REPUBLIQUE DU SENEGAL

Un peuple-un but-une foi

Ministère de l'Enseignement Supérieur, de la Recherche et de l'Innovation

Direction de l'Enseignement Supérieur Privé

ISI **INSTITUT SUPÉRIEUR D'INFORMATIQUE L'institut de référence dans les TIC**

Km1, Avenue Cheikh Anta Diop BP : 28 110 Dakar Sénégal / Tel : 33 822 19 81 / Fax : 33 822 31 90
Site Web : www.isi.sn

PROJET D' INSTALLATION ET CONFIGURATION SERVEUR DE MESSAGERIE ROUNDCUBE WEBMAIL ET DE PHPLDAPADMIN

Présenté et soutenu par :
MAME MBAYE DIA
Mamembayedia36@gmail.com

Sous la direction de
Mr LO

2024-2025

PLAN

INTRODUCTION

1-Definition

2-Information

3-Deploiement

Conclusion

INTRODUCTION

De nos jours, les entreprises migrent vers l'automatisation de système d'informations. Ils ne cessent d'évoluer et leur utilisation devient de plus en plus importante. Cependant, les entreprises sont souvent équipées d'un réseau local au minimum, et de réseaux de longues distances pour les plus importantes d'entre elles. Leurs parcs informatiques englobent une vingtaine voire une centaine d'équipements, engendrés par des serveurs de bases de données et des serveurs de traitement... D'où le rôle de l'administrateur qui doit veiller au bon fonctionnement de ces systèmes d'information et de garantir la sécurité. En effet, les administrateurs font appel à des logiciels de surveillance et de supervision de réseaux afin de vérifier l'état du réseau en temps réel et l'ensemble du parc informatique qui est sous leur responsabilité. Et être aussi informés automatiquement (par email) en cas de problèmes. Dans ce cas nous allons Définir ROUNDCUBE et PHPLDAPADMIN qui est un outil de supervision pour la, en outre nous passerons aux informations nécessaires pour mettre en place cette solution retenu, en suite on verra les déploiements de notre solution en fin de passer à la conclusion.

1- DEFINITION

Roundcube est une interface web open source pour la gestion des e-mails. C'est un client de messagerie web qui permet aux utilisateurs d'accéder à leurs e-mails via un navigateur web. Il offre une interface conviviale, des fonctionnalités avancées telles que le glisser-déposer, le regroupement de messages, la gestion des contacts, et prend en charge divers protocoles de messagerie tels que IMAP et SMTP.

Définition : OpenLDAP est une implémentation open source du protocole LDAP (Lightweight Directory Access Protocol). LDAP est un protocole standard pour l'accès et la maintenance des services d'annuaire distribués sur un réseau IP. OpenLDAP est souvent utilisé pour créer et gérer des annuaires LDAP, qui stockent des informations sur les utilisateurs, les groupes, les ordinateurs et d'autres objets dans un format hiérarchique.

Définition : phpLDAPadmin est une application web open source écrite en PHP qui permet d'administrer et de gérer des annuaires LDAP via une interface graphique. C'est un outil d'administration convivial qui simplifie les tâches liées à la gestion des informations stockées dans un annuaire LDAP. Il offre des fonctionnalités telles que la création, la modification et la suppression d'entrées LDAP, ainsi que la gestion des schémas et des droits d'accès.

En résumé, Roundcube est un client de messagerie web, OpenLDAP est une implémentation open source du protocole LDAP utilisée pour la gestion d'annuaires, et phpLDAPadmin est une interface web permettant l'administration graphique d'annuaires LDAP.

2-INFORMATION

Avant de commencer l’installation de la solution retenue, nous allons tout d’abord avoir besoin de configurer, DNS, DHCP, Apache2 ou Nginx et en fin OpenLDAP, Roundcube(Postfix et Dovcot) et PHPLDAPadmin Qu’on va vous détailler ci-dessous : Dns : Le Domain Name System ou DNS est un service informatique distribué utilisé qui traduit les noms de domaine Internet en adresse IP ou autres enregistrements Apache2: Le logiciel libre Apache HTTP Server est un serveur HTTP créé et maintenu au sein de la fondation Apache. Jusqu'en avril 2019, ce fut le serveur HTTP le plus populaire du World Wide Web. Il est distribué selon les termes de la licence Apache Nginx : NGINX Open Source ou NGINX est un logiciel libre de serveur Web ainsi qu'un proxy inverse écrit par Igor Sysoev, dont le développement a débuté en 2002 pour les besoins d'un site russe à très fort trafic. La documentation est disponible dans plusieurs langues

3-Deploiement

• Configuration de roundcube et PHPLDAPadmin

Nous allons installer roundcube et PHPLDAPadmin sur CentOS Stream 9. De ce fait, nous allons utiliser un serveur web apache. Nous commencerons par installer les différents paquets nécessaires puis ensuite nous ferons les configurations et nous finirons par un test de fonctionnement.

✓ Configuration du DNS

Il va falloir installer tout d'abord les paquets named avant de commencer la configuration de Dns comme montre ci-dessous :

```
[root@server ~]# yum install named -y
```

Ensuite nous allons procéder à la configuration en commençant a Editer le fichier hosts : vim /etc/hosts

```
127.0.0.1   localhost localhost.localdomain
192.168.0.1
```

Vim /etc/hostname

```
server
```

Vim /etc/resolv.conf

```
# Generated by NetworkManager
search mamembaye.sn
nameserver 192.168.0.1
~
```

vim /etc/named.conf

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

options {
        listen-on port 53 { 127.0.0.1; 192.168.0.1; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        secroots-file   "/var/named/data/named.secroots";
        recursing-file  "/var/named/data/named.recursing";
        allow-query     { localhost; 192.168.0.0/24; };

        /*
         - If you are building an AUTHORITATIVE DNS server, do NOT enable recurs
ion.
```

Et puis dans la même fichier on créer les zones (direct et inverse) : /etc/named. Conf

```
zone "." IN {
        type hint;
        file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";

zone "mamembaye.sn" IN {
        type master;
        file "direct";
};
zone "0.168.192.in-addr.arpa" IN {
        type master;
        file "inverse";
};
```

Maintenant nous allons venir au niveau des fichiers /var/named/ pour configurer nos zones :

```
$TTL 1D
@       IN SOA  server.mamembaye.sn. root.server.mamembaye.sn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
                IN NS           server.mamembaye.sn.
server          IN A            192.168.0.1
www             IN CNAME        server.mamembaye.sn.
~
~
~
~
```

Ensuite nous allons copier les contenus du zones direct dans zone inverse un fichier qui sera créer lors de la copie : Toujours dans le répertoire /var/named/ Cp direct inverse Vim inverse

```
$TTL 1D
@       IN SOA  server.mamembaye.sn. root.server.mamembaye.sn. (
                                        0       ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
                IN NS           server.mamembaye.sn.
server          IN A            192.168.0.1
1               IN PTR          server.mamembaye.sn.
~
~
~
~
```

On fait la commande pour enregistrer et quitter : echap + : wq. Une fois enregistrer, nous allons fixer l'adresse en fin de redémarrer les services.

