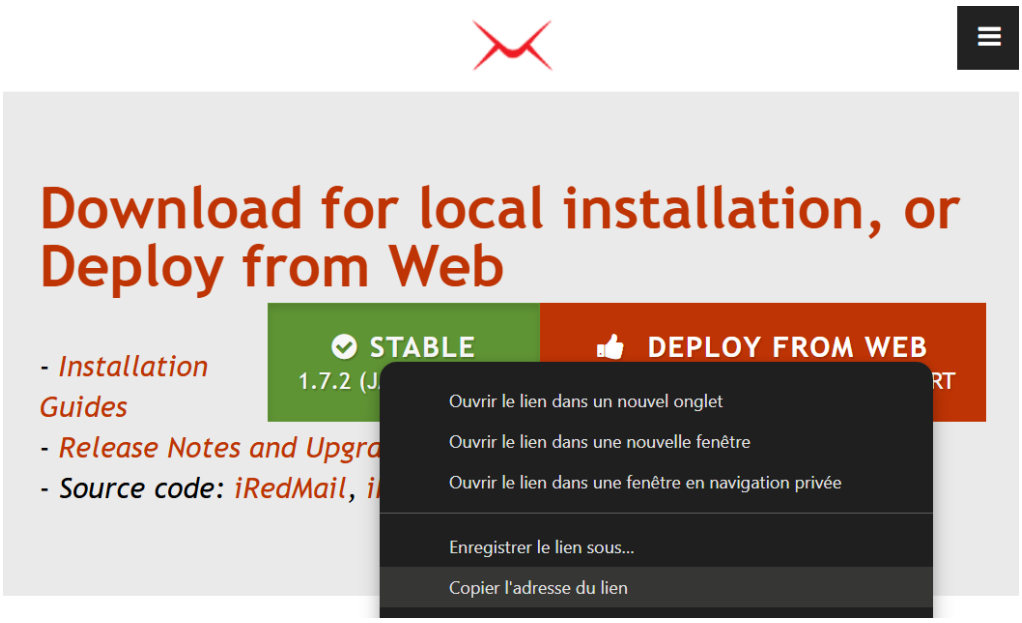
Table des matières :

Présentation de iRedMail

iRedMail offre une solution de messagerie mail complète, facile à installer et à administrer, avec un accent particulier sur la sécurité et la fiabilité. C'est un choix populaire pour les petites et moyennes entreprises ainsi que pour les utilisateurs individuels souhaitant déployer leur propre serveur de messagerie mail.

Téléchargement

Sur le site de iRedMail (https://www.iredmail.org/download.html), il faut copier le lien du dossier contenant les paquets nécessaires :



Ici nous sommes sur la version 1.7.2 de iRedMail, le lien est :

```
https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.2.tar.gz
```

Sur une machine Debian 12 avec au moins 4Go de mémoire installé, se connecter en root puis télécharger le dossier iRedMail grâce à la commande **wget** avec le lien précédemment copié :

```
wget https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.2.tar.gz
```

```
root@srv-mail:~# wget https://github.com/iredmail/iRedMail/archive/refs/tags/1.7.2.tar.gz
--2025-02-27 09:08:32--  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]
--2025-02-27 09:08:32--  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 : non indiqué [application/x-gzip]
Sauvegarde en : « 1.7.2.tar.gz »

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

2025-02-27 09:08:33 (1,71 MB/s) - « 1.7.2.tar.gz » sauvegardé [249156]

root@srv-mail:~# ls
1.7.2.tar.gz
```

Une fois l'opération terminée, décompresser le dossier 1.7.2.tar.gz

```
tar xzvf 1.7.2.tar.gz
```

```
root@srv-mail:~# tar xzvf 1.7.2.tar.gz
```

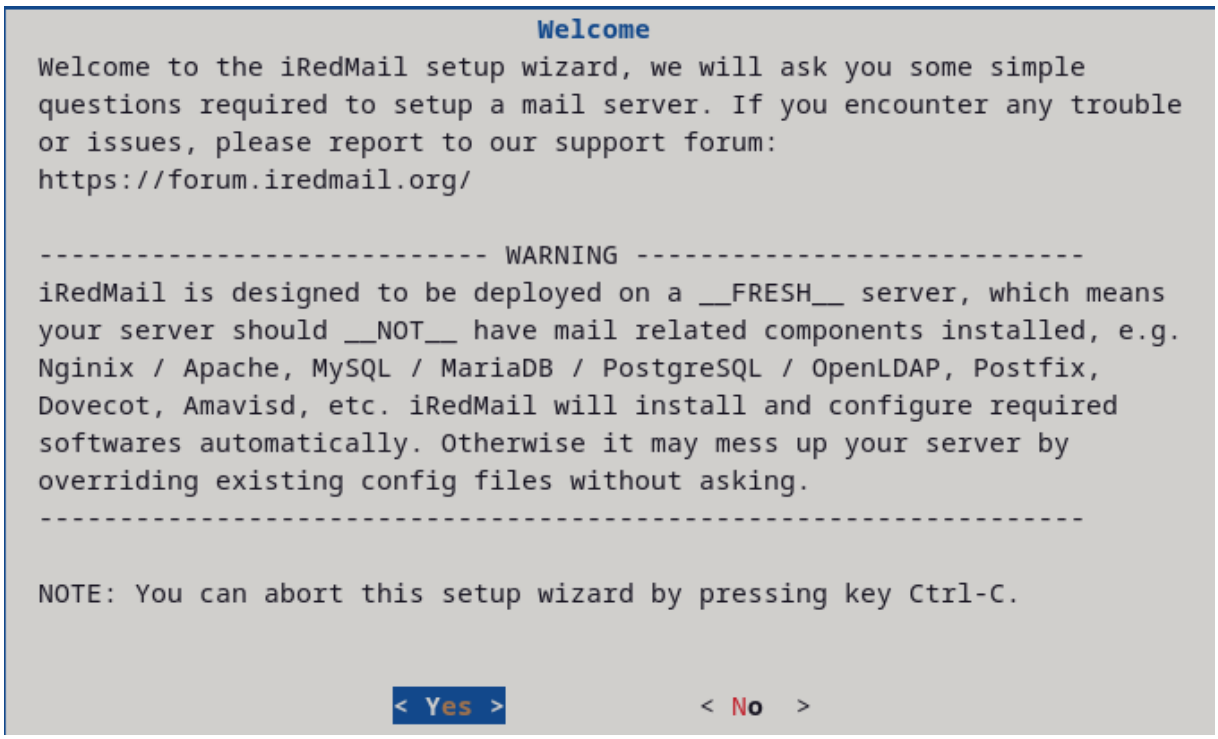
Maintenant déplaçons nous dans le dossier décompressé iRedMail-1.7.2 puis changeons les droits du script d'installation iRedMail.sh pour le rendre exécutable et lancer le script :

```
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
```

```
chmod u+x iRedMail.sh

./iRedMail.sh
```

