Comprenez et dépannez le CoA de RAYON et déconnectez les messages

Contenu

Introduction

Ce document décrit des messages de déconnexion RADIUS (SGD).

Définition des messages CoA de RAYON

Une modification de message de l'autorisation (CoA) est utilisée afin de changer des attributs et les filtres de données associés avec une session d'utilisateur. Les messages CoA d'assistances techniques du serveur d'Authentification, autorisation et comptabilité (AAA) pour changer des filtres de données ont associé avec une session d'abonné.

> Remarque: Les filtres dans des attributs de filtre-id (si actuel dans la demande) devraient être configurés dans l'ASR 5000 pour application au trafic d'utilisateur. C'est la forme du Listes de contrôle d'accès (ACL) et est configurée dans l'ASR 5000 avec des commandes d'**ip access-list**.

Le message de demande CoA devrait contenir des attributs pour identifier la session d'utilisateur ; des attributs et les filtres de données doivent être appliqués à la session d'utilisateur. L'attribut de filtre-id (id 11 d'attribut) contient les noms des filtres. Si l'ASR 5000 exécute avec succès la

demande CoA, un CoA ACK est renvoyé au serveur de RAYON et les nouveaux filtres d'attributs et de données sont appliqués à la session d'utilisateur. Autrement, un NAK CoA est envoyé avec la raison appropriée comme attribut de code d'erreur sans n'apporter aucune modification à la session d'utilisateur.

RAYON DM

Le message DM est utilisé afin de démonter des sessions d'utilisateur dans l'ASR 5000 d'un serveur de RAYON. Le message de demande DM devrait contenir des attributs nécessaires afin d'identifier la session d'utilisateur. Si le système déconnecte avec succès la session d'utilisateur, DM ACK est renvoyé au serveur de RAYON. Autrement, DM-NAK est envoyé avec des raisons appropriées d'erreur.

Comme mentionné précédemment, il est possible que le NAS ne puisse pas honorer des messages de Débranchement-demande ou de CoA-demande pour quelque raison. L'attribut de cause d'erreur fournit plus de détail sur la cause du problème. Il PEUT être inclus dans le disconnect-ack, les messages Débranchement-NAK, et CoA-NAK.

Le champ de valeur est quatre octets, qui contient un entier qui spécifie la cause de l'erreur.

- Les valeurs 0-199 et 300-399 sont réservées.
- Les valeurs 200-299 représentent la réussite, de sorte que ces valeurs pourraient seulement être envoyées dans le disconnect-ack ou le message CoA-ACK et NE DOIVENT PAS être envoyées dans un Débranchement-NAK ou le CoA-NAK.
- Les valeurs 400-499 représentent des erreurs fatales commises par le serveur de RAYON, de sorte qu'elles PUISSENT être envoyées dans les messages CoA-NAK ou Débranchement-NAK et NE DOIVENT PAS être envoyées dans des messages CoA-ACK ou de disconnect-ack.
- Les valeurs 500-599 représentent les erreurs fatales qui se produisent sur NAS ou proxy RADIUS, de sorte qu'elles PUISSENT être envoyées dans les messages CoA-NAK et Débranchement-NAK, et NE DOIVENT PAS être envoyées dans des messages CoA-ACK ou de disconnect-ack. Les valeurs de cause d'erreur êtes enregistré par le serveur de RAYON.

Les éléments de code (exprimés en décimale) incluent :

```
 #     Value
---  -----
201   Residual Session Context Removed>
202   Invalid EAP Packet (Ignored)
401   Unsupported Attribute
402   Missing Attribute
403   NAS Identification Mismatch
404   Invalid Request
405   Unsupported Service
406   Unsupported Extension
501   Administratively Prohibited
502   Request Not Routable (Proxy)
503   Session Context Not Found
504   Session Context Not Removable
505   Other Proxy Processing Error
506   Resources Unavailable
507   Request Initiated
```

Attributs pour l'identification de session

Pour l'identification de l'ASR 5000, une de ces méthodes peut être utilisée :

- Nas-IP-adresse : L'adresse IP de NAS si actuel dans la demande COA/DM devrait s'assortir avec l'adresse IP de NAS ASR 5000.
- Nas-identifiant : Si cet attribut est présent, sa valeur devrait s'assortir au nas-identifiant généré pour la session d'utilisateur.
  C'est un attribut obligatoire pour l'identification de session, si l'ASR 5000 est configuré avec le Nas-identifiant.

