Test de fonctionnement du serveur Radius



Organisme : Centre Hospitalier Henri Laborit Adresse : 370 Av. Jacques Cœur, 86021 Poitiers

Direction : Service Informatique Auteur : LOUINEAU Noah

Durée : 6 semaines

1. Présentation de la mission

J'ai précédemment installé un nouveau serveur FreeRadius en développement pour remplacer le serveur FreeRadius actuel en production.

Cependant maintenant il faut vérifier que les résultats de test correspondent au résultat attendu pour ce serveur.

Résultat attendu

Les résultats attendus du fonctionnement du serveur FreeRADIUS sont les suivants :

- En mode filaire : les postes obtiennent une adresse IP et un VLAN s'ils sont authentifiés.
- En mode liaison sans fil : les postes obtiennent une adresse IP et un VLAN s'ils sont authentifiés.

3. Résultat mesuré

Avec le serveur freeRadius exécuter en mode debug grâce à la commande :

./radiusd -X

Le mode débogage nous permet de visualiser en temps réel les journaux du serveur, les appareils qui s'y connectent, ainsi que les erreurs rencontrées...

1er test : Réalisé en filaire.

Image en annexe 1

Nous avons observé qu'aucun VLAN n'était attribué aux clients en raison d'une erreur survenue lors de la vérification de la table Radgroupcheck du serveur RADIUS.

Après avoir examiné la table, nous avons remarqué que le switch de test n'était pas inclus dans le hunt group. Par conséquent, aucun groupe n'était attribué au switch de test, ce qui signifie que lorsqu'un client se connectait via ce switch, il ne pouvait pas être vérifié par Radgroupcheck et aucun VLAN ne lui était attribué.

2ème test : Après correction du test 1 en filaire

Le poste obtient désormais un VLAN et une adresse IP après s'être authentifier Nous obtenons le message sent access accept.

<u>Image en annexe 2</u>

3ème test : Réalisé avec une borne wifi

La solution et la compréhension de ce test n'ont pas été réalisées par moi, j'ai donc seulement pris connaissance du message d'erreur et de sa résolution.

Le test réalisé non indiqué que l'authentification via Idap échoue à cause de l'utilisation du mauvais mot de passe. Le problème a été réglé en changeant le mot passe utilisé pour l'authentification Idap.

4ème test : Réalisé avec une borne wifi correction du test 3

Les postes en wifi obtiennent désormais un VLAN et une adresse IP après s'être authentifier

4. Mise en production

L'administrateur système et réseau s'est occupé de mettre en production le nouveau serveur FreeRadius. Puis nous avons vérifié la continuité du service en effectuant les mêmes tests réalisés en développement.

5. Conclusion

Les erreurs rencontrées lors du test de fonctionnement étaient simplement des erreurs liées à l'environnement et aux mots de passe. Le serveur FreeRadius a désormais été mis à niveau et est fonctionnel.

□ Projet-numéro-2-Radius

Annexe n°1

```
eady to process requests
         Received Access-Request Id 229 from 172.19.5.250:52866 to 172.27.10.128:1812 length 345
User-Name = "6c4b9085701a"
            Wiser-Name = "6c4b9085701a"

NAS-Identifier = "sw-site0"

Framed-Protocol = PPP

Called-Station-Id = "BC-EA-FA-92-DC-3F"

H3C-Ip-Host-Addr = "0.0.0.0 6c:4b:90:85:70:1a"

Calling-Station-Id = "6C-4B-90-85-70-1A"
 (0)
(0)
(0)
             Calling-Station-Id = "6C-4B-90-85-70-1A"

NAS-Port-Type = Ethernet

H3C-NAS-Port-Name = "GigabitEthernet1/0/16"

NAS-Port = 16846752

NAS-Port-Id = "slot=1;subslot=0;port=16;vlanid=4000"

H3C-Av-Pair = "nas:ifindex=16"

Acct-Session-Id = "00000004202402141502170000000308100192"

User-Password = "6C4490085701a"

Service-Type = Call-Check

NAS-TP-Address = 172.19.5.250
 NAS-IP-Address = 172.19.5.250

H3C-Product-ID = "HPE 5130 24G POE+ 4SFP+ EI Switch"

H3C-NAS-Startup-Timestamp = 1356998391

# Executing section authorize from file /opt/freeradius/etc/raddb/sites-enabled/port-1812-filaire authorize {
                (0) SQL query returned no results
rlm_sql (sql): Released connection (1)
(0) EXPAND %{sql:select groupname from radhuntgroup where nasipaddress="%{NAS-IP-Address}"}
 (0)
(0)
(0)
                       Huntgroup-Name :=
        Huntgroup-Name :=
} # update request = noop
eap-pro-filaire: No EAP-Message, not doing EAP
[eap-pro-filaire] = noop
if (Service-Type == Call-Check) {
if (Service-Type == Call-Check) -> TRUE
if (Service-Type == Call-Check) {
if (!Calling-Station-Id) {
if (!Calling-Station-Id) -> FALSE
undate request {
 (0)
(0)
(0)
(0)
(0)
(0)
(0)
(0)
(0)
                       update request {
   EXPAND %{tolower:%{User-Name}}
   --> 6c4b9085701a
   User-Name := 6c4b9085701a
   EXPAND %{tolower:%{User-Password}}
```

