



**ÉCOLE SUPÉRIEURE POLYTECHNIQUE DE DAKAR**  
**DÉPARTEMENT GÉNIE INFORMATIQUE**

**GÉNIE LOGICIEL ET SYSTÈMES D'INFORMATION**

**Module SERVICES RESEAUX**

**Projet de fin de module :**  
**Mise en place d'une infrastructure réseau centralisée et avancée avec ToIP**

**Présenté par :**  
**Ndeye Ndella DIOP**  
**Sokhna Diarra DIOP**  
**Japhet Mokoumbou**  
**Aissata SY**

**Master 1 GLSI**

<u>Introduction</u> .....	1
I. <u>Conception de l'architecture réseau</u> .....	2
II. <u>Déploiement des services</u> .....	3
1. <u>Ldap/Kerberos</u> .....	3
a. <u>LDAP</u> .....	3
b. <u>KERBEROS</u> .....	6
c. <u>Intégration LDAP/Kerberos</u> .....	9
d. <u>Automatisation de la création de LDAP</u> .....	18
2. <u>Freeradius</u> .....	22
3. <u>Samba</u> .....	26
4. <u>Messagerie avancée avec iRedMail</u> .....	33
5. <u>DNS avancé</u> .....	54
6. <u>Accès distant</u> .....	60
a. <u>SSH</u> .....	60
b. <u>RDP</u> .....	62
c. <u>NoVNC</u> .....	63
7. <u>TFTP/FTP</u> .....	65
a. <u>TFTP</u> .....	65
b. <u>FTP</u> .....	67
8. <u>Téléphonie sur IP (ToIP)</u> .....	68
<u>Conclusion</u> .....	75

## **INTRODUCTION**

Dans un monde où la gestion des services réseau est de plus en plus complexe, les entreprises recherchent des solutions centralisées et sécurisées pour gérer les accès, les utilisateurs et les services de communication. L'entreprise SmartTech souhaite mettre en place une infrastructure réseau moderne intégrant plusieurs services.

L'objectif est de **concevoir, déployer et sécuriser** une infrastructure réseau complète, en mettant en place **une gestion centralisée des utilisateurs** et une **authentification unique**, tout en intégrant des services de communication avancés tels que la **téléphonie IP (ToIP)**.

L'architecture repose sur plusieurs machines virtuelles interconnectées via un **switch** et un **routeur**, offrant une infrastructure modulaire et scalable. Chaque machine est dédiée à une fonction spécifique :

- **Machine1** : Gère l'authentification et les services réseau via **LDAP/Kerberos, DNS, FreeRADIUS et Samba**.
- **Machine2** : Assure la communication avec une **messagerie iRedMail**, du **WebRTC** et du **XMPP** pour les échanges en temps réel.
- **Machine3** : Fournit les services d'**accès distant** et le stockage via **FTP/TFTP**.
- **Machine4** : Implémente une **solution de téléphonie sur IP (ToIP)** avec **Asterisk**.

Ces services sont interconnectés par un **switch central**, relié à un **routeur** qui assure l'accès à un **point d'accès Wi-Fi** et à **Internet**.

L'objectif est de créer un environnement fonctionnel, simulant une infrastructure réseau d'entreprise avec une authentification centralisée, une communication sécurisée et une gestion des accès optimisée.

## **I. Conception de l'architecture réseau :**

L'architecture réseau mise en place repose sur une infrastructure modulaire et sécurisée intégrant plusieurs services critiques pour assurer l'authentification, la communication et la gestion des accès au sein du système. Elle est composée de quatre machines virtuelles, un switch, un routeur, un point d'accès Wi-Fi et une connexion vers Internet.

### **Machine 1 : Service d'authentification et de gestion réseau**

La **première machine** joue un rôle central dans la sécurité et l'administration des utilisateurs du réseau. Elle embarque plusieurs services :

- **LDAP/Kerberos** : Gestion centralisée des identités et authentification sécurisée.
- **DNS** : Service de résolution de noms pour assurer une connectivité fluide entre les machines.
- **FreeRADIUS** : Authentification et contrôle d'accès, notamment pour les connexions Wi-Fi via le point d'accès.
- **Samba** : Partage de fichiers et gestion des ressources réseau pour les utilisateurs authentifiés.

Cette machine agit comme **serveur d'authentification**, garantissant que seuls les utilisateurs autorisés peuvent accéder aux ressources du réseau.

### **Machine 2 : Messagerie et communication en temps réel**

La **deuxième machine** est dédiée aux services de communication et de collaboration :

- **iRedMail** : Fournit un serveur de messagerie sécurisé.
- **WebRTC** : Permet la communication en temps réel via voix et vidéo.
- **XMPP** : Protocole de messagerie instantanée, utilisé pour les échanges entre utilisateurs internes.

Elle assure une communication **sécurisée et fluide** entre les membres du réseau, notamment grâce aux protocoles chiffrés de messagerie et d'appel.

### **Machine 3 : Accès distant et gestion des fichiers**

La **troisième machine** est conçue pour **faciliter l'accès distant et le transfert de fichiers** :

- **Accès distant** : Permet aux utilisateurs d'accéder au réseau à distance via VPN ou SSH.
- **FTP/TFTP** : Services de transfert de fichiers, notamment pour le stockage de configurations et d'images système.

Elle joue un rôle **essentiel pour la maintenance et la gestion des équipements** du réseau, notamment les mises à jour et la configuration des machines.

### **Machine 4 : Téléphonie sur IP (VoIP)**

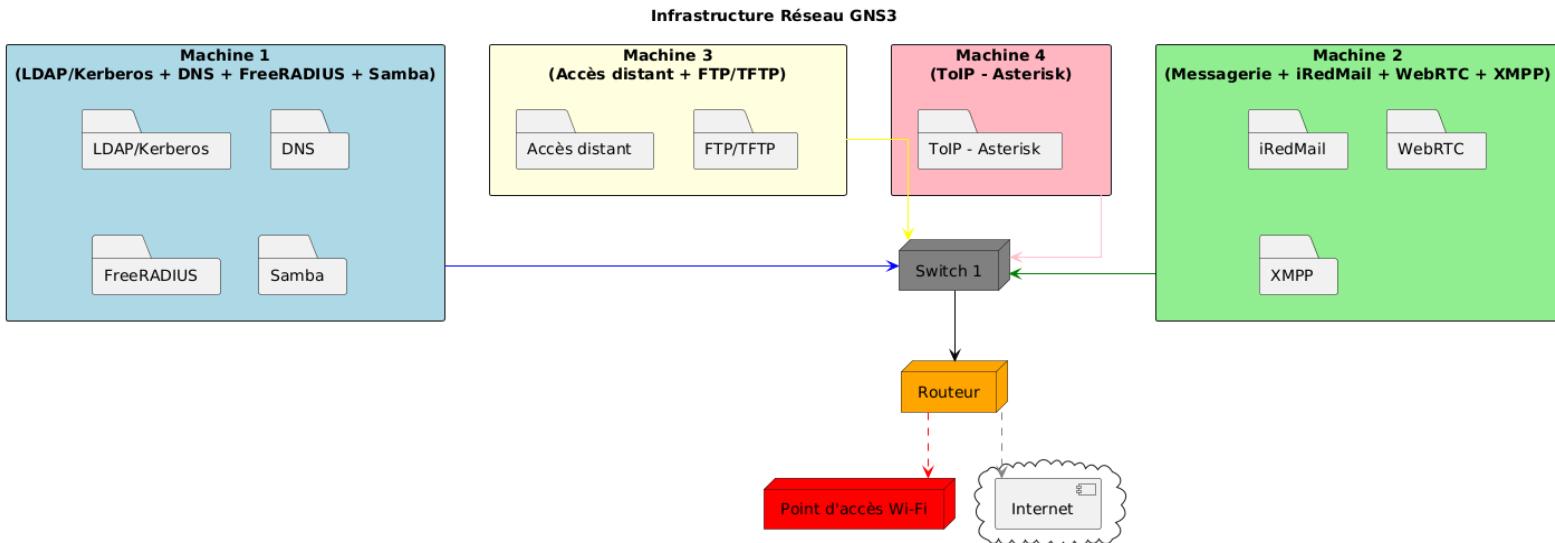
La **quatrième machine** est dédiée à la **téléphonie IP** via **Asterisk**, un serveur permettant de :

- Gérer les **appels internes et externes**.
- Offrir des **services avancés** (messagerie vocale, transfert d'appel, conférences).

Ce serveur assure la communication téléphonique entre les postes du réseau, optimisant la collaboration et la réactivité des utilisateurs.

### **Infrastructure réseau : Connectivité et sécurité**

- **Switch 1** : Relie l'ensemble des machines et assure la **communication locale**.
- **Routeur** : Gère l'interconnexion avec le réseau externe et applique des **règles de sécurité**.
- **Point d'accès Wi-Fi** : Permet la connexion des utilisateurs mobiles via une authentification sécurisée par **FreeRADIUS**.
- **Internet** : L'accès au réseau mondial est contrôlé via le routeur, qui peut appliquer des **politiques de filtrage et de sécurité**.



**Titre :** Schéma détaillé de l'infrastructure avec les services déployés.

## **II. Déploiement des services :**

### **1. LDAP/Kerberos:**

Dans un environnement réseau, la gestion des utilisateurs et de leurs accès est essentielle pour garantir la sécurité et la cohérence des authentications. LDAP (Lightweight Directory Access Protocol) et Kerberos sont deux technologies complémentaires utilisées pour la gestion centralisée des utilisateurs.

L'association de LDAP et Kerberos permet une gestion centralisée robuste :

- LDAP stocke les informations des utilisateurs et des groupes.
- Kerberos gère l'authentification sécurisée sans exposer les mots de passe.
- Ensemble, ils permettent un Single Sign-On (SSO), où un utilisateur se connecte une seule fois et accède à plusieurs services sans devoir resaisir ses identifiants.

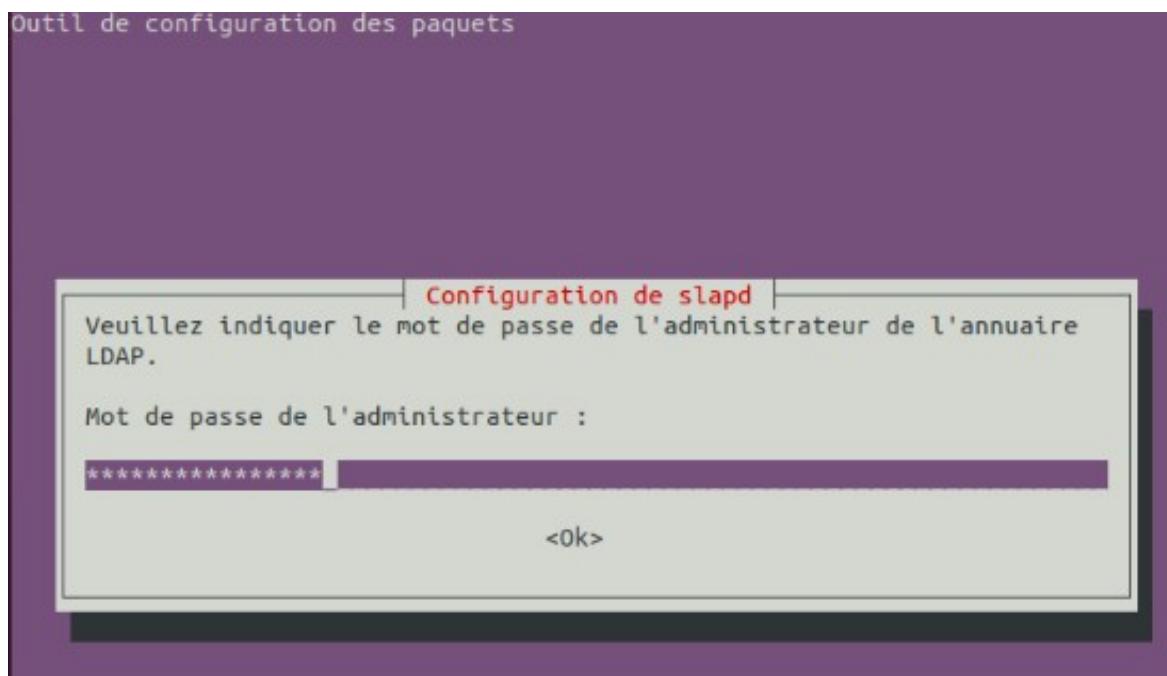
#### **a. LDAP:**

- **Installation d'OpenLDAP et Configuration :**

On commence par installer OpenLDAP sur un serveur Ubuntu par la commande : **apt install slapd ldap-utils**. Pendant l'installation, un mot de passe administrateur LDAP sera demandé :

Nom de domaine : smarttech.sn

On va reconfigurer OpenLDAP pour s'assurer qu'il est bien paramétré par la commande :**sudo dpkg-reconfigure slapd** .



Testons si le serveur LDAP fonctionne bien :

```
ubuntu@ndella:~$ sudo systemctl status slapd
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access >
   Loaded: loaded (/etc/init.d/slapd; generated)
   Drop-In: /usr/lib/systemd/system/slapd.service.d
             └─slapd-remain-after-exit.conf
     Active: active (running) since Sat 2025-03-01 13:35:27 UTC; 43s ago
       Docs: man:systemd-sysv-generator(8)
   Process: 7265 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
   Tasks: 3 (limit: 4600)
  Memory: 3.4M (peak: 4.5M)
    CPU: 39ms
   CGroup: /system.slice/slapd.service
           └─7272 /usr/sbin/slapd -h "ldap:/// ldapi://" -g openldap -u openl>

mars 01 13:35:16 ndella systemd[1]: Starting slapd.service - LSB: OpenLDAP standa>
mars 01 13:35:16 ndella slapd[7265]: * Starting OpenLDAP slapd
mars 01 13:35:27 ndella slapd[7271]: @(#) $OpenLDAP: slapd 2.6.7+dfsg-1~exp1ubun>
                                         Ubuntu Developers <ubuntu-devel-dis>
mars 01 13:35:27 ndella slapd[7272]: slapd starting
lines 1-18...skipping...
```

Testons si LDAP fonctionne bien : ldapsearch -x -LLL -D "cn=admin,dc=smarttech,dc=sn" -W -b "dc=smarttech,dc=sn"

```
root@jjk:/home/soxna# ldapsearch -x -LLL -D "cn=admin,dc=smarttech,dc=sn" -W -b
"dc=smarttech,dc=sn"
Enter LDAP Password:
dn: dc=smarttech,dc=sn
objectClass: top
objectClass: dcObject
objectClass: organization
o: smarttech.sn
dc: smarttech

dn: cn=admin,dc=smarttech,dc=sn
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
userPassword:: e1NTSEF9TW9kOS93UkR6UXVZS0Y3TUNRUHBRTFU0OHlsMUMxV2k=
root@jjk:/home/soxna#
```

- **Création d'un fichier base.ldif :**

Nous allons ajouter des utilisateurs à l'annuaire. Ce fichier contient les informations de la structure LDAP.

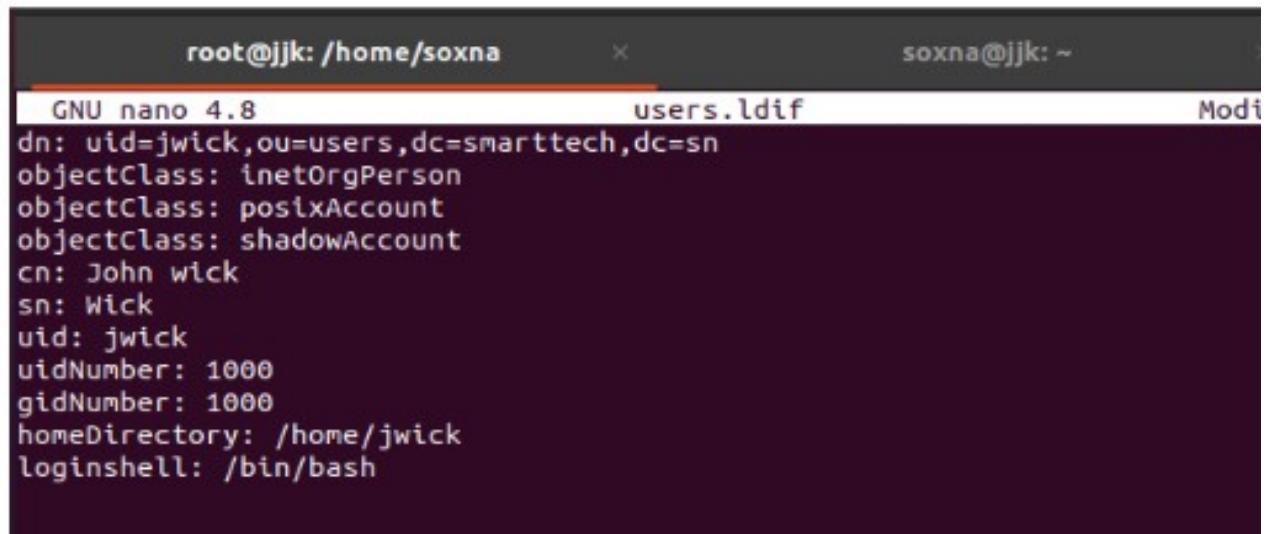
```
GNU nano 7.2                                base.ldif *
dn: ou=people,dc=smarttech,dc=local
objectClass: organizationalUnit
ou: people

dn: ou=groups,dc=smarttech,dc=local
objectClass: organizationalUnit
ou: groups
```

Appliquons les modifications de la manière suivante :

```
ubuntu@ubuntu:~$ ldapadd -x -D "cn=admin,dc=smarttech,dc=local" -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=people,dc=smarttech,dc=local"
adding new entry "ou=groups,dc=smarttech,dc=local"
```

Ajoutons un utilisateur de test :



The screenshot shows a terminal window with two tabs. The left tab is titled 'root@jjk: /home/soxna' and the right tab is titled 'soxna@jjk: ~'. The left tab contains a file named 'users.ldif' which is being edited with 'nano 4.8'. The file contains the following LDAP entry:

```
dn: uid=jwick,ou=users,dc=smarttech,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: John wick
sn: Wick
uid: jwick
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/jwick
loginshell: /bin/bash
```

Ajoutons cet utilisateur à LDAP : ldapadd -x -D "cn=admin,dc=smarttech,dc=sn" -W -f user.ldif

```
root@jjk:/home/soxna# nano users.ldif
root@jjk:/home/soxna# ldapadd -x -D "cn=admin,dc=smarttech,dc=sn" -W -f users.ldif
Enter LDAP Password:
adding new entry "uid=jwick,ou=users,dc=smarttech,dc=sn"
```

Et vérifions qu'il a bien été ajouté :

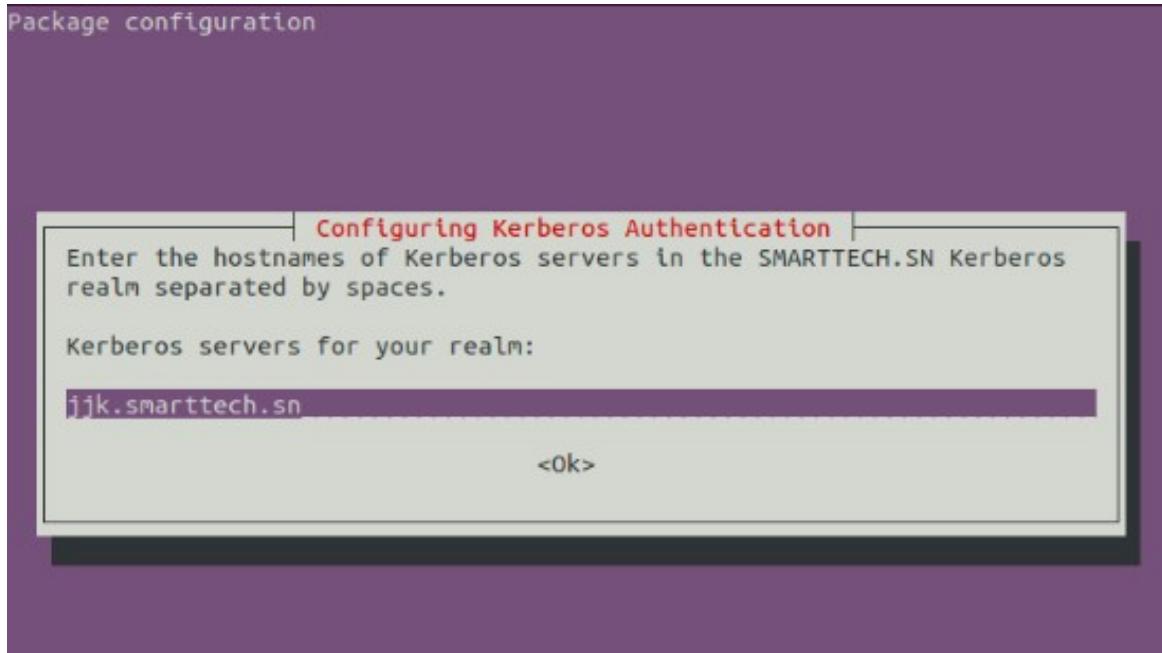
```
root@jjk:/home/soxna# ldapsearch -x -LLL -D "cn=admin,dc=smarttech,dc=sn" -W -b
"dc=smarttech,dc=sn" "(uid=jwick)"
Enter LDAP Password:
dn: uid=jwick,ou=users,dc=smarttech,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
cn: John wick
sn: Wick
uid: jwick
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/jwick
loginShell: /bin/bash

root@jjk:/home/soxna#
```

## b. KERBEROS :

- Installation et Configuration de Kerberos :

Kerberos est utilisé pour l'authentification centralisée. On va installer les paquets nécessaires par la commande : **sudo apt install krb5-kdc krb5-admin-server**



Éditons le fichier /etc/krb5.conf pour vérifier la correspondance à notre domaine :

```
GNU nano 4.8          /etc/krb5.conf
# the enctype is if you have local software that will break on ticket
# caches containing ticket encryption types it doesn't know about (such as
# old versions of Sun Java).

#      default_tgs_enctypes = des3-hmac-sha1
#      default_tkt_enctypes = des3-hmac-sha1
#      permitted_enctypes = des3-hmac-sha1

# The following libdefaults parameters are only for Heimdal Kerberos.
fcc-mit-ticketflags = true

[realms]
    SMARTTECH.SN = {
        kdc = jjk.smarttech.sn
        admin_server = jjk.smarttech.sn
    }
    ATHENA/MIT.EDU = {
        kdc = kerberos.mit.edu
        kdc = kerberos-1.mit.edu
        kdc = kerberos-2.mit.edu:88
        admin_server = kerberos.mit.edu
        default_domain = mit.edu
    }

^G Get Help  ^O Write Out  ^W Where Is  ^K Cut Text  ^J Justify
^X Exit     ^R Read File   ^\ Replace   ^U Paste Text  ^T To Spell
```

- **Initialiser la base de données Kerberos :**

On va initialiser la base de données Kerberos. Cela crée une base de données pour stocker les tickets d'authentification. **sudo krb5\_newrealm**

```
Re-enter KDC database master key to verify:  
kdb5_util: Password mismatch while reading master key from keyboard  
root@jjk:/home/soxna# sudo krb5_newrealm  
This script should be run on the master KDC/admin server to initialize  
a Kerberos realm. It will ask you to type in a master key password.  
This password will be used to generate a key that is stored in  
/etc/krb5kdc/stash. You should try to remember this password, but it  
is much more important that it be a strong password than that it be  
remembered. However, if you lose the password and /etc/krb5kdc/stash,  
you cannot decrypt your Kerberos database.  
Loading random data  
Initializing database '/var/lib/krb5kdc/principal' for realm 'SMARTTECH.SN',  
master key name 'K/M@SMARTTECH.SN'  
You will be prompted for the database Master Password.  
It is important that you NOT FORGET this password.
```

On configure le serveur KDC :

```
GNU nano 4.8                               /etc/krb5kdc/kdc.conf  
[kdcdefaults]  
    kdc_ports = 750,88  
  
[realms]  
    SMARTTECH.SN = {  
        database_name = /var/lib/krb5kdc/principal  
        admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab  
        acl_file = /etc/krb5kdc/kadm5.acl  
        key_stash_file = /etc/krb5kdc/stash  
        kdc_ports = 750,88  
        max_life = 10h 0m 0s  
        max_renewable_life = 7d 0h 0m 0s  
        master_key_type = des3-hmac-sha1  
        #supported_enctypes = aes256-cts:normal aes128-cts:normal  
        default_principal_flags = +preauth  
    }  
}
```

Ajout d'un administrateur Kerberos : sudo kadmin.local -q "addprinc [admin/admin@SMARTTECH.SN](#)". **Définir un mot de passe sécurisé.**

```
root@jjk:/home/soxna# sudo kadmin.local -q "addprinc admin/admin@SMARTTECH.SN"  
Authenticating as principal root/admin@SMARTTECH.SN with password.  
WARNING: no policy specified for admin/admin@SMARTTECH.SN; defaulting to no policy  
Enter password for principal "admin/admin@SMARTTECH.SN":  
Re-enter password for principal "admin/admin@SMARTTECH.SN":  
Principal "admin/admin@SMARTTECH.SN" created.  
root@jjk:/home/soxna#
```

