



Rapport de Projet

Réseau

Filière : Génie Informatique

DNS, HTTPS, LDAP, FTP, SMTP, IMAP

Réalisé par :

Yassine NOUREDDINE
Slimani MOHAMED AMINE
Assadiki ZAID

Encadré par :

Rghioui ANASS

Année universitaire
2024/2025

I Introduction

Dans le paysage en constante évolution de l'informatique et des technologies de l'information, la configuration adéquate des protocoles réseau est un élément crucial pour assurer la connectivité, la sécurité et le bon fonctionnement des systèmes. Avec l'essor des technologies numériques, la demande en infrastructures réseau fiables et performantes s'intensifie. C'est dans ce contexte que notre projet s'inscrit, visant à mettre en œuvre une configuration robuste des principaux protocoles réseau tels que DNS, HTTPS, FTP, SMTP, IMAP, ainsi qu'un annuaire centralisé via LDAP, pour répondre aux exigences croissantes en termes de communication, de gestion des utilisateurs et de protection des données.

Le Domain Name System (DNS) joue un rôle fondamental en permettant la traduction des noms de domaine en adresses IP, rendant les sites web accessibles aux utilisateurs finaux de manière transparente et rapide. Une configuration optimisée du DNS garantit une résolution de nom fluide tout en protégeant contre des attaques telles que l'empoisonnement de cache ou le détournement de requêtes.

Le protocole HTTPS, devenu un standard incontournable, assure une communication sécurisée via le chiffrement des données échangées entre les clients et les serveurs web. Ce protocole est essentiel pour protéger les informations sensibles, comme les identifiants ou les transactions financières, et pour établir la confiance des utilisateurs en leur garantissant une navigation sécurisée.

Les protocoles de transfert et de gestion des données, tels que FTP, SMTP, et IMAP, occupent des fonctions spécifiques mais tout aussi importantes. FTP permet un échange efficace de fichiers entre systèmes, essentiel pour la gestion documentaire ou la synchronisation des données. SMTP (Simple Mail Transfer Protocol) est le moteur de l'envoi de courriels, tandis que IMAP (Internet Message Access Protocol) offre un accès flexible aux boîtes de messagerie, permettant une consultation en temps réel des courriels sur divers dispositifs.

En complément, LDAP (Lightweight Directory Access Protocol) joue un rôle central dans la gestion des identités et des accès au sein des systèmes réseau. Ce protocole permet de centraliser les informations sur les utilisateurs, les groupes, et les ressources, simplifiant ainsi l'administration tout en renforçant la sécurité. En intégrant OpenLDAP dans notre projet, nous avons mis en place un service d'annuaire qui garantit une gestion unifiée et efficace des données tout en facilitant l'accès sécurisé aux ressources réseau.

Cependant, la mise en œuvre de ces protocoles n'est pas sans défis. Les aspects techniques tels que la compatibilité des systèmes, les performances, ou encore la mise en place de mesures de sécurité avancées comme l'authentification multi-facteurs, représentent des étapes complexes mais nécessaires. En outre, des considérations telles que la protection contre les attaques de type déni de service (DDoS), le chiffrement des communications et la gestion des certificats numériques viennent compléter les enjeux de configuration.

Ce rapport détaille les étapes de notre projet, incluant une analyse approfondie des besoins, une planification rigoureuse des configurations, et la mise en œuvre de solutions adaptées. Les méthodologies suivies, combinées à une veille technologique constante, ont permis d'identifier et de résoudre les difficultés rencontrées, tout en optimisant les performances des protocoles.

En examinant minutieusement ces composants essentiels, nous visons à renforcer la résilience, la performance et la sécurité de notre infrastructure réseau, offrant ainsi une base solide pour soutenir les opérations actuelles.

Table des matières

I	Introduction	1
II	Configuration d'un Serveur DNS avec BIND	4
III	Configuration d'un Serveur HTTPS	8
IV	Installation et Configuration de FTP	13
V	Installation et Configuration du Serveur de Messagerie (SMTP/IMAP)	18
VI	Installation et Configuration du Serveur LDAP	22
VII	Conclusion	26

Table des figures

1	le service est actif	4
2	Configuration du fichier <code>db.direct</code>	5
3	Configuration du fichier <code>db.inverse</code>	5
4	Configuration de <code>named.conf.local</code>	6
5	Vérification de <code>db.direct</code>	6
6	Vérification de <code>db.inverse</code>	6
7	Vérification avec <code>nslookup</code>	7
8	Résultat de la vérification	7
9	Certificat SSL auto-signé généré	9
10	Fichier <code>groupe7.conf</code>	10
11	Configuration de <code>groupe7-ssl.conf</code>	10
12	Modification du fichier <code>/etc/hosts</code>	11
13	Contenu du fichier <code>index.html</code>	11
14	Vérification du statut du service Apache2	12
15	Vérification du site HTTPS	12
16	État du service <code>vsftpd</code>	13
17	Exemple de configuration de <code>vsftpd</code> (partie 1)	14
18	Exemple de configuration de <code>vsftpd</code> (partie 2)	14
19	Configuration du pare-feu	14
20	Test du répertoire FTP	15
21	Ajout de l'utilisateur à la liste <code>vsftpd.userlist</code>	15
22	Connexion via FileZilla	16
23	Connexion via l'invite de commande Windows	17
24	le serveur écoute sur le port 25	18
25	le serveur écoute sur le port 143	18
26	Configuration du compte utilisateur <code>user1</code> dans Thunderbird	19
27	Tableau de bord de Thunderbird avant le test	20
28	Envoi d'un email via l'invite de commande	21
29	Réception de l'email dans Thunderbird	21
30	Résultat de la commande <code>slapcat</code>	22
31	Exemple de contenu du fichier <code>utilisateurs_et_groupes.ldif</code>	23
32	Génération de mots de passe avec <code>slappasswd</code>	23
33	Ajout des données dans l'annuaire LDAP	24
34	Vérification des utilisateurs dans l'annuaire LDAP	24
35	Configuration du fichier <code>config.php</code>	25
36	Connexion à PHPLDAPADMIN via le navigateur	25
37	Tableau de bord de PHPLDAPADMIN	25
38	Visualisation des utilisateurs et groupes dans PHPLDAPADMIN	25

II Configuration d'un Serveur DNS avec BIND

Le DNS (*Domain Name System*) convertit les noms de domaine en adresses IP. Apache utilise ensuite ces informations pour déterminer quel site doit être servi et renvoyer la page correspondante. Cela permet d'établir une communication fluide et rapide entre les utilisateurs et les serveurs web.

Dans ce projet, nous allons configurer un serveur DNS. Le logiciel utilisé est **BIND** (*Berkeley Internet Name Domain*), qui est l'un des serveurs DNS les plus populaires. L'adresse IP de la machine configurée est : **192.168.245.49**.

