802.1X, radius et Kerberos (archive)

802.1X est un protocole qui a pour but d'ouvrir l'accès au réseau en fonction d'une authentification des usagers ou des machines qui essaient de s'y raccorder. Le processus d'authentification peut être varié et déporté vers un service d'authentification centralisé. De nombreux cas d'usage utilisent un serveur *freeRadius* pour l'authentification. Les clients **802.1X** (commutateurs, bornes Wi-Fi, ...) sont alors configurés pour interroger un serveur *freeRadius* qui gère différents scénarios d'authentification. Pour configurer un serveur *freeRadius* s'appuyant sur une base d'usagers Kerberos, on peut procéder de la manière suivante :

```
- compiler un freeRadius à partir de la distribution SRC
- un module  rlm_krb5 est alors produit
- dans le fichier radiusd.conf insérer ce qui suit dans la configuration des modules
 krb5 {
           keytab = /etc/krb5.keytab
           service_principal = radius/fqdn.du.serveur.radius      }
- toujours dans radiusd.conf dans la section authenticate ajouter
  Auth-Type Kerberos {
    krb5
  }
- la configuration du reste dépend du cas d'usage, ci-dessous un ajout effectué dans le fichier users :

  tutu        Auth-Type := kerberos
        Fall-Through = No
```

Il convient également de créer les principaux suivants :

- le host qui héberge le serveur radius (addprinc -randkey host/fqdn.du.serveur.radius)
- le service radius (addprinc -randkey radius/fqdn.du.serveur.radius)
- extraire le fichier keytab correspondant et l'installer comme indiqué dans le radiusd.conf

Si ce scénario permet d'intégrer une base kerberos dans le processus d'ouverture des accès au réseau, notons que la propagation des tickets ne s'effectue pas jusqu'aux machines connectées (à suivre ...).