Dépannage des interruptions AAAAccSrvUnreachable et AAAAuthSrvUnreachable

Contenu

Introduction

Cet article explique comment dépanner les déroutements SNMP AAAAccSrvUnreachable et AAAAuthSrvUnreachable, qui sont déclenchés en raison de problèmes d'accessibilité avec un serveur RADIUS (Remote Authentication Dial-In User Service) utilisé pour authentifier les abonnés (ou les opérateurs se connectant au noeud, mais ce n'est pas ce qui est discuté ici). Il existe deux approches qui peuvent être utilisées pour déterminer quand l'un de ces pièges se déclenchera. Cet article explique quelles conditions déclenchent ces pièges et quelles approches de dépannage et de collecte de données peuvent être prises pour déterminer la cause première et les résoudre. Il traite également de certaines mesures correctives possibles qui peuvent être envisagées.

Notez que le RÉSULTAT de l'inaccessibilité sera des échecs d'appel ou des échecs de comptabilisation, comme si les réponses de rayon sont des rejets au lieu d'acceptations. Bien que le taux de réussite/d'échec (authentification) soit mesuré indépendamment du délai d'attente/d'accessibilité (il y a des interruptions et des alarmes pour cela) et peut certainement être analysé à lui seul, l'objet de cet article sera de se concentrer sur le problème d'accessibilité et non sur le problème de rejet.

Des exemples de résultats du LAB et des tickets réels sont utilisés tout au long de la discussion pour aider à les comprendre. Ce qui semble être des adresses IP publiques dans cet article sont

de **fausses** adresses.

Déclencheurs de déroutement

Il existe deux modèles/algorithmes/approches différents parmi lesquels choisir pour déterminer l'état d'un serveur RADIUS et quand essayer un serveur différent en cas de défaillance :

Échecs consécutifs dans une approche de processus aaamgr

L'approche originale et celle utilisée plus souvent par les opérateurs implique de suivre le nombre de défaillances qui se sont produites dans une ligne pour un processus aamgr particulier. Un processus aamgr est responsable du traitement et de l'échange des messages radius avec un serveur radius, et de nombreux processus aamgr existent dans un châssis, chacun associé aux processus sessmgr (qui sont les principaux processus responsables du contrôle des appels). (Voir tous les processus aamgr avec la commande « show task resources ») Un processus aamgr particulier traitera donc des messages radius pour de nombreux appels, pas seulement un appel, et cet algorithme consiste à suivre le nombre de fois dans une ligne qu'un processus aamgr particulier n'a pas obtenu de réponse à la même demande qu'il a eu à renvoyer - un « délai de demande d'accès » comme indiqué dans « show radius counters ».

Le compteur correspondant « Erreurs consécutives actuelles de demande d'accès dans un gestionnaire », également de « show radius counters » est incrémenté lorsque cela se produit, et la commande « show radius accounting (ou authentication) servers detail » indique les horodatages du changement d'état de rayon d'Active à Not Responding (mais aucun déroutement ou journal SNMP n'est généré pour une seule défaillance). Voici un exemple de comptabilité de rayon :

```
[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
```

Si ce compteur atteint la valeur configurée (par défaut = 4) sans jamais être réinitialisé, par configurable : (notez que les crochets [ ] sont utilisés pour indiquer un qualificatif facultatif et, dans ces cas, capture la comptabilité de dépannage (l'authentification est la valeur par défaut si la comptabilité n'est pas spécifiée)

radius [accounting] detect-dead-server consécutifs-échecs 4

Ensuite, ce serveur est marqué « Arrêté » pour la période (minutes) configurée :

radius [accounting] délai 10

Un déroutement et des journaux SNMP sont également déclenchés, par exemple, pour l'authentification et/ou la comptabilité respectivement :

```
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
```

Les déroutements indiquent le serveur inaccessible. Prenez note de tout motif. Par exemple, est-ce que cela se produit avec un serveur ou un autre ou tous les serveurs, et quelle est la fréquence des rebondissements - est-ce que cela se produit continuellement ou occasionnellement ?

