

# Procédure mise en place d'un serveur Mail IRedMail (Linux)

## Mise en place d'un serveur Mail

Procédure mise en place d'un serveur Mail IRedMail (Linux).....	1
1- Prérequis.....	1
2- Installation des packages.....	1
3- Interface Web.....	8
4- Création d'un utilisateur « spécial » LDAP.....	9
5- Configuration de OpenLDAP.....	11
6- Activation de requête LDAP dans Postfix.....	12
7- Activation de l'intégration de l'AD dans Dovecot.....	14
8-Tests de validation .....	17

## 1-Prérequis

Récupérer le lien de téléchargement de la dernière version de IRedMail sur le site officiel (<https://www.iredmail.org/download.html>).

Voici le lien de ma version (1.7.2) : <https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.2.tar.gz>

-Nous avons besoin d'une machine Debian avec au moins 4Go de mémoire RAM installé.

Commençons par mettre à jours les packages présents sur la machine .

## 2-Installation des packages

Commençons par récupérer le dossier de téléchargement avec le lien que nous avons copié, grâce à la commande wge :

**wget <https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.2.tar.gz>**



Mathias Vételé BTS SIO

```
root@srv-mail:~# wget https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.2.tar.gz
--2025-03-12 14:58:04-- https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.2.tar.gz
Résolution de github.com (github.com)... 140.82.121.4
Connexion à github.com (github.com)[140.82.121.4]:443... connecté.
requête HTTP transmise, en attente de la réponse... 302 Found
Emplacement : https://codeload.github.com/iredmail/iRedMail/tar.gz/refs/tags/1.7.2 [suivant]
--2025-03-12 14:58:04-- https://codeload.github.com/iredmail/iRedMail/tar.gz/refs/tags/1.7.2
Résolution de codeload.github.com (codeload.github.com)... 140.82.121.10
Connexion à codeload.github.com (codeload.github.com)[140.82.121.10]:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 249156 (243K) [application/x-gzip]
Sauvegarde en : « 1.7.2.tar.gz »
```

```
1.7.2.tar.gz          100%[=====>] 243,32K  --.-KB/s  ds 0,1s
```

```
2025-03-12 14:58:04 (2,06 MB/s) - « 1.7.2.tar.gz » sauvegardé [249156/249156]
```

Nous allons ensuite décompresser le dossier 1.7.2.tar.gz :

***tar xzvf 1.7.2.tar.gz***

Maintenant, nous allons devoir modifier les droits du script d'installation iRedMail.sh pour le rendre exécutable et lancer le script. Nous allons donc nous déplacer dans le dossier décompressé iRedMail-1.7.2 .

```
root@srv-mail:~# ls
1.7.2.tar.gz  iRedMail-1.7.2
root@srv-mail:~# cd iRedMail-1.7.2/
root@srv-mail:~/iRedMail-1.7.2# ls
ChangeLog  conf  dialog  Documentations  functions  iRedMail.sh  LICENSE  pkgs  README.md  samples  tools  update
```

Modifions les droits de ce dossier :

***chmod u+x iRedMail.sh***

Puis, lançons le script :

***./iRedMail.sh***

Une fois que le script à terminer d'installer les premiers packages, une fenêtre apparaît, il faut sélectionner « **YES** »

**Welcome**

Welcome to the iRedMail setup wizard, we will ask you some simple questions required to setup a mail server. If you encounter any trouble or issues, please report to our support forum:  
<https://forum.iredmail.org/>

----- WARNING -----  
iRedMail is designed to be deployed on a \_\_FRESH\_\_ server, which means your server should \_\_NOT\_\_ have mail related components installed, e.g. Nginix / Apache, MySQL / MariaDB / PostgreSQL / OpenLDAP, Postfix, Dovecot, Amavisd, etc. iRedMail will install and configure required softwares automatically. Otherwise it may mess up your server by overriding existing config files without asking.  
-----

NOTE: You can abort this setup wizard by pressing key Ctrl-C.

