

Nom	Prénom	Distribution	Version
Divaret	Nathan	Debian 8.5	1.0

Intégration de SQUID3

SOMMAIRE

Contenu

1) Objectif	2
2) Prérequis	2
3) Intégration de la machine au domaine Active Directory	2
4) Installation des paquets nécessaires.....	2
5) Synchronisation de l'heure locale	3
6) Configuration de Kerberos	3
7) Configuration de Samba	4
8) Rejoindre le domaine	5

Nom	Prénom	Distribution	Version
Divaret	Nathan	Debian 8.5	1.0

1) Objectif

Dans cette procédure, nous allons voir comment configurer le serveur proxy pour qu'il puisse rejoindre et donc intégrer l'Active Directory.

2) Prérequis

- ➔ Un réseau Windows
- ➔ Un contrôleur de domaine sous Windows server
- ➔ Un domaine Active Directory
- ➔ Une machine sous Debian

3) Intégration de la machine au domaine Active Directory

Pour cela, nous donnerons des noms à certains éléments comme suit :

- Le nom du domaine, s'appellera ici **GSB.local** ;
- Le nom du DC (Contrôleur de domaine), s'appellera ici **LABANNU1** ;
- Le compte administrateur du DC, s'appellera ici **Administrateur** ;
- Le nom de la machine Squid s'appellera ici **squid** ;

4) Installation des paquets nécessaires

Pour rejoindre le domaine, il va falloir installer les paquets **samba krb5-user libpam-krb5 ntpdate winbind**.

- **samba** servira à faire le lien entre des machines Linux et Windows ;
- **krb5-user** et **libpam-krb5** sont les bibliothèques liées à Kerberos, le protocole d'authentification utilisé par Active Directory ;
- **ntpdate** permet de synchroniser les horloges machines pour Kerberos ;
- **winbind** est le composant de samba communiquant avec Active Directory.

Lors de l'installation, il se peut que Kerberos demande le nom des KDC (*Kerberos Domain Controler*), qui est généralement le nom du DC

Nom	Prénom	Distribution	Version
Divaret	Nathan	Debian 8.5	1.0

5) Synchronisation de l'heure locale

Ntpdate « adresse de l'Active Directory »

```
root@Proxy:~# ntpdate 192.168.1.130
8 Jun 00:02:09 ntpdate[1789]: adjust time server 192.168.1.130 offset 0.020141
sec
```

6) Configuration de Kerberos

Editer le fichier /etc/krb5.conf et n'y mettre que le contenu suivant :

```
[logging]
    default = FILE:/var/log/krb5libs.log
    kdc = FILE:/var/log/krb5kdc.log
    admin_server = FILE:/var/log/kadmind.log

[libdefaults]
    default_realm = GSB.LOCAL
    dns_lookup_realm = false
    dns_lookup_kdc = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
```

```
[realms]
    GSB.LOCAL = {
        kdc = labannu1.GSB.local
        admin_server = labannu1.GSB.local
        default_domain = GSB.local
    }
```

```
[domain_realm]
    .gsb.local = GSB.LOCAL
    gsb.local = GSB.LOCAL
    .media.mit.edu = MEDIA-LAB.MIT.EDU
    media.mit.edu = MEDIA-LAB.MIT.EDU
    .csail.mit.edu = CSAIL.MIT.EDU
    csail.mit.edu = CSAIL.MIT.EDU
    .who.i.edu = ATHENA.MIT.EDU
    whoi.edu = ATHENA.MIT.EDU
    .stanford.edu = stanford.edu
    .slac.stanford.edu = SLAC.STANFORD.EDU
    .toronto.edu = UTORONTO.CA
    .utoronto.ca = UTORONTO.CA
```

Remarque : Ne toucher pas au reste du fichier, les lignes seront ignoré.

Nom	Prénom	Distribution	Version
Divaret	Nathan	Debian 8.5	1.0

Maintenant, tester vos paramètres Kerberos en lançant la commande :

```
root@Proxy:~# kinit administrateur
Password for administrateur@GSB.LOCAL:
```

Et entrer le mot de passe du compte administrateur du DC. Si cela ne fonctionne toujours pas, redémarrer votre machine et reprenez la ligne.

Pour voir les tickets Kerberos en cache **klist** :

7) Configuration de Samba

Avant de procéder à cette étape, arrêter temporairement les services Winbind et Samba :

- ➔ /etc/init.d/winbind stop
- ➔ /etc/init.d/samba stop

Éditer le fichier **/etc/samba/smb.conf**, et n'y mettre **que** le contenu suivant :

```
[global]
workgroup = GSB
netbios name = Proxy
server string = Proxy
load printers = no
log file = /var/log/samba/log.%m
max log size = 150
password server = labannu1.gsb.local
realm = gsb.local
security = ADS
winbind separator = /
encrypt passwords = yes
winbind cache time = 15
winbind enum users = yes
winbind enum groups = yes
winbind use default domain = yes
idmap uid = 10000-20000
idmap gid = 10000-20000
idmap uid = 10000-20000
idmap gid = 10000-20000
local master = no
os level = 223
domain master = no
preferred master = no

## Browsing/Identification ###
# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = GSB
```

Remarque : N'oubliez pas le workgroup à la fin.

Nom	Prénom	Distribution	Version
Divaret	Nathan	Debian 8.5	1.0

Redémarrer les services

- ➔ /etc/init.d/winbind start
- ➔ /etc/init.d/samba start

8) Rejoindre le domaine

Rejoindre le domaine avec la commande suivante :

```
root@Proxy:~# net ads join -U administrateur
Enter administrateur's password:
```

Si vous obtenez le message suivant :

*The workgroup in smb.conf does not match the short domain name obtained from the server.
Using the name [AUTRE_DOMAINE] from the server.
You should set "workgroup = AUTRE_DOMAINE" in smb.conf*

Alors modifier votre **/etc/samba/smb.conf** comme dit, puis redémarrer les services Samba et Winbind et recommencer.

- Si vous récupérez l'erreur suivante :

ads_connect: No logon servers

C'est que vous n'avez pas installé ou démarré Winbind.

On peut voir que le proxy rejoint bien l'Active Directory.

```
root@Proxy:~# net ads testjoin
Join is OK
```

Nom	Prénom	Distribution	Version
Divaret	Nathan	Debian 8.5	1.0

On peut récupérer les utilisateurs avec la commande `wbinfo -u`

```
_modele_communicatio
_modele_rédaction
_modele_laborecherch
taccueil
adauvilaire
amariette
sdetroz
ahirbec
lletort
aarchambault
pbihel
bettori
adupont
jbbecquet
vsabine
ndivaret
cdubois
ofsense
owncloudadmin
leoletort
testsync
test_situationp
ad_letort
ad_dauvilaire
```