

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.

2. 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 authentifié
Nous obtenons le message sent access accept.

[Image en annexe 2](#)

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 ldap 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 ldap.

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

```
Listening on proxy address - port 32337
Ready to process requests
(0) Received Access-Request 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
(0) Called-Station-Id = "BC-EA-FA-92-DC-3F"
(0) H3C-IP-Host-Addr = "0.0.0.0 6c:4b:90:85:70:1a"
(0) Calling-Station-Id = "6C-4B-90-85-70-1A"
(0) NAS-Port-Type = Ethernet
(0) H3C-NAS-Port-Name = "GigabitEthernet1/0/16"
(0) NAS-Port = 16846752
(0) NAS-Port-Id = "slot=1;subslot=0;port=16;vlanid=4000"
(0) H3C-Av-Pair = "nas:ifindex=16"
(0) Acct-Session-Id = "00000004202402141502170000000308100192"
(0) User-Password = "6c4b9085701a"
(0) Service-Type = Call-Check
(0) NAS-IP-Address = 172.19.5.250
(0) H3C-Product-ID = "HPE 5130 24G PoE+ 4SFP+ EI Switch"
(0) H3C-NAS-Startup-Timestamp = 1356998391
(0) # Executing section authorize from file /opt/freeradius/etc/raddb/sites-enabled/port-1812-filaire
(0) authorize {
(0)   update request {
(0)     CHL-Auth-Module := "1812-filaire"
(0)   } # update request = noop
(0)   if ( User-Name =~ /^host\[^\.\+\]/ ) {
(0)     if ( User-Name =~ /^host\[^\.\+\]/ ) -> FALSE
(0)   } policy filter_username {
(0)     if (&User-Name) {
(0)       if (&User-Name) -> TRUE
(0)       if (&User-Name) {
(0)         if (&User-Name =~ / /) {
(0)           if (&User-Name =~ / /) -> FALSE
(0)           if (&User-Name =~ /@[^@]*@/ ) {
(0)             if (&User-Name =~ /@[^@]*@/ ) -> FALSE
(0)             if (&User-Name =~ /\.\/\./ ) {
(0)               if (&User-Name =~ /\.\/\./ ) -> FALSE
(0)               if ((&User-Name =~ /@/) && (&User-Name !~ /@(\.+)\.(\.+)$/)) {
(0)                 if ((&User-Name =~ /@/) && (&User-Name !~ /@(\.+)\.(\.+)$/)) -> FALSE
(0)                 if (&User-Name =~ /\.\/\./) {
(0)                   if (&User-Name =~ /\.\/\./) -> FALSE
(0)                   if (&User-Name =~ /@\.\/\./) {
(0)                     if (&User-Name =~ /@\.\/\./) -> FALSE
(0)                   } # if (&User-Name) = noop
(0)                 } # policy filter_username = noop
(0)               } update request {
rlm_sql (sql): Reserved 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
(0)   EXPAND %{User-Name}
(0)   --> 6c4b9085701a
(0)   SQL-User-Name set to '6c4b9085701a'
rlm_sql (sql): Reserved connection (1)
(0)   Executing select query: select groupname from radhuntgroup where nasipaddress="172.19.5.250"
(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)   Huntgroup-Name :=
(0) } # update request = noop
(0) eap-pro-filaire: No EAP-Message, not doing EAP
(0) [eap-pro-filaire] = noop
(0) if (Service-Type == Call-Check) {
(0)   if (Service-Type == Call-Check) -> TRUE
(0)   if (Service-Type == Call-Check) {
(0)     if (!Calling-Station-Id) {
(0)       if (!Calling-Station-Id) -> FALSE
(0)     } update request {
(0)       EXPAND %{tolower:%{User-Name}}
(0)       --> 6c4b9085701a
(0)       User-Name := 6c4b9085701a
(0)       EXPAND %{tolower:%{User-Password}}
```

