FreeRADIUS ile Kimlik Denetimi

Gökhan AKIN, Hüseyin Yüce, ve Hüsnü DEMIR
gokhan.akin@itu.edu.tr, huseyin@marmara.edu.tr, hdemir@metu.edu.tr

Ag Kimlik Denetimi Çalisma Grubu

FreeRADIUS Kurulumu

Sunum dahilinde Fedora Core8 üzerine FreeRADIUS 2.0.3 kurulumu anlatilmaktadir.

Ayrica çalismanin dökümaninda FreeRADIUS1.0.7'nin kurulumunu da bulabilirsiniz.

FreeRADIUS Kurulumu

```
[root@localhost freeradius-server-2.0.3]# ./configure
checking for gcc... gcc
checking for C compiler default output file name... a.out
checking whether the C compiler works... yes
checking whether we are cross compiling... no
checking for suffix of executables...
checking for suffix of object files... o
checking whether we are using the GNU C compiler... yes
checking whether gcc accepts -g... yes
checking for gcc option to accept ISO C89... none needed
checking for g++... g++
checking whether we are using the GNU C++ compiler... _
```

./configure

make

make install

Kurulum Tamamlandi

```
/root/freeradius-server-2.0.3/libtool --finish /usr/local/lib
PATH="$PATH:/sbin" ldconfig -n /usr/local/lib
----------------------------------------------------------------------
Libraries have been installed in:
   /usr/local/lib

If you ever happen to want to link against installed libraries
in a given directory, LIBDIR, you must either use libtool, and
specify the full pathname of the library, or use the `-LLIBDIR'
flag during linking and do at least one of the following:
   - add LIBDIR to the `LD_LIBRARY_PATH' environment variable
     during execution
   - add LIBDIR to the `LD_RUN_PATH' environment variable
     during linking
   - use the `-Wl,--rpath -Wl,LIBDIR' linker flag
   - have your system administrator add LIBDIR to `/etc/ld.so.conf'

See any operating system documentation about shared libraries for
more information, such as the ld(1) and ld.so(8) manual pages.
----------------------------------------------------------------------
[root@localhost freeradius-server-2.0.3]#
[root@localhost freeradius-server-2.0.3]# cd /usr/local/etc/raddb
[root@localhost raddb]# pwd
/usr/local/etc/raddb
[root@localhost raddb]# _
```

Kuruldugu klasör: /usr/local/etc/raddb

Sertifika Klasörü

```
[root@localhost raddb]# cd certs/
[root@localhost certs]# ls
01.pem      ca.key       index.txt       random      server.cnf  server.p12
bootstrap   ca.pem       index.txt.attr  README      server.crt  server.pem
ca.cnf      client.cnf   index.txt.old   serial      server.csr  xpextensions
ca.der      dh           Makefile        serial.old  server.key
[root@localhost certs]# rm -f *.pem *.der *.csr *.crt *.key *.p12 serial* index.
txt*_
```

← *Test amaçli olusturulmus sertifikalar silinir.*

Sertifika klasörü: /usr/local/etc/raddb/certs

Kök Sertifikasi Ayar Dosyasi

Kök sertifikasi için gereken konfigürasyon dosyasina girilir.

Kök Sertifikasi Ayarlari

```
[ ca ]
default_ca              = CA_default

[ CA_default ]
dir                     = ./
certs                   = $dir
crl_dir                 = $dir/crl
database                = $dir/index.txt
new_certs_dir           = $dir
certificate             = $dir/ca.pem
serial                  = $dir/serial
crl                     = $dir/crl.pem
private_key             = $dir/ca.key
RANDFILE                = $dir/.rand
name_opt                = ca_default
cert_opt                = ca_default
default_days            = 365
default_crl_days        = 30
default_md              = md5
preserve                = no
policy                  = policy_match

[ policy_match ]
countryName             = match
```

← *Default Days ile Sertifika geçerlilik süresi degistirilebilir.*

Kök Sertifikanin 5-10 yil için geçerli olmasi önerilir.

Kurumunuz ile ilgili degerlerde degistirilmelidir. →

Burada Kök Sertifika 2048 bit olusturulmaktadir. Bu deger ihitiyaca bagli artirilabilir.

```
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
prompt                  = no
distinguished_name      = certificate_authority
default_bits            = 2048
input_password          = whatever
output_password         = whatever
x509_extensions         = v3_ca

[certificate_authority]
countryName             = FR
stateOrProvinceName     = Radius
localityName            = Somewhere
organizationName        = Example Inc.
emailAddress            = admin@example.com
commonName              = "Example Certificate Authority"

[v3_ca]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always,issuer:always
basicConstraints        = CA:true
```

Sunucu Sertifikasi Ayar Dosyasi

Sunucu sertifikasi için gereken konfigürasyon dosyasina girilir.