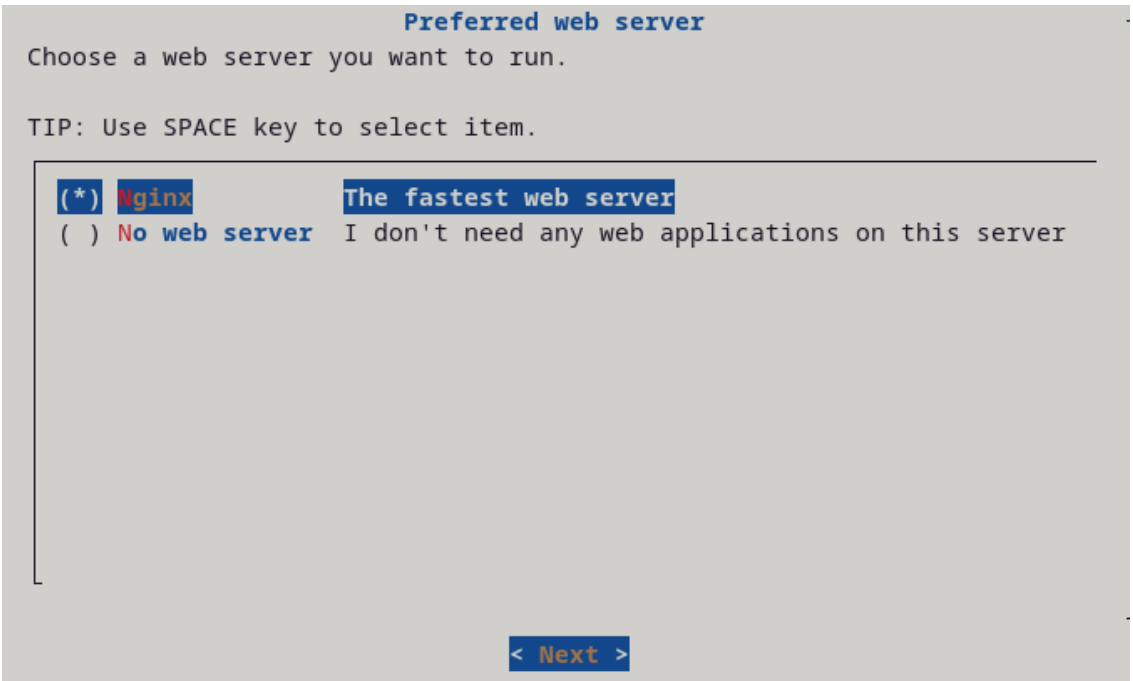
Installation

Une fois que le script a fini d'installer les premiers packages une fenêtre s'ouvre, sélectionner YES :

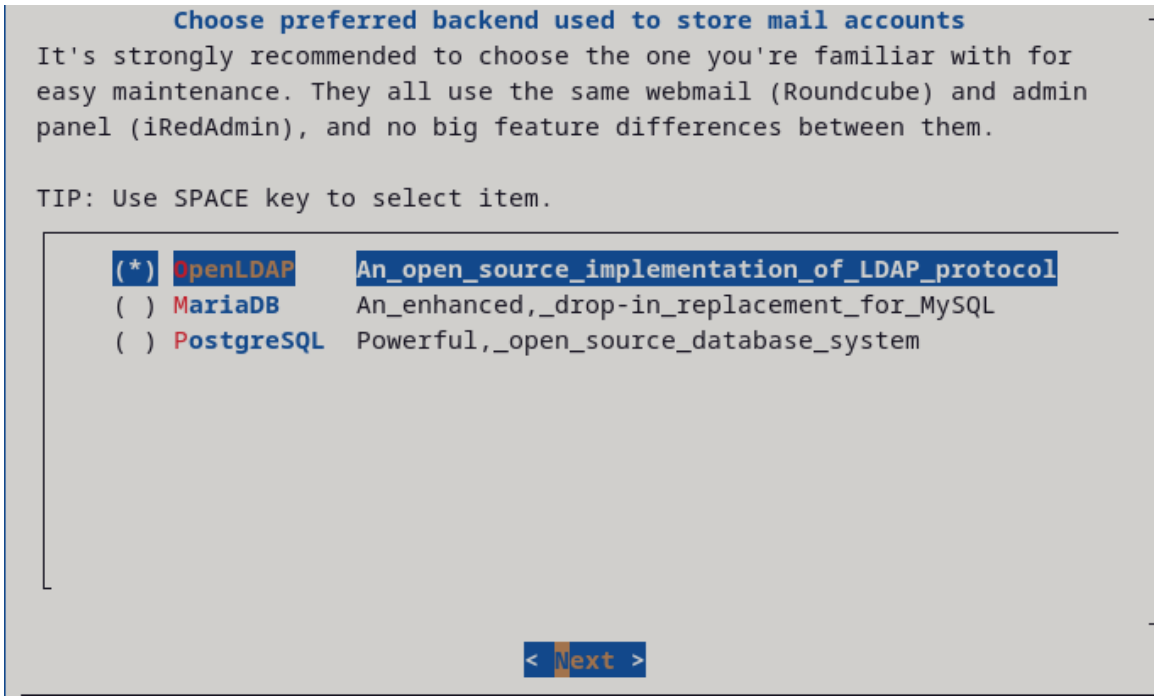


Ici il nous est demandé de sélectionner un dossier où seront stocké les boites mails, par défaut /var/vmail :