Ici est renseigné le dossier par défaut où seront stockés les boites mails :

**Default mail storage path**

Please specify a directory (in lowercase) used to store user mailboxes.  
Default is: /var/vmail

NOTES:

- \* Depends on the mail traffic, it may take large disk space.
- \* Maildir path will be converted to lowercases, so please create this directory in lowcases.
- \* It cannot be /var/mail or /root.
- \* Mailboxes will be stored under its sub-directory: /var/vmail/vmail1/
- \* Daily backup of SQL/LDAP databases will be stored under another sub-directory: /var/vmail/backup.

Sélectionnons « **Nginx** » pour installer l'interface Web

**Preferred web server**

Choose a web server you want to run.

TIP: Use SPACE key to select item.

<input checked="" type="checkbox"/> (*)	<b>Nginx</b>	<b>The fastest web server</b>
<input type="checkbox"/> ( )	<b>No web server</b>	I don't need any web applications on this server

< Next >

Nous devons ensuite sélectionner la base de données de notre choix. Ici, nous allons utiliser « **OpenLDAP** » afin de pouvoir récupérer les utilisateurs de notre Active Directory. En utilisant **MariaDB** ou **PostgreSQL** nous devons créer les utilisateurs manuellement.

**Choose preferred backend used to store mail accounts**

It's strongly recommended to choose the one you're familiar with for easy maintenance. They all use the same webmail (Roundcube) and admin panel (iRedAdmin), and no big feature differences between them.

TIP: Use SPACE key to select item.

<input checked="" type="checkbox"/> (*)	<b>OpenLDAP</b>	<b>An open source implementation of LDAP protocol</b>
<input type="checkbox"/> ( )	<b>MariaDB</b>	An enhanced, drop-in replacement for MySQL
<input type="checkbox"/> ( )	<b>PostgreSQL</b>	Powerful, open source database system

< Next >

Renseignons ici notre domaine :

**LDAP suffix (root dn)**  
Please specify your LDAP suffix (root dn):

EXAMPLE:

- \* Domain 'example.com': dc=example,dc=com
- \* Domain 'test.com.cn': dc=test,dc=com,dc=cn

Note: Password for LDAP rootdn (cn=Manager,dc=xx,dc=xx) will be generated randomly.

dc=vetele,dc=mv

< Next >

Il faut renseigner un mot de passe pour l'administrateur de la base de données :

**Password for MySQL administrator: root**  
Please specify password for MySQL administrator root on server 127.0.0.1.

WARNING:

- \* Do \*NOT\* use double quote (") in password.
- \* EMPTY password is \*NOT\* permitted.
- \* Sample password: 2fnpTyEP7M0mJWg0J9LdZa2EIlqPBAsD