Annexe n°2

```
Ready to process requests
(0) Received Access-Requests Id 229 from 172.19.5.250:52866 to 172.27.10.128:1812 length 345
(0) User-Name = "6c4b9085701a"
(0) NAS-Identifier = "sw-site0"
(0) Framed-Protocol = PPP
              Called-Station-Id = "BC-EA-FA-92-DC-3F"
H3C-Ip-Host-Addr = "0.0.0.0 6c:4b:90:85:70:1a"
Calling-Station-Id = "6C-4B-90-85-70-1A"
(0)
(0)
(0)
(0)
(0)
(0)
               NAS-Port-Type = Ethernet
H3C-NAS-Port-Name = "GigabitEthernet1/0/16"
              NAS-Port = 16846752

NAS-Port-Id = "slot=1;subslot=0;port=16;vlanid=4000"

H3C-Av-Pair = "nas:ifindex=16"
(e)
               Acct-Session-Id = "00000004202402141502170000000308100192"
User-Password = "6c4b9085701a"
 (θ)
(0)
        | Service-Type = Call-Check
| NAS-IP-Address = 172.19.5.250
| H3C-Product-ID = "HPE 5130 24G PoE+ 4SFP+ EI Switch"
| H3C-NAS-Startup-Timestamp = 1356998391
| # Executing section authorize from file /opt/freeradius/etc/raddb/sites-enabled/port-1812-filaire
(0)
(0)
(0)
(0)
authorize {
                    update request {
		CHL-Auth-Module := "1812-filaire"
                   CHL-Auth-Module := "1812-filaire"
} # update request = noop
if ( User-Name =~ /^host\/[^.]+\.(.+)/ ) {
if ( User-Name =~ /^host\/[^.]+\.(.+)/ ) -> FALSE
policy filter_username {
  if (&User-Name) {
  if (&User-Name) -> TRUE
  if (&User-Name) {
  if (&User-Name) {

                         if (&User-Name) {
   if (&User-Name =~ / /) {
      if (&User-Name =~ / /) -> FALSE
      if (&User-Name =~ /@[^@]*@/ ) {
      if (&User-Name =~ /@[^@]*@/ ) -> FALSE
      if (&User-Name =~ /\.\./ ) {
       if (&User-Name =~ /\.\./ ) -> FALSE
      if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) {
       if ((&User-Name =~ /@/) && (&User-Name !~ /@(.+)\.(.+)$/)) -:
      if (&User-Name =~ /\.$/) {
       if (&User-Name =~ /\.$/) -> FALSE
      if (&User-Name =~ /@\./) {
       if (&User-Name =~ /@\./) {
       if (&User-Name =~ /@\./) -> FALSE
      }
      # if (&User-Name) = noop
# policy filter_username = noop
                     } # policy filter_username = noop
 (ø)
                    update request {
rlm_sql (sql): Reserved connection (1)
rlm_sql (sql): Released connection (1)
rlm_sql (sql): Released connection (1)

rlm_sql (sql): Closing connection (2) - Too many unused connections.

rlm_sql_mysql: Socket destructor called, closing socket

rlm_sql (sql): Closing expired connection (4) - Hit idle_timeout limit

rlm_sql_mysql: Socket destructor called, closing socket

rlm_sql (sql): You probably need to lower "min"
rlm_sql (sql): Closing expired connection (3) - Hit idle_timeout limit rlm_sql_mysql: Socket destructor called, closing socket rlm_sql (sql): You probably need to lower "min" rlm_sql (sql): Closing expired connection (0) - Hit idle_timeout limit rlm_sql mysql; Socket destructor called closing socket
 rlm_sql_mysql: Socket destructor called, closing socket
(0) EXPAND %{User-Name}
(θ)
                                  --> 6c4b9085701a
 (0)
 (B)
(B)
                         EXPAND %{sql:select groupname from radhuntgroup where nasipaddress="%{NAS-IP-Address}"}
(0)
(0)
                         Huntgroup-Name :=
(e)
                     } # update request = noop
        # update request = noop
eap-pro-filaire: No EAP-Message, not doing EAP
[eap-pro-filaire] = noop
if (Service-Type == Call-Check) {
   if (Service-Type == Call-Check) -> TRUE
   if (Service-Type == Call-Check) {
      if (!Calling-Station-Id) {
      if (!Calling-Station-Id) -> FALSE
      update request {
(0)
(0)
(0)
(0)
(0)
(0)
(0)
(0)
(0)
                         update request {
   EXPAND %{tolower:%{User-Name}}
   --> 6c4b9085701a
                               User-Name := 6c4b9085701a
EXPAND %{tolower:%{User-Password}}
```

```
User-Password := 6c4b9085701a
     0) sql: EXPAND %[User-Name}
0) sql: --> 6c4b9085701a