Pour l'identification de la session d'utilisateur, l'un ou l'autre une de ces méthodes est utilisé :

- ACCT-SESSION-ID : Si cet attribut est présent, sa valeur devrait s'assortir au l'acct-session-id pour la session d'utilisateur.
- Encadrer-IP-adresse : Si cet attribut est présent, ses valeurs devraient s'assortir à l'adresse IP encadrée de la session.
- Nom d'utilisateur : Si cet attribut est présent, ses valeurs devraient s'assortir au nom d'utilisateur de la session.
- Calling-station-id : C'est l'identité d'abonné mobile internationale (IMSI) de l'utilisateur.

Configuration de SGD de RAYON

La configuration d'un RAYON DM est tout à fait facile. Toutes les lignes doit être configurées dans le contexte de destination (celui avec la configuration RADIUS).

valeur **principale d'***ip_address modification-autoriser-nas*-**IP de rayon [chiffrés] [***port de* **port] [***fenêtre d'eventtimestamp*-**fenêtre] [NO--nas-identification-contrôle]**
[NO--inverse-chemin-en avant-contrôle] [*in_label_value d'***entrée de mpls label | sortie** *out_label_value1*
[*out_label_value2***]**

> Remarque: Le « modification-autoriser-nas-IP de rayon » devrait être l'adresse locale d'interface de l'AAA de votre contexte. Cette commande CLI est parfois une source de confusion.

Exemple de configuration

```
radius change-authorize-nas-ip 192.168.88.40 encrypted key <key value>
no-reverse-path-forward-check
no-nas-identification-check
```

Exemples de scénario de panne

Message DM n'a pas reçu du côté ASR 5000

Il est possible que le socket ne soit pas prêt pour le port UDP 3799. (Selon le RFC 3756, le paquet de Débranchement-demande de RAYON est envoyés au port UDP 3799).

Ce comportement peut être simplifié. Le processus qui traite toutes les demandes CoA est l'exemple 385 d'aaamgr, qui est celui sur la carte active SMC/MIO. Cette commande CLI doit être exécutée dans le contexte de destination.

```
#cli test-commands password <xx> #show radius info radius group all instance 385
```

Une telle sortie ressemble à :

```
# show radius info radius group all instance 385 AAAMGR instance 385:
cb-list-en: 3 AAA Group: <>
-----------------------------------------
socket number: 19
socket state: ready
local ip address: 10.176.81.215
local udp port: 50954
flow id: 0
use med interface: no
VRF context ID: 66
```

Dans cet exemple, il n'y a aucun port 3799 et c'est la raison pour le comportement signalé. Si vous voyez la même chose dans votre cas, la solution est de retirer et re-ajouter la configuration CoA afin de recréer le socket de écoute. Supplémentaire, vous pouvez essayer de détruire l'exemple 385 d'aaamgr si la première solution n'aide pas.

Après les actions décrites, vous devriez voir cette sortie :

```
# show radius info radius group all instance 385 AAAMGR instance 385:
cb-list-en: 3 AAA Group: <>
----------------------------------------->
socket number: 19>
socket state: ready
local ip address: 10.176.81.215
local udp port: 50954
flow id: 0
use med interface: no
VRF context ID: 66
socket number: 21   <--------------------
socket state: ready
local ip address: 10.176.81.215
local udp port: 3799 <--------------------
flow id: 0
use med interface: no
```

et le socket devrait être visible du shell de débogage sur le context/VR approprié :

```
bash-2.05b# netstat -lun | grep 3799
udp 0 0 10.176.81.215:3799 0.0.0.0:*
```

Le port UDP 3379 a le socket prêt sans des messages DM

Le port UDP 3379 a le socket prêt, toutefois vous ne voyez toujours pas les messages DM. Ceci est probablement provoqué par une configuration incorrecte de modification-autoriser-nas-IP de rayon. L'un ou l'autre les valeurs d'attribut qui ont été livré dans le message de demande DM n'apparient pas ceux qui ont été introduits une demande de comptabilité vers le RAYON.