On ajoute le principe de l'utilisateur administrateur au contrôle d'accès. Ajout de la ligne suivante à la fin : **root/admin@SMARTTECH.SN \***

```
Thunderbird Mail /etc/krb5kdc/kadm5.acl Modified
# This file is the access control list for krb5 administration.
# When this file is edited run service krb5-admin-server restart to activate
# One common way to set up Kerberos administration is to allow any principal
# ending in /admin is given full administrative rights.
# To enable this, uncomment the following line:
# */admin *
*/admin@SMARTTECH.SN*
```

Redémarrage de Kerberos :

```
root@jjk:/home/soxna# sudo systemctl restart krb5-kdc krb5-admin-server
root@jjk:/home/soxna# sudo systemctl enable krb5-kdc krb5-admin-server
Synchronizing state of krb5-kdc.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable krb5-kdc
Synchronizing state of krb5-admin-server.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable krb5-admin-server
root@jjk:/home/soxna#
```

On ajoute naruto à Kerberos : Il demandera un mot de passe : **sudo kadmin.local -q "addprinc naruto@SMARTTECH.SN"**

```
root@jjk:/home/soxna# kadmin.local -q "addprinc naruto@SMARTTECH.SN"
Authenticating as principal root/admin@SMARTTECH.SN with password.
WARNING: no policy specified for naruto@SMARTTECH.SN; defaulting to no policy
Enter password for principal "naruto@SMARTTECH.SN":
Re-enter password for principal "naruto@SMARTTECH.SN":
Principal "naruto@SMARTTECH.SN" created.
root@jjk:/home/soxna#
```

Vérifions si naruto peut s'authentifier et affichons le ticket obtenu :

```
root@jjk:/home/soxna# kinit naruto@SMARTTECH.SN
nPassword for naruto@SMARTTECH.SN:
root@jjk:/home/soxna# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: naruto@SMARTTECH.SN

Valid starting      Expires          Service principal
01.03.2025 17:59:44  02.03.2025 03:59:44  krbtgt/SMARTTECH.SN@SMARTTECH.SN
    renew until 02.03.2025 17:59:37
root@jjk:/home/soxna#
```

Pour voir tous les utilisateurs créés : **kadmin.local -q "listprincs"**

```
root@jjk:/home/soxna# kadmin.local -q "listprincs"
Authenticating as principal naruto/admin@SMARTTECH.SN with password.
K/M@SMARTTECH.SN
admin/admin@SMARTTECH.SN
kadmin/admin@SMARTTECH.SN
kadmin/changepw@SMARTTECH.SN
kadmin/jjk.smarttech.sn@SMARTTECH.SN
kiprop/jjk.smarttech.sn@SMARTTECH.SN
krbtgt/SMARTTECH.SN@SMARTTECH.SN
naruto@SMARTTECH.SN
root@jjk:/home/soxna#
```

### c. Intégration LDAP et Kerberos :

Installons les paquets nécessaires :

```
root@jjk:/home/soxna# sudo apt install -y krb5-kdc-ldap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  krb5-kdc-ldap
0 upgraded, 1 newly installed, 0 to remove and 360 not upgraded.
Need to get 85,4 kB of archives.
After this operation, 336 kB of additional disk space will be used.
Get:1 http://sn.archive.ubuntu.com/ubuntu focal-updates/universe amd64 krb5-kdc-
-ldap amd64 1.17-6ubuntu4.8 [85,4 kB]
Fetched 85,4 kB in 1s (121 kB/s)
Selecting previously unselected package krb5-kdc-ldap.
(Reading database ... 179811 files and directories currently installed.)
Preparing to unpack .../krb5-kdc-ldap_1.17-6ubuntu4.8_amd64.deb ...
Unpacking krb5-kdc-ldap (1.17-6ubuntu4.8) ...
Setting up krb5-kdc-ldap (1.17-6ubuntu4.8) ...
Processing triggers for man-db (2.9.1-1) ...
root@jjk:/home/soxna#
```

Si le fichier schema.kdc.ldif n'existe pas, il faut d'abord l'extraire :

```
zcat /usr/share/doc/krb5-kdc-ldap/kerberos.openldap.ldif.gz > /etc/krb5kdc/schema.kdc.ldif
```

```
root@jjk:/home/soxna# zcat /usr/share/doc/krb5-kdc-ldap/kerberos.openldap.ldif.
gz > /etc/krb5kdc/schema.kdc.ldif
root@jjk:/home/soxna# sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/krb5kdc/sch
ema.kdc.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"

root@jjk:/home/soxna#
```

Créons un fichier LDIF et voici le contenu de notre fichier **acl.ldif**:

```

root@jjk: /home/soxna          x      soxna@jjk: ~
GNU nano 4.8                      acl.ldif           Modified
dn: olcDatabase={1}mdb,cn=config
changetype: modify
add: olcAccess
olcAccess: {0}to attrs=userPassword,krbPrincipalKey by self write by dn="cn=admin,dc=smarttech,dc=sn" write
olcAccess: {1}to * by * read

```

```

root@jjk:/home/soxna# nano acl.ldif
root@jjk:/home/soxna# sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f acl.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}mdb,cn=config"
root@jjk:/home/soxna#

```

Configurons Kerberos pour utiliser LDAP sudo nano /etc/krb5kdc/kdc.conf

```

root@JJk: /home/soxna          x      soxna@JJk: ~
GNU nano 4.8                      /etc/krb5kdc/kdc.conf           Modified
database_module = openldap_ldapconf
database_name = /var/lib/krb5kdc/principal
admin_keytab = FILE:/etc/krb5kdc/kadm5.keytab
acl_file = /etc/krb5kdc/kadm5.acl
key_stash_file = /etc/krb5kdc/stash
kdc_ports = 750,88
max_life = 10h 0m 0s
max_renewable_life = 7d 0h 0m 0s
master_key_type = des3-hmac-sha1
#supported_enctypes = aes256-cts:normal aes128-cts:normal
default_principal_flags = +preauth
}

[dbmodules]
openldap_ldapconf = {
    db_library = kldap
    ldap_kerberos_container_dn = "cn=krbContainer,dc=smarttech,dc=sn"
    ldap_kdc_dn = "cn=admin,dc=smarttech,dc=sn"
    ldap_kadmind_dn = "cn=admin,dc=smarttech,dc=sn"
    ldap_service_password_file = /etc/krb5kdc/service.keyfile
    ldap_servers = "ldap://localhost"
}

```

Définir le conteneur Kerberos dans LDAP

Il faut d'abord créer un conteneur LDAP pour Kerberos. Pour cela, crée un fichier krbContainer.ldif :

```
GNU nano 4.8                      krbContainer.ldif
dn: cn=krbContainer,dc=smarttech,dc=sn
objectClass: krbContainer
cn: krbContainer
```

Puis, ajoutons le dans LDAP avec :

```
ldapadd -x -D "cn=admin,dc=smarttech,dc=sn" -W -f krbContainer.ldif
```

```
root@jjk:/home/soxna# sudo nano /etc/krb5kdc/kdc.conf
root@jjk:/home/soxna# nano krbContainer.ldif
root@jjk:/home/soxna# sudo nano /etc/krb5kdc/kdc.conf
root@jjk:/home/soxna# ldapadd -x -D "cn=admin,dc=smarttech,dc=sn" -W -f krbContainer.ldif
Enter LDAP Password:
adding new entry "cn=krbContainer,dc=smarttech,dc=sn"

root@jjk:/home/soxna#
```

Reprendre l'initialisation de la base Kerberos

Maintenant que le conteneur cn=krbContainer,dc=smarttech,dc=sn existe, relance la commande :

```
root@jjk:/home/soxna# sudo kdb5_ldap_util -D cn=admin,dc=smarttech,dc=sn create
  -subtrees dc=smarttech,dc=sn -r SMARTTECH.SN -s
Password for "cn=admin,dc=smarttech,dc=sn":
Initializing database for realm 'SMARTTECH.SN'
You will be prompted for the database Master Password.
It is important that you NOT FORGET this password.
Enter KDC database master key:
Re-enter KDC database master key to verify:
root@jjk:/home/soxna#
```

Vérifier que nsswitch.conf est bien configuré

Si "ldap" n'est pas présent, ajoute-le et redémarre nscd :

```
GNU nano 4.8                      /etc/nsswitch.conf          Modifi
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:      files  systemd  ldap
group:       files  systemd  ldap
shadow:      files   ldap
gshadow:     files
```

Vérifier que libnss-ldapd est installé

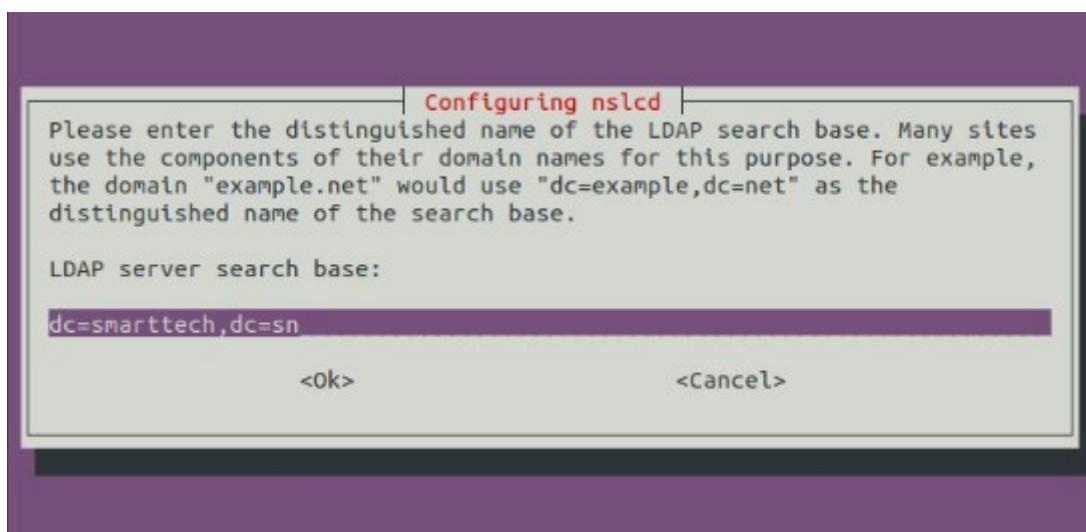
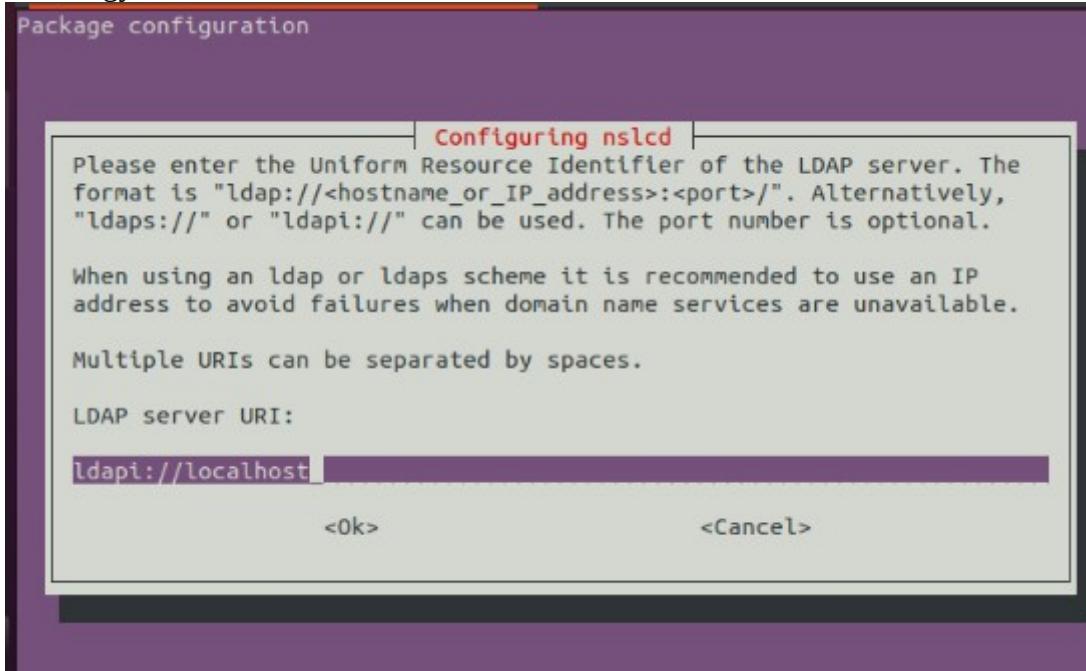
Exécute :

```
dpkg -l | grep nss-ldapd
```

Si c pas le ca installe sudo apt install libnss-ldapd

Mettre ldap://localhost (faut pas mettre le I c une erruer qu'on rectifiera plus tard dans le

## fichier de configuration



Après avoir validé, vérifie /etc/nsswitch.conf et assure-toi qu'il contient ces lignes :

```

GNU nano 4.8                               /etc/nsswitch.conf                         Modified |
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the 'glibc-doc-reference' and 'info' packages installed, try:
# 'info libc "Name Service Switch"' for information about this file.

passwd:        files      systemd    ldap
group:         files      systemd    ldap
shadow:        files      ldap
gshadow:       files

hosts:          files      mdns4_minimal [NOTFOUND=return] dns
networks:      files

protocols:     db   files
services:      db   files
ethers:        db   files
rpc:           db   files

netgroup:       files      ldap
automount:     sss

```

^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify  
^X Exit ^R Read File ^\\ Replace ^U Paste Text ^T To Spell

Puis redémarre nscd et nsLCD :

sudo systemctl restart nscd

sudo systemctl restart nsLCD

Vérifier Kerberos

Maintenant, on va tester l'authentification Kerberos : kadmin.local

```

root@jjk:/home/soxna# kadmin.local
Authenticating as principal naruto/admin@SMARTTECH.SN with password.
kadmin.local: naruto2025
kadmin.local: Unknown request "naruto2025". Type "?" for a request list.
kadmin.local: addprinc japhet
WARNING: no policy specified for japhet@SMARTTECH.SN; defaulting to no policy
Enter password for principal "japhet@SMARTTECH.SN":
Re-enter password for principal "japhet@SMARTTECH.SN":
Principal "japhet@SMARTTECH.SN" created.
kadmin.local: quit
root@jjk:/home/soxna#

```

Vérification LDAP

ldapsearch -x -LLL -H ldap://localhost -b "dc=smarttech,dc=sn" "(objectClass=\*)"

```

# japhet@SMARTTECH.SN, SMARTTECH.SN, krbContainer, smarttech.sn
dn: krbPrincipalName=japhet@SMARTTECH.SN,cn=SMARTTECH.SN,cn=krbContainer,dc=smarttech,dc=sn
  arttech,dc=sn
krbLoginFailedCount: 0
krbPrincipalName: japhet@SMARTTECH.SN
krbPrincipalKey:: MIG2oAMCAQGhAwIBAAIDAgEBowMCAQGkgZ8wgZwwVKAHMAWgAwIBAKFJMEeg
  AwIBEqFABD4gACqW67WxzF2CoQRSGnxIkVFMHfHyzBD0sh1zMlRVb3tKaU05D1vCojInVhLsm/H3d
  Lz+kORrN6fLfjavzjBEOAcwBaADAgEAoTkwN6ADAgERoTAELhAAzih9Eu+vQfmvTci11YAJhpObzR
  IMQn0Ay/8n3JoM90palGfA8nUTsjiM2Do=
krbLastPwdChange: 20250301200143Z
krbExtraData:: AAKnZ8NnbmFydXRvL2FkbWluQFNNQVJUVEVDSC5TTgA=
krbExtraData:: AAgBAA==

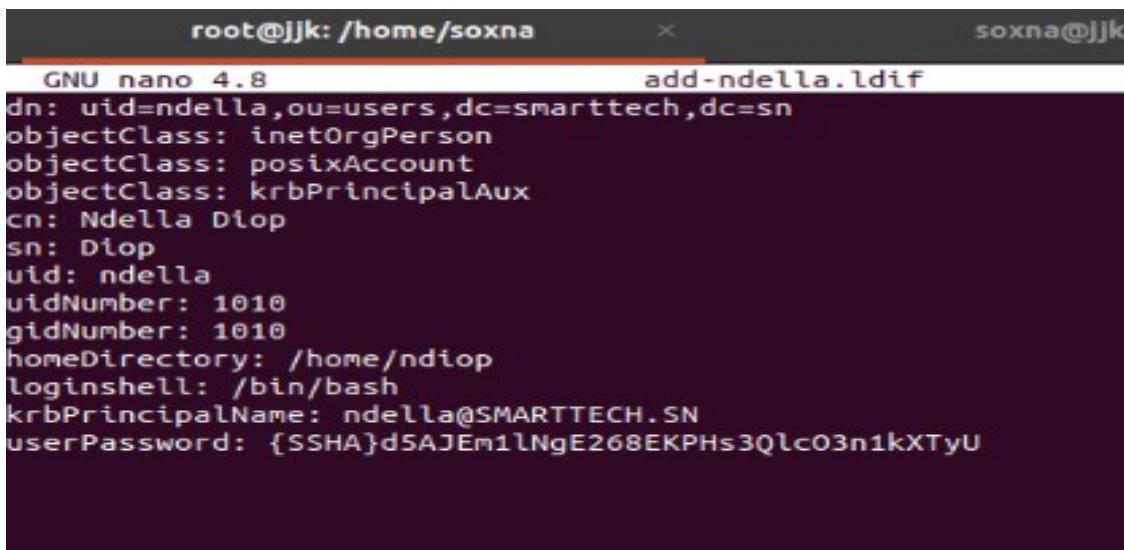
objectClass: krbPrincipal
objectClass: krbPrincipalAux
objectClass: krbTicketPolicyAux

# search result
search: 2
result: 0 Success

# numResponses: 15
# numEntries: 14
root@jjk:/home/soxna# ldapsearch -LLL -ldap://localhost -b "dc=smarttech,dc=sn"

```

Faisons un test avec un nouveau user :



```

root@jjk:/home/soxna          ×          soxna@jjk
GNU nano 4.8                  add-ndella.ldif
dn: uid=ndella,ou=users,dc=smarttech,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: krbPrincipalAux
cn: Ndella Diop
sn: Diop
uid: ndella
uidNumber: 1010
gidNumber: 1010
homeDirectory: /home/ndiop
loginshell: /bin/bash
krbPrincipalName: ndella@SMARTTECH.SN
userPassword: {SSHA}d5AJEm1lNgE268EKPHs3QlcO3n1kXTyU

```

Vérifions la présence de Ndella :

```

root@jjk:/home/soxna# ldapsearch -x -LLL -H ldap://localhost -b "dc=smarttech,d
c=sn" -D "cn=admin,dc=smarttech,dc=sn" -W "(uid=ndella)"
Enter LDAP Password:
dn: uid=ndella,ou=users,dc=smarttech,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: krbPrincipalAux
cn: Ndella Diop
sn: Diop
uid:: bmRlbGxhIA==
uidNumber: 1010
gidNumber: 1010
homeDirectory: /home/ndiop
loginShell: /bin/bash
krbPrincipalName: ndella@SMARTTECH.SN
userPassword:: e1NTSEF9ZDVBSkVtMWxOZ0UyNjhFS1B1czNRbGNPM24xa1hUeVU=
root@jjk:/home/soxna#

```

Ndella est déjà présent dans Kerberos donc il faut changer son mot de passe dans kerberos pour generer le hash quon va stocker dans ldap et pour pouvoir faire un kinit

```

root@jjk:/home/soxna# kadmin.local -q "cpw ndella"
Authenticating as principal naruto/admin@SMARTTECH.SN with password.
Enter password for principal "ndella@SMARTTECH.SN":
Re-enter password for principal "ndella@SMARTTECH.SN":
Password for "ndella@SMARTTECH.SN" changed.
root@jjk:/home/soxna#

```

Test avec kinit

```

root@jjk:/home/soxna# kinit ndella
Password for ndella@SMARTTECH.SN:
root@jjk:/home/soxna# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: ndella@SMARTTECH.SN

Valid starting      Expires              Service principal
02.03.2025 00:13:35  02.03.2025 10:13:35  krbtgt/SMARTTECH.SN@SMARTTECH.SN
        renew until 03.03.2025 00:13:25

```

Recherche dans la base ldap le user ndella :

```

root@jjk:/home/soxna# ldapsearch -x -LLL -H ldap://localhost -b "dc=smarttech,d
c=sn" -D "cn=admin,dc=smarttech,dc=sn" -W "(uid=ndella)"
Enter LDAP Password:
ldap_bind: Invalid credentials (49)
root@jjk:/home/soxna# ldapsearch -x -LLL -H ldap://localhost -b "dc=smarttech,d
c=sn" -D "cn=admin,dc=smarttech,dc=sn" -W "(uid=ndella)"
Enter LDAP Password:
dn: uid=ndella,ou=users,dc=smarttech,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: krbPrincipalAux
objectClass: krbTicketPolicyAux
cn: Ndella Diop
sn: Diop
uid:: bmRlbGxhIA==
uidNumber: 1010
gidNumber: 1010

```

Créons un utilisateur dans kerberos et verifions dans ldap :

```

root@jjk:/home/soxna# kadmin.local
Authenticating as principal ndella/admin@SMARTTECH.SN with password.
kadmin.local: addprinc aissata
WARNING: no policy specified for aissata@SMARTTECH.SN; defaulting to no policy
Enter password for principal "aissata@SMARTTECH.SN":
Re-enter password for principal "aissata@SMARTTECH.SN":
Principal "aissata@SMARTTECH.SN" created.
kadmin.local: 

```

Recherche de aissata

```

root@jjk:/home/soxna# ldapsearch -x -LLL -H ldap://localhost -b "dc=smarttech,d
c=sn" -D "cn=admin,dc=smarttech,dc=sn" -W "(krbPrincipalName=aissata@SMARTTECH.
SN)"
Enter LDAP Password:
dn: krbPrincipalName=aissata@SMARTTECH.SN,cn=SMARTTECH.SN,cn=krbContainer,dc=s
marttech,dc=sn
krbLoginFailedCount: 0
krbPrincipalName: aissata@SMARTTECH.SN
krbPrincipalKey:: MIG2oAMCAQGhAwIBAAiDAgEBowMCAQGkgZ8wgZwwVKAHMAWgAwIBAKFJMEeg
AwIBEqFABD4gAN2S6Z8pf1fie6LKDDqK0PyDNETqwRMEQRqp9brkwqd0MQRhT5Qd+hy9aD4sgoIJr
wKhaHf8hsNl8jY7VDBEoAcwBaADAgEAoTkWn6ADAgERoTAELhAAuSfopFPuobefv504II2KGXrQtR
58l5Uw89YldizgqhTB2bj+lefHV8A6efc=
krbLastPwdChange: 20250302001822Z
objectClass: krbPrincipal
objectClass: krbPrincipalAux
objectClass: krbTicketPolicyAux
krbLastSuccessfulAuth: 20250302002048Z
krbExtraData:: AALOo8NnbmRlbGxhL2FkbWluQFNNQVJUVEVDSC5TTgA=
krbExtraData:: AAgBAA==

root@jjk:/home/soxna# 

```

Test avec kinit

```

root@jjk:/home/soxna# kinit aissata
Password for aissata@SMARTTECH.SN:
root@jjk:/home/soxna# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: aissata@SMARTTECH.SN

Valid starting      Expires              Service principal
02.03.2025 00:20:48  02.03.2025 10:20:48  krbtgt/SMARTTECH.SN@SMARTTECH.SN
    renew until 03.03.2025 00:20:41
root@jjk:/home/soxna#

```

#### **d. Automatisation de la création d'un utilisateur LDAP :**

Installation du module ldap :

```

root@jjk:/home/soxna# sudo apt-get install python3-ldap
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-pyasn1 python3-pyasn1-modules
The following NEW packages will be installed:
  python3-ldap python3-pyasn1 python3-pyasn1-modules
0 upgraded, 3 newly installed, 0 to remove and 56 not upgraded.
Need to get 170 kB of archives.
After this operation, 1154 kB of additional disk space will be used.
Do you want to continue? [Y/n]
Get:1 http://sn.archive.ubuntu.com/ubuntu focal/main amd64 python3-pyasn1 all 0
.4.2-3build1 [46,7 kB]
Get:2 http://sn.archive.ubuntu.com/ubuntu focal/main amd64 python3-pyasn1-modul
es all 0.2.1-0.2build1 [32,9 kB]
Get:3 http://sn.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3-ldap
  amd64 3.2.0-4ubuntu2.1 [90,1 kB]
Fetched 170 kB in 1s (159 kB/s)
Selecting previously unselected package python3-pyasn1.
(Reading database ... 197414 files and directories currently installed.)
Preparing to unpack .../python3-pyasn1_0.4.2-3build1_all.deb ...

