Cookbook Radius Taillefer

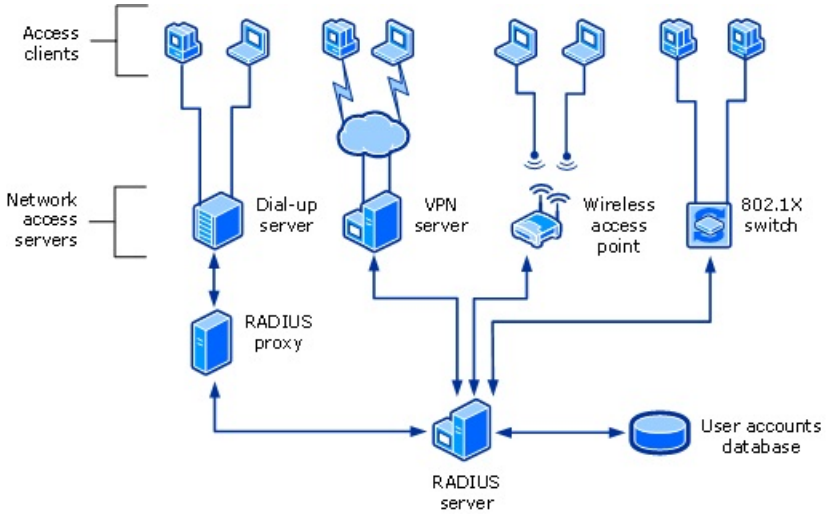
Taillefer Jordan

Octobre 2016

1 Résumé

Radius est un protocole client serveur qui a vu le jour en 1991. Le but était de créer un protocole permettant d'authentifier des utilisateurs chacun pouvant être connectés à des serveurs différents, tout en ne conservant qu'une seule base de donnée centralisée dans un seul serveur.

La base de donnée est donc dupliquée entre le serveur principal et les différents serveurs.



2 La recette de Radius

2.1 Les caractéristiques de Radius

Radius est un protocole qui réalise l'authentification, l'autorisation et la traçabilité (AAA : Authentication, Authorization, Accounting)

Radius est notamment utilisé dans les réseaux mobiles UMTS et LTE afin d'authentifier et d'autoriser l'accès d'un mobile à un réseau. On le retrouve aussi dans les serveurs d'authentification nécessaires pour le standard 802.1x.

2.2 La recette

2.2.1 Les ingrédients

Dans notre cas, nous allons utiliser Linux Debian ainsi que FreeRadius, qui est une implémentation de Radius libre et permettant l'authentification.

2.2.2 Etape : Installation

FreeRadius dispose de plusieurs paquets permettant d'avoir des bases de données différentes.

On retrouve :

- freeradius-mysql
- freeradius-ldap
- freeradius-postgresql

Dans notre cas nous n'avons besoin que de LDAP, on a donc la commande d'installation suivante :

```
aptitude install freeradius freeradius-ldap
```

Figure 1: Installation de radius sous Debian

2.2.3 Étape : Bien choisir les saveurs

FreeRadius propose de configurer le serveur en accédant au dossier "/etc/freeradius"

Vous pouvez changer la taille du buffer de requête, la configuration suggère 256 fois le nombre de clients simultanés souhaité (cependant vous ne pouvez pas dépasser 1024 fois).

```
// nom d'hôte dans les logs
hostname_lookups = no
```

Figure 2: Taille de buffer

Vous avez la possibilité de recevoir les noms d'hôtes au lieu des adresses IP dans les logs, mais cela ralentit les exécutions. Pour le désactiver, changer la ligne suivante :

```
// nom d'hôte dans les logs
hostname_lookups = no
```

Figure 3: Nom d'hôte dans logs

Enfin, changer la ligne suivante afin d'afficher dans les logs les authentifications ayant échoué :

```
//Mauvaise authentification dans les logs
auth_badpass = yes
```

Figure 4: Mauvaise authentification dans logs

2.2.4 Étape : Préparation du client Radius

Dans le fichier "clients.conf", vous retrouverez les différents clients, identifiés par leur adresse IP ou l'adresse du réseau.

```
// Configuration des clients
client 127.0.0.1 {
    secret      = pwdTest
    shortname   = localhost
    nastype     = other
}
client 192.168.1.0/24 {
    secret      = wifiPwd
    shortname   = wifiAP
    nastype     = other
}
```

Figure 5: Configuration client

2.2.5 Étape : Préparation de l'authentification à l'annuaire LDAP

Maintenant que le serveur Radius est configuré, il va falloir mettre en place le serveur LDAP correspondant à notre annuaire.

Pour cela allez dans le fichier de configuration "modules/ldap" et remplissez les champs associés à votre annuaire LDAP.

```
// Configuration du serveur LDAP à adapter
//en fonction de l'annuaire
ldap ldap_1 {
    server = "ldaps://ldaps.domain.tld"
    identity = "cn=admin,dc=domain,dc=tld"
    password = admPwd
    basedn = "ou=people,dc=domain,dc=tld"
    filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
    dictionary_mapping = "${raddbdir}/ldap.attrmap"
    ldap_connections_number = 5
    access_attr = "uid"
    timeout = 4
    timelimit = 3
    net_timeout = 1
    tls {
            start_tls = no
    }
    set_auth_type = yes
    edir_account_policy_check = no
}
```

Figure 6: Configuration serveur LDAP

2.2.6 Étape : Dressage final

Notre serveur dispose maintenant d'un serveur lié à un annuaire LDAP, il va donc falloir maintenant l'activer durant les phases d'autorisation et d'authentification.

Pour cela, rendez vous dans le fichier de configuration "sites-enabled/default"
Activez les phases en rentrant les lignes suivantes :

```
//Activation de l'annuaire lors de l'autorisation
authorize {
    preprocess
    suffix
    files
    group {
            ldap_1
    }
}

//Activation de l'annuaire lors de l'authentification
authenticate {
    unix

    Auth-Type LDAP1 {
            ldap_1
    }
}
```

Figure 7: Activation des phases

2.2.7 Étape : Le service

La configuration étant terminé, vous pouvez démarrer votre serveur radius :

```
// demarre le service freeradius
service freeradius start
```

Figure 8: Démarrage du service de Radius

Enfin vous pouvez tester la connexion grâce à la commande

```
//commande de test de radius
radtest username password localhost:1812 0 radiusSecret
```

Figure 9: Test d'un client Radius

References

[1] Cisco. Détail technique de radius. https://cisco.com.

[2] UnixExperience. Fonctionnement de radius. http://www.unix-experience.fr/2012/freeradius-serveur-radius-opensource.

[3] Wiki. Presentation de radius. https://en.wikipedia.org/wiki/RADIUS.