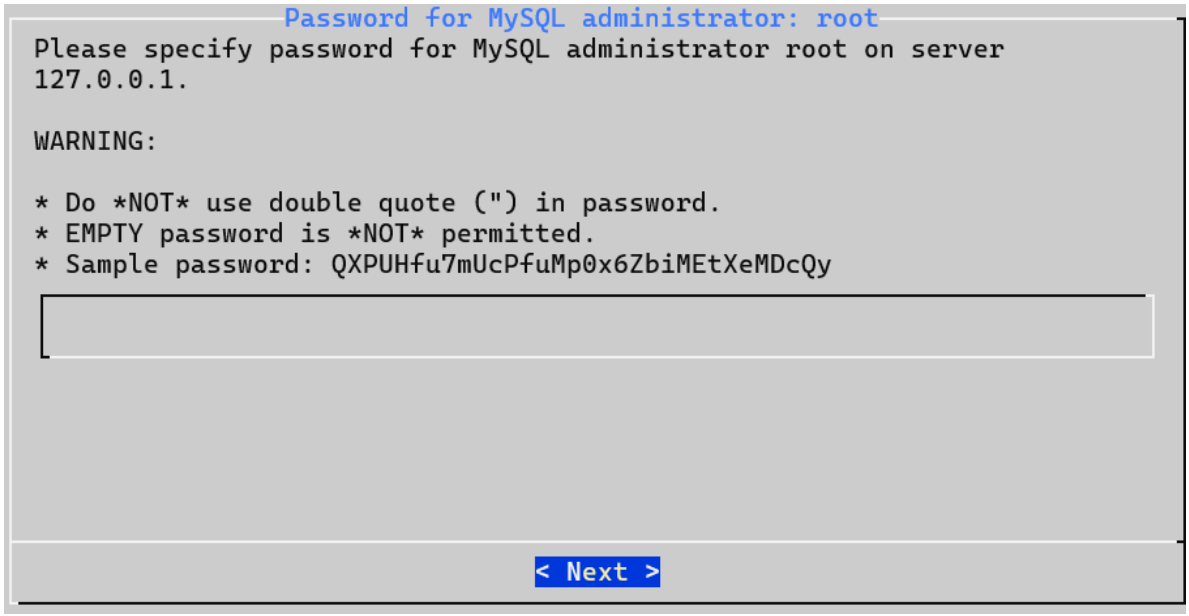
Ici sélectionner Nginx pour installer l'interface web :



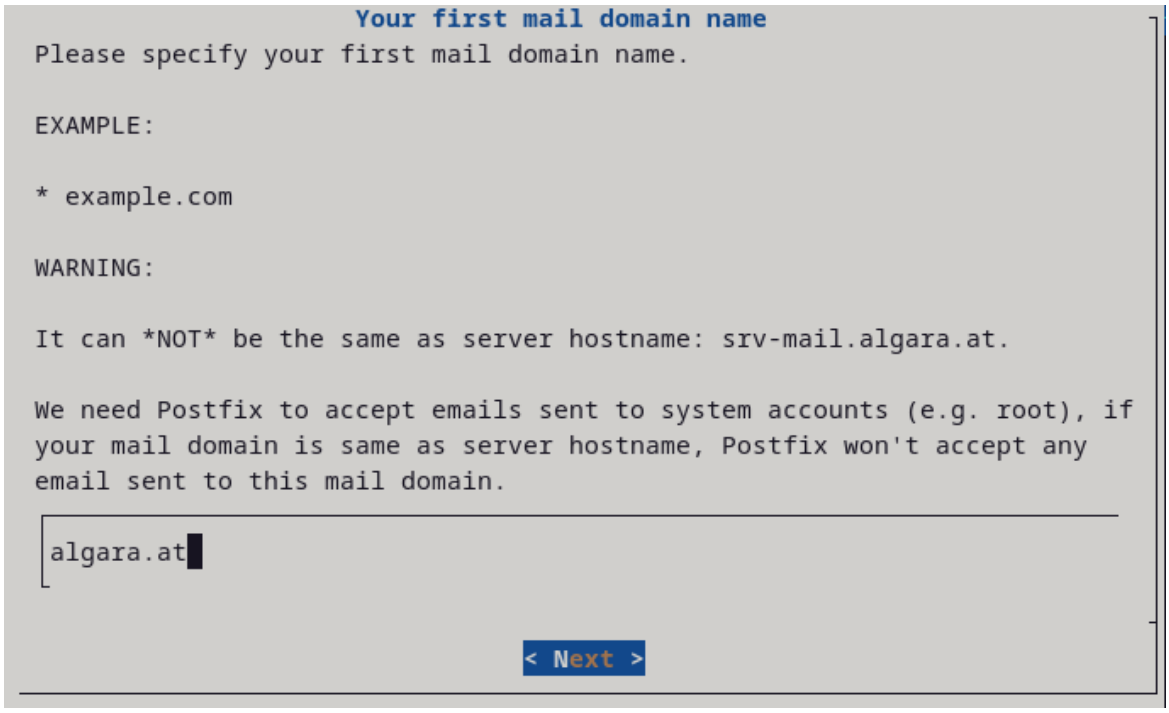
Sélectionner la base de donner de votre choix, ici nous utilisons OpenLDAP afin de récupérer les utilisateurs de notre Active directory, si nous sélectionnons MariaDB ou SQL, les utilisateurs devront être créés à la main :