< Next >

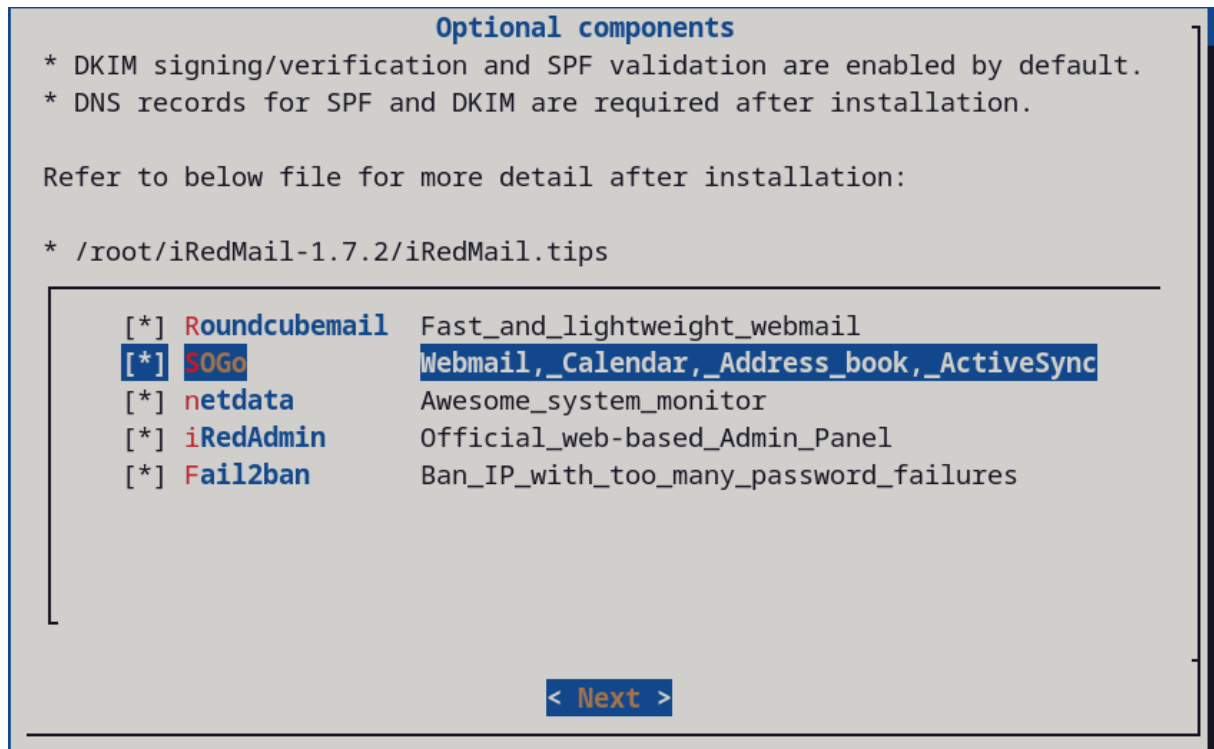
Renseigner de nouveau notre nom de domaine :

**Your first mail domain name**  
Please specify your first mail domain name.  
  
EXAMPLE:  
  
\* example.com  
  
WARNING:  
  
It can \*NOT\* be the same as server hostname: srv-mail.vetele.mv.  
  
We need Postfix to accept emails sent to system accounts (e.g. root), if your mail domain is same as server hostname, Postfix won't accept any email sent to this mail domain.  
  
  
  
[< Next >](#)

Renseigner de nouveau un mot de passe, ici pour l'Administrateur du serveur Mail :

**Password for the mail domain administrator**  
Please specify password for the mail domain administrator:  
  
\* postmaster@vetele.mv  
  
You can login to webmail and iRedAdmin with this account.  
  
WARNING:  
  
\* Do \*NOT\* use special characters (like \$, white space) in password.  
\* EMPTY password is \*NOT\* permitted.  
\* Sample password: ycSF40xTlbrfnwpudHb3jYPbF6lzq1Eh  
  
  
  
[< Next >](#)

Sélectionner ces composants :



A la fin du script, il y'a deux questions auxquelles il faut répondre **YES**

```
*****
* iRedMail-1.7.2 installation and configuration complete.
*****

< Question > Would you like to use firewall rules provided by iRedMail?
< Question > File: /etc/nftables.conf, with SSHD ports: 22. [Y|n][ INFO ] Copy firewall sample rules.
< Question > Restart firewall now (with ssh ports: 22)? [y|N]
```

A la fin de l'installation, un récapitulatif des paramètres s'affichera :

```

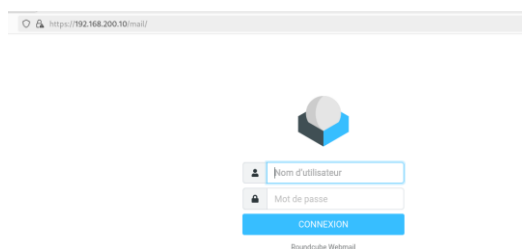
r
r - Web admin panel (iRedAdmin): https://srv-mail.vetele.mv/iredadmin/
r
r You can login to above links with below credential:
r
r - Username: postmaster@vetele.mv
r - Password: [REDACTED]
r
*****
r Congratulations, mail server setup completed successfully. Please
r read below file for more information:
r
r - /root/iRedMail-1.7.2/iRedMail.tips
r
r And it's sent to your mail account postmaster@vetele.mv.
r
***** WARNING *****
r
r Please reboot your system to enable all mail services.
r
*****

