Risoluzione dei problemi relativi alle trap AAAAccSrvUnreachable e AAAAuthSrvUnreachable

Sommario

Introduzione

In questo articolo viene descritto come risolvere i problemi relativi alle trap SNMP AAAAccSrvUnreachable e AAAAuthSrvUnreachable, attivate a causa di problemi di raggiungibilità con un server RADIUS (Remote Authentication Dial-In User Service) utilizzato per autenticare i sottoscrittori (o gli operatori che accedono al nodo, ma non è questo il problema trattato in questa sezione). Esistono due approcci per determinare quando attivare una di queste trap. In questo articolo vengono illustrate le condizioni che attivano queste trap e gli approcci per la risoluzione dei problemi e la raccolta dei dati che è possibile adottare per determinare la causa principale e risolverla. Vengono inoltre illustrate alcune possibili misure correttive da prendere in considerazione.

Notare che il RISULTATO di irraggiungibilità sarà errori di chiamata o errori di contabilità, come se le risposte radius sono rifiuti invece di accettazioni. Anche se la percentuale di successo/fallimento (autenticazione) viene misurata indipendentemente dal timeout/raggiungibilità (esistono trap e allarmi per questo) e può certamente essere analizzata a pieno titolo, il focus di questo articolo sarà sul problema della raggiungibilità e non sul problema del rifiuto.

L'output di esempio del laboratorio e i biglietti effettivi vengono utilizzati in tutto per aiutare a portare a casa le discussioni. In questo articolo, gli indirizzi IP pubblici sembrano essere indirizzi **falsi**.

Trigger Trap

Esistono due modelli/algoritmi/approcci diversi tra cui scegliere per determinare lo stato di un server radius e quando provare un server diverso in caso di errori:

Errori consecutivi in un approccio al processo di amgr

L'approccio originale e quello utilizzato più spesso dagli operatori prevede di tenere traccia del numero di errori che si sono verificati in una fila per un particolare processo di gestione. Un processo aamgr è responsabile dell'elaborazione e dello scambio di tutti i messaggi radius con un server radius e molti processi aamgr saranno presenti in uno chassis, ciascuno associato ai processi sessmgr (che sono i processi principali responsabili del controllo delle chiamate). (Visualizzare tutti i processi di amgr con il comando "show task resources") Un particolare processo di amgr elaborerà quindi messaggi radius per molte chiamate, non solo una singola chiamata, e questo algoritmo implica il rilevamento di quante volte in una riga un particolare processo di amgr non è riuscito a ottenere una risposta alla stessa richiesta che ha dovuto rinviare - un "Timeout di richiesta di accesso" come riportato in "show radius counters".

Il rispettivo contatore "Access-Request Current Consecutive Failures in a mgr", anche da "show radius counters", viene incrementato quando ciò si verifica e il comando "show radius accounting (o authentication) servers detail" indica i timestamp della modifica dello stato del raggio da Attivo a Non risponde (ma non vengono generate trap o registri SNMP per un solo errore). Di seguito è riportato un esempio di accounting RADIUS:

```
[source]PDSN> show radius accounting servers detail
Friday November 28 23:23:34 UTC 2008

+-----Type:       (A) - Authentication   (a) - Accounting
|                 (C) - Charging         (c) - Charging Accounting
|                 (M) - Mediation       (m) - Mediation Accounting
|
|+----Preference: (P) - Primary         (S) - Secondary
||
||+---State:     (A) - Active          (N) - Not Responding
|||               (D) - Down             (W) - Waiting Accounting-On
|||               (I) - Initializing     (w) - Waiting Accounting-Off
|||               (a) - Active Pending   (U) - Unknown
|||
|||+--Admin       (E) - Enabled         (D) - Disabled
|||| Status:
||||
||||+-Admin
||||| status     (O) - Overridden       (.) - Not Overridden
||||| Overridden:
|||||
vvvvv IP             PORT GROUP
------ ------------- ----- ----------------------
PNE. 198.51.100.1    1813 default

Event History:
2008-Nov-28+23:18:36       Active
2008-Nov-28+23:18:57       Not Responding
2008-Nov-28+23:19:12       Active
2008-Nov-28+23:19:30       Not Responding
2008-Nov-28+23:19:36       Active
```

```
2008-Nov-28+23:20:57       Not Responding
2008-Nov-28+23:21:12       Active
2008-Nov-28+23:22:31       Not Responding
2008-Nov-28+23:22:36       Active
2008-Nov-28+23:23:30       Not Responding
```

Se il contatore raggiunge il valore configurato (Predefinito = 4) senza essere reimpostato, in base alla configurazione: si noti che le parentesi [ ] vengono utilizzate per indicare il qualificatore facoltativo e in questi casi acquisisce la risoluzione dei problemi di accounting (l'autenticazione è l'impostazione predefinita se accounting non è specificato)

radius [accounting] rileva errori consecutivi del server inattivo 4

Il server viene quindi contrassegnato come "Inattivo" per il periodo (minuti) configurato:

deadtime [accounting] radius 10

Vengono attivati anche una trap SNMP e i log, ad esempio, rispettivamente per l'autenticazione e/o l'accounting:

```
Fri Jan 30 06:17:19 2009 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 172.28.221.178
Fri Jan 30 06:22:19 2009 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
172.28.221.178
```

```
Fri Nov 28 21:59:12 2008 Internal trap notification 42 (AAAAccSvrUnreachable) server 6 ip
address 172.28.221.178
Fri Nov 28 22:28:29 2008 Internal trap notification 43 (AAAAccSvrReachable) server 6 ip address
172.28.221.178
```

```
2008-Nov-28+21:59:12.899 [radius-acct 24006 warning] [8/0/518 <aaamgr:231> aaamgr_config.c:1060]
[context: source, contextID: 2] [software internal security config user critical-info] Server
172.28.221.178:1813 unreachable

2008-Nov-28+22:28:29.280 [radius-acct 24007 info] [8/0/518 <aaamgr:231> aaamgr_config.c:1068]
[context: source, contextID: 2] [software internal security config user critical-info] Server
172.28.221.178:1813 reachable
```

I trap indicano che il server non è raggiungibile. Prendere nota di qualsiasi modello. Ad esempio, si verifica in un server o in un altro o in tutti i server e con quale frequenza si verifica il rimbalzo?

Notate anche che tutto ciò che serve per far scattare questa trappola è che un amgr fallisca, e quindi la parte difficile di questa trappola è che non indica l'entità del problema. Potrebbe essere molto esteso o molto marginale - che è l'operatore da determinare, e gli approcci per capire che fuori sono discussi in questo articolo.

show snmp trap statistics riporta il numero di volte in cui è stato attivato dall'avvio, anche se le trap meno recenti sono state eliminate da molto tempo. Nell'esempio viene mostrato un problema di contabilità irraggiungibile:

```
[source]PDSN> show snmp trap statistics | grep -i aaa
Wednesday September 10 08:38:19 UTC 2014

Trap Name                          #Gen #Disc  Disable Last Generated
```

```
--------------------------------- ----- -----  ------- --------------------
AAAAccSvrUnreachable                833     0       0  2014:09:10:08:36:54
AAAAccSvrReachable                  839     0       0  2014:09:10:08:37:00
```

Si noti che l'amgr riportato nell'esempio precedente è #231. Si tratta dell'amgr di gestione di ASR 5000 che risiede nella scheda di gestione del sistema (SMC, System Management Card). Ciò che è ingannevole in questo output è che quando un singolo amgr o amgr riscontra problemi di raggiungibilità, il numero di istanza riportato nei log è l'istanza di management amgr e non le istanze particolari che riscontrano il problema. Ciò è dovuto al fatto che se molte istanze stanno sperimentando problemi di raggiungibilità, allora la registrazione si riempirebbe rapidamente se fossero tutte segnalate come tali, e quindi il progetto è stato quello di riferire genericamente sull'istanza di gestione, che se non si sapesse questo, sarebbe certamente ingannevole. Nella sezione Risoluzione dei problemi verranno forniti ulteriori dettagli su come determinare quali sono i responsabili degli errori. A partire da alcune versioni di StarOS 17 e v18+, questo comportamento è stato modificato in modo che il numero dell'istanza di gestione corrispondente con problemi di connettività (come segnalato nelle trap SNMP) venga segnalato nei log con l'ID specifico (Cisco CDETS CSCum84773), sebbene venga segnalata solo la prima occorrenza (tra più farm) di questo evento.

Il management manager è il numero massimo di istanza sessmgr + 1, quindi in un ASR 5500 è 385 per DPC (Data Processing Card) o 1153 (per DPC 2).

A questo scopo, il management manager è responsabile della gestione degli accessi di operatore/amministratore e delle richieste di modifica delle autorizzazioni avviate dagli stessi server RADIUS.

Continuando, il comando "show radius accounting (or authentication) servers detail" indica i timestamp delle modifiche dello stato su Down che corrispondono ai trap/log (promemoria: La mancata risposta definita in precedenza è un singolo amministratore che ottiene un timeout, mentre Down è un singolo amministratore che ottiene un numero di timeout consecutivi sufficiente per ciascuna configurazione per attivare Down)

```
vvvvv IP              PORT GROUP
----- --------------- ----- ----------------------
aSDE. 172.28.221.178 1813 default

Event History:
2008-Nov-28+21:59:12       Down
2008-Nov-28+22:28:29       Active
2008-Nov-28+22:28:57       Not Responding
2008-Nov-28+22:32:12       Down
2008-Nov-28+23:01:57       Active
2008-Nov-28+23:02:12       Not Responding
2008-Nov-28+23:05:12       Down
2008-Nov-28+23:19:29       Active
2008-Nov-28+23:19:57       Not Responding
2008-Nov-28+23:22:12       Down
```

Se è configurato un solo server, non viene contrassegnato come non attivo, in quanto ciò sarebbe fondamentale per la corretta configurazione della chiamata.

Èopportuno ricordare che esiste un altro parametro che può essere configurato sulla riga di configurazione detect-dead-server denominata "response-timeout". Se specificato, un server viene contrassegnato come inattivo solo quando vengono soddisfatte entrambe le condizioni di errore consecutivo e timeout di risposta. Il timeout di risposta specifica un periodo di tempo in cui non

viene ricevuta alcuna risposta a TUTTE le richieste inviate a un server specifico. Si noti che questo timer verrà continuamente reimpostato durante la ricezione delle risposte. Questa condizione si verifica quando un server o la connessione di rete è completamente inattiva, mentre è parzialmente compromessa o danneggiata.

In questo caso, uno scenario in cui un'interruzione del traffico causa l'attivazione di errori consecutivi, ma non si desidera contrassegnare immediatamente un server come non attivo. Al contrario, il server viene contrassegnato solo dopo un determinato periodo di tempo in cui non viene ricevuta alcuna risposta, il che rappresenta effettivamente una reale irraggiungibilità del server.

Questo metodo appena descritto per il controllo delle modifiche della macchina a stati del raggio dipende dall'analisi di tutti i processi di amgr e dalla ricerca di un processo che attivi la condizione di tentativi non riusciti. Questo metodo è soggetto ad una certa casualità degli errori e quindi potrebbe non essere l'algoritmo ideale per rilevare gli errori. Ma è particolarmente bravo a trovare uno o più amgr che sono rotti mentre tutti gli altri stanno funzionando bene.

Approccio keepalive

Un altro metodo per rilevare la raggiungibilità del server radius consiste nell'utilizzare messaggi di test keepalive fittizi. Questo comporta l'invio costante di messaggi radio contraffatti invece di monitorare il traffico in diretta. Un altro vantaggio di questo metodo è che è sempre attivo, rispetto ai guasti consecutivi in un approccio amgr, dove ci potrebbero essere periodi in cui non viene inviato traffico radius, e quindi non c'è modo di sapere se un problema esiste durante quei tempi, con conseguente rilevamento ritardato quando i tentativi cominciano a verificarsi. Inoltre, quando un server è contrassegnato, questi pacchetti keepalive continuano ad essere inviati in modo che il server possa essere contrassegnato al più presto. Lo svantaggio di questo approccio consiste nel fatto che non rileva i problemi legati a specifiche istanze di amgr che potrebbero riscontrare problemi, in quanto utilizza l'istanza di management amgr per i messaggi di test.