```
[root@server named]# nmcli networking off
[root@server named]# nmcli networking on
```

Redémarrage de service et tester le Dns

```
[root@server ~]# systemctl restart named
```

On teste avec la commande suivant nslookup www :

```
[root@server ~]# nslookup www
Server:         192.168.0.1
Address:        192.168.0.1#53

www.mamembaye.sn        canonical name = server.mamembaye.sn.
Name:   server.mamembaye.sn
Address: 192.168.0.1
```

- ✓ Configuration de DHCP

Il va falloir installer tout d'abord les paquets dhcp-server avant de commencer la configuration de dhcp comme montre ci-dessous :

```
[root@server ~]# yum install dhcp-server -y
```

Ensuite nous allons procéder à la configuration en commençant a Editer le fichier Vim /etc/dhcp/dhcpd

Ligne 18 on doit décommenter

```
18 authoritative;
```

C'est la ligne 47 a 55 qui nous intéresse

```
47 subnet 192.168.0.0 netmask 255.255.255.0 {
48   range 192.168.0.10 192.168.0.100;
49   option domain-name-servers 192.168.0.1;
50   option domain-name "mamembaye.sn";
51   option routers 192.168.0.1;
52   option broadcast-address 192.168.0.255;
53   default-lease-time 600;
54   max-lease-time 7200;
55 }
```

On fait la commande pour enregistrer et quitter : echap + : wq.

Une fois enregistrer, nous allons redémarrer le service et activer le demarrage

```
[root@server ~]# systemctl restart dhcpd
[root@server ~]# systemctl enable dhcpd
```

- ✓ Configuration de httpd

Un serveur HTTP utilise alors par défaut le port 80. Les clients HTTP les plus connus sont les navigateurs web permettant à un utilisateur d'accéder à un serveur contenant des données. Pour configurer donc le serveur HTTP, on suit les étapes suivantes.

Commençons à installer les paquets

```
[root@server ~]# yum install httpd -y
```

Ensuite nous allons Editer le fichier vim /etc/httpd/conf/httpd.conf

```
90 #
91 ServerAdmin root@localhost
92
93 #
94 # ServerName gives the name and port that the server uses to identify itself
   .
95 # This can often be determined automatically, but we recommend you specify
96 # it explicitly to prevent problems during startup.
97 #
98 # If your host doesn't have a registered DNS name, enter its IP address here
   .
99 #
00 ServerName www.mamembaye.sn:80
```

Nous allons venir dans le répertoire /var/www/html/ pour créer notre propre site.

```
[root@server ~]# vim /var/www/html/index.html
```

Création de notre propre page web

```
<marquee><h1>Bienvenue sur mon site</h1></marquee>
~
```

Bienvenue sur mon site

✓ Installation les dépendances requises de OPENLDAP

D'abord avant d'installer openldap nous avons mettre à jour le SELINUX et installer les dépendances

```
[root@server ~]# vim /etc/selinux/config
```

Mettre le SELINUX=DISABLED ; sauvegarder quitter et reboot la machine

```
22 SELINUX=disabled
```

Installation des dépendances

```
[root@server ~]# yum install -y cyrus-sasl-devel make libtool autoconf libtool-ltdl-devel
 openssl-devel libdb-devel tar gcc perl perl-devel wget vim
```

Apres l'installation des dépendances on Créer un compte system pour OpenLDAP

```
[root@server ~]# useradd -r -M -d /var/lib/openldap -u 55 -s /usr/sbin/nologin ldap
```

Télécharger le fichier source de OpenLDAP et ensuite le décompresser

```
[root@server ~]# wget ftp://ftp.openldap.org/pub/OpenLDAP/
openldap-release/openldap-2.4.50.tgz
```

On décompresse

```
[root@server ~]# tar -xvzf openldap-2.4.50.tgz -C /etc/openldap/
```

Procéder à l'installation de OpenLDAP

```
[root@server ~]# cd /etc/openldap/
ls
cd openldap-2.4.50/
certs                 schema                slapd.ldif
check_password.conf   schema.83874          slapd.ldif.bak
ldap.conf             slapd.conf            slapd.ldif.default
ldap.conf.default     slapd.conf.default
openldap-2.4.50       slapd.d
[root@server openldap-2.4.50]#
```

On copie la commande et on colle

```
[root@server openldap-2.4.50]# ./configure --prefix=/usr --sy
sconfdir=/[root@server openldap-2.4.50]# ./configure --prefix
=/[root@server openldap-2.4.50]# ./configure --prefix=/usr --
[root@server openldap-2.4.50]# ./configure --prefix=/usr --sy
sconfdir=/etc --disable-static --enable-debug --with-tls=open
ssl --with-cyrus-sasl --enable-dynamic --enable-crypt --enabl
e-spasswd --enable-slapd --enable-modules --enable-rlookups -
-enable-backends=mod --disable-ndb --disable-sql --disable-sh
ell --disable-bdb --disable-hdb --enable-overlays=mod
```

Apres l'installation on tape make depend pour faire la dépendance

```
[root@server openldap-2.4.50]# make depend
```

Apres avoir fait sa on tape la commande make

```
[root@server openldap-2.4.50]# make
```

ET enfin on passe à l'installation et on tape la commande make installation

```
[root@server openldap-2.4.50]# make install
```

Apres l'installation on passe à la configuration de openLDAP
Créer les répertoires de openLDAP, le Service de openLDAP, base de données...

```
[root@server openldap-2.4.50]# mkdir /var/lib/openldap /etc/
openldap/slapd.d
chown -R ldap:ldap /var/lib/openldap/
chown root:ldap /etc/openldap/slapd.conf
chmod 640 /etc/openldap/slapd.conf
```

Ensuite nous allons procéder à la Création du service pour OpenLDAP en commençant à éditer ce fichier

```
[root@server openldap-2.4.50]# vim /etc/systemd/system/slapd
.service
```

Ajouter ce contenu :

```
[Unit]
Description=OpenLDAP Server Daemon
After=syslog.target network-online.target
Documentation=man:slapd
Documentation=man:slapd-mdb

[Service]
Type=forking
PIDFile=/var/lib/openldap/slapd.pid
Environment="SLAPD_URLS=ldap:/// ldapi:/// ldaps:///"
Environment="SLAPD_OPTIONS=-F /etc/openldap/slapd.d"
ExecStart=/usr/libexec/slapd -u ldap -g ldap -h ${SLAPD_URLS
} $SLAPD_OPTIONS

[Install]
WantedBy=multi-user.target
```

On fait la commande pour enregistrer et quitter : echap + : wq

Création du schema Sudo d'openLDAP

```
[root@server openldap-2.4.50]# sudo -V | grep -i "ldap"
```

On Copier le ficher de schema

```
[root@server openldap-2.4.50]#
cp /usr/share/doc/sudo/schema.OpenLDAP /etc/openldap/schema/
sudo.schema
```

Créer le fichier schema : sudo.ldif

```
[root@server openldap-2.4.50]# cat << 'EOL' > /etc/openldap/
schema/sudo.ldif
```

On insérer ce contenu

```
> dn: cn=sudo,cn=schema,cn=configt << 'EOL' > /etc/openldap/schema/sudo.ldif
objectClass: olcSchemaConfigonfig
> dn: cn=sudo,cn=schema,cn=config
objectClass: olcSchemaConfig.4.1.15953.9.1.1 NAME 'sudoUser' DESC 'User(s) who may  run sudo' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch SY
cn: sudo.6.1.4.1.1466.115.121.1.cn: sudobuteTypes: ( 1.3.6.1.4.1.15953.9.1.1 NAME 'sudoUser' DESC 'User(s) who may  run sudo' EQUALITY caseExactIA5Match SUBST
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.1 NAME 'sudoUser' DESC 'User(s) who may  run sudo' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch SY
NTAX 1.3.6.1.4.1.1466.115.121.1.26 )seExactIA5SubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )ttributeTypes: ( 1.3.6.1.4.1.15953.9.1.2 NAME 'sudoHost' D
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.2 NAME 'sudoHost' DESC 'Host(s) who may run sudo' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch SYN
TAX 1.3.6.1.4.1.1466.115.121.1.26 ) 'Host(s) who may run sudo' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.3 NAME 'sudoCommand' DESC 'Command(s) to be executed by sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.11
5.121.1.26 )1.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.4 NAME 'sudoRunAs' DESC 'User(s) impersonated by sudo (deprecated)' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1
466.115.121.1.26 )
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.5 NAME 'sudoOption' DESC 'Options(s) followed by sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.121.1
.26 ) Class: olcSchemaConfig
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.6 NAME 'sudoRunAsUser' DESC 'User(s) impersonated by sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115.1
21.1.26 )sudo' EQUALITY caseExactIA5Match SUBSTR caseExactIA5SubstringsMatch SYNTAX 1.3.6.1.4.1.1466.115.121.1.26 )53.9.1.2 NAME 'sudoHost' DESC 'Host(s) who
olcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.7 NAME 'sudoRunAsGroup' DESC 'Group(s) impersonated by sudo' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1466.115
.121.1.26 ).4.1.1466.115.121.1.26 )953.9.1.3 NAME 'sudoCommand' DESC 'Command(solcAttributeTypes: ( 1.3.6.1.4.1.15953.9.1.3 NAME 'sudoCommand' DESC 'Command(s
olcObjectClasses: ( 1.3.6.1.4.1.15953.9.2.1 NAME 'sudoRole' SUP top STRUCTURAL DESC 'Sudoer Entries' MUST ( cn ) MAY ( sudoUser $ sudoHost $ sudoCommand $ sud
oRunAs $ sudoRunAsUser $ sudoRunAsGroup $ sudoOption $ description ) )er(s) impersonated by sudo (deprecated)' EQUALITY caseExactIA5Match SYNTAX 1.3.6.1.4.1.1
EOL
```

Nous Editons le fichier slapd. Ldif