```

Nous avons crée un script qui va permettre d'ajouter les utilisateurs de manière automatique :

```

GNU nano 4.8                                     script ajout ldap.py
import ldap
import ldap.modlist as modlist
import subprocess
import getpass

LDAP_SERVER = "ldap://ldap.smarttech.sn"
LDAP_BIND_DN = "cn=admin,dc=smarttech,dc=sn"
LDAP_BIND_PASSWORD = "mourideAdmin1927"
LDAP_BASE_DN = "ou=users,dc=smarttech,dc=sn"
KERBEROS_REALM = "SMARTTECH.SN"

def get_next_uid(conn):
    """Récupère le plus grand uidNumber et l'incrémenté"""
    search_filter = "(uidNumber=*)"
    result = conn.search_s(LDAP_BASE_DN, ldap.SCOPE_SUBTREE, search_filter, [">
    uid_numbers = [int(entry[1]["uidNumber"][0]) for entry in result if "uidNu>
    return max(uid_numbers) + 1 if uid_numbers else 1000 # Commence à 1000 si >

try:
    conn = ldap.initialize(LDAP_SERVER)
    conn.simple_bind_s(LDAP_BIND_DN, LDAP_BIND_PASSWORD)

    new_user = input("Nom d'utilisateur (uid) : ")
    full_name = input("Nom complet (cn) : ")
    password = getpass.getpass("Mot de passe : ")

```

```

GNU nano 4.8                      script ajout ldap.py
password = getpass.getpass("Mot de passe : ")

next_uid = get_next_uid(conn)
gid_number = next_uid # Utilisation du même ID pour gidNumber
user_dn = f"uid={new_user},{LDAP_BASE_DN}"
krb_principal = f"{new_user}@{KERBEROS_REALM}"

# Générer un hash SHA pour le mot de passe LDAP
password_hash = subprocess.check_output(
    ["slappasswd", "-s", password], text=True
).strip()

user_attrs = {
    "objectClass": [b"inetOrgPerson", b"posixAccount", b"krbPrincipalAux"],
    "cn": [full_name.encode()],
    "sn": [full_name.split()[1].encode() if " " in full_name else full_name],
    "uid": [new_user.encode()],
    "uidNumber": [str(next_uid).encode()],
    "gidNumber": [str(gid_number).encode()],
    "homeDirectory": [f"/home/{new_user}".encode()],
    "loginShell": [b"/bin/bash"],
    "userPassword": [password_hash.encode()], # Stocke le mot de passe hashé
    "krbPrincipalName": [krb_principal.encode()],
}

ldif = modlist.addModlist(user_attrs)
conn.add_s(user_dn, ldif)
print(f"\n✓ Utilisateur {new_user} ajouté à LDAP avec uidNumber={next_uid}>

# Ajouter l'utilisateur à Kerberos avec le même mot de passe
add_kerb_cmd = f'echo "{password}" | kadmin.local -q "addprinc -pw {password} {new_user}@{KERBEROS_REALM}"'
subprocess.run(add_kerb_cmd, shell=True, check=True)
print(f"✓ Utilisateur {new_user} ajouté à Kerberos avec principal {krb_principal}>

conn.unbind_s()

except ldap.LDAPError as e:
    print(f"\n✗ Erreur LDAP : {e}")
except subprocess.CalledProcessError as e:
    print(f"\n✗ Erreur lors de l'ajout à Kerberos : {e}")

```

Nous allons exécuter le script. Il nous demandera : le nom de l'utilisateur, le nom complet, le mot de passe après on verra que l'utilisateur est ajouté à LDAP. On aura son uidNumber, gidNumber et en plus d'être un utilisateur Ldap il est maintenant reconnu comme principal de kerberos :

```

root@jjk:/home/soxna# nano script\ ajout\ ldap.py
root@jjk:/home/soxna# python3 script\ ajout\ ldap.py
Nom d'utilisateur (uid) : peter
Nom complet (cn) : Peter Pan
Mot de passe :

 Utilisateur peter ajouté à LDAP avec uidNumber=10001 et gidNumber=10001 !
Authenticating as principal root/admin@SMARTTECH.SN with password.
WARNING: no policy specified for peter@SMARTTECH.SN; defaulting to no policy
add_principal: Principal or policy already exists while creating "peter@SMARTTECH.SN".
 Utilisateur peter ajouté à Kerberos avec principal peter@SMARTTECH.SN !
root@jjk:/home/soxna# nano script\ ajout\ ldap.py
root@jjk:/home/soxna#
```

On va vérifier si l'utilisateur peter a bien été ajouté à la base de données LDAP avec la commande ldapsearch :

```

root@jjk:/home/soxna# ldapsearch -x -b "dc=smarttech,dc=sn" "uid=peter"
# extended LDIF
#
# LDAPv3
# base <dc=smarttech,dc=sn> with scope subtree
# filter: uid=peter
# requesting: ALL
#
# peter, users, smarttech.sn
dn: uid=peter,ou=users,dc=smarttech,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: krbPrincipalAux
cn: Peter Pan
sn: Pan
uid: peter
uidNumber: 10001
gidNumber: 10001
homeDirectory: /home/peter
loginShell: /bin/bash
krbPrincipalName: peter@SMARTTECH.SN

# search result
search: 2
result: 0 Success
```

On voit bien que l'utilisateur peter a bien été ajouté.

La commande Kadmin nous spécifie que l'utilisateur Peter existe déjà dans la base de données LDAP :

```

root@jjk:/home/soxna# kadmin.local -q "addprinc peter@SMARTTECH.SN"
Authenticating as principal root/admin@SMARTTECH.SN with password.
WARNING: no policy specified for peter@SMARTTECH.SN; defaulting to no policy
Enter password for principal "peter@SMARTTECH.SN":
Re-enter password for principal "peter@SMARTTECH.SN":
add_principal: Principal or policy already exists while creating "peter@SMARTTECH.SN".
root@jjk:/home/soxna# 

```

Après on change le mot de passe de peter et on fait des tests pour voir si tout à marcher :

```

root@jjk:/home/soxna# kadmin.local -q "cpw peter"
Authenticating as principal root/admin@SMARTTECH.SN with password.
Enter password for principal "peter@SMARTTECH.SN":
Re-enter password for principal "peter@SMARTTECH.SN":
Password for "peter@SMARTTECH.SN" changed.
root@jjk:/home/soxna# kinit peter
Password for peter@SMARTTECH.SN:
root@jjk:/home/soxna# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: peter@SMARTTECH.SN

Valid starting      Expires              Service principal
05.03.2025 07:10:44  05.03.2025 17:10:44  krbtgt/SMARTTECH.SN@SMARTTECH.SN
    renew until 06.03.2025 07:10:37
root@iik:/home/soxna#

```

## **2. FreeRadius :**

Maintenant que LDAP/KERBEROS est en place , on va intégrer FreeRadius pour sécuriser l'accès réseau (Wi-Fi et filiaire).

- Principe de fonctionnement :**

FreeRADIUS est un serveur d'authentification, d'autorisation et d'audit (AAA) basé sur le protocole RADIUS (Remote Authentication Dial-In User Service). Il est couramment utilisé pour gérer l'accès aux réseaux, notamment pour le Wi-Fi, les VPN, et d'autres systèmes nécessitant un contrôle des utilisateurs.

- Architecture AAA : Authentification, Autorisation, Audit**

**Authentification** : Vérifie l'identité de l'utilisateur en validant ses informations d'identification (nom d'utilisateur/mot de passe, certificat, etc.).

**Autorisation** : Détermine les permissions de l'utilisateur après authentification (accès à un service ou une ressource spécifique).

**Audit (Accounting)** : Enregistre les activités de l'utilisateur (connexion, durée, volume de données transférées, etc.).

- Avantages principaux :**

**Évolutivité** : Capable de gérer un grand nombre de requêtes simultanées.

**Sécurité** : Prise en charge des protocoles sécurisés comme EAP-TLS.

**Open Source** : Personnalisable et extensible selon les besoins.

### Installation et configuration de radius pour utiliser LDAP:

Nous allons installer le serveur freeradius pour commencer :

```
root@ubuntu:/home/ubuntu# sudo apt update
sudo apt install freeradius freeradius-ldap freeradius-utils
Ign :1 cdrom://Ubuntu 24.04.2 LTS _Noble Numbat_ - Release amd64 (20250215) n
oible InRelease
Atteint :2 cdrom://Ubuntu 24.04.2 LTS _Noble Numbat_ - Release amd64 (2025021
5) noble Release
Atteint :4 http://archive.ubuntu.com/ubuntu noble InRelease
Réception de :5 http://archive.ubuntu.com/ubuntu noble-updates InRelease [126
 kB]
Atteint :6 http://security.ubuntu.com/ubuntu noble-security InRelease
Atteint :7 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Réception de :8 http://archive.ubuntu.com/ubuntu noble-updates/main amd64 Pac
kages [890 kB]
Réception de :9 http://archive.ubuntu.com/ubuntu noble-updates/main i386 Pack
ages [433 kB]
Réception de :10 http://archive.ubuntu.com/ubuntu noble-updates/universe i386
 Packages [625 kB]
Réception de :11 http://archive.ubuntu.com/ubuntu noble-updates/universe amd6
```

Après installation on va déclarer les NAS ( ceux sont des entités qui agissent comme des intermédiaires entre les utilisateurs finaux et le serveur ) en se déplaçant sur le répertoire **etc/freeradius/3.0/clients.conf**

```
GNU nano 7.2          /etc/freeradius/3.0/clients.conf *
#}
client wifi-access-point {
    ipaddr = 192.168.1.6
    secret = passer@123
}
```

On a déclarer 1 client : **wifi-access-point**

Après on édite le fichier users et crée un utilisateur : ndella qui a pour mot de passe passer123 :

```
GNU nano 7.2          /etc/freeradius/3.0/users *
#####
# You should add test accounts to the TOP of this file! #
# See the example user "bob" above.                      #
#####

ndella  Cleartext-Password := "passer123"
```

On sauvegarde et on teste si l' utilisateur ndella parvient à se connecter en utilisant le client radtest :

```

root@ubuntu:/home/ubuntu# radtest ndella passer123 127.0.0.1 1812 testing123
Sent Access-Request Id 169 from 0.0.0.0:36964 to 127.0.0.1:1812 length 76
    User-Name = "ndella"
    User-Password = "passer123"
    NAS-IP-Address = 127.0.1.1
    NAS-Port = 1812
    Message-Authenticator = 0x00
    Cleartext-Password = "passer123"
Received Access-Accept Id 169 from 127.0.0.1:1812 to 127.0.0.1:36964 length 38
    Message-Authenticator = 0xb83440c65d4e224e2cbf8e706dcfdacf

```

FreeRadius doit utiliser LDAP pour authentifier les utilisateurs. On édite le fichier de configuration LDAP on cherche la section server et on le configure :

```

GNU nano 7.2          /etc/freeradius/3.0/mods-available/ldap
#
ldap {
    # Note that this needs to match the name(s) in the LDAP server
    # certificate, if you're using ldaps. See OpenLDAP documentation
    # for the behavioral semantics of specifying more than one host.
    #
    # Depending on the libldap in use, server may be an LDAP URI.
    # In the case of OpenLDAP this allows additional the following
    # additional schemes:
    # - ldaps:// (LDAP over SSL)
    # - ldapi:// (LDAP over Unix socket)
    # - ldapc:// (Connectionless LDAP)
    server = 'ldap.smarttech.local'
    identity = 'cn=admin,dc=smarttech,dc=local'
    password = 'passer@123'
    basedn = 'dc=smarttech,dc=local'
    filter = '(uid=%{jdoe})'
    start_tls = yes
    tls_require_cert = never

```

Activons LDAP en créant un lien symbolique :

```

root@ubuntu:/home/ubuntu# sudo ln -s /etc/freeradius/3.0/mods-available/ldap
/etc/freeradius/3.0/mods-enabled/

```

Modifions le fichier sites-enabled/default et décommentons la ligne ldap dans authorize puis dans authenticate :

```

GNU nano 7.2      /etc/freeradius/3.0/sites-enabled/default

#
# The ldap module reads passwords from the LDAP database.
ldap

GNU nano 7.2      /etc/freeradius/3.0/sites-enabled/default
# section. Put them in the "post-auth" section instead. That's what
# the post-auth section is for.
#
authenticate {
    #
    # PAP authentication, when a back-end database listed
    # in the 'authorize' section supplies a password. The
    # password can be clear-text, or encrypted.
    Auth-Type PAP {
        pap
    }
    Auth-Type LDAP {
        ldap
    }
}

```

\_ FreeRADIUS utilise le module LDAP pour authentifier les utilisateurs par rapport à un annuaire LDAP.

\_ La configuration spécifie l'emplacement du serveur LDAP et les informations d'identification pour s'y connecter.

\_ Le module LDAP est activé et l'authentification est configurée pour utiliser LDAP.

### Tester l'authentification LDAP via FreeRADIUS :

Avant d'intégrer avec le réseau, on teste l'authentification d'un utilisateur LDAP .

Ici on a utilisé un client ldap ndella créé lors de l'intégration ldap/kerberos **add-ndella.ldif**:

```

GNU nano 4.8                                add-ndella.ldif
dn: uid=ndella,ou=users,dc=smarttech,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: krbPrincipalAux
cn: Ndella Diop
sn: Diop
uid: ndella
uidNumber: 1010
gidNumber: 1010
homeDirectory: /home/ndiop
loginshell: /bin/bash
krbPrincipalName: ndella@SMARTTECH.SN
userPassword: {SSHA}d5AJEm1lNgE268EKPHs3Qlc03n1kXTyU

```

On alimente le fichier **add-ndella.ldif** :

```

root@jjk:/home/soxna# nano add-ndella.ldif
root@jjk:/home/soxna# ldapadd -x -D "cn=admin,dc=smarttech,dc=sn" -W -f add-ndella.ldif
Enter LDAP Password:
adding new entry "uid=ndella,ou=users,dc=smarttech,dc=sn"

```

Testons avec le client radtest :

```

root@jjk:/home/soxna# radtest ndella "ndella2025" localhost 1812 testing123
Sent Access-Request Id 71 from 0.0.0.0:47707 to 127.0.0.1:1812 length 76
    User-Name = "ndella"
    User-Password = "ndella2025"
    NAS-IP-Address = 192.168.1.25
    NAS-Port = 1812
    Cleartext-Password = "ndella2025"
Received Access-Accept Id 71 from 127.0.0.1:1812 to 127.0.0.1:47707 length 38

```

Et on voit que le test d'authentification a recu un accept ce qui deduit la bonne integration de ldap et freeradius.

### 3. Samba :

- **Installation et configuration de base de Samba :**

Installons les paquets nécessaires :

```

root@jjk:/home/soxna# apt install samba smbclient -y
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  attr ibverbs-providers libcephfs2 libibverbs1 librados2 librdmacm1
  libsmbclient libwbclient0 python3-crypto python3-dnspython python3-gpg
  python3-markdown python3-packaging python3-pgments python3-pyparsing
  python3-samba python3-tdb samba-common samba-common-bin samba-dsdb-modules
  samba-libs samba-vfs-modules tdb-tools
Suggested packages:
  python-markdown-doc python-pgments-doc ttf-bitstream-vera
  python-pyparsing-doc bind9 bind9utils ctdb ldb-tools ntp | chrony
  smbldap-tools winbind heimdal-clients cifs-utils
The following NEW packages will be installed:
  attr ibverbs-providers libcephfs2 libibverbs1 librados2 librdmacm1
  python3-crypto python3-dnspython python3-gpg python3-markdown
  python3-packaging python3-pgments python3-pyparsing python3-samba
  python3-tdb samba samba-common samba-common-bin samba-dsdb-modules
  samba-vfs-modules smbclient tdb-tools
The following packages will be upgraded:
  libsmbclient libwbclient0 samba-libs
3 upgraded, 22 newly installed, 0 to remove and 134 not upgraded.

```

Configurons samba dans /etc/samba/smb.conf pour activer l'authentification LDAP comme suit :

```

GNU nano 4.8                               /etc/samba/smb.conf
[global]
  workgroup = SMARTTECH
  server string = Samba Server
  security = user
  passdb backend = ldapsam:ldap://localhost
  ldap admin dn = cn=admin,dc=smarttech,dc=sn
  ldap suffix = dc=smarttech,dc=sn
  ldap user suffix = ou=Users
  ldap group suffix = ou=Groups
  ldap machine suffix = ou=Computers
  ldap idmap suffix = ou=Idmap
  ldap ssl = no
  idmap config * : backend = ldap
  idmap config * : range = 10000-20000
  ldap passwd sync = yes
  log file = /var/log/samba/log.%m
  max log size = 50
  load printers = no
  domain logons = no
  domain master = no
  local master = no
  preferred master = no

```

[ Read 33 lines ]

```
preferred master = no
wins support = no

[partage]
path = /srv/samba/partage
browseable = yes
read only = no
force group = sambashare
create mask = 0660
directory mask 0770
valid users = @sambashare
```

Ajoutons l'utilisateur Samba à LDAP :

```
root@jjk:/home/soxna# smbpasswd -w "mourideAdmin1927"
Setting stored password for "cn=admin,dc=smarttech,dc=sn" in secrets.tdb
[...]
```

Ajoutez le schéma LDAP pour Samba :

```
root@jjk:/home/soxna# ldapadd -Y EXTERNAL -H ldapi:/// -f /usr/share/doc/samba/
examples/LDAP/samba.ldif
SASL/EXTERNAL authentication started
SASL username: gIdNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=samba,cn=schema,cn=config"
```

#### • Partage de fichiers :

Créons un dossier de partage et configurons les permissions On hache d'abord le mdp ldap en vu de l'utiliser pour le NTPassword :

```
root@jjk:/home/soxna# python3 -c 'from Crypto.Hash import MD4; print(MD4.new("m
ourideAdmin1927".encode("utf-16le")).hexdigest().upper())'
C740A3ED738BBAD53BCBD8547256BDE4
[...]
```

On cherche le SID du domaine avec la commande get located et on ajoute un compte samba :

```
root@jjk:/home/soxna# ldapadd -x -D cn=admin,dc=smarttech,dc=sn -W <<EOF
dn: uid=smbadmin,ou=Users,dc=smarttech,dc=sn
objectClass: top
objectClass: posixAccount
objectClass: sambaSamAccount
objectClass: inetOrgPerson
cn: smbadmin
sn: Admin
uid: smbadmin
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/smbadmin
loginshell: /bin/bash
sambaSID: S-1-5-21-2413625038-2710674170-795289963-10000
sambaNTPassword: C740A3ED738BBAD53BCBD8547256BDE4
sambaPwdLastSet: 1740992623
EOF
Enter LDAP Password:
adding new entry "uid=smbadmin,ou=Users,dc=smarttech,dc=sn"

root@jjk:/home/soxna#
```

On crée le dossier de partage et on lui donne les permissions nécessaires :

```
root@jjk:/home/soxna# mkdir -p /srv/samba/partage
root@jjk:/home/soxna# chmod 770 /srv/samba/partage
root@jjk:/home/soxna# chown root:sambashare /srv/samba/partage
```

Ajoutez un groupe Samba et ajoutez des utilisateurs à ce groupe.

```
root@jjk:/home/soxna# groupadd sambashare
groupadd: group 'sambashare' already exists
root@jjk:/home/soxna# usermod -aG sambashare smbadmin
root@jjk:/home/soxna#
```

On ajoute le groupe sambashare à ldap

On ajoute smbadmin au groupe avec la commande :

```
root@jjk:/home/soxna# ldapadd -x -D cn=admin,dc=smarttech,dc=sn -W <<EOF
dn: cn=sambashare,ou=Groups,dc=smarttech,dc=sn
changetype: modify
add: memberUid
memberUid: smbadmin
EOF
Enter LDAP Password:
modifying entry "cn=sambashare,ou=Groups,dc=smarttech,dc=sn"

root@jjk:/home/soxna#
```

On vérifie que smbadmin appartient au groupe sambashare avec la commande ldapsearch :

```
root@jjk:/home/soxna# ldapsearch -x -LLL -D cn=admin,dc=smarttech,dc=sn -W -b d
c=smarttech,dc=sn "(cn=sambashare)"
Enter LDAP Password:
dn: cn=sambashare,ou=Groups,dc=smarttech,dc=sn
objectClass: top
objectClass: posixGroup
cn: sambashare
gidNumber: 1000
memberUid: smbadmin

root@jjk:/home/soxna#
```

On voit que c'est le cas.

Redémarrage :

```
root@jjk:/home/soxna# systemctl restart smbd nmbd
root@jjk:/home/soxna# systemctl enable smbd nmbd
Synchronizing state of smbd.service with SysV service script with /lib/systemd/
systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable smbd
Synchronizing state of nmbd.service with SysV service script with /lib/systemd/
systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable nmbd
root@jjk:/home/soxna#
```

Puis on teste (normalement depuis le client)

```

root@jjk:/home/soxna# systemctl restart smbd nmbd
root@jjk:/home/soxna# smbclient -L //192.168.1.25 -U smbadm
lpcfg_do_global_parameter: WARNING: The "domain logons" option is deprecated
Password for [SMARTTECH\smbadmin]:
      Sharename          Type        Comment
      -----            ----       -----
      partage           Disk
      IPC$              IPC        IPC Service (Samba Server)
SMB1 disabled -- no workgroup available
root@jjk:/home/soxna# █

```

On fait ce test sur le serveur :

```

root@jjk:/home/soxna# smbclient -L //192.168.1.25/partage -U smbadm
lpcfg_do_global_parameter: WARNING: The "domain logons" option is deprecated
Password for [SMARTTECH\smbadmin]:
      Sharename          Type        Comment
      -----            ----       -----
      partage           Disk
      IPC$              IPC        IPC Service (Samba Server)
SMB1 disabled -- no workgroup available
root@jjk:/home/soxna# █

```

On crée un fichier puis on le mets dans le dossier partage et on liste et on voit que le fichier testSamba.txt :

```

root@jjk:/home/soxna# echo "Hello there !" > testSamba.txt
root@jjk:/home/soxna# smbclient //192.168.1.25/partage -U smbadm
lpcfg_do_global_parameter: WARNING: The "domain logons" option is deprecated
Password for [SMARTTECH\smbadmin]:
Try "help" to get a list of possible commands.
smb: \> put testSamba.txt
putting file testSamba.txt as \testSamba.txt (0,7 kb/s) (average 0,7 kb/s)
smb: \> ls
.
..
testSamba.txt
                D          0  Mon Mar  3 09:24:44 2025
                D          0  Sun Mar  2 20:21:49 2025
25107716 blocks of size 1024. 13773320 blocks available
smb: \> █

```

### Explications :

- \_ Samba utilise LDAP pour authentifier les utilisateurs et gérer les informations de compte.
- \_ La configuration spécifie l'emplacement du serveur LDAP et les informations d'identification pour s'y connecter.
- \_ Un dossier de partage est créé et les permissions sont configurées pour contrôler l'accès.

### Scénarios de test :

- Accès au partage :

Depuis un client Linux ou Windows, essayons d'accéder au partage Samba en utilisant un utilisateur LDAP.

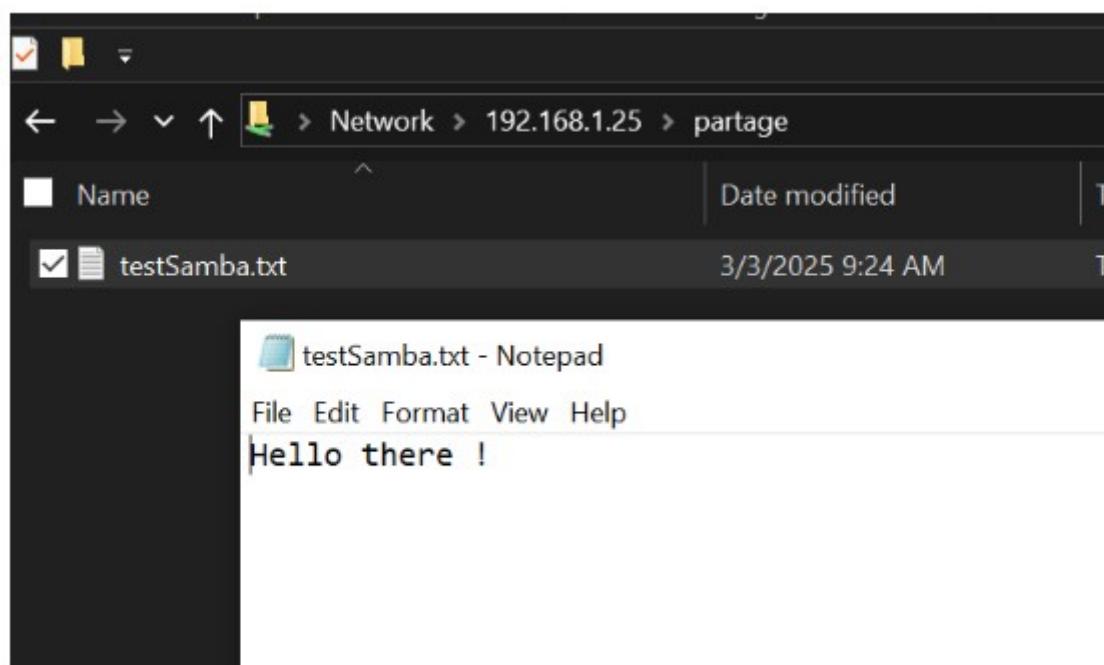
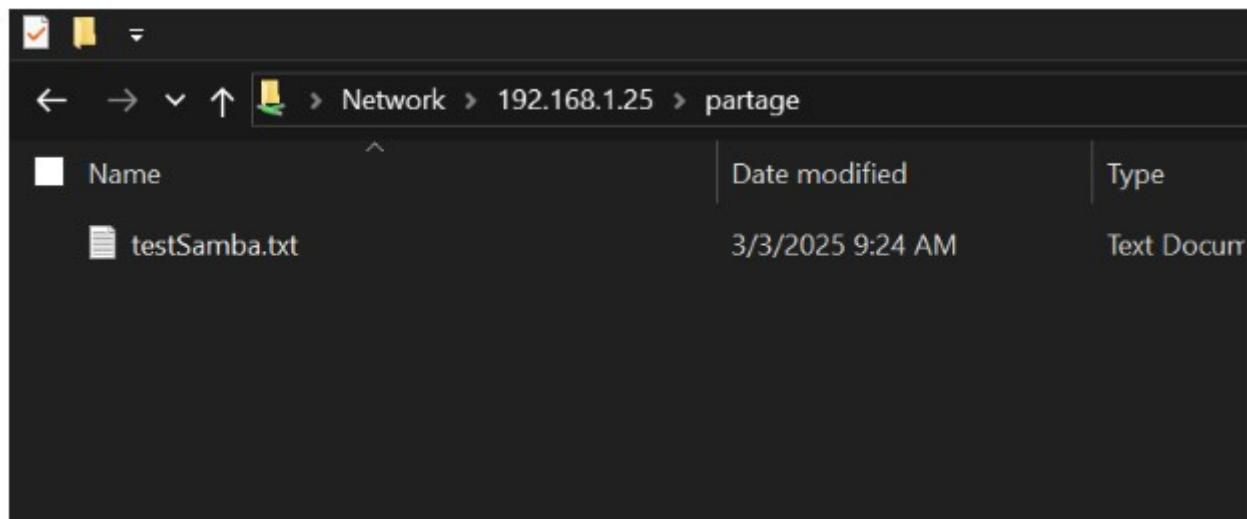
### 1. Accéder au partage Samba depuis Windows

Ouvrons l'Explorateur de fichiers sur notre machine Windows. Dans la barre d'adresse de l'Explorateur de fichiers, on tape l'adresse du partage Samba et on appuis sur entrée :

```
\\"192.168.1.25\partage
```

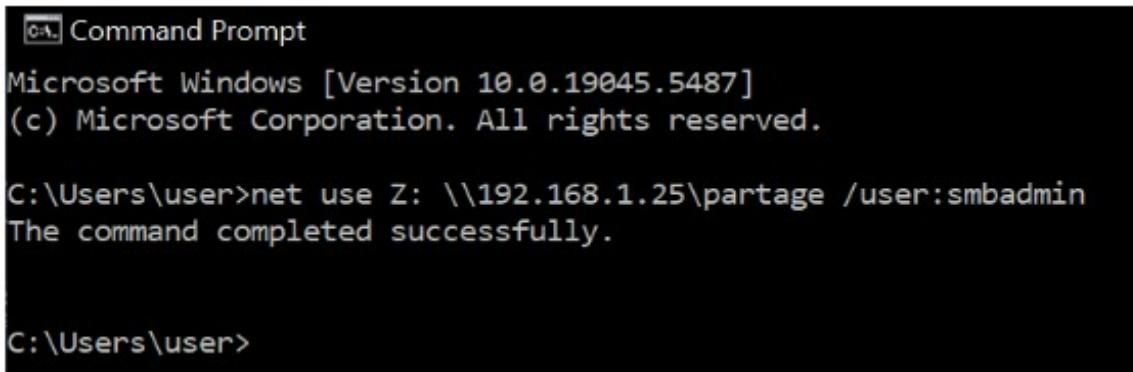
Nous sommes invités à entrer nos informations d'identification : Nom d'utilisateur et Mot de passe

Une fois connecté, on voit le fichier testSamba.txt créé.