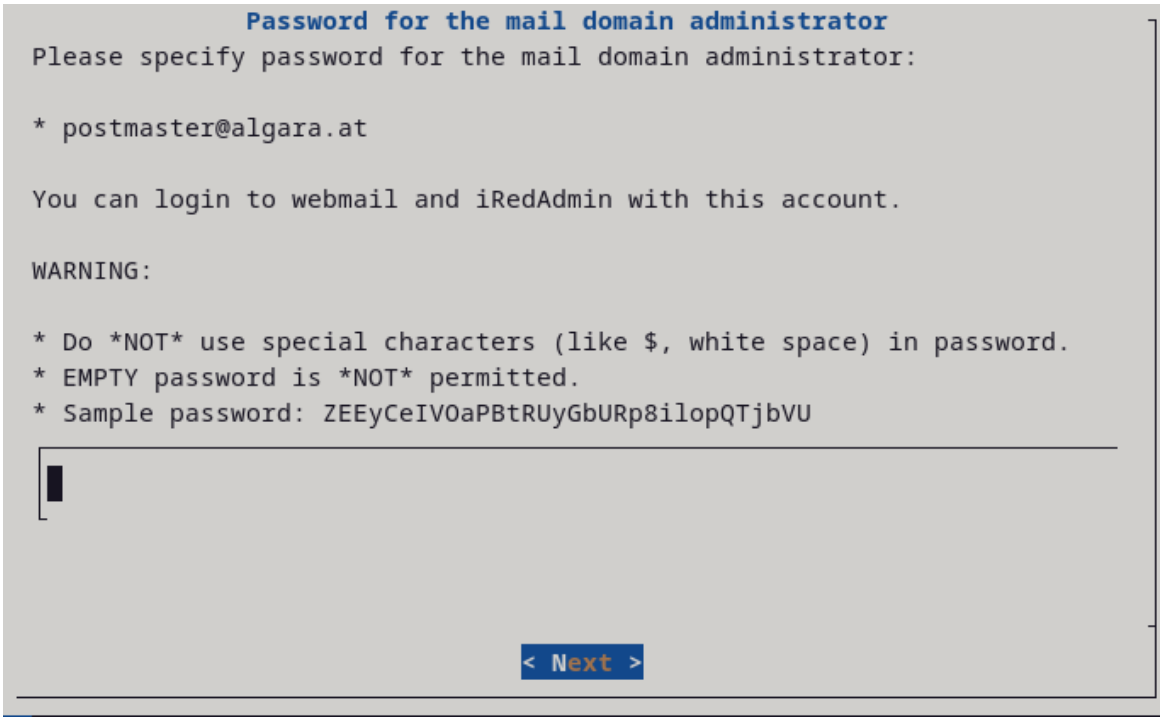
Renseigner un mot de passe pour l'administrateur de la base de données :



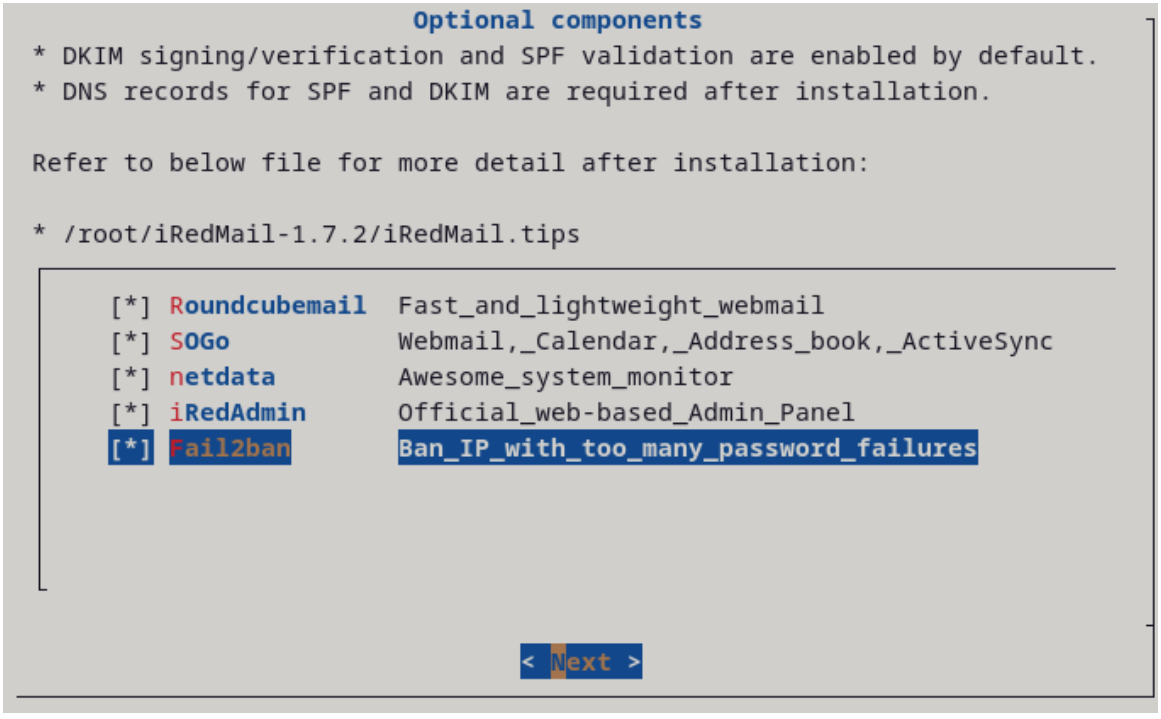
Renseigner le même domaine que l'AD :



