Authentification proxy depuis un annuaire LDAP

1 - Prérequis

Serveur squid fonctionnel

Les paquets suivants

```
apt install samba krb5-user libpam-krb5 ntpdate winbind -y
```

Synchronisation de l'heure

```
ntpdate <IPServeurAD>
```

2 - Configuration de krb5

```
nano /etc/krb5.conf
```

Remplacer tout le contenu par :

```
[realms]
      <DOMAINE.DC> = {
                  kdc = <FQDN AD>
                  admin_server = <FQDN AD>
                  default_domain = <DOMAINE.DC>
                  }
[domain_realm]
      .<domaine.dc> = <DOMAINE.DC>
      <domaine.dc> = <DOMAINE.DC>
```

Test de la liaison

```
kinit Administrateur
```

Théo PERDIGON

Voir les tickets de Kerberos en cache

```
klist
```

3 - Configuration de samba

```
nano /etc/samba/smb.conf

[global]
  workgroup = <DOMAINE>
  realm = <DOMAINE.DC>
  security = ads
  encrypt passwords = yes

  password server = <FQDN AD>

  idmap uid = 10000-20000
  idmap gid = 10000-20000
  winbind offline logon = false
  winbind enum groups = yes
  winbind enum users = yes
  winbind use default domain = yes

[homes]
comment = Home Directories
browseable = no
writable = yes
```

```
nano /etc/nsswitch.conf
passwd:           compat winbind
group:            compat winbind
shadow:           compat winbind
gshadow:          compat winbind
#files winbind

hosts:            files dns
#myhostname
networks:         files

protocols:        db winbind
services:         db winbind
ethers:           db winbind
rpc:              db windbind
```

```
#files winbind

netgroup:         nis
```

Démarrage des services Samba et Winbind

```
/etc/init.d/samba start
/etc/init.d/winbind start
```

Rejoindre le domaine

```
net join -U Administrateur
```

4 - Configuration de Squid

```
visible_hostname PROXY

# Sites bloqués
url_rewrite_program /usr/bin/squidGuard -c
/etc/squidguard/squidGuard.conf

# AD
auth_param ntlm program /usr/bin/ntlm_auth
--helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 5

auth_param basic program /usr/bin/ntlm_auth
--helper-protocol=squid-2.5-basic
auth_param basic children 5
auth_param basic realm Squid AD
auth_param basic credentialsttl 2 hours

acl ntlm proxy_auth REQUIRED

# ACL pour le réseau
acl lan src <Réseau>
http_access allow ntlm
http_access allow lan
http_access deny all

append_domain .<domaine.dc>
```

```
forwarded_for off

# Utilisateur faisant les requêtes sur le serveur
cache_effective_user proxy
cache_effective_group proxy
cache_effective_group winbindd_priv
```

Démarrage de Squid

```
systemctl squid reload
```