Notez également que tout ce qu'il faut pour déclencher ce piège est qu'un aamgr échoue, et donc la partie délicate de ce piège est qu'il n'indique pas l'étendue du problème. Il pourrait s'agir d'une question très vaste ou très mineure - c'est à l'exploitant de déterminer, et les approches pour le déterminer sont discutées dans cet article.

show snmp trap statistics indique le nombre de fois qu'il a déclenché depuis le démarrage, même si les anciennes interruptions ont été supprimées depuis longtemps. Cet exemple montre un problème de comptabilité inaccessible :

```
[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
```

Notez que l'aaamgr signalé dans l'exemple ci-dessus est #231. Il s'agit de l'analyseur de gestion de l'ASR 5000 qui réside sur la carte de gestion du système (SMC). Ce qui est trompeur dans ce résultat est que lorsqu'un aamgr ou aamgrs individuel rencontre des problèmes d'accessibilité, le numéro d'instance indiqué dans les journaux est l'instance de management aamgr et non les instances particulières qui rencontrent le problème. Cela est dû au fait que si de nombreux cas rencontrent des problèmes d'accessibilité, alors la journalisation se remplirait rapidement si elles étaient toutes signalées comme telles, et donc la conception a été de faire rapport de manière générique sur l'instance de gestion, qui si on ne le savait pas, serait certainement trompeuse. Dans la section de dépannage, des détails supplémentaires seront fournis sur la façon de déterminer quels sont les correcteurs aaamgr qui échouent. À partir de certaines versions de StarOS 17 et v18+, ce comportement a été modifié de sorte que le numéro d'instance aamgr correspondant ayant des problèmes de connectivité (comme indiqué dans les déroutements SNMP) est signalé dans les journaux avec l'ID particulier (Cisco CDETS CSCum84773), bien que seule la première occurrence (sur plusieurs aamgrs) de ce qui se produit soit signalée.

L'aamgr de gestion est le numéro d'instance maximum sessmgr + 1, et ainsi sur un ASR 5500 il est 385 pour DPC (Data Processing Card) ou 1153 (pour DPC 2).

En tant que sidenote, l'administrateur de gestion est responsable du traitement des connexions opérateur/administrateur ainsi que du traitement des demandes de modification d'autorisation initiées à partir des serveurs RADIUS eux-mêmes.

En continuant, la commande « show radius accounting (ou authentication) servers detail » indique les horodatages des changements d'état sur Down qui correspondent aux déroutements/journaux (rappel : Ne pas répondre défini précédemment est seulement un aamgr unique obtenant un délai d'attente, tandis que Down est un aamgr unique obtenant suffisamment de délais consécutifs par configuration pour déclencher 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
```

S'il n'y a qu'un seul serveur configuré, il n'est pas marqué comme désactivé, car cela serait essentiel pour la réussite de la configuration des appels.

Il convient de mentionner qu'il existe un autre paramètre qui peut être configuré sur la ligne de configuration detect-dead-server appelée “ response-timeout ”. Lorsqu'il est spécifié, un serveur n'est marqué comme inactif que lorsque les conditions d'échec consécutif et de délai d'attente de réponse sont toutes deux remplies. Le délai de réponse spécifie une période pendant laquelle AUCUNE réponse n'est reçue à TOUTES les requêtes envoyées à un serveur particulier. (Notez que ce compteur sera continuellement réinitialisé à mesure que les réponses seront reçues.) Cette condition est attendue lorsqu'un serveur ou une connexion réseau est complètement hors service, par rapport à une compromission ou une dégradation partielle.

Le cas d'utilisation pour cela serait un scénario où une rafale de trafic provoque le déclenchement des échecs consécutifs, mais le marquage d'un serveur immédiatement en cas de panne n'est pas souhaité. Au contraire, le serveur n'est marqué comme inaccessible qu'après une période spécifique de temps où aucune réponse n'est reçue, ce qui représente une réelle inaccessibilité du serveur.

Cette méthode qui vient d'être discutée pour contrôler les modifications de la machine d'état de rayon dépend de l'examen de tous les processus aamgr et de la recherche d'un qui déclenche la condition des tentatives échouées. Cette méthode est soumise dans une certaine mesure à une certaine aléa des défaillances, et il se peut donc qu'elle ne soit pas l'algorithme idéal pour détecter les défaillances. Mais il est particulièrement bon de trouver aamgr(s) qui sont cassés alors que tous les autres fonctionnent bien.

Approche de maintien de la vie

Une autre méthode de détection de l'accessibilité du serveur radius consiste à utiliser des messages de test keepalive factices. Cela implique l'envoi constant de faux messages de rayon au lieu de surveiller le trafic en direct. Un autre avantage de cette méthode est qu'elle est toujours active, par rapport aux échecs consécutifs dans une approche aamgr, où il peut y avoir des périodes où aucun trafic de rayon n'est envoyé, et donc il n'y a aucun moyen de savoir si un problème existe pendant ces périodes, ce qui entraîne un retard de détection lorsque des tentatives commencent à se produire. En outre, lorsqu'un serveur est marqué comme inactif, ces messages de test d'activité continuent d'être envoyés afin que le serveur puisse être marqué dès que possible. L'inconvénient de cette approche est qu'elle ne détecte pas les problèmes liés à des instances aamgr spécifiques qui peuvent rencontrer des problèmes car elle utilise l'instance d'aamgr de gestion pour les messages de test.

Voici les différents paramètres de configuration pertinents pour cette approche :