Di seguito sono riportati i vari parametri di configurazione relativi a questo approccio:

```
radius (accounting) detect-dead-server keepalive
radius (accounting) keepalive interval 30
radius (accounting) keepalive retries 3
radius (accounting) keepalive timeout 3
radius (accounting) keepalive consecutive-response 1
radius (accounting) keepalive username Test-Username
radius keepalive encrypted password 2ec59b3188f07d9b49f5ea4cc44d9586
radius (accounting) keepalive calling-station-id 000000000000000
radius keepalive valid-response access-accept
```

Il comando "radius (accounting) detect-dead-server keepalive" attiva l'approccio keep-alive anziché i guasti consecutivi in un approccio amgr. Nell'esempio sopra riportato, il sistema invia un messaggio di prova con nome utente Test-Username e password Test-Username ogni 30 secondi, quindi esegue un nuovo tentativo ogni 3 secondi se non viene ricevuta alcuna risposta, quindi esegue un nuovo tentativo fino a 3 volte, dopodiché il server viene contrassegnato come non attivo. Una volta ottenuta la prima risposta, la contrassegna di nuovo.

Di seguito è riportato un esempio di richiesta/risposta di autenticazione per le impostazioni precedenti:

```
<<<<OUTBOUND 17:50:12:657 Eventid:23901(6)

RADIUS AUTHENTICATION Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1812 (142) PDU-
dict=starent-vsa1
Code: 1 (Access-Request)
Id: 16
Length: 142
Authenticator: 51 6D B2 7D 6A C6 9A 96 0C AB 44 19 66 2C 12 0A
     User-Name = Test-Username
     User-Password = B7 23 1F D1 86 46 4D 7F 8F E0 2A EF 17 A1 F3 BF
     Calling-Station-Id = 000000000000000
     Service-Type = Framed
     Framed-Protocol = PPP
     NAS-IP-Address = 192.168.50.151
     Acct-Session-Id = 00000000
     NAS-Port-Type = HRPD
     3GPP2-MIP-HA-Address = 255.255.255.255
     3GPP2-Correlation-Id = 00000000
     NAS-Port = 4294967295
     Called-Station-ID = 00

INBOUND>>>>> 17:50:12:676 Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 192.168.50.200:1812 to 192.168.50.151:32783 (34) PDU-
dict=starent-vsa1
Code: 2 (Access-Accept)
Id: 16
Length: 34
Authenticator: 21 99 F4 4C F8 5D F8 28 99 C6 B8 D9 F9 9F 42 70
     User-Password = testpassword
```

Le stesse trap SNMP vengono utilizzate per indicare gli stati del raggio irraggiungibile/inferiore e raggiungibile/superiore come con gli errori consecutivi in un approccio di gestione:

```
Fri Feb 27 17:54:55 2009 Internal trap notification 39 (AAAAuthSvrUnreachable) server 1 ip
address 192.168.50.200
Fri Feb 27 17:57:04 2009 Internal trap notification 40 (AAAAuthSvrReachable) server 1 ip address
192.168.50.200
```

La sezione "show radius counters all" consente di tenere traccia delle richieste keepalive per l'autenticazione e l'accounting. Di seguito sono riportati i contatori di autenticazione:

```
   Server-specific Keepalive Auth Counters
   ---------------------------------------
     Keepalive Access-Request Sent:                          33
     Keepalive Access-Request Retried:                       3
     Keepalive Access-Request Timeouts:                      4
     Keepalive Access-Accept Received:                       29
     Keepalive Access-Reject Received:                       0
     Keepalive Access-Response Bad Authenticator Received:   0
     Keepalive Access-Response Malformed Received:           0
     Keepalive Access-Response Malformed Attribute Received: 0
     Keepalive Access-Response Unknown Type Received:        0
     Keepalive Access-Response Dropped:                      0
```

Comandi/approcci per la risoluzione dei problemi

Ora che è stato spiegato il trigger per AAA Unreachable traps, il passo successivo è capire i vari

comandi di risoluzione dei problemi da usare per determinare l'impatto e cercare di capire la causa principale. L'irraggiungibilità è un termine molto ampio. Non spiega dove si trovi l'irraggiungibilità: nella rete, sul server o sull'ASR. Ad esempio, è noto se le richieste siano state inviate? Il server ha ricevuto le richieste? Ha risposto alle richieste? Le risposte sono tornate all'ASR e, in caso affermativo, sono state elaborate o eliminate nel percorso interno (ad esempio i flussi). In questa sezione viene illustrato come rispondere a queste domande.

Nozioni fondamentali sulla configurazione di Radius

Innanzitutto, è necessario conoscere alcune nozioni di base relative alla configurazione RADIUS. La maggior parte della configurazione di RADIUS si trova in un gruppo denominato in modo specifico e tutti i contesti dispongono di un gruppo di default che può essere configurato nel modo seguente. Molte volte le configurazioni hanno un solo gruppo, quello predefinito.

```
[local]CSE2# config
[local]CSE2(config)# context aaa_ctx
[aaa_ctx]ASR5000(config-ctx)# aaa group default
[aaa_ctx]ASR5000(config-aaa-group)#
```

Se vengono utilizzati gruppi aaa specifici denominati, questi vengono indicati dall'istruzione seguente configurata in un profilo del sottoscrittore o in un nome del punto di applicazione (APN) (a seconda della tecnologia di controllo delle chiamate), ad esempio:

```
subscriber name <subscriber name>
  aaa group <group name>
```

Nota: Il sistema controlla innanzitutto il gruppo aaa specifico assegnato al sottoscrittore, quindi controlla l'impostazione predefinita del gruppo aaa per rilevare eventuali altri elementi configurabili non definiti nel gruppo specifico.

Di seguito sono riportati comandi utili che riepilogano tutti i valori assegnati a tutti gli elementi configurabili nelle varie configurazioni del gruppo aaa. In questo modo è possibile visualizzare rapidamente tutti gli elementi configurabili, inclusi i valori predefiniti, senza dover esaminare manualmente la configurazione. In questo modo è possibile evitare errori quando si assumono determinate impostazioni. Questi comandi restituiscono informazioni in tutti i contesti:

```
show aaa group all
show aaa group name <group name>
```

La configurazione più importante è ovviamente costituita dai server di accesso e accounting radius. Di seguito è riportato un esempio:

```
radius server 209.165.201.1 key testtesttesttest port 1645 priority 1 max-rate 5
radius server 209.165.201.2 key testtesttesttest port 1645 priority 2 max-rate 5
radius accounting server 209.165.201.1 key testtesttesttest port 1646 priority 1
radius accounting server 209.165.201.2 key testtesttesttest port 1646 priority 2
```

Si noti la funzionalità di frequenza massima che limita il numero di richieste inviate al server per amgr al secondo

Èinoltre necessario definire l'indirizzo IP del server NAS, ovvero l'indirizzo IP di un'interfaccia nel contesto da cui vengono inviate le richieste radius e ricevute le risposte. Se non definita, le

richieste non vengono inviate e le tracce del sottoscrittore di monitoraggio potrebbero non inviare un errore ovvio (nessuna richiesta radius inviata e nessuna indicazione del motivo).

attributo radius indirizzo-ip-nas 10.211.41.129

Poiché sia l'autenticazione che l'accounting vengono spesso gestiti dallo stesso server, per distinguere il traffico di autenticazione dal traffico di accounting sul server RADIUS viene utilizzato un numero di porta diverso. Per il lato ASR5K, il numero della porta di origine UDP NON è specificato e viene scelto dallo chassis su base amgr (ulteriori informazioni in proposito sono disponibili più avanti).
Normalmente sono specificati più server di accesso e di accounting a scopo di ridondanza. È possibile configurare un round robin o un ordine di priorità:

algoritmo radius [accounting] {first-server | round robin}

L'opzione primo server consente di inviare tutte le richieste al server con la priorità con il numero più basso. Il server con la priorità successiva verrà tentato solo quando si verificano errori o, peggio, quando un server è contrassegnato come non attivo. Ulteriori informazioni su questo argomento sono disponibili di seguito.

Quando viene inviata una richiesta radius (accounting o accesso), è prevista una risposta. Se non si riceve una risposta entro il periodo di timeout (secondi):

timeout radius [accounting] 3

La richiesta viene inviata fino al numero di volte specificato:

radius [accounting] max-tentativi 5

Ciò significa che una richiesta può essere inviata un totale di max-retries + 1 volta fino a quando non cede sul server radius specifico che si sta tentando. A questo punto, tenta la stessa sequenza con il server radius successivo in ordine. Se per ognuno dei server è stato eseguito il tentativo max-retries + 1 volta senza risposta, la chiamata viene rifiutata, supponendo che fino a quel momento non esistano altri motivi di errore.

Come nota secondaria, esistono configurabili che consentono agli utenti di accedere anche se l'autenticazione e l'accounting hanno esito negativo a causa di timeout di tutti i server, anche se un'implementazione commerciale probabilmente non implementerebbe quanto segue:

radius consenti autenticazione [accounting] - inattivo

Inoltre, esistono configurabili che possono limitare il numero totale assoluto di trasmissioni di una determinata richiesta in tutti i server configurati e che sono disabilitati per impostazione predefinita:

radius [accounting] max trasmissioni 256

Ad esempio, se è impostato su = 1, anche se è presente un server secondario, non verrà mai eseguito un tentativo perché verrà eseguito un solo tentativo di configurazione per un sottoscrittore specifico.

mostra tutte le risorse delle attività

Ogni processo di gestione è associato a un processo sessmgr associato (responsabile della gestione complessiva delle chiamate) e "funziona" su una scheda Packet Services Card (PSC) o Data Processing Card (DPC) diversa, ma utilizzando lo stesso ID istanza. Anche in questo esempio si nota l'output della speciale istanza di gestione 231 in esecuzione su System Management Card (SMC) per ASR 5000 (o Management Input Output Card per ASR 5500 (MIO)) che NON elabora le richieste dei sottoscrittori ma viene utilizzata per i comandi di test radius (vedere la sezione successiva per maggiori dettagli su questo) E per l'elaborazione dell'accesso da parte dell'operatore CLI.

In questo frammento, aamgr 107 che si trova in PSC 13 è responsabile della gestione di tutta l'elaborazione RADIUS per la sessione accoppiata sessmgr 107 che si trova in PSC 1. I problemi di raggiungibilità per aamgr 107 influiscono sulle chiamate a sessmgr 107.

```
                  task   cputime       memory     files     sessions
cpu facility     inst used allc   used alloc used allc used allc S status
----------------------- --------- ------------ --------- ------------ -----
1/0 sessmgr       107 1.6% 100% 119.6M 155.0M   26 500   83 6600 I   good
13/1 aaamgr       107 0.3% 94% 30.8M 77.0M   18 500   --   -- -   good
8/0 aaamgr        231 0.1% 30% 11.6M 25.0M   19 500   --   -- -   good
```

Nell'esempio seguente, si noti che i problemi con aamgr 92 influiscono sul sessmgr accoppiato in modo molto semplice rispetto ad altri sessmgr per quanto riguarda il numero di sessioni:

```
                   task   cputime        memory     files      sessions
cpu facility      inst used allc   used  alloc used allc  used  allc S status
----------------------- --------- ------------ --------- ------------ ------
12/0 sessmgr         92 1.2% 100% 451.5M  1220M   43  500   643 21120 I   good
16/0 aaamgr          92 0.0%  95% 119.0M 315.0M   20  500    --    -- -   good
12/0 sessmgr         95 6.9% 100% 477.3M  1220M   41  500  2626 21120 I   good
12/0 sessmgr        105 7.7% 100% 600.5M  1220M   45  500  2626 21120 I   good
12/0 sessmgr        126 3.4% 100% 483.0M  1220M   44  500  2625 21120 I   good
12/0 sessmgr        131 8.1% 100% 491.7M  1220M   45  500  2627 21120 I   good
```

show radius counters { {all} | server <IP server>} [istanza <amgr #>] | riepilogo}

Il comando numero uno a cui prestare attenzione è la varietà di "show radius counters"

Questo comando restituisce molti contatori utili per la risoluzione dei problemi relativi al raggio. Il comando "show radius counters all" è molto utile per tenere traccia delle operazioni riuscite e non riuscite sul server. È importante comprendere il significato dei vari contatori che compongono questo comando, in quanto potrebbe non essere ovvio. Il comando è sensibile al contesto, pertanto deve essere eseguito nello stesso contesto in cui sono definiti i gruppi aaa.

