Tutorial installation intimail™

Table des matières

Après une nouvelle installation de l'OS

Exécutez ces commandes pour mettre à jour à la dernière version. Ces opérations peuvent prendre un certain temps. Nous avons utilisé pour cet exemple Raspbian Jessie Lite sur une Raspberry Pi 2.

```
apt-get update
apt-get upgrade && apt-get dist-upgrade
apt-get install linux-headers-$(uname -r)
reboot
```

Puis lancer :

```
raspi-config
```

Etendre au maximum l'espace de stockage en navigant dans les menus :

```
Expand Filesystem
```

Régler une ip statique avec la box, fichier `/etc/network/interfaces` :

```
iface eth0 inet static
    address 192.168.1.31
    netmask 255.255.255.0
    gateway 192.168.1.1
```

Nous avons aussi supprimé wpasupplicant.

Sécurisation du serveur

Changement de l'utilisateur par défaut

Changez le nom d'utilisateur par défaut ainsi que son mot de passe.

```
sudo passwd root
```

Sortie et login en tant que root, puis :

```
usermod -l myuname pi
usermod -m -d /home/myuname myuname
groupmod -n myuname pi
passwd myuname
```

Voir cette adresse pour l'utilisation de clés privées/publiques.

Changement du port SSH

```
sed -i 's/Port 22/Port 2222/g' /etc/ssh/sshd_config
```

Interdire l'authentification SSH pour root

```
sed -i 's/PermitRootLogin yes/PermitRootLogin no/g' /etc/ssh/sshd_config
```

Installation de LDAP

Configuration de base

Installation du package :

```
apt-get install slapd
```

Choisir un mot de passe administrateur, puis lancer la commande :

```
dpkg-reconfigure slapd
```

Répondre non à la question 1.
Entrez le nom de domaine utilisé à la question 2, sous la forme : domaine.tld.
Entrez ce que vous voulez au 3ème écran, le nom de l'organisation ne sera pas utilisé.
Entrez un mot de passe.
Choisissez HDB.
Choisissez si la base de données est supprimée à la désinstallation de slapd.
Déplacez l'ancienne base de données.
N'utilisez pas LDAPv2.

Installer les outils de conversion pour ldap (slaptest, ldapmodify notamment) :

```
apt-get install ldap-utils
```

On peut maintenant vérifier que la configuration est valable :

```
ldapsearch -x -h localhost -b "dc=domaine,dc=tld" -LLL "dc=domaine" dn
```

Cette commande doit retourner quelque chose comme :

```
dn: dc=domaine,dc=tld
```

Il faut maintenant sécuriser le serveur LDAP, en effet on peut y accéder en anonyme avec la commande :

```
ldapsearch -Y EXTERNAL -H ldapi:// -b cn=config
"(&(objectClass=olcDatabaseConfig)(olcSuffix=dc=domaine,dc=tld))"
```

Cette commande retourne un certain nombre d'informations, notamment à propos des champs suivants :

```
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by
anonymous auth by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by * read
```

On va modifier ces champs avec la commande ldapmodify. Pour cela on va créer un fichier ldif :

```
cat > changeAccess.ldif << EOF
dn: olcDatabase={1}hdb,cn=config
changetype: modify
delete: olcAccess
-
add: olcAccess
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by
anonymous auth by dn="cn=admin,dc=domaine,dc=tld" write by * none
-
add: olcAccess
olcAccess: {1}to dn.base="" by * read
-
```

```
add: olcAccess
olcAccess: {2}to * by self write by dn="cn=admin,dc=domaine,dc=tld" write by
* none
-
EOF
```

On peut maintenant appliquer les changements avec ldapmodify :

```
ldapmodify –c –Y EXTERNAL –H ldapi:/// -f changeAccess.ldif
```

La commande devrait vous confirmer que la modification s'est bien effectuée :

```
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={1}hdb,cn=config"
```

On peut vérifier qu'on ne peut plus accéder aux informations avec la commande :

```
ldapsearch -x -c -h localhost -b dc=domaine,dc=tld
```

On peut vérifier la configuration en se connectant en tant qu'administrateur :

```
ldapsearch -c -h localhost -b dc=domaine,dc=tld -D
"cn=admin,dc=domaine,dc=tld" –W
```

Configuration des Schémas

Nous allons utiliser les schémas de courier-ldap. Pour éviter une manipulation compliquée, vous trouverez directement le schéma avec le fichier authldap.schema. On place ce fichier dans le dossier :

```
mv authldap.schema /etc/ldap/schema
```

Nous créons un fichier qui incluera tous les schémas de base en plus du nouveau. On peut les afficher avec la commande :

```
ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=schema,cn=config" -LLL
"(objectClass=*)" cn
```

Création du fichier de configuration, pour notre exemple cela donne :

```
mkdir /tmp/ldapconf
cat > /tmp/ldapconf/ldap.conf << EOF
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/authldap.schema
EOF
```

On lance ensuite la commande :

```
slaptest -f /tmp/ldapconf/ldap.conf -F /tmp/ldapconf
```

Elle revoie un message de succès. Cette commande a créé dans le répertoire /tmp/ldapconf une arborescence correspondant à la configuration de notre LDAP.