```
[root@server ~]# mv /etc/openldap/slapd.ldif /etc/openldap/slapd.ldif.bak
```

```
[root@server openldap-2.4.50]# vim /etc/openldap/slapd.ldif
```

On insérer ce contenu

```
dn: cn=config
objectClass: olcGlobal
cn: config
olcArgsFile: /var/lib/openldap/slapd.args
olcPidFile: /var/lib/openldap/slapd.pid

dn: cn=schema,cn=config
objectClass: olcSchemaConfig
cn: schema

dn: cn=module,cn=config
objectClass: olcModuleList
cn: module
olcModulepath: /usr/libexec/openldap
olcModuleload: back_mdb.la

include: file:///etc/openldap/schema/core.ldif
include: file:///etc/openldap/schema/cosine.ldif
include: file:///etc/openldap/schema/nis.ldif
include: file:///etc/openldap/schema/inetorgperson.ldif
include: file:///etc/openldap/schema/ppolicy.ldif
include: file:///etc/openldap/schema/sudo.ldif

dn: olcDatabase=frontend,cn=config
objectClass: olcDatabaseConfig
objectClass: olcFrontendConfig
olcDatabase: frontend
olcAccess: to dn.base="cn=Subschema" by * read
olcAccess: to *
  by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
  by * none

dn: olcDatabase=config,cn=config
objectClass: olcDatabaseConfig
olcDatabase: config
olcRootDN: cn=config
olcAccess: to *
  by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
  by * none
~
```

Ensuite on doit Mettre à jour la base de données

```
[root@server openldap-2.4.50]# slapadd -n 0 -F /etc/openldap/slapd.d -l /etc/openldap/slapd.ldif -u
slapadd -n 0 -F /etc/openldap/slapd.d -l /etc/openldap/slapd.ldif
ls /etc/openldap/slapd.d/
slapadd: could not add entry dn="cn=config" (line=1):
Closing DB...
slapadd: could not add entry dn="cn=config" (line=1):
Closing DB...
'cn=config'  'cn=config.ldif'
```

Mettre les droits pour l'utilisateur ldap

```
[root@server openldap-2.4.50]# chown -R ldap:ldap /etc/openldap/slapd.d/
```

Démarrer le service SLAPD

```
[root@server openldap-2.4.50]# systemctl daemon-reload
systemctl enable --now slapd.service
systemctl status slapd.service
```

Configurer la connexion OpenLDAP

```
[root@server openldap-2.4.50]# vim enable-ldap-log.ldif
```

Insérer ce contenu:

```
dn: cn=config
changetype: modify
replace: olcLogLevel
olcLogLevel: stats
~
~
```

Tapez cette commande ensuite :

```
[root@server openldap-2.4.50]# ldapmodify -Y EXTERNAL -H ldapi:/// -f enable-ldap-log.ldif
```

Effectuer une recherche de vérification

```
[root@server openldap-2.4.50]# ldapsearch -Y EXTERNAL -H ldapi:/// -b cn=config "(objectClass=olcGlobal)" olcLogLevel -LLL -Q
```

Ajuster les variables d'environnements

```
[root@server openldap-2.4.50]# echo "local4.* /var/log/slapd.log" >> /etc/rsyslog.conf
```

On redémarrer le système

```
[root@server openldap-2.4.50]# systemctl restart rsyslog.service
```

Créer un DN ROOT

```
[root@server openldap-2.4.50]# vim rootdn.ldif
```

Insérer ce contenu:

```
dn: olcDatabase=mdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcMdbConfig
olcDatabase: mdb
olcDbMaxSize: 42949672960
olcDbDirectory: /var/lib/openldap
olcSuffix: dc=mamembaye,dc=sn
olcRootDN: cn=admin,dc=mamembaye,dc=sn
olcRootPW: {SSHA}W5f+snCuGBmbxVrip8erbTP/M3ukbh5K
olcDbIndex: uid pres,eq
olcDbIndex: cn,sn pres,eq,approx,sub
olcDbIndex: mail pres,eq,sub
olcDbIndex: objectClass pres,eq
olcDbIndex: loginShell pres,eq
olcDbIndex: sudoUser,sudoHost pres,eq
olcAccess: to attrs=userPassword,shadowLastChange,shadowExpire
  by self write
  by anonymous auth
  by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
  by dn.subtree="ou=system,dc=mamembaye,dc=sn" read
  by * none
olcAccess: to dn.subtree="ou=system,dc=mamembaye,dc=sn" by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
  by * none
olcAccess: to dn.subtree="dc=mamembaye,dc=sn" by dn.subtree="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
  by users read
  by * none
```

Mettre a jour la base de donnée

```
[root@server openldap-2.4.50]# ldapadd -Y EXTERNAL -H ldapi:/// -f rootdn.ldif
```

Configuration SSL/TLS

```
[root@server openldap-2.4.50]# openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/pki/tls/ldapserver.key -out /etc/pki/tls/ldapserver.crt
```

Je dois mettre les droits

```
[root@server openldap-2.4.50]# chown ldap:ldap /etc/pki/tls/{ldapserver.crt,ldapserver.key}
```

Créer le fichier pour TLS Nous va éditer le fichier

```
[root@server openldap-2.4.50]# vim add-tls.ldif
```

Insérer ce contenu

```
dn: cn=config
changetype: modify
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/pki/tls/ldapserver.crt
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/pki/tls/ldapserver.key
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/pki/tls/ldapserver.crt
~
~
~
```

Mettre à jour la BD

```
[root@server openldap-2.4.50]# ldapadd -Y EXTERNAL -H ldapi:/// -f add-tls.ldif
```

Vérifier le certificat

```
[root@server openldap-2.4.50]# slapcat -b "cn=config" | grep olcTLS
```

Changer la localisation de notre certificat nous éditons ce fichier

```
[root@server openldap-2.4.50]# vim /etc/openldap/ldap.conf
```

Ajouter dans le fichier: Dans la ligne 19

```
 1 #
 2 # LDAP Defaults
 3 #
 4
 5 # See ldap.conf(5) for details
 6 # This file should be world readable but not world writable.
 7
 8 #BASE   dc=example,dc=com
 9 #URI    ldap://ldap.example.com ldap://ldap-master.example.com:666
10
11 #SIZELIMIT      12
12 #TIMELIMIT      15
13 #DEREF          never
14
15 # When no CA certificates are specified the Shared System Certificates
16 # are in use. In order to have these available along with the ones specified
17 # by TLS_CACERTDIR one has to include them explicitly:
18 #TLS_CACERT     /etc/pki/tls/cert.pem
19 TLS_CACERT      /etc/pki/tls/ldapserver.crt
20 # System-wide Crypto Policies provide up to date cipher suite which should
21 # be used unless one needs a finer grinded selection of ciphers. Hence, the
22 # PROFILE=SYSTEM value represents the default behavior which is in place
23 # when no explicit setting is used. (see openssl-ciphers(1) for more info)
24 #TLS_CIPHER_SUITE PROFILE=SYSTEM
25
26 # Turning this off breaks GSSAPI used with krb5 when rdns = false
27 SASL_NOCANON    on
28
```

CREATION D'UN SCHEMA

CREER LE FICHIER DE BASE POUR NOTRE SCHEMA