### 2. Tester avec des commandes Windows (optionnel)

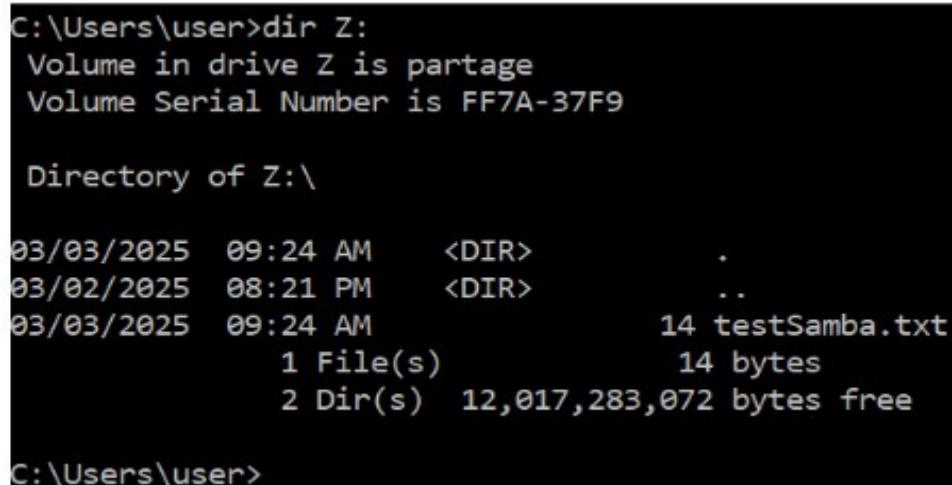
Appuyons sur Win + R, tapons cmd, puis on appuis sur Entrée. Utilisons la commande suivante pour accéder au partage Samba :



```
Command Prompt  
Microsoft Windows [Version 10.0.19045.5487]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\user>net use Z: \\192.168.1.25\partage /user:smbadmin  
The command completed successfully.  
  
C:\Users\user>
```

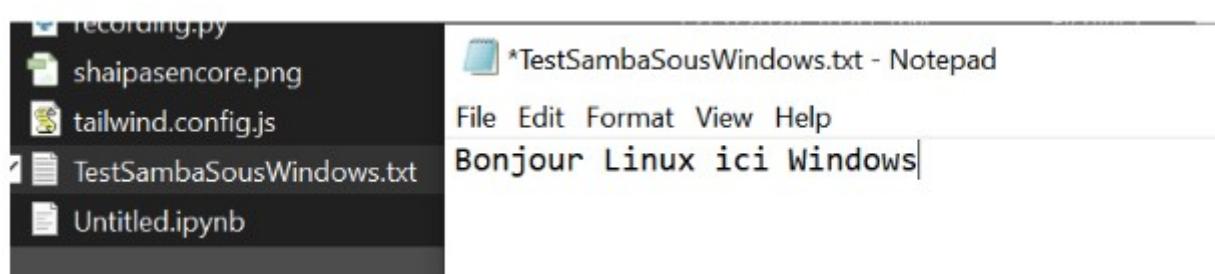
Puisque qu'on a déjà fourni les paramètres de connexion et spécifier à windows de s'en rappeler on a pas pu retaper le mot de passe.

On peut vérifier le contenu :



```
C:\Users\user>dir Z:  
Volume in drive Z is partage  
Volume Serial Number is FF7A-37F9  
  
Directory of Z:\  
  
03/03/2025  09:24 AM    <DIR>      .  
03/02/2025  08:21 PM    <DIR>      ..  
03/03/2025  09:24 AM            14 testSamba.txt  
                      1 File(s)       14 bytes  
                      2 Dir(s)  12,017,283,072 bytes free  
  
C:\Users\user>
```

On peut créer un fichier dans windows et le copier :

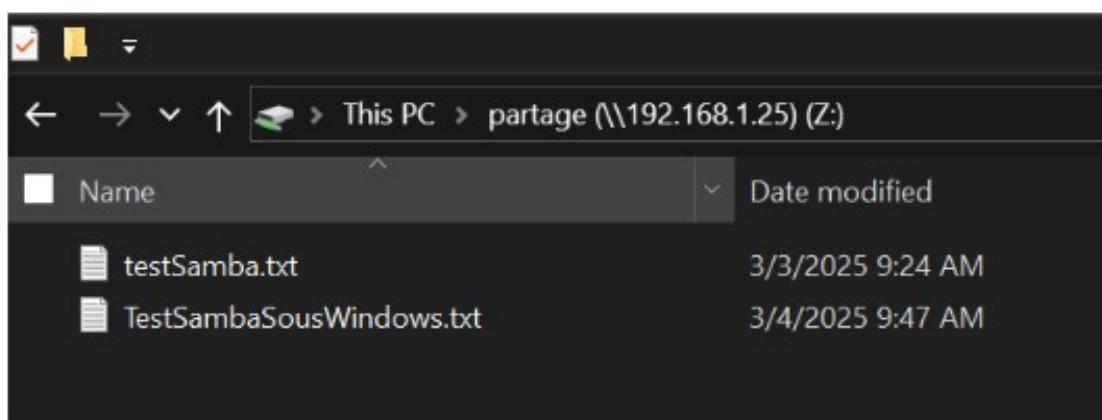


Le fichier a bien été copié :

```
C:\Users\user>copy TestSambaSousWindows.txt Z:\  
1 file(s) copied.  
  
C:\Users\user>dir Z:  
Volume in drive Z is partage  
Volume Serial Number is FF7A-37F9  
  
Directory of Z:\  
  
03/04/2025  09:33 AM    <DIR>          .  
03/02/2025  08:21 PM    <DIR>          ..  
03/03/2025  09:24 AM           14 testSamba.txt  
03/04/2025  09:31 AM           0 TestSambaSousWindows.txt  
                  2 File(s)        14 bytes  
                  2 Dir(s)   12,017,283,072 bytes free  
  
C:\Users\user>
```

La commande net use pour vérifier le partage tout est ok :

```
C:\Users\user>net use  
New connections will be remembered.  
  
Status      Local       Remote             Network  
-----  
OK          Z:          \\192.168.1.25\partage  Microsoft Windows Network  
OK          Z:          \\192.168.1.25\partage  Microsoft Windows Network  
The command completed successfully.
```



Depuis le serveur on vérifie :

```

soxna@jjk:~$ sudo smbclient //192.168.1.25/partage -U smbadm
[sudo] password for soxna:
lpcfg_do_global_parameter: WARNING: The "domain logons" option is deprecated
Password for [SMARTTECH\smbadm]:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
testSamba.txt
TestSambaSousWindows.txt

          D      0  Tue Mar  4 09:33:51 2025
          D      0  Sun Mar  2 20:21:49 2025
          A     14  Mon Mar  3 09:24:44 2025
          A      0  Tue Mar  4 09:31:19 2025

      25107716 blocks of size 1024. 11735620 blocks available
smb: \>

```

On récupère le fichier :

```

smb: \> get TestSambaSousWindows.txt
getting file \TestSambaSousWindows.txt of size 25 as TestSambaSousWindows.txt (
6,1 KiloBytes/sec) (average 6,1 KiloBytes/sec)
smb: \>

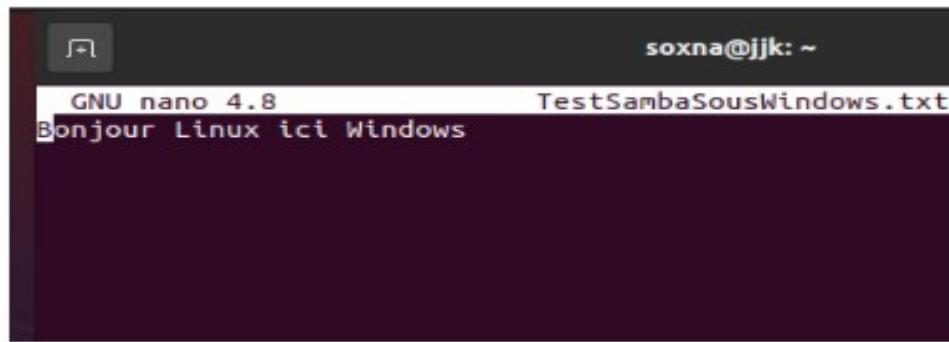
```

```

smb: \> exit
soxna@jjk:~$ ls
acl.ldif           Desktop           Public
add-ndella.ldif   Documents         Templates
adduser.sh         Downloads         TestSambaSousWindows.txt
asterisk-20-current.tar.gz group.ldif
asterisk.schema    krbContainer.ldif testSamba.txt
base.ldif          Music             users.ldif
configLdapKerberos.txt Pictures        Videos
soxna@jjk:~$ █

```

Lisons le fichier :



Nous constatons après plusieurs tests que Samba/Ldap marche .

#### 4. Messagerie avancées avec iRedMail :

iRedMail est une solution open-source qui permet d'installer un serveur de messagerie complet avec des fonctionnalités comme :

- SMTP, IMAP, POP3
- Anti-spam (SpamAssassin)
- Antivirus (ClamAV)
- Webmail (Roundcube)

- Support LDAP, MySQL ou PostgreSQL pour l'authentification

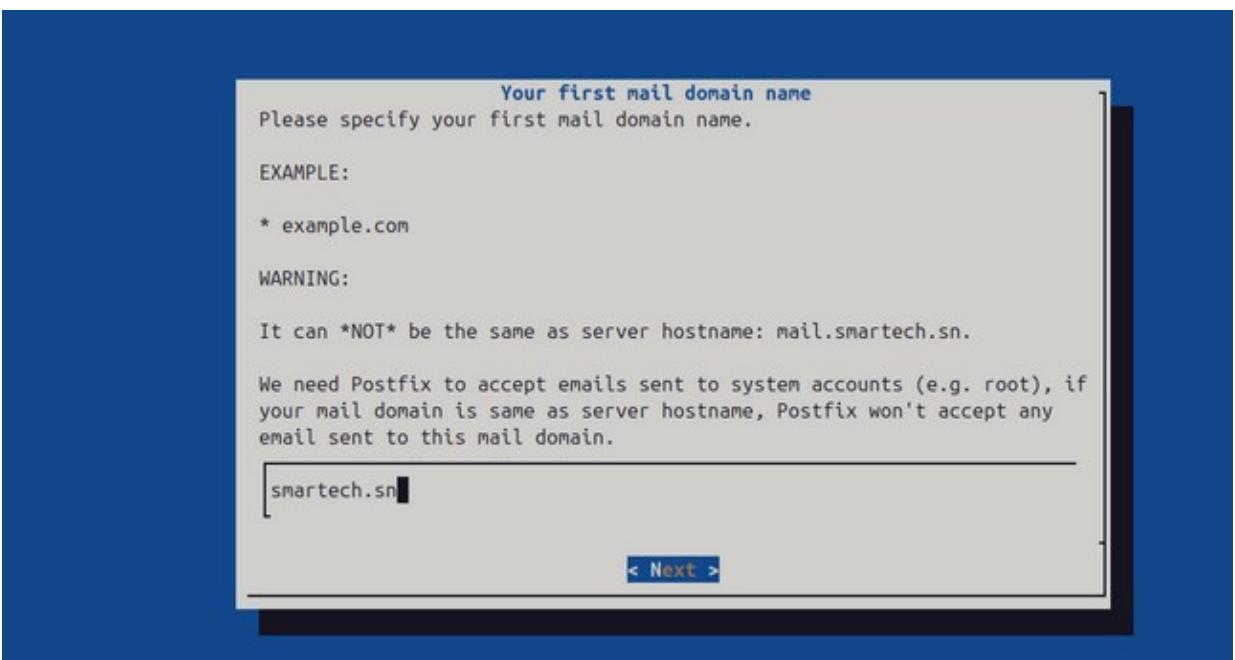
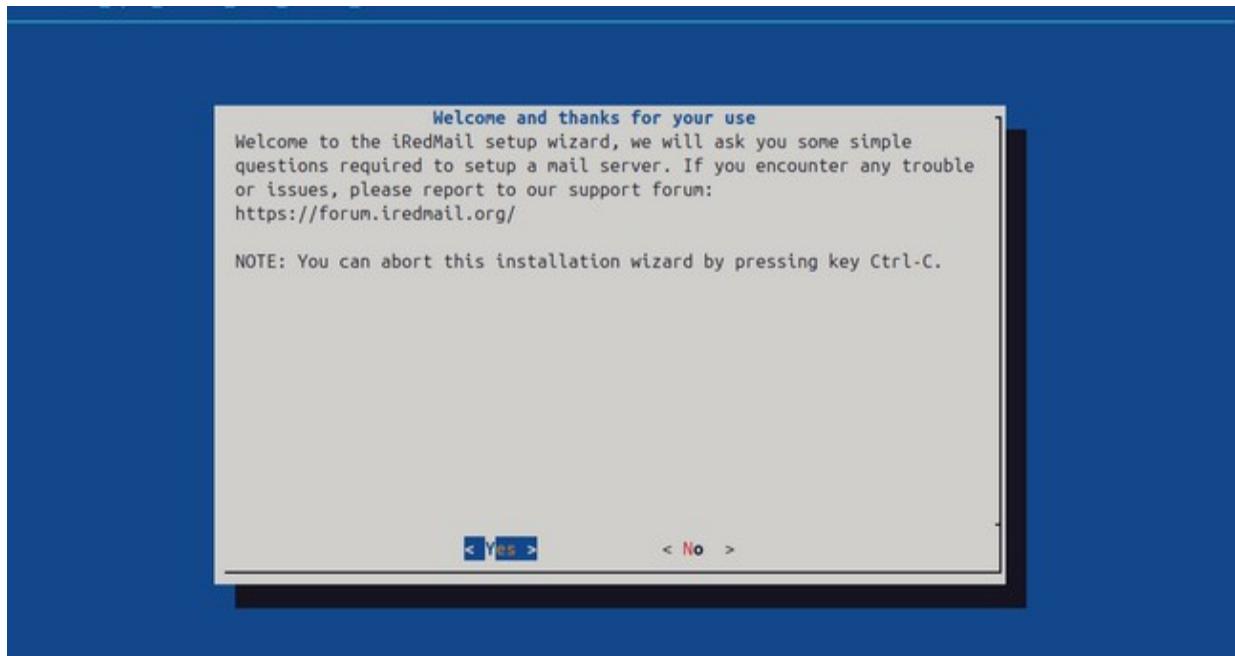
Commençons d'abord par l'installation d'iRedMail et faisons les configurations nécessaire pour ce dernier :

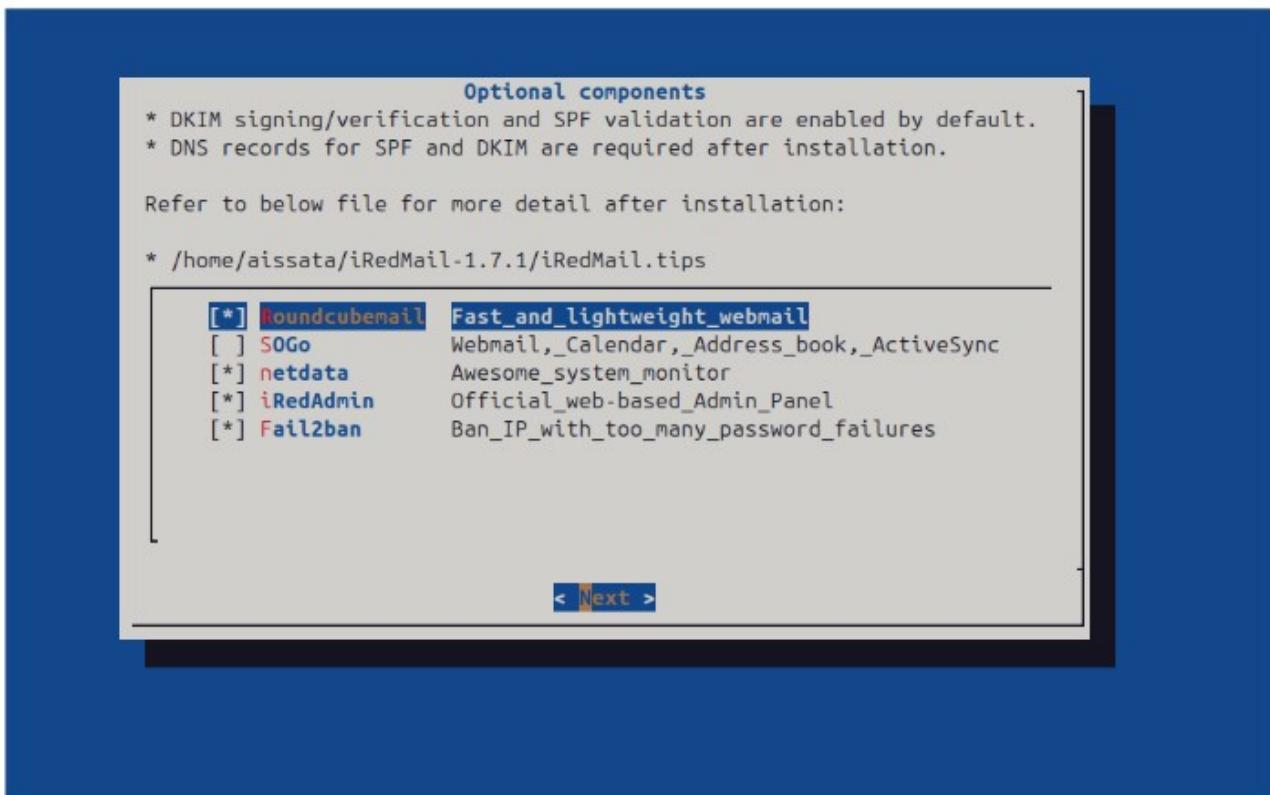
```
root@mail:/home/aissata# wget https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.1.tar.gz
--2025-03-02 14:21:06-- https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.1.tar.gz
Résolution de github.com (github.com)... 140.82.121.4
Connexion à github.com (github.com)|140.82.121.4|:443... connecté.
requête HTTP transmise, en attente de la réponse... 302 Found
Emplacement : https://codeload.github.com/iredmail/iRedMail/tar.gz/refs/tags/1.7.1 [suivant]
--2025-03-02 14:21:11-- https://codeload.github.com/iredmail/iRedMail/tar.gz/refs/tags/1.7.1
Résolution de codeload.github.com (codeload.github.com)... 140.82.121.9
Connexion à codeload.github.com (codeload.github.com)|140.82.121.9|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : non indiqué [application/x-gzip]
Enregistre : '1.7.1.tar.gz'

1.7.1.tar.gz          [ =>                               ] 242,02K  593KB/s   ds 0,4s
2025-03-02 14:21:13 (593 KB/s) - '1.7.1.tar.gz' enregistré [247831]

root@mail:/home/aissata#
```

```
root@mail:/home/aissata# tar xvf 1.7.1.tar.gz
iRedMail-1.7.1/
iRedMail-1.7.1/.github/
iRedMail-1.7.1/.github/ISSUE_TEMPLATE/
iRedMail-1.7.1/.github/ISSUE_TEMPLATE/issue-or-bug-report.md
iRedMail-1.7.1/.gitignore
iRedMail-1.7.1/ChangeLog
iRedMail-1.7.1/Documentations
iRedMail-1.7.1/LICENSE
iRedMail-1.7.1/README.md
iRedMail-1.7.1/conf/
iRedMail-1.7.1/conf/amavisd
iRedMail-1.7.1/conf/clamav
iRedMail-1.7.1/conf/core
iRedMail-1.7.1/conf/dovecot
iRedMail-1.7.1/conf/fail2ban
iRedMail-1.7.1/conf/global
iRedMail-1.7.1/conf/iredadmin
iRedMail-1.7.1/conf/iredapd
iRedMail-1.7.1/conf/logwatch
iRedMail-1.7.1/conf/memcached
iRedMail-1.7.1/conf/mlmmj
iRedMail-1.7.1/conf/mysql
iRedMail-1.7.1/conf/netdata
iRedMail-1.7.1/conf/nginx
iRedMail-1.7.1/conf/openldap
iRedMail-1.7.1/conf/php
iRedMail-1.7.1/conf/postfix
iRedMail-1.7.1/conf/postgresql
iRedMail-1.7.1/conf/roundcube
iRedMail-1.7.1/conf/sogo
iRedMail-1.7.1/conf/zenity
```





```
Sun Mar  2 15:39:30 2025 -> main.cvd updated (version: 62, sigs: 6647427, f-level: 90, builder: sigmgr)
Sun Mar  2 15:39:30 2025 -> bytecode database available for download (remote version: 335)
Testing database: '/var/lib/clamav/tmp.3d254c1302/clamav-ac9395571b6d1986e8efe4d53204e663.tmp-bytecode.cvd' ...
Database test passed.
Sun Mar  2 15:39:31 2025 -> bytecode.cvd updated (version: 335, sigs: 86, f-level: 90, builder: raynman)
*****
* URLs of installed web applications:
*
* - Roundcube webmail: https://mail.smartech.sn/mail/
* - netdata (monitor): https://mail.smartech.sn/netdata/
*
* - Web admin panel (iRedAdmin): https://mail.smartech.sn/iredadmin/
*
* You can login to above links with below credential:
*
* - Username: postmaster@smartech.sn
*
● postfix.service - Postfix Mail Transport Agent
● mariadb.service - MariaDB 10.11.8 database server
  Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; preset: enabled)
  Drop-In: /etc/systemd/system/mariadb.service.d
    └─override.conf
    Active: active (running) since Sun 2025-03-02 15:43:38 GMT; 8min ago
      Docs: man:mariadb(8)
             https://mariadb.com/kb/en/library/systemd/
     Process: 1195 ExecStartPre=/usr/bin/install -m 755 -o mysql -g root -d /var/run/mysqld (code=exited, status=0/SUCCESS)
     Process: 1268 ExecStartPre=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
     Process: 1297 ExecStartPre=/bin/sh -c [ ! -e /usr/bin/galera_recovery ] && VAR= || VAR=`cd /usr/bin/..; /usr/bin/>
     Process: 1721 ExecStartPost=/bin/sh -c systemctl unset-environment _WSREP_START_POSITION (code=exited, status=0/SUCCESS)
     Process: 1740 ExecStartPost=/etc/mysql/debian-start (code=exited, status=0/SUCCESS)
  Main PID: 1532 (mariadb)
    Status: "Taking your SQL requests now..."
      Tasks: 18 (limit: 14994)
     Memory: 13.9M (peak: 121.6M swap: 85.7M swap peak: 85.8M)
        CPU: 7.378s
       CGroup: /system.slice/mariadb.service
                 └─1532 /usr/sbin/mariadb

mars 02 15:43:36 mail.smartech.sn mariadb[1532]: 2025-03-02 15:43:36 0 [Note] Plugin 'FEEDBACK' is disabled.
mars 02 15:43:36 mail.smartech.sn mariadb[1532]: 2025-03-02 15:43:36 0 [Note] InnoDB: Loading buffer pool(s) from /var/
mars 02 15:43:36 mail.smartech.sn mariadb[1532]: 2025-03-02 15:43:36 0 [Warning] You need to use --log-bin to make --op
mars 02 15:43:36 mail.smartech.sn mariadb[1532]: 2025-03-02 15:43:36 0 [Note] Server socket created on IP: '127.0.0.1'.
mars 02 15:43:36 mail.smartech.sn mariadb[1532]: 2025-03-02 15:43:36 0 [Note] /usr/sbin/mariadb: ready for connection>
mars 02 15:43:36 mail.smartech.sn mariadb[1532]: Version: '10.11.8-MariaDB-Ubuntu0.24.04.1' socket: '/run/mysqld/mys>
mars 02 15:43:38 mail.smartech.sn systemd[1]: Started mariadb.service - MariaDB 10.11.8 database server.
mars 02 15:43:38 mail.smartech.sn /etc/mysql/debian-start[1756]: Upgrading MariaDB tables if necessary.
mars 02 15:43:40 mail.smartech.sn mariadb[1532]: 2025-03-02 15:43:40 0 [Note] InnoDB: Buffer pool(s) load completed at>
mars 02 15:43:41 mail.smartech.sn /etc/mysql/debian-start[1818]: Triggering myisam-recover for all MyISAM tables and ar>
lines 1-30/30 (END)
```

```
root@mail:/home/aissata# cd iRedMail-1.7.1/
root@mail:/home/aissata/iRedMail-1.7.1# sudo ufw allow 25,80,443,587,993,995/tcp
Les règles ont été mises à jour
Les règles ont été mises à jour (IPv6)
root@mail:/home/aissata/iRedMail-1.7.1# █
```

```
root@mail:/home/aissata/iRedMail-1.7.1# sudo ufw enable
Le pare-feu est actif et lancé au démarrage du système
root@mail:/home/aissata/iRedMail-1.7.1# █
```

- **Configuration de boîtes aux lettres virtuelles :**

Les boîtes aux lettres virtuelles dans iRedMail sont gérées par Postfix et Dovecot, avec le stockage des comptes dans MariaDB (ou LDAP selon la configuration). Vérifier la base de données des boîtes aux lettres Les informations des utilisateurs sont généralement stockées dans MariaDB.