```
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
```

La commande “ radius (accounting) detect-dead-server keepalive ” active l'approche keep-alive au lieu des échecs consécutifs dans une approche aamgr. Dans l'exemple ci-dessus, le système envoie un message de test avec le nom d'utilisateur Test-Username et le mot de passe Test-Username toutes les 30 secondes, et recommence toutes les 3 secondes si aucune réponse n'est reçue, puis recommence jusqu'à 3 fois, après quoi il marque le serveur hors service. Une fois qu'il

a reçu sa première réponse, il la marque à nouveau.

Voici un exemple de demande/réponse d'authentification pour les paramètres ci-dessus :

```
<<<<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 = 0000000000000000
     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
```

Les mêmes déroutements SNMP sont utilisés pour indiquer les états de rayon inaccessible/inaccessible et accessible/actif/actif comme pour les pannes consécutives dans une approche aamgr :

```
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 “ show radius counters all ” comporte également une section permettant de suivre les demandes keepalive pour l'authentification et la comptabilité. Voici les compteurs d'authentification :

```
   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
```

Commandes/approches de dépannage

Maintenant que le déclencheur des pièges AAA inaccessibles a été expliqué, l'étape suivante consiste à comprendre les différentes commandes de dépannage à utiliser pour déterminer l'impact et essayer de déterminer la cause première. L'inaccessibilité est un terme très large. Il n'explique pas où se trouve l'inaccessibilité - dans le réseau, sur le serveur ou sur l'ASR. Par exemple, est-il connu que les demandes ont même été envoyées en premier lieu ? Le serveur a-t-il reçu les requêtes ? A-t-elle répondu à ces demandes ? Les réponses sont-elles retournées à l'ASR et, dans l'affirmative, ont-elles été traitées ou abandonnées sur le chemin interne (c.-à-d. les flux). Cette section tente d'aborder la façon de répondre à ces questions.

Notions de base sur la configuration de Radius

Il y a d'abord quelques notions de base que l'on doit connaître en ce qui concerne la configuration RADIUS. La plupart de la configuration de RADIUS se trouve dans un groupe spécifiquement nommé et tous les contextes ont un groupe par défaut qui peut être configuré comme suit. Souvent, les configurations n'ont qu'un seul groupe, le groupe par défaut.

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

Si des groupes aaa spécifiques nommés sont utilisés, ils sont signalés par l'instruction suivante configurée dans un profil d'abonné ou un nom de point d'application (APN) (selon la technologie de contrôle des appels), par exemple :

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

Note: Le système vérifie d'abord le groupe aaa spécifique attribué à l'abonné, puis vérifie la valeur par défaut du groupe aaa pour les paramètres configurables supplémentaires non définis dans le groupe spécifique.

Voici des commandes utiles qui résument toutes les valeurs attribuées à tous les configurables dans les différentes configurations de groupe aaa. Cela permet d'afficher rapidement tous les paramètres configurables, y compris les valeurs par défaut, sans avoir à examiner la configuration manuellement, et peut-être d'éviter de faire des erreurs lors de l'hypothèse de certains paramètres. Ces commandes font état de tous les contextes :

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

Le configurable le plus important est bien sûr les serveurs d'accès et de comptabilité RADIUS eux-mêmes. Voici un exemple :

```
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
```

Notez la fonction max-rate qui limite le nombre de requêtes envoyées au serveur par aamgr par seconde

En outre, l'adresse IP NAS doit également être définie, c'est-à-dire l'adresse IP d'une interface dans le contexte à partir duquel les requêtes RADIUS sont envoyées et les réponses reçues. Si elles ne sont pas définies, les requêtes ne sont pas envoyées et le suivi des traces d'abonnés peut ne pas afficher d'erreur évidente (aucune requête de rayon n'est envoyée et aucune indication de pourquoi).

radius, attribut nas-ip-address adresse 10.211.41.129

Notez que comme l'authentification et la comptabilité sont souvent gérées par le même serveur, un numéro de port différent est utilisé pour différencier le trafic d'authentification et le trafic de comptabilité sur le serveur RADIUS. Pour le côté ASR5K, le numéro de port source UDP n'est PAS spécifié et est choisi par le châssis sur une base aamgr (plus d'informations sur ce point ultérieurement).
Normalement, plusieurs serveurs d'accès et de comptabilité sont spécifiés à des fins de redondance. Il est possible de configurer un round robin ou une commande hiérarchisée :

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

L'option du premier serveur entraîne l'envoi de TOUTES les requêtes au serveur dont la priorité est la plus faible. Ce n'est que lorsque des échecs de nouvelle tentative se produisent, ou pire, qu'un serveur est marqué comme inactif, que le serveur dont la priorité suivante a été tentée est le serveur. Plus d'informations sur ce sujet ci-dessous.