```

Il faut maintenant redémarrer la machine avec la commande **reboot**

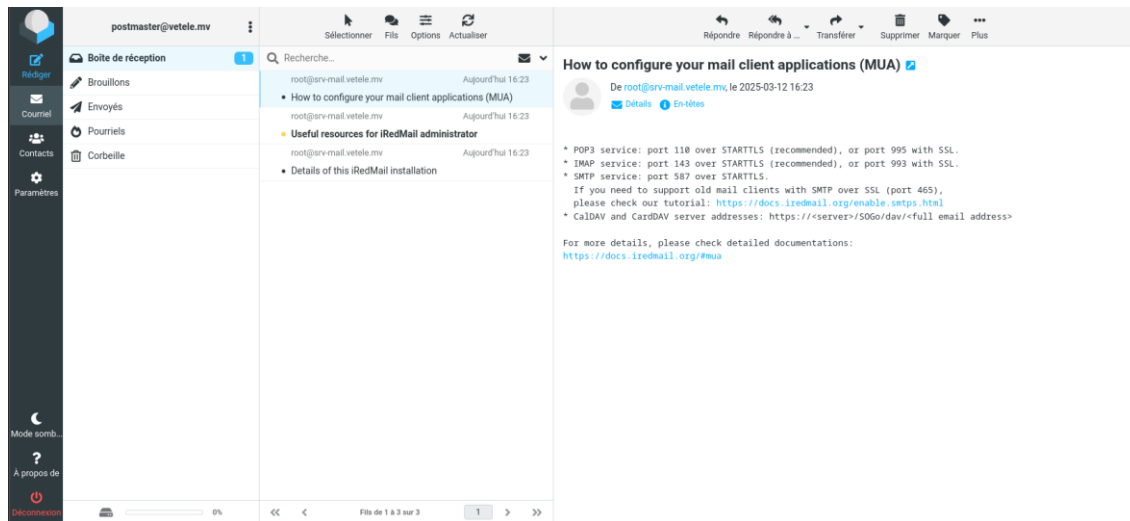
### 3-Interface Web

Sur un client dans le même réseau que notre serveur web, accéder à un navigateur et taper l'adresse IP du server en question, nous devons atterrir sur cette page web :



Nous allons maintenant essayer de nous connecter avec l'adresse configuré plus tôt ([postmaster@vetele.mv](mailto:postmaster@vetele.mv)) :