Nota importante: In un periodo di tempo non monitorato, è difficile trarre conclusioni dai valori dei contatori o dalle relazioni tra contatori. Per trarre conclusioni accurate, l'approccio migliore consiste nel reimpostare i contatori e monitorarli in un periodo di tempo in cui si verifica il problema da risolvere.

Nell'output seguente, la nota "Access-Request Sent" = 1, mentre "Access-Request Retries" = 3. Pertanto, qualsiasi nuova richiesta a un determinato server radius viene conteggiata una sola volta e tutti i tentativi vengono conteggiati separatamente. In questo caso, si tratta di un totale di 3 + 1 = 4 richieste di accesso inviate. Notare il contatore "Access-Request Timeouts" = 1. Un singolo timeout si verifica solo quando TUTTI i tentativi hanno esito negativo, quindi in questo caso 3 tentativi senza un risultato di risposta in 1 Timeout (non 4). Questo avviene su tutti i server configurati fino al completamento o fino a quando tutti i tentativi non sono riusciti. Prestare quindi

attenzione ai contatori che vengono rilevati separatamente per ogni server. Di seguito è riportato un esempio:

```
radius max-retries 3
radius server 192.168.50.200 encrypted key 01abd002c82b4a2c port 1812 priority 1
radius server 192.168.50.250 encrypted key 01abd002c82b4a2c port 1812 priority 2

[destination]CSE2# show radius counters all

   Server-specific Authentication Counters
   ---------------------------------------
   Authentication server address 192.168.50.200, port 1812:
     Access-Request Sent:                                  1
     Access-Request with DMU Attributes Sent:              0
     Access-Request Pending:                               0
     Access-Request Retried:                               3
     Access-Request with DMU Attributes Retried:           0
     Access-Challenge Received:                            0
     Access-Accept Received:                               0
     Access-Reject Received:                               0
     Access-Reject Received with DMU Attributes:           0
     Access-Request Timeouts:                              1
     Access-Request Current Consecutive Failures in a mgr:     1
     Access-Request Response Bad Authenticator Received:       0
     Access-Request Response Malformed Received:               0
     Access-Request Response Malformed Attribute Received:     0
     Access-Request Response Unknown Type Received:            0
     Access-Request Response Dropped:                          0
     Access-Request Response Last Round Trip Time:             0.0 ms
     Access-Request Response Average Round Trip Time:          0.0 ms
Current Access-Request Queued: 0 ... Authentication server address 192.168.50.250, port 1812:
Access-Request Sent: 1 Access-Request with DMU Attributes Sent: 0 Access-Request Pending: 0
Access-Request Retried: 3 Access-Request with DMU Attributes Retried: 0 Access-Challenge
Received: 0 Access-Accept Received: 0 Access-Reject Received: 0 Access-Reject Received with DMU
Attributes: 0 Access-Request Timeouts: 1 Access-Request Current Consecutive Failures in a mgr: 1
Access-Request Response Bad Authenticator Received: 0 Access-Request Response Malformed
Received: 0 Access-Request Response Malformed Attribute Received: 0 Access-Request Response
Unknown Type Received: 0 Access-Request Response Dropped: 0 Access-Request Response Last Round
Trip Time: 0.0 ms Access-Request Response Average Round Trip Time: 0.0 ms
Current Access-Request Queued: 0
```

Si noti inoltre che i timeout NON vengono conteggiati come errori, con il risultato che il numero di accessi accettati e di accessi rifiutati non corrisponderà alla somma di richieste di accesso inviate se si verificano timeout.

L'analisi di questi contatori potrebbe non essere del tutto semplice. Ad esempio, per il protocollo MIP (Mobile IP), poiché le autenticazioni non riescono, non viene inviata alcuna risposta di registrazione MIP (RRP) e il dispositivo mobile può continuare ad avviare nuove richieste di registrazione MIP (RQ) perché non ha ricevuto un RRP MIP. Ogni nuova RQ MIP determina l'invio da parte del PDSN di una nuova richiesta di autenticazione che può disporre di una propria serie di tentativi. Questa condizione può essere rilevata nel campo Id nella parte superiore di una traccia del pacchetto ed è univoca per ogni set di tentativi. Di conseguenza, i contatori per Inviato, Riprovato e Timeout possono essere molto più alti del previsto per il numero di chiamate ricevute. È disponibile un'opzione che può essere abilitata per ridurre al minimo questi tentativi aggiuntivi e può essere impostata nel servizio Agente estero (FA) (ma non nel servizio Agente locale (HA)): "authentication mn-aaa <6 options here> optimize-retries"

Altri contatori utili:

"Access-Request Response Dropped" - si verifica se la chiamata non riesce a configurare durante

l'attesa di risposte alle richieste di autenticazione.

"Access-Request Response Last Round Trip Time": indica qualsiasi ritardo tra gli endpoint, anche se ovviamente non indica dove potrebbe essere il ritardo.

L'argomento "Access-Request Current Consecutive Failures in a mgr" si riferisce a quanto descritto nella prima sezione sui trigger per le trap AAA irraggiungibili. Rappresenta gli amministratori con il numero più alto di timeout consecutivi.

"Current Access/Accounting-Request Queued" indica le richieste a cui non viene data risposta e che rimangono nella coda (l'accounting consente la creazione della coda per un periodo di tempo indefinito, a differenza dell'autenticazione)

Lo scenario più comune rilevato quando viene segnalato che il server AAA è irraggiungibile è che si verificano anche timeout di accesso e/o mancate risposte, mentre le risposte di accesso non vengono aggiornate con le richieste.

Se è disponibile l'accesso alla modalità di supporto tecnico privilegiata, è possibile eseguire ulteriori indagini a livello di istanza dell'amministratore per determinare se una o più schede specifiche sono la causa dell'aumento del numero complessivo di schede "errate". Ad esempio, cercate le immagini che si trovano su uno specifico PSC/DPC con conteggi alti o magari un singolo amgr o amigr casuali con problemi - cercate modelli. Se tutti o la maggior parte dei campioni presentano problemi, è più probabile che la causa principale sia esterna allo chassis OPPURE che si manifesti su larga scala sullo chassis. In tal caso si dovrebbero effettuare controlli sanitari generali.

Di seguito è riportato un output di esempio che mostra un problema con un responsabile specifico per l'accounting. (Il problema si è rivelato essere un bug in un firewall tra l'ASR5K e il server RADIUS che bloccava il traffico proveniente da una porta specifica dell'istanza di gestione (114)). In un periodo di tre settimane, sono state ricevute solo 48 risposte, ma si sono verificati oltre 100.000 timeout (senza includere ritrasmissioni).

```
[source]PDSN> show radius counters server 209.165.201.1 instance  114 | grep -E "Accounting-
Request Sent|Accounting-Response Received|Accounting-Request Timeouts"
Wednesday October 01 18:12:24 UTC 2014
     Accounting-Request Sent:                                  14306189
     Accounting-Response Received:                             14299843
     Accounting-Request Timeouts:                              6342

[source]PDSN> show radius counters server 209.165.201.1 instance 114 | grep -E "Accounting
server address|Accounting-Request Sent|Accounting-Response Received|Accounting-Request Timeouts"
Wednesday October 22 20:26:35 UTC 2014
   Accounting server address 209.165.201.1, port 1646:
     Accounting-Request Sent:                                  15105872
     Accounting-Response Received:                             14299891
     Accounting-Request Timeouts:                              158989

[source]PDSN> show radius counters server 209.165.201.1 instance 114 | grep Accounting
Wednesday October 22 20:33:09 UTC 2014
   Per-Context RADIUS Accounting Counters
   Accounting Response
   Server-specific Accounting Counters
   Accounting server address 209.165.201.1, port 1646:
     Accounting-Request Sent:                                  15106321
     Accounting-Start Sent:                                    7950140
     Accounting-Stop Sent:                                     7156129
     Accounting-Interim Sent:                                  52
     Accounting-On Sent:                                       0
     Accounting-Off Sent:                                      0
     Accounting-Request Pending:                               3
```

```
    Accounting-Request Retried:                                283713
    Accounting-Start Retried:                                  279341
    Accounting-Stop Retried:                                   4372
    Accounting-Interim Retried:                                0
    Accounting-On Retried:                                     0
    Accounting-Off Retried:                                    0
    Accounting-Response Received:                              14299891
    Accounting-Request Timeouts:                               159000
    Accounting-Request Current Consecutive Failures in a mgr: 11
    Accounting-Response Bad Response Received:                 0
    Accounting-Response Malformed Received:                    0
    Accounting-Response Unknown Type Received:                 0
    Accounting-Response Dropped:                               21
    Accounting-Response Last Round Trip Time:                  52.5 ms
    Accounting-Response Average Round Trip Time:               49.0 ms
    Accounting Total G1 (Acct-Output-Octets):                  4870358614798
    Accounting Total G2 (Acct-Input-Octets):                   714140547011
    Current Accounting-Request Queued:                         17821
```

In conclusione, determinare quali contatori sono in aumento, per quali server e a quale velocità.

mostra funzionalità sottosistema di sessione {aamgr | sessmgr} {tutto | instance <istanza #>}

Anche se l'esame di tutti gli output superflui di questo comando esula dalle finalità di questo articolo, vale la pena esaminare un paio di esempi. Come per qualsiasi altra risoluzione dei problemi, il confronto dell'output tra le istanze di amgr ritenute buone e cattive spesso rivela differenze evidenti nei valori riportati. Ciò può riflettersi sul numero totale di richieste, sulla percentuale di errori/operazioni riuscite, su autorizzazioni annullate e così via. Ricordarsi di cancellare il sottosistema della sessione (un'istanza non può essere cancellata, tutte devono essere cancellate) in modo da eliminare qualsiasi cronologia che potrebbe potenzialmente fornire un'immagine offuscata dello stato corrente.

