BCP FreeRADIUS-tietokantaliitos

Tämän sivun sisältö:

- Liittäminen Active Directoryyn
- Liittäminen LDAP-tietokantaan (OpenLDAP)
- Useamman tietokannan huomioonottaminen
- EAP-TLS-autentikointi
- Kommentteja

Tunniste	Funetin Parhaat käytännöt -dokumentti
Versio	1.0
Tila	Kommentointikierros päättynyt 31.5.2012. Funetin TVK hyväksynyt dokumentin 30.8.2012.
Päiväys	4.6.2012
Otsikko	FreeRADIUS-tietokantaliitos
Työryhmä	MobileFunet
Laatijat	Wenche Backman-Kamila/CSC, Tuukka Vainio/TY, Miika Räisänen/OY, Thomas Backa/ÅA
Vastuutaho	Wenche Backman-Kamila/CSC
Tyyppi	suositus

Näissä ohjeissa käsitellään miten FreeRADIUS-palvelin liitetään ulkoiseen käyttäjätietokantaan. Ennen kuin siirrytään tähän vaiheeseen, on syytä konfiguroida FreeRADIUS-palvelimen perusasetukset. Ohjeita tähän löytyy sivulta FreeRADIUS-konfigurointi.

Näiden ohjeiden pääkirjoittajana on toiminut Wenche Backman-Kamila paitsi lukujen "Useamman tietokannan huomioonottaminen" ja "EAP-TLS-autentikointi" osalta, jotka on kirjoittanut Tuukka Vainio.

Liittäminen Active Directoryyn

Samba ja Kerberos

Samba ja Kerberos tarvitaan liittämään FreeRADIUS-palvelin Active Directory (AD) -käyttäjätietokantaan. RHELin tapauksessa Sambasta voidaan asentaa joko distribuution oma versio yum-komennon avulla tai uusin versio Sambasta voidaan asentaa lataamalla tarvittavat paketit netistä ja käyttämällä rpm-komentoa. Kunhan distribuution oma versio on tuoreempi kuin 3.0.0 kannattaa käyttää yum:ia, sillä näin päivityksen hallinta helpottuu.

Vaihtoehto 1 - Samban asentamien yum:in avulla

Distribuution oma versio Sambasta ja Samban yhteydessä asentavasta Winbind-ohjelmasta selviää *yum info* -komennon avulla (*yum info **samba** ja yum info *winbind**). Samba ja Winbind asennetaan *yum install*-komennon avulla. Itse ohjelman lisäksi kannattaa myös installoida mukana tulevat dokumentaatiotiedostot samba*-doc.

Vaihtoehto 2 - Samban pakettien lataaminen ja asentaminen rpm:llä

Aloitetaan lataamalla Samba vaikka downloads-sivulla olevan enterprisesamba.com-linkin kautta. Ladataan ainakin seuraavat paketit:

- *samba3*.rpm*, joka tarvitsee
  - *libwbclient*.rpm*
  - *samba3-client*.rpm*
- *samba3-winbind*.rpm*

Seuraavaksi installoidaan paketit ajamalla *rpm -ihv (tai -Uhv) libwbclient*.rpm, rpm -ihv (tai -Uhv) samba3-client*.rpm, rpm -ihv (tai -Uhv)samba3*.rpm* ja *rp m -ihv (tai -Uhv) samba3-winbind*.rpm* . Voi olla järkevää installoida myös paketit *samba3-utils*.rpm, samba3-debuginfo*.rpm* ja *samba3-doc*.rpm* vastaavalla tavalla. *samba3-doc* saattaa tarvita lisäpaketteja, jotka voidaan etsiä täältä.

Samban konfigurointi

Kokeile ensin että Samba ja Winbind käynnistyvät ajamalla komennot: */etc/init.d/smb start* ja */etc/init.d/winbind start*.