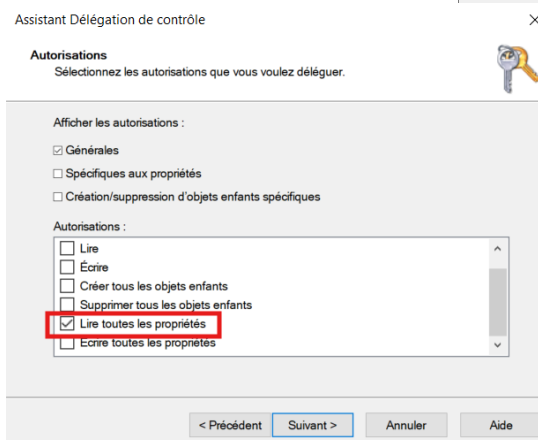
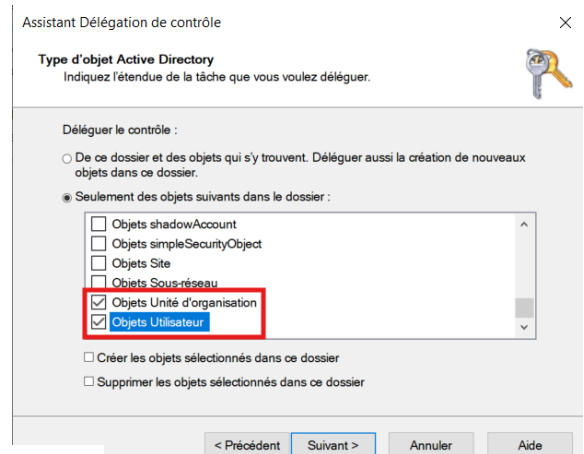
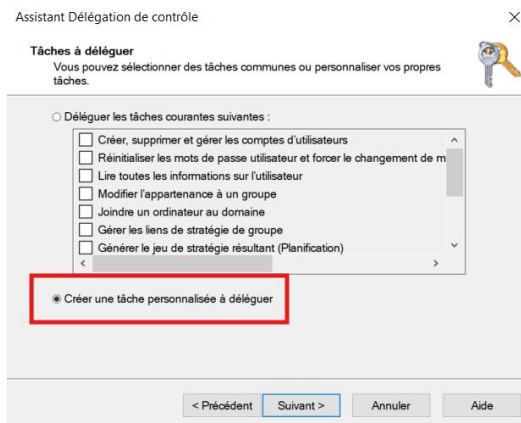
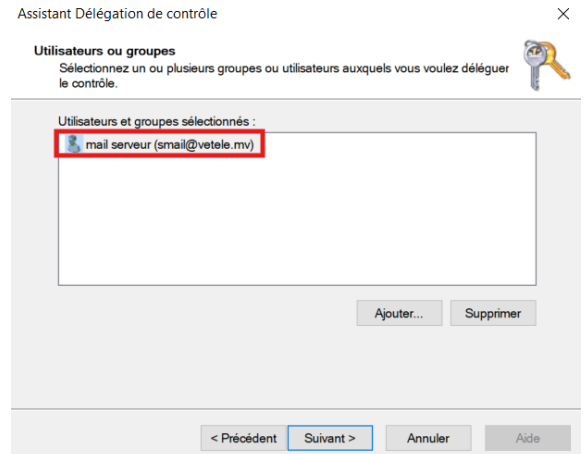
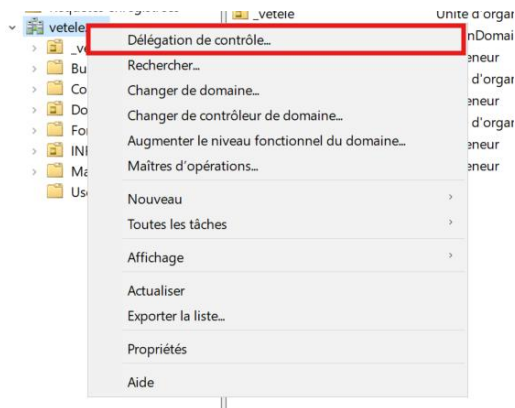
Nous avons bien accès à sa boîte mail. Elle comporte 3 messages avec des informations sur votre serveur.

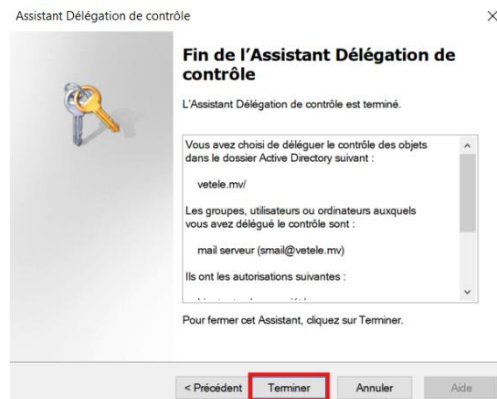
## 4-Création d'un utilisateur « spécial » LDAP

Sur notre Active Directory, nous allons devoir créer un nouvel utilisateur qui sera utilisé pour effectuer la transmission d'informations de nos utilisateurs Active Directory avec le protocole

LDAP. Nous allons donc devoir lui appliquer des droits en lecture Seule. Ici, notre utilisateur sera celui-ci :  mail serveur Utilisateur

Nous allons donc devoir créer une délégation de contrôle :





## 5-Configuration de OpenLDAP

Nous allons maintenant configurer OpenLDAP, mais avant tout, il faut qu'on s'assure que la recherche LDAP fonctionne correctement avec notre utilisateur précédemment créé ([smail@vetele.mv](mailto:smail@vetele.mv)).