Renseigner un mot de passe pour l'administrateur du serveur mail :



Sélectionner les composants suivants :



A la fin du script, répondre « y » aux deux dernières questions :

```
********************************************************************
* 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]y
[ INFO ] Copy firewall sample rules.
< Question > Restart firewall now (with ssh ports: 22)? [y|N]y
```

Une fois l'installation terminée, un récapitulatif du paramétrage s'affiche :

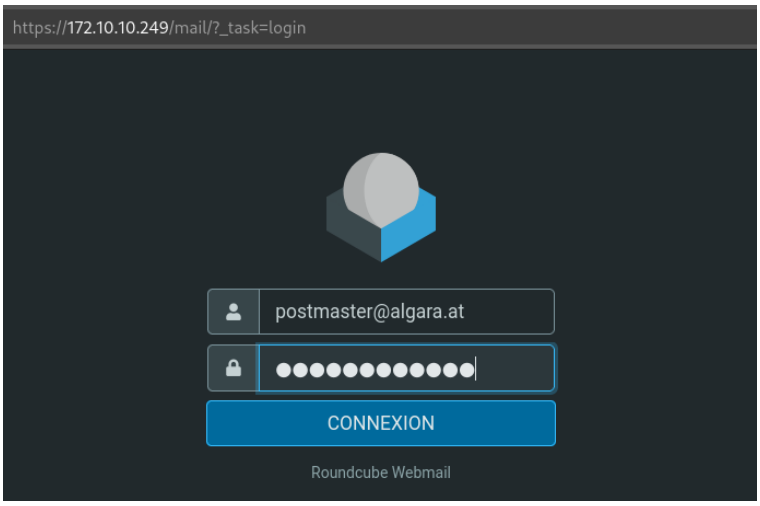
```
********************************************************************
* URLs of installed web applications:
*
* - Roundcube webmail: https://srv-mail.algara.at/mail/
* - SOGo groupware: https://srv-mail.algara.at/SOGo/
* - netdata (monitor): https://srv-mail.algara.at/netdata/
*
* - Web admin panel (iRedAdmin): https://srv-mail.algara.at/iredadmin/
*
* You can login to above links with below credential:
*
* - Username: postmaster@algara.at
* - Password: [redacted]
*
********************************************************************
* Congratulations, mail server setup completed successfully. Please
* read below file for more information:
*
*   - /root/iRedMail-1.7.2/iRedMail.tips
*
* And it's sent to your mail account postmaster@algara.at.
*
********************** WARNING ***********************************
*
* Please reboot your system to enable all mail services.
*
********************************************************************
```

Il faut impérativement redémarrer la machine :

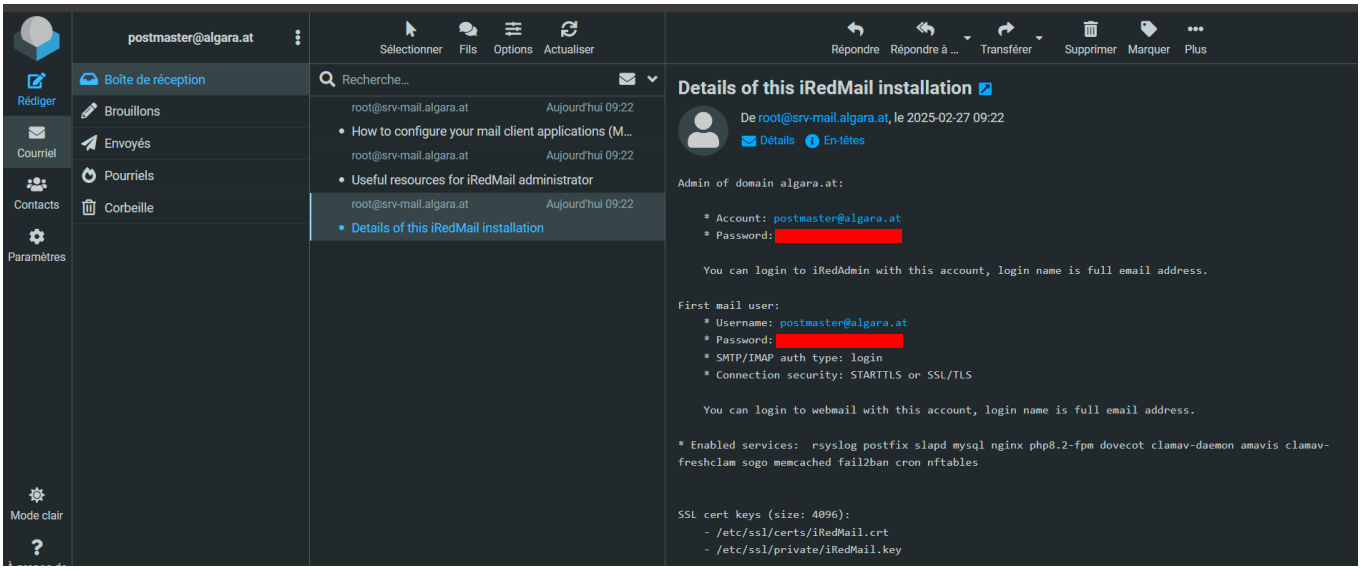
```
reboot
```

```
root@srv-mail:~/iRedMail-1.7.2# reboot
```

Nous pouvons tester sur un navigateur web à l'adresse IP du serveur avec l'adresse postmaster@algara.at configuré plus tôt :