Annexe n°2

```
Listening on proxy address port 32321
Ready to process requests
(0) Received Access-Request 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
(0) Called-Station-Id = "BC-EA-FA-92-DC-3F"
(0) H3C-Ip-Host-Addr = "0.0.0.0 6c4b9085701a"
(0) Calling-Station-Id = "6C-4B-90-85-70-1A"
(0) NAS-Port-Type = Ethernet
(0) H3C-NAS-Port-Name = "GigabitEthernet1/0/16"
(0) NAS-Port = 16846752
(0) NAS-Port-Id = "slot=1;subslot=0;port=16;vlanid=4000"
(0) H3C-Av-Pair = "nas:ifindex=16"
(0) Acct-Session-Id = "00000004202402141502170000000308100192"
(0) User-Password = "6c4b9085701a"
(0) Service-Type = Call-Check
(0) NAS-IP-Address = 172.19.5.250
(0) H3C-Product-ID = "HPE 5130 24G PoE+ 4SFP+ EI Switch"
(0) H3C-NAS-Startup-Timestamp = 1356998391
(0) # Executing section authorize from file /opt/freeradius/etc/raddb/sites-enabled/port-1812-filaire
(0) authorize {
(0)   update request {
(0)     CHL-Auth-Module := "1812-filaire"
(0)   } # update request = noop
(0)   if ( User-Name =~ /^host\[^\.\+\.\+\]/ ) {
(0)     if ( User-Name =~ /^host\[^\.\+\.\+\]/ ) -> FALSE
(0)   }
(0)   policy filter_username {
(0)     if (&User-Name) {
(0)       if (&User-Name) -> TRUE
(0)       if (&User-Name) {
(0)         if (&User-Name =~ / /) {
(0)           if (&User-Name =~ / /) -> FALSE
(0)           if (&User-Name =~ /@\[^\@\]*@/ ) {
(0)             if (&User-Name =~ /@\[^\@\]*@/ ) -> FALSE
(0)             if (&User-Name =~ /\.\/\./ ) {
(0)               if (&User-Name =~ /\.\/\./ ) -> FALSE
(0)               if ((&User-Name =~ /@/) && (&User-Name !~ /@(\.\+\.)(\.\+)$/)) {
(0)                 if ((&User-Name =~ /@/) && (&User-Name !~ /@(\.\+\.)(\.\+)$/)) -> FALSE
(0)                 if (&User-Name =~ /\.$/ ) {
(0)                   if (&User-Name =~ /\.$/ ) -> FALSE
(0)                   if (&User-Name =~ /@\./ ) {
(0)                     if (&User-Name =~ /@\./ ) -> FALSE
(0)                   } # if (&User-Name) = noop
(0)                 } # policy filter_username = noop
(0)               }
(0)             }
(0)           }
(0)         }
(0)       }
(0)     }
(0)   }
(0)   rln_sql (sql): Reserved connection (1)
(0)   rln_sql (sql): Released connection (1)
(0)   rln_sql (sql): Closing connection (2) - Too many unused connections.
(0)   rln_sql_mysql: Socket destructor called, closing socket
(0)   rln_sql (sql): Closing expired connection (4) - Hit idle_timeout limit
(0)   rln_sql_mysql: Socket destructor called, closing socket
(0)   rln_sql (sql): You probably need to lower "min"
(0)   rln_sql (sql): Closing expired connection (3) - Hit idle_timeout limit
(0)   rln_sql_mysql: Socket destructor called, closing socket
(0)   rln_sql (sql): You probably need to lower "min"
(0)   rln_sql (sql): Closing expired connection (0) - Hit idle_timeout limit
(0)   rln_sql_mysql: Socket destructor called, closing socket
(0)   EXPAND %{User-Name}
(0)   --> 6c4b9085701a
(0)   SQL-User-Name set to '6c4b9085701a'
(0)   rln_sql (sql): Reserved connection (1)
(0)   Executing select query: select groupname from radhuntgroup where nasipaddress="172.19.5.250"
(0)   SQL query returned no results
(0)   rln_sql (sql): Released connection (1)
(0)   EXPAND %{sql:select groupname from radhuntgroup where nasipaddress="%{NAS-IP-Address}"}
(0)   -->
(0)   Huntgroup-Name :=
(0) } # update request = noop
(0) eap-pro-filaire: No EAP-Message, not doing EAP
(0) [eap-pro-filaire] = noop
(0) if (Service-Type == Call-Check) {
(0) if (Service-Type == Call-Check) -> TRUE
(0) if (Service-Type == Call-Check) {
(0)   if (!Calling-Station-Id) {
(0)     if (!Calling-Station-Id) -> FALSE
(0)   }
(0)   update request {
(0)     EXPAND %{tolower:%{User-Name}}
(0)     --> 6c4b9085701a
(0)     User-Name := 6c4b9085701a
(0)     EXPAND %{tolower:%{User-Password}}
```