Demande de comptabilité

```
Thursday August 06 2015
<<<<OUTBOUND
Code: 4 (Accounting-Request)
     Attribute Type: 44 (Acct-Session-Id)
               Length: 18
               Value: 42 43 37 31 44 46 32 36 BC71DF26
                      30 36 30 33 41 32 42 46 0603A2BF
     Attribute Type: 31 (Calling-Station-Id)
               Length: 14
               Value: 39 39 38 39 33 31 37 32 99893172
                      30 39 31 31             0911
     Attribute Type: 4 (NAS-IP-Address)
               Length: 6
               Value: C0 A8 58 E1             ..X.
                      (192.168.88.225)
     Attribute Type: 8 (Framed-IP-Address)
               Length: 6
               Value: 0A 55 12 21             .U.!
                      (10.85.18.33)
```

Débranchement-demande

```
Radius Protocol
   Code: Disconnect-Request (40)
   Packet identifier: 0x2 (2)
   Length: 71
   Authenticator: 4930a228f13da294550239f5187b08b9

   Attribute Value Pairs
       AVP: l=6 t=NAS-IP-Address(4): 192.168.88.225
           NAS-IP-Address: 192.168.88.225 (192.168.88.225)

       AVP: l=6 t=Framed-IP-Address(8): 10.85.18.33
           Framed-IP-Address: 10.85.18.33 (10.85.18.33)

       AVP: l=14 t=Calling-Station-Id(31): 998931720911
           Calling-Station-Id: 998931720911

       AVP: l=18 t=Acct-Session-Id(44): BC71DF260603A2BF
           Acct-Session-Id: BC71DF260603A200
```

Dans cet exemple, la valeur du l'Acct-Session-id qui est livré à l'ASR 5000 est différent que celui envoyé vers le RAYON et ceci est la raison pour la question. Ce problème peut être réparé par les modifications appropriées du côté de RAYON.

L'Acct-Session-id pour la session active peut être vérifié avec le **<> actif d'imsi d'AAA-configuration réservée ggsn d'abonnés d'exposition de** commande.

```
[local]# show subscribers ggsn-only aaa-configuration active imsi 434051801170727

Username: 998931720911@mihc1             Status: Online/Active
 Access Type: ggsn-pdp-type-ipv4        Network Type: IP
 Access Tech: WCDMA UTRAN               Access Network Peer ID: n/a
 callid: 057638b8                       imsi: 434051801170727
 3GPP2 Carrier ID: n/a
 3GPP2 ESN: n/a
 RADIUS Auth Server: 192.168.88.40  RADIUS Acct Server: n/a
 NAS IP Address: 192.168.88.225
 Acct-session-id: BC71DF260603A2BF
```

Tous les attributs s'assortissent, mais l'ASR 5000 envoie le NAK DM avec le

message d'erreur : 401 - Attribut non vérifié

En ce moment on le sait que ce genre de message d'erreur signifie que la question provient le serveur de RAYON. Cependant, il n'est toujours pas clair ce qui est erroné. Ici, la limite de l'ASR 5000 ne prend en charge pas l'Appeler-station-id dans le rayon DM. Par conséquent, si on le voit là, il répond avec l'erreur mise en valeur.

```
INBOUND>>>>>
RADIUS COA Rx PDU, from 192.168.1.254:38073 to 192.168.1.2:1800
Code: 40 (Disconnect-Request)
Id: 106
Length: 61
Authenticator: 8D F1 50 2E DD 79 49 39 79 A0 B5 FC 59 3E C4 51
    Attribute Type: 32 (NAS-Identifier)
              Length: 9
              Value: 73 74 61 72 65 6E 74   starent
    Attribute Type: 1 (User-Name)
              Length: 10
              Value: 74 65 73 74 75 73 65 72 testuser
    Attribute Type: 30 (Called-Station-ID)
              Length: 9
              Value: 65 63 73 2D 61 70 6E   ecs-apn
    Attribute Type: 31 (Calling-Station-Id)
              Length: 13
              Value: 36 34 32 31 31 32 33 34 64211234
                     35 36 37               567

<<<<OUTBOUND 06:57:42:683 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:38073
Code: 42 (Disconnect-Nak)
Id: 106
Length: 26
Authenticator: 34 2E DE B4 77 22 4A FE A5 16 93 91 0D B2 E6 3B
    Attribute Type: 101 (Error-Cause)
              Length: 6
              Value: 00 00 01 91             ....
                     (Unsupported-Attribute)
```

Le système a configuré « NO--nas-identification-contrôle » dans la ligne « modification-autoriser-nas-IP de rayon », erreur de « Nas-Identification-non-concordance » toujours retournée

