Maquette

Albert.dupond@xxxx.yyy.fr

MailHub

Doit à la réception d'un mail pour un utilisateur du campus l'envoyer sur le serveur hébergeant la boite aux lettre de l'utilisateur – Fait via postfix avec requête dans un annuaire ldap

MailStore A (postfix/dovecot/ ldap/comptes virtuels)

MailStore B (courrier/postfix)

Anciens serveurs de messageries des différents laboratoires
Nouveau serveurs avec comptes virtuels

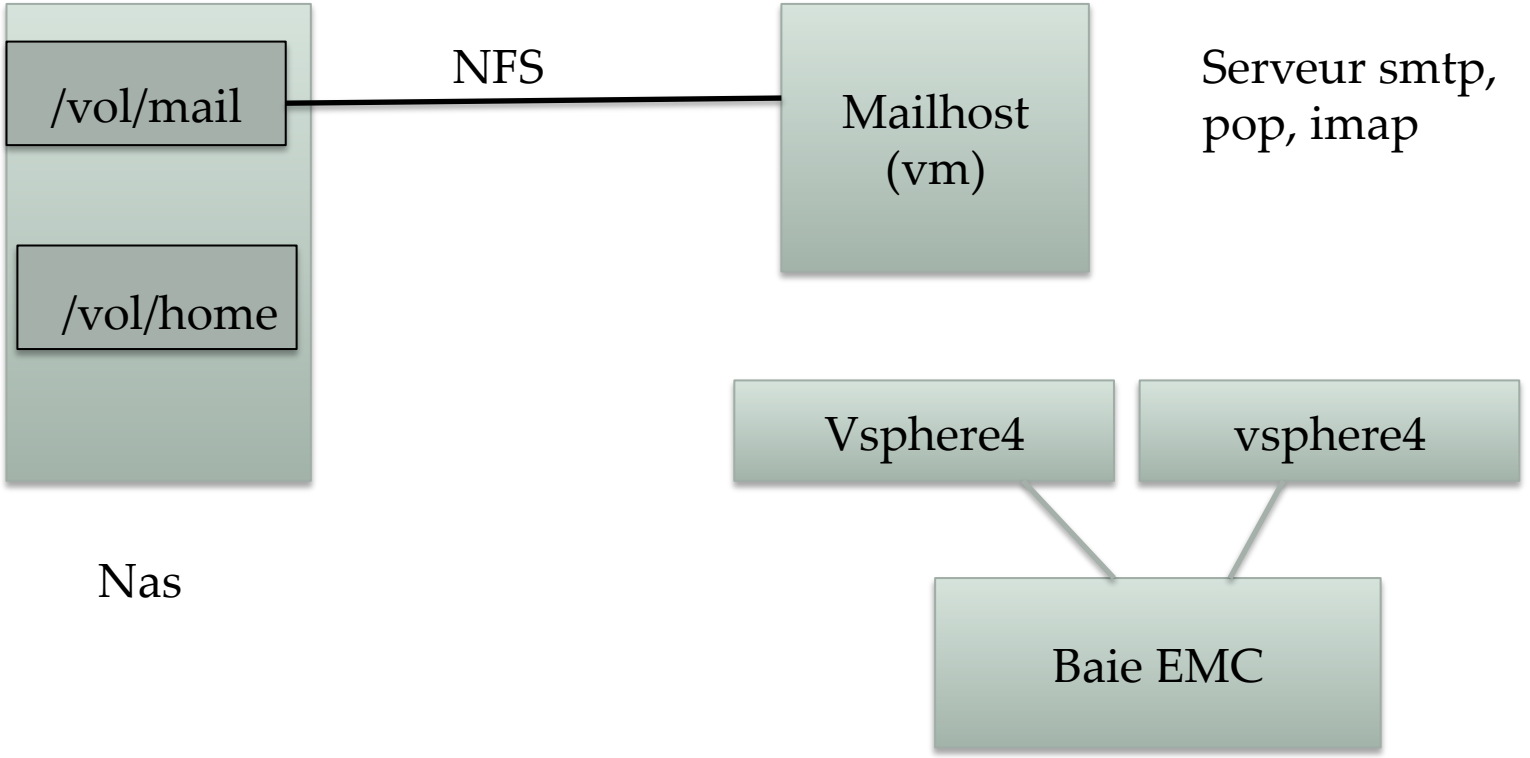
L'existant

- Un serveur de messagerie avec courrier / postfix
- Les boites mail au format Maildir
- Les boites Mail stockées les homedir des utilisateurs, montés en NFS sur le serveur de mail
- Authentification ldap, utilisateurs « systèmes »

Mise en place

- Finalement un seul serveur qui gère l'envoie et la réception des courriers électronique pour l'ICSN
- Migration transparente pour les utilisateurs
- Choix de postfix / Dovecot / comptes virtuels stockés dans ldap

Architecture



Mailhost

- Réplica LDAP (openldap)
- Cache DNS
- Postfix
- Dovecot
- Mailscanner

Schéma ldap

- dn: uid=albertd,ou=People,dc=xxxx,dc=yyy,dc=fr
- objectClass: top
- objectClass: inetOrgPerson
- objectClass: icsnAccount
- objectClass: inetLocalMailRecipient
- Uid: albertd
- uidNumber: 1365
- gidNumber: 1000
- homeDirectory: /home/chem/albertd
- gecos: Albert Dupont,27/207,4004,50
- cn: Albert Dupont
- displayName: Albert Dupont
- givenName: Albert
- sn: Dupont
- mail: Albert.Dupont@xxxx.yyy.fr
- mailLocalAddress: Albert.Dupont
- loginShell: /bin/bash
- userPassword