Kun Samba on installoitu konfiguroidaan /etc/samba/smb.conf-tiedostoa. Malli löytyy mm. Samba-wikin sivuilta mutta pelkästään autentikoinnin tarpeisiin räätälöidystä konfigurointitiedosta löytyy esimerkki selityksineen liitetiedostosta. Lisätietoja eri parametreista löytyy ainakin samba3-doc-lisäpaketin smb.conf.5.html-tiedostosta ..../samba3/htmldocs/manpages/-hakemistosta. Asetukset voidaan testata ajamalla *testparm smb.conf* .

Kerberos

Seuraavaksi määritellään Kerberos-sovelluksen parametrit. Riittää, että palvelimelle on installoitu seuraavat paketit:

- *krb5-workstation*
- *krb5-libs*

Kerberoksen parametrit määritellään /etc/krb5.conf-tiedostoon. Myös Kerberoksen parametrien suhteen löytyy malli Samba-wikin sivuilta. Liitetiedostosta löytyy FreeRADIUS-palvelimen ja AD:n liittämiselle esimerkkiparametreja. Huomioi, että isot tai pienet kirjaimet ovat eri merkkejä.

Koska Kerberoksen toiminta on riippuvainen täsmällisestä ajasta, kannattaa tässä vaiheessa tarkistaa että palvelin käyttää samoja NTP-palvelimia kuin AD. NTP-palvelimet määritellään tiedostossa *etc/ntp.conf*. Funetin NTP-palvelimet ntp1.funet.fi ja ntp2.funet.fi määritellään seuraavalla tavalla:

```
restrict 193.166.5.177 mask 255.255.255.255 nomodify notrap noquery
server 193.166.5.177
restrict 193.166.5.197 mask 255.255.255.255 nomodify notrap noquery
server 193.166.5.197
```

Liitos Active Directoryyn

Käynnistä seuraavaksi samba ja winbind komennoilla */etc/init.d/smb start* ja */etc/init.d/winbind start*. Liitetään palvelin AD:hen ajamalla komento *net ads join –S <domain_controller> –U <administrator-tunnus> –W windows*. Tämän jälkeen winbind tulisi käynnistää uudelleen: */etc/init.d/winbind restart*. Liittymisen onnistumista voidaan testata kaikilla käyttäjätunnuksilla, jotka on määritelty AD:hen, esim. näin: *wbinfo -a kayttajatunnus*. Syötä salasanasi ja varmista että testi päättyy ilmoituksella *authentication succeeded*. FreeRADIUS-palvelimen kanssa tullaan käyttämään Samban ntlm_auth-sovellusta, joten sitä kannattaa myös testata:

ntlm_auth --username kayttajatunnus --password
password:
NT_STATUS_OK: Success (0x0)

Ennen kuin siirrytään FreeRADIUS-palvelimen konfigurointiin on määriteltävä radiusd-käyttäjälle oikeudet käyttää winbindia. Tämä tehdään muuttamalla winbindd_privileged-kansion oikeudet. Jos winbindd_privileged-kansion ryhmäkäyttäjäksi on määritelty wbpriv, kannattaa lisätä radiusd-käyttäjä wbpriv-ryhmään esim. useradd-komennolla (*useradd -G wbpriv radiusd*). Jos wbpriv-ryhmä puuttuu, voidaan lisätä radiusd suoraan winbindd_privileged-kansion ryhmäkäyttäjäksi komennolla *chown root:radiusd /var/lib/samba/winbindd_privileged*.

Lopuksi kannattaa varmistaa, että ryhmällä on luku- ja ajo-oikeudet kansioon. Jos ei, ne lisätään komennlla *chmod 750 /var/lib/samba/winbindd_privileged.*

Konfigurointi

AD:ssä käyttäjien salasanat on tallennettu NTHASH-muodossa ja mahdolliset EAP- ja EAP-tyyppiset menetelmät määräytyvät seuraavan taulukon mukaan . Yleensä tuetaan FreeRADIUS-palvelimen ollessa liitettynä AD:hen menetelmät PEAP-MSCHAPv2, TTLS-MSCHAPv2 sekä TTLS-PAP. Ennen kuin aloitat varsinaisen konfiguroimisen, varmista että **proxy.conf**-tiedostoon on määritelty oma realmisi muodostamaan erikoistapaus (esimerkkinä csc.fi):

```
realm csc.fi {
}
```

Autentikointi kaikilla menetelmillä hoidetaan ntlm_auth-sovelluksen avulla, mutta sitä kutsutaan hieman eri tavalla menetelmästä riippuen.