On modifie le chemin de configuration :

```
sed -i '0,/dn:.*authldap/ s/authldap/authldap,cn=schema,cn=config/'
cn\=\{*\}authldap.ldif
```

On supprime ensuite les 7 dernières lignes du fichier :

```
head -n -7 cn\=\{*\}authldap.ldif > tmp.ldif
mv tmp.ldif cn\=\{*\}authldap.ldif
```

On peut maintenant importer notre fichier de configuration. Pour ce faire :

```
ldapadd -Y EXTERNAL -H ldapi:/// -f
/tmp/ldapconf/cn=config/cn=schema/cn={*}authldap.ldif
```

Si tout va bien, l'entrée devrait avoir été ajoutée. On peut vérifier avec la commande vue tout à l'heure :

```
ldapsearch -Y EXTERNAL -H ldapi:/// -b "cn=schema,cn=config" -LLL
"(objectClass=*)" cn
```

On devrait voir en plus le nouveau schéma authldap.

Constitution de la base de données LDAP

Le remplissage de la base se fait à l'aide de fichiers ldif. Nous donnons ici un exemple de structure.

Fichier pour la structure de base :

```
dn: dc=mail,dc=domaine,dc=tld
o: intimail.pw
description: Global mail tree
dc: mail
objectClass: top
objectClass: dcObject
objectClass: organization

dn: dc=people,dc=mail,dc=domaine,dc=tld
description: Informations of all users
o: people
dc: people
objectClass: top
objectClass: dcObject
objectClass: organization

dn: dc=groups,dc=mail,dc=domaine,dc=tld
description: All groups of users
o: groups
dc: groups
objectClass: top
objectClass: dcObject
objectClass: organization
```

Fichier pour ajouter un utilisateur :

```
dn: cn=jbond,dc=people,dc=mail,dc=domaine,dc=tld
uid: jbond
mail: jbond@domaine.tld
sn: Moulin
givenName: James
displayName: James Bond
mailbox: domaine.tld/jbond/
quota: 50M
homeDirectory: /home/vmail/
objectClass: top
objectClass: inetOrgPerson
objectClass: CourierMailAccount
userPassword: {SSHA}367PSXiU//Aegy8dpJbPU8OepEf8L5ye
```

Pour obtenir un hash du mot de passe :

```
slappasswd -s password -h {SSHA}
```

On peut par la suite ajouter la configuration à la base de données avec la commande :

```
ldapadd -D "cn=admin,dc=domaine,dc=tld" -W -h localhost -f path/to/file
```

Si les champs proposés ne sont pas suffisants, il faudra alors effectuer les modifications dans le fichier autldap.schema proposé plus haut, et refaire la manipulation de configuration.

De plus, les standards du Mail décrit par l'IETF (RFC822 6.3, RFC1123 5.2.7 and RFC2821 4.5.1) impliquent d'avoir une adresse Postmaster et une Abuse. Pour cela, nous pourrions créer ces adresses avec la méthode vue au-dessus, mais ce n'est pas la meilleure. Il est préférable d'utiliser un alias, comme nous le ferons avec les listes de diffusion. Ici, nous proposons de rediriger ces deux adresses vers une adresse administrateur. Pour cela, la méthode est la même, sauf que le fichier ldif n'est pas tout à fait identique. En voici un exemple :

```
dn: cn=postmaster,dc=groups,dc=mail,dc=domaine,dc=tld
uid: postmaster
mail: postmaster@domaine.tld
sn: Postmaster
displayName: Postmaster
maildrop: admin@domaine.tld
objectClass: top
objectClass: inetOrgPerson
objectClass: CourierMailAlias
```

Pour faire une liste de diffusion, la méthode est la même. Il suffit d'ajouter toutes les adresses destinataires dans le champ maildrop, séparées par des virgules (,).

Installation de Postfix

Installation des packages :

```
apt-get install postfix postfix-ldap
```

Lors de l'installation, deux écrans défilent :

- Configuration Internet Site
- Valeur par défaut pour le mail name

On crée l'utilisateur qui servira à exécuter Postfix :

```
groupadd vmail
useradd -g vmail -d /home/vmail -s /bin/false -m vmail
```

Nous aurons besoin dans la suite des GID et UID créés à cet instant. Ils peuvent être affichés avec les commandes :

```
cat /etc/group | grep vmail | cut -d: -f3
cat /etc/passwd | grep vmail | cut -d: -f3
```

On ajoute les paramètres au fichier /etc/postfix/main.cf (remplacer les valeurs de GID et d'UID avec vos valeurs) :

```
smtpd_banner = mail.domaine.tld
virtual_mailbox_base = /home/vmail
virtual_mailbox_domains = dmaine.tld
virtual_mailbox_maps = ldap:/etc/postfix/ldap_accounts.cf
virtual_alias_maps = ldap:/etc/postfix/ldap_aliases.cf
virtual_minimum_uid = 100
virtual_gid_maps = static:1001 # Remplacez ici par votre valeur de GID
virtual_uid_maps = static:1001 # Remplacez ici par votre valeur d'UID
```

