

UNIVERSITÉ CHEIKH ANTA DIOP DE DAKAR

École Supérieure Polytechnique



ECOLE SUPERIEURE
POLYTECHNIQUE

Configuration DNS et Couplage Kerberos/LDAP

Présenté par :

Salif BIAYE

Ndeye Astou DIAGOURAGA

Sous la direction de :

Dr Keba

Enseignant

Année universitaire 2024-2025

Table des Matières

I. Configuration DNS

I.1. Introduction

I.2. Configuration Serveur

I.3. Tests et Validation

II. Couplage Kerberos/LDAP

II.1. Configuration LDAP

II.2. Intégration Kerberos

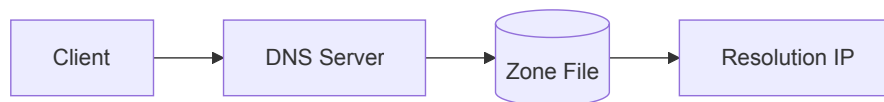
II.3. Tests d'Intégration

III. Conclusion

I. Configuration du Serveur DNS

I.1. Introduction

Ce rapport présente les étapes pour configurer un serveur DNS (Domain Name System) pour le domaine [smarttech.sn](#). La configuration du DNS est cruciale pour permettre la résolution des noms de domaine vers les adresses IP, facilitant ainsi l'accès aux services associés à ce domaine.



Avant de commencer la configuration du serveur DNS, il est essentiel de remplir les pré-requis suivants :

- Disposer d'un serveur DNS fonctionnel (par exemple, [BIND](#) sous Linux).
- Un domaine enregistré ([smarttech.sn](#)).
- Des droits administratifs sur le serveur DNS.
- Un fichier de zone pour le domaine [smarttech.sn](#).

I.2. Configuration du Serveur

✍ Pour installer bind (le serveur dns le plus couramment utilisé), on exécute les commandes suivantes sur un système ubuntu :

```
sudo apt update
sudo apt install bind9 bind9utils bind9-doc
```

Le fichier [named.conf](#) est utilisé pour configurer BIND et définir les zones de DNS. Ce fichier se trouve généralement dans le répertoire [/etc/bind/](#). Ajoutez la configuration suivante pour inclure la zone [smarttech.sn](#) :

```
zone "smarttech.sn" {
    type master;
    file "/etc/bind/db.smarttech.sn";
};
```

Le fichier de zone contient les enregistrements DNS pour le domaine. On crée un fichier [/etc/bind/db.smarttech.sn](#) avec le contenu suivant :

```

TTL      86400
@        **IN**      **SOA**      kdc.smarttech.sn. admin.smarttech.sn. (
                               20250303 ; Serial          3600 ; Refres
@        **IN**      **NS**      kdc.smarttech.sn.kdc      **IN**      **A**      192.168.1.201

www      **IN**      **A**      192.168.1.200
mail     **IN**      **A**      192.168.1.201 ; Enregistrement A pour mail

@        IN          MX          10 mail.smarttech.sn. ; Enregistrement MX pour le serveur c

```

- **SOA (Start of Authority)** : Indique les informations de base sur la zone.
- **NS (Name Server)** : Définit les serveurs DNS autoritaires pour le domaine.
- **A (Address)** : Associe des noms d'hôtes à des adresses IP.
- **MX (Mail Exchanger)** : Pour la gestion des emails.

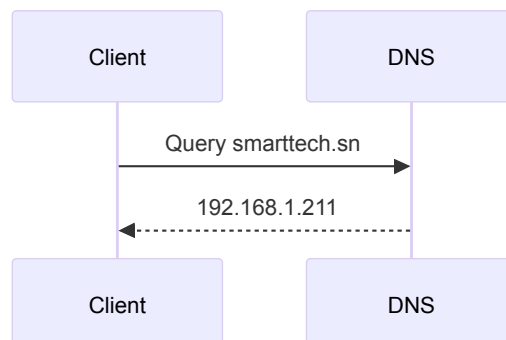
I.3. Validation DNS

Une fois les configurations effectuées, redémarrez le service BIND pour appliquer les modifications :

```
sudo systemctl restart bind9
```

Vérifiez que le serveur DNS fonctionne correctement en utilisant des outils comme **dig** ou **nslookup** :

```
dig @localhost smarttech.sn
nslookup mail.smarttech.sn
```