Continuando con lo stesso problema menzionato in precedenza per quanto riguarda un singolo amgr che non riesce a eseguire l'accounting, di seguito viene riportato l'output da un nodo diverso con lo stesso problema ad eccezione di un'istanza di sessmr diversa 36. Prendere nota di tutti i campi interessanti per l'amgr che non riesce e di come questi valori aumentano nel tempo con le due acquisizioni del comando. Nel frattempo, l'output dell'istanza 37 viene mostrato come esempio di un amgr funzionante.

```
[source]PDSN> show session subsystem  facility aaamgr instance 36
Wednesday September 10 08:51:18 UTC 2014

AAAMgr:  Instance 36
39947440 Total aaa requests              17985 Current aaa requests
24614090 Total aaa auth requests             0 Current aaa auth requests
       0 Total aaa auth probes               0 Current aaa auth probes
       0 Total aaa aggregation requests
       0 Current aaa aggregation requests
       0 Total aaa auth keepalive            0 Current aaa auth keepalive
15171628 Total aaa acct requests         17985 Current aaa acct requests
       0 Total aaa acct keepalive            0 Current aaa acct keepalive
20689536 Total aaa auth success        1322489 Total aaa auth failure
   86719 Total aaa auth purged            1016 Total aaa auth cancelled
       0 Total auth keepalive success        0 Total auth keepalive failure
       0 Total auth keepalive purged
       0 Total aaa aggregation success requests
       0 Total aaa aggregation failure requests
       0 Total aaa aggregation purged requests
   15237 Total aaa auth DMU challenged
   17985/70600 aaa request (used/max)
```

```
      14 Total diameter auth responses dropped
 6960270 Total Diameter auth requests        0 Current Diameter auth requests
   23995 Total Diameter auth requests retried
      52 Total Diameter auth requests dropped
 9306676 Total radius auth requests          0 Current radius auth requests
       0 Total radius auth requests retried
     988 Total radius auth responses dropped
      13 Total local auth requests           0 Current local auth requests
 8500275 Total pseudo auth requests          0 Current pseudo auth requests
    8578 Total null-username auth requests (rejected)
       0 Total aggregation responses dropped
15073834 Total aaa acct completed        79763 Total aaa acct purged     <== If issue started
recently, this may not have yet started incrementing
       0 Total acct keepalive success        0 Total acct keepalive timeout
       0 Total acct keepalive purged
       4 CLI Test aaa acct purged
       0 IP Interface down aaa acct purged
       0 No Radius Server found aaa acct purged
       0 No Response aaa acct purged
14441090 Total acct sess alloc
14422811 Total acct sess delete
   18279 Current acct sessions
       0 Auth No Wait Suppressed
       0 Aggr No Wait Suppressed
       0 Disc No Wait Suppressed
       0 Start No Wait Suppressed
       0 Interim No Wait Suppressed
       0 Stop No Wait Suppressed
       0 Acct OnOff Custom14
       0 Acct OnOff Custom67
       0 Acct OnOff
       0 Recovery Str Suppressed
       0 Recovery Stop Suppressed
       0 Med Chrg Gtpp Suppressed
       0 Med Chrg Radius Suppressed
       0 Radius Probe Trigger
       0 Recovery Stop Acct Session Suppressed
      46 Total aaa acct cancelled
       0 Total Diameter acct requests        0 Current Diameter acct requests
       0 Total Diameter acct requests retried
       0 Total diameter acct requests dropped
       0 Total diameter acct responses dropped
       0 Total diameter acct cancelled
       0 Total diameter acct purged
15171628 Total radius acct requests      17985 Current radius acct requests
      46 Total radius acct cancelled
   79763 Total radius acct purged
   11173 Total radius acct requests retried
      49 Total radius acct responses dropped
       0 Total radius sec acct requests      0 Current radius sec acct requests
       0 Total radius sec acct cancelled
       0 Total radius sec acct purged
       0 Total radius sec acct requests retried
       0 Total gtpp acct requests            0 Current gtpp acct requests
       0 Total gtpp acct cancelled           0 Total gtpp acct purged
       0 Total gtpp sec acct requests        0 Total gtpp sec acct purged
       0 Total null acct requests            0 Current null acct requests
16218236 Total aaa acct sessions         21473 Current aaa acct sessions
    8439 Total aaa acct archived             2 Current aaa acct archived
   21473 Current recovery archives        4724 Current valid recovery records
       1 Total aaa sockets opened            1 Current aaa sockets opened
       1 Total aaa requests pend socket opened
       0 Current aaa requests pend socket open
  133227 Total radius requests pend server max-outstanding
```

```
   17982 Current radius requests pend server max-outstanding
       0 Total radius auth req queued server max-rate
       0 Max radius auth req queued server max-rate
       0 Current radius auth req queued server max-rate
       0 Total radius acct req queued server max-rate
       0 Max radius acct req queued server max-rate
       0 Current radius acct req queued server max-rate
       0 Total radius charg auth req queued server max-rate
       0 Max radius charg auth req queued server max-rate
       0 Current radius charg auth req queued server max-rate
       0 Total radius charg acct req queued server max-rate
       0 Max radius charg acct req queued server max-rate
       0 Current radius charg acct req queued server max-rate
       0 Total aaa radius coa requests       0 Total aaa radius dm requests
       0 Total aaa radius coa acks           0 Total aaa radius dm acks
       0 Total aaa radius coa naks           0 Total aaa radius dm naks
       0 Total radius charg auth             0 Current radius charg auth
       0 Total radius charg auth success     0 Total radius charg auth failure
       0 Total radius charg auth purged      0 Total radius charg auth cancelled
       0 Total radius charg acct             0 Current radius charg acct
       0 Total radius charg acct success     0 Total radius charg acct purged
       0 Total radius charg acct cancelled
       0 Total gtpp charg                    0 Current gtpp charg
       0 Total gtpp charg success            0 Total gtpp charg failure
       0 Total gtpp charg cancelled          0 Total gtpp charg purged
       0 Total gtpp sec charg                0 Total gtpp sec charg purged
  161722 Total prepaid online requests       0 Current prepaid online requests
  141220 Total prepaid online success    20392 Current prepaid online failure
       0 Total prepaid online retried      102 Total prepaid online cancelled
       8 Current prepaid online purged
...

[source]PDSN> show session subsystem facility aaamgr instance 37
Wednesday September 10 08:51:28 UTC 2014

AAAMgr:  Instance 37
39571859 Total aaa requests                  0 Current aaa requests
24368622 Total aaa auth requests             0 Current aaa auth requests
       0 Total aaa auth probes               0 Current aaa auth probes
       0 Total aaa aggregation requests
       0 Current aaa aggregation requests
       0 Total aaa auth keepalive            0 Current aaa auth keepalive
15043217 Total aaa acct requests             0 Current aaa acct requests
       0 Total aaa acct keepalive            0 Current aaa acct keepalive
20482618 Total aaa auth success        1309507 Total aaa auth failure
   85331 Total aaa auth purged             968 Total aaa auth cancelled
       0 Total auth keepalive success        0 Total auth keepalive failure
       0 Total auth keepalive purged
       0 Total aaa aggregation success requests
       0 Total aaa aggregation failure requests
       0 Total aaa aggregation purged requests
   15167 Total aaa auth DMU challenged
       1/70600 aaa request (used/max)
      41 Total diameter auth responses dropped
 6883765 Total Diameter auth requests         0 Current Diameter auth requests
   23761 Total Diameter auth requests retried
      37 Total Diameter auth requests dropped
 9216203 Total radius auth requests           0 Current radius auth requests
       0 Total radius auth requests retried
     927 Total radius auth responses dropped
      15 Total local auth requests            0 Current local auth requests
 8420022 Total pseudo auth requests           0 Current pseudo auth requests
    8637 Total null-username auth requests (rejected)
       0 Total aggregation responses dropped
```

```
15043177 Total aaa acct completed            0 Total aaa acct purged
       0 Total acct keepalive success        0 Total acct keepalive timeout
       0 Total acct keepalive purged
       0 CLI Test aaa acct purged
       0 IP Interface down aaa acct purged
       0 No Radius Server found aaa acct purged
       0 No Response aaa acct purged
14358245 Total acct sess alloc
14356293 Total acct sess delete
    1952 Current acct sessions
       0 Auth No Wait Suppressed
       0 Aggr No Wait Suppressed
       0 Disc No Wait Suppressed
       0 Start No Wait Suppressed
       0 Interim No Wait Suppressed
       0 Stop No Wait Suppressed
       0 Acct OnOff Custom14
       0 Acct OnOff Custom67
       0 Acct OnOff
       0 Recovery Str Suppressed
       0 Recovery Stop Suppressed
       0 Med Chrg Gtpp Suppressed
       0 Med Chrg Radius Suppressed
       0 Radius Probe Trigger
       0 Recovery Stop Acct Session Suppressed
      40 Total aaa acct cancelled
       0 Total Diameter acct requests        0 Current Diameter acct requests
       0 Total Diameter acct requests retried
       0 Total diameter acct requests dropped
       0 Total diameter acct responses dropped
       0 Total diameter acct cancelled
       0 Total diameter acct purged
15043217 Total radius acct requests          0 Current radius acct requests
      40 Total radius acct cancelled
       0 Total radius acct purged
     476 Total radius acct requests retried
      37 Total radius acct responses dropped
       0 Total radius sec acct requests      0 Current radius sec acct requests
       0 Total radius sec acct cancelled
       0 Total radius sec acct purged
       0 Total radius sec acct requests retried
       0 Total gtpp acct requests            0 Current gtpp acct requests
       0 Total gtpp acct cancelled           0 Total gtpp acct purged
       0 Total gtpp sec acct requests        0 Total gtpp sec acct purged
       0 Total null acct requests            0 Current null acct requests
16057760 Total aaa acct sessions          4253 Current aaa acct sessions
      14 Total aaa acct archived             0 Current aaa acct archived
    4253 Current recovery archives        4249 Current valid recovery records
       1 Total aaa sockets opened            1 Current aaa sockets opened
       1 Total aaa requests pend socket opened
       0 Current aaa requests pend socket open
   29266 Total radius requests pend server max-outstanding
       0 Current radius requests pend server max-outstanding
       0 Total radius auth req queued server max-rate
       0 Max radius auth req queued server max-rate
       0 Current radius auth req queued server max-rate
       0 Total radius acct req queued server max-rate
       0 Max radius acct req queued server max-rate
       0 Current radius acct req queued server max-rate
       0 Total radius charg auth req queued server max-rate
       0 Max radius charg auth req queued server max-rate
       0 Current radius charg auth req queued server max-rate
       0 Total radius charg acct req queued server max-rate
       0 Max radius charg acct req queued server max-rate
```

```
       0 Current radius charg acct req queued server max-rate
       0 Total aaa radius coa requests       0 Total aaa radius dm requests
       0 Total aaa radius coa acks           0 Total aaa radius dm acks
       0 Total aaa radius coa naks           0 Total aaa radius dm naks
       0 Total radius charg auth             0 Current radius charg auth
       0 Total radius charg auth success     0 Total radius charg auth failure
       0 Total radius charg auth purged      0 Total radius charg auth cancelled
       0 Total radius charg acct             0 Current radius charg acct
       0 Total radius charg acct success     0 Total radius charg acct purged
       0 Total radius charg acct cancelled
       0 Total gtpp charg                    0 Current gtpp charg
       0 Total gtpp charg success            0 Total gtpp charg failure
       0 Total gtpp charg cancelled          0 Total gtpp charg purged
       0 Total gtpp sec charg                0 Total gtpp sec charg purged
  160020 Total prepaid online requests       0 Current prepaid online requests
  139352 Total prepaid online success    20551 Current prepaid online failure
...



[source]PDSN> show session subsystem facility aaamgr instance 36
Wednesday September 10 09:12:13 UTC 2014

AAAMgr:  Instance 36

39949892 Total aaa requests             17980 Current aaa requests
24615615 Total aaa auth requests            0 Current aaa auth requests
       0 Total aaa auth probes              0 Current aaa auth probes
       0 Total aaa aggregation requests
       0 Current aaa aggregation requests
       0 Total aaa auth keepalive           0 Current aaa auth keepalive
15172543 Total aaa acct requests        17980 Current aaa acct requests
       0 Total aaa acct keepalive           0 Current aaa acct keepalive
20690768 Total aaa auth success       1322655 Total aaa auth failure
   86728 Total aaa auth purged           1016 Total aaa auth cancelled
       0 Total auth keepalive success       0 Total auth keepalive failure
       0 Total auth keepalive purged
       0 Total aaa aggregation success requests
       0 Total aaa aggregation failure requests
       0 Total aaa aggregation purged requests
   15242 Total aaa auth DMU challenged
   17981/70600 aaa request (used/max)
      14 Total diameter auth responses dropped
 6960574 Total Diameter auth requests       0 Current Diameter auth requests
   23999 Total Diameter auth requests retried
      52 Total Diameter auth requests dropped
 9307349 Total radius auth requests         0 Current radius auth requests
       0 Total radius auth requests retried
     988 Total radius auth responses dropped
      13 Total local auth requests          0 Current local auth requests
 8500835 Total pseudo auth requests         0 Current pseudo auth requests
    8578 Total null-username auth requests (rejected)
       0 Total aggregation responses dropped
15074358 Total aaa acct completed       80159 Total aaa acct purged
       0 Total acct keepalive success       0 Total acct keepalive timeout
       0 Total acct keepalive purged
       4 CLI Test aaa acct purged
       0 IP Interface down aaa acct purged
       0 No Radius Server found aaa acct purged
       0 No Response aaa acct purged
14441768 Total acct sess alloc
14423455 Total acct sess delete
   18313 Current acct sessions
       0 Auth No Wait Suppressed
```

```
       0 Aggr No Wait Suppressed
       0 Disc No Wait Suppressed
       0 Start No Wait Suppressed
       0 Interim No Wait Suppressed
       0 Stop No Wait Suppressed
       0 Acct OnOff Custom14
       0 Acct OnOff Custom67
       0 Acct OnOff
       0 Recovery Str Suppressed
       0 Recovery Stop Suppressed
       0 Med Chrg Gtpp Suppressed
       0 Med Chrg Radius Suppressed
       0 Radius Probe Trigger
       0 Recovery Stop Acct Session Suppressed
      46 Total aaa acct cancelled
       0 Total Diameter acct requests        0 Current Diameter acct requests
       0 Total Diameter acct requests retried
       0 Total diameter acct requests dropped
       0 Total diameter acct responses dropped
       0 Total diameter acct cancelled
       0 Total diameter acct purged
15172543 Total radius acct requests      17980 Current radius acct requests
      46 Total radius acct cancelled
   80159 Total radius acct purged
   11317 Total radius acct requests retried
      49 Total radius acct responses dropped
       0 Total radius sec acct requests      0 Current radius sec acct requests
       0 Total radius sec acct cancelled
       0 Total radius sec acct purged
       0 Total radius sec acct requests retried
       0 Total gtpp acct requests            0 Current gtpp acct requests
       0 Total gtpp acct cancelled           0 Total gtpp acct purged
       0 Total gtpp sec acct requests        0 Total gtpp sec acct purged
       0 Total null acct requests            0 Current null acct requests
16219251 Total aaa acct sessions         21515 Current aaa acct sessions
    8496 Total aaa acct archived             0 Current aaa acct archived
   21515 Current recovery archives        4785 Current valid recovery records
       1 Total aaa sockets opened            1 Current aaa sockets opened
       1 Total aaa requests pend socket opened
       0 Current aaa requests pend socket open
  133639 Total radius requests pend server max-outstanding
   17977 Current radius requests pend server max-outstanding
...
```

Èinoltre consigliabile eseguire il comando show task resources per verificare l'eventuale presenza di un numero di sessioni non uniforme (colonna utilizzata) tra tutte le sessioni. Se vengono rilevate delle sessioni, controllare le coppie di sessioni con questo comando per verificare se sono presenti campi non in linea. Se il problema è dovuto a RADIUS, è possibile trovare qualcosa.