```
[root@server openldap-2.4.50]# vim base.ldif
```

Insérer le contenu :

```
dn: dc=mamembaye,dc=sn
objectClass: dcObject
objectClass: organization
objectClass: top
dc: mamembaye
o: it

dn: ou=groupe,dc=mamembaye,dc=sn
objectClass: organizationalUnit
objectClass: top
ou: groupe

dn: ou=utilisateurs,dc=mamembaye,dc=sn
objectClass: organizationalUnit
objectClass: top
ou: utilisateurs

dn: ou=rh,dc=mamembaye,dc=sn
objectClass: organizationalUnit
objectClass: top
ou: rh
~
```

Nous allons faire la mise à jour de la base

```
[root@server openldap-2.4.50]# ldapadd -Y EXTERNAL -H ldapi:/// -f base.ldif
```

CREER UN FICHIER POUR METTRE DES USERS DANS LA BD

```
[root@server openldap-2.4.50]# vim user1.ldif
```

Insérer le contenu

```
dn: uid=cheikh,ou=utilisateurs,dc=mamembaye,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: cheikh
cn: cheikh
sn: cheikh
loginShell: /bin/cheikh
uidNumber: 10000
gidNumber: 10000
homeDirectory: /home/cheikh
shadowMax: 60
shadowMin: 1
shadowWarning: 7
shadowInactive: 7
shadowLastChange: 0

dn: cn=cheikh,ou=groupe,dc=mamembaye,dc=sn
objectClass: posixGroup
cn: cheikh
gidNumber: 10000
memberUid: cheikh
~
```

On ajout a la base users1

```
[root@server openldap-2.4.50]# ldapadd -Y EXTERNAL -H ldapi:/// -f user1.ldif
```

Pour users2

```
[root@server openldap-2.4.50]# vim user2.ldif
```

Insérer ce contenu :

```
dn: uid=marc,ou=rh,dc=mamembaye,dc=sn
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: marc
cn: marc
sn: marc
loginShell: /bin/marc
uidNumber: 10001
gidNumber: 10001
homeDirectory: /home/marc
shadowMax: 60
shadowMin: 1
shadowWarning: 7
shadowInactive: 7
shadowLastChange: 0

dn: cn=marc,ou=groupe,dc=mamembaye,dc=sn
objectClass: posixGroup
cn: marc
gidNumber: 10001
memberUid: marc
```

On ajoute a la base users2

```
[root@server openldap-2.4.50]# vim bindDNuser.ldif
```

Insérer ce contenu :

```
dn: ou=system,dc=mamembaye,dc=sn
objectClass: organizationalUnit
objectClass: top
ou: system

dn: cn=readonly,ou=system,dc=mamembaye,dc=sn
objectClass: organizationalRole
objectClass: simpleSecurityObject
cn: readonly
userPassword: {SSHA}QpBJjY7MZa4S933aCf/T4+pwDHqrU00C
description: Bind DN user for LDAP Operations
~
~
```

Générer le mot de passe pour readonly

```
[root@server openldap-2.4.50]# slappasswd
```

On copie le mot de passe et on colle dans le fichier vim bindDNuser.ldif

```
userPassword: {SSHA}QpBJjY7MZa4S933aCf/T4+pwDHqrU00C
```

Mettre à jour la base de données

```
[root@server openldap-2.4.50]#
ldapadd -Y EXTERNAL -H ldapi:/// -f bindDNuser.ldif
```

Ajuster le pare-feu

```
[root@server openldap-2.4.50]# firewall-cmd --add-service={ldap,ldaps} --permanent
firewall-cmd --reload
```

- ✓ Configuration de PhpLDAPadmin

D'abord avant d'installer phpldapadmin nous avons faire l'installation de PHP et les modules

```
[root@server ~]# dnf install php php-cgi php-mbstring php-common php-pear php-{gd,json,zip} php-ldap git
```

Installation de phpldapadmin a partir de son repository github. Il va l'installer dans ce répertoire /usr/share/phpldapadmin

```
[root@server ~]# git clone https://github.com/breisig/phpLDAPadmin.git /usr/share/phpldapadmin
```

Renommer le fichier de configuration

```
[root@server ~]# cp /usr/share/phpldapadmin/config/config.php{.example,}
```

Edition du fichier de config de phpldapadmin

```
[root@server ~]# vim /usr/share/phpldapadmin/config/config.php
```

Ensuite nous avons décommenter des ligne et ajouter notre adresse IP

```
310 /*****************************************
311  * Define your LDAP servers in this section  *
312  *****************************************/
313
314 $servers = new Datastore();
315
316 /* $servers->NewServer('ldap_pla') must be called before each new LDAP server
317    declaration. */
318 $servers->newServer('ldap_pla');
319
320 /* A convenient name that will appear in the tree viewer and throughout
321    phpLDAPadmin to identify this LDAP server to users. */
322 $servers->setValue('server','name','Local LDAP Server');
323
324 /* Examples:
325    'ldap.example.com',
326    'ldaps://ldap.example.com/',
327    'ldapi://%2fusr%local%2fvar%2frun%2fldapi'
328           (Unix socket at /usr/local/var/run/ldap) */
329  $servers->setValue('server','host','127.0.0.1','192.168.0.1');
330
331 /* The port your LDAP server listens on (no quotes). 389 is standard. */
332  $servers->setValue('server','port',389);
333
334 /* Array of base DNs of your LDAP server. Leave this blank to have phpLDAPadmin
335    auto-detect it for you. */
336  $servers->setValue('server','base',array(''));
```

Dans ce contenu nous allons décommenter la ligne 314,318,322,329(dans la ligne on ajout notre adresse IP) 332 et 336

```
363  $servers->setValue('login','bind_id','');
364  $servers->setValue('login','bind_id','cn=admin,dc=mamembaye,dc=sn');
365
366 /* Your LDAP password. If you specified an empty bind_id above, this MUST also
367    be blank. */
368  $servers->setValue('login','bind_pass','');
369  $servers->setValue('login','bind_pass','secret');
```

Ensuite nous allons décommenter la ligne 363, 364(dans la ligne nous ajoutons notre DNS comme suit) 368 et 369

Ajuster les droits

```
[root@server ~]# chown -R apache:apache /usr/share/phpldapadmin
```

Créer un fichier apache de conf pour phpldapadmin

```
[root@server ~]# vim /etc/httpd/conf.d/phpldapadmin.conf
```

Ajouter ce contenu :

```
<VirtualHost *:80>
        ServerName mamembaye.sn
        DocumentRoot /usr/share/phpldapadmin/htdocs

        <Directory /usr/share/phpldapadmin/htdocs>
          <IfModule mod_authz_core.c>
            # Apache 2.4
            Require all granted
          </IfModule>
        </Directory>
</VirtualHost>
```

Test httpd :