Vérifions d'abord si tout est bien configuré :

### 1. Se connecter à MariaDB

Pour s'assurer que les boîtes aux lettres sont bien enregistrées, on vérifie les bases de données disponibles dans MariaDB :

```
root@mail:/home/aissata/iRedMail-1.7.1# sudo ufw enable
Le pare-feu est actif et lancé au démarrage du système
root@mail:/home/aissata/iRedMail-1.7.1# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 219
Server version: 10.11.8-MariaDB-0ubuntu0.24.04.1 Ubuntu 24.04

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> █
```

Lister les bases de données:

On peut voir une base nommée vmail

```
MariaDB [(none)]> show databases;
+-----+
| Database      |
+-----+
| amavisd      |
| fail2ban      |
| information_schema |
| iredadmin     |
| iredapd       |
| mysql         |
| performance_schema |
| roundcubemail |
| sys           |
| vmail          |
+-----+
10 rows in set (0,117 sec)

MariaDB [(none)]> █
```

Sélectionner la base et voir les tables

Les tables importantes à vérifier sont : mailbox : stocke les informations des utilisateurs, alias : gère les alias email, domain : liste les domaines gérés :

**Database changed**

```
MariaDB [vmail]> show tables;
+-----+
| Tables_in_vmail      |
+-----+
| admin                |
| alias                |
| alias_domain          |
| anyone_shares         |
| deleted_mailboxes    |
| domain               |
| domain_admins         |
| forwardings          |
| last_login            |
| mailbox              |
| maillist_owners       |
| maillists             |
| moderators            |
| recipient_bcc_domain |
| recipient_bcc_user   |
| sender_bcc_domain    |
| sender_bcc_user       |
| sender_relayhost      |
| share_folder          |
| used_quota            |
+-----+
20 rows in set (0,002 sec)
```

```
MariaDB [vmail]> █
```

## 2. Ajouter une boîte aux lettres virtuelle

Ajout d'un nouvel utilisateur :

```

MariaDB [vmail]> INSERT INTO mailbox (username, password, name, maildir, quota, domain, created)
-> VALUES ('alice@exemple.com', ENCRYPT('MotDePasse123', CONCAT('$6$', SUBSTRING(SHA(RAND()), -16))), 
->          'Alice Dupont', 'exemple.com/alice/', 1024, 'exemple.com', NOW());
Query OK, 1 row affected (0,306 sec)

MariaDB [vmail]>
MariaDB [vmail]> select * from mailbox WHERE username = 'alice@exemple.com';
+-----+-----+-----+-----+-----+-----+-----+
| username | password | name | language | mailboxformat | mailboxfolder | storagebasedirectory | storagenode | maildir |
| quota | domain | transport | department | rank | employeedid | isadmin | isglobaladmin | enablesmtp | enable
esmtptsecured | enablepop3 | enablepop3secured | enablepop3tsl | enableimap | enableimapsecured | enableimaptl | enabled
oliver | enablelda | enablemanagesieve | enablemanagesievesecured | enablesieve | enablesievesecured | enablesievetl | enable
internal | enabledoveadm | enablelib-storage | enablequota-status | enableindexer-worker | enablelmtp | enableedsyn
c | enablesogo | enablesogowebmail | enablesogocalendar | enablesogoadvivesync | allow_nets | disclaimer | settings | pa
sswordlastchange | created | modified | expired | active |
+-----+-----+-----+-----+-----+-----+-----+

```

### 3. Vérifier la configuration Postfix pour les boîtes aux lettres virtuelles

Editons /etc/postfix/main.cf :

```

GNU nano 7.2                               /etc/postfix/main.cf
proxy:mysql:/etc/postfix/mysql/transport_maps_user.cf
proxy:mysql:/etc/postfix/mysql/transport_maps_maillist.cf
proxy:mysql:/etc/postfix/mysql/transport_maps_domain.cf

sender_dependent_relayhost_maps =
    proxy:mysql:/etc/postfix/mysql/sender_dependent_relayhost_maps.cf

# Lookup table with the SASL login names that own the sender (MAIL FROM) addresses.
smtpd_sender_login_maps =
    proxy:mysql:/etc/postfix/mysql/smtpd_sender_login_maps.cf

virtual_mailbox_domains =
    proxy:mysql:/etc/postfix/mysql/virtual_mailbox_domains.cf

relay_domains =
    $mydestination
    proxy:mysql:/etc/postfix/mysql/relay_domains.cf

virtual_mailbox_maps =
    proxy:mysql:/etc/postfix/mysql/virtual_mailbox_maps.cf

virtual_alias_maps =
    proxy:mysql:/etc/postfix/mysql/virtual_alias_maps.cf
    proxy:mysql:/etc/postfix/mysql/domain_alias_maps.cf
    proxy:mysql:/etc/postfix/mysql/catchall_maps.cf
    proxy:mysql:/etc/postfix/mysql/domain_alias_catchall_maps.cf

```

Une fois les modifications effectuées, on redémarre postfix et dovecot

### 4. Tester la connexion à la boîte aux lettres

Connexion avec un client IMAP/SMTP (comme Thunderbird) ou avec telnet :

Tester l'authentification IMAP :

```

root@mail:/home/aissata/iRedMail-1.7.1# telnet localhost 143
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^A'.
* OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE LITERAL+ STARTTLS AUTH=PLAIN AUTH=LOGIN] Dovecot (Ubuntu)
tu) ready.

```

Ensuite, on vérifie sur mariadb l'utilisateur crée :

```

root@mail:/home/aissata/mariadb> SELECT * FROM vmail;
+-----+-----+-----+-----+-----+-----+-----+-----+
| node | maildir | quota | domain | transport | department | rank | employeeid | | | | | | | |
| isadmin | isglobaladm | in | enablesmtp | enablesmtpsecured | enablepop3 | enablepop3secured | enablepop3tls | enableimap | enableimapsecured |
| enableimaptls | enabledeliver | enablellda | enablemanagesieve | enablemanagesievesecured | enablesieve | enablestivese | red | enablesievetls | enableinternal | enabledoveadm | enablelib-storage | enablequota-status | enableindexer-worker |
| enablelmtp | enabledsync | enablesogoa | enablesogowebmail | enablesogocalendar | enablesogactivesync | allow_nets | dis | claimer | settings | passwordlastchange | created | modified | expired | active |
+-----+-----+-----+-----+-----+-----+-----+-----+
| aissata@example.com | passer2025 | Aissata | | maildir | Maildir | /var/vmail | vmail |
| exemple.com/aissata@ | 1024 | exemple.com | | | normal | | 0 | |
0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
L | NULL | 1970-01-01 01:01:01 | 2025-03-03 11:20:26 | 1970-01-01 01:01:01 | 9999-12-31 00:00:00 | 1 |
+-----+-----+-----+-----+-----+-----+-----+-----+
1 row in set (0,029 sec)

MariaDB [vmail]>

```

- Intégration du protocole Sieve pour la gestion des règles de filtrage des emails.**

Dovecot supporte Sieve, qui permet de créer des règles pour trier automatiquement les emails. Il faut activer et configurer le plugin Pigeonhole pour Dovecot.

Pour intégrer Sieve avec Dovecot et activer le plugin Pigeonhole, voici les étapes à suivre :

1. Installer le plugin Pigeonhole

```

root@mail:/home/aissata# apt install dovecot-sieve dovecot-managesieved
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
dovecot-sieve est déjà la version la plus récente (1:2.3.21+dfsg1-2ubuntu6).
dovecot-managesieved est déjà la version la plus récente (1:2.3.21+dfsg1-2ubuntu6).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libaio1t64 libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 libllvmm17t64 libmecab2 libprotobuf-lite32t64
  linux-headers-6.8.0-51 linux-headers-6.8.0-51-generic linux-image-6.8.0-51-generic linux-modules-6.8.0-51-generic
  linux-modules-extra-6.8.0-51-generic linux-tools-6.8.0-51 linux-tools-6.8.0-51-generic mecab-ipadic
  mecab-ipadic-utf8 mecab-utils
Veuillez utiliser « apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@mail:/home/aissata#

```

2. Activer le service ManageSieve

On Vérifie que le service ManageSieve est activé dans /etc/dovecot/dovecot.conf :

```

root@mail:/home/aissata# vim /etc/dovecot/dovecot.conf
GNU nano 7.2                               /etc/dovecot/dovecot.conf

#base_dir = /var/run/dovecot
mail_plugins = quota mailbox_alias acl mail_log notify

# Enabled mail protocols.
protocols = pop3 imap sieve lmtp

# User/group who owns the message files:
mail_uid = 2000
mail_gid = 2000

# Assign uid to virtual users.
first_valid_uid = 2000
last_valid_uid = 2000

# Logging. Reference: http://wiki2.dovecot.org/Logging
#
# Use syslog
syslog_facility = local5

# Debug
#mail_debug = yes
#auth_verbose = yes
#auth_debug = yes
#auth_debug_passwords = yes

```

Dans /etc/dovecot/conf.d/20-managesieve.conf, on s'assure que ces lignes ne sont pas commentées :

```

GNU nano 7.2                               /etc/dovecot/conf.d/20-managesieve.conf

service managesieve {
    # Max. number of ManageSieve processes (connections)
    #process_limit = 1024
}

# Service configuration

protocol sieve {
    # Maximum ManageSieve command line length in bytes. ManageSieve usually does
    # not involve overly long command lines, so this setting will not normally
    # need adjustment
    #managesieve_max_line_length = 65536

    # Maximum number of ManageSieve connections allowed for a user from each IP
    # address.
    # NOTE: The username is compared case-sensitively.
    #mail_max_userip_connections = 10

    # Space separated list of plugins to load (none known to be useful so far).
    # Do NOT try to load IMAP plugins here.
    #mail_plugins =

    # MANAGESIEVE logout format string:
    # %i - total number of bytes read from client
    # %o - total number of bytes sent to client
}

```

### 3. Configurer Sieve

On Crée un répertoire pour stocker les scripts Sieve :

```

root@mail:/home/aissata# mkdir -p /var/mail/sieve-scripts
root@mail:/home/aissata# chown -R vmail:vmail /var/mail/sieve-scripts
root@mail:/home/aissata# chmod -R 770 /var/mail/sieve-scripts
root@mail:/home/aissata# 

```

On Ajoute cette configuration à /etc/dovecot/conf.d/90-sieve.conf :

```

GNU nano 7.2                               /etc/dovecot/conf.d/90-sieve.conf *

#sieve_trace_dir = 

# The verbosity level of the trace messages. Trace debugging is disabled if
# this setting is not configured. Possible values are:
#
# "actions"      - Only print executed action commands, like keep,
#                   fileinto, reject and redirect.
# "commands"     - Print any executed command, excluding test commands.
# "tests"        - Print all executed commands and performed tests.
# "matching"    - Print all executed commands, performed tests and the
#                  values matched in those tests.
#
#sieve_trace_level = 

# Enables highly verbose debugging messages that are usually only useful for
# developers.
#sieve_trace_debug = no

# Enables showing byte code addresses in the trace output, rather than only
# the source line numbers.
#sieve_trace_addresses = no
}

plugin {
  sieve = /var/mail/sieve-scripts/%u.sieve
  sieve_global_path = /var/mail/sieve-scripts/default.sieve
  sieve_dir = /var/mail/sieve-scripts/%u/
}

```

On Crée un fichier default.sieve :

```

GNU nano 7.2                               /var/mail/sieve-scripts/default.sieve
require ["fileinto"];
if header :contains "Subject" "SPAM" {
  fileinto "Junk";
  stop;
}

```

Et on Compile ce script :

```

root@mail:/home/aissata# nano /var/mail/sieve-scripts/default.sieve
root@mail:/home/aissata# sievec /var/mail/sieve-scripts/default.sieve
root@mail:/home/aissata# 

```

Tester la configuration

On Vérifie que le port ManageSieve (4190) est ouvert :

```

root@mail:/home/aissata# netstat -tulpn | grep :4190
tcp        0      0 127.0.0.1:4190          0.0.0.0:*
                                              LISTEN      11672/dovecot
root@mail:/home/aissata# 

```

- [\*\*Mise en place de solutions anti-spam et antivirus \(ex : SpamAssassin, ClamAV\).\*\*](#)

Dans cette partie, nous avons eu à utiliser entièrement ClamAV car ayant un problème avec la configuration de SpamAssassin :

## 1. Vérifier le statut des services ClamAV

J'ai lancé la commande suivante pour voir s'il fonctionne correctement :

```
● clamav-daemon.service - Clam AntiVirus userspace daemon
  Loaded: loaded (/usr/lib/systemd/system/clamav-daemon.service; enabled; preset: enabled)
  Drop-In: /etc/systemd/system/clamav-daemon.service.d
            └── extend.conf
  Active: active (running) since Mon 2025-03-03 11:36:24 GMT; 31min ago
  TriggeredBy: ● clamav-daemon.socket
    Docs: man:clamd(8)
          man:clamd.conf(5)
          https://docs.clamav.net/
  Process: 10286 ExecStartPre=/bin/mkdir -p /run/clamav (code=exited, status=0/SUCCESS)
  Process: 10288 ExecStartPre=/bin/chown clamav /run/clamav (code=exited, status=0/SUCCESS)
 Main PID: 10290 (clamd)
   Tasks: 2 (limit: 2271)
  Memory: 478.0M (peak: 1.2G swap: 925.3M swap peak: 925.3M)
    CPU: 52.345s
   CGroup: /system.slice/clamav-daemon.service
             └─10290 /usr/sbin/clamd --foreground=true

mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> Portable Executable support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> ELF support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> Mail files support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> OLE2 support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> PDF support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> SWF support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> HTML support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> XMLDOCS support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> HWP3 support
mars 03 11:37:33 mail.smartech.sn clamd[10290]: Mon Mar  3 11:37:33 2025 -> Self checking
lines 1-29
```

## Mettre à jour la base de signatures de ClamAV :

ClamAV a besoin d'une base de données de virus à jour.

**sudo freshclam**

On va constater que freshclam est bloqué, il faudra donc activer les mises à jour automatiques en modifiant son fichier de configuration avec :

**sudo nano /etc/clamav/freshclam.conf**

**sudo systemctl restart clamav-freshclam**

```
GNU nano 7.2                               /etc/clamav/freshclam.conf
DatabaseOwner clamav
UpdateLogFile /var/log/clamav/freshclam.log
LogVerbose false
LogSyslog false
LogFacility LOG_LOCAL6
LogFileMaxSize 0
LogRotate true
LogTime true
Foreground false
Debug false
MaxAttempts 5
DatabaseDirectory /var/lib/clamav
DNSDatabaseInfo current.cvd.clamav.net
ConnectTimeout 30
ReceiveTimeout 0
TestDatabases yes
ScriptedUpdates yes
CompressLocalDatabase no
Bytecode true
NotifyClamd /etc/clamav/clamd.conf
# Check for new database 24 times a day
Checks 24
DatabaseMirror db.local.clamav.net
DatabaseMirror database.clamav.net
#Example
```

```
root@mail:/home/aissata# sudo nano /etc/clamav/freshclam.conf
root@mail:/home/aissata# sudo systemctl restart clamav-freshclam
root@mail:/home/aissata#
```

### Tester ClamAV avec un faux virus (EICAR)

ClamAV peut être testé avec EICAR, un fichier de test inoffensif utilisé pour les antivirus.

Nous avons crée un fichier de test et scanné avec ClamAV :

```
root@mail:/home/aissata# echo "X50\!P%@AP[4\PZX54(P^)7CC)7]$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*" > eicar.com

echo "X50\!P%@AP[4\PZX54(P^)7CC)7]$EICAR-STANDARD-ANTIVIRUS-TEST-FILEclamav-daemonH+H*" > eicar.com
root@mail:/home/aissata# ls -l eicar.com
-rw-r--r-- 1 root root 75 mars 3 22:27 eicar.com
root@mail:/home/aissata# clamscan eicar.com
Loading: 49s, ETA: 0s [=====] 8.66M/8.72M sigs
```

Lors de l'exécution de la commande clamscan eicar.com, l'analyse antivirus commence correctement, mais au bout d'un certain temps, la machine virtuelle devient extrêmement lente jusqu'à ce qu'elle finisse par planter complètement. On a été obligé de l'éteindre et de la rallumer pour pouvoir continuer à travailler.

Ce problème pourrait être dû à la taille importante des fichiers présents dans /var/vmail/, ce qui entraîne une consommation excessive des ressources (CPU, RAM, disque). Il est possible que l'analyse soit trop lourde pour la capacité de la machine virtuelle, ce qui la fait geler avant même d'atteindre la fin du scan.

### Configurer un scan automatique des emails

iRedMail utilise Amavis pour scanner les emails avec ClamAV. Il faut s'assurer qu'Amavis fonctionne :

```
● amavis.service - Interface between MTA and virus scanner/content filters
   Loaded: loaded (/usr/lib/systemd/system/amavis.service; enabled; preset: enabled)
   Active: active (running) since Mon 2025-03-03 23:06:54 GMT; 5min ago
     Docs: http://www.ljs.si/software/amavisd/#doc
   Process: 1178 ExecStartPre=/usr/bin/find /var/lib/amavis -maxdepth 1 -name amavis-* -type d -exec rm -rf {} ; (code=0)
   Process: 1221 ExecStartPre=/usr/bin/find /var/lib/amavis/tmp -maxdepth 1 -name amavis-* -type d -exec rm -rf {} ; (code=0)
 Main PID: 1246 (/usr/sbin/amavis)
    Tasks: 3 (limit: 2271)
   Memory: 3.1M (peak: 180.3M swap: 164.9M swap peak: 164.9M)
      CPU: 7.065s
     CGroup: /system.slice/amavis.service
             └─1246 "/usr/sbin/amavisd (master)"
               ├─2750 "/usr/sbin/amavisd (virgin child)"
               ├─2751 "/usr/sbin/amavisd (virgin child)"

mars 03 23:06:54 mail.smartech.sn systemd[1]: Started amavis.service - Interface between MTA and virus scanner/content filters.
mars 03 23:09:01 mail.smartech.sn amavis[1246]: starting. /usr/sbin/amavisd at mail.smartech.sn amavis-2.13.0 (20230106)
mars 03 23:09:01 mail.smartech.sn amavis[1246]: perl=5.038002, user=984, EUID: 984 (984); group=(), EGID: 984 984 (984)
mars 03 23:09:05 mail.smartech.sn amavis[1246]: Net::Server: Group Not Defined. Defaulting to EGID '984 984'
mars 03 23:09:05 mail.smartech.sn amavis[1246]: Net::Server: User Not Defined. Defaulting to EUID '984'
mars 03 23:09:05 mail.smartech.sn amavis[1246]: No ext program for .F, tried: unfreeze, freeze -d, melt, fc当地
mars 03 23:09:05 mail.smartech.sn amavis[1246]: No ext program for .zoo, tried: zoo, unzoo
mars 03 23:09:05 mail.smartech.sn amavis[1246]: No decoder for .F
mars 03 23:09:05 mail.smartech.sn amavis[1246]: No decoder for .zoo
mars 03 23:09:05 mail.smartech.sn amavis[1246]: Using primary internal av scanner code for clamav-socket
-
-
-
-
-
```

Si tu veux un scan manuel de ton dossier mail :

```
lines 1-25/25 (END)
root@mail:/home/aissata# clamscan -r /var/vmail/
Loading: 1m 45s, ETA: 1s [=====] 8.58M/8.72M sigs
```

Pour voir l'activité d'Amavis avec ClamAV :

```
root@mail:/home/aissata# tail -f /var/log/mail.log
2025-03-03T23:31:36.812870+00:00 mail amavis[1368]: perl=5.038002, user=984, EUID: 984 (984); group=(), EGID: 984 984 (984)
2025-03-03T23:31:39.864348+00:00 mail postfix/postfix-script[2600]: starting the Postfix mail system
2025-03-03T23:31:39.964445+00:00 mail postfix/master[2605]: daemon started -- version 3.8.6, configuration /etc/postfix
2025-03-03T23:31:40.669794+00:00 mail amavis[1368]: Net::Server: Group Not Defined. Defaulting to EGID '984 984'
2025-03-03T23:31:40.671275+00:00 mail amavis[1368]: Net::Server: User Not Defined. Defaulting to EUID '984'
2025-03-03T23:31:40.699838+00:00 mail amavis[1368]: No ext program for .F, tried: unfreeze, freeze -d, melt, fc当地
2025-03-03T23:31:40.701206+00:00 mail amavis[1368]: No ext program for .zoo, tried: zoo, unzoo
2025-03-03T23:31:40.701665+00:00 mail amavis[1368]: No decoder for .F
2025-03-03T23:31:40.701771+00:00 mail amavis[1368]: No decoder for .zoo
2025-03-03T23:31:40.701887+00:00 mail amavis[1368]: Using primary internal av scanner code for clamav-socket
```

- **Déploiement d'un service de messagerie instantanée XMPP.**

Il existe plusieurs serveurs XMPP, mais voici les plus populaires compatibles avec iRedMail :

Prosody → Léger, facile à configurer.

ejabberd → Plus robuste, adapté aux grandes infrastructures.

Nous allons partir sur **Prosody**, qui est simple et efficace.