Nell'esempio di visualizzazione delle risorse dell'attività di una sezione precedente, il conteggio delle sessioni di sessmgr 92 è stato significativamente ridotto, in seguito all'associazione con aamgr 92. L'output del sottosistema di visualizzazione delle sessioni mostra un aumento significativo dei contatori totale max in attesa e aaa auth eliminato e dei contatori elevati Current max in attesa. È possibile utilizzare la funzione grep in tempo reale sullo chassis e/o Notepad++ o altro potente editor di ricerca per analizzare rapidamente i dati. Eseguire il comando più volte per verificare quali valori sono in aumento o rimanenti elevati:

```
[Ingress]PGW# show session subsystem facility aaamgr all
Tuesday January 10 04:42:29 UTC 2012
    4695 Total aaa auth purged
    4673 Total radius auth requests         16 Current radius auth requests
    4167 Total radius requests pend server max-outstanding
```

```
      76 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"
Tuesday January 10 04:51:00 UTC 2012
    4773 Total radius requests pend server max-outstanding
      67 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"
Tuesday January 10 04:56:10 UTC 2012
    5124 Total radius requests pend server max-outstanding
      81 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr instance 92
Tuesday January 10 04:57:03 UTC 2012
    5869 Total aaa auth purged
    5843 Total radius auth requests         12 Current radius auth requests
    5170 Total radius requests pend server max-outstanding
      71 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr instance 92
Tuesday January 10 05:10:05 UTC 2012
    6849 Total aaa auth purged
    6819 Total radius auth requests          6 Current radius auth requests
    5981 Total radius requests pend server max-outstanding
      68 Current radius requests pend server max-outstanding

[Ingress]PGW# show session subsystem facility aaamgr all | grep "max-outstanding"
Tuesday January 10 05:44:22 UTC 2012
      71 Total radius requests pend server max-outstanding
       0 Current radius requests pend server max-outstanding
      61 Total radius requests pend server max-outstanding
       0 Current radius requests pend server max-outstanding

    7364 Total radius requests pend server max-outstanding   <== instance #92
      68 Current radius requests pend server max-outstanding

      89 Total radius requests pend server max-outstanding
       0 Current radius requests pend server max-outstanding
      74 Total radius requests pend server max-outstanding
       0 Current radius requests pend server max-outstanding

[Ingress]PGW#radius test instance 92 auth server 65.175.1.10 port 1645 test test
Tuesday January 10 06:13:38 UTC 2012

Authentication from authentication server 65.175.1.10, port 1645
Communication Failure: No response received
```

ping

traceroute

Un ping ICMP esegue un test della connettività di base per verificare se il server AAA è raggiungibile o meno. Il ping può richiedere la parola chiave src a seconda della rete e deve essere eseguito dal contesto AAA per avere un valore. Se il ping al server ha esito negativo, provare a eseguire il ping degli elementi intermedi, incluso l'indirizzo dell'hop successivo, nel contesto, per verificare che esista una voce ARP per l'indirizzo dell'hop successivo se il ping ha esito negativo. Il comando traceroute può essere utile anche per risolvere i problemi di routing.

```
[source]CSE2# ping 192.168.50.200
PING 192.168.50.200 (192.168.50.200) 56(84) bytes of data.
```

```
64 bytes from 192.168.50.200: icmp_seq=1 ttl=64 time=0.411 ms
64 bytes from 192.168.50.200: icmp_seq=2 ttl=64 time=0.350 ms
64 bytes from 192.168.50.200: icmp_seq=3 ttl=64 time=0.353 ms
64 bytes from 192.168.50.200: icmp_seq=4 ttl=64 time=0.321 ms
64 bytes from 192.168.50.200: icmp_seq=5 ttl=64 time=0.354 ms

--- 192.168.50.200 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.321/0.357/0.411/0.037 ms
```

istanza test radius x auth {radius group <gruppo> | tutto | server <IP> porta <porta>} <nomeutente> <password>

istanza test radius x accounting {radius group <nome gruppo> | tutto | server <IP> porta <porta>}

Grazie all'accesso ai comandi di test del supporto tecnico, è possibile verificare ulteriormente se un determinato manager è in grado di raggiungere un qualsiasi server RADIUS. Per un test di connettività RADIUS di base, indipendente da qualsiasi istanza di gestione specifica, utilizzare la versione generica di questo comando che non specifica alcun numero di istanza specifico ma utilizza l'istanza di gestione per impostazione predefinita. Se ciò non riesce, allora può puntare a un problema più ampio indipendente da istanze specifiche.

Questo comando invia una richiesta di autenticazione di base o richieste di **avvio** e **arresto dell'**accounting e attende una risposta. Per l'autenticazione, utilizzare nome utente e password, nel qual caso è prevista una risposta di rifiuto per confermare che RADIUS funziona come previsto, oppure è possibile utilizzare un nome utente e una password noti, nel qual caso deve essere ricevuta una risposta di accettazione

Di seguito è riportato un esempio di output del protocollo del monitor e dell'esecuzione della versione di autenticazione del comando su uno chassis lab:

```
[source]CSE2# radius test authentication server 192.168.50.200 port 1812 test test

Authentication from authentication server 192.168.50.200, port 1812
Authentication Success: Access-Accept received
Round-trip time for response was 12.3 ms

<<<<OUTBOUND 14:53:49:202 Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1812 (58) PDU-
dict=starent-vsa1
Code: 1 (Access-Request)
Id: 5
Length: 58
Authenticator: 56 97 57 9C 51 EF A4 08 20 E1 14 89 40 DE 0B 62
     User-Name = test
     User-Password = 49 B0 92 4D DC 64 49 BA B0 0E 18 36 3F B6 1B 37
     NAS-IP-Address = 192.168.50.151
     NAS-Identifier = source

INBOUND>>>>> 14:53:49:214 Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 192.168.50.200:1812 to 192.168.50.151:32783 (34) PDU-
dict=starent-vsa1
Code: 2 (Access-Accept)
Id: 5
Length: 34
Authenticator: D7 94 1F 18 CA FE B4 27 17 75 5C 99 9F A8 61 78
     User-Password = testpassword
```

Di seguito è riportato un esempio da uno chassis live:

```
<<<<OUTBOUND 12:45:49:869 Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 10.209.28.200:33156 to 209.165.201.1:1645 (72) PDU-
dict=custom150
Code: 1 (Access-Request)
Id: 6
Length: 72
Authenticator: 67 C2 2B 3E 29 5E A5 28 2D FB 85 CA 0E 9F A4 17
     User-Name = test
     User-Password = 8D 95 3B 31 99 E2 6A 24 1F 81 13 00 3C 73 BC 53
     NAS-IP-Address = 10.209.28.200
     NAS-Identifier = source
     3GPP2-Session-Term-Capability = Both_Dynamic_Auth_And_Reg_Revocation_in_MIP

INBOUND>>>>> 12:45:49:968 Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 209.165.201.1:1645 to 10.209.28.200:33156 (50) PDU-
dict=custom150
Code: 3 (Access-Reject)
Id: 6
Length: 50
Authenticator: 99 2E EC DA ED AD 18 A9 86 D4 93 52 57 4C 2F 84
     Reply-Message = Invalid username or password
```

Di seguito è riportato un output di esempio dell'esecuzione della versione di accounting del comando. Non è necessaria una password.

```
[source]CSE2# radius test accounting server 192.168.50.200 port 1813 test
RADIUS Start to accounting server 192.168.50.200, port 1813
Accounting Success: response received
Round-trip time for response was 7.9 ms

RADIUS Stop to accounting server 192.168.50.200, port 1813
Accounting Success: response received
Round-trip time for response was 15.4 ms


<<<<OUTBOUND 15:23:14:974 Eventid:24901(6)
RADIUS ACCOUNTING Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1813 (62) PDU-
dict=starent-vsa1
Code: 4 (Accounting-Request)
Id: 8
Length: 62
Authenticator: DA 0F A8 11 7B FE 4B 1A 56 EB 0D 49 8C 17 BD F6
     User-Name = test
     NAS-IP-Address = 192.168.50.151
     Acct-Status-Type = Start
     Acct-Session-Id = 00000000
     NAS-Identifier = source
     Acct-Session-Time = 0

INBOUND>>>>> 15:23:14:981 Eventid:24900(6) RADIUS ACCOUNTING Rx PDU, from 192.168.50.200:1813 to
192.168.50.151:32783 (20) PDU-dict=starent-vsa1 Code: 5 (Accounting-Response) Id: 8 Length: 20
Authenticator: 05 E2 82 29 45 FC BC D6 6C 48 63 AA 14 9D 47 5B <<<<OUTBOUND 15:23:14:983
Eventid:24901(6) RADIUS ACCOUNTING Tx PDU, from 192.168.50.151:32783 to 192.168.50.200:1813 (62)
PDU-dict=starent-vsa1 Code: 4 (Accounting-Request) Id: 9 Length: 62 Authenticator: 29 DB F1 0B
EC CE 68 DB C7 4D 60 E4 7F A2 D0 3A User-Name = test NAS-IP-Address = 192.168.50.151 Acct-
Status-Type = Stop Acct-Session-Id = 00000000 NAS-Identifier = source Acct-Session-Time = 0
INBOUND>>>>> 15:23:14:998 Eventid:24900(6) RADIUS ACCOUNTING Rx PDU, from 192.168.50.200:1813 to
192.168.50.151:32783 (20) PDU-dict=starent-vsa1 Code: 5 (Accounting-Response) Id: 9 Length: 20
Authenticator: D8 3D EF 67 EA 75 E0 31 A5 31 7F E8 7E 69 73 DC
```