✎ On obtient ce qui suit:

```
root@server:/home/server# dig @localhost smarttech.sn

; <<>> DiG 9.18.30-0ubuntu0.22.04.2-Ubuntu <<>> @localhost smarttech.sn
; (1 server found)

;; global options: +cmd
;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1894
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags: udp: 1232
;; COOKIE: 2fcc35a089dbda54010000067c5b8ca05c24d5c69afd507 (good)

;; QUESTION SECTION:
;smarttech.sn.                IN      A

;; AUTHORITY SECTION:
smarttech.sn.                 604800 IN      SOA      kdc.smarttech.sn. admin.smarttech.sn.

;; Query time: 274 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Mon Mar 03 14:12:26 GMT 2025
```

✎ On peut aussi faire un nslookup pour verifier

```
root@server:/home/server# nslookup kdc.smarttech.sn
Server:                127.0.0.53
Address:               127.0.0.53#53

Name:   kdc.smarttech.sn
Address: 192.168.1.211

Name:   kdc.smarttech.sn
Address: fd00::ae77:529b:c27d:59db

Name:   kdc.smarttech.sn
Address: fd00::eb47:b1a2:2d20:e082

Name:   kdc.smarttech.sn
Address: fe80::989c:7743:7e28:7163

root@server:/home/server#
```

```
root@server:/home/server# named-checkzone smarttech.sn /etc/bind/db.smarttech.sn
zone smarttech.sn/IN: loaded serial 20250303
OK
```

La configuration du serveur DNS pour le domaine [smarttech.sn](#) assure une résolution correcte des noms de domaine et une gestion efficace des services réseau. Cependant, pour renforcer la sécurité, il est essentiel d'intégrer [Kerberos](#), un protocole d'authentification centralisée. Tandis que le DNS garantit l'accès aux ressources, [Kerberos](#) assure que seules les entités authentifiées peuvent y accéder. Cette transition permet de sécuriser les communications et d'assurer un contrôle d'accès solide au sein de notre réseau.

II. Intégration Kerberos/LDAP

Introduction

Kerberos et LDAP sont deux technologies essentielles dans les environnements d'entreprise pour assurer une authentification centralisée et sécurisée. LDAP (Lightweight Directory Access Protocol) est un protocole utilisé pour accéder et gérer un annuaire d'utilisateurs, tandis que Kerberos est un protocole d'authentification sécurisé basé sur un système de tickets.

Le couplage de Kerberos et LDAP permet d'utiliser LDAP comme base d'annuaire centralisée et d'exploiter Kerberos pour authentifier nos utilisateurs de manière sécurisée.

Objectif du couplage

L'intégration de Kerberos avec LDAP vise à :

- Centraliser la gestion des utilisateurs et des mots de passe.
- Sécuriser l'authentification avec Kerberos.
- Faciliter l'administration des accès réseau.
- Permettre l'authentification unique (SSO - Single Sign-On).

Prerequis

Avant de procéder à l'installation et à la configuration, il est nécessaire de disposer :

- D'un serveur Linux (Ubuntu dans notre cas).
- Des paquets `krb5-kdc`, `krb5-admin-server`, `krb5-user` pour Kerberos.
- D'un serveur LDAP fonctionnel (ex : OpenLDAP).
- Des paquets `libnss-ldap`, `libpam-krb5`, `krb5-config`, `krb5-user` pour l'intégration LDAP-Kerberos.

Remarque:

- notre nom de domaine est `smarttech.sn`
- l'adresse IP de notre serveur est `192.168.1.211`
- le hostname de notre machine `kdc.smarttech.sn`

II.1. Configuration LDAP

Nous allons installer le serveur OpenLDAP sur le même hôte que le KDC, afin de simplifier la communication entre eux.