0) sql: SQL-User-Name set to '6c4b9085701a'
1m_sql (sql): Reserved connection (1)
0) sql: EXPAND SELECT id, username, attribute, value, op FROM radcheck WHERE username = '%{SQL-User-Name}' ORDER BY id
0) sql: Executing select query: SELECT id, username, attribute, value, op FROM radcheck WHERE username = '6c4b9085701a' ORDER BY id
0) sql: Executing select query: SELECT id, username, attribute, value, op FROM radcheck WHERE username = '6c4b9085701a' ORDER BY id
0) sql: User found in radcheck table
0) sql: Conditional check items matched, merging assignment check items
0) sql: Cleartext-Password := "6c4b9085701a"
0) sql: EXPAND SELECT id, username, attribute, value, op FROM radreply WHERE username = '%{SQL-User-Name}' ORDER BY id
0) sql: EXPAND SELECT id, username, attribute, value, op FROM radreply WHERE username = '6c4b9085701a' ORDER BY id
0) sql: EXPAND SELECT goupname FROM radusergroup WHERE username = '%{SQL-User-Name}' ORDER BY id
0) sql: EXPAND SELECT groupname FROM radusergroup WHERE username = '%{SQL-User-Name}' ORDER BY priority
0) sql: EXPAND SELECT groupname FROM radusergroup WHERE username = '6c4b9085701a' ORDER BY priority
0) sql: Executing select query: SELECT groupname FROM radusergroup WHERE username = '6c4b9085701a' ORDER BY priority
0) sql: User found in the group table
0) sql: User found in the group table
0) sql: User Found in the group table
0) sql: EXPAND SELECT id, groupname, attribute, Value, op FROM radgroupcheck WHERE groupname = 'pcs-miletrie' ORDER BY id
0) sql: Executing select query: SELECT id, groupname, attribute, Value, op FROM radgroupcheck WHERE groupname = 'pcs-miletrie' ORDER BY id
0) sql: Executing select query: SELECT id, groupname, attribute, Value, op FROM radgroupcheck WHERE groupname = 'pcs-miletrie' ORDER BY id
0) sql: executing select query: SELECT id, groupname, attribute, Value, op FROM radgroupcheck WHERE groupname = 'pcs-miletrie' ORDER BY id
0) sql: executing select query: SELECT id, groupname, attribute, Valu
       0) [pap] = updated
0) } # authorize = updated
0) Found Auth-Type = PAP
    0) Found Auth-Type = PAP

0) # Executing group from file /opt/freeradius/etc/raddb/sites-enabled/port-1812-filaire

0) Auth-Type PAP {

0) pap: Login attempt with password

0) pap: Comparing with "known good" Cleartext-Password

0) pap: User authenticated successfully

0) [pap] = ok

0) } # Auth-Type PAP = ok

0) # Executing section post-auth from file /cot/freesadius/etc/coddb/sites-enable//
    b) } # Auth-!ype PAP = OK
b) # Executing section post-auth from file /opt/freeradius/etc/raddb/sites-enabled/port-1812-filaire
b) post-auth {
b) sql: EXPAND .query
b) sql: --> .query
b) sql: Using query template 'query'
lm_sql (sql): Reserved connection (1)
b) sql: EXPAND %{User-Name}
b) sql: EXPAND %{User-Name}
c) sql: --> .query
c) sql: --> .query
c) sql: --> .query
0) sql: EXPAND %{User-Name}
0) sql: CYPAND %{User-Name}
1) sql: SQL-User-Name set to '6c4b9085701a'
1) sql: SQL-User-Name set to '6c4b9085701a'
2) sql: EXPAND INSERT INTO radpostauth
2) sql: EXPAND INSERT INTO radpostauth
3) sql: EXPAND INSERT INTO radpostauth
4) sql: -> INSERT INTO radpostauth
5) sql: --> INSERT INTO radpostauth
6) sql: --> INSERT INTO radpostauth
6) sql: --> INSERT INTO radpostauth
7) sql: Executing query: 
                                                   policy remove_reply_message_if_eap {
  if (&reply:EAP-Message && &reply:Reply-Message) {
   if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE
                                                                   else {
                                                                   [noop] = noop
} # else = noop
                                    } # policy remove_reply_message_if_eap = noop
} # post-auth = ok
                        Sent Access-Accept Id 229 from 172.27.10.128:1812 to 172.19.5.250:52866 length 20
```