Konfigurointi TTLS-PAP-menetelmän tukemiseksi

TTLS-PAP-menetelmä tuetaan luomalla ensin /etc/raddb/modules-hakemistoon tiedosto nimeltään *ntlm_auth* ja lisäämällä siihen seuraavat rivit:

```
exec ntlm_auth{
wait = yes
program = "/usr/bin/ntlm_auth --request-nt-key --domain=windows --username=%{Stripped-User-Name} --password=%
{User-Password}"
}
```

Muuta --domain-parametrin arvoa jos haluat tässä käyttää tiettyä omaa domainia (--domain=MYDOMAIN).

Seuraavaksi lisätään /etc/raddb/sites-available-hakemistossa olevalle **eduroam-inner-tunnel**-tiedostolle merkityt rivit:

```
authorize {
 auth_log
 files
 suffix
 mschap
 #Jos mschap palauttaa "noop", laitetaan Auth-Type:n arvoksi "ntlm_auth", jotta TTLS-PAP toimisi AD:n kanssa.
 #mschap palauttaa "ok" TTLS-MSCHAPv2:lle ja "noop" TTLS-PAP:ille. mschap palautaaa "noop" myös jos sisempi
 #menetelmä on EAP-tyyppinen, eli PEAP-MSCHAPv2 tai TTLS-(EAP-MSCHAPv2).
 #PEAPin sisäinen menetelmä on aina oltava EAP-tyyppinen.
 if (noop) { #lisätään
         update control{ #lisätään
                 Auth-Type := ntlm_auth #lisätään
                 } #lisätään
 } #lisätään
 pap
 eap {
         ok = return
 }

 #Jos eap palauttaa "updated", autentikointimenetelmä (Auth-Type) on EAP ja aikaisemmin määritelty ntlm_auth
 #voidaan poistaa. eap palauttaa "updated" jos sisempi menetelmä on EAP-tyyppinen eli PEAP-MSCHAPv2 tai TTLS-
(EAP-MSCHAPv2).
 #eap palauttaa "noop" TTLS-MSCHAPv2:lle ja TTLS-PAP:lle.
 #Jos tämä if-lohko poistetaan autentikointi toimii edelleen, mutta kaksi autentikointimenetelmää tulee siinä
tapauksessa
 #määritellyksi tilanteissa, jossa sisempi menetelmä on EAP-tyyppinen: EAP ja ntlm_auth.
 if (updated) { #lisätään
         update control{ #lisätään
                 Auth-Type -= ntlm_auth #lisätään
         } #lisätään
 } #lisätään
}

authenticate {
 Auth-Type PAP{
 pap
 }
 Auth-Type MS-CHAP{
 mschap
 }
 Auth-Type ntlm_auth{ #lisätään
 ntlm_auth #lisätään
 } #lisätään
 # Allow EAP authentication.
 eap
}
.
.
.
```

Kun eduroam-inner-tunnel muokataan tällä tavalla, voidaan tukea myös PEAP-MSCHAPv2-, TTLS-MSCHAPv2- ja TTLS-EAP-MSCHAPv2-menetelmiä.

FreeRADIUS-palvelimen konfiguroinnin yhteydessä kannattaa myös tutustua sen omaan prosessointikieleen (FreeRADIUS Processing un-language). Tähän voidaan perehtyä palvelimen mukana tulevan ohjeen avulla, joka avataan kirjoittamalla komentoriville *man unlang*.