```
[root@server ~]# httpd -t
Syntax OK
```

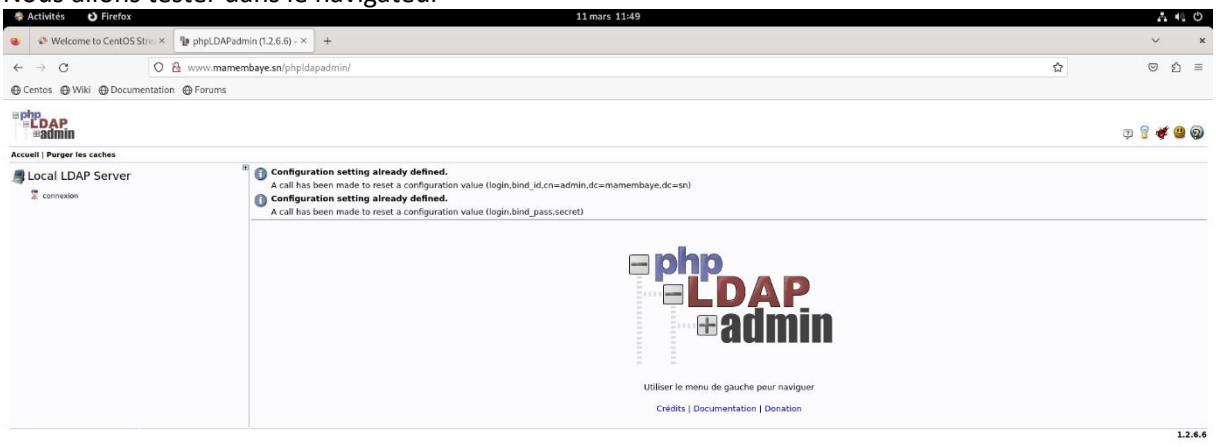
Pare-feu

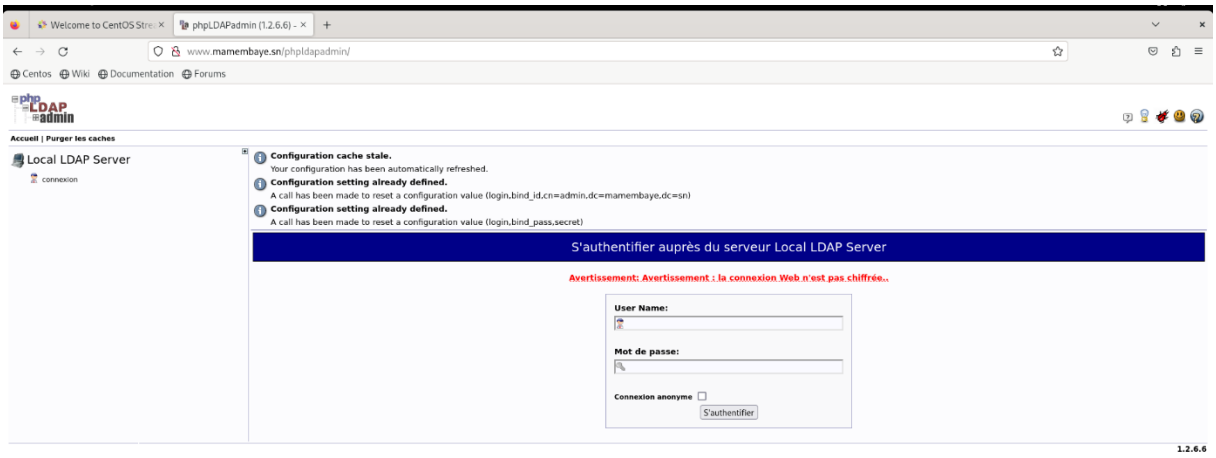
```
[root@server ~]# firewall-cmd --add-port=80/tcp --permanent
firewall-cmd --reload
```

AUTORISATIONS

```
[root@server ~]# setsebool -P httpd_can_network_connect 1
setsebool -P httpd_can_connect_ldap 1
setsebool -P authlogin_nsswitch_use_ldap 1
setsebool -P nis_enabled 1
systemctl enable --now httpd
```

Nous allons tester dans le navigateur





✓ Configuration Roundcube

D'abord avant de faire l'installation de roundcube nous avons d'installer Postfix et Dovecot

• Configuration de postfix

Il va falloir installer tout d'abord les paquets postfix avant de commencer la configuration de postfix comme montre ci-dessous :

```
[root@server ~]# yum install postfix -y
```

Apres l'installation du paquet nous éditons ce fichier

```
[root@server ~]# vim /etc/postfix/main.cf
```

Ensuite nous décommenter des ligne(95,102 et 118) et faire des insertion

```
 93 #
 94 #myhostname = host.domain.tld
 95 myhostname = server.mamembaye.sn
 96
 97 # The mydomain parameter specifies the local internet domain name.
 98 # The default is to use $myhostname minus the first component.
 99 # $mydomain is used as a default value for many other configuration
100 # parameters.
101 #
102 mydomain = mamembaye.sn
103
104 # SENDING MAIL
105 #
106 # The myorigin parameter specifies the domain that locally-posted
107 # mail appears to come from. The default is to append $myhostname,
108 # which is fine for small sites.  If you run a domain with multiple
109 # machines, you should (1) change this to $mydomain and (2) set up
110 # a domain-wide alias database that aliases each user to
111 # user@that.users.mailhost.
112 #
113 # For the sake of consistency between sender and recipient addresses,
114 # myorigin also specifies the default domain name that is appended
115 # to recipient addresses that have no @domain part.
116 #
117 #myorigin = $myhostname
118 myorigin = $mydomain
119
```

Pour la suite la ligne 135 on remplace localhost par all et la ligne 138 all on remplace par ipv4

```
135 inet_interfaces = all
136
137 # Enable IPv4, and IPv6 if supported
138 inet_protocols = ipv4
```

Dans la ligne 183 on décommente et ajout à la fin $mydomain

```
283 mynetworks = 192.168.0.1/24, 127.0.0.0/8
```

Au niveau de la ligne 283 on va décommenter cette ligne mynetwork et effacer la première adresse

```
438 home_mailbox = Maildir/
```

Dans cette ligne on va décommenter le répertoire Mailbox

```
593 smtpd_banner = $myhostname ESMTP
```

Dans cette on ajout sa SMTP…

A la fin de ce fichier on ajout ce contenu

```
40 #email size for 10M
41 message_size_limit = 10485760
42 # 1G
43 mailbox_size_limit = 1073741824
44
45 #SMTP-AUTH settings
46 #smtpd_sasl_type = dovecot
47 #smtpd_sasl_path = private/auth
48 #smtpd_sasl_auth_enable = yes
49 #smtpd_sasl_security_options = noanonymous
50 #smtpd_sasl_local_domain = $myhostname
51 #smtpd_recipient_restrictions = permit_mynetworks, permit_auth_destination, permit_sasl_authenticated, reject
```

Apres avoir faire sa on enregistrer en mettant Echap : wq

Ensuite on activer le service postfix

```
[root@server ~]# systemctl enable --now postfix.service
```

Ajout service smtp au pare feu

```
[root@server ~]# firewall-cmd --add-service=smtp --permanent
[root@server ~]# firewall-cmd --reload
```

Maintenant nous allons la configuration du dovecot avec test de mail

- Configuration dovecot

  Il va falloir installer tout d'abord les paquets dovecot avant de commencer la configuration de dovecot comme montre ci-dessous :

  ```
  [root@server ~]# yum install dovecot -y
  ```

  Apres l'installation nous allons éditer ce fichier

  ```
  [root@server ~]# vim /etc/dovecot/dovecot.conf
  ```

  Dans la ligne 30 on décommente

  ```
  30 listen = *, ::
  ```

  Nous éditons ce fichier

  ```
  [root@server ~]# vim /etc/dovecot/conf.d/10-auth.conf
  ```

  Dans la ligne 10 on décommente et ont enlevé le yes on met sa a no

  ```
  10 disable_plaintext_auth = no
  ```

  Dans la ligne 100 on décommente et on ajout à la fin login

```
100 auth_mechanisms = plain login
```

Ensuite on doit éditer ce fichier

```
[root@server ~]# vim /etc/dovecot/conf.d/10-master.conf
```

Dans ce contenu nous allons décommenter les lignes (107 jusqu'à 11) et ajouter user=postfix et group=postfix

```
105
106   # Postfix smtp-auth
107   unix_listener /var/spool/postfix/private/auth {
108     mode = 0666
109     user = postfix
110     group = postfix
111   }
```

Ensuite nous éditons ce fichier

```
[root@server ~]# vim /etc/dovecot/conf.d/10-ssl.conf
```

Dans ce contenu nous allons décommente la ligne 8 et changer le required en mettant yes