Lorsqu'une demande radius (de comptabilité ou d'accès) est envoyée, une réponse est attendue. Lorsqu'une réponse n'est pas reçue dans le délai imparti (secondes) :

radius [accounting] timeout 3

La demande est envoyée jusqu'au nombre de fois spécifié :

radius [accounting] max-retries 5

Cela signifie qu'une requête peut être envoyée au total de max-retries + 1 fois jusqu'à ce qu'elle abandonne sur le serveur radius particulier essayé. À ce stade, il tente la même séquence vers le serveur radius suivant dans l'ordre. Si chacun des serveurs a été testé max-retries + 1 fois sans réponse, alors l'appel est rejeté, en supposant qu'il n'y ait aucune autre raison de défaillance jusqu'à ce point.

En tant que remarque, il existe des paramètres configurables qui permettent aux utilisateurs d'avoir accès même en cas d'échec de l'authentification et de la comptabilité en raison de délais d'attente sur tous les serveurs, bien qu'un déploiement commercial n'implémente probablement pas ceci :

radius allow [accounting] authentication down

En outre, il existe des paramètres configurables qui peuvent limiter le nombre total absolu de transmissions d'une demande particulière sur tous les serveurs configurés, et ceux-ci sont

désactivés par défaut :

radius [accounting] max-transmissions 256

Par exemple, si cette valeur est définie sur 1, alors même s'il existe un serveur secondaire, elle n'est jamais tentée car une seule tentative de configuration d'un abonné spécifique est jamais tentée.

show task resources installation aaamgr all

Chaque processus aamgr est associé et fonctionne pour un processus sessmgr associé (responsable de la gestion globale des appels) et se trouve sur une carte de services de paquets (PSC) ou une carte de traitement de données (DPC) différente mais utilisant le même ID d'instance. Dans cet exemple également, notez l'instance aamgr spéciale 231 exécutée sur la carte de gestion du système (SMC) pour ASR 5000 (ou la carte de sortie d'entrée de gestion pour ASR 5500 (MIO)) qui ne traite PAS les demandes d'abonnés mais qui est utilisée pour les commandes de test radius (voir plus loin pour plus de détails) ET pour le traitement de connexion CLI opérateur.

Dans cet extrait, aamgr 107 situé sur PSC 13 est responsable du traitement de tous les traitements RADIUS pour le sessmgr 107 apparié situé sur PSC 1. Les problèmes d'accessibilité pour aamgr 107 affectent les appels sur 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
```

Dans l'exemple suivant, notez que les problèmes avec aamgr 92 affectent le sessmgr apparié comme on le voit facilement par rapport aux autres sessions en ce qui concerne le nombre de sessions :

```
                   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 | serveur <IP du serveur>} [instance <aamgr #>] | résumé}

La commande numéro un à connaître est une variété de « show radius counters »

Cette commande renvoie de nombreux compteurs utiles pour le dépannage des problèmes de rayon. La commande « show radius counters all » est très utile pour suivre les succès et les échecs sur une base de serveur, et il est important de comprendre la signification des différents compteurs qui composent cette commande, car elle n'est peut-être pas évidente. La commande

est sensible au contexte et doit donc être exécutée dans le même contexte où les groupes aaa sont définis.

Remarque importante : Sur une période non contrôlée, il est difficile de tirer des conclusions à partir des valeurs des compteurs ou des relations entre les compteurs. Pour tirer des conclusions précises, la meilleure approche consiste à réinitialiser les compteurs et à les surveiller pendant une période de temps où le problème est en cours de dépannage.