Konfigurointi PEAP-MSCHAPv2-, TTLS-MSCHAPv2- ja TTLS-(EAP-MSCHAPv2)-menetelmien tukemiseksi

PEAP-MSCHAPv2-, TTLS-MSCHAPv2- ja TTLS-(EAP-MSCHAPv2)-menetelmien tapauksessa ntlm_auth-sovellus kutsutaan mschap-moduulista, kun halutaan käyttää AD:ta autentikointiin. Muokkaa /etc/raddb/modules/mschap-tiedoston viimeistä riviä seuraavasti:

```
 ntlm_auth = "/usr/bin/ntlm_auth --request-nt-key --username=%{%{Stripped-User-Name}:-%{User-Name:-None}} --
domain=%{%{mschap:NT-Domain}:-windows} --challenge=%{mschap:Challenge:-00} --nt-response=%{mschap:NT-Response:
-00}"
```

Poista rivin alussa oleva ruksi. Tällä määrityksellä asetetaan domainin arvoksi "windows", jos NT-Domain-attribuuttia ei tule muualta. Jos haluat tässä käyttää omaa domainia kannattaa määritellä --domain = MYDOMAIN.

Myös mschap-moduulin muut parametrit kannattaa samalla säätää:

```
use_mppe = yes
require_encryption = yes
require_strong = yes
with_ntdomain_hack = no
```

Muuta

Jos AD-domainia ei haluta kovakoodata, voidaan se myös määritellä esim. realmin perusteella. Määrittely voidaan tehdä esim. /etc/raddb/sites-enabled /eduroam-inner-tunnel-tiedoston authorize-lohkossa:

```
authorize {
.
.
 # Strip domain to ntlm_auth attribute
 if ("%{User-Name}" =~ /@myorganisation.fi$/i){
 update request {
         Stripped-User-Domain = 'my-windows-domain'
         }
 }
}
```

Tässä tapauksessa ntlm_auth-kutsun domain-parametrille annetaan arvoksi Stripped-User-Domain:

```
--domain=%{Stripped-User-Domain}
```

Stripped-User-Domain on määritettävä ennen kuin sitä voidaan käyttää. Määrittely tehdään lisäämällä seuraava rivi etc/raddb/directory-tiedostoon:

```
ATTRIBUTE Stripped-User-Domain 3009 string
```

Kokemuksia

- Ainakin Samban versio 3.5.10-114(.el6.i686) toimii hyvin Windows 2008 R2:n kanssa.
- Jos on käytössä SELinux, saattaa olla, että lisäkonfigurointi on tarpeen.
- On huomattu, että winbind-daemon saattaa välillä kaatua, ilmeisesti muistivuodon vuoksi. Ongelma voidaan kiertää käynnistämällä winbind uudestaan esim. kerran viikossa, jos winbindin päivittäminen ei auta.

Liittäminen LDAP-tietokantaan (OpenLDAP)

FreeRADIUS-palvelimen liittäminen LDAP-tietokantaan onnistuu rlm_ldap-moduulin kautta. Jos moduulia ei ole asennettu RADIUS-palvelimen installointivaiheessa, se tehdään nyt ajamalla komento *rpm -Uhv freeradius-ldap-2.1.3-1.x86_64.rpm* /usr/src/redhat/RPMS/x86_64–hakemistosta.

FreeRADIUS-palvelin liitetään LDAP-tietokantaan muokkaamalla konfigurointitiedostot seuraavalla tavalla:

proxy.conf

Määritellään LDAP:ia vastaan autentikoitava realm erikoistapaukseksi:

```
realm ldapdomain.fi {
}
```

eduroam-inner-tunnel

authorize-lohkoon lisätään suffix-määritelmä realm-osuuden poistamiseksi sekä ldap-määritelmä. Ilman suffix-määritelmää tietokantahaku tullaan suorittamaan käyttäjälle *kayttajatunnus@ldapdomain.fi*, mutta suffix-määritelmällä haku suoritetaan vain käyttäjälle *kayttajatunnus*.

```
authorize {
 auth_log
 files
 suffix #lisätään
 ldap #lisätään
 mschap
 pap
 eap {
 ok = return
 }
}
```