Installation des paquets nécessaires

```
sudo apt install krb5-kdc-ldap krb5-admin-server
```

Extraction du fichier `kerberos.schema.gz`

`kerberos.schema.gz` contient la définition des objets et attributs nécessaires pour stocker des informations Kerberos dans un annuaire LDAP.

```
sudo cp /usr/share/doc/krb5-kdc-ldap/kerberos.schema.gz /etc/ldap/schema/  
sudo gunzip /etc/ldap/schema/kerberos.schema.gz
```

✍ Ajout du schema kerberos dans l'arborescence

Le fichier schema doit etre converti au format ldif avant de pouvoir etre ajoute. Pour cela on installe:

```
sudo apt install schema2ldif
```

✍ Pour importer le schéma kerberos, on execute:

```
$ sudo ldap-schema-manager -i kerberos.schema  
SASL/EXTERNAL authentication started  
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth  
SASL SSF: 0executing 'ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/kerberos.  
SASL/EXTERNAL authentication started  
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth  
SASL SSF: 0**adding** new entry "cn=kerberos,cn=schema,cn=config"
```

✍ Indexons un attribut souvent utilisé dans les recherches

```
$ sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// <<EOF  
dn: olcDatabase={1}mdb,cn=config  
add: olcDbIndex  
olcDbIndex: krbPrincipalName eq,pres,sub  
EOF  
modifying entry "olcDatabase={1}mdb,cn=config"
```

✍ Creation des entrees ldap pour les entrees administratives kerberos

```
**$ ldapadd -x -D cn=admin,dc=smarttech,dc=sn -W <<EOF  
dn: uid=kdc-service,dc=smarttech,dc=sn  
uid: kdc-service  
objectClass: account  
objectClass: simpleSecurityObject  
userPassword: {CRYPT}x  
description: Account used for the Kerberos KDC  
  
dn: uid=kadmin-service,dc=smarttech,dc=sn  
uid: kadmin-service  
objectClass: account  
objectClass: simpleSecurityObject  
userPassword: {CRYPT}x  
description: Account used for the Kerberos Admin server  
EOF  
Enter LDAP Password:  
adding new entry "uid=kdc-service,dc=smarttech,dc=sn"  
  
adding new entry "uid=kadmin-service,dc=smarttech,dc=sn"**
```

✍ On va ensuite devenir un mot de passe pour chaque entree: kdc service et kadmin service


```
$ ldapasswd -x -D cn=admin,dc=smarttech,dc=sn -W -S uid=kdc-service,dc=smarttech,dc=sn
**New** password:*****Re-enter **new** password:*****
Enter LDAP Password: *****
```

 Mise a jour des listes de controle d'accès acl

```
**$ sudo ldapmodify -Q -Y EXTERNAL -H ldapi:/// <<EOF
dn: olcDatabase={1}mdb,cn=config
add: olcAccess
olcAccess: {2}to attrs=krbPrincipalKey by anonymous auth by dn.exact="uid=kdc-service,dc=smarttech,dc=sn" read by dn.exact="uid=kadmin-se
-
add: olcAccess
olcAccess: {3}to dn.subtree="cn=krbContainer,dc=smarttech,dc=sn" read by dn.exact="uid=kadmin-se
EOF

modifying entry "olcDatabase={1}mdb,cn=config"
```

Notre annuaire LDAP est maintenant prêt à servir de base de données principale Kerberos.

LDAP


dc=smarttech
dc=sn
ou=Users
krbPrincipalName

II.2. Configuration Kerberos

 Editons le fichier /etc/krb5.conf

```
**[realms]
EXAMPLE.COM = {
    kdc = kdc.smarttech.sn
    admin_server = kdc.smarttech.sn
    default_domain = smarttech.sn
    database_module = openldap_ldapconf
}
```

```
[dbdefaults]
    ldap_kerberos_container_dn = cn=krbContainer,dc=smarttech,dc=sn
[dbmodules]
    openldap_ldapconf = {
        db_library = kldap
        disable_last_success = true
        disable_lockout = true
        ldap_kdc_dn = "uid=kdc-service,dc=smarttech,dc=sn"
        ldap_kadmin_dn = "uid=kadmin-service,dc=smarttech,dc=sn"
        ldap_service_password_file = /etc/krb5kdc/service.keyfile
        ldap_servers = ldapi:///
        ldap_conns_per_server = 5
    }
```

 Créer le domaine avec kdb5_ldap_util

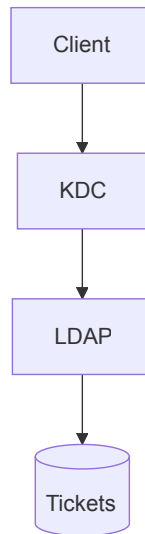
```
$ sudo ldap-schema-manager -i kerberos.schema
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0executing 'ldapadd -Y EXTERNAL -H ldapi:///
-f /etc/ldap/schema/kerberos.ldif'
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0**adding** new entry "cn=kerberos,cn=schema,cn=config"
```

