sessioni in un tunnel specifico, la funzionalità echo GTP viene interrotta. Se non è presente alcun sottoscrittore connesso, l'eco GTPC non deve essere inviata.

Di seguito sono riportati gli errori che si verificano quando la funzionalità echo viene arrestata:

```
2019-Jul-26+08:41:51.261 [egtpmgr 143047 debug] [1/0/4626 <egtpinmgr:2> egtpmgr_pm.c:798] [context: EPC
```

Soluzione alternativa

È possibile provare a riavviare l'attività egtpinmgr per eseguire il ripristino. Tuttavia, il riavvio di egtpinmgr può avere un impatto a breve termine, non percepibile per l'utente finale, mentre i flussi NPU vengono reinstallati nella nuova attività.

Il completamento dell'operazione deve richiedere meno di 1 secondo.

1. Disabilitare il rilevamento errori percorso:

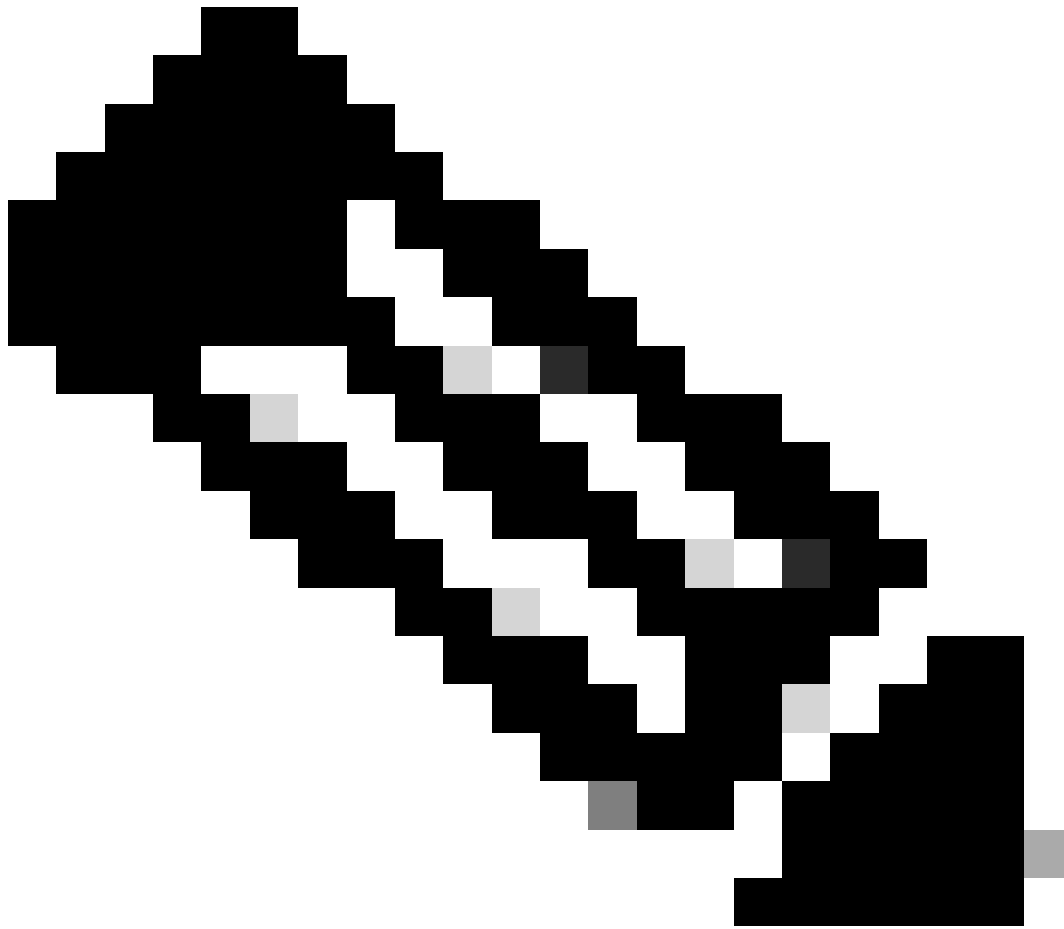
```
egtp-service S5-PGW
    no gtpc path-failure detection-policy
```

2. Termina attività egtpinmgr:

```
task kill facility egtpinmgr all
```

3. Abilitare il rilevamento degli errori di percorso:

```
egtp-service S5-PGW
    gtpc path-failure detection-policy
```



Nota: questa soluzione deve essere implementata solo in MW, in quanto può causare un certo impatto.

Modifiche alla configurazione

È possibile controllare la configurazione in termini di DSCP/QOS/EGTP IP path/service mapping.



Nota: queste sono le cause principali che contribuiscono agli errori dei percorsi EGTP, ma nel caso in cui nessuno degli scenari viene trovato, è possibile raccogliere alcune tracce e i log di debug ulteriormente.

Registri di debug

(Se richiesto)

```
logging filter active facility egtpc level<critical/error/debug>  
logging filter active facility egtpmgr level<critical/error/debug>  
logging filter active facility egtpinmgr level<critical/error/debug>
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).