Configuration et Vérification

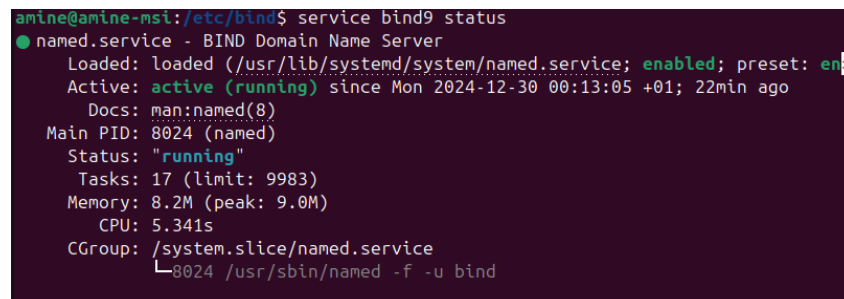
Toutes les commandes nécessaires seront exécutées en tant qu'administrateur afin d'avoir les permissions requises. Une fois BIND installé et configuré, il est important de vérifier que le service fonctionne correctement.

Pour vérifier l'état du service `bind9`, nous utilisons la commande suivante :

```
sudo systemctl status bind9
```

Cette commande permet d'afficher l'état du service. Si le service est actif, vous verrez une sortie similaire à celle-ci :

```
service bind9 status
```



```
amine@amine-msi:/etc/bind$ service bind9 status
● named.service - BIND Domain Name Server
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: en
   Active: active (running) since Mon 2024-12-30 00:13:05 +01; 22min ago
     Docs: man:named(8)
    Main PID: 8024 (named)
      Status: "running"
        Tasks: 17 (limit: 9983)
       Memory: 8.2M (peak: 9.0M)
          CPU: 5.341s
    CGroup: /system.slice/named.service
            └─8024 /usr/sbin/named -f -u bind
```

FIGURE 1 – le service est actif

Le service `bind9` est en activité et fonctionne correctement.

Configuration des fichiers de zone

Le nom de ma machine est : `DNSserver`. Le nom de domaine est : `groupe7.ehtp`. Le FQDN (Fully Qualified Domain Name) est : `Dnsserver.groupe7.ehtp`.

Les fichiers utilisés pour la configuration sont :

- `named.conf` : Configuration principale du serveur BIND.
- `named.conf.default-zones` : Configuration des zones par défaut.
- `db.local` : Fichier de configuration des enregistrements DNS pour une zone spécifique.

Création des fichiers de zone

Nous avons créé deux fichiers supplémentaires dans le dossier `/etc/bind` : `db.zonedirect` et `db.zoneinverse`.

Le fichier `db.direct` contient les enregistrements DNS pour la résolution directe (nom de domaine vers adresse IP). Voici la configuration de ce fichier :

```
GNU nano 7.2 db.direct *
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA Dnsserver.groupe7.ehtp. root.groupe7.ehtp. (
    2      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS Dnsserver.groupe7.ehtp.
Dnsserver IN A 192.168.245.100
www IN A 192.168.245.110
mail IN A 192.168.245.120
```

FIGURE 2 – Configuration du fichier `db.direct`

Le fichier `db.inverse` permet de configurer la résolution inverse (adresse IP vers nom de domaine). Voici la configuration de ce fichier :

```
GNU nano 7.2 db.inverse *
;
; BIND data file for local loopback interface
;
$TTL 604800
@ IN SOA Dnsserver.groupe7.ehtp. root.groupe7.ehtp. (
    2      ; Serial
    604800 ; Refresh
    86400  ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;
@ IN NS Dnsserver.groupe7.ehtp.
100 IN PTR Dnsserver.groupe7.ehtp.
110 IN PTR www.groupe7.ehtp.
120 IN PTR mail.groupe7.ehtp.
```

FIGURE 3 – Configuration du fichier `db.inverse`

Ensuite, nous avons modifié le fichier `named.conf.local` pour configurer les zones, comme suit :

```

GNU nano 7.2                                named.conf.local
//
// 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 "groupe7.ehtp" IN {
    type master;
    file "/etc/bind/db.direct";
};
zone "245.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/db.inverse";
};

```

FIGURE 4 – Configuration de `named.conf.local`

Pour vérifier s'il n'y a pas d'erreurs dans notre fichier `named.conf`, nous utilisons la commande suivante :

```
named - checkconf
```

Ensuite, pour vérifier les fichiers `db.direct` et `db.inverse`, nous exécutons les commandes suivantes :

```
sudo named-checkzone groupe7.ehtp /etc/bind/db.direct
```

```

amine@amine-msi:/etc/bind$ sudo named-checkzone groupe7.ehtp /etc/bind/db.direct
zone groupe7.ehtp/IN: loaded serial 2
OK

```

FIGURE 5 – Vérification de `db.direct`

```
sudo named-checkzone 245.168.192.in-addr.arpa /etc/
bind/db.inverse
```

```

amine@amine-msi:/etc/bind$ sudo named-checkzone 245.168.192.in-addr.arpa /etc/bind/db.inverse
zone 245.168.192.in-addr.arpa/IN: loaded serial 2
OK

```

FIGURE 6 – Vérification de `db.inverse`

Pour redémarrer le service BIND9, nous utilisons la commande suivante :

```
sudo systemctl restart bind9
```

Enfin, pour tester la configuration DNS, nous ajoutons l'adresse IP du serveur DNS à une autre machine et exécutons la commande suivante :

```
nslookup
```

Et voici le résultat de la commande avec l'adresse IP du serveur DNS :

```
C:\Users\MSI GF63 11UD>nslookup www.groupe7.ehtp
Serveur :    UnKnown
Address:  192.168.245.49

Nom :      www.groupe7.ehtp
Address:  192.168.245.110
```

FIGURE 7 – Vérification avec nslookup

```
C:\Users\MSI GF63 11UD>nslookup 192.168.245.110
Serveur :    UnKnown
Address:  192.168.245.49

Nom :      www.groupe7.ehtp
Address:  192.168.245.110
```

FIGURE 8 – Résultat de la vérification

La configuration du serveur DNS est maintenant terminée avec succès.

III Configuration d'un Serveur HTTPS

Le nom d'hôte du serveur : `groupe7.ehtp` Et son adresse IP : `192.168.245.49`.

Apache et OpenSSH sont des composants fondamentaux dans la mise en place d'un serveur web sécurisé et fonctionnel. Apache est un logiciel de serveur Web largement utilisé, réputé pour sa fiabilité et sa polyvalence dans la diffusion de contenu Web. Configurer Apache pour prendre en charge HTTPS implique d'activer le protocole SSL/TLS, qui crypte les données transmises entre le serveur et le client, garantissant ainsi une communication sécurisée. Cette sécurité est cruciale pour la transmission de données sensibles, telles que les identifiants de connexion, les informations financières et les détails personnels, faisant du HTTPS un protocole essentiel pour protéger la confidentialité des utilisateurs et l'intégrité des données.

D'autre part, OpenSSL, une implémentation robuste du protocole SSH (Secure Shell), offre un accès à distance sécurisé et facilite les transferts de fichiers sécurisés entre les systèmes. L'intégration d'OpenSSL dans l'environnement du serveur améliore la sécurité en permettant un accès à distance crypté pour l'administration du serveur et les transferts de fichiers sécurisés. Ensemble, Apache avec HTTPS et OpenSSH fournissent un environnement fortifié, garantissant la confidentialité et l'intégrité des communications Web tout en permettant une gestion à distance sécurisée du serveur.