etc/raddb/modules/ldap

Tähän tiedostoon määritellään LDAP-palvelin ja sen tietokannan tiedot. Jos LDAP-palvelin on samalla palvelimella kuin FreeRADIUS-palvelin, määritelmäksi riittää *localhost*. Jos ei, määritellään tähän palvelimen nimi *ldapserver.realm.fi*. Tiedostoon voidaan myös määritellä LDAP-tietokannan käyttäjä, jolloin tietokantaan liitytään tällä käyttäjätunnuksella ja salasanalla. Jos LDAP-tietokannan käyttäjää jätetään määrittelemättä, liitytään tietokantaan autentikoitavan käyttäjän tunnuksella ja salasanalla, mikä on tietoturvallisempi vaihtoehto. Tästä syystä LDAP-tietokannan käyttäjän tiedot on alhaalla kommenteissa. Käyttäjien Organisation Unit (ou) määritellään myös.

```
ldap {
 server = "localhost" #tai "ldapserver.realm.fi"
 #identity = "cn=Manager,dc=ldaprealm,dc=fi"
 #password = ldaptestsecret
 basedn = "ou=Funetpeople,dc=ldaprealm,dc=fi"
 filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})
 .
 .
}
```

etc/raddb/ldap.attrmap

Tähän tiedostoon määritellään mikä RADIUS-attributti vastaa mitä LDAP-attribuuttia. Jos käyttäjien salasanat ovat tietokannassa selkokielisenä määritellään *Cleartext-Password* ja jos ne ovat NTHASH-muodossä määritellään *NT-Password*.

```
checkItem User-Name uid
checkItem Cleartext-Password userPassword
#TAI
checkItem NT-Password userPassword
```

Useamman tietokannan huomioonottaminen

Mikäli FreeRADIUS liitetään useampaan ulkoiseen käyttäjätietokantaan, kannattaa huomioida, että yhdenkin autentikointimoduulin epäonnistuminen aiheuttaa oletuksena koko autentikoinnin epäonnistumisen. Ryhmittämällä autentikointimoduulit saadaan autentikointi tehtyä vikasietoisesti:

```
server eduroam {
 authorize {
         auth_log
         suffix
         group {
                 eap {
                         fail = 1
                         ok = return
                 }
                 ldap {
                         fail = 1
                         ok = return
                 }
                 sql {
                         fail = 1
                         ok = return
                 }
         }
 }
 authenticate {
.
.
.
```

Tällöin ensimmäinen OK:n palauttava moduuli lopettaa autentikoinnin. Jos mikään moduuli ei palauta OK:ta, käyttäjälle palautetaan Access-Reject-vastaus.

EAP-TLS-autentikointi

Varmenteita käyttävä EAP-TLS-autentikointi tarvitsee FreeRADIUS-konfiguroinnin lisäksi julkisten avainten hallintajärjestelmän, jollaiseksi soveltuu Windows-ympäristössä helposti Windows Server Active Directory Certificate Services (Active Directory Certificate Services Step-by-Step Guide). Tämä ohje ei auta PKI:n käyttöönotossa, vaan kuvaa tarvittavat muutokset FreeRADIUS-palvelimen liittämiseksi PKI-ympäristöön. Oletuksena on, että FreeRADIUS-palvelimella on jo toimiva eduroam-konfiguraatio.

PKI-ympäristöstä tarvitaan sen juurivarmenne (alla UniversityOfKaupunkiCA.crt), ja mahdollisesti FreeRADIUS-palvelimille myönnetyt palvelinvarmenteet, mikäli eduroamissa käytettyjä varmenteita ei haluta käyttää RADIUS-palvelimen tunnistamiseen.

Periaatteessa FreeRADIUS-palvelimen pitäisi tunnistaa mitä EAP-metodia käytetään, mutta helpoimmalla pääsee kopioimalla uuden eap-instanssin (eap-tls) **eap.conf**:n loppuun:

```
eap {
    # EAP-konfiguraatio, joka toimii eduroamin kanssa.
    ....
}

eap eap-tls {
    default_eap_type = tls
    timer_expire = 60
    ignore_unknown_eap_types = no
    cisco_accounting_username_bug = no
    max_sessions = 4096
    tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        private_key_file = ${certdir}/radius.yo.fi.key
        certificate_file = ${certdir}/radius.yo.fi-bundle.crt
        CA_file = ${cadir}/UniversityOfKaupunkiCA.crt

        dh_file = ${certdir}/dh
        random_file = ${certdir}/random
        cipher_list = "HIGH:!ADH:!MD5"
        fragment_size = 1024
        include_length = yes
        check_crl = no
        check_cert_issuer = "/DC=fi/DC=yo/CN=University of Kaupunki"
    }
}
```