Dans le résultat suivant, notez « Demande d'accès envoyée » = 1, alors que « Demande d'accès renouvelée » = 3. Ainsi, toute nouvelle requête donnée à un serveur radius particulier n'est comptée qu'une seule fois, et toutes les tentatives sont comptées séparément. Dans ce cas, cela représente un total de 3 + 1 = 4 demandes d'accès envoyées. Notez le compteur « Délais d'attente des demandes d'accès » = 1. Un délai d'attente unique se produit uniquement lorsque TOUTES les tentatives échouent. Dans ce cas, 3 tentatives sans réponse ont pour résultat 1 délai d'attente (et non 4). Cela se produit sur tous les serveurs configurés jusqu'à ce qu'il y ait succès ou que toutes les tentatives aient échoué. Faites donc attention aux compteurs qui sont suivis séparément pour chaque serveur. Voici un exemple, où :

```
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
```

Notez également que les délais d'attente NE sont PAS comptabilisés comme des échecs, ce qui signifie que le nombre d'Access-Accept reçu et d'Access-Reject reçu ne correspond pas à Access-Request Sent s'il y a des délais d'attente.

L'analyse de ces compteurs n'est peut-être pas tout à fait simple. Par exemple, pour le protocole MIP (Mobile IP), les authentifications échouant, aucune réponse d'enregistrement MIP (RRP) n'est envoyée et le téléphone mobile peut continuer à lancer de nouvelles demandes d'enregistrement MIP (RRQ) parce qu'il n'a pas reçu de RRP MIP. Chaque nouveau RRQ MIP entraîne l'envoi par le PDSN d'une nouvelle demande d'authentification qui peut lui-même avoir sa propre série de nouvelles tentatives. Ceci peut être vu dans le champ Id en haut d'une trace de paquet - il est unique pour chaque jeu de nouvelles tentatives. En conséquence, les compteurs des appels envoyés, renouvelés et arrivés à expiration peuvent être beaucoup plus élevés que prévu pour le nombre d'appels reçus. Il existe une option qui peut être activée pour minimiser ces nouvelles tentatives, et elle peut être définie dans le service Agent étranger (FA) (mais pas dans le service Agent domestique (HA)) : “ authentication mn-aaa <6 choix ici> optimisation-retries ”

Autres compteurs utiles :

« Réponse de demande d'accès abandonnée » - se produit si l'appel ne parvient pas à se configurer en attendant les réponses aux demandes d'authentification.

« Access-Request Response Last Round Trip Time » : indique tout retard entre les points d'extrémité, bien qu'il ne soit pas indiqué où le retard pourrait être.

« Échecs consécutifs de demande d'accès dans un gestionnaire » se rapporte à ce qui a été discuté dans la première section sur les déclencheurs pour les déroutements AAA inaccessibles. Il représente le ou les aamgr avec le plus grand nombre de temporisations consécutives.

« Current Access/Accounting-Request Queued » indique les demandes qui ne reçoivent pas de réponse et restent dans la file d'attente (la comptabilité permet une accumulation indéfinie de la file d'attente alors que l'authentification ne le fait pas)

Le scénario le plus courant observé lorsque AAA Unreachable est signalé est que des délais d'attente d'accès et/ou des abandons de réponse se produisent également, alors que les réponses d'accès ne correspondent pas aux demandes.

Si l'accès au mode d'assistance technique privilégié est disponible, une enquête plus approfondie peut être effectuée au niveau de l'instance aamgr pour déterminer si une ou plusieurs aamgrs spécifiques sont à l'origine de l'augmentation du nombre global de « mauvais » comptes. Par exemple, recherchez les aamgrs qui se trouvent sur un PSC/DPC spécifique ayant un grand nombre ou peut-être un aamgr unique ou un aamgrs aléatoire ayant des problèmes - recherchez des modèles. Si la plupart ou l'ensemble des alarmes rencontrent des problèmes, il est plus probable que la cause première soit externe au châssis OU manifeste une grande échelle sur le châssis. Dans ce cas, il convient de procéder à des contrôles sanitaires généraux.

Voici un exemple de sortie montrant un problème avec un aamgr spécifique pour la comptabilité. (Le problème s'est avéré être un bogue dans un pare-feu entre l'ASR5K et le serveur RADIUS qui bloquait le trafic à partir d'une instance aamgr spécifique (114) port). Sur une période de trois semaines, seulement 48 réponses ont été reçues, mais plus de 100 000 délais d’attente ont été enregistrés (et cela ne comprend pas les retransmissions).

```
[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
```

En conclusion, déterminez quels compteurs incrémentent, pour quels serveurs et à quelle vitesse.

show session subsystem, installation {aamgr | sessmgr} {all | instance <instance #>

Bien qu'il soit hors de portée de cet article d'examiner tous les résultats superflus de cette commande, quelques exemples valent la peine d'être examinés. Comme pour tout autre dépannage, la comparaison des résultats entre les instances d'aamgr jugées bonnes et mauvaises révèle souvent des différences évidentes dans les valeurs signalées. Cela pourrait se refléter dans le nombre total de demandes, le taux d'échec/de réussite, l'authentification annulée, etc. Pour rappel, assurez-vous d'effacer le sous-système de session (une instance ne peut pas être effacée, elles doivent toutes être effacées) afin d'éliminer tout historique qui pourrait fournir une image nuageuse de l'état actuel.