L'output seguente è relativo alla stessa istanza di gestione 36 indicata in precedenza in cui la

connettività a un server di accounting RADIUS specifico viene interrotta:

```
[source]PDSN> radius test instance 36 accounting all test
Wednesday September 10 10:06:29 UTC 2014

RADIUS Start to accounting server 209.165.201.1, port 1646
Accounting Success: response received
Round-trip time for response was 51.2 ms

RADIUS Stop to accounting server 209.165.201.1, port 1646
Accounting Success: response received
Round-trip time for response was 46.2 ms

RADIUS Start to accounting server 209.165.201.2, port 1646
Accounting Success: response received
Round-trip time for response was 89.3 ms

RADIUS Stop to accounting server 209.165.201.2, port 1646
Accounting Success: response received
Round-trip time for response was 87.8 ms


RADIUS Start to accounting server 209.165.201.3, port 1646
Communication Failure: no response received

RADIUS Stop to accounting server 209.165.201.3, port 1646
Communication Failure: no response received

RADIUS Start to accounting server 209.165.201.4, port 1646
Accounting Success: response received
Round-trip time for response was 81.6 ms

RADIUS Stop to accounting server 209.165.201.4, port 1646
Accounting Success: response received
Round-trip time for response was 77.1 ms

RADIUS Start to accounting server 209.165.201.5, port 1646
Accounting Success: response received
Round-trip time for response was 46.7 ms

RADIUS Stop to accounting server 209.165.201.5, port 1646
Accounting Success: response received
Round-trip time for response was 46.7 ms

RADIUS Start to accounting server 209.165.201.6, port 1646
Accounting Success: response received
Round-trip time for response was 79.6 ms

RADIUS Stop to accounting server 209.165.201.6, port 1646
Accounting Success: response received
Round-trip time for response was 10113.0 ms
```

show radius info [radius group <nome gruppo>] istanza { X | tutti}

Questo comando segnala l'ID di flusso NPU (Network Processor Unit) e la porta UDP utilizzati dall'indirizzo IP del server NAS configurato per la connessione ai server RADIUS. Questa condizione viene segnalata nella sezione predefinita del gruppo aaa dell'output. Certamente il numero di porta può essere utile se è necessario far corrispondere i pacchetti RADIUS in un'acquisizione di pacchetti con un numero di istanza di gestione specifico. (Notare che i flussi NPU sono complicati e non è una questione discussa in questo articolo, bensì un'entità che un

tecnico di supporto potrebbe approfondire.) Consente inoltre di tenere traccia delle richieste in sospeso inviate al server. Nello stesso problema di esempio utilizzato in questo articolo, solo una coppia di porte IP/UDP di un server RADIUS **<=>** NAS ha avuto esito negativo, come evidenziato.

```
[source]PDSN> show radius info radius group all instance 114
Wednesday October 01 11:39:15 UTC 2014

Context source:
-----------------------------------------

  AAAMGR instance 114:  cb-list-en: 1 AAA Group: aaa-roamingprovider.com
  -----------------------------------------
    Authentication servers:
    -----------------------------------------
    Primary  authentication server address 209.165.201.1, port 1645
      state Active
      priority 1
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0
    Secondary  authentication server address 209.165.201.2, port 1645
      state Active
      priority 2
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0

    Accounting servers:
    -----------------------------------------
    Primary  accounting server address 209.165.201.1, port 1646
      state Active
      priority 1
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0
    Secondary  accounting server address 209.165.201.2, port 1646
      state Active
      priority 2
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0

  AAAMGR instance 114:  cb-list-en: 1 AAA Group: aaa-maingroup.com
  -----------------------------------------
    Authentication servers:
    -----------------------------------------
    Primary  authentication server address 209.165.201.3, port 1645
      state Active
      priority 1
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0
    Secondary  authentication server address 209.165.201.4, port 1645
      state Active
      priority 2
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0

    Accounting servers:
    -----------------------------------------
    Primary  accounting server address 209.165.201.3, port 1646
      state Down
```

```
      priority 1
      requests outstanding 3
      max requests outstanding 3
      consecutive failures 7
      dead time expires in 146 seconds
    Secondary  accounting server address 209.165.201.4, port 1646
      state Active
      priority 2
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0

  AAAMGR instance 114:  cb-list-en: 1 AAA Group: default
  ------------------------------------------
  socket number: 388550648
  socket state: ready
  local ip address: 10.210.21.234
  local udp port: 25808
  flow id: 20425379
  use med interface: yes
  VRF context ID: 2

    Authentication servers:
    ------------------------------------------
    Primary  authentication server address 209.165.201.5, port 1645
      state Active
      priority 1
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0
    Secondary  authentication server address 209.165.201.6, port 1645
      state Not Responding
      priority 2
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0

    Accounting servers:
    ------------------------------------------
    Primary  accounting server address 209.165.201.5, port 1646
      state Active
      priority 1
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0
    Secondary  accounting server address 209.165.201.6, port 1646
      state Active
      priority 2
      requests outstanding 0
      max requests outstanding 3
      consecutive failures 0

[source]PDSN>
```

monitorare il sottoscrittore

Il sottoscrittore di monitoraggio può essere utilizzato per determinare se viene eseguito almeno un tentativo di autenticazione e se viene elaborata una risposta per le chiamate monitorate. Attivare l'opzione 'S', che sta per Sessmgr Sender Info - segnalando in modo efficace il numero di istanza di sessmgr o di amgr che gestisce il messaggio in questione. Di seguito è riportato un esempio di chiamata MIP su un HA connessione alle istanze di sessmgr / aamgr 132.

```
Incoming Call:
------------------------------------------------------------------------
 MSID/IMSI   :                              Callid      : 2719afb2
 IMEI        : n/a                          MSISDN      : n/a
 Username    : 6667067222@cisco.com         SessionType : ha-mobile-ip
 Status      : Active                       Service Name: HAService
 Src Context : source
------------------------------------------------------------------------

*** Sender Info (ON ) ***
Thursday June 11 2015
INBOUND>>>>>  From sessmgr:132 sessmgr_ha.c:861 (Callid 2719afb2) 15:42:35:742 Eventid:26000(3)
MIP Rx PDU, from 203.0.113.11:434 to 203.0.113.1:434 (190)
        Message Type: 0x01 (Registration Request)
               Flags: 0x02
            Lifetime: 0x1C20
        Home Address: 0.0.0.0
  Home Agent Address: 255.255.255.255

Thursday June 11 2015
<<<<OUTBOUND  From aaamgr:132 aaamgr_radius.c:367 (Callid 2719afb2) 15:42:35:743
Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 203.0.113.1:59933 to 209.165.201.3:1645 (301) PDU-
dict=custom9
 Code: 1 (Access-Request)
 Id: 12
 Length: 301

Thursday June 11 2015
INBOUND>>>>>  From aaamgr:132 aaamgr_radius.c:1999 (Callid 2719afb2) 15:42:35:915
Eventid:23900(6)
RADIUS AUTHENTICATION Rx PDU, from 209.165.201.3:1645 to 203.0.113.1:59933 (156) PDU-
dict=custom9
 Code: 2 (Access-Accept)
 Id: 12

Thursday June 11 2015
<<<<OUTBOUND  From sessmgr:132 mipha_fsm.c:6617 (Callid 2719afb2) 15:42:36:265 Eventid:26001(3)
MIP Tx PDU, from 203.0.113.1:434 to 203.0.113.11:434 (112)
        Message Type: 0x03 (Registration Reply)
                Code: 0x00 (Accepted)
            Lifetime: 0x1C20
        Home Address: 10.229.6.167
```

C'è anche un esempio di fallimento alla fine di questo articolo.

Acquisizione pacchetti

A volte le informazioni sull'ASR non sono sufficienti per capire perché si sono verificati problemi di raggiungibilità, nel qual caso è necessario acquisire un pacchetto. Quando si risolvono i problemi dei singoli sottoscrittori, l'identificazione dei rispettivi pacchetti in una traccia dovrebbe essere semplice. In caso contrario, la conoscenza della porta UDP utilizzata a una delle estremità di una determinata coppia di server RADIUS # **<=>** istanza di amgr potrebbe essere utile se il problema è legato a porte/istanze di amgr specifiche. Il tentativo di acquisizione in più punti della rete può essere necessario per determinare dove i pacchetti vengono scartati. Nel problema analizzato in questo articolo, per risolvere il problema è stata l'acquisizione di un pacchetto nella posizione corretta nel percorso di trasporto tra l'ASR e il server RADIUS.

Correzioni

In questa sezione vengono fornite alcune idee per risolvere i problemi di connettività RADIUS.

Non vengono presentati in un ordine particolare, bensì semplicemente in un elenco da prendere in considerazione nel processo di risoluzione dei problemi.

Se il server RADIUS è sovraccarico, è possibile ridurre il carico mediante il valore (predefinito 256) configurato per "radius (accounting) max-standing", che imposta un limite al numero di richieste in attesa (senza risposta) per ogni processo di gestione specificato. Se il limite viene raggiunto, i registri potrebbero indicare quanto segue: "Impossibile assegnare l'ID messaggio per il server di autenticazione radius x.x.x:1812".

I messaggi RADIUS che limitano la velocità a server specifici possono inoltre contribuire a ridurre il carico tramite la parola chiave rate-limit per le rispettive linee di configurazione del server.

A volte non si tratta di un problema di connettività, ma di traffico di accounting aumentato, che non è un problema con RADIUS persay, ma punta a un'altra area, ad esempio le rinegoziazioni ppp aumentate che causano un numero maggiore di avvii e arresti di accounting. Quindi potrebbe essere necessario risolvere i problemi al di fuori di RADIUS per trovare una causa o innesco per i sintomi osservati.

Se durante il processo di risoluzione dei problemi è stato deciso di rimuovere un server di autenticazione o accounting radius dall'elenco dei server attivi per qualsiasi motivo, è disponibile un comando (non config) che disattiva un server per un periodo di tempo indefinito fino a quando non si desidera rimetterlo in servizio. Questo è un approccio più pulito rispetto alla necessità di rimuoverlo manualmente dalla configurazione:

```
{disabilita | enable} server radius [accounting] x.x.x
```

```
[source]CSE2# show radius authentication servers detail

+-----Type:       (A) - Authentication   (a) - Accounting
|                 (C) - Charging         (c) - Charging Accounting
|                (M) - Mediation       (m) - Mediation Accounting
|
|+----Preference: (P) - Primary         (S) - Secondary
||
||+---State:     (A) - Active           (N) - Not Responding
|||               (D) - Down             (W) - Waiting Accounting-On
|||              (I) - Initializing     (w) - Waiting Accounting-Off
|||               (a) - Active Pending   (U) - Unknown
|||
|||+--Admin       (E) - Enabled         (D) - Disabled
|||| Status:
||||
||||+-Admin
||||| status     (O) - Overridden       (.) - Not Overridden
||||| Overridden:
|||||
vvvvv IP             PORT GROUP
----- -------------- ----- ----------------------
APNDO 192.168.50.200 1812 default
```

Una migrazione PSC o DPC o il passaggio a una scheda di linea può spesso risolvere i problemi dovuti al fatto che la migrazione determina il riavvio dei processi sulla scheda, inclusa la npumgr che è stata la causa di problemi di tanto in tanto relativi ai flussi NPU.

Ma in una svolta interessante con il già citato esempio di amgr 92, i fallimenti irraggiungibili di AAA in realtà SONO INIZIATI quando è stata fatta una migrazione PSC. Questa condizione è stata attivata a causa della mancanza di un flusso della NPU quando è stata eseguita una migrazione di PSC durante lo standby di PSC 11. Quando è stato attivato un'ora dopo, l'impatto effettivo del

flusso mancante è iniziato per amgr 92. Problemi come questo sono molto difficili da risolvere senza l'assistenza del supporto tecnico.

```
[Ingressc]PGW# show rct stat

RCT stats Details (Last 6 Actions)
Action            Type      From To   Start Time                Duration
----------------- --------- ---- ---- ------------------------  ----------
Migration         Planned    11   16  2012-Jan-09+16:27:38.135  36.048 sec
Migration         Planned     3   11  2012-Jan-09+17:28:57.413  48.739 sec

Mon Jan 09 17:31:11 2012 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.3
Mon Jan 09 17:31:16 2012 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.3
```

Il problema è stato temporaneamente risolto con un cambio di porta che ha fatto sì che la scheda PSC che aveva un flusso NPU mancante per aamgr 92 non fosse più collegata a una scheda di linea attiva.

```
Tue Jan 10 06:52:17 2012 Internal trap notification 93 (CardStandby) card 27
Tue Jan 10 06:52:17 2012 Internal trap notification 1024 (PortDown) card 27 port 1 ifindex
453050375port type 10G Ethernet
Tue Jan 10 06:52:17 2012 Internal trap notification 55 (CardActive) card 28
Tue Jan 10 06:52:17 2012 Internal trap notification 1025 (PortUp) card 28 port 1 ifindex
469827588port type 10G Ethernet
```