1. Installer Apache

Ouvrez un terminal et exécutez les commandes suivantes pour installer Apache sur votre serveur Ubuntu :

```
sudo apt update
sudo apt install apache2
```

2. Vérifier le statut du service Apache

Une fois Apache installé, vous pouvez vérifier que le service fonctionne correctement avec la commande suivante :

```
sudo systemctl status apache2
```

Nous devons d'abord installer à la fois Apache et OpenSSL en exécutant la commande suivante :

```
sudo apt-get install openssl apache2
```

La commande `a2enmod ssl` est utilisée dans le serveur HTTP Apache sur les systèmes basés sur Debian (tels que Ubuntu) pour activer le module SSL (Secure Sockets Layer) pour Apache. Après avoir exécuté cette commande, redémarrez le service Apache2 avec la commande suivante :

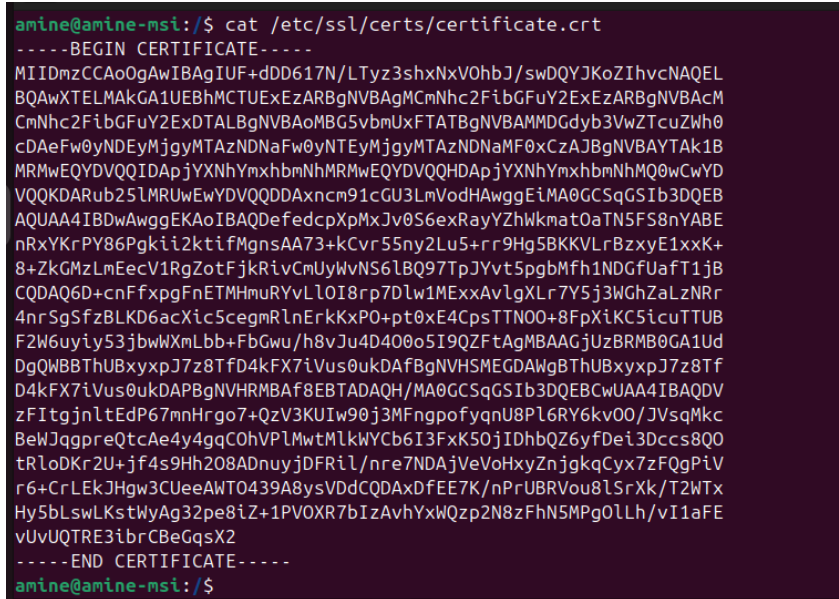
```
sudo systemctl restart apache2
```

3. Créer un certificat SSL auto-signé

Un certificat SSL auto-signé est un certificat numérique généré et signé par l'entité qu'il identifie, plutôt que par une autorité de certification (CA) tierce de confiance. Voici la commande pour générer un certificat SSL auto-signé :

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -  
keyout /etc/ssl/private/private.key -out /etc/ssl/certs/  
certificate.crt
```

Lors de l'exécution de cette commande, vous devrez répondre aux invites.
Après avoir exécuté la commande, nous obtenons la clé générée dans le fichier spécifié.



```
amine@amine-msi:/$ cat /etc/ssl/certs/certificate.crt  
-----BEGIN CERTIFICATE-----  
MIIDmzCCAoOgAwIBAgIUf+dDD617N/LTyZ3shxNxV0hbJ/swDQYJKoZIhvcNAQEL  
BQAwXTElMAkGA1UEBhMCTUEuExARBgNVBAgMCmNhczFibGFuY2ExARBgNVBAcM  
CmNhczFibGFuY2ExDTALBgNVBAoMBG5vbmUxFTATBgNVBAMMDGdyb3VwZTcuZW00  
cDAeFw0yNDEyMjgyMTAzNDNaFw0yNTEyMjgyMTAzNDNaMF0xCzAJBgNVBAYTAk1B  
MRMwEQYDVQIDApjYXNhYm9hbmNhMRMwEQYDVQQHDApjaXNhYm9hbmNhMQ0wCwYD  
VQQKDARub25LMRUwEwYDVQQDDAxcncm91cGU3LmVodHAwggEiMA0GCSqGSIb3DQEB  
AQUAA4IBDwAwggEKAoIBAQDefedcpXpMxJv0S6exRayYZhWkmat0aTN5FS8nYABE  
nRxYKrPY86Pgkii2ktifMgnsAA73+kCvr55ny2Lu5+rr9Hg5BKKVLRBzxyE1xxK+  
8+ZkGMzLmEecV1RgZotFjkRivCmUyWvNS6LBQ97TpJYvt5pgbMfh1NDGfUafT1jB  
CQDAQ6D+cnFfxpgFnETMHmuRyVlL0I8rp7Dlw1MExxAvgXLr7Y5j3WGHZaLzNRr  
4nrSgSfzBLKD6acXicScegmlnErkKxPO+pt0xE4CpsTTN00+8FpXikC5icuTTUB  
F2W6uyiy53jBwXmLbb+fbGwu/h8vJu4D400o5I9QZFtAgMBAAGjUzBRMB0GA1Ud  
DgQWB8ThUBxyxpJ7z8TfD4kFX7iVus0ukDAfBgNVHSMEGDAwG8ThUBxyxpJ7z8Tf  
D4kFX7iVus0ukDAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBGwUAA4IBAQDV  
zFIItgjnltEdP67mnHrgo7+QzV3KUIw90j3MFngpofyqnU8P16RY6kv00/JVsqMkc  
BeWJqgpreQtCae4y4gqC0hVPLMwtMlKwYCb6I3FxK50jIDhbQZ6yFDei3Dccs8Q0  
tRl0DKr2U+jf4s9Hh208ADnuyjDFRil/nre7NDAjVeVoHxyZnjgkqCyx7zFQgPiV  
r6+CrLEKJHgw3CUeeAWT0439A8ysVDdCQDAxDfEE7K/nPrUBRVou8LSrXk/T2WTx  
Hy5blswLKstWyAg32pe8iZ+1PVOXR7bIzAvhYxwQzp2N8zFhN5MPg0LLh/vI1aFE  
vUvUQTRE3ibrCBeGqsX2  
-----END CERTIFICATE-----  
amine@amine-msi:/$
```

FIGURE 9 – Certificat SSL auto-signé généré

4. Créer un fichier VirtualHost

Créons maintenant notre fichier VirtualHost. Le fichier est à créer dans le dossier : `/etc/apache2/sites-available/`. Puisque Apache est livré avec un fichier VirtualHost par défaut, utilisons-le comme base. Nous copions le fichier `000-default.conf` vers `groupe7.conf` :

```
sudo cp 000-default.conf groupe7.conf
```

Le fichier `groupe7.conf` devrait ressembler à ceci :

```

GNU nano 7.2                               groupe7.conf *
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/groupe7
    ServerName groupe7.ehtp

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

```

FIGURE 10 – Fichier `groupe7.conf`

Après avoir configuré notre site Web, nous devons activer le fichier de configuration des hôtes virtuels pour l'activer. Nous faisons cela en exécutant la commande suivante dans le répertoire du fichier de configuration :

```
sudo a2ensite groupe7.conf
```

5. Activer SSH sur Apache

Maintenant que nous avons créé notre site, nous allons essayer d'activer SSH sur Apache. Créons le fichier `groupe7-ssl.conf` et ajoutons la configuration suivante :

```

GNU nano 7.2                               groupe7-ssl.conf
<VirtualHost *:443>

    SSLEngine on
    SSLCertificateKeyFile /etc/ssl/private/private.key
    SSLCertificateFile /etc/ssl/certs/certificate.crt

    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/groupe7
    ServerName groupe7.ehtp

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

```

FIGURE 11 – Configuration de `groupe7-ssl.conf`

Ensuite, nous devons ajouter `192.168.245.49 groupe7.ehtp` dans le fichier `/etc/hosts`.