Testons donc la recherche avec cette commande :

```
ldapsearch -x -H ldap://SRV1.vetele.mv -D 'smail@vetele.mv' -W -b 'ou=_vetele,dc=vetele,dc=mv'
```

```
root@srv-mail:~# ldapsearch -x -H ldap://SRV1.vetele.mv -D 'smail@vetele.mv' -W -b 'ou=_vetele,dc=vetele,dc=mv'
```

Préciser bien le bonne OU, où est stocké notre utilisateur.

Il faudra renseigner le mot de passe de l'utilisateur **smail**.

Cette commande nous renvoie des informations sur nos utilisateurs :

```
# Ophelie Louineaux, IT, _vetele, vetele.mv
dn: CN=Ophelie Louineaux,OU=IT,OU=_vetele,DC=vetele,DC=mv
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Ophelie Louineaux
sn: Louineaux
description: IT1
givenName: Ophelie
distinguishedName: CN=Ophelie Louineaux,OU=IT,OU=_vetele,DC=vetele,DC=mv
instanceType: 4
whenCreated: 20250311145119.0Z
whenChanged: 20250311145119.0Z
displayName: Ophelie Louineaux
uSNCreated: 114965
uSNChanged: 114969
name: Ophelie Louineaux
objectGUID:: 0UIltSNOck2sXp6MdD0PhQ==
userAccountControl: 512
badPwdCount: 0
```

## 6-Activation de requête LDAP dans Postfix

Sur notre serveur mail, nous allons devoir désactiver des paramètres spéciaux iRedMail, inutilisés, afin de pouvoir activer la requête LDAP :

Utilisons ces commandes :

```
postconf -e virtual_alias_maps=""  
postconf -e sender_bcc_maps=""  
postconf -e recipient_bcc_maps=""  
postconf -e relay_domains=""  
postconf -e relay_recipient_maps=""  
postconf -e sender_dependent_relayhost_maps=""
```

-Ajoutons maintenant notre nom de domaine de messagerie :

```
postconf -e smtpd_sasl_local_domain='vetele.mv'  
postconf -e virtual_mailbox_domains='vetele.mv'
```

Modifier les paramètres de cartes de transport :

```
postconf -e transport_maps='hash:/etc/postfix/transport'
```

-Activer la requête AD

```
postconf -e smtpd_sender_login_maps='proxy:ldap:/etc/postfix/ad_sender_login_maps.cf'  
postconf -e virtual_mailbox_maps='proxy:ldap:/etc/postfix/ad_virtual_mailbox_maps.cf'  
postconf -e virtual_alias_maps='proxy:ldap:/etc/postfix/ad_virtual_group_maps.cf'
```

-Il nous faut créer ce fichier **/etc/postfix/transport**, puis écrire dedans :

```
nano /etc/postfix/transport
```

```
GNU nano 7.2 /etc/postfix/transport *  
vetele.mv dovecot
```

-Exécuter postmap pour que Postfix puisse lire le fichier :

***postmap hash:/etc/postfix/transport***

-Créer le fichier : /etc/postfix/ad\_sender\_login\_maps.cf , puis le remplir de cette manière :

***nano /etc/postfix/ad\_sender\_login\_maps.cf***

```
GNU nano 7.2 /etc/postfix/ad_sender_login_maps.cf *  
server_host      = SRV1.vetele.mv  
server_port      = 389  
version          = 3  
bind             = yes  
start_tls        = no  
bind_dn          = smail  
bind_pw          =   
search_base      = ou=_vetele,dc=vetele,dc=mv  
scope            = sub  
query_filter     = (&(userPrincipalName=%s)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))  
result_attribute = userPrincipalName  
debuglevel       = 0
```

-Créer le fichier /etc/postfix/ad\_virtual\_mailbox\_maps.cf, puis le remplir de cette manière :

***nano /etc/postfix/ad\_virtual\_mailbox\_maps.cf***

```
GNU nano 7.2 /etc/postfix/ad_virtual_mailbox_maps.cf  
server_host      = SRV1.vetele.mv  
server_port      = 389  
version          = 3  
bind             = yes  
start_tls        = no  
bind_dn          = smail  
bind_pw          =   
search_base      = ou=_vetele,dc=vetele,dc=mv  
scope            = sub  
query_filter     = (&(objectclass=person)(userPrincipalName=%s))  
result_attribute = userPrincipalName  
result_format    = %d/%u/Maildir/  
debuglevel       = 0
```