En continuant avec le même problème mentionné précédemment en ce qui concerne un seul aamgr échouant pour la comptabilité, voici la sortie d'un noeud différent avec ce même problème, sauf une instance sessmr différente 36. Notez tous les champs intéressants pour l'aamgr défaillant et comment ces valeurs augmentent avec le temps avec les deux captures de la commande. Pendant ce temps, la sortie de l'instance 37 est présentée comme un exemple d'aaamgr de travail.

```
[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
...
```

Vous devez également exécuter show task resources pour vérifier les nombres de sessions inégales (colonne utilisée) parmi toutes les sessions. Si vous en trouvez, vérifiez les messages aamgrs associés pour les sessions avec cette commande pour voir s'il y a des champs qui ne sont pas en ligne - si le problème est dû à RADIUS, alors il y a une bonne chance de trouver quelque

chose.

Dans l'exemple show task resources dans une section précédente, il y avait un nombre de sessions nettement inférieur sur sessmgr 92 qui a été jumelé à aamgr 92. Le résultat du sous-système show session montre une augmentation significative du total des compteurs en attente max et aaa auth purged, et des compteurs en attente max en augmentation Current. Vous pouvez utiliser la fonction grep en direct sur le châssis et/ou le Bloc-notes++ ou tout autre puissant éditeur de recherche pour analyser rapidement les données. Exécutez la commande plusieurs fois pour voir quelles valeurs augmentent ou restent élevées :

```
[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

Une requête ping ICMP teste la connectivité de base pour voir si le serveur AAA peut être atteint ou non. La requête ping peut avoir besoin d'être source avec le mot clé src en fonction du réseau et doit être effectuée à partir du contexte AAA pour avoir une valeur. Si la requête ping envoyée au serveur échoue, essayez d'envoyer une requête ping aux éléments intermédiaires, y compris l'adresse du tronçon suivant dans le contexte, en confirmant qu'il y a une entrée ARP à l'adresse du tronçon suivant si la requête ping échoue. Traceroute peut également aider à résoudre les problèmes de routage.

```
[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
```

instance de test radius x auth {radius group <group> | tout | serveur <IP> port <port>} <nom d'utilisateur> <mot de passe>

radius test instance x accounting {radius group <nom du groupe> | tout | serveur <IP> port <port>}

Avec l'accès aux commandes Tech Support Test, on peut tester plus avant si un aamgr spécifique est capable d'atteindre n'importe quel serveur RADIUS. Pour un test de connectivité RADIUS de base, indépendant de toute instance aamgr spécifique, utilisez la version générique de cette commande qui ne spécifie aucun # d'instance spécifique mais utilise l'instance de gestion par défaut. Si cela échoue, il peut alors indiquer un problème plus large indépendamment d'instances spécifiques.

Cette commande envoie une requête d'authentification de base ou une requête **de début** et d'**arrêt** de comptabilité et attend une réponse. Pour l'authentification, utilisez n'importe quel nom d'utilisateur et mot de passe, auquel cas une réponse de rejet est attendue, confirmant que RADIUS fonctionne comme prévu ou qu'un nom d'utilisateur/mot de passe fonctionnel connu peut être utilisé, auquel cas une réponse d'acceptation doit être reçue

Voici un exemple de sortie du protocole de surveillance et de l'exécution de la version d'authentification de la commande sur un châssis de travaux pratiques :

```
[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
```

Voici un exemple tiré d'un châssis actif :

```
<<<<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
```

Voici un exemple de sortie provenant de l'exécution de la version comptable de la commande. Aucun mot de passe n'est nécessaire.