Ceci se produit dans cette configuration :

```
radius change-authorize-nas-ip 192.168.1.2 encrypted key
+A27wvxlgy06ia30pcqswmdajxd11ckg4ns88i6l92dghsqw7v77f1 port 1800
event-timestamp-window 0 no-reverse-path-forward-check no-nas-identification-check
   aaa group default
   radius attribute nas-ip-address address 192.168.1.2
   radius server 192.168.1.128 encrypted key
+A3ec01d8zs92ed1gz2mytddjjrf11af3u0watpyr3gd0rs8mthlzc port 1812
   radius accounting server 192.168.1.128 encrypted key
+A24x0pj4mjgnqh0sclbnen1lm6f1d6drn2nw3yf31tmfldk9fr38e         port 1813
#exit
```

Pour un contexte actif PDP, la demande de débranchement est nue :

```
INBOUND>>>>>  04:27:13:898 Eventid:70901(6)
RADIUS COA Rx PDU, from 192.168.1.254:42082 to 192.168.1.2:1800 (52) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
```

```
 Id: 115
 Length: 52
 Authenticator: BF 95 05 0B 87 B4 42 59 5F C6 CC 78 D7 17 77 7F
     Attribute Type: 32 (NAS-Identifier)
               Length: 9
               Value: 73 74 61 72 65 6E 74    starent
     Attribute Type: 1 (User-Name)
               Length: 10
               Value: 74 65 73 74 75 73 65 72 testuser
     Attribute Type: 31 (Calling-Station-Id)
                          Value: 36 34 32 31 31 32 33 34 64211234;     Length: 13

                        35 36 37               567

Monday October 19 2015
<<<<OUTBOUND  04:27:13:898 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:42082 (26) PDU-dict=starent-vsa1
 Code: 42 (Disconnect-Nak)
 Id: 115
 Length: 26
 Authenticator: 75 D1 04 3E 31 19 9C 92 B2 2E 5D 5F 98 B9 34 99
     Attribute Type: 101 (Error-Cause)
               Length: 6
               Value: 00 00 01 93             ....
                      (NAS-Identification-Mismatch)
```

Cependant, quand cette ligne est incluse dans le groupe par défaut d'AAA :

```
    radius attribute nas-identifier starent
```

il commence à fonctionner :

```
Monday October 19 2015
INBOUND>>>>>  05:19:01:798 Eventid:70901(6)
RADIUS COA Rx PDU, from 192.168.1.254:55426 to 192.168.1.2:1800 (52) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
 Id: 171
 Length: 52
 Authenticator: 3A 67 43 25 DC 18 5C E3 23 08 04 C0 9C 31 68 68
     NAS-Identifier = starent
     User-Name = testuser
     Calling-Station-Id = 64211234567


Monday October 19 2015
<<<<OUTBOUND  05:19:01:799 Eventid:70902(6)
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:55426 (26) PDU-dict=starent-vsa1
 Code: 41 (Disconnect-Ack)
 Id: 171
 Length: 26
 Authenticator: 45 07 79 C5 E0 92 53 28 8F AD A3 E3 C4 B4 52 10
     Acct-Termination-Cause = Admin_Reset
```

Ou cela fonctionnera également sans configuration du nas-identifiant sur le groupe d'AAA, mais avec le Nas-identifiant AVP retiré de la Débranchement-demande :

```
INBOUND>>>>>  05:14:41:374 Eventid:70901(6)
RADIUS COA Rx PDU, from 192.168.1.254:54757 to 192.168.1.2:1800 (43) PDU-dict=starent-vsa1
 Code: 40 (Disconnect-Request)
 Id: 78
 Length: 43
 Authenticator: 84 5D FE 5E 90 0D C8 16 84 7A 11 67 FF 82 40 DB
     User-Name = testuser
     Calling-Station-Id = 64211234567
```

```
Monday October 19 2015
<<<<OUTBOUND  05:14:41:375 Eventid:70902(6
RADIUS COA Tx PDU, from 192.168.1.2:1800 to 192.168.1.254:54757 (26) PDU-dict=starent-vsa1
 Code: 41 (Disconnect-Ack)
 Id: 78
 Length: 26
 Authenticator: 34 84 5B 8E AF 02 1C F2 58 26 1B 0C 20 37 93 33
     Acct-Termination-Cause = Admin_Reset
```

L'ID de bogue Cisco CSCuw78786 a été soumis. Ceci a été testé sur la version 17.2.0 et la version 15.