Sunucu Sertifikasi Ayarlari

```
[ ca ]
default_ca              = CA_default

[ CA_default ]
dir                     = ./
certs                   = $dir
crl_dir                 = $dir/crl
database                = $dir/index.txt
new_certs_dir           = $dir
certificate             = $dir/ca.pem
serial                  = $dir/serial
crl                     = $dir/crl.pem
private_key             = $dir/ca.key
RANDFILE                = $dir/.rand
name_opt                = ca_default
cert_opt                = ca_default
default_days            = 365
default_crl_days        = 30
default_md              = md5
preserve                = no
policy                  = policy_match

[ policy_match ]
countryName             = match
```

← *Default Days ile Sertifika geçerlilik süresi degistirilebilir.*

Sunucu sertifikanin köke göre daha kisa süreler için geçerli olmasi önerilir.

Yine kurumunuz ile ilgili degerler girilmelidir. →

Burada sunucu sertifikasida 2048 bit ile olusturulmaktadir. Bu deger ihitiyaca bagli artirilabilir.

```
organizationalUnitName  = optional
commonName              = supplied
emailAddress            = optional

[ req ]
prompt                  = no
distinguished_name      = certificate_authority
default_bits            = 2048
input_password          = whatever
output_password         = whatever
x509_extensions         = v3_ca

[certificate_authority]
countryName             = FR
stateOrProvinceName     = Radius
localityName            = Somewhere
organizationName        = Example Inc.
emailAddress            = admin@example.com
commonName              = "Example Certificate Authority"

[v3_ca]
subjectKeyIdentifier    = hash
authorityKeyIdentifier  = keyid:always,issuer:always
basicConstraints        = CA:true
```

Sertifikalarin Basimi

← ***Video***

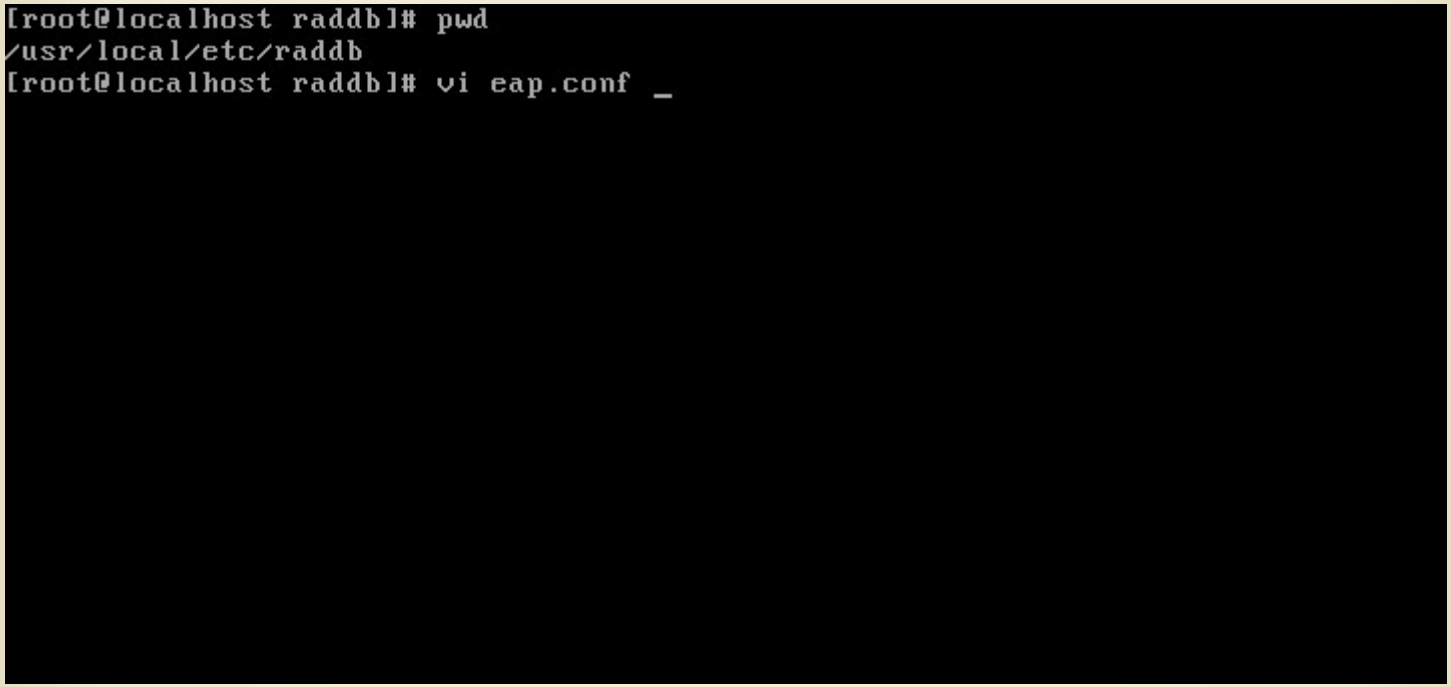
./bootstrap komudu ile sertifikalar basilir.