Ultima trap di errore:

```
Tue Jan 10 06:53:11 2012 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address
209.165.201.3

[Ingress]PGW# radius test instance 93 authen server 209.165.201.3 port 1645 test test
Tuesday January 10 07:18:22 UTC 2012

Authentication from authentication server 209.165.201.3, port 1645
Authentication Failure: Access-Reject received
Round-trip time for response was 38.0 ms

[Ingress]PGW# show session subsystem facility aaamgr instance 92
Tuesday January 10 07:39:47 UTC 2012
   12294 Total aaa auth purged
   14209 Total radius auth requests          0 Current radius auth requests
    9494 Total radius requests pend server max-outstanding
       0 Current radius requests pend server max-outstanding
```

Analogamente, anche il riavvio di etichette specifiche che rimangono "bloccate" può risolvere i problemi, anche se si tratta di un'attività che il supporto tecnico deve eseguire in quanto prevede comandi limitati del supporto tecnico. Nell'esempio di aamgr 92 introdotto nella sezione di visualizzazione delle risorse delle attività in precedenza, si è tentato di eseguire questa operazione, ma non è stato di aiuto poiché la causa principale non era aamgr 92, bensì il flusso NPU mancante di cui aamgr 92 aveva bisogno (si trattava di un problema relativo alla NPU, non di un problema relativo ad aamgr). Di seguito è riportato l'output del tentativo. "show task table" viene eseguita per mostrare l'associazione dell'id processo e dell'istanza dell'operazione n. 92.

```
5  2012-Jan-10+06:20:53 aaamgr   16/0/04722 12.0(40466) PLB27085474/PLB38098237
```

```
[Ingress]PGW# show crash number 5
******************** CRASH #05 **********************
Build: 12.0(40466)
Fatal Signal 6: Aborted
  PC: [b7eb6b90/X] __poll()
  Note: User-initiated state dump w/core.

******** show task table *******
     task                            parent
cpu facility      inst    pid pri  facility      inst    pid
---- ----------------------------  ------------------------
16/0 aaamgr          92   4722   0  sessctrl         0   2887
```

Esempio finale

Di seguito è riportato l'ultimo esempio di interruzione effettiva di una rete attiva che riunisce molti dei comandi e degli approcci per la risoluzione dei problemi descritti in questo articolo. Si noti che questo nodo gestisce i tipi di chiamata 3G MIP e 4G Long Term Evolution (LTE) e Evolved High Rate Packet Data (eHRPD).

mostra cronologia trap snmp

Solo dalle trappole, si può confermare che il punto di partenza corrisponde a quello che il cliente ha segnalato come 19:25 UTC. Inoltre, si noti che le trap AAuthSvrUnreachable per il server primario 209.165.201.3 non sono iniziate fino a qualche ora dopo (non è chiaro perché, ma è bene notare; ma l'**accounting non raggiungibile** per il server è stato avviato immediatamente)

```
Sun Dec 29 19:28:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 5 ip
address 209.165.201.3
Sun Dec 29 19:32:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.3
Sun Dec 29 19:33:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.3
Sun Dec 29 19:34:13 2013 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address
209.165.201.3
Sun Dec 29 19:34:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.3
Sun Dec 29 19:35:05 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.3
Sun Dec 29 19:38:13 2013 Internal trap notification 42 (AAAAccSvrUnreachable) server 6 ip
address 209.165.201.8
...
Sun Dec 29 23:12:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:13:03 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:54:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:54:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Sun Dec 29 23:58:13 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Sun Dec 29 23:58:14 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
```

mostra risorse attività

Il risultato mostra un numero molto inferiore di chiamate al DPC 8/1. Basandosi solo su questo, senza ulteriori analisi, si potrebbe suggerire che c'è un problema sul DPC 8 e proporre l'opzione di

migrare al DPC in standby. Ma è importante riconoscere quale sia l'effettivo impatto dell'abbonato - in questi scenari tipicamente gli abbonati si connetteranno con successo a un successivo tentativo e quindi l'impatto non è troppo significativo per l'abbonato e probabilmente non segnaleranno nulla al provider, supponendo che non si verifichi anche un'interruzione dell'aereo utente (che è possibile a seconda di cosa si è rotto).

```
 7/1 sessmgr        230  27% 100% 586.2M  2.49G   43  500  4123 35200 I   good
 7/1 aaamgr         237 0.9%  95% 143.9M 640.0M   22  500    --    -- -   good
 7/1 sessmgr        243  22% 100% 588.1M  2.49G   42  500  4118 35200 I   good
 7/1 sessmgr        258  19% 100% 592.8M  2.49G   43  500  4122 35200 I   good
 7/1 aaamgr         268 0.9%  95% 143.5M 640.0M   22  500    --    -- -   good
 7/1 sessmgr        269  23% 100% 586.7M  2.49G   43  500  4115 35200 I   good
 7/1 aaamgr         274 0.4%  95% 144.9M 640.0M   22  500    --    -- -   good
 7/1 sessmgr        276  30% 100% 587.9M  2.49G   43  500  4123 35200 I   good
 7/1 aaamgr         285 1.0%  95% 142.7M 640.0M   22  500    --    -- -   good
 7/1 aaamgr         286 0.8%  95% 143.8M 640.0M   22  500    --    -- -   good
 7/1 sessmgr        290  28% 100% 588.2M  2.49G   41  500  4115 35200 I   good

 8/0 sessmgr        177  23% 100% 588.7M  2.49G   48  500  4179 35200 I   good
 8/0 sessmgr        193  24% 100% 591.3M  2.49G   44  500  4173 35200 I   good
 8/0 aaamgr         208 0.9%  95% 143.8M 640.0M   22  500    --    -- -   good
 8/0 sessmgr        211  23% 100% 592.1M  2.49G   45  500  4173 35200 I   good
 8/0 sessmgr        221  27% 100% 589.2M  2.49G   44  500  4178 35200 I   good
 8/0 aaamgr         222 0.9%  95% 142.0M 640.0M   22  500    --    -- -   good
 8/0 sessmgr        225  25% 100% 592.0M  2.49G   43  500  4177 35200 I   good
 8/0 aaamgr         238 0.9%  95% 140.0M 640.0M   22  500    --    -- -   good
 8/0 aaamgr         243 1.0%  95% 144.9M 640.0M   22  500    --    -- -   good
 8/0 sessmgr        244  31% 100% 593.3M  2.49G   43  500  4177 35200 I   good
 8/0 aaamgr         246 0.9%  95% 138.5M 640.0M   22  500    --    -- -   good
 8/0 aaamgr         248 0.9%  95% 141.4M 640.0M   22  500    --    -- -   good
 8/0 aaamgr         258 0.9%  95% 138.3M 640.0M   22  500    --    -- -   good
 8/0 aaamgr         259 0.8%  95% 139.2M 640.0M   22  500    --    -- -   good
 8/0 aaamgr         260 0.8%  95% 142.9M 640.0M   22  500    --    -- -   good
 8/0 aaamgr         262 0.9%  95% 145.0M 640.0M   22  500    --    -- -   good
 8/0 aaamgr         264 0.9%  95% 143.4M 640.0M   22  500    --    -- -   good
 8/0 sessmgr        270  24% 100% 592.2M  2.49G   44  500  4171 35200 I   good
 8/0 sessmgr        277  20% 100% 593.7M  2.49G   43  500  4176 35200 I   good
 8/0 sessmgr        288  23% 100% 591.9M  2.49G   43  500  4177 35200 I   good
 8/0 sessmgr        296  24% 100% 593.0M  2.49G   42  500  4170 35200 I   good

 8/1 sessmgr        186 2.0% 100% 568.3M  2.49G   48  500  1701 35200 I   good
 8/1 sessmgr        192 2.0% 100% 571.1M  2.49G   46  500  1700 35200 I   good
 8/1 aaamgr         200 1.0%  95% 147.3M 640.0M   22  500    --    -- -   good
 8/1 sessmgr        210 2.1% 100% 567.1M  2.49G   46  500  1707 35200 I   good
 8/1 aaamgr         216 0.9%  95% 144.6M 640.0M   22  500    --    -- -   good
 8/1 sessmgr        217 2.0% 100% 567.7M  2.49G   45  500  1697 35200 I   good
 8/1 sessmgr        231 2.2% 100% 565.7M  2.49G   45  500  1705 35200 I   good
 8/1 sessmgr        240 2.0% 100% 569.8M  2.49G   45  500  1702 35200 I   good
 8/1 aaamgr         242 0.9%  95% 148.5M 640.0M   22  500    --    -- -   good
 8/1 sessmgr        252 1.8% 100% 566.5M  2.49G   44  500  1704 35200 I   good
 8/1 aaamgr         261 0.9%  95% 142.0M 640.0M   22  500    --    -- -   good
 8/1 aaamgr         263 1.0%  95% 144.1M 640.0M   22  500    --    -- -   good
 8/1 aaamgr         265 1.0%  95% 146.4M 640.0M   22  500    --    -- -   good
 8/1 aaamgr         267 1.0%  95% 144.4M 640.0M   22  500    --    -- -   good
 8/1 aaamgr         269 1.0%  95% 143.8M 640.0M   22  500    --    -- -   good
 8/1 sessmgr        274 1.9% 100% 570.5M  2.49G   44  500  1704 35200 I   good
 8/1 sessmgr        283 2.0% 100% 570.0M  2.49G   44  500  1708 35200 I   good
 8/1 sessmgr        292 2.1% 100% 567.6M  2.49G   44  500  1703 35200 I   good

 9/0 sessmgr          1  30% 100% 587.2M  2.49G   48  500  4161 35200 I   good
 9/0 diamproxy        1 5.2%  90% 37.74M 250.0M  420 1000    --    -- -   good
```

```
 9/0 sessmgr         14  25% 100% 587.4M  2.49G   48  500  4156 35200 I   good
 9/0 sessmgr         21  20% 100% 591.5M  2.49G   47  500  4156 35200 I   good
 9/0 sessmgr         34  23% 100% 586.5M  2.49G   48  500  4155 35200 I   good
 9/0 aaamgr          44 0.9%  95% 145.1M 640.0M   21  500    --    -- -   good
 9/0 sessmgr         46  29% 100% 592.1M  2.49G   48  500  4157 35200 I   good
```

monitorare il sottoscrittore

Èstata rilevata una configurazione di chiamata in cui non è stata ricevuta alcuna risposta alla richiesta di autenticazione per l'autenticazione primaria 209.165.201.3 per sessmgr 242 su DPC 9/1, che si verifica se il relativo amgr associato risiede su DPC 8/1, confermando errori 3G dovuti a AAA non raggiungibile su 8/1. Conferma inoltre che, anche se non sono state rilevate trap AAAAuthSrvUnreachable per 209.165.201.3 fino a quel momento, non è Ciò significa che non esiste alcun problema per la gestione delle risposte per il server (come illustrato in precedenza, le trap vengono avviate solo dopo alcune ore).

```
8/1 aaamgr         242 0.9%  95% 148.5M 640.0M   22  500    --    -- -   good
9/1 sessmgr        242  20% 100% 589.7M  2.49G   43  500  4167 35200 I   good

------------------------------------------------------------------------
Incoming Call:
------------------------------------------------------------------------
MSID/IMSI   :                           Callid      : 4537287a
IMEI        : n/a                       MSISDN      : n/a
Username    : 6664600074@cisco.com      SessionType : ha-mobile-ip
Status      : Active                    Service Name: HAService
Src Context : Ingress
------------------------------------------------------------------------

INBOUND>>>>>  From sessmgr:242 sessmgr_ha.c:880 (Callid 4537287a) 23:18:19:099 Eventid:26000(3)
MIP Rx PDU, from 203.0.113.1:434 to 203.0.113.3:434 (190)
        Message Type: 0x01 (Registration Request)

<<<<OUTBOUND  From aaamgr:242 aaamgr_radius.c:370 (Callid 4537287a) 23:18:19:100
Eventid:23901(6)
RADIUS AUTHENTICATION Tx PDU, from 203.0.113.3:27856 to 209.165.201.3:1645 (301) PDU-
dict=custom9
Code: 1 (Access-Request)
Id: 195
Length: 301
Authenticator: CD 59 0C 6D 37 2C 5D 19 FB 60 F3 35 23 BB 61 6B
      User-Name = 6664600074@cisco.com

INBOUND>>>>>  From sessmgr:242 mipha_fsm.c:8438 (Callid 4537287a) 23:18:21:049 Eventid:26000(3)
MIP Rx PDU, from 203.0.113.1:434 to 203.0.113.3:434 (140)
        Message Type: 0x01 (Registration Request)
               Flags: 0x02
            Lifetime: 0x1C20

<<<<OUTBOUND  From sessmgr:242 mipha_fsm.c:6594 (Callid 4537287a) 23:18:22:117 Eventid:26001(3)
MIP Tx PDU, from 203.0.113.3:434 to 203.0.113.1:434 (104)
        Message Type: 0x03 (Registration Reply)
                Code: 0x83 (Mobile Node Failed Authentication)

***CONTROL*** From sessmgr:242 sessmgr_func.c:6746 (Callid 4537287a) 23:18:22:144 Eventid:10285
CALL STATS: <6664600074@cisco.com>, msid <>, Call-Duration(sec): 0
  Disconnect Reason: MIP-auth-failure
  Last Progress State: Authenticating
```