Olennaiset muutokset muuttujiin:

muuttuja	eduroam-varmenteilla	oman CA:n varmenteilla
default_eap_type	tls	
private_key_file	eduroamissa käytetty avain	oman CA:n kanssa käytetty avain
certificate_file	eduroam-palvelinvarmenne ja varmenneketju (esim. TERENA-bundle)	oman CA:n palvelinvarmenne
CA_file	oman CA:n juurivarmenne, koska klientien varmenteet tarkastetaan tätä vasten	
check_cert_issuer	openssl x509 -noout -in UniversityOfKaupunkiCA.crt -issuer	

Mikäli klientien varmenteet halutaan tarkistaa peruuttamisen varalta, kannattaa käyttää OCSP:tä (tuki tuli FreeRADIUS 2.1.11:ssä, FreeRADIUS-wikin mallikonfiguraatio). CRL-tarkistukset eivät ole näppäriä, koska FreeRADIUS-palvelimen itse tekemä tarkastus edellyttää paikallista CRL-tiedostoa ja FreeRADIUS-palvelimen uudelleenkäynnistystä CRL-tiedoston muuttuessa. Lisäksi ulkoisena komentona kutsuttu OpenSSL vaatii myös paikallisen CRL-tiedoston, koska se ei osaa tarkistaa tiedostoa HTTP:n yli (ks. FreeRADIUS and CRLs).

Jos EAP-TLS:n kanssa ei voida käyttää omaa virtual serveriä (esim. koska sama WLAN-kontrolleri on käytössä), voidaan eap-tls-instanssia kutsua esim. toisen SSID:n autentikointien kohdalla. Tällöin tehdään seuraavat muutokset **sites-available/eduroam**-tiedostoon:

```
server eduroam {
    authorize {
        ...
    }
    authenticate {
        Auth-Type eap {
            if (Aruba-Essid-Name == "YO Staff") { # tai muu tapa kaivaa SSID
                eap-tls
            } else {
                eap
            }
        }
        ...
```

Windows 7-suplikantin EAP-TLS-asetukset

Security-välilehdeltä:

- Security type: ***WPA2-Enterprise***
- Encryption type: ***AES***
- Choose a network authentication method: ***Microsoft: Smart Card or other certificate***
- Remember my credentials for this connection each time I'm logged on
- Settings-napin takaa:
  - When connecting: ***Use a certificate on this computer***
    - Use simple certificate selection
  - Validate server certificate
    - Servers: ***radius.yo.fi;radius2.yo.fi***
    - Trusted Root Certification Authorities: ***University of Kaupunki CA*** (tai TERENA-varmenteiden tarvitsema luottosuhde)
    - Do not prompt user to authorize new servers or trusted certification
- Advanced settings -napin takaa:
  - 802.1X settings -välilehti:
    - Specify authentication mode: ***Computer authentication***

Kommentteja

Ole hyvä ja lisää kommentteja tai omaa tekstiä.

Linuxin liittäminen Active Directoryyn onnistuu myös ohjeen http://deployingradius.com/documents/configuration/active_directory.html mukaisesti. RHEL6:ssa tarvitsee asentaa samba-common- ja samba-winbind-paketit, lisätä radiusd-käyttäjä wbpriv-ryhmään, ja käynnistää winbind-demoni pyörimään. -- Tuukka Vainio/TY

Lisäsin yhden puuttuneen aaltosulun kohtaan "Konfigurointi PEAP-MSCHAPv2-, TTLS-MSCHAPv2 ja TTLS-(EAP-MSCHAPv2)-menetelmien tukemiseksi". – Tomi Salmi/CSC,Funet 2013-08-30