-Créer le fichier `/etc/postfix/ad_virtual_group_maps.cf`, puis le remplir de cette manière :

**`nano /etc/postfix/ad_virtual_group_maps.cf`**

```
GNU nano 7.2 /etc/postfix/ad_virtual_group_maps.cf *
server_host      = SRV1.vetele.mv
server_port      = 389
version          = 3
bind             = yes
start_tls        = no
bind_dn          = smail
bind_pw          = 
search_base      = ou=_vetele,dc=vetele,dc=mv
scope            = sub
query_filter     = (&(objectClass=group)(mail=%s))
special_result_attribute = member
leaf_result_attribute = mail
result_attribute = userPrincipalName
debuglevel       = 0
```

-Vérifions la requête LDAP avec l'AD dans Postfix. Interrogeons un compte AD déjà présent :

-Vérifions la connexions à l'expéditeur :

**`postmap -q fferland@vetele.mv ldap:/etc/postfix/ad_sender_login_maps.cf`**

```
root@srv-mail:~# postmap -q fferland@vetele.mv ldap:/etc/postfix/ad_sender_login_maps.cf
fferland@vetele.mv
```

## 7- Activation de l'intégration de l'AD dans Dovecot

Pour interroger l'AD, au lieu du serveur LDAP local, nous allons devoir modifier le fichier de configuration de Dovecot, situé ici : **`/etc/dovecot/dovecot-ldap.conf`** .

**`nano /etc/dovecot/dovecot-ldap.conf`**

Nous allons devoir le modifier comme ceci :

```
GNU nano 7.2 /etc/dovecot/dovecot-ldap.conf *
auth_bind      = yes
dn             = smail@vetele.mv
dnpass        = 
base          = ou=_vetele,dc=vetele,dc=mv
scope         = subtree
deref         = never

# Below two are required by command 'doveadm mailbox ...'
iterate_attrs  = userPrincipalName=user
iterate_filter = (&(userPrincipalName=*)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))

user_filter    = (&(userPrincipalName=%u)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
pass_filter    = (&(userPrincipalName=%u)(objectClass=person)(!(userAccountControl:1.2.840.113556.1.4.803:=2)))
pass_attrs     = userPassword=password
default_pass_scheme = CRYPT
user_attrs     = mail=master_user,mail=user,=home=/var/vmail/vmail1/%Ld/%Ln/,=mail=maildir:~/Maildir/
```

-Enfin, redémarrons le service Dovecot, pour qu'il puisse prendre en compte les modifications apportées :

***systemctl restart dovecot***

-Testons maintenant la connexion via telnet :

***telnet localhost 143***

***. login user@example.com password\_of\_user***

```
. login fferland@vetele.mv Passw0rd
. OK [CAPABILITY IMAP4rev1 SASL-IR LOGIN-REFERRALS ID ENABLE IDLE SORT SORT=DISPLAY THREAD=REFERENCES THREAD=REFS
THREAD=ORDEREDSUBJECT MULTIAPPEND URL-PARTIAL CATENATE UNSELECT CHILDREN NAMESPACE UIDPLUS LIST-EXTENDED I18NLEV
EL=1 CONDSTORE QRESYNC ESEARCH ESORT SEARCHRES WITHIN CONTEXT=SEARCH LIST-STATUS BINARY MOVE SNIPPET=FUZZY PREVIE
W=FUZZY PREVIEW STATUS=SIZE SAVEDATE LITERAL+ NOTIFY SPECIAL-USE QUOTA ACL RIGHTS=texk] Logged in
■
```

La connexion fonctionne

-Il ne nous reste plus qu'à activer l'intégration AD dans la messagerie Web Roundcube. Nous allons donc devoir modifier le fichier de configuration avec nos informations (utilisateurs « vmail », domaine, etc)