```
 8 ssl = yes
```

Ensuite on doit éditer le fichier

```
[root@server ~]# vim /etc/dovecot/conf.d/10-mail.conf
```

Dans ce contenu dans la ligne 30 on décommente et on va ajouter Mail…

```
29 #
30 mail_location = maildir:~/Maildir
```

Apres nous allons activer le service dovecot

```
[root@server ~]# systemctl enable --now dovecot
```

Ensuite on ajout le protocole dans le pare feu

```
[root@server ~]# firewall-cmd --add-service={pop3,imap} --permanent

[root@server ~]# firewall-cmd --reload
```

Apres l'installation de Postfix et Dovecot nous procédons à l'installation de roundcube

Nous allons télécharger le package de roundcube

```
[root@server named]# wget https://github.com/roundcube/roundcubemail/releases/download/1.4.4/roundcubemail-1.4.4-comp
lete.tar.gz
```

- ✓ L'installation de MySQL

```
[root@server Téléchargements]# mysql_secure_installation
```

On crée la base de données

```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| roundcube          |
| webmail            |
+--------------------+
5 rows in set (0,017 sec)
```

Ensuite nous allons procéder dans l'installation de roundcube

D'abord nous allons dans le fichier /var/www/html pour télécharger

```
[root@server ~]# cd /var/www/html/
[root@server html]#
```

Nous telechargeons le paquet dans GitHub

```
[root@server html]# wget https://github.com/roundcube/roundcubemail/releases/download/1.4.11/roundcubemail-1.4.11-complete.tar.gz
```

Ensuite nous allons décompresser le roundcube

```
[root@server html]# tar -zxvf roundcubemail-1.4.4-complete.tar.gz
```

Et on va le déplacer dans le dossier mail

```
[etudiant@server config]$ mv roundcubemail-1.4.4 mail
```

```
[etudiant@server html]$ cd mail/
[etudiant@server mail]$ ls
bin        composer.json      composer.lock  index.php  installer  logs     program      README.md  SQL      UPGRADING
CHANGELOG  composer.json-dist  config         INSTALL    LICENSE    plugins  public_html  skins      temp     vendor
[etudiant@server mail]$
```

Ensuite on déplacer dans config

```
[etudiant@server mail]$ cd config/
[etudiant@server config]$
```

On copie le fichier config.inc.php.sample dans config.inc.php

```
[etudiant@server config]$ cp config.inc.php.sample config.inc.php
```

On va éditer le fichier config.inc.php

```
[etudiant@server config]$ vim config.inc.php
```

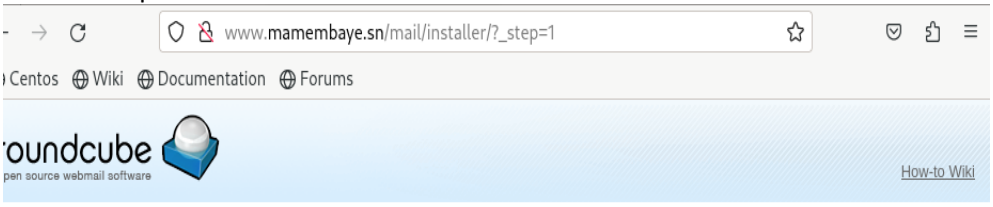
Nous allons faire des modifications dans les lignes qui suit de 25,41,53,56 et 71

```
// For example %n = mail.domain.tld, %t = domain.tld
$config['default_host'] = 'server.mamembaye.sn';

// SMTP server host (for sending mails).
// Enter hostname with prefix ssl:// to use Implicit TLS, or use
// prefix tls:// to use STARTTLS.
// Supported replacement variables:
// %h - user's IMAP hostname
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %z - IMAP domain (IMAP hostname without the first part)
// For example %n = mail.domain.tld, %t = domain.tld
$config['smtp_server'] = 'server.mamembaye.sn';

// SMTP port. Use 25 for cleartext, 465 for Implicit TLS, or 587 for STARTTLS (default)
$config['smtp_port'] = 25;

// SMTP username (if required) if you use %u as the username Roundcube
// will use the current username for login
$config['smtp_user'] = '%u';

// SMTP password (if required) if you use %p as the password Roundcube
// will use the current user's password for login
$config['smtp_pass'] = '%p';

// provide an URL where a user can get support for this Roundcube installation
// PLEASE DO NOT LINK TO THE ROUNDCUBE.NET WEBSITE HERE!
$config['support_url'] = '';

// Name your service. This is displayed on the login screen and in the window title
$config['product_name'] = ' Webmail mamembaye';
```

Ensuite on va faire l'activation des droits

```
[etudiant@server config]$ chown -R apache:apache /var/www

[etudiant@server config]$ chmod -R 755 /var/www/html/mail/
```

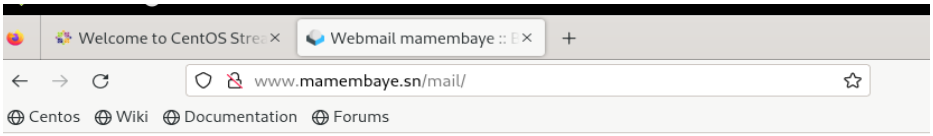
On vois sa que notre roundcube et bien installer

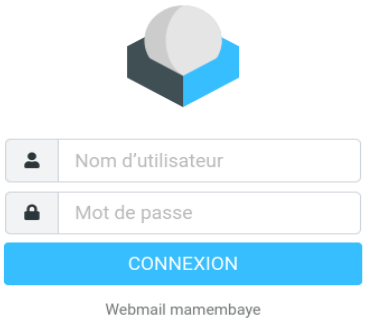


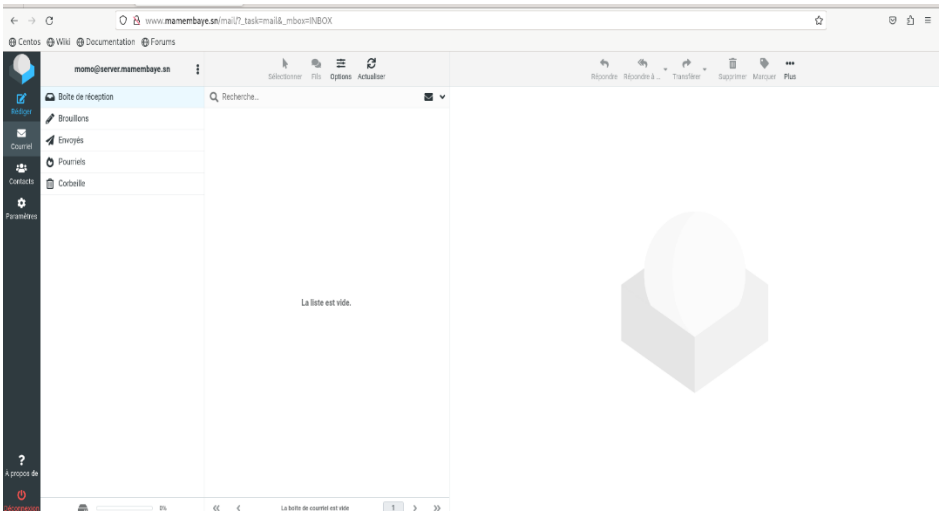
On copie cette commande et on va le mettre dans le fichier de configuration

```
#$config['enable_installer'] = true;
```

Notre roundcube et bien installer







✓ Couplage Roundcube et ldap

D'abord nous installons ce paquet postfix-ldap

```
[root@server ~]# yum install postfix-ldap -y
```

Ensuite nous allons créer un utilisateur LDIF pour le mailing