```
[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
```

Le résultat suivant est pour la même instance aamgr 36 qui vient d'être mentionnée où la connectivité à un serveur de comptabilité RADIUS spécifique est interrompue :

```
[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 <group name>] instance { X | tous}

Cette commande signale l'ID de flux NPU (Network Processor Unit) et le port UDP utilisés par l'adresse IP NAS configurée pour la connexion aux serveurs RADIUS. Ceci est signalé dans la section par défaut du groupe aaa du résultat. Il est certain que le numéro de port peut être utile si l'on a besoin de faire correspondre des paquets RADIUS dans une capture de paquets avec un numéro d'instance aamgr spécifique. (Notez que les flux NPU sont complexes et ne sont pas abordés dans cet article, mais une entité qu'un ingénieur d'assistance pourrait étudier plus avant.) Il effectue également le suivi des demandes en attente au serveur. Dans le même exemple de problème utilisé tout au long de cet article, seule une paire de ports IP/UDP NAS/serveur RADIUS spécifique a échoué comme souligné.

```
[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>
```

contrôler l'abonné

L'abonné de surveillance peut être utilisé pour déterminer si l'authentification est au moins tentée et si une réponse est traitée pour les appels surveillés. Activez l'option 'S' qui signifie Informations sur l'expéditeur de Sessmgr - en rapportant efficacement l'instance sessmgr ou aamgr # qui gère le message en question. Voici un exemple d'appel MIP sur une HA attachement aux instances 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
```

Il y a également un exemple d'échec à la fin de cet article.

Capture de paquets

Parfois, il n'y a pas assez d'informations sur l'ASR pour déterminer pourquoi des problèmes d'accessibilité surviennent, auquel cas une capture de paquets est nécessaire. Lors du dépannage de problèmes d'abonnés individuels, il devrait être facile d'identifier les paquets respectifs dans une trace. Sinon, connaître le port UDP utilisé à l'une ou l'autre extrémité d'une paire de serveurs RADIUS d'instance aamgr donnée **<==>** pourrait être utile si le problème est lié à des instances de ports/aamgr spécifiques. La tentative de capture à plusieurs endroits du réseau peut être nécessaire pour déterminer où les paquets sont abandonnés. Dans le problème analysé tout au long de cet article, c'est une capture de paquets au bon endroit dans le chemin de transport entre l'ASR et le serveur RADIUS qui a été le point de rupture dans la résolution du problème.

Corrections

Cette dernière section présente quelques idées pour résoudre les problèmes de connectivité RADIUS. Elles ne sont présentées dans aucun ordre particulier, mais simplement dans une liste à prendre en compte dans le processus de dépannage.

Si le serveur RADIUS est surchargé, la charge peut être réduite via la valeur (256 par défaut) configurée pour “ rayon (comptabilité) max-en ”, qui définit une limite sur le nombre de demandes en attente (sans réponse) pour un processus aamgr donné. Si la limite est atteinte, les journaux peuvent indiquer ceci : “ n'a pas pu attribuer l'ID de message pour la ” du serveur d'authentification RADIUS x.x.x.x:1812.

Les messages RADIUS de limitation de débit vers des serveurs spécifiques peuvent également contribuer à réduire la charge via le mot clé rate-limit pour les lignes de configuration de serveur respectives.

Parfois, il ne s'agit pas d'un problème de connectivité, mais d'un trafic de comptabilité accru, ce qui n'est pas un problème avec le persévérance RADIUS, mais de pointer vers un autre domaine, comme l'augmentation des renégociations ppp qui provoquent plus de mises en route et d'arrêts de comptabilité. Il peut donc être nécessaire de dépanner en dehors de RADIUS pour trouver une cause ou un déclencheur pour les symptômes observés.

Si, au cours de la procédure de dépannage, il a été décidé de supprimer un serveur d'authentification ou de comptabilité radius de la liste des serveurs actifs pour une raison quelconque, il existe une commande (non-config) qui met un serveur hors service indéfiniment jusqu'à ce qu'il soit nécessaire de le remettre en service. Il s'agit d'une approche plus propre que d'avoir à la supprimer manuellement de la configuration :

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

Une migration PSC ou DPC ou un basculement de carte de ligne peut souvent résoudre des problèmes en raison du fait que la migration entraîne le redémarrage des processus sur la carte, y compris le npumgr qui a été la cause de problèmes de temps à autre en ce qui concerne les flux NPU.

Mais dans un tournant intéressant avec l'exemple mentionné ci-dessus d'aamgr 92, les échecs AAA Unreachable ont en fait COMMENCÉ quand une migration PSC a été effectuée. Cela a été déclenché en raison de l'absence d'un flux NPU lorsqu'une migration de PSC a été effectuée, ce qui a rendu PSC 11 en veille. Quand il a été rendu actif une heure plus tard, l'impact réel du flux manquant a commencé pour aamgr 92. Des problèmes comme celui-ci sont très difficiles à résoudre sans l'assistance du support technique.

