

# Serveur Proxy Squid.

## Présentation :

Un proxy est un composant logiciel informatique qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges donc il sert à mettre en cache des éléments et à filtrer des données.

Par extension, on appelle aussi proxy un matériel comme un serveur mis en place pour assurer le fonctionnement de tels services. Il peut être en mode serveur ou en mode transparent

## Objectif :

Installer et configurer un serveur Proxy par authentification LDAP (Lightweight Directory Access Protocol).

## Pré requis :

- Deux ordinateurs sur Linux (ici, on utilisera la Debian 8.2)
- Avoir une connexion internet pour télécharger les paquets.
- Avoir deux IP fixe pour le Samba et Proxy.
- Mes VM s'appellent dcsamba et squidlab. Les @IP sont 192.168.1.134/24 et 192.168.1.135/24

## Sommaire :

- 1) Installation et promotion en contrôleur de domaine du Samba
- 2) Installation et Configuration de l'annuaire LDAP
- 3) Installation et Configuration de Phpldapadmin
- 4) Installation et Configuration de Bind9
- 5) Installation et Configuration de Squid3
- 6) Installation, Configuration et Phase de test de SquidGuard
- 7) Installation et Configuration de LightSquid

## I. Installation et promotion en contrôleur de domaine du Samba

J'ai choisit d'installer Samba manuellement comme nous l'avions en cours de PPE. J'ai pris la version 4.3.5 de samba que j'ai compilée et installée.

Ainsi, pour lancer la promotion du contrôleur de domaine, j'ai entré cette commande :

```
samba-tool domain provision --use-rfc2307 --realm=STURSULE.LOCAL --domain STURSULE --adminpass @mot_de_passe --server-role=dc --interactive
```

On voit ainsi les processus engendrés par le serveur samba:

```
Service: PID
-----
dnupdate 775
nbt_server 764
rpc_server 763
cldap_server 767
winbind_server 774
winbind_server 772
winbind_server 757
winbind_server 788
winbind_server 808
winbind_server 816
winbind_server 837
winbind_server 840
winbind_server 846
winbind_server 863
kdc_server 769
samba 0
dreplsrv 770
kccsrv 773
```

## II. Installation et Configuration de l'annuaire LDAP

J'ai installé OpenLDAP depuis les ressources :

```
apt-get install slapd ldap-utils migrationtools
```

Puis j'ai réalisé la liaison Samba/LDAP. J'ai inséré les schémas Samba dans LDAP. On peut vérifier la bonne configuration des fichiers :

```
root@dcsamba:/# slapttest -f /etc/ldap/slapd.conf -F /etc/ldap/slapd.d
config file testing succeeded
```

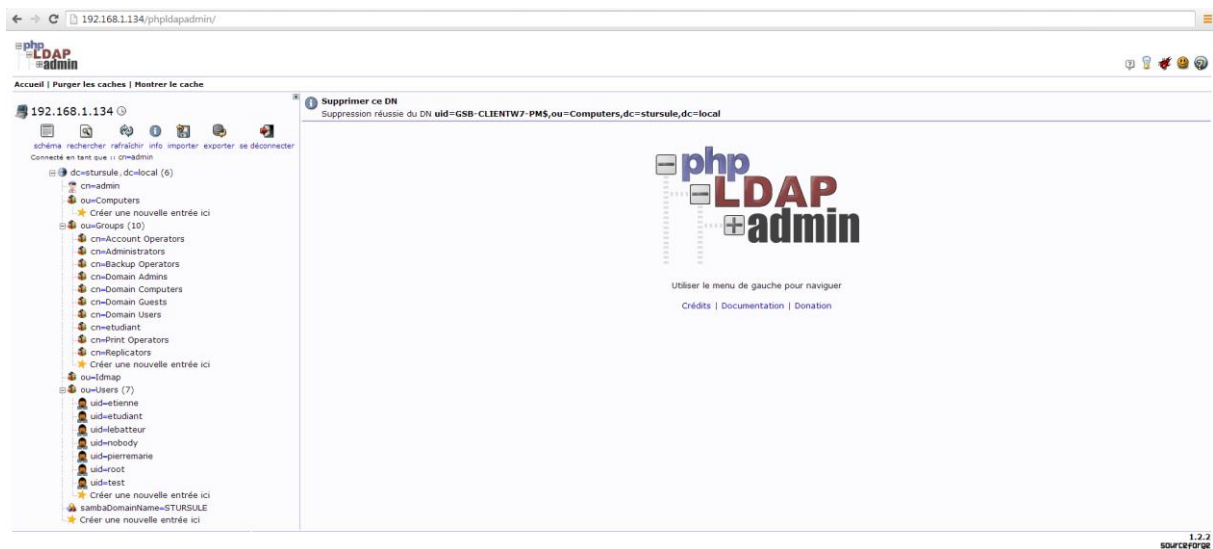
De plus, j'ai renseigné le fichier smb.conf. Enfin, j'ai configuré Smbldap-Tools en récupérant le SID du domaine :

```
root@dcsamba:/# net getlocalsid
SID for domain STURSULE is: S-1-5-21-2252255531-4061614174-2474224977
```