## 1. Installation de Prosody

```
root@mail:/home/aissata# apt install prosody -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
 libaio1t64 libevent-core-2.1-7t64 libevent-pthreads-2.1-7t64 liblvm17t64
 libmecab2 libprotobuf-lite32t64 linux-headers-6.8.0-51
 linux-headers-6.8.0-51-generic linux-image-6.8.0-51-generic
 linux-modules-6.8.0-51-generic linux-modules-extra-6.8.0-51-generic
 linux-tools-6.8.0-51 linux-tools-6.8.0-51-generic mecab-ipadic
 mecab-ipadic-utf8 mecab-utils
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
 libunbound8 lua-bit32 lua-bitop lua-event lua-expat lua-filesystem lua-posix
 lua-readline lua-sec lua-socket lua-unbound lua5.4
Paquets suggérés :
 lua-dbi-mysql lua-dbi-postgresql lua-dbi-sqlite3 lua-zlib
Les NOUVEAUX paquets suivants seront installés :
 libunbound8 lua-bit32 lua-bitop lua-event lua-expat lua-filesystem lua-posix
 lua-readline lua-sec lua-socket lua-unbound lua5.4 prosody
0 mis à jour, 13 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 1 404 ko dans les archives.
```

Le fichier de configuration principal est :sudo nano /etc/prosody/prosody.cfg.lua

## 2.Ajouter mon domaine XMPP

```

GNU nano 7.2           /etc/prosody/prosody.cfg.lua
----- Additional config files -----
-- For organizational purposes you may prefer to add VirtualHost and
-- Component definitions in their own config files. This line includes
-- all config files in /etc/prosody/conf.d/

VirtualHost "localhost"
-- Prosody requires at least one enabled VirtualHost to function. You can
-- safely remove or disable 'localhost' once you have added another.

--VirtualHost "example.com"
enabled = true
authentication = "internal_hashed"
ssl = {
key = "/etc/letsencrypt/live/exemple.com/privkey.pem";
certificate = "/etc/letsencrypt/live/exemple.com/fullchain.pem";
}

----- Components -----
[ 279 lignes écrites ]
^G Aide      ^O Écrire      ^W Chercher  ^K Couper      ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller      ^J Justifier ^/ Aller ligne

-- Documentation for bundled modules can be found at: https://prosody.im/doc/modules
modules_enabled = {

    -- Generally required
    "disco"; -- Service discovery
    "roster"; -- Allow users to have a roster. Recommended ;
    "saslauth"; -- Authentication for clients and servers. Recommended
    "tls"; -- Add support for secure TLS on c2s/s2s connections

    -- Not essential, but recommended
    "blocklist"; -- Allow users to block communications with other clients
    "bookmarks"; -- Synchronise the list of open rooms between clients
    "carbons"; -- Keep multiple online clients in sync
    "dialback"; -- Support for verifying remote servers using DNS
    "limits"; -- Enable bandwidth limiting for XMPP connections
    "pep"; -- Allow users to store public and private data in their accounts
    "private"; -- Legacy account storage mechanism (XEP-0049)
    "smacks"; -- Stream management and resumption (XEP-0198)
    "vcard4"; -- User profiles (stored in PEP)
    "vcard_legacy"; -- Conversion between legacy vCard and PEP Avatars

^G Aide      ^O Écrire      ^W Chercher  ^K Couper      ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich. ^\ Remplacer ^U Coller      ^J Justifier ^/ Aller ligne

```

3.Ajouter un utilisateur pour tester :

Entrer un mot de passe sécurisé.

```

root@mail:/home/aissata# sudo prosodyctl adduser aissata@exemple.com
The host 'exemple.com' is not listed in the configuration file (or is not enabled).
The user will not be able to log in until this is changed.
That user already exists
root@mail:/home/aissata#

```

#### 4. Ouvrir les ports XMPP

On va vérifier l'état des règles avec :

```

root@mail:/home/aissata# sudo ufw status verbose
État : actif
Journalisation : on (low)
Par défaut : deny (incoming), allow (outgoing), disabled (routed)
Nouveaux profils : skip

Vers          Action      De
---          ----
3389/tcp      ALLOW IN   Anywhere
25,80,443,587,993,995/tcp  ALLOW IN   Anywhere
5222/tcp      ALLOW IN   Anywhere
5269/tcp      ALLOW IN   Anywhere
3389/tcp (v6) ALLOW IN   Anywhere (v6)
25,80,443,587,993,995/tcp (v6) ALLOW IN   Anywhere (v6)
5222/tcp (v6) ALLOW IN   Anywhere (v6)
5269/tcp (v6) ALLOW IN   Anywhere (v6)

root@mail:/home/aissata#

```

Prosody utilise les ports suivants, il faut donc s'assurer qu'ils sont ouverts :

5222,5269,5289,443,80

```

La règle a été ajoutée
La règle a été ajoutée (v6)
root@mail:/home/aissata# sudo ufw allow 443/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
root@mail:/home/aissata# sudo ufw allow 80/tcp
La règle a été ajoutée
La règle a été ajoutée (v6)
root@mail:/home/aissata# sudo ufw status verbose
État : actif
Journalisation : on (low)
Par défaut : deny (incoming), allow (outgoing), disabled (routed)
Nouveaux profils : skip

Vers          Action      De
---          ----
3389/tcp      ALLOW IN   Anywhere
25,80,443,587,993,995/tcp  ALLOW IN   Anywhere
5222/tcp      ALLOW IN   Anywhere
5269/tcp      ALLOW IN   Anywhere
5280/tcp      ALLOW IN   Anywhere
443/tcp       ALLOW IN   Anywhere
80/tcp        ALLOW IN   Anywhere
3389/tcp (v6) ALLOW IN   Anywhere (v6)
25,80,443,587,993,995/tcp (v6) ALLOW IN   Anywhere (v6)
5222/tcp (v6) ALLOW IN   Anywhere (v6)
5269/tcp (v6) ALLOW IN   Anywhere (v6)
5280/tcp (v6) ALLOW IN   Anywhere (v6)
443/tcp (v6)  ALLOW IN   Anywhere (v6)
80/tcp (v6)   ALLOW IN   Anywhere (v6)

root@mail:/home/aissata# ■

```

## 5. Redémarrer Prosody

```
root@mail:/home/aissata# sudo systemctl restart prosody
root@mail:/home/aissata# sudo systemctl enable prosody
Synchronizing state of prosody.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable prosody
```

## 6. Tester la connexion XMPP

Depuis un autre serveur : on fait telnet exemple.com 5222

- Problème de connexion avec Telnet sur le port 5222

Lorsqu'on exécute la commande telnet exemple.com 5222 depuis un autre serveur pour tester la connexion, celle-ci reste bloquée sur "Trying [adresse IP]..." pendant plus de 15 minutes, sans établir de connexion. Finalement, la commande plante, et la machine devient inutilisable, nous obligeant à la redémarrer. Nous pensons que le problème vient principalement d'une surcharge du serveur distant, ce qui entraîne un temps de réponse anormalement long. Il est possible que le serveur ait des ressources limitées (mémoire, CPU) ou qu'il gère un trop grand nombre de connexions simultanées, ce qui l'empêche de répondre correctement à notre requête.

```
Dépaquetage de libssh2-1t64:amd64 (1.11.0-4.1build2) ...
Sélection du paquet nmap-common précédemment désélectionné.
Préparation du dépaquetage de .../nmap-common 7.94+git20230807.3be01efb1+dfsg-3build2_all.deb ...
Dépaquetage de nmap-common (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Sélection du paquet nmap précédemment désélectionné.
Préparation du dépaquetage de .../nmap_7.94+git20230807.3be01efb1+dfsg-3build2_amd64.deb ...
Dépaquetage de nmap (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Paramétrage de libblas3:amd64 (3.12.0-3build1.1) ...
update-alternatives: utilisation de « /usr/lib/x86_64-linux-gnu/blas/libblas.so.3 » pour fournir « /usr/lib/x86_64-linux-gnu/libblas.so.3 » (libblas.so.3-x86_64-linux-gnu) en mode automatique
Paramétrage de nmap-common (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Paramétrage de libssh2-1t64:amd64 (1.11.0-4.1build2) ...
Paramétrage de liblinear4:amd64 (2.3.0+dfsg-5build1) ...
Paramétrage de nmap (7.94+git20230807.3be01efb1+dfsg-3build2) ...
Traitement des actions différées (« triggers ») pour man-db (2.12.0-4build2) ...
Traitement des actions différées (« triggers ») pour libc-bin (2.39-0ubuntu8.4) ...
root@mail:/home/aissata# nmap -p 5222 exemple.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-04 11:33 GMT
Nmap scan report for exemple.com (103.224.182.245)
Host is up (0.27s latency).
rDNS record for 103.224.182.245: lb-182-245.above.com

PORT      STATE      SERVICE
5222/tcp  filtered  xmpp-client

Nmap done: 1 IP address (1 host up) scanned in 3.93 seconds
root@mail:/home/aissata# telnet exemple.com 5222
Trying 103.224.182.245...
```

- **Mise en place d'un service WebRTC pour les communications en temps réel.**

Voici les étapes générales :

### 1. Choisir un serveur WebRTC

On peut utiliser un serveur WebRTC comme :

- Coturn (serveur STUN/TURN pour la traversée de NAT)
- Jitsi Meet (solution complète de visioconférence)
- Janus Gateway (serveur WebRTC modulaire)

## Installation de Jitsi Meet

Vérifie que ton domaine pointe vers ton serveur :

```
root@mail:/home/aissata# ping meet.exemple.com
PING meet.exemple.com (103.224.182.245) 56(84) bytes of data.
64 bytes from lb-182-245.above.com (103.224.182.245): icmp_seq=2 ttl=51 time=231 ms
64 bytes from lb-182-245.above.com (103.224.182.245): icmp_seq=3 ttl=51 time=263 ms
64 bytes from lb-182-245.above.com (103.224.182.245): icmp_seq=4 ttl=51 time=214 ms
64 bytes from lb-182-245.above.com (103.224.182.245): icmp_seq=5 ttl=51 time=215 ms
64 bytes from lb-182-245.above.com (103.224.182.245): icmp_seq=6 ttl=51 time=212 ms
64 bytes from lb-182-245.above.com (103.224.182.245): icmp_seq=7 ttl=51 time=212 ms
64 bytes from lb-182-245.above.com (103.224.182.245): icmp_seq=8 ttl=51 time=213 ms
^C
--- meet.exemple.com ping statistics ---
8 packets transmitted, 7 received, 12.5% packet loss, time 7017ms
rtt min/avg/max/mdev = 212.052/222.916/263.247/17.589 ms
root@mail:/home/aissata#
```

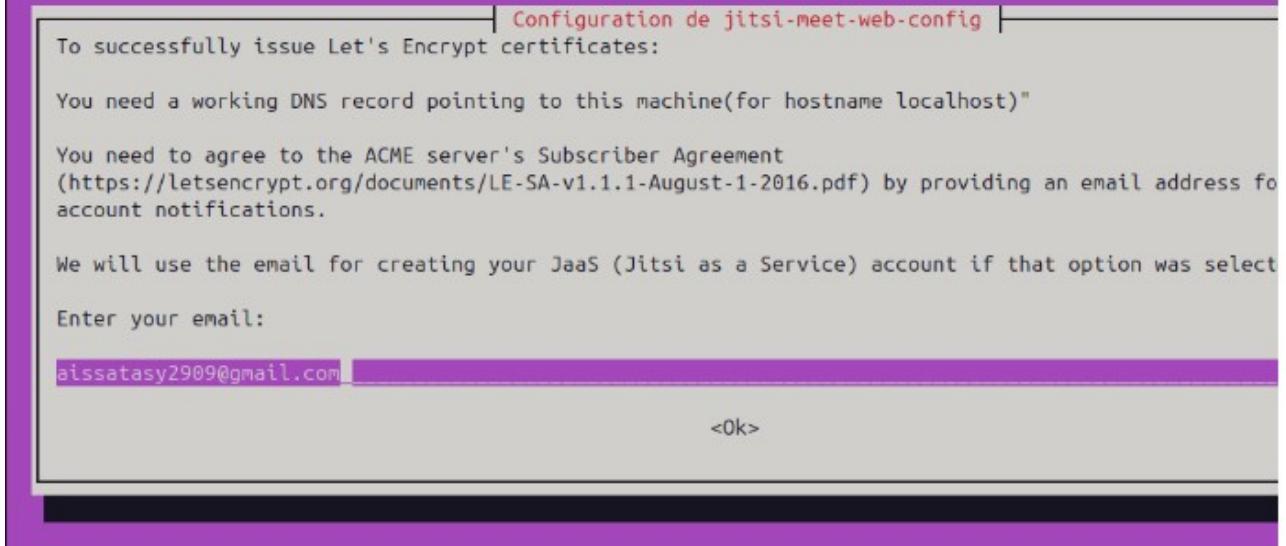
Ajoutons le dépôt Jitsi :

```
root@mail:/home/aissata# curl https://download.jitsi.org/jitsi-key.gpg.key | sudo gpg --dearmor -o /usr/share/keyrings/jitsi-keyring.gpg
echo 'deb [signed-by=/usr/share/keyrings/jitsi-keyring.gpg] https://download.jitsi.org stable/' | sudo tee /etc/apt/sources.list.d/jitsi-stable.list
% Total    % Received % Xferd  Average Speed   Time     Time      Current
          Dload  Upload   Total Spent    Left Speed
100  3114  100  3114    0     8  2671      0  0:00:01  0:00:01  --:--:-- 2672
deb [signed-by=/usr/share/keyrings/jitsi-keyring.gpg] https://download.jitsi.org stable/
root@mail:/home/aissata#
```

Rechargeons les dépôts et installons Jitsi Meet :

```
root@mail:/home/aissata# apt install jitsi-meet -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
 libaudio16 libl10n17t64 libmecab2 libprotobuf-lite32t64 linux-headers-6.8.0-51 linux-headers-6.8.0-51-generic
 linux-image-6.8.0-51-generic linux-modules-6.8.0-51-generic linux-modules-extra-6.8.0-51-generic
 linux-tools-6.8.0-51 linux-tools-6.8.0-51-generic mecab-ipadic mecab-ipadic-utf8 mecab-utils
Veuillez utiliser « apt autoremove » pour les supprimer.
Les paquets supplémentaires suivants seront installés :
 ca-certificates-java coturn fonts-lato java-common jicofo jitsi-meet-prosody jitsi-meet-turnserver jitsi-meet-web
 jitsi-meet-web-config jitsi-videobridge2 libevent-extra-2.1-7t64 libevent-openssl-2.1-7t64 libhiredis1.1.0 libpq5
 libruby libruby3.2 lua-base6xx lua-cjson lua-inspect lua-luaossl openjdk-11-jre-headless rake ruby ruby-hacon
 ruby-net-telnet ruby-rubygems ruby-sdbm ruby-webrick ruby-xmlrpc ruby3.2 rubygems-integration sqlite3
Paquets suggérés :
 sip-router default-jre fonts-dejavu-extra fonts-ipafont-gothic fonts-ipafont-mincho fonts-wqy-microhei
 | fonts-wqy-zenhei fonts-indic ri ruby-dev bundler sqlite3-doc
Les NOUVEAUX paquets suivants seront installés :
 ca-certificates-java coturn fonts-lato java-common jicofo jitsi-meet jitsi-meet-prosody jitsi-meet-turnserver
 jitsi-meet-web jitsi-meet-web-config jitsi-videobridge2 libevent-extra-2.1-7t64 libevent-openssl-2.1-7t64
 libhiredis1.1.0 libpq5 libruby libruby3.2 lua-base6xx lua-cjson lua-inspect lua-luaossl openjdk-11-jre-headless rake
 ruby ruby-hacon ruby-net-telnet ruby-rubygems ruby-sdbm ruby-webrick ruby-xmlrpc ruby3.2 rubygems-integration
 sqlite3
0 mis à jour, 33 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 153 Mo dans les archives.
Après cette opération, 374 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 http://sn.archive.ubuntu.com/ubuntu noble-updates/main amd64 sqlite3 amd64 3.45.1-1ubuntu2.1 [144 kB]
Réception de :2 http://sn.archive.ubuntu.com/ubuntu noble/main amd64 libevent-extra-2.1-7t64 amd64 2.1.12-stable-9ubuntu2 [64,2 kB]
Réception de :3 http://sn.archive.ubuntu.com/ubuntu noble/main amd64 libevent-openssl-2.1-7t64 amd64 2.1.12-stable-9ubuntu2 [64,2 kB]
```

## Outil de configuration des paquets



```
3 partiellement installés ou enlevés.
Après cette opération, 0 o d'espace disque supplémentaires seront utilisés.
Paramétrage de jitsi-meet-prosody (1.0.8448-1) ...
modulemanager      error      Unable to load module 'roster_command': /usr/lib/prosody/modules/share/lua/5.4/mod_roster_command.lua: No such file or directory
Failed to load module 'roster_command': /usr/lib/prosody/modules/share/lua/5.4/mod_roster_command/mod_roster_command.lua: No such file or directory
dpkg: erreur de traitement du paquet jitsi-meet-prosody (--configure):
  le sous-processus paquet jitsi-meet-prosody script post-installation installé a renvoyé un état de sortie d'erreur non zéro
dpkg: des problèmes de dépendances empêchent la configuration de jitsi-meet-turnserver :
  jitsi-meet-turnserver dépend de jitsi-meet-prosody; cependant :
    Le paquet jitsi-meet-prosody n'est pas encore configuré.

dpkg: erreur de traitement du paquet jitsi-meet-turnserver (--configure):
  problèmes de dépendances - laissé non configuré
dpkg: des problèmes de dépendances empêchent la configuration de jitsi-meet :
  jitsi-meet dépend de jitsi-meet-prosody (= 1.0.8448-1); cependant :
    Le paquet jitsi-meet-prosody n'est pas encore configuré.

dpkg: erreur de traitement du paquet jitsi-meet (--configure):
  problèmes de dépendances - laissé non configuré
Aucun rapport « apport » n'a été créé car le message d'erreur indique une erreur consécutive à un échec précédent.
rapport « apport » n'a été créé car le message d'erreur indique une erreur consécutive à un échec précédent.
Des erreurs ont été rencontrées pendant l'exécution :
  jitsi-meet-prosody
  jitsi-meet-turnserver
  jitsi-meet
E: Sub-process /usr/bin/dpkg returned an error code (1)
root@mail:/home/aissata#
```

Pour résoudre ce problème, nous avons essayé de nettoyer les paquets cassés, Vérifier le module Prosody, Retenter l'installation, et même de Vérifier le statut des services mais toujours rien.

## 5. DNS avancées :

Le DNS (Domain Name System) est un système essentiel sur Internet et les réseaux locaux, permettant de convertir les noms de domaine en adresses IP. Plutôt que de mémoriser des adresses IP complexes comme, le DNS permet d'utiliser des noms compréhensibles .

On installe bind9 et bind9utils par la commande `apt install bind9 bind9utils`

```
soxna@jjk:~$ sudo apt update && sudo apt install -y bind9 bind9utils bind9-
[sudo] password for soxna:
Hit:1 http://sn.archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://security.ubuntu.com/ubuntu focal-security InRelease [128 kB]
Get:3 http://sn.archive.ubuntu.com/ubuntu focal-updates InRelease [128 kB]
Get:4 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Me
ta [65,3 kB]
Get:5 http://sn.archive.ubuntu.com/ubuntu focal-backports InRelease [128 kB]
Get:6 http://security.ubuntu.com/ubuntu focal-security/restricted amd64 DEP
Metadata [212 B]
Get:7 http://security.ubuntu.com/ubuntu focal-security/universe amd64 DEP-1
tadata [160 kB]
Get:8 http://security.ubuntu.com/ubuntu focal-security/multiverse amd64 DEP
Metadata [940 B]
Get:9 http://sn.archive.ubuntu.com/ubuntu focal-updates/main i386 Packages
7 kB
Get:10 http://sn.archive.ubuntu.com/ubuntu focal-updates/main amd64 Package
800 kB
Get:11 http://sn.archive.ubuntu.com/ubuntu focal-updates/main amd64 DEP-11
data [276 kB]
Get:12 http://sn.archive.ubuntu.com/ubuntu focal-updates/restricted amd64 D
1 Metadata [212 B]
Get:13 http://sn.archive.ubuntu.com/ubuntu focal-updates/universe amd64 DEP
```

On regarde s'il est bien allumé :

```
Processing triggers for urw (0.50+ubuntu1) ...
s Files jjk:~$ sudo systemctl status bind9
● named.service - BIND Domain Name Server
   Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset=>
   Active: active (running) since Mon 2025-03-03 10:26:04 GMT; 44s ago
     Docs: man:named(8)
   Main PID: 37182 (named)
      Tasks: 8 (limit: 2247)
     Memory: 7.0M
    CGroup: /system.slice/named.service
            └─37182 /usr/sbin/named -f -u bind

mar 03 10:26:04 jjk.smarttech.sn named[37182]: network unreachable resolving '>
mar 03 10:26:04 jjk.smarttech.sn named[37182]: network unreachable resolving '>
mar 03 10:26:04 jjk.smarttech.sn named[37182]: network unreachable resolving '>
mar 03 10:26:04 jjk.smarttech.sn named[37182]: network unreachable resolving '>
mar 03 10:26:05 jjk.smarttech.sn named[37182]: managed-keys-zone: Initializing>
mar 03 10:26:05 jjk.smarttech.sn named[37182]: managed-keys-zone: Initializing>
mar 03 10:26:05 jjk.smarttech.sn named[37182]: checkhints: b.root-servers.net/>
lines 1-20/20 (END)
```

Modifions /etc/bind/named.conf.local pour définir nos zones DNS.

```
GNU nano 4.8          /etc/bind/named.conf.local      Modif
// Do any local configuration here
//
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

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

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.192.168.1.25";
};
```

Créons les fichiers de zone (par exemple, /etc/bind/db.smarttech.sn) :

```
GNU nano 4.8          /etc/bind/db.smarttech.sn
;
; BIND data file for local loopback interface
;
$TTL    604800
@      IN      SOA     ns1.smarttech.sn. admin.smarttech.sn. (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )     ; Negative Cache TTL
; DNS SERVER
@      IN      NS      ns1.smarttech.sn.

; MAIN DNS SERVER
ns1    IN      A       192.168.1.25

; KERBEROS SERVER
;          IN      A       192.168.1.25
```

Ajoutons les enregistrements DNS nécessaires (A, MX, SRV, NAPTR, etc.).

```
; BIND data file for local loopback interface
;
$TTL    604800
@      IN      SOA     ns1.smarttech.sn. admin.smarttech.sn. (
                      2           ; Serial
                      604800      ; Refresh
                      86400       ; Retry
                     2419200     ; Expire
                     604800 )     ; Negative Cache TTL
; DNS SERVER
```

```

; DNS SERVER          604800 )      ; Negative Cache TTL
@       IN      NS      ns1.smarttech.sn.

; MAIN DNS SERVER
ns1     IN      A       192.168.1.25

; KERBEROS SERVER
jjk     IN      A       192.168.1.25

; LDAP SERVER
ldap   IN      A       192.168.1.25

; IREDMAIL SERVER
mail   IN      A       192.168.1.25
@       IN      MX 10  mail.smarttech.sn.

; SIP SERVER
sip    IN      A       192.168.1.25

```

```

; ENREGISTREMENTS SRV
_kerberos._udp.smarttech.sn.    IN SRV 0 100 88 jjk.smarttech.sn.
_kerberos._tcp.smarttech.sn.    IN SRV 0 100 88 jjk.smarttech.sn.
_kpasswd._udp.smarttech.sn.    IN SRV 0 100 464 jjk.smarttech.sn.
_ldap._tcp.smarttech.sn.        IN SRV 0 100 88 ldap.smarttech.sn.
_sip._udp.smarttech.sn.        IN SRV 0 100 5060 sip.smarttech.sn.
_sip._tcp.smarttech.sn.        IN SRV 0 100 5060 sip.smarttech.sn.

; ENREGISTREMENTS NAPTR
smarttech.sn. [REDACTED] IN      NAPTR 10 100 "S" "SIP+D2U" "" _sip._udp.smarttech.sn.
smarttech.sn.   IN      NAPTR 10 100 "S" "SIP+D2T" "" _sip._tcp.smarttech.sn. >

```

On vérifie que la configuration fonctionne :

```

root@jjk:/home/soxna# sudo named-checkzone smarttech.sn /etc/bind/db.smarttech.
sn
zone smarttech.sn/IN: loaded serial 2
OK
root@jjk:/home/soxna# sudo systemctl reload bind9
root@jjk:/home/soxna#

```

On vérifie la résolution local du DNS :

```

GNU nano 4.8                               /etc/resolv.conf
# This file is managed by man:systemd-resolved(8). Do
#
# This is a dynamic resolv.conf file for connecting lo
# internal DNS stub resolver of systemd-resolved. This
# configured search domains.
#
# Run "resolvectl status" to see details about the up
# currently in use.
#
# Third party programs must not access this file direc
# symlink at /etc/resolv.conf. To manage man:resolv.co
# replace this symlink by a static file or a different
#
# See man:systemd-resolved.service(8) for details abo
# operation for /etc/resolv.conf.

nameserver 192.168.1.25
options edns0 trust-ad
search home smarttech.sn

```

## Explications :

- \_ Bind9 est configuré pour résoudre les noms de domaine pour votre réseau.
- \_ Les fichiers de zone contiennent les enregistrements DNS qui associent les noms de domaine aux adresses IP et aux services.

## Scénarios de test :

Utilisons nslookup ou dig pour interroger votre serveur DNS pour différents enregistrements.  
Vérifions que les réponses DNS sont correctes :

```
root@jjk:/home/soxna# nslookup ldap.smarttech.sn 192.168.1.25
Server:      192.168.1.25
Address:     192.168.1.25#53

Name:   ldap.smarttech.sn
Address: 192.168.1.25

root@jjk:/home/soxna#
```

## **Intégration Kerberos/LDAP**

Modifions /etc/krb5.conf pour pointer vers notre serveur LDAP. On a ajoute la ligne dns\_lookup\_kdc :

```
GNU nano 4.8                               /etc/krb5.conf
•
[libdefaults]
    default_realm = SMARTTECH.SN
    dns_lookup_kdc = true
# The following krb5.conf variables are only for MIT
    kdc_timeout = 1

[realms]
    SMARTTECH.SN = {
        kdc = jjk.smarttech.sn
        admin_server = jjk.smarttech.sn
        kpasswd_server = jjk.smarttech.sn
    }
```

## **Configuration du KDC :**

Modifions /etc/krb5kdc/kdc.conf pour spécifier l'emplacement du serveur LDAP.