Kök Sertifikasinin Der Formatina Çevirimi

```
[root@localhost certs]# make ca.der
openssl x509 -inform PEM -outform DER -in ca.pem -out ca.der
[root@localhost certs]# _
```

make ca.der *komudu ile basilmis olan kök sertifikasini Windows istemcilerin daha kolay kurulum yapmalarini saglayacak der formatina cevirilir.*

“eap.conf” Ayar Dosyasi



Sunucu Sertifikasinin anahtar kelimesini degistirmek için eap.conf konfigürasyon dosyasina girilir.

“eap.conf” Dosyasindaki Degisiklikler (1)

```
#
#  EAP types NOT listed here may be supported via the "eap2" module.
#  See experimental.conf for documentation.
#
        eap {
                #  Invoke the default supported EAP type when
                #  EAP-Identity response is received.
                #
                #  The incoming EAP messages DO NOT specify which EAP
                #  type they will be using, so it MUST be set here.
                #
                #  For now, only one default EAP type may be used at a time.
                #
                #  If the EAP-Type attribute is set by another module,
                #  then that EAP type takes precedence over the
                #  default type configured here.
                #
                default_eap_type = md5
```

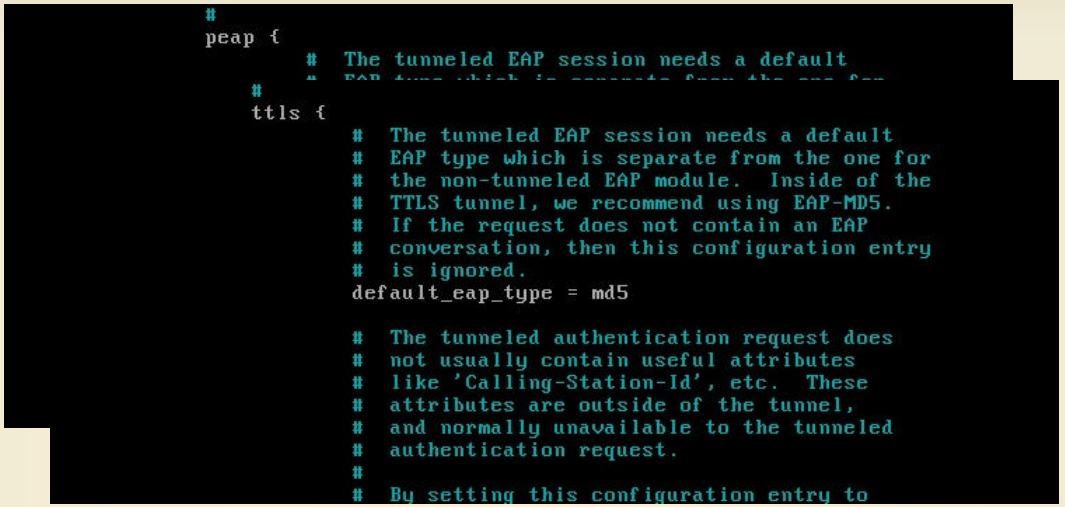
Burdaki default_eap_type degeri md5’den kullanacaginiz protokole bagli olarak peap veya ttls olarak degistirilebilir. Bu sadece kimlik denetimin daha hizli yapilmasini saglar.

“eap.conf” Dosyasindaki Degisiklikler (2)

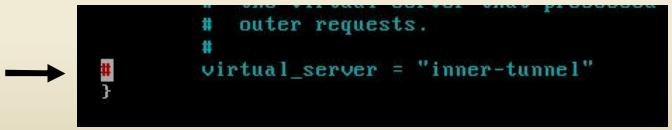
```
        #  http://www.dslreports.com/forum/remark,9286052~mode=flat
        #
        tls {
                #
                #  These is used to simplify later configurations.
                #
                certdir = ${confdir}/certs
                cadir = ${confdir}/certs

                private_key_password = whatever
                private_key_file = ${certdir}/server.pem

                #  If Private key & Certificate are located in
                #  the same file, then private_key_file &
                #  certificate_file must contain the same file
                #  name.
                #
```

Sunucu Sertifikasinin anahtar kelimesi “private_key_password” kismina yazilmalidir.