Ainsi, notre configuration pour un serveur Samba/LDAP est opérationnelle.

### III. Installation et Configuration de Phpldapadmin

J'ai installé PhpLDAPAdmin pour avoir un accès à mon annuaire LDAP. Après installation depuis les sources et une légère configuration, on accède à une interface graphique :



## IV. Installation et Configuration de Bind9

Comme pour toute base d'annuaire, il faut un DNS. J'ai ainsi installé Bind et configuré une zone directe et inverse.

Zone directe :

```
GNU nano 2.2.6 Fichier : /etc/bind/db.stursule.local
;
; BIND data file for local loopback interface
;
$TTL 604800
$ORIGIN stursule.local.
@ IN SOA dcsamba.stursule.local. root.stursule.local. (
        2           ; Serial
        604800      ; Refresh
        86400       ; Retry
        2419200    ; Expire
        604800 )   ; Negative Cache TTL
;
IN NS dcsamba.
dcsamba IN A 192.168.1.134
squidlab IN A 192.168.1.135
clientw7 IN A 192.168.1.136
samba-partage IN A 192.168.1.125
```

Zone inversée :

```
GNU nano 2.2.6 Fichier : /etc/bind/db.stursule.local.inv
;
; BIND reverse data file for local loopback interface
;
$TTL 604800
$ORIGIN 1.168.192.in-addr.arpa.
@ IN SOA dcsamba.stursule.local. root.stursule.local. (
        1           ; Serial
        604800      ; Refresh
        86400       ; Retry
        2419200    ; Expire
        604800 )   ; Negative Cache TTL
;
IN NS dcsamba.stursule.local.
125 IN PTR samba-partage.stursule.local.
134 IN PTR dcsamba.stursule.local.
135 IN PTR squidlab.stursule.local.
136 IN PTR clientw7.stursule.local.
```

On vérifie avec la commande nslookup :

```
root@dcsamba:/# nslookup
> 192.168.1.136
Server:          192.168.1.134
Address:         192.168.1.134#53

136.1.168.192.in-addr.arpa    name = clientw7.stursule.local.
> clientw7
Server:          192.168.1.134
Address:         192.168.1.134#53

Name:   clientw7.stursule.local
Address: 192.168.1.136
```

## V. Installation et Configuration de Squid3

On va installer le paquet d'installation de Squid :

```
apt-get install squid3
```

On remarque que le port d'écoute par défaut de Squid est 3128 :

```
# Squid normally listens to port 3128
http_port 3128
```

On remarque aussi que lors de l'installation de Squid, un utilisateur proxy appartenant au groupe proxy a été créé :

```
root@SQUIDLAB:~# cat /etc/passwd | grep proxy
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,:/run/systemd:/bin/false
root@SQUIDLAB:~# cat /etc/group | grep proxy
proxy:x:13:
systemd-bus-proxy:x:106:
```

Pour le début, nous allons nous authentifier avec un utilisateur local. Nous allons commencer par ajouter les règles d'authentification :

```
auth_param basic program /usr/lib/squid3/basic_ldap_auth -R -b "ou=Users,dc=stursule,dc=local" -W Root123 -h 192.168.1.134
auth_param basic children 10
auth_param basic realm Internet Proxy St-Ursule
auth_param basic credentialsttl 1 minute
```