```
[root@server ~]# vim msg.ldif
```

Ajouter ce fichier

```
dn: cn=msg,cn=schema,cn=config
objectClass: olcSchemaConfig
cn: msg
olcAttributeTypes: (1.3.6.1.4.1.8869.2.3.1 NAME 'mailEnabled'
    DESC 'Mailbox Enabled'
    EQUALITY booleanMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.7 SINGLE-VALUE)
olcAttributeTypes: (1.3.6.1.4.1.8869.2.3.2 NAME 'mailQuota'
        DESC 'defines how much mail quota is available for the user'
        EQUALITY caseIgnoreMatch
        SUBSTR caseIgnoreSubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 SINGLE-VALUE)
olcAttributeTypes: (1.3.6.1.4.1.8869.2.3.3 NAME 'mailGroup'
        DESC 'RFC1274: RFC822 Mailbox'
        EQUALITY caseIgnoreIA5Match
        SUBSTR caseIgnoreIA5SubstringsMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.26{256})
olcObjectClasses: ( 1.3.6.1.4.1.8869.2.4.1 NAME 'mailExtension'
        DESC 'More Mail Options'
        SUP top AUXILIARY
        MUST ( cn  )
        MAY ( mailEnabled $ mailQuota )
        )
olcObjectClasses: ( 1.3.6.1.4.1.8869.2.4.2 NAME 'groupMail'
        DESC 'Group mail address'
        SUP top AUXILIARY
        MUST ( cn  )
        MAY ( mailGroup )
        )
```

Ensuite nous allons effectuer une mise à jour

```
[root@server ~]# ldapadd -Y EXTERNAL -H ldapi:/// -f msg.ldif
```

Ensuite nous allons créer deux utilisateurs

User1

```
[root@server ~]# vim user1.ldif
```

Ajoutons ce fichier

```
dn: uid=lala,ou=utilisateurs,dc=mamembaye,dc=sn
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: mailExtension
homeDirectory: /home/lala
loginShell: /bin/bash
uidNumber: 1000
gidNumber: 1000
uid: lala
sn: lala
givenName: lala
cn: lala
displayName: lala
userPassword: {SSHA}
mail: lala@amamembaye.sn
mailEnabled: TRUE
mailQuota: 2G
```

#USER 2

```
[root@server ~]# vim user2.ldif
```

Ajoutons ce fichier

```
dn: uid=fifi,ou=utilisateurs,dc=mamembaye,dc=sn
objectClass: top
objectClass: posixAccount
objectClass: shadowAccount
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: mailExtension
homeDirectory: /home/fifi
loginShell: /bin/bash
uidNumber: 10001
gidNumber: 10001
uid: fifi
sn: fifi
givenName: fifi
cn: fifi
displayName: fifi
userPassword: {SSHA}
mail: fifi@mamembaye.sn
mailEnabled: TRUE
mailQuota: 2G
~
```

Mise a jour de la base des utilisateurs

```
[root@server ~]# ldapadd -x -W -D "cn=admin,dc=mamembaye,dc=sn" -f user1.ldif
```

```
[root@server ~]# ldapadd -x -W -D "cn=admin,dc=mamembaye,dc=sn" -f user2.ldif
```

Configuration Mail virtuel

```
[root@server ~]# mkdir /usr/local/vmail
chmod 700 /usr/local/vmail
groupadd --gid 5000 vmail
useradd -g vmail -u 5000 vmail -d /home/vmail -m
chown vmail: /home/vmail -R
chown vmail: /usr/local/vmail -R
```

Configuration liaison POSTFIX LDAP

```
[root@server ~]# vim /etc/postfix/sender_login_maps.cf
```

Insérer ce contenu

```
server_host     = 192.168.0.1
server_port     = 389
bind            = yes
start_tls       = no
version         = 3
bind_dn         = cn=admin,dc=mamembaye,dc=sn
bind_pw         = passer
search_base     = dc=mamembaye,dc=sn
scope           = sub
query_filter    = (&(mail=%s)(objectClass=person)(mailEnabled=TRUE))
result_attribute = mail
~
~
```

Ensuite nous allons éditer ce fichier

```
[root@server ~]# vim msg.ldif
```

Insérer ce contenu

```
server_host              = 192.168.0.1
server_port              = 389
bind                     = yes
start_tls                = no
version                  = 3
bind_dn                  = cn=admin,dc=mamembaye,dc=sn
bind_pw                  = passer
search_base              = dc=mamembaye,dc=sn
scope                    = sub
query_filter             = (&(objectClass=groupOfNames)(mailGroup=%s))
leaf_result_attribute    = mail
special_result_attribute = member
result_attribute         = mail
debuglevel               = 0
```

Ensuite nous allons éditer ce fichier

```
[root@server ~]# vim /etc/postfix/virtual_forward_maps.cf
```

Inférer ce contenu

```
server_host      = 192.168.0.1
server_port = 389
bind             = yes
start_tls        = no
version          = 3
bind_dn          = cn=admin,dc=mamembaye,dc=sn
bind_pw          = passer
search_base      = dc=mamembaye,dc=sn
scope            = sub
query_filter     = (&(mail=%s)(mailGroup=*)(mailEnabled=TRUE)(objectClass=person))
result_attribute = mailGroup
debuglevel       = 0
```

Ensuite nous allons éditer ce fichier

```
[root@server ~]# vim /etc/postfix/transport
```

On écrit dans le fichier mon domaine + dovecot

```
#
# NAME
#        transport - Postfix transport table format
mamembaye.sn dovecot
# SYNOPSIS
```

Ensuite nous allons éditer ce fichier

```
[root@server ~]# vim /etc/postfix/virtual_mailbox_maps.cf
```

Insérer ce contenu

```
server_host       = 192.168.0.1
server_port       = 389
bind              = yes
start_tls         = no
version           = 3
bind_dn           = cn=admin,dc=mamembaye,dc=sn
bind_pw           = passer
search_base       = dc=mamembaye,dc=sn
scope             = sub
query_filter      = (&(mail=%s)(objectClass=person))
result_attribute  = mail
result_format     = /home/vmail/%d/%u/mailbox/
debuglevel        = 0
~
~
~
```

Ensuite nous allons éditer ce fichier

```
[root@server ~]# vim /etc/postfix/main.cf
```

commenter: ou il y'a smtp, mydestination, html_directory, readme_directory

```
# The mail_spool_directory parameter specifies the directory where
# UNIX-style mailboxes are kept. The default setting depends on the
# system type.
#
#mail_spool_directory = /var/mail
#mail_spool_directory = /var/spool/mail

# The mailbox_command parameter specifies the optional external
# command to use instead of mailbox delivery. The command is run as
# the recipient with proper HOME, SHELL and LOGNAME environment settings.
# Exception:  delivery for root is done as $default_user.
#
# Other environment variables of interest: USER (recipient username),
# EXTENSION (address extension), DOMAIN (domain part of address),
# and LOCAL (the address localpart).
#
# Unlike other Postfix configuration parameters, the mailbox_command
# parameter is not subjected to $parameter substitutions. This is to
# make it easier to specify shell syntax (see example below).
#
# Avoid shell meta characters because they will force Postfix to run
# an expensive shell process. Procmail alone is expensive enough.
#
# IF YOU USE THIS TO DELIVER MAIL SYSTEM-WIDE, YOU MUST SET UP AN
# ALIAS THAT FORWARDS MAIL FOR ROOT TO A REAL USER.
#
#mailbox_command = /some/where/procmail
#mailbox_command = /usr/bin/procmail

# The mailbox_transport specifies the optional transport in master.cf
# to use after processing aliases and .forward files. This parameter
# has precedence over the mailbox_command, fallback_transport and
# luser_relay parameters.
#
# Specify a string of the form transport:nexthop, where transport is
# the name of a mail delivery transport defined in master.cf.  The
# :nexthop part is optional. For more details see the sample transport
# configuration file.
#
# NOTE: if you use this feature for accounts not in the UNIX password
# file, then you must update the "local_recipient_maps" setting in
# the main.cf file, otherwise the SMTP server will reject mail for
# non-UNIX accounts with "User unknown in local recipient table".
#
# Cyrus IMAP over LMTP. Specify ``lmtpunix      cmd="lmtpd"
# listen="/var/imap/socket/lmtp" prefork=0'' in cyrus.conf.
#mailbox_transport = lmtp:unix:/var/lib/imap/socket/lmtp
```

Ajouter à la fin du fichier