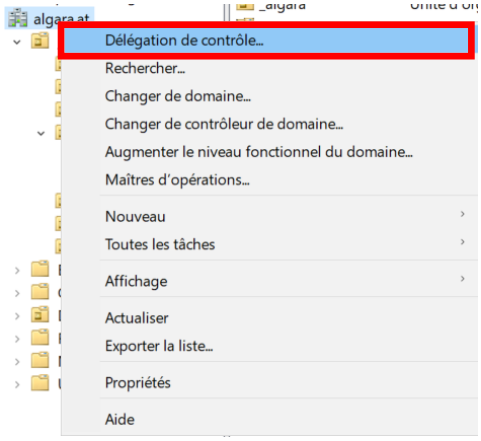
Dans la boite de postmaster, il a 3 messages vous indiquant des informations de votre serveur :

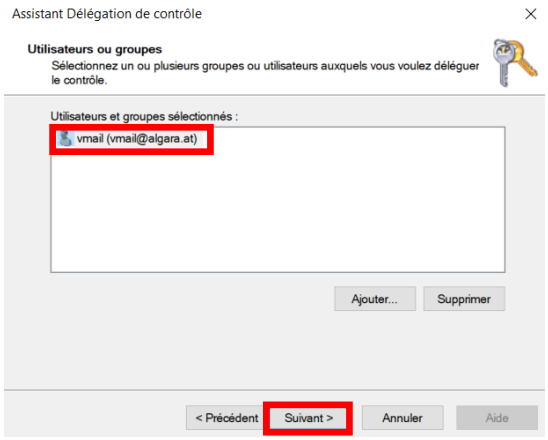


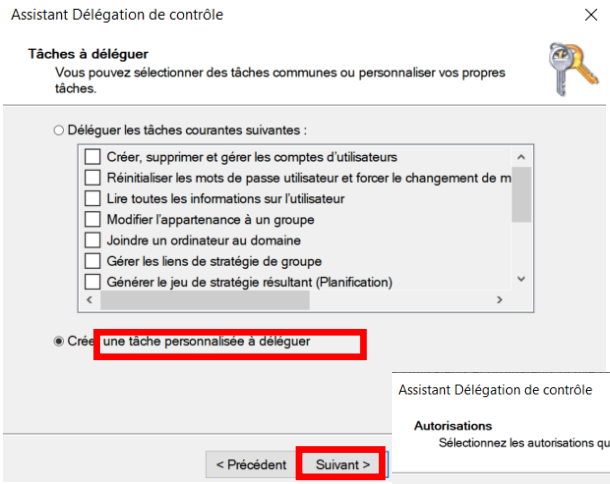
Création d'un utilisateur « spécial » LDAP :

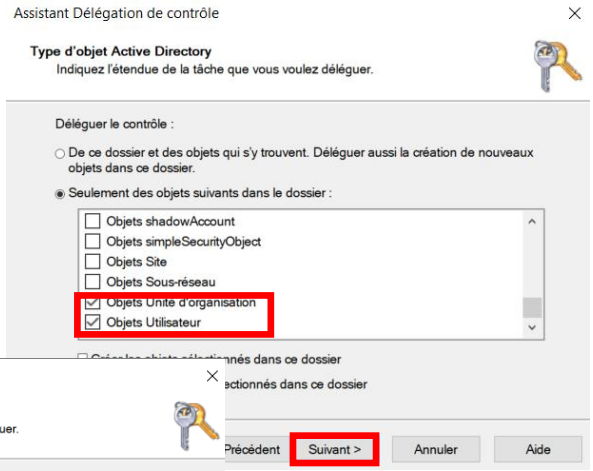
Sur notre serveur Active Directory, nous devons créer un utilisateur qui sera utilisé pour la transmission des informations de nos utilisateurs AD via le protocole LDAP, nous devons donc y appliquer des droits de Lecture Seule, ici notre utilisateur est vmail :

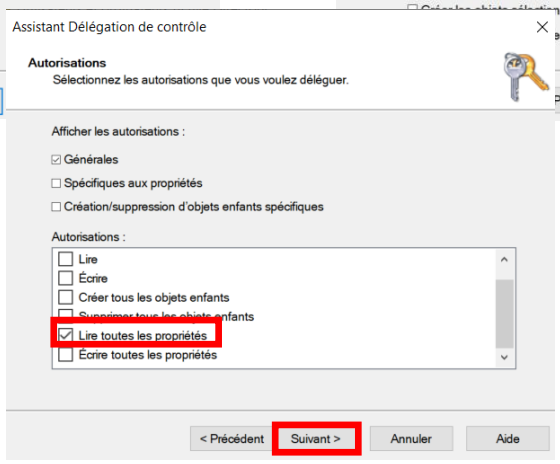
Nous devons donc créer une délégation de contrôle :











Configuration de OpenLDAP

Maintenant nous allons configurer OpenLDAP, avant tout il faut s'assurer que le recherche LDAP fonctionne correctement avec notre utilisateur vmail.

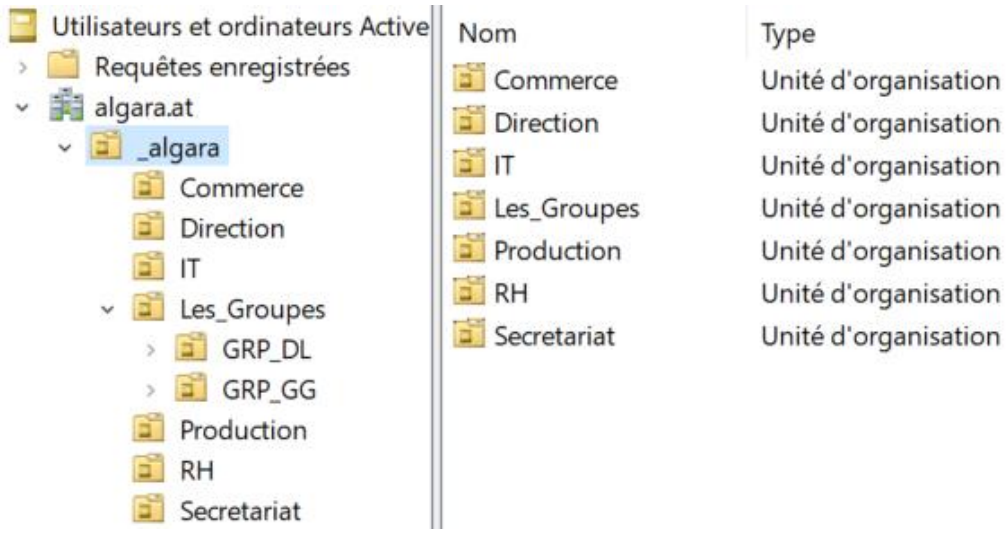
Pour cela testons avec la commande ldapsearch sur notre serveur mail :

```
ldapsearch -x -H ldap://srv-dc1.algara.at -D 'vmail' -W -b 'ou=_algara,dc=algara,dc=at'
```