***/opt/www/roundcubemail/config/config.inc.php :***

***nano /opt/www/roundcubemail/config/config.inc.php***

```
// Global LDAP address book.
$config['ldap_public']['global_ldap_abook'] = array(
    'name'      => 'Global LDAP Address Book',
    'hosts'     => array("srv-dc1.algara.at"),
    'port'      => 389,
    'use_tls'   => false,
    'ldap_version' => '3',
    'network_timeout' => 10,
    'user_specific' => true,

    // Search mail users under same domain.
    'base_dn'   => 'ou=algara,dc=algara,dc=at',
    'bind_dn'   => 'vmail',
    'bind_pass' => 'THRO7daOqqAAhpmSfu6hcX9R0kNwaOWT',
    'writable'   => false,
    'search_fields' => array('mail', 'cn', 'sAMAccountName', 'displayName', 'sn', 'givenName'),

    // mapping of contact fields to directory attributes
    'fieldmap' => array(
        'name'      => 'cn',
        'displayname' => 'displayName',
        'surname'   => 'sn',
        'firstname' => 'givenName',
        'title'     => 'title',
        'email'     => 'mail:*',
        'phone:work' => 'telephoneNumber',
        'phone:mobile' => 'mobile',
        'phone:workfax' => 'facsimileTelephoneNumber',
        'street'    => 'street',
        'zipcode'   => 'postalCode',
        'locality'  => 'l',
        'department' => 'departmentNumber',
        'notes'     => 'description',
        'photo'     => 'jpegPhoto',
    ),

    'sort'      => 'cn',
    'scope'     => 'sub',
    'filter'    =>
        '(&((objectclass=person)(objectclass=group))(!(userAccountControl:1.2.840.113556.1.4.803:=2)))',
    'fuzzy_search' => true,
    'vlv'       => false, // Enable Virtual List View to more efficiently fetch paginated data (if server supports it)
    'sizelimit' => '0', // Enables you to limit the count of entries fetched. Setting this to 0 means no limit.
    'timelimit' => '0', // Sets the number of seconds how long is spend on the search. Setting this to 0 means no limit.
    'referrals'  => false, // Sets the LDAP_OPT_REFERRALS option. Mostly used in multi-domain Active Directory setups

    'group_filters' => array(
        'departments' => array(
            'name' => 'Mailing Lists',
            'scope' => 'sub',
            'base_dn' => 'domainName=%d,o=domains,dc=algara,dc=at',
            'filter' =>
                '(&((objectclass=mailList)(objectClass=mailAlias))(accountStatus=active)(enabledService=displayedInGlobalAddressBook))',
            'name_attr' => 'cn',
            'email' => 'mail',
        ),
    ),
);
$config['autocomplete_addressbooks'] = array('sql', 'global_ldap_abook');
```

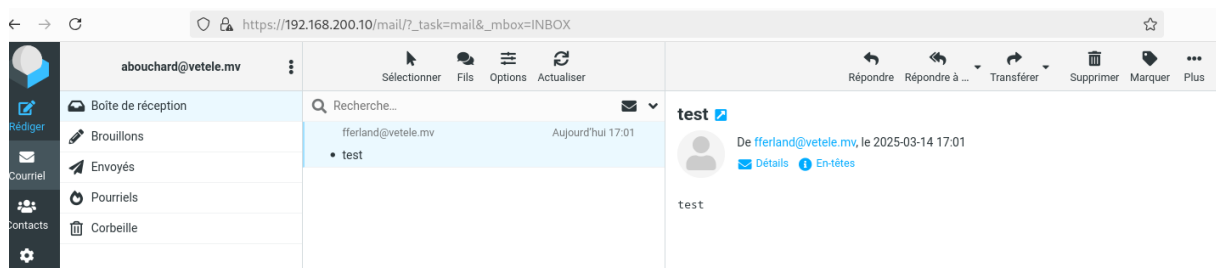


## 8-Tests de validation

-Nous allons maintenant tester la connexion via nos utilisateurs AD :



Puis envoyons un mail avec un utilisateurs, vers un deuxième :



Tout ceci fonctionne correctement.

Nous avons maintenant un serveur mail interne, fonctionnel.