```
mydestination = $myhostname localhost
disable_vrfy_command = yes
smtpd_helo_required = yes
smtpd_sasl_type=dovecot
smtpd_sasl_path=private/auth_dovecot
smtpd_sasl_auth_enable = yes
smtpd_sasl_authenticated_header = yes
broken_sasl_auth_clients = yes
proxy_read_maps = $local_recipient_maps $mydestination $virtual_alias_maps $virtual_alias_domains $virtual_mailbox_maps $virtual_mailbox_domains $relay_recipient_maps $relay_domains $canonical_maps $sender_canonical_maps $recipient_canon
cal_maps $relocated_maps $transport_maps $mynetworks $smtpd_sender_login_maps
smtpd_sender_restrictions = reject_authenticated_sender_login_mismatch, reject_unknown_sender_domain, permit_sasl_authenticated
smtpd_recipient_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_rbl_client zen.spamhaus.org, reject_unauth_destination, reject_unknown_reverse_client_hostname,
smtpd_banner = $myhostname ESMTP
biff = no
append_dot_mydomain = no
readme_directory = /usr/share/doc/postfix
smtpd_sasl_security_options = noanonymous
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache
disable_vrfy_command = yes
smtpd_helo_required = yes
smtpd_data_restrictions = reject_unauth_pipelining, permit
virtual_mailbox_base = /home/vmail/
virtual_alias_domains =
virtual_minimum_uid = 104
virtual_uid_maps = static:5000
virtual_gid_maps = static:5000
virtual_transport = dovecot
html_directory = /usr/share/doc/postfix/html
relayhost =
sender_bcc_maps =
recipient_bcc_maps =
relay_domains =
relay_recipient_maps =
smtpd_sasl_local_domain = $mydomain
virtual_mailbox_domains = $mydomain
smtpd_sender_login_maps = ldap:/etc/postfix/sender_login_maps.cf
virtual_mailbox_maps = ldap:/etc/postfix/virtual_mailbox_maps.cf
virtual_alias_maps = ldap:/etc/postfix/virtual_group_maps.cf ldap:/etc/postfix/virtual_forward_maps.cf
dovecot_destination_recipient_limit=1
transport_maps = hash:/etc/postfix/transport
local_recipient_maps = $virtual_mailbox_maps
```

Nous déplaçons ce fichier

```
[root@server ~]# mv /etc/postfix/master.cf /home/etudiant/Documents
```

Ensuite nous allons éditer ce fichier

```
[root@server ~]# vim /etc/postfix/master.cf
```

Ajouter ce contenu

```
smtp      inet  n       -       -       -       -       smtpd
submission inet n       -       -       -       -       smtpd
  -o smtpd_enforce_tls=yes
  -o smtpd_tls_security_level=encrypt
  -o tls_preempt_cipherlist=yes
pickup    fifo  n       -       -       60      1       pickup
cleanup   unix  n       -       -       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
tlsmgr    unix  -       -       -       1000?   1       tlsmgr
rewrite   unix  -       -       -       -       -       trivial-rewrite
bounce    unix  -       -       -       -       0       bounce
defer     unix  -       -       -       -       0       bounce
trace     unix  -       -       -       -       0       bounce
verify    unix  -       -       -       -       1       verify
flush     unix  n       -       -       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
smtp      unix  -       -       -       -       -       smtp
relay     unix  -       -       -       -       -       smtp
showq     unix  n       -       -       -       -       showq
error     unix  -       -       -       -       -       error
retry     unix  -       -       -       -       -       error
discard   unix  -       -       -       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       -       -       -       lmtp
anvil     unix  -       -       -       -       1       anvil
scache    unix  -       -       -       -       1       scache
maildrop  unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail argv=/usr/bin/maildrop -d ${recipient}
uucp      unix  -       n       n       -       -       pipe
  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
ifmail    unix  -       n       n       -       -       pipe
  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
bsmtp     unix  -       n       n       -       -       pipe
  flags=Fq. user=bsmtp argv=/usr/lib/bsmtp/bsmtp -t$nexthop -f$sender $recipient
scalemail-backend unix  -       n       n       -       2       pipe
  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store ${nexthop} ${user} ${extension}
mailman   unix  -       n       n       -       -       pipe
  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
  ${nexthop} ${user}
dovecot   unix  -       n       n       -       -       pipe
#  flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/deliver -d ${recipient}
   flags=DRhu user=vmail:vmail argv=/usr/libexec/dovecot/deliver -d ${recipient}
```

Ensuite nous allons faire la vérification

```
[root@server ~]# postmap -q fifi@mamembaye.sn ldap:/etc/postfix/sender_login_maps.cf
```

Nous démarrons le service

```
[root@server ~]# service postfix restart
```

Ensuite nous éditer le fichier dovecot

```
[root@server ~]# vim /etc/dovecot/dovecot.conf
```

Insérer ce contenu

```
!include_try local.conf


auth_mechanisms = plain login
mail_uid = vmail
mail_gid = vmail
login_log_format_elements = "user=<%u> method=%m rip=%r lip=%l mpid=%e %c %k"
mail_plugins = quota
log_timestamp = "%Y-%m-%d %H:%M:%S "
protocols = imap
listen = *
auth_cache_size = 50000
auth_cache_ttl = 300s
auth_cache_negative_ttl = 30s

userdb {
  args = /etc/dovecot/dovecot-ldap-user.conf.ext
  driver = ldap
}
passdb {
  args = /etc/dovecot/dovecot-ldap-pass.conf.ext
  driver = ldap
}

service auth {
  unix_listener /var/spool/postfix/private/auth_dovecot {
    group = postfix
mode = 0660
    user = postfix
  }
  unix_listener auth-userdb {
    mode = 0600
    user = vmail
  }
  user = root
}

service dict {
    unix_listener dict {
        mode = 0660
        user = vmail
        group = vmail
    }
}

namespace inbox {
  inbox = yes
  location =
```

Ensuite nous allons éditer ce fichier

```
[root@server ~]#
vim /etc/dovecot/dovecot-ldap-user.conf.ext
```

Insérer ce contenu

```
hosts = 192.168.0.1
dn = cn=admin,dc=mamembaye,dc=sn
dnpass = passer
debug_level = 0
auth_bind = no
ldap_version = 3
base = dc=mamembaye,dc=sn
scope = subtree
user_attrs = \
  =quota_rule=*:bytes=%{ldap:mailQuota}, \
  =home=/home/vmail/%d/%{ldap:uid}, \
  =mail=maildir:/home/vmail/%d/%{ldap:uid}/mailbox
user_filter = (&(mail=%u)(objectClass=person)(mailEnabled=TRUE))
iterate_attrs        = mail=user
iterate_filter       = (objectClass=person)

~
~
~
```

Ensuite nous allons éditer ce fichier

```
[root@server ~]# vim /etc/dovecot/dovecot-ldap-pass.conf.ext
```

Insérer ce contenu

```
hosts  = 192.168.0.1
dn = cn=admin,dc=mamembaye,dc=sn
dnpass = passer
debug_level = 0
auth_bind = no
ldap_version = 3
base = dc=passer,dc=sn
scope = subtree

pass_attrs = mail=user,userPassword=password
pass_filter = (&(mail=%u)(objectClass=person)(mailEnabled=TRUE))
default_pass_scheme = CRYPT
```

HASH

```
[root@server ~]# postmap hash:/etc/postfix/transport
```

CONCLUSION

A l'issu de ce travail on a pu configurer un serveur de messagerie « Roundcube » et PhpLDAPadmin sous RedHat (CentOS Stream 9). Ce travail nous a été facilité pour nous familiariser de l'environnement linux (Webmail Roundcube) et revêt d'une importance capitale car il nous permet de consolider nos connaissances en administration Linux, ce qui est fréquent dans les entreprises.