show sub [summary] smgr-instance X

La cosa interessante è che il conteggio delle sessioni per sessmgr 242 è simile a quello di altre

sessioni di lavoro. Ulteriori indagini hanno dimostrato che le chiamate 4G, anch'esse ospitate su questo chassis, erano in grado di connettersi e quindi hanno compensato la mancanza di chiamate IP mobili 3G in grado di connettersi. È possibile stabilire che, tornando indietro fino a 8 ore dopo l'inizio dell'interruzione, non ci sono chiamate MIP per questa sessione mgr 242, mentre tornando indietro di 9 ore prima dell'inizio dell'interruzione, ci sono chiamate connesse:

```
[local]PGW# show sub sum smgr-instance 242 connected-time less-than 28800  (8 hours)
Monday December 30 03:38:23 UTC 2013

Total Subscribers:             1504
Active:                        1504          Dormant:                       0
hsgw-ipv4-ipv6:                0             pgw-pmip-ipv6:                 98
pgw-pmip-ipv4:                 0             pgw-pmip-ipv4-ipv6:            75
pgw-gtp-ipv6:                  700           pgw-gtp-ipv4:                  3
pgw-gtp-ipv4-ipv6:             628           sgw-gtp-ipv6:                  0
..
ha-mobile-ip:                  0             ggsn-pdp-type-ppp:             0

[local]PGW# show sub sum smgr-instance 242 connected-time less-than 32400 (9 hours)
Monday December 30 03:38:54 UTC 2013 ...
ha-mobile-ip: 63 ggsn-pdp-type-ppp: 0
```

Le chiamate LTE e eHRPD mostrano un rapporto più elevato rispetto alle chiamate MIP quando si confrontano le sessmgrs connesse con le schede funzionanti e interrotte:

```
[local]PGW# show sub sum smgr-instance 272
Monday December 30 03:57:51 UTC 2013
hsgw-ipv4-ipv6: 0 pgw-pmip-ipv6: 125 pgw-pmip-ipv4: 0 pgw-pmip-ipv4-ipv6: 85 pgw-gtp-ipv6: 1530
pgw-gtp-ipv4-ipv6: 1126
ha-mobile-ip: 1103

[local]PGW# show sub sum smgr-instance 242
Monday December 30 03:52:35 UTC 2013
hsgw-ipv4-ipv6: 0 pgw-pmip-ipv6: 172 pgw-pmip-ipv4: 0 pgw-pmip-ipv4-ipv6: 115
pgw-gtp-ipv6: 1899
pgw-gtp-ipv4-ipv6: 1348

ha-mobile-ip: 447
```

server di autenticazione X istanza test radius

Tutti gli aamgrs su 8/1 sono morti - nessun comando di istanza di test del raggio funziona per uno di questi aamgrs ma funziona per aamgrs su 8/0 e altre schede:

```
9/1 sessmgr        242  22% 100% 600.6M  2.49G   41  500  3989 35200 I   good
4/1 sessmgr         20  27% 100% 605.1M  2.49G   47  500  3965 35200 I   good
4/0 sessmgr         27  25% 100% 592.8M  2.49G   46  500  3901 35200 I   good

8/1 aaamgr         242 0.9%  95% 150.6M 640.0M   22  500    --    -- -   good
8/1 aaamgr          20 1.0%  95% 151.9M 640.0M   21  500    --    -- -   good
8/0 aaamgr          27 1.0%  95% 146.4M 640.0M   21  500    --    -- -   good

[Ingress]PGW# radius test instance 242 auth server 209.165.201.3 port 1645 test test
Monday December 30 01:03:08 UTC 2013

Authentication from authentication server 209.165.201.3, port 1645
Communication Failure: No response received

[Ingress]PGW# radius test instance 20 auth server 209.165.201.3 port 1645 test test
```

```
Monday December 30 01:08:45 UTC 2013

Authentication from authentication server 209.165.201.3, port 1645
Communication Failure: No response received

[Ingress]PGW# radius test instance 27 auth server 209.165.201.3 port 1645 test test
Monday December 30 01:11:40 UTC 2013

Authentication from authentication server 209.165.201.3, port 1645
Authentication Failure: Access-Reject received
Round-trip time for response was 16.8 ms
```

mostra tutti i contatori del raggio

Il comando di punta per la risoluzione dei problemi relativi a RADIUS mostra un aumento rapido di molti timeout:

```
[Ingress]PGW> show radius counters all | grep -E "Authentication server address|Access-Request
Timeouts"
Monday December 30 00:42:24 UTC 2013
  Authentication server address 209.165.201.3, port 1645, group default
    Access-Request Timeouts:                                  400058
  Authentication server address 209.165.201.5, port 1645, group default
     Access-Request Timeouts:                                  26479

[Ingress]PGW> show radius counters all | grep -E "Authentication server address|Access-Request
Timeouts"
Monday December 30 00:45:23 UTC 2013
  Authentication server address 209.165.201.3, port 1645, group default
    Access-Request Timeouts:                                  400614
  Authentication server address 209.165.201.5, port 1645, group default
     Access-Request Timeouts:                                  26679


[Ingress]PGW> show radius counters all
Monday December 30 00:39:15 UTC 2013
...
   Authentication server address 209.165.201.3, port 1645, group default
     Access-Request Sent:                                     233262801
     Access-Request with DMU Attributes Sent:                 0
     Access-Request Pending:                                  22
     Access-Request Retried:                                  0
     Access-Request with DMU Attributes Retried:              0
     Access-Challenge Received:                               0
     Access-Accept Received:                                  213448486
     Access-Reject Received:                                  19414836
     Access-Reject Received with DMU Attributes:              0
     Access-Request Timeouts:                                 399438
     Access-Request Current Consecutive Failures in a mgr:    3
     Access-Request Response Bad Authenticator Received:      16187
     Access-Request Response Malformed Received:              1
     Access-Request Response Malformed Attribute Received:    0
     Access-Request Response Unknown Type Received:           0
     Access-Request Response Dropped:                         9039
     Access-Request Response Last Round Trip Time:            267.6 ms
     Access-Request Response Average Round Trip Time:         201.9 ms
     Current Access-Request Queued:                           2

    Authentication server address 209.165.201.5, port 1645, group default
     Access-Request Sent:                                     27731
     Access-Request with DMU Attributes Sent:                 0
     Access-Request Pending:                                  0
```

```
     Access-Request Retried:                                  0
     Access-Request with DMU Attributes Retried:              0
     Access-Challenge Received:                               0
     Access-Accept Received:                                  1390
     Access-Reject Received:                                  101
     Access-Reject Received with DMU Attributes:              0
     Access-Request Timeouts:                                 26240
     Access-Request Current Consecutive Failures in a mgr:    13
     Access-Request Response Bad Authenticator Received:      0
     Access-Request Response Malformed Received:              0
     Access-Request Response Malformed Attribute Received:    0
     Access-Request Response Unknown Type Received:           0
     Access-Request Response Dropped:                         0
     Access-Request Response Last Round Trip Time:            227.5 ms
     Access-Request Response Average Round Trip Time:         32.3 ms
     Current Access-Request Queued:                           0
```

Correzione

Durante le finestre di manutenzione, una migrazione DPC da 8 a 10 ha risolto il problema, le trap AAAuthSrvUnreachable sono state arrestate e DPC 8 è stato sottoposto a RMA e la causa principale è stata determinata come un guasto hardware su DPC 8 (i dettagli di tale guasto non sono importanti ai fini di questo articolo).

```
Mon Dec 30 05:58:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Mon Dec 30 05:58:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 2 ip
address 209.165.201.5
Mon Dec 30 05:58:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 2 ip address
209.165.201.5
Mon Dec 30 05:58:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3
Mon Dec 30 05:59:14 2013 Internal trap notification 43 (AAAAccSvrReachable) server 5 ip address
209.165.201.5
Mon Dec 30 06:01:14 2013 Internal trap notification 39 (AAAAuthSvrUnreachable) server 4 ip
address 209.165.201.3
Mon Dec 30 06:01:27 2013 Internal trap notification 40 (AAAAuthSvrReachable) server 4 ip address
209.165.201.3

Mon Dec 30 06:01:28 2013 Internal trap notification 16 (PACMigrateStart) from card 8 to card 10

Mon Dec 30 06:01:49 2013 Internal trap notification 60 (CardDown) card 8 type Data Processing
Card
Mon Dec 30 06:01:50 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 10 operational status changed to Active
Mon Dec 30 06:01:50 2013 Internal trap notification 55 (CardActive) card 10 type Data Processing
Card
Mon Dec 30 06:01:50 2013 Internal trap notification 17 (PACMigrateComplete) from card 8 to card
10

Mon Dec 30 06:02:08 2013 Internal trap notification 5 (CardUp) card 8 type Data Processing Card
Mon Dec 30 06:02:08 2013 Internal trap notification 1502 (EntStateOperEnabled) Card(8) Severity:
Warning
Mon Dec 30 06:02:08 2013 Internal trap notification 93 (CardStandby) card 8 type Data Processing
Card

Mon Dec 30 06:08:41 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 08 operational status changed to Offline
Mon Dec 30 06:08:41 2013 Internal trap notification 60 (CardDown) card 8 type Data Processing
Card
Mon Dec 30 06:08:41 2013 Internal trap notification 1503 (EntStateOperDisabled) Card(8)
Severity: Critical
```

```
Mon Dec 30 06:09:24 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity
Card : 08 Power OFF
Mon Dec 30 06:09:24 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 08 operational status changed to Empty
Mon Dec 30 06:09:24 2013 Internal trap notification 7 (CardRemoved) card 8 type Data Processing
Card
Mon Dec 30 06:09:24 2013 Internal trap notification 1507 (CiscoFruRemoved) FRU entity Card : 08
removed
Mon Dec 30 06:09:24 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity
Card : 08 Power OFF
Mon Dec 30 06:09:50 2013 Internal trap notification 1505 (CiscoFruPowerStatusChanged) FRU entity
Card : 08 Power ON
Mon Dec 30 06:09:53 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 08 operational status changed to Offline
Mon Dec 30 06:09:53 2013 Internal trap notification 8 (CardInserted) card 8 type Data Processing
Card
Mon Dec 30 06:09:53 2013 Internal trap notification 1506 (CiscoFruInserted) FRU entity Card : 08
inserted
Mon Dec 30 06:10:00 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 08 operational status changed to Booting
Mon Dec 30 06:11:59 2013 Internal trap notification 1504 (CiscoFruCardStatusChanged) FRU entity
Card : 08 operational status changed to Standby
Mon Dec 30 06:11:59 2013 Internal trap notification 5 (CardUp) card 8 type Data Processing Card
Mon Dec 30 06:11:59 2013 Internal trap notification 93 (CardStandby) card 8 type Data Processing
Card

[local]PGW# show rct stat
Wednesday January 01 16:47:21 UTC 2014

RCT stats Details (Last 2 Actions)
Action            Type      From To   Start Time                Duration
----------------- --------- ---- ---- ------------------------  ----------
Migration         Planned     8   10  2013-Dec-30+06:01:28.323  21.092 sec
Shutdown          N/A         8    0  2013-Dec-30+06:08:41.483   0.048 sec
```