Il faut renseigner le mot de passe de l'utilisateur utilisé pour LDAP :

```
root@srv-mail:/# ldapsearch -x -H ldap://srv-dc1.algara.at -D 'vmail' -W -b 'ou=_algara,dc=algara,dc=at'
Enter LDAP Password:
```

Ici j'utilise « ou=_algara » car mes utilisateurs sont dans cette OU « racine » :



La commande ldapsearch doit retourner les informations de nos utilisateurs :

```
# Franck Ferland, Direction, _algara, algara.at
dn: CN=Franck Ferland,OU=Direction,OU=_algara,DC=algara,DC=at
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Franck Ferland
sn: Ferland
description: Directeur2
givenName: Franck
distinguishedName: CN=Franck Ferland,OU=Direction,OU=_algara,DC=algara,DC=at
instanceType: 4
whenCreated: 20250222105423.0Z
whenChanged: 20250226131015.0Z
displayName: Franck Ferland
```

Activation de la requête LDAP dans Postfix

De retour sur notre serveur mail, pour activer la requête LDAP nous devons :

- Désactiver les paramètres spéciaux iRedMail inutilisés :

```
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=''
```

- Ajoutez notre nom de domaine de messagerie

```
postconf -e smtpd_sasl_local_domain='algara.at'
postconf -e virtual_mailbox_domains='algara.at'
```

- Modifier les paramètres des 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'
```

- Créer le fichier /etc/postfix/transport :

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

```
  GNU nano 7.2     /etc/postfix/transport *
algara.at 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 :

```
nano /etc/postfix/ad_sender_login_maps.cf
```

```
  GNU nano 7.2                                  /etc/postfix/ad_sender_login_maps.cf *
server_host     = srv-dc1.algara.at
server_port     = 389
version         = 3
bind            = yes
start_tls       = no
bind_dn         = vmail
bind_pw         = [redacted]
search_base     = ou=_algara,dc=algara,dc=at
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 :

```
nano /etc/postfix/ad_virtual_mailbox_maps.cf
```

```
  GNU nano 7.2                                  /etc/postfix/ad_virtual_mailbox_maps.cf *
server_host     = srv-dc1.algara.at
server_port     = 389
version         = 3
bind            = yes
start_tls       = no
bind_dn         = vmail
bind_pw         = [redacted]
search_base     = ou=_algara,dc=algara,dc=at
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 :

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

```
 GNU nano 7.2          /etc/postfix/ad_virtual_group_maps.cf
server_host     = srv-dc1.algara.at
server_port     = 389
version         = 3
bind            = yes
start_tls       = no
bind_dn         = vmail
bind_pw         = [redacted]
search_base     = ou=_algara,dc=algara,dc=at
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 AD dans Postfix, nous interrogeons un compte AD préalablement créé :

```
postmap -q fferland@algara.at ldap:/etc/postfix/ad_virtual_mailbox_maps.cf
```

```
root@srv-mail:~# postmap -q fferland@algara.at ldap:/etc/postfix/ad_virtual_mailbox_maps.cf
algara.at/fferland/Maildir/
```

Vérifions la connexion à l'expéditeur :

```
postmap -q fferland@algara.at ldap:/etc/postfix/ad_sender_login_maps.cf
```

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

Activation de l'intégration d'AD dans Dovecot :

Pour interroger AD au lieu du serveur LDAP local, nous devons modifier le fichier de configuration de Dovecot /etc/dovecot/dovecot-ldap.conf comme ci-dessous :

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

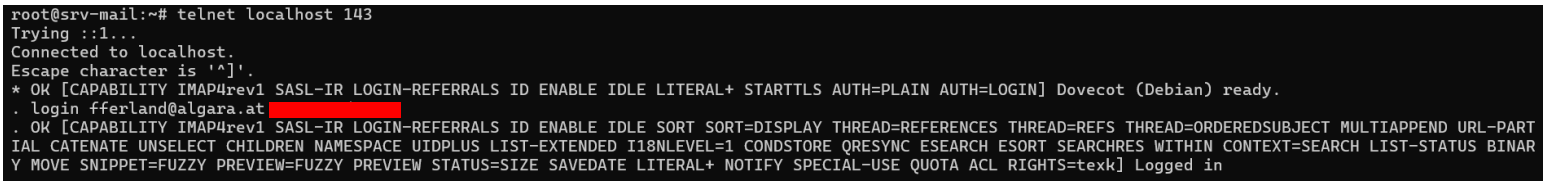
```
hosts        = srv-dc1.algara.at:389
ldap_version    = 3
auth_bind      = yes
dn           = vmail
dnpass        = passwd_of_vmail
base         = cn=users,dc=example,dc=com
scope         = subtree
deref         = never

# 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/
```

Puis redémarrer le service dovecot :

```
systemctl restart dovecot
```

Testons avec telnet :