 Créons les mots de passe pour chacun

```
sudo kdb5_ldap_util -D cn=admin,dc=smarttech,dc=sn stashesrvpw
-f /etc/krb5kdc/service.keyfile uid=kdc-
service,dc=smarttech,dc=sn
sudo kdb5_ldap_util -D cn=admin,dc=smarttech,dc=sn stashesrvpw
-f /etc/krb5kdc/service.keyfile uid=kadmin-
service,dc=smarttech,dc=sn**
```

 Redémarrage des services

```
sudo systemctl start krb5-kdc.service
sudo systemctl start krb5-admin-server.service
```



II.3. Tests d'Intégration

Testons l'authentification kerberos LDAP avec Kerberos
Créons un utilisateur dans kerberos avec

```
sudo kadmin.local -q "addprinc salif@SMARTTECH.SN"
```

Vérifions si le principal est dans ldap avec la commande:

```
ldapsearch -x -D "cn=admin,dc=smarttech,dc=sn" -W  
-b "dc=smarttech,dc=sn"
```

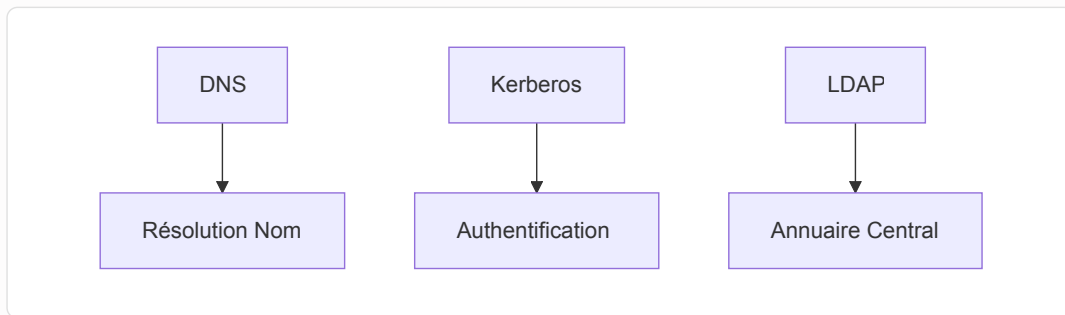
On peut voir avec la capture suivante que l'utilisateur salif a été ajouté dans ldap

```
# salif@SMARTTECH.SN, SMARTTECH.SN, krbContainer, smarttech.sn  
dn: krbPrincipalName=salif@SMARTTECH.SN,cn=SMARTTECH.SN,cn=krbContainer,dc=smarttech,dc=sn  
krbLoginFailedCount: 0  
krbPrincipalName: salif@SMARTTECH.SN  
krbPrincipalKey:: MIG20AMCAQGhAwIBAAIDAQEBowMCAQKgZ8wgZwwVKAHMAWgAwIBAKFJMEegAwIBEA  
krbLastPwdChange: 20250303084201Z  
krbExtraData:: AAJZa8Vncm9vdC9hZG1pbkBTUUFVSFRFRQ0gUU04A  
krbExtraData:: AAg8AA==  
objectClass: krbPrincipal  
objectClass: krbPrincipalAux  
objectClass: krbTicketPolicyAux  
  
# host/kdc.smarttech.sn@SMARTTECH.SN, SMARTTECH.SN, krbContainer, smarttech.sn
```

III. Conclusion

L'intégration de **Kerberos** avec **LDAP** offre une solution robuste pour la gestion centralisée des identités et l'authentification sécurisée des utilisateurs. En exploitant **LDAP** comme annuaire de stockage des identités et **Kerberos** comme mécanisme d'authentification, cette architecture permet de garantir une **sécurité renforcée**, une **administration simplifiée** et une **expérience utilisateur améliorée** grâce au Single Sign-On (SSO).

Cette architecture combinant DNS, Kerberos et LDAP permet :



- Gestion centralisée des identités
- Sécurité renforcée avec tickets Kerberos
- Single Sign-On (SSO)