“eap.conf” Dosyasindaki Degisiklikler (3)



FreeRADIUS’un virtual server özelligi kullanilmayacaktir. Bunun için eap.conf dosyasinda ki peap ve ttls kisimlarinda bu özellik ile ilgili satirlarin basina # sembolu konulur.



“clients.conf” Dosyasindaki Degisiklikler

```
[root@localhost raddb]# vi clients.conf _
```

```
client 192.168.1.60 {
secret = 1234
shortname =test_switch
}
client 192.168.1.10 {
secret = 1234
shortname =test_ap
}
```

“client.conf” dosyasina kimlik denetimi yapacak ag cihazinin IP adresleri ve sifreleri belirtilir.

“users” Dosyasindaki Degisiklikler

```
[root@localhost raddb]# vi users _
```

```
# Note that there is NO 'Fall-Through' attribute, so the user will not
# be given any additional resources.



test    Cleartext-Password := "pass1234"
test2   Cleartext-Password := "pass2222"
_
```

Son olarak “users” dosyasina aginiza dahil olacak kullanicilarin kullanici adlari ve sifreleri belirtilmelidir.

FreeRADIUS'un Çalistirilmasi

```
[root@localhost raddb]# radiusd -X_
```

```
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on proxy address * port 1814
Ready to process requests.
_
```

*Artik FreeRADIUS **radiusd –X** komudu ile çalistirilabilir. Bu komut ile kimlik denetimi ile ilgili sunucu detayli log verecektir. Sunucunun düzgün çalistiginda eminseniz uygulamayi bir servis olarak devreye alabilirsiniz.*

PEAP ve TTLS Karsilastirmasi (1)

```
  rlm_eap: processing type peap
  rlm_eap_peap: Authenticate
  rlm_eap_tls: processing TLS
  eaptls_verify returned 7
  rlm_eap_tls: Done initial handshake
  eaptls_process returned 7
  rlm_eap_peap: EAPTLS_OK
  rlm_eap_peap: Session established.  Decoding tunneled attributes.
  rlm_eap_peap: Received EAP-TLV response.
  rlm_eap_peap: Success
  rlm_eap: Freeing handler
++[eap] returns ok
Login OK: [test/<via Auth-Type = EAP>] (from client test_switch port 50001 cli 0
0-16-D3-0C-A4-7B)
        MS-MPPE-Recv-Key = 0xef822417172605cf7e07c765f1103ae56fdaef449a3f1a96208
1d5aa5bc99486
        MS-MPPE-Send-Key = 0xdded84f2132540ad417175d993000a2157b9fd5540bb5fae9e5
515e71784e7ea
        EAP-Message = 0x030a0004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "test"
Finished request 10.
```

PEAP kullanici adi TLS tüneli disinda yolladigi için sifresiz gider. Ancak sifre TLS tünelinde ve MSCHAP2 ile sifrelenmis gider. Buda sunucu logunda bile kullanicinin sifresinin tespit edilmesini engeller.

PEAP ve TTLS Karsilastirmasi (2)

```
auth: type "PAP"
+- entering group PAP
rlm_pap: login attempt with password "pass1234"
rlm_pap: Using clear text password "pass1234"
rlm_pap: User authenticated successfully
++[pap] returns ok
Login OK: [test/pass1234] (from client test_switch port 0)
  TTLS: Got tunneled Access-Accept
  rlm_pap: Freeing handler
++[eap] returns ok
Login OK: [anonymous/<via Auth-Type = EAP>] (from client test_switch port 50001
cli 00-16-D3-0C-A4-7B)
        MS-MPPE-Recv-Key = 0xf36160279890d3e42343a2a265a0f9dc5d0d0ca6a7bcb47a630
c9a6d194e84e3
        MS-MPPE-Send-Key = 0xd1e9f1d356835346d6982caf31399a4da3a9b827a5f330f6d5d
cf3c326195542
        EAP-Message = 0x03060004
        Message-Authenticator = 0x00000000000000000000000000000000
        User-Name = "anonymous"
Finished request 6.
```

TTLS'de kullanici adi ve sifre TLS tünelinden gider. Ancak tünel içinde çogu zaman PAP kimlik denetimi seçildiginden kullanici adi sifre açik gider. Buda sunucu logunda kullanicinin sifresi açik olarak gözükmesine sebep olur.

Tesekkürler

csirt@ulakbim.gov.tr

http://csirt.ulakbim.gov.tr/gruplar/nac.uhtml
http://www2.itu.edu.tr/~akingok