Il nous faut maintenant constituer nos fichiers de configuration, ldap_accounts.cf :

```
cat > /etc/postfix/ldap_accounts.cf << EOF
server_host = localhost
server_port = 389
search_base = dc=people,dc=mail,dc=domaine,dc=tld
query_filter = (&(objectClass=CourierMailAccount)(mail=%s))
result_attribute = mailbox
bind = yes
bind_dn = cn=admin,dc=domaine,dc=tld
bind_pw = <mdp_en_clair>
version = 3
EOF
```

Et pour ldap_aliases.cf :

```
cat > ldap_aliases.cf << EOF
server_host = localhost
server_port = 389
search_base = dc=groups,dc=mail,dc=domaine,dc=tld
query_filter = (&(objectClass=CourierMailAlias)(mail=%s))
result_attribute = maildrop
bind = yes
bind_dn = cn=admin,dc=domaine,dc=tld
bind_pw = <mdp_en_clair>
version = 3
EOF
```

On peut maintenant vérifier la configuration de Postfix avec (cette commande ne doit rien retourner si c'est bon) :

```
postfix check
```

Si c'est bon, alors on recharge le serveur :

```
postfix reload
```

On peut alors faire un envoi de mail test via telnet :

```
telnet localhost 25
```

Si vous souhaitez délivrer les mails à votre manière, il faut dans le fichier /etc/postfix/main.cf la ligne :

```
virtual_transport = nomdevotreregle
```

Et de même, dans le fichier /etc/postfix/master.cf :

```
nomdevotreregle    unix  -       n       n       -       5       pipe
  flags=Rq user=vmail null_sender=
  argv=/chemin/de/votre/programme
```

Il nous reste maintenant à configurer les différents enregistrements DNS nécessaire au fonctionnement d'un serveur mail. Vous pouvez utiliser la solution de votre choix. Dans la suite vous trouverez une méthode utilisant Bind9.

Installation de Bind9

Dans toute cette partie, on se situera dans le dossier /etc/bind/. Dans la suite, notre IP sera a.b.c.d.

Dans le fichier named.conf.options, on ajoutera dans le champ options :

```
version "Not supported";
```

Dans un dossier zones, on écrit le fichier db.domaine.tld :

```
$TTL    604800

@       IN      SOA     ns.domaine.tld. root.domaine.tld. (
                    2015122111          ; Serial
                         43200          ; Refresh
                          3600          ; Retry
                       2419200          ; Expire
                         86400 )        ; Negative Cache TTL

@       IN      NS      ns.domaine.tld.
@       IN      NS      ns11.ovh.net.
ns      IN      A       a.b.c.d
www     IN      A       a.b.c.d
@       IN      A       a.b.c.d

@       IN      MX      10 mail.domaine.tld.
mail    IN      A       a.b.c.d
```

Dans le même dossier zones, on a c.b.a.in-addr.arpa :

```
$TTL    604800

@       IN      SOA     ns.domaine.tld. root.domaine.tld.     (
       2015122101       ;serial
       14400            ;refresh
       3600             ;retry
       604800           ;expire
       10800            ;minimum
)

c.b.a.in-addr.arpa.          IN      NS      ns.domaine.tld.
c.b.a.in-addr.arpa.          IN      NS      ns11.ovh.net.

d                             IN      PTR     mail.domaine.tld.
```

Il faut faire attention à bien incrémenter le serial pour chaque modification des fichiers.

Dans le fichier named.conf.local :

```
zone "domaine.tld" {
       type master;
       file "/etc/bind/zones/db.domaine.tld";
       allow-transfer { 213.251.128.130; };
       notify yes;
};

zone "c.b.a.in-addr.arpa" IN {
       type master;
       file "/etc/bind/zones/c.b.a.in-addr.arpa";
       allow-transfer { 213.251.128.130; };
};
```

Ici, 213.251.128.130 est l'adresse IP du serveur ns11.ovh.net.

Il faut bien sûr configurer le DNS avec votre fournisseur (Gandi, OVH, …). Pour ça, amusez-vous bien. Vous pouvez aussi tester votre configuration avec des outils en ligne tels que DNSstuff.

En test final, si votre configuration est bonne, vous devriez pouvoir envoyer un mail depuis un service neutre (Gmail, yahoo, …) et le voir dans votre arborescence (ici /home/vmail/domaine.tld/).

Dépendances

Slapd

Ldap-utils

Postfix

Postfix-ldap

Bind9

Sources

https://wiki.gandi.net/fr/hosting/using-linux/tutorials/debian/mail-server-ldap

http://www.postfix.org/pipe.8.html

http://www.postfix.org/FILTER_README.html

http://www.postfix.org/

http://www.postfix.org/transport.5.html