## **Configuration de LDAP :**

Modifieons /etc/ldap/ldap.conf et /etc/hosts pour assurer la cohérence avec votre DNS.

```
[dbmodules]
openldap_ldapconf = {
    db_library = kldap
    ldap_kerberos_container_dn = "cn=krbContainer,dc=smarttech,dc=sn"
    ldap_kdc_dn = "cn=admin,dc=smarttech,dc=sn"
    ldap_kadmind_dn = "cn=admin,dc=smarttech,dc=sn"
    ldap_service_password_file = /etc/krb5kdc/service.keyfile
    ldap_servers = "ldap://ldap.smarttech.sn"
}
```

Configurons slapd pour écouter sur toutes les interfaces en ajoutant 0.0.0.0 :

```

GNU nano 4.8                               /etc/default/slapd

# slapd normally serves ldap only on all TCP-ports 389. slapd
# service requests on TCP-port 636 (ldaps) and requests via u
# sockets.
# Example usage:
# SLAPD_SERVICES="ldap://127.0.0.1:389/ ldaps:/// ldapi:///"
SLAPD_SERVICES="ldap://0.0.0.0/ ldapi:///"

# If SLAPD_NO_START is set, the init script will not start or

```

Faire la correspondance dans hosts :

```

GNU nano 4.8                               /etc/hosts

127.0.0.1      localhost
127.0.1.1      soxna-VirtualBox
192.168.1.25   jjk.smarttech.sn ldap.smarttech.sn
# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

```

Configurons nslcd et libnss-ldapd pour utiliser notre DNS :

```

GNU nano 4.8                               /etc/nslcd.conf

# /etc/nslcd.conf
# nslcd configuration file. See nslcd.conf(5)
# for details.

# The user and group nslcd should run as.
uid nslcd
gid nslcd

# The location at which the LDAP server(s) should
uri ldap://ldap.smarttech.sn

```

```

GNU nano 4.8                               /etc/ldap/ldap.conf

#
# LDAP Defaults
#

# See ldap.conf(5) for details
# This file should be world readable but not world wri

BASE    dc=smarttech,dc=sn
URI    ldap://ldap.smarttech.sn
#URI   ldap://ldap.example.com ldap://ldap-master.ex

```

```
soxna@jjk:~$ sudo systemctl restart krb5-kdc
soxna@jjk:~$ sudo systemctl restart slapd
soxna@jjk:~$ sudo systemctl restart nscd
soxna@jjk:~$ sudo systemctl restart ns lcd
```

### Explications :

- \_ Kerberos et LDAP sont configurés pour s'intégrer et utiliser les mêmes informations d'identification.
- \_ Les configurations pointent vers le serveur LDAP et assurent la cohérence entre les services.

### Scénarios de test

Utilisons kinit pour obtenir un ticket Kerberos avec un utilisateur LDAP. Vérifions que l'authentification réussit :

```
root@j jk:/home/soxna# kinit jwick
Password for jwick@SMARTTECH.SN:
root@j jk:/home/soxna# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: jwick@SMARTTECH.SN

Valid starting      Expires          Service principal
03.03.2025 13:30:59  03.03.2025 23:30:59  krbtgt/SMARTTECH.SN@SMARTTECH.SN
                  renew until 04.03.2025 13:30:49
root@j jk:/home/soxna#
```

Testons la résolution des utilisateurs DNS :

```
root@j jk:/home/soxna# getent passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
root@j jk:/home/soxna#
```

```
se
avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
saned:x:117:123::/var/lib/saned:/usr/sbin/nologin
nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
fwupd-refresh:x:122:127:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin
geooclue:x:123:128::/var/lib/geooclue:/usr/sbin/nologin
pulse:x:124:129:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:125:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:126:131:Gnome Display Manager:/var/lib/gdm3:/bin/false
sssd:x:127:132:sssd system user,,,:/var/lib/sss:/usr/sbin/nologin
soxna:x:1000:1000:Soxna,,,:/home/soxna:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper,:/usr/sbin/nologin
openldap:x:128:135:OpenLDAP Server Account,,,:/var/lib/ldap:/bin/false
ns lcd:x:129:136:ns lcd name service LDAP connection daemon,,,:/var/run/ns lcd:/usr/sbin/nologin
freerad:x:130:137::/etc/freeradius:/usr/sbin/nologin
bind:x:131:140::/var/cache/bind:/usr/sbin/nologin
jwick:x:1000:1000:John wick:/home/jwick:/bin/bash
smbadmin:*:10000:10000:smbadmin:/home/smbadmin:/bin/bash
root@j jk:/home/soxna#
```

Utilisons ldapsearch pour interroger le serveur LDAP avec un utilisateur Kerberos :

```
root@jjk:/home/soxna# ldapsearch -x -H ldap://ldap.smarttech.sn -b "dc=smarttech,dc=sn"
# extended LDIF
#
# LDAPv3
# base <dc=smarttech,dc=sn> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#
# smarttech.sn
dn: dc=smarttech,dc=sn
objectClass: top
objectClass: dcObject
objectClass: organization
o: smarttech.sn
dc: smarttech

# admin, smarttech.sn
dn: cn=admin,dc=smarttech,dc=sn
objectClass: simpleSecurityObject
```

```
objectClass: krbTicketPolicyAux

# kiprop/jjk.smarttech.sn@SMARTTECH.SN, SMARTTECH.SN, krbContainer, smarttech.s
n
dn: krbPrincipalName=kiprop/jjk.smarttech.sn@SMARTTECH.SN,cn=SMARTTECH.SN,cn=k
rbContainer,dc=smarttech,dc=sn
krbLoginFailedCount: 0
krbMaxTicketLife: 36000
krbMaxRenewableAge: 604800
krbTicketFlags: 0
krbPrincipalName: kiprop/jjk.smarttech.sn@SMARTTECH.SN
krbPrincipalExpiration: 19700101000000Z
krbLastPwdChange: 19700101000000Z
krbExtraData:: AALSXMNnZGJfY3JLYXRpb25AU01BULRURUNILLNOAA==
krbExtraData:: AAcBAAIAAlUAAAAAAA=
objectClass: krbPrincipal
objectClass: krbPrincipalAux
objectClass: krbTicketPolicyAux

# search result
search: 2
result: 0 Success

# numResponses: 24
# numEntries: 23
root@jjk:/home/soxna# █
```

## 6. Accès Distant :

### a. SSH :

- Installation et configuration de ssh :

```
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openSSH-server est déjà la version la plus récente (1:8.9p1-3ubuntu0.11).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libmecab2 libprotobuf-lite23
  mecab-ipadic mecab-ipadic-utf8 mecab-utils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 178 non mis à jour.
ndella@mail:~$
```

On voit que le serveur SSH est déjà installé.

Démarrons et activons SSH :

```
ndella@mail:~$ sudo systemctl start ssh
sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /lib/systemd/system
d-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable ssh
ndella@mail:~$
```

Vérifions que SSH tourne bien :

```
ndella@mail:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
  Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
  Active: active (running) since Mon 2025-03-03 20:33:21 GMT; 13min ago
    Docs: man:sshd(8)
          man:sshd_config(5)
   Main PID: 1053 (sshd)
      Tasks: 1 (limit: 9280)
     Memory: 1.1M
        CPU: 41ms
       CGroup: /system.slice/ssh.service
               └─1053 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

mars 03 20:33:20 mail.smarttech.sn systemd[1]: Starting OpenBSD Secure Shell server...
mars 03 20:33:21 mail.smarttech.sn systemd[1]: Started OpenBSD Secure Shell server.
mars 03 20:33:21 mail.smarttech.sn sshd[1053]: Server listening on 0.0.0.0 port 22.
mars 03 20:33:21 mail.smarttech.sn sshd[1053]: Server listening on :: port 22.
lines 1-16/16 (END)
```

L'ajout du compte **ndella** sur le serveur par la commande : #**useradd -m -s /bin/bash ndella** . On teste par la commande : **kadmin.local**

```
#addprinc ndella
```

```
root@mail:/home/ndella# useradd -m -s /bin/bash ndella
useradd : l'utilisateur 'ndella' existe déjà
root@mail:/home/ndella# kadmin.local
Authenticating as principal root/admin@SMARTTECH.LOCAL with password.
kadmin.local: addprinc ndella
No policy specified for ndella@SMARTTECH.LOCAL; defaulting to no policy
Enter password for principal "ndella@SMARTTECH.LOCAL":
Re-enter password for principal "ndella@SMARTTECH.LOCAL":
Principal "ndella@SMARTTECH.LOCAL" created.
```

On édite le fichier **/etc/ssh/sshd\_config** pour décommenter les deux lignes suivantes :

```
#GSSAPIAuthentication yes
#GSSAPICleanupCredentials yes
```

```

GNU nano 6.2                               /etc/ssh/sshd_config *
#KerberosGetAFSToken no

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

```

Puis on redémarre ssh : **systemctl restart ssh**

### b. RDP:

Installons xRDP sur le serveur :

```

ndella@mail:~$ sudo apt install xrdp -y
[sudo] Mot de passe de ndella :
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
xrdp est déjà la version la plus récente (0.9.17-2ubuntu2).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 165 non mis à jour.
ndella@mail:~$ 

```

Démarrons et activons xRDP :

```

ndella@mail:~$ sudo systemctl start xrdp
sudo systemctl enable xrdp
Synchronizing state of xrdp.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable xrdp

```

Ajoutons l'utilisateur à xRDP :

```

ndella@mail:~$ sudo adduser jdoe
Ajout de l'utilisateur « jdoe » ...
Ajout du nouveau groupe « jdoe » (1006) ...
Ajout du nouvel utilisateur « jdoe » (1005) avec le groupe « jdoe » ...
Création du répertoire personnel « /home/jdoe » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour jdoe
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
    NOM []:
        Numéro de chambre []:
        Téléphone professionnel []:
        Téléphone personnel []:
        Autre []:
Ces informations sont-elles correctes ? [0/n]
ndella@mail:~$ 

```

Ajoute-le au groupe ssl-cert pour éviter les erreurs d'accès :

```

ndella@mail:~$ sudo adduser xrdp ssl-cert
[sudo] Mot de passe de ndella :
Ajout de l'utilisateur « xrdp » au groupe « ssl-cert » ...
Ajout de l'utilisateur xrdp au groupe ssl-cert
Fait.
ndella@mail:~$ 

```

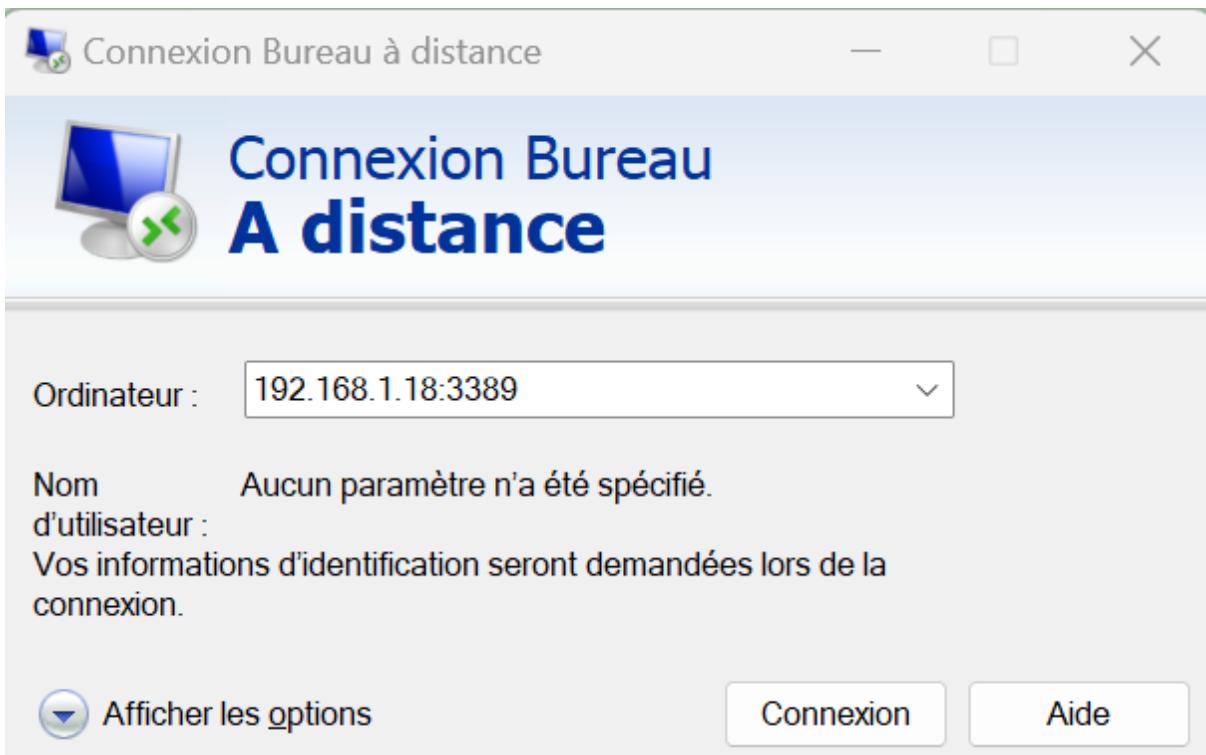
Redémarrons xRDP :

```

ndella@mail:~$ sudo systemctl restart xrdp
ndella@mail:~$ 

```

Sur un PC Windows, ouvre **Connexion Bureau à Distance (mstsc)** et entre :



### c. NoVNC :

NoVNC permet d'accéder à l'interface graphique via un navigateur web. Installons le serveur VNC :

```
ndella@mail:~$ sudo apt install tightvncserver -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  tightvncpasswd
Paquets suggérés :
  tightvnc-java
Les NOUVEAUX paquets suivants seront installés :
  tightvncpasswd tightvncserver
0 mis à jour, 2 nouvellement installés, 0 à enlever et 160 non mis à jour.
Il est nécessaire de prendre 690 ko dans les archives.
Après cette opération, 1 827 ko d'espace disque supplémentaires seront utilisés.
Réception de :1 http://sn.archive.ubuntu.com/ubuntu jammy/universe amd64 tightvncpasswd amd64 1:1.3.10-5 [14,5 kB]
Réception de :2 http://sn.archive.ubuntu.com/ubuntu jammy/universe amd64 tightvncserver amd64 1:1.3.10-5 [676 kB]
690 ko réceptionnés en 48s (14,4 ko/s)
Sélection du paquet tightvncpasswd précédemment désélectionné.
(Lecture de la base de données... 488798 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../tightvncpasswd_1%3a1.3.10-5_amd64.deb ...
Dépaquetage de tightvncpasswd (1:1.3.10-5) ...
Sélection du paquet tightvncserver précédemment désélectionné.
Préparation du dépaquetage de .../tightvncserver_1%3a1.3.10-5_amd64.deb ...
Dépaquetage de tightvncserver (1:1.3.10-5) ...
Paramétrage de tightvncpasswd (1:1.3.10-5) ...
Paramétrage de tightvncserver (1:1.3.10-5) ...
update-alternatives: renommer le lien secondaire Xvnc.1.gz de /usr/share/man/man1/Xvnc.1.gz à /usr/share/man/man1/Xvnc
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
ndella@mail:~$
```

Configurons le mot de passe VNC :

```

ndella@mail:~$ vncserver

You will require a password to access your desktops.

Password:
Verify:
Would you like to enter a view-only password (y/n)? y
Password:
Verify:

New Xtigervnc server 'mail.smarttech.sn:2 (ndella)' on port 5902 for display :2.
Use xtigervncviewer -SecurityTypes VncAuth -passwd /home/ndella/.vnc/passwd :2 to connect to the VNC server.

=====
[mi] mieq: warning: overriding existing handler (nil) with 0x5e0df8a3db90 for event 2
[mi] mieq: warning: overriding existing handler (nil) with 0x5e0df8a3db90 for event 3
Terminated
X connection to :2 broken (explicit kill or server shutdown).

Mon Mar  3 23:52:29 2025
ComparingUpdateTracker: 0 pixels in / 0 pixels out
ComparingUpdateTracker: (1:-nan ratio)
Killing Xtigervnc process ID 50782... success!
=====

Session startup via '/etc/X11/Xtigervnc-session' cleanly exited too early (< 3 seconds)!

Maybe try something simple first, e.g.,
    tigervncserver -xstartup /usr/bin/xterm
The Xtigervnc server cleanly exited!
The X session cleanly exited!

```

Arrêtons VNC avant d'installer NoVNC et Instalions NoVNC :

```

ndella@mail:~$ sudo apt install novnc websockify -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  docutils-common ieee-data python3-dateutil python3-debtcollector python3-deprecated python3-docutils
  python3-is08601 python3-jwcrypto python3-msgpack python3-netaddr python3-novnc python3-oslo.config
  python3-oslo.context python3-oslo.i18n python3-oslo.log python3-oslo.serialization python3-oslo.utils
  python3-rfc3986 python3-roman python3-stevedore python3-websockify python3-wrapt
Paquets suggérés :
  python-nova python-debtcollector-doc docutils-doc fonts-linuxlibertine | ttf-linux-libertine
  texlive-lang-french texlive-latex-base texlive-latex-recommended ipython3 python-netaddr-docs
  python3-nova python-oslo.log-doc
Les NOUVEAUX paquets suivants seront installés :
  docutils-common ieee-data novnc python3-dateutil python3-debtcollector python3-deprecated
  python3-docutils python3-is08601 python3-jwcrypto python3-msgpack python3-netaddr python3-novnc
  python3-oslo.config python3-oslo.context python3-oslo.i18n python3-oslo.log
  python3-oslo.serialization python3-oslo.utils python3-rfc3986 python3-roman python3-stevedore
  python3-websockify python3-wrapt websockify
0 mis à jour, 24 nouvellement installés, 0 à enlever et 160 non mis à jour.
Il est nécessaire de prendre 4 242 ko dans les archives.
Après cette opération, 24,0 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 docutils-common all 0.17.1+dfsg-2 [17 kB]
Réception de :2 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 ieee-data all 20210605.1 [1 887 kB]
Réception de :3 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 python3-wrapt amd64 1.13.3-1build1 [34,0 kB]
Réception de :4 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 python3-debtcollector all 2.3.0-0ubuntu1 [13,7 kB]
Réception de :5 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 python3-roman all 3.3-1 [10,6 kB]
Réception de :6 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 python3-docutils all 0.17.1+dfsg-2 [387 kB]
Réception de :7 http://sn.archive.ubuntu.com/ubuntu jammy/main amd64 python3-netaddr all 0.8.0-2 [309 kB]

```

Démarrons le service NoVNC :

```
ndella@mail:~$ websockify --web=/usr/share/novnc/ --cert=./self.pem 6080 localhost:5901
websockify --web=/usr/share/novnc/ --cert=./self.pem 6080 localhost:5901
WebSocket server settings:
- Listen on :6080
- Web server. Web root: /usr/share/novnc
- No SSL/TLS support (no cert file)
- proxying from :6080 to localhost:5901
192.168.1.19 - [03/Mar/2025 23:57:57] code 404, message File not found
```

Accémons à NoVNC via un navigateur :



- [app/](#)
- [core/](#)
- [include/](#)
- [utils/](#)
- [vendor/](#)
- [vnc.html](#)
- [vnc\\_auto.html@](#)
- [vnc\\_lite.html](#)

## 7. TFTP ET FTP :

### a. TFTP :

Le TFTP (Trivial File Transfer Protocol) est un protocole simplifié utilisé pour le transfert de fichiers. Contrairement au FTP qui utilise le protocole TCP (Transmission Control Protocol) sur le port 21, le TFTP fonctionne sur UDP (User Datagram Protocol) sur le port 69. Cette différence implique que tant le client que le serveur doivent gérer la perte potentielle de paquets de données. Comparé au FTP, le TFTP présente plusieurs simplifications. Par exemple, il ne prend pas en charge le listing des fichiers, ni les méthodes d'authentification ou de chiffrement. De plus, il nécessite la connaissance préalable du nom du fichier à transférer. Le TFTP se limite essentiellement au transfert de fichiers entre deux hôtes réseau, sans fonction d'authentification.

En raison de l'absence de mécanisme de fenêtrage, le TFTP peut être moins efficace sur des liaisons à forte latence, ce qui le rend généralement adapté aux réseaux locaux. Il est couramment utilisé pour des tâches telles que la sauvegarde de configurations d'équipements réseau ou le démarrage de stations de travail sans disque dur.

- Installation et configuration du serveur TFTP :

Nous allons tout d'abord télécharger FTP avec la commande : **apt install tftp-hpa tftpd-hpa**

```

ndella@mail:~$ sudo apt install tftp-hpa tftpd-hpa
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
tftp-hpa est déjà la version la plus récente (5.2+20150808-1.2build2).
tftpd-hpa est déjà la version la plus récente (5.2+20150808-1.2build2).
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libmecab2 libprotobuf-lite23
  mecab-ipadic mecab-ipadic-utf8 mecab-utils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
0 mis à jour, 0 nouvellement installés, 0 à enlever et 133 non mis à jour.

```

Maintenant on édite le fichier **/etc/default/tftpd-hpa** comme suit :

TFTP\_USERNAME : le nom d'utilisateur du service

TFTP\_DIRECTORY : on met /var/lib/tftpboot qui est le répertoire de base

TFTP\_ADDRESS : on met notre adresse ip et le port d'écoute du service

TFTP\_OPTION : on ajoute -c pour permettre au client d'envoyer des fichiers au niveau du serveur

```

GNU nano 6.2                               /etc/default/tftpd-hpa *
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/var/lib/tftpboot"
TFTP_ADDRESS="192.168.1.19:69"
TFTP_OPTIONS="--secure -c"

□

```

On crée le répertoire **/var/lib/tftpboot** et on accorde les droits par **chown -R tftp /var/lib/tftpboot**.

```

ndella@mail:~$ sudo chown -R tftp:tftp /var/lib/tftpboot/
[sudo] Mot de passe de ndella :
ndella@mail:~$ sudo chown -R 777 /var/lib/tftpboot/
ndella@mail:~$ □

```

On va démarrer les service pour regarder si le port d'écoute est fonctionnel.

```

ndella@mail:~$ sudo systemctl status tftpd-hpa
● tftpd-hpa.service - LSB: HPA's tftp server
  Loaded: loaded (/etc/init.d/tftpd-hpa; generated)
  Active: active (running) since Wed 2025-02-12 17:16:00 GMT; 50s ago
    Docs: man:systemd-sysv-generator(8)
  Process: 32371 ExecStart=/etc/init.d/tftpd-hpa start (code=exited, status=0/SUCCESS)
  Tasks: 1 (limit: 9282)
  Memory: 776.0K
    CPU: 16ms
   CGroup: /system.slice/tftpd-hpa.service
           └─32379 /usr/sbin/in.tftpd --listen --user tftp --address 192.168.1.19:69

févr. 12 17:16:00 mail.smarttech.sn systemd[1]: Starting LSB: HPA's tftp server...
févr. 12 17:16:00 mail.smarttech.sn tftpd-hpa[32371]: * Starting HPA's tftpd in.tft...
févr. 12 17:16:00 mail.smarttech.sn tftpd-hpa[32371]: ...done.
févr. 12 17:16:00 mail.smarttech.sn systemd[1]: Started LSB: HPA's tftp server.
lines 1-15 (END)□

```

## b. FTP:

File Transfer Protocol ( Protocole de Transfert de Fichiers ) ou encore FTP, est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer, modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

- Installation et configuration du serveur ftp :

Nous allons tout d'abord télécharger FTP avec la commande : **apt install vsftpd**.

```
ndella@mail:~$ sudo apt install vsftpd -y
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :
  libevent-core-2.1-7 libevent-pthreads-2.1-7 libmecab2 libprotobuf-lite23
  mecab-ipadic mecab-ipadic-utf8 mecab-utils
Veuillez utiliser « sudo apt autoremove » pour les supprimer.
Les paquets suivants seront mis à jour :
  vsftpd
1 mis à jour, 0 nouvellement installés, 0 à enlever et 132 non mis à jour.
Il est nécessaire de prendre 123 ko dans les archives.
Après cette opération, 0 o d'espace disque supplémentaires seront utilisés.
Réception de :1 http://sn.archive.ubuntu.com/ubuntu jammy-updates/main amd64 vsftpd a
md64 3.0.5-0ubuntu1.1 [123 kB]
123 ko réceptionnés en 1s (153 ko/s)
Préconfiguration des paquets...
(Lecture de la base de données... 488553 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de .../vsftpd_3.0.5-0ubuntu1.1_amd64.deb ...
Dépaquetage de vsftpd (3.0.5-0ubuntu1.1) sur (3.0.5-0ubuntu1) ...
Paramétrage de vsftpd (3.0.5-0ubuntu1.1) ...
vsftpd user (ftp) already exists, doing nothing.

vsftpd directory (/srv/ftp) already exists, doing nothing.
Traitement des actions différées (« triggers ») pour man-db (2.10.2-1) ...
```

Et ensuite, nous allons dans le fichier de configuration du serveur qui est: **/etc/vsftpd.conf** ou nous allons modifier les valeurs des paramètres selon nos besoins et finir par redémarrer le service.

```
GNU nano 6.2                               /etc/vsftpd.conf *
# daemon started from an initscript.
listen=YES
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
listen_ipv6=YES
#
# Allow anonymous FTP? (Disabled by default).
anonymous_enable=NO
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
```

```
ndella@mail:~$ service vsftpd restart
ndella@mail:~$ █
```

## **8. Serveur de téléphonie sur IP (TOIP) :**

Le service de téléphonie sur IP (ToIP) révolutionne la manière dont nous communiquons en permettant la transmission de la voix via Internet plutôt que par les réseaux téléphoniques traditionnels. Cette technologie offre des avantages considérables en termes de coût, de flexibilité et de fonctionnalités.