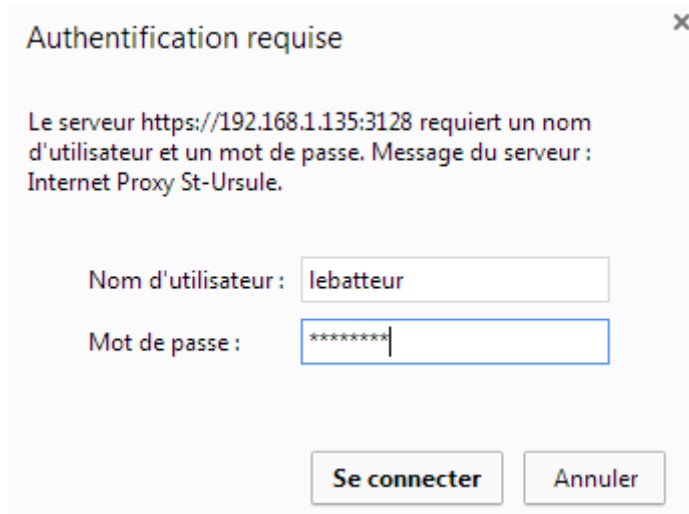
Puis les règles d'ACL et d'http\_access :

```
acl ldap-auth proxy_auth REQUIRED
http_access allow ldap-auth
```

Enfin, ajouter ces 4 lignes en fin de fichier qui vont permettre à l'utilisateur proxy de faire des requêtes sur le serveur et créer un emplacement de stockage des données et réglage des niveaux :

```
cache_effective_user proxy
cache_effective_group proxy
cache_mem 16 Mb
cache_dir ufs /var/spool/squid3 120 16 128
```

On peut tester dans un navigateur configuré au préalable le bon fonctionnement du proxy



Authentification requise

Le serveur https://192.168.1.135:3128 requiert un nom d'utilisateur et un mot de passe. Message du serveur : Internet Proxy St-Ursule.

Nom d'utilisateur : lebatteur

Mot de passe : \*\*\*\*\*

Se connecter Annuler

## VI. Installation, Configuration et phase de Test de SquidGuard

Pour utiliser SquidGard, il faut installer apache2 avant :

```
apt-get install apache2 squidguard
```

L'université de Toulouse diffuse une liste noire d'URL afin de permettre un meilleur contrôle de l'utilisation d'Internet. C'est cette liste noire que je vais utiliser dans mon contexte.

A la fin du fichier squid.conf, j'ai ajouté ces lignes qui redirigent Squid et le nombre de processus engendré (SQUIDLAB est le nom de ma machine) :

```
url_rewrite_program /usr/bin/squidGuard
url_rewrite_children 5
visible_hostname SQUIDLAB
```

Enfin, on configure le fichier squidguard.conf situé dans /etc/squidguard comme suit (ici, on interdit les sites de jeux) :

```

GNU nano 2.2.6      Fichier : squidGuard.conf
dbhome /var/lib/squidguard/db/blacklists _
logdir /var/log/squid3/
src lan {
    ip 192.168.1.0-192.168.1.100
}
dest games {
    domainlist games/domains
    urllist games/urls
}
dest local {
}
acl {
    lan {
        pass !games all
        redirect http://127.0.0.1/proxy.html
    }
    default {
        pass local none
    }
}

```

Ainsi dans un navigateur, on ne peut aller sur le site [www.games.com](http://www.games.com):



## VII. Installation de LightSquid

Pour approfondir mon contexte, j'ai installé Lightsquid qui est un analyseur de log SQUID open source écrit en perl permettant d'afficher sous forme de page web l'utilisation de son proxy. Avec ce petit logiciel, nous pouvons visualiser les sites les plus utilisés, les sites qui utilisent le plus de bande passante, les utilisateurs qui se sont connectés à ces sites.

Après le téléchargement et l'installation de LightSquid, nous pouvons l'utiliser dans un navigateur web :