```
[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
```

Le problème a été temporairement résolu avec un basculement de port qui a fait que la carte PSC qui avait un flux NPU manquant pour aamgr 92 n'était plus connectée à une carte de ligne active.

```
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
```

Dernier déroutement :

```
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
```

De même, le redémarrage d'aamgrs spécifiques qui sont bloqués peut également résoudre des problèmes, même si c'est une activité que le support technique doit effectuer car elle implique des commandes d'assistance technique limitées. Dans l'exemple aamgr 92 présenté précédemment dans la section show task resources, ceci a été tenté mais n'a pas aidé parce que la cause principale n'était pas aamgr 92 mais plutôt le flux NPU manquant dont aamgr 92 avait besoin (il s'agissait d'un problème NPU, pas un problème aamgr). Voici le résultat pertinent de la tentative. « show task table » est exécuté afin d'afficher l'association de l'ID de processus et de l'instance de tâche 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
```

Exemple final

Voici un dernier exemple d'une panne réelle d'un réseau en direct qui rassemble de nombreuses commandes et approches de dépannage abordées dans cet article. Notez que ce noeud gère les protocoles 3G MIP et 4G Long Term Evolution (LTE) et les types d'appel High Rate Packet Data (eHRPD) évolués.

show snmp trap history

Rien que par les pièges, il peut être confirmé que le point de départ correspond à ce que le client a signalé comme 19:25 UTC. De plus, notez que AAAAuthSvrUnreachable traps pour le serveur principal 209.165.201.3 n'a commencé à se produire que quelques heures plus tard (pas clair pourquoi, mais bon à noter ; mais **la comptabilité inaccessible** à ce serveur a démarré immédiatement)

```
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
```

show task resources

Le résultat montre un nombre d'appels beaucoup plus faible sur DPC 8/1. Sur la base de cette seule analyse, sans autre analyse, on pourrait suggérer qu'il y a un problème sur DPC 8 et proposer l'option de migrer vers le DPC de secours. Mais il est important de reconnaître l'impact réel de l'abonné : dans ces scénarios, généralement, les abonnés se connectent correctement lors d'une tentative ultérieure et par conséquent l'impact n'est pas trop important pour l'abonné et il est probable qu'ils ne signalent rien au fournisseur, en supposant qu'il n'y a pas de panne de plan utilisateur également en cours (ce qui est possible selon ce qui est cassé).

```
 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
```

contrôler l'abonné

Une configuration d'appel a été interceptée alors qu'il n'y avait pas de réponse à la demande d'authentification au serveur principal 209.165.201.3 pour sessmgr 242 sur DPC 9/1, qui se trouve que son aamgr apparié réside sur DPC 8/1, confirmant les échecs 3G dus à AAA inaccessible le 8/1. Il confirme également que même s'il n'y avait pas eu de pièges AAAAuthSrvUnreachable pour 209.165.201.3 jusqu'à ce moment, cela ne signifie pas qu'il n'y a pas de problème pour le traitement des réponses pour ce serveur (comme indiqué ci-dessus, les pièges commencent mais quelques heures plus tard).

```
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

Ce qui est intéressant, c'est que le nombre de sessions pour sessmgr 242 est similaire à d'autres sessions de travail. Une enquête plus approfondie a montré que les appels 4G, également hébergés sur ce châssis, étaient en mesure de se connecter et ils ont donc compensé l'absence d'appels IP 3G mobiles pouvant se connecter. Il est possible de déterminer que jusqu'à 8 heures après le début de la panne, il n'y a pas d'appels MIP pour ce sessmgr 242, tout en remontant 9 heures avant le début de la panne, il y a des appels connectés :

```
[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
```

Les appels LTE et eHRPD affichent un ratio plus élevé par rapport aux appels MIP lors de la comparaison des sessions connectées aux messages de travail et rompus :

```
[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
```

serveur d'authentification RADIUS Test Instance X

Toutes les aamgrs sur 8/1 sont inactives - aucune commande d'instance de test radius ne fonctionne pour ces aamgrs mais fonctionne pour les aamgrs sur 8/0 et d'autres cartes :

```
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
```

show radius counters all

La commande phare de dépannage RADIUS affiche de nombreux délais d'attente qui augmentent rapidement :

```
[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
```

Correction

Pendant les fenêtres de maintenance, une migration DPC de 8 à 10 a résolu le problème, les pièges AAAAuthSrvUnreachable se sont arrêtés et DPC 8 était RMA et la cause première a été déterminée comme une défaillance matérielle sur DPC 8 (les détails de cette défaillance ne sont pas importants à connaître aux fins de cet article).

```
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
```