### **✓ Installation et configuration d'un serveur Asterisk pour la gestion des appels**

On va commencer par installer les dépendances nécessaires pour la compilation d'asterisk :

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo apt-get install gcc g++ make libncurses5-dev
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  binutils binutils-common binutils-x86-64-linux-gnu g++-11 gcc-11 libasan6 libbinutils libc-dev-bin libc-devtools libc6 libc6-dbg
  libcc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libgcc-11-dev libitm liblsan0 libncurses-dev libnsl-dev libquadmath0
  libstdc++-11-dev libtirpc-dev libtsan0 libubsan1 linux-libc-dev manpages-dev rpcsvc-proto
Paquets suggérés :
  binutils-doc g++-multilib g++-11-multilib gcc-11-doc gcc-multilib autoconf automake libtool flex bison gcc-doc gcc-11-multilib
  gcc-11-locales glibc-doc ncurses-doc libstdc++-11-doc make-doc
Paquets recommandés :
  libnss-nis libnss-nisplus
Les NOUVEAUX paquets suivants seront installés :
  binutils binutils-common binutils-x86-64-linux-gnu g++ g++-11 gcc gcc-11 libasan6 libbinutils libc-dev-bin libc-devtools
  libcc6-dev libcc1-0 libcrypt-dev libctf-nobfd0 libctf0 libgcc-11-dev libitm liblsan0 libncurses-dev libnsl-dev
  libquadmath0 libstdc++-11-dev libtirpc-dev libtsan0 libubsan1 linux-libc-dev make manpages-dev rpcsvc-proto
Les paquets suivants seront mis à jour :
  libc6 libc6-dbg
2 mis à jour, 31 nouvellement installés, 0 à enlever et 200 non mis à jour.
Il est nécessaire de prendre 53,2 Mo/70,3 Mo dans les archives.
Après cette opération, 183 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n]
```

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo ./contrib/scripts/install_prereq install
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Les paquets supplémentaires suivants seront installés :
  aptitude-common libcwidget4 libdpkg-perl libfile-fcntllock-perl libxapian30
Paquets suggérés :
  apt-xapian-index aptitude-doc-en | aptitude-doc debtags tasksel libcwidget-dev debian-keyring git bzr xapian-tools
Les NOUVEAUX paquets suivants seront installés :
  aptitude aptitude-common libcwidget4 libdpkg-perl libfile-fcntllock-perl libxapian30
0 mis à jour, 6 nouvellement installés, 0 à enlever et 200 non mis à jour.
Il est nécessaire de prendre 4097 ko dans les archives.
Après cette opération, 19,8 Mo d'espace disque supplémentaires seront utilisés.
Réception de :1 http://sn.archive.ubuntu.com/ubuntu jammy/universe amd64 aptitude-common all 0.8.13-3ubuntu1 [1719 kB]
23% [1 aptitude-common 1175 kB/1719 kB 68%]
```

Téléchargement et extraction de Asterisk :

```
japhet@asterisk:/usr/src/asterisk$ sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-18-current.tar.gz
--2025-03-04 13:32:26- http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-18-current.tar.gz
Résolution de downloads.asterisk.org (downloads.asterisk.org)... 165.22.184.19, 2604:a880:400:d0::14:9001
Connexion à downloads.asterisk.org (downloads.asterisk.org)|165.22.184.19|:80... connecté.
réquête HTTP transmise, en attente de la réponse.. 200 OK
Taille : 28565082 (27M) [application/octet-stream]
Enregistre : 'asterisk-18-current.tar.gz'

asterisk-18-current.tar.gz      100%[=====] 27,24M 1,18MB/s   ds 23

2025-03-04 13:32:49 (1,21 MB/s) - 'asterisk-18-current.tar.gz' enregistré [28565082/28565082]

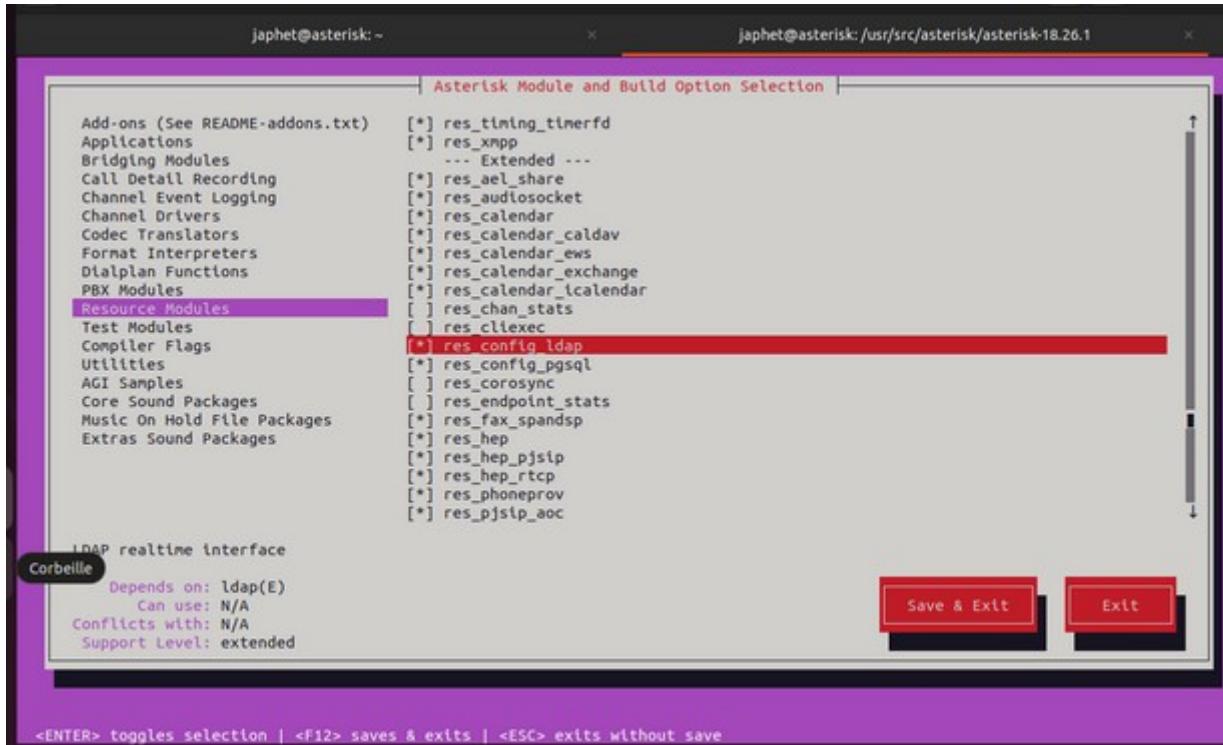
japhet@asterisk:/usr/src/asterisk$ sudo tar -xvzf asterisk-18-current.tar.gz
asterisk-18.26.1/
asterisk-18.26.1/.cleanccount
asterisk-18.26.1/.gitignore
asterisk-18.26.1/.lastclean
asterisk-18.26.1/.version
asterisk-18.26.1/BSDDMakefile
asterisk-18.26.1/BUGS
asterisk-18.26.1/CHANGES.md
asterisk-18.26.1/COPYING
asterisk-18.26.1/CREDITS
asterisk-18.26.1/ChangeLogs/
asterisk-18.26.1/ChangeLogs/Changelog-18.18.0.md
asterisk-18.26.1/ChangeLogs/Changelog-18.18.1.md
asterisk-18.26.1/ChangeLogs/Changelog-18.19.0.md
asterisk-18.26.1/ChangeLogs/Changelog-18.20.0.md
asterisk-18.26.1/ChangeLogs/Changelog-18.20.1.md
asterisk-18.26.1/ChangeLogs/Changelog-18.20.2.md
asterisk-18.26.1/ChangeLogs/Changelog-18.21.0.md
asterisk-18.26.1/ChangeLogs/Changelog-18.22.0.md
asterisk-18.26.1/ChangeLogs/Changelog-18.23.0.md
asterisk-18.26.1/ChangeLogs/Changelog-18.23.1.md
asterisk-18.26.1/ChangeLogs/Changelog-18.24.0.md
asterisk-18.26.1/ChangeLogs/Changelog-18.24.1.md
asterisk-18.26.1/ChangeLogs/Changelog-18.24.2.md
asterisk-18.26.1/ChangeLogs/Changelog-18.24.3.md
```

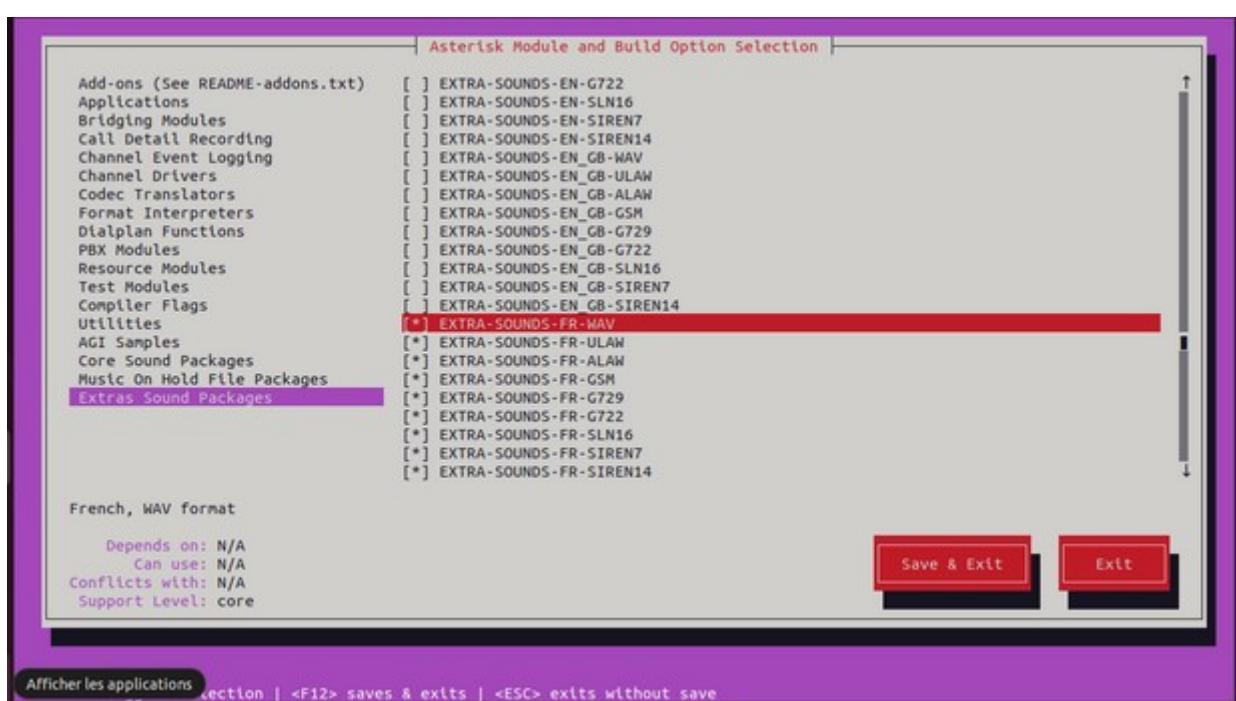
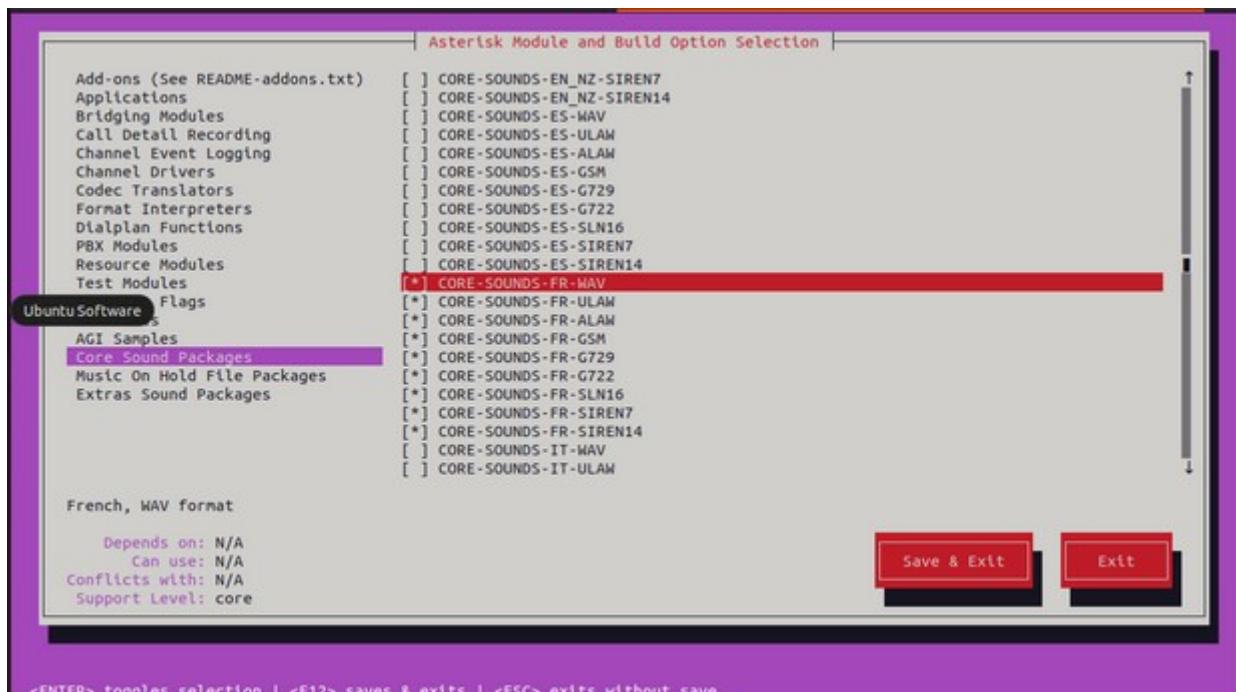
## Compilation d'Asterisk :

## Ajout du module LDAP pour asterisk et sélection des voix françaises :

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo make menuconfig
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="--silent" cmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk/asterisk-18.26.1/menuselect »
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES -I/usr/include/libxml2 -c -o menuselect.o menuselect.c
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES -c -o strcompat.o strcompat.c
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES -c -o menuselect_curses.o menuselect_curses.c
gcc -o menuselect menuselect.o strcompat.o menuselect_curses.o -lncurses -ltinfo -lxml2
make[1] : on quitte le répertoire « /usr/src/asterisk/asterisk-18.26.1/menuselect »
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="--silent" nmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk/asterisk-18.26.1/menuselect »
gcc -g -D_GNU_SOURCE -Wall -Wno-deprecated-declarations -DHAVE_NCURSES -c -o menuselect_newt.o menuselect_newt.c
gcc -o nmenuselect menuselect.o strcompat.o menuselect_newt.o -lnewt -lxml2
make[1] : on quitte le répertoire « /usr/src/asterisk/asterisk-18.26.1/menuselect »
CC="cc" CXX="g++" LD="" AR="" RANLIB="" CFLAGS="" LDFLAGS="" make -C menuselect CONFIGURE_SILENT="--silent" gmenuselect
make[1] : on entre dans le répertoire « /usr/src/asterisk/asterisk-18.26.1/menuselect »
make[1]: rien à faire pour « gmenuselect ».
make[1] : on quitte le répertoire « /usr/src/asterisk/asterisk-18.26.1/menuselect »
make[1] : on entre dans le répertoire « /usr/src/asterisk/asterisk-18.26.1 »
Generating input for menuselect ...

```





## Compilation du code source d'asterisk

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo make
[CC] astcanary.c -> astcanary.o
[LD] astcanary.o -> astcanary
[CC] astdb2sqlite3.c -> astdb2sqlite3.o
[CC] hash/hash.c -> hash/hash.o
[CC] hash/hash_bigkey.c -> hash/hash_bigkey.o
[CC] hash/hash_buf.c -> hash/hash_buf.o
[CC] hash/hash_func.c -> hash/hash_func.o
[CC] hash/hash_log2.c -> hash/hash_log2.o
[CC] hash/hash_page.c -> hash/hash_page.o
[CC] hash/ndbm.c -> hash/ndbm.o
[CC] btree/bt_close.o -> btree/bt_close.o
[CC] btree/bt_conv.c -> btree/bt_conv.o
```

```

[japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ make
[CC] res_timing_timerfd.c -> res_timing_timerfd.o
[LD] res_timing_timerfd.o -> res_timing_timerfd.so
[CC] res_tonedetect.c -> res_tonedetect.o
[LD] res_tonedetect.o -> res_tonedetect.so
[CC] res_xmpp.c -> res_xmpp.o
[LD] res_xmpp.o -> res_xmpp.so
Building Documentation For: channels pbx apps codecs formats cdr cel bridges funcs tests main res addons
----- Asterisk Build Complete -----
+ Asterisk has successfully been built, and +
+ can be installed by running:
+
+     make install
+
+japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$
```

Installation des fichiers nécessaires après la compilation du code source d'Asterisk :

```

japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo make install
Installing modules from channels...
Installing modules from pbx...
Installing modules from apps...
Installing modules from codecs...
Installing modules from formats...
Installing modules from cdr...
Installing modules from cel...
Installing modules from bridges...
Installing modules from funcs...
Installing modules from tests...
Installing modules from main...
Installing modules from res...
Installing modules from addons...
/usr/bin/install -c -m 755 contrib/scripts/astversion "/usr/sbin/"
/usr/bin/install -c -m 755 contrib/scripts/astgenkey "/usr/sbin/"
/usr/bin/install -c -m 755 contrib/scripts/autosupport "/usr/sbin/"
./build_tools/install_subst contrib/scripts/safe_asterisk "/usr/sbin/safe_asterisk";
/usr/bin/install -c -m 644 doc/core-*.xml "/var/lib/asterisk/documentation"
/usr/bin/install -c -m 644 doc/appdocsxml.xslt "/var/lib/asterisk/documentation"
/usr/bin/install -c -m 644 doc/appdocsxml.dtd "/var/lib/asterisk/documentation"
/usr/bin/install -c -m 644 doc/asterisk.8 "/usr/share/man/man8"
/usr/bin/install -c -m 644 doc/astdb*.8 "/usr/share/man/man8"
/usr/bin/install -c -m 644 contrib/scripts/astgenkey.8 "/usr/share/man/man8"
done
----- Asterisk Installation Complete -----
+
+ YOU MUST READ THE SECURITY DOCUMENT +
+
+ Asterisk has successfully been installed. +
+ If you would like to install the sample +
+ configuration files (overwriting any +
+ existing config files), run:
+
+ For generic reference documentation:
+     make samples
+
+ For a sample basic PBX:
+     make basic-pbx
+
+
+----- or -----+
+
+ You can go ahead and install the asterisk +
+ program documentation now or later run:
+
+     make progdocs
+
+ **Note** This requires that you have +
+ doxygen installed on your local system
+japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$
```

Installation des fichiers de configuration par défaut dans le répertoire :

```

japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo make samples
Installing adst config files...
/usr/bin/install -c -d "/etc/asterisk"
Installing configs/samples/asterisk.adst
Installing configs/samples/telcordia-1.adst
Installing other config files...
Installing file configs/samples/acl.conf.sample
Installing file configs/samples/adst.conf.sample
Installing file configs/samples/aep.conf.sample
Installing file configs/samples/agents.conf.sample
Installing file configs/samples/alarmreceiver.conf.sample
Installing file configs/samples/alsa.conf.sample
Installing file configs/samples/and.conf.sample
Installing file configs/samples/app_mysql.conf.sample
Installing file configs/samples/app_skel.conf.sample
Installing file configs/samples/ari.conf.sample
Installing file configs/samples/ast_debug_tools.conf.sample
Installing file configs/samples/asterisk.conf.sample
Installing file configs/samples/calendar.conf.sample
Installing file configs/samples/crccr.conf.sample
```

Activons le service Asterisk pour le gérer avec systemctl :

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo make config
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$
```

Démarrage du service asterisk :

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo /etc/init.d/asterisk start
Starting asterisk (via systemctl): asterisk.service.
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$
```

Lancement de la console pour vérifier le fonctionnement du serveur asterisk :

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1$ sudo asterisk -rvvvvvv
Asterisk 18.26.1, Copyright (C) 1999 - 2022, Sangoma Technologies Corporation and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY: type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 18.26.1 currently running on asterisk (plid = 40962)
asterisk*CLI>
```

Copions le schéma LDAP d'Asterisk dans le répertoire des schémas LDAP et redémarrez le service LDAP :

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1/contrib/scripts$ sudo cp asterisk.ldap-schema /etc/ldap/schema/
[sudo] Mot de passe de japhet :
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1/contrib/scripts$
```

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1/contrib/scripts$ sudo service slapd restart
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1/contrib/scripts$
```

Ajoutons le schéma à l'annuaire LDAP :

```
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1/contrib/scripts$ sudo service slapd restart
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1/contrib/scripts$ sudo ldapadd -Y EXTERNAL -H ldap:// -f ./asterisk.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=asterisk,cn=schema,cn=config"
japhet@asterisk:/usr/src/asterisk/asterisk-18.26.1/contrib/scripts$
```

Configurons ldap.conf pour asterisk :

```
GNU nano 6.2                                     /etc/asterisk/ldap.conf *

[general]
hostname = ldap://localhost
basedn = dc=smarttech,dc=sn
binddn = cn=admin,dc=smarttech,dc=sn
bindpw = 13052001

[asterisk]
basedn = ou=slp,dc=smarttech,dc=sn
filter = (&(objectClass=AsteriskSIPUser)(cn=%u))
username = cn=%u
password = AstAccountSecret
```

Configurons extconfig.conf pour asterisk :

```

GNU nano 6.2                               /etc/asterisk/extconfig.conf *
;
; Static and realtime external configuration
; engine configuration
;
; See https://docs.asterisk.org/Fundamentals/Asterisk-Configuration/Database-Support-Configuration/Realtime-Database-Configuration/
; for basic table formatting information.
;
[settings]
sippeers => ldap,"ou=sip,dc=smarttech,dc=sn",sip
sipusers => ldap,"ou=sip,dc=smarttech,dc=sn",sip
extensions => ldap,"ou=sip,dc=smarttech,dc=sn",extensions
;
; Static configuration files:
;
; file.conf => driver,database[,table[,priority]]
;
; maps a particular configuration file to the given
; database driver, database and table (or uses the
; name of the file as the table if not specified)
;
; Uncomment to load queues.conf via the odbc engine.
;
;queues.conf => odbc,asterisk,ast_config
;extensions.conf => sqlite,asterisk,ast_config
;
; The following files CANNOT be loaded from Realtime storage:
; asterisk.conf
; extconfig.conf (this file)
; logger.conf
;
; Additionally, the following files cannot be loaded from
; Realtime storage unless the storage driver is loaded
;
```

Redémarrage de asterisk :

```
japhet@asterisk:~$ sudo systemctl restart asterisk
japhet@asterisk:~$
```

## Difficultés rencontrées au niveau de ToIP

Malgré plusieurs tentatives, l'intégration n'a pas abouti. Les principales difficultés ont été :

Problèmes de chargement du module LDAP :

Lors de l'installation **du module reload**, des erreurs indiquant l'absence ou l'échec du chargement du module LDAP ont été rencontrées.

Échec du **realtime show ldap status** :

La commande ne renvoyait pas d'informations sur la connexion avec LDAP, indiquant un problème de communication ou de configuration.

Problèmes avec **sip reload** :

La tentative de recharge des utilisateurs SIP via LDAP n'a pas abouti, probablement en raison d'un mauvais mapping des attributs LDAP.

Seul **dialplan reload** a fonctionné :

Contrairement aux autres commandes, celle-ci a fonctionné correctement, ce qui suggère que la configuration du dialplan était correcte, mais que l'intégration avec LDAP posait problème.

## **CONCLUSION:**

Ce projet de fin de module nous a offert une immersion profonde dans l'administration des infrastructures réseau, en intégrant plusieurs technologies essentielles pour assurer la sécurité et la gestion centralisée des services. L'objectif était clair : mettre en place une architecture complète où l'authentification unique, la gestion des accès et les services de communication fonctionnent de manière fluide et cohérente.

L'intégration de \*Samba avec LDAP\* et de \*FreeRADIUS avec LDAP\* nous a permis de comprendre l'importance d'un annuaire centralisé pour contrôler les accès aux ressources partagées et aux réseaux sécurisés. Ces étapes, bien que complexes, ont été surmontées grâce à une analyse rigoureuse des configurations et une bonne gestion des logs.

Cependant, nous avons rencontré des difficultés plus tenaces, notamment avec \*Asterisk et LDAP, où la connexion entre le serveur de téléphonie et l'annuaire centralisé n'a pas pu être établie correctement. De même, l'installation et la configuration de \*\*iRedMail\* ont posé des défis qui restent à approfondir pour assurer un déploiement fiable du service de messagerie.

Au-delà des succès et des échecs, ce projet nous a surtout appris la \*rigueur et la méthodologie\* nécessaires en administration réseau. Chaque service dépendant des autres, il était essentiel de maîtriser leur interconnexion, de tester minutieusement chaque configuration et de savoir diagnostiquer les problèmes en profondeur.

Cette expérience met en évidence une réalité fondamentale : l'administration des systèmes et réseaux est un domaine où \*rien ne fonctionne parfaitement du premier coup, mais où chaque problème est une opportunité d'apprentissage\*. Ce projet n'est donc pas une finalité, mais une base solide sur laquelle nous pourrons continuer à bâtir et à affiner nos compétences pour des architectures réseau encore plus robustes et sécurisées.