

Freeradius + AD

Le principe est que le serveur Radius récupère les identifiants et mots de passe des utilisateurs directement depuis le serveur Active Directory grâce au protocole NTLM (NT Lan Manager).

1 - Prérequis

Installation de samba, freeradius et krb5

```
apt install freeradius samba krb5-user winbindd
```

Ajout de l'utilisateur de freeradius dans le groupe winbindd pour l'accès aux comptes utilisateurs de l'AD

```
adduser freerad winbindd_privileged
```

2 - Ajout du serveur Radius dans le domaine

Déclaration du contrôleur de domaine dans samba

```
nano /etc/samba/smb.conf
  workgroup = <NomDomaine>

# Security mode. Most people will want user level
# security. See security_level.txt for details.
  security = ads

===== Share Definitions =====

...
winbind use default domain = no
password server = <NomFQDNContrôleurDeDomaine>
realm = <NomDomaine>
```

Toujours dans le même fichier, vérification des lignes suivantes dans le partage [homes]

```
comment = Home Directories  
browseable = no  
writable = yes
```

Déclaration du contrôleur de domaine dans krb5

```
nano /etc/krb5.conf  
<Domaine> = {  
    kdc = <NomFQDNContrôleurDomaine>  
}
```

Modification du fichier nsswith.conf et ajouter "files winbind" à chaque fin de ligne

```
nano /etc/nsswith.conf  
passwd:    files winbind  
shadow:    files winbind  
group:     files winbind  
  
protocols: files winbind  
  
services:  files winbind  
  
netgroup:  files winbind  
  
automount: files winbind
```

Vérification de que service samba est en fonctionnement

```
ps -ef | grep nmbd  
ps -ef | grep smbd
```

Entrer dans le domaine

```
net join -U <NomAdminContrôleurDomaine>
```

Vérification du fonctionnement du démon winbindd

```
ps -ef | grep winbindd
```

Tentative de connexion avec un utilisateur du domaine

```
wbinfo -a <Utilisateur>%<MotDePasse>
```

Une erreur survient généralement, elle est dû au serveur qui essaye de se connecter sans l'accord de l'AD.

Test du protocole NTLM

```
ntlm_auth --request-nt-key --domain=<NomDomaine>
--username=<Utilisateur>
```

Résultat :

```
NT_STATUS_OK : Success (0x0)
```

3 - Configuration de Freeradius

Dans le dossier /etc/freeradius/3.0/

```
nano ./mods-available/mschap
with_ntdomain_hack = yes
```

Décommenter la ligne

```
ntlm_auth = "/path/to/ntlm_auth --request-nt-key
--username=%{%{Stripped-User-Name}:-%{%{User-Name}:-None}}
--challenge=%{%{mschap:Challenge}:-00}
--nt-response=%{%{mschap:NT-Response}:-00}"
```

Ajouter

```
--domain=%{mschap:NT-Domain}
```

```
nano ./mods-available/eap
```

Dans la section `tls-config tls-common {`

Remplacer `random_file = ${certdir}/random` par `random_file = /dev/urandom`

Relancer le service freeradius

```
systemctl restart freeradius
```