```
telnet localhost 143
. login user@example.com password_of_user
```



La connexion fonctionne.

Il ne nous reste plus quà activer l'intégration AD dans la messagerie Web Roundcube, il faut donc modifier le fichier de configuration dans /opt/www/roundcubemail/config/config.inc.php :

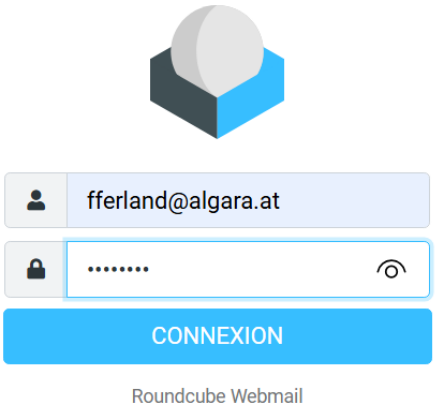
```
nano /opt/www/roundcubemail/config/config.inc.php
```

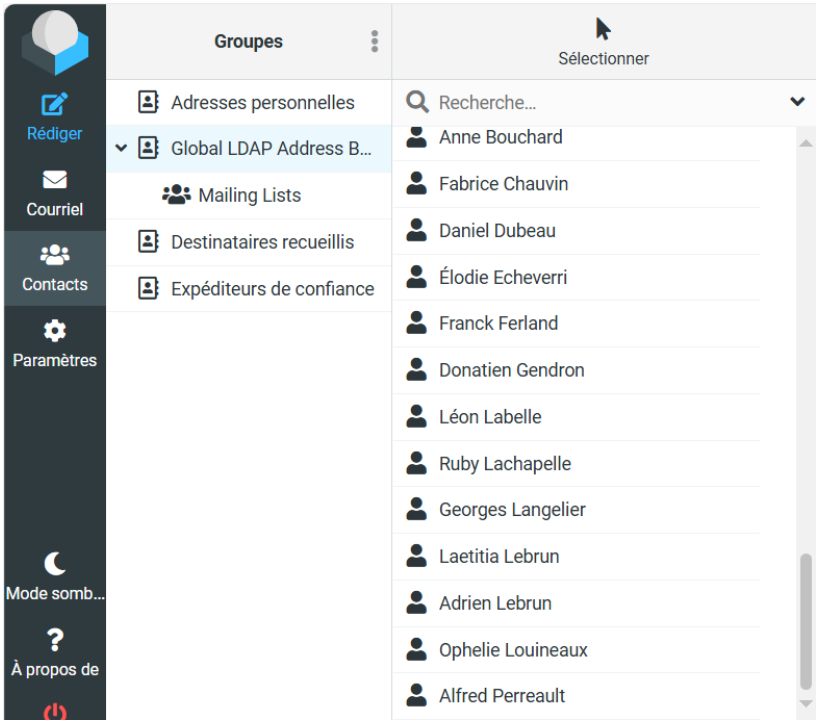
Voir la configuration du fichier page suivante.

```
// 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=displayedInGl
obalAddressBook))',
      'name_attr' => 'cn',
      'email'    => 'mail',
    ),
  ),
);
$config['autocomplete_addressbooks'] = array('sql', 'global_ldap_abook');
```

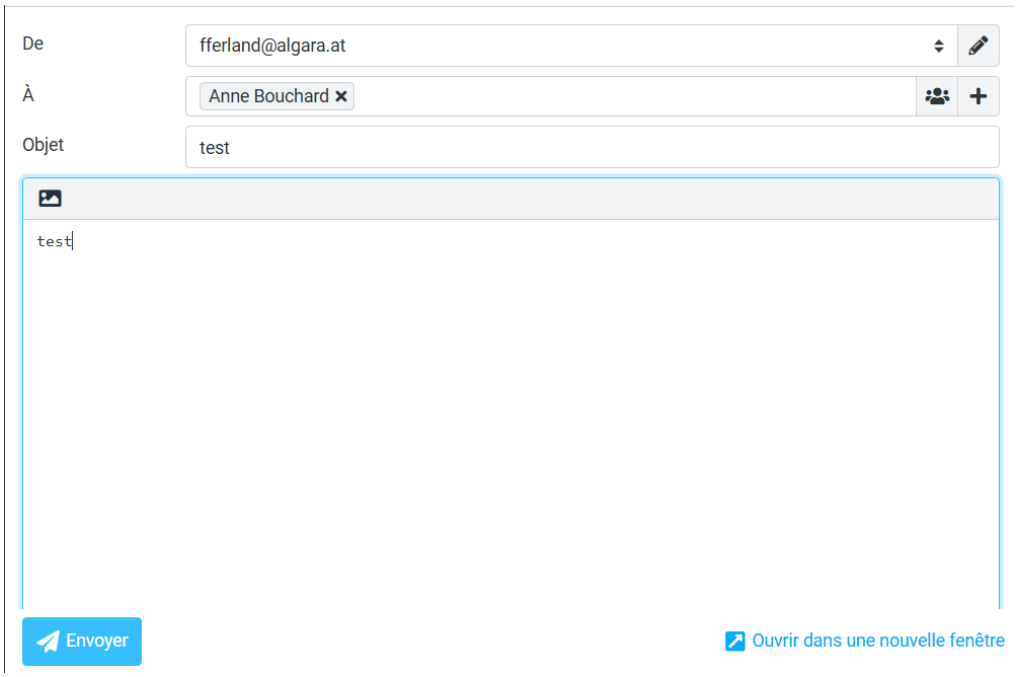
Une fois la configuration terminée, redémarrer le serveur mail puis testons sur un client. Les utilisateurs peuvent donc s'authentifié avec leurs identifiants de leur session windows :

Nous pouvons observer que tous les utilisateurs ont bien été importé dans Rouncube :





Envoyons un mail de test à un autre utilisateur :



Le mail a bien été reçu :