```
GNU nano 7.2 /etc/hosts
127.0.0.1 localhost
127.0.1.1 amine-msi
192.168.245.49 groupe7.ehtp

# 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
```

FIGURE 12 – Modification du fichier `/etc/hosts`

6. Créer le fichier `index.html`

Ensuite, nous allons créer un fichier `index.html` dans le chemin `/var/www/groupe7/` :

```
amine@amine-msi: /var/www/groupe7
GNU nano 7.2 index.html
<!DOCTYPE html>
<html lang="fr">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>Bienvenue sur Groupe7</title>
  <style>
    body {
      font-family: Arial, sans-serif;
      background-color: #f4f4f9;
      color: #333;
      text-align: center;
      padding: 50px;
    }
    h1 {
      color: #4CAF50;
    }
    p {
      font-size: 1.2em;
    }
  </style>
</head>
<body>
  <h1>Bienvenue sur Groupe7</h1>
  <p>Ceci est le site web de Groupe7</p>
</body>
</html>
```

FIGURE 13 – Contenu du fichier `index.html`

7. Activer la version SSL de votre site

Après cela, nous devons activer la version SSL de notre site. Nous pouvons exécuter cette commande pour activer le site :

```
sudo a2ensite groupe7-ssl.conf
```

Nous pouvons vérifier la configuration Apache2 avec la commande suivante :

```
sudo apache2ctl -t
```

S'il y avait des erreurs ou des fautes, elles apparaîtraient. Une fois aucune erreur, nous redémarrons le service Apache2 :

```
sudo systemctl restart apache2
```

8. Vérification du statut d'Apache

Une fois Apache redémarré, nous vérifions le statut avec la commande suivante :

```
sudo systemctl status apache2
```

Voici le résultat affiché lorsque le serveur est actif :

```
amine@amine-msi:/var/www/groupe7$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-12-30 01:31:14 +01; 19s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 12221 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
    Main PID: 12225 (apache2)
      Tasks: 55 (limit: 9983)
     Memory: 6.7M (peak: 7.4M)
        CPU: 54ms
   CGroup: /system.slice/apache2.service
           └─12225 /usr/sbin/apache2 -k start
             └─12227 /usr/sbin/apache2 -k start
               └─12228 /usr/sbin/apache2 -k start

Dec 30 01:31:14 amine-msi systemd[1]: Starting apache2.service - The Apache HTTP Server...
Dec 30 01:31:14 amine-msi apachectl[12224]: AH00558: apache2: Could not reliably determine the
Dec 30 01:31:14 amine-msi systemd[1]: Started apache2.service - The Apache HTTP Server.
lines 1-17/17 (END)
```

FIGURE 14 – Vérification du statut du service Apache2

9. Vérification du site

Enfin, voici à quoi ressemble notre site après l'activation :

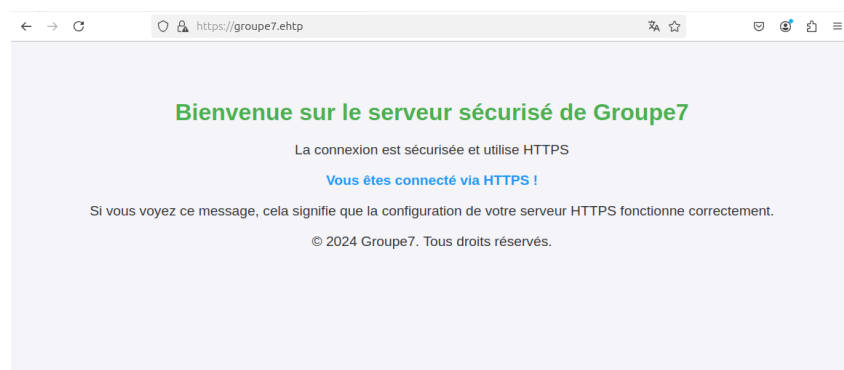


FIGURE 15 – Vérification du site HTTPS

IV Installation et Configuration de FTP

1. Installation de vsftpd

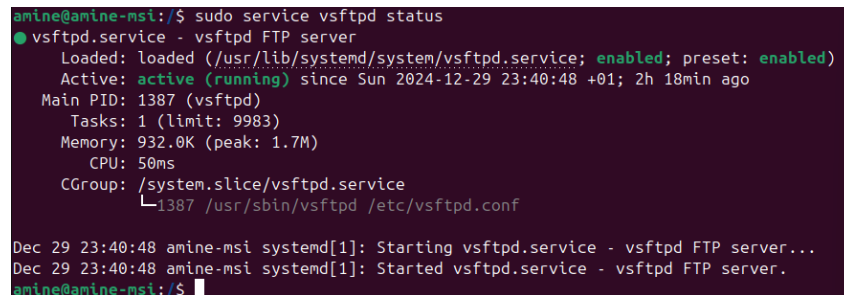
Pour installer `vsftpd`, commencez par mettre à jour la liste des paquets disponibles, puis exécutez les commandes suivantes :

```
sudo apt update
sudo apt install vsftpd
```

2. Vérification de l'état du service FTP

Après l'installation, assurez-vous que le service `vsftpd` est actif et en cours d'exécution en utilisant la commande suivante :

```
sudo systemctl status vsftpd
```



```
amine@amine-msi:/$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
   Active: active (running) since Sun 2024-12-29 23:40:48 +01; 2h 18min ago
     Main PID: 1387 (vsftpd)
       Tasks: 1 (limit: 9983)
      Memory: 932.0K (peak: 1.7M)
         CPU: 50ms
        CGroup: /system.slice/vsftpd.service
                └─1387 /usr/sbin/vsftpd /etc/vsftpd.conf

Dec 29 23:40:48 amine-msi systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Dec 29 23:40:48 amine-msi systemd[1]: Started vsftpd.service - vsftpd FTP server.
amine@amine-msi:/$
```

FIGURE 16 – État du service `vsftpd`


3. Configuration du serveur FTP

Le fichier de configuration principal de `vsftpd` se trouve à l'emplacement suivant :

```
/etc/vsftpd.conf
```

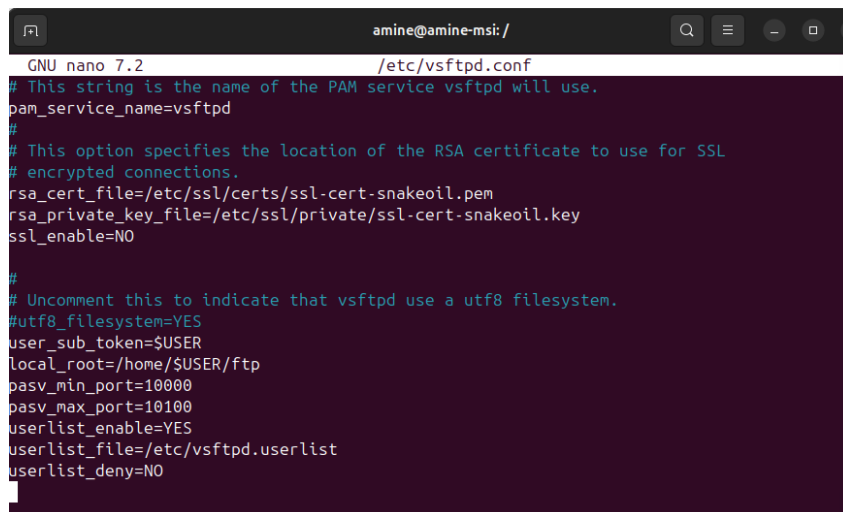
Pour le modifier, utilisez la commande suivante :

```
sudo nano /etc/vsftpd.conf
```



```
amine@amine-msi: /etc/vsftpd.conf
GNU nano 7.2
# daemon started from an initscript.
listen=NO
#
# 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
#
```

FIGURE 17 – Exemple de configuration de vsftpd (partie 1)



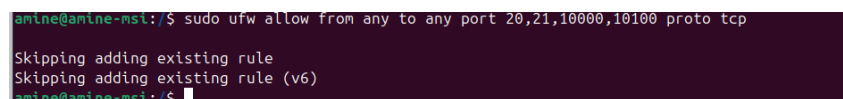
```
amine@amine-msi: /etc/vsftpd.conf
GNU nano 7.2
# This string is the name of the PAM service vsftpd will use.
pam_service_name=vsftpd
#
# This option specifies the location of the RSA certificate to use for SSL
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO
#
# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES
user_sub_token=$USER
local_root=/home/$USER/ftp
pasv_min_port=10000
pasv_max_port=10100
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

FIGURE 18 – Exemple de configuration de vsftpd (partie 2)

4. Configuration du pare-feu

Pour permettre au serveur FTP de fonctionner correctement, ouvrez les ports requis en utilisant la commande suivante :

```
sudo ufw allow from any to any port 20,21,10000,10100 proto tcp
```



```
amine@amine-msi:/$ sudo ufw allow from any to any port 20,21,10000,10100 proto tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
amine@amine-msi:/$
```

FIGURE 19 – Configuration du pare-feu

5. Création d'un utilisateur FTP

Pour ajouter un utilisateur ayant accès au serveur FTP, exécutez la commande suivante :

```
sudo adduser nourddine
```

Ensuite, créez un répertoire FTP pour cet utilisateur :

```
sudo mkdir /home/nourddine/ftp
```

Affectez les permissions appropriées au répertoire :

```
sudo chown nobody:nogroup /home/nourddine/ftp
```

Enfin, ajoutez un sous-répertoire pour les téléchargements :

```
sudo mkdir /home/nourddine/ftp/upload
```



FIGURE 20 – Test du répertoire FTP

6. Ajout de l'utilisateur à la liste FTP

Modifiez le fichier `/etc/vsftpd.userlist` pour y ajouter le nouvel utilisateur :

```
sudo nano /etc/vsftpd.userlist
```

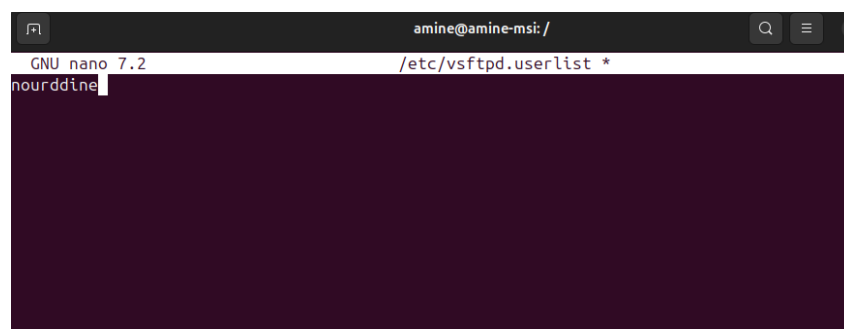


FIGURE 21 – Ajout de l'utilisateur à la liste `vsftpd.userlist`

7. Test de la connexion FTP

Vous pouvez tester la connexion au serveur FTP en utilisant deux méthodes :

Méthode 1 : Via FileZilla Utilisez FileZilla pour vous connecter au serveur en fournissant les informations de connexion.

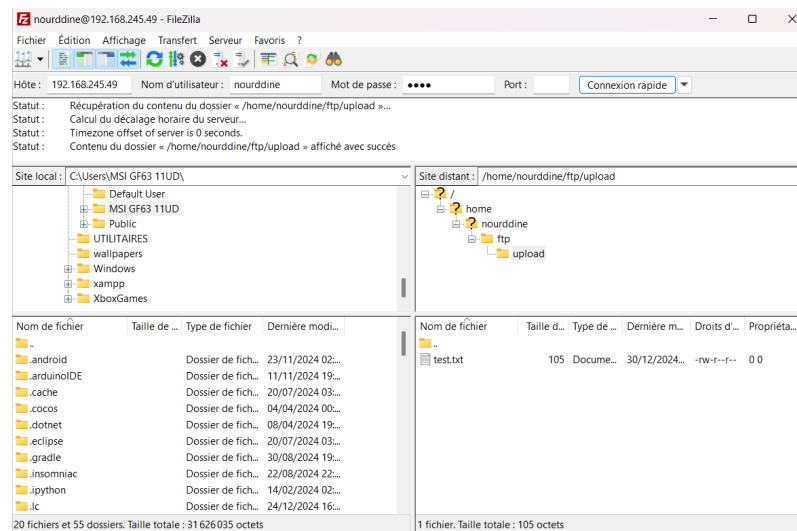


FIGURE 22 – Connexion via FileZilla

Méthode 2 : Via la ligne de commande Utilisez la commande FTP dans l'invite de commandes de Windows :

```

C:\Users\MSI GF63 11UD\Documents\fichier>dir
Le volume dans le lecteur C s'appelle Windows
Le numéro de série du volume est 8270-984D

Répertoire de C:\Users\MSI GF63 11UD\Documents\fichier

30/12/2024  02:46    <DIR>          .
30/12/2024  02:41    <DIR>          ..
               0 fichier(s)                0 octets
               2 Rép(s)    4 542 513 152 octets libres

C:\Users\MSI GF63 11UD\Documents\fichier>ftp 192.168.245.49
Connecté à 192.168.245.49.
220 Welcome to server FTP service.
200 Always in UTF8 mode.
Utilisateur (192.168.245.49:(none)) : nourddine
331 Please specify the password.
Mot de passe :

230 Login successful.
ftp> cd upload
250 Directory successfully changed.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0      0          105 Dec 30 02:32 test.txt
226 Directory send OK.
ftp : 69 octets reçus en 0.01 secondes à 9.86 Ko/s.
ftp> get test.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for test.txt (105 bytes).
226 Transfer complete.
ftp : 105 octets reçus en 0.00 secondes à 105.00 Ko/s.
ftp> by
221 Goodbye.

C:\Users\MSI GF63 11UD\Documents\fichier>dir
Le volume dans le lecteur C s'appelle Windows
Le numéro de série du volume est 8270-984D

Répertoire de C:\Users\MSI GF63 11UD\Documents\fichier

30/12/2024  02:47    <DIR>          .
30/12/2024  02:41    <DIR>          ..
30/12/2024  02:47                105 test.txt
               1 fichier(s)                105 octets
               2 Rép(s)    4 541 652 992 octets libres

C:\Users\MSI GF63 11UD\Documents\fichier>

```

FIGURE 23 – Connexion via l'invite de commande Windows

V Installation et Configuration du Serveur de Messagerie (SMTP/IMAP)

1. Installer et Configurer Postfix

Tout d'abord, installez le serveur de messagerie **Postfix** en exécutant la commande suivante :

```
sudo apt-get install postfix
```

Ensuite, reconfigurez **Postfix** en utilisant la commande suivante pour définir les options de configuration, telles que la liste des domaines gérés par le serveur (par exemple, `groupe7.ehtp`) :

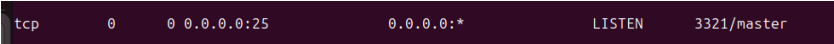
```
sudo dpkg-reconfigure postfix
```

Après la configuration, redémarrez le service **Postfix** :

```
sudo systemctl restart postfix
```

Vérifiez que le serveur écoute sur le port 25 en exécutant la commande suivante :

```
sudo netstat -apn --inet
```



tcp	0	0 0.0.0.0:25	0.0.0.0:*	LISTEN	3321/master
-----	---	--------------	-----------	--------	-------------

FIGURE 24 – le serveur écoute sur le port 25

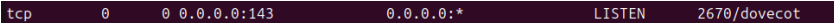
2. Installer et Configurer Dovecot IMAP

Installez le serveur **IMAP** en exécutant la commande suivante pour installer **Dovecot** **IMAP** :

```
sudo apt-get install dovecot-imapd
```

Vérifiez ensuite que le serveur écoute sur le port **IMAP** (port 143) avec la commande suivante :

```
sudo netstat -apn --inet
```



tcp	0	0 0.0.0.0:143	0.0.0.0:*	LISTEN	2670/dovecot
-----	---	---------------	-----------	--------	--------------

FIGURE 25 – le serveur écoute sur le port 143

3. Créer des Utilisateurs et Répertoires

Créez deux utilisateurs `user1` et `user2` et leurs répertoires respectifs avec les commandes suivantes :

```
sudo useradd -m -d /home/user1 user1
sudo useradd -m -d /home/user2 user2
```

4. Installer le Client de Messagerie Thunderbird

Installez le client de messagerie **Thunderbird** en exécutant la commande suivante :

```
sudo apt-get install thunderbird
```

Après l'installation, définissez le mot de passe de **user1** avec la commande suivante :

```
sudo passwd user1
```

Lancez ensuite **Thunderbird**, créez un nouvel utilisateur et configurez-le pour tester la réception et l'envoi d'emails.

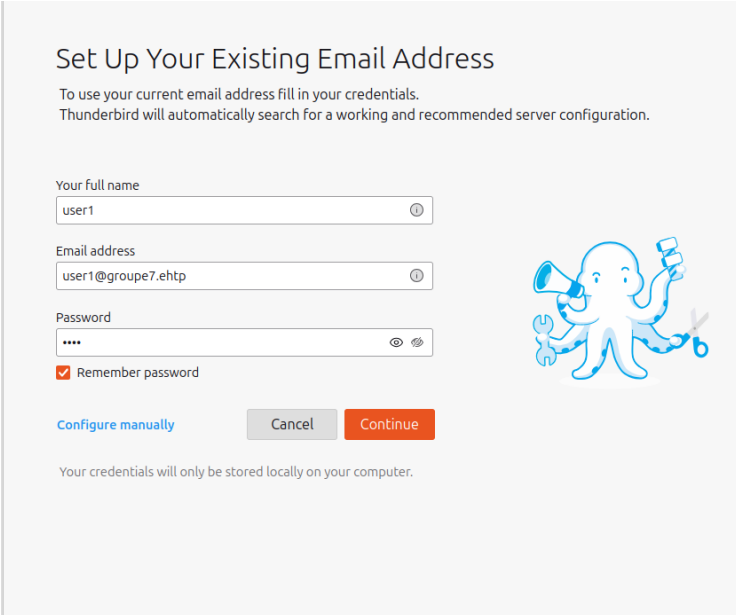


FIGURE 26 – Configuration du compte utilisateur **user1** dans Thunderbird

5. Tester l'Envoi et la Réception des Emails

Avant le test, voici le tableau de bord de **Thunderbird** avec le compte configuré :

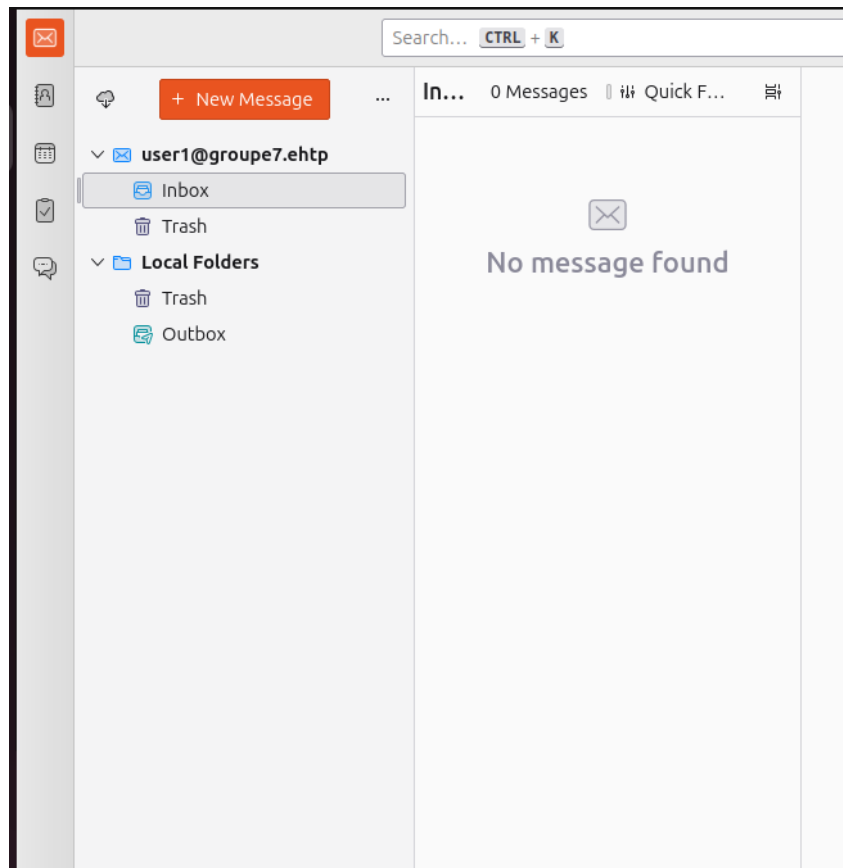


FIGURE 27 – Tableau de bord de Thunderbird avant le test

Pour tester l'envoi d'un email, connectez-vous au serveur SMTP en utilisant la commande suivante dans l'invite de commande :

```
telnet 127.0.0.1 25
```

Ensuite, envoyez un email en utilisant les commandes SMTP et vérifiez que l'email est bien reçu dans la boîte de réception de **Thunderbird** :

```

amine@amine-msi:/$ telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 amine-msi ESMTP Postfix (Ubuntu)
MAIL from:user2@groupe7.ehtp
250 2.1.0 Ok
RCPT TO:user1@groupe7.ehtp
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Bonjour tout le monde.
.
250 2.0.0 Ok: queued as 85003888FA

```

FIGURE 28 – Envoi d'un email via l'invite de commande

Enfin, voici la réception de l'email dans la boîte de réception de Thunderbird :

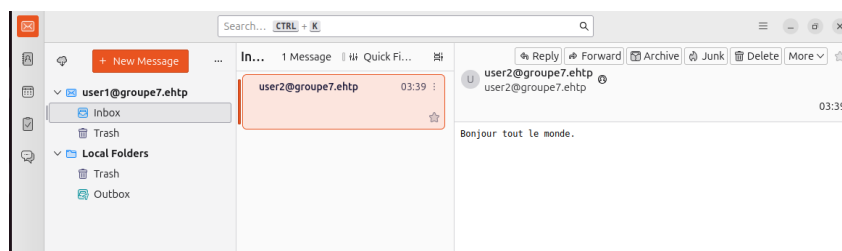


FIGURE 29 – Réception de l'email dans Thunderbird

VI Installation et Configuration du Serveur LDAP

Dans le cadre de notre projet réseau, nous avons implémenté OpenLDAP comme serveur d'annuaire centralisé. Le serveur, identifié par le nom d'hôte `ldap.groupe7.ehtp` et l'adresse IP `192.168.245.29`, joue un rôle crucial en stockant et organisant les informations relatives aux utilisateurs, groupes, et ressources réseau. Cette configuration vise à garantir une gestion efficace et sécurisée des données.

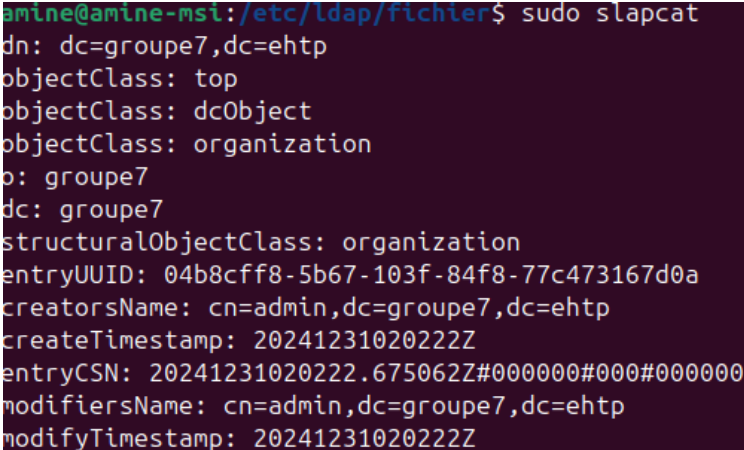
Installation d'OpenLDAP

nous procédons à l'installation d'OpenLDAP :

```
sudo apt install slapd ldap-utils -y
```

Une fois l'installation terminée, la commande suivante permet de vérifier la configuration initiale :

```
sudo slapcat
```



```
amine@amine-msi:/etc/ldap/fichier$ sudo slapcat
dn: dc=groupe7,dc=ehtp
objectClass: top
objectClass: dcObject
objectClass: organization
o: groupe7
dc: groupe7
structuralObjectClass: organization
entryUUID: 04b8cff8-5b67-103f-84f8-77c473167d0a
creatorsName: cn=admin,dc=groupe7,dc=ehtp
createTimestamp: 20241231020222Z
entryCSN: 20241231020222.675062Z#000000#000#000000
modifiersName: cn=admin,dc=groupe7,dc=ehtp
modifyTimestamp: 20241231020222Z
```

FIGURE 30 – Résultat de la commande `slapcat`

Configuration de l'Annuaire

Nous créons un répertoire dédié pour stocker les fichiers de configuration :

```
sudo mkdir /etc/ldap/fichier
```

Dans ce répertoire, un fichier `utilisateurs_et_groupes.ldif` est créé pour définir les utilisateurs et groupes. Voici un exemple du contenu :

Gestion des Mots de Passe

Les mots de passe des utilisateurs sont hachés avec l'algorithme SSHA. Pour générer un mot de passe sécurisé, utilisez :

```
slappasswd
```

```

GNU nano 7.2      utilisateurs_et_groupes.ldif
# Unité organisationnelle : Utilisateurs
dn: ou=utilisateurs,dc=groupe7,dc=ehtp
objectClass: organizationalUnit
ou: utilisateurs

# Unité organisationnelle : Groupes
dn: ou=groupes,dc=groupe7,dc=ehtp
objectClass: organizationalUnit
ou: groupes

# Utilisateur : Amine Slimani
dn: cn=Amine Slimani,ou=utilisateurs,dc=groupe7,dc=ehtp
objectClass: inetOrgPerson
cn: Amine Slimani
sn: Slimani
mail: amine.slimani@groupe7.ehtp
userPassword: {SSHA}RRIm60npbqZCNTpDc2H3x0Miz+b2XAwM

# Utilisateur : Yassine Nourddine
dn: cn=Yassine Nourddine,ou=utilisateurs,dc=groupe7,dc=ehtp
objectClass: inetOrgPerson
cn: Yassine Nourddine
sn: Nourddine
mail: yassine.nourddine@groupe7.ehtp
userPassword: {SSHA}U2qmLNJQrPzb+g8t/wllcNTY+MCuXnUn

# Utilisateur : Zaid Assadiki
dn: cn=Zaid Assadiki,ou=utilisateurs,dc=groupe7,dc=ehtp
objectClass: inetOrgPerson
cn: Zaid Assadiki
sn: Assadiki
mail: zaid.assadiki@groupe7.ehtp
userPassword: {SSHA}97FEHJeImRJV7LYmC35n9aRBWocMaWa

```

FIGURE 31 – Exemple de contenu du fichier utilisateurs_et_groupes.ldif

```

amine@amine-msi:/etc/ldap/fichier$ slappasswd
New password:
Re-enter new password:
{SSHA}0hvSOPTZgMIe94Jm2e0VLslWpywpkzsF

```

FIGURE 32 – Génération de mots de passe avec slappasswd

Ajout des Données dans l'Annuaire

Pour intégrer les données définies dans utilisateurs_et_groupes.ldif dans l'annuaire :

```
ldapadd -x -D "cn=admin,dc=groupe7,dc=ehtp" -w admin_password
-f utilisateurs_et_groupes.ldif
```

La commande suivante permet de vérifier les données ajoutées :

```
sudo slapcat
```

Installation et Configuration de l'Interface Web PHPLDAPADMIN

PHPLDAPADMIN est un outil graphique qui simplifie la gestion du serveur LDAP. Pour l'installer :

```
sudo apt-get install phpldapadmin
```



```

amine@amine-nst:/etc/ldap/fichier$ ldapadd -x -D "cn=admin,dc=groupe7,dc=ehp" -w 1610 -f utilisateurs_et_groupes.ldif
adding new entry "ou=utilisateurs,dc=groupe7,dc=ehp"
adding new entry "ou=groupes,dc=groupe7,dc=ehp"
adding new entry "cn=Amine Slimani,ou=utilisateurs,dc=groupe7,dc=ehp"
adding new entry "cn=Yassine Nourddine,ou=utilisateurs,dc=groupe7,dc=ehp"
adding new entry "cn=Zaid Assadiki,ou=utilisateurs,dc=groupe7,dc=ehp"
adding new entry "cn=Developeurs,ou=groupes,dc=groupe7,dc=ehp"
adding new entry "cn=Utilisateurs,ou=groupes,dc=groupe7,dc=ehp"

```

FIGURE 33 – Ajout des données dans l'annuaire LDAP

```

dn: ou=groupes,dc=groupe7,dc=ehp
objectClass: organizationalUnit
ou: groupes
structuralObjectClass: organizationalUnit
entryUUID: 6bb0d7a4-5b68-103f-9176-73e7a3995e05
creatorsName: cn=admin,dc=groupe7,dc=ehp
createTimestamp: 20241231021224Z
entryCSN: 20241231021224.924933Z#000000#000#000000
modifiersName: cn=admin,dc=groupe7,dc=ehp
modifyTimestamp: 20241231021224Z

dn: cn=Amine Slimani,ou=utilisateurs,dc=groupe7,dc=ehp
objectClass: inetOrgPerson
cn: Amine Slimani
sn: Slimani
mail: amine.slimani@groupe7.ehp
userPassword:: e1NTSEF9ULJJbTZPbnBicVpDTLRwRGMYSdN4ME1peitiMlhBd00=
structuralObjectClass: inetOrgPerson
entryUUID: 6bb2a066-5b68-103f-9177-73e7a3995e05
creatorsName: cn=admin,dc=groupe7,dc=ehp
createTimestamp: 20241231021224Z
entryCSN: 20241231021224.936624Z#000000#000#000000
modifiersName: cn=admin,dc=groupe7,dc=ehp
modifyTimestamp: 20241231021224Z

dn: cn=Yassine Nourddine,ou=utilisateurs,dc=groupe7,dc=ehp
objectClass: inetOrgPerson
cn: Yassine Nourddine
sn: Nourddine
mail: yassine.nourddine@groupe7.ehp
userPassword:: e1NTSEF9VTJxbUx0S1FyUHpiK2c4dC93bGxjTLRZK01DdVhuVW4=
structuralObjectClass: inetOrgPerson
entryUUID: 6bb3d51c-5b68-103f-9178-73e7a3995e05
creatorsName: cn=admin,dc=groupe7,dc=ehp
createTimestamp: 20241231021224Z

```

FIGURE 34 – Vérification des utilisateurs dans l'annuaire LDAP

Configuration :

```
sudo gedit /etc/phpldapadmin/config.php
```

Les paramètres suivants sont ajoutés au fichier :

```

317 $servers->setValue('server','name','Projet groupe7 LDAP Server');
318
319 $servers->setValue('server','host','192.168.245.49');
320
321 $servers->setValue('server','base',array('dc=groupe7,dc=ehtp'));
322
323 $servers->setValue('login','bind_id','cn=admin,dc=groupe7,dc=ehtp');

```

FIGURE 35 – Configuration du fichier config.php

Pour accéder à l'interface, ouvrez un navigateur et saisissez :

192.168.245.49/phpldapadmin/

FIGURE 36 – Connexion à PHPLDAPADMIN via le navigateur

Le tableau de bord de l'interface Web ressemble à ceci :

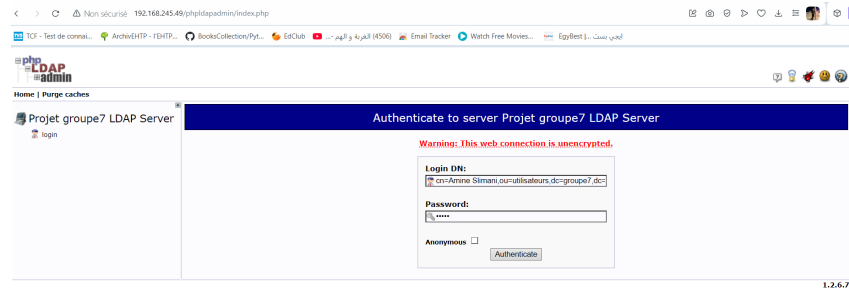


FIGURE 37 – Tableau de bord de PHPLDAPADMIN

Après connexion, les utilisateurs et groupes peuvent être visualisés et gérés via cette interface conviviale.

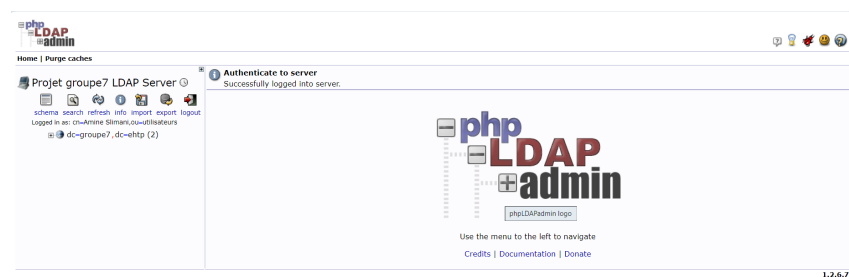


FIGURE 38 – Visualisation des utilisateurs et groupes dans PHPLDAPADMIN

VII Conclusion

En conclusion, ce projet nous a permis de mettre en œuvre et de configurer des protocoles réseau essentiels tels que DNS, HTTPS, FTP, SMTP, IMAP, et LDAP, afin de garantir une infrastructure réseau fiable, performante et sécurisée. Ces configurations, bien que techniquement exigeantes, ont renforcé la connectivité et la protection des données tout en facilitant la gestion centralisée des utilisateurs et des ressources grâce à OpenLDAP.

Les défis rencontrés, notamment en matière de compatibilité, de sécurité, et de performances, ont été surmontés grâce à une méthodologie rigoureuse et une veille technologique continue. Ce travail nous a permis d'acquérir une meilleure compréhension des exigences et des bonnes pratiques liées à la gestion des réseaux modernes.

Ainsi, le projet pose les bases d'une infrastructure résiliente et évolutive, prête à répondre aux besoins actuels et futurs, tout en offrant un environnement sécurisé et performant pour les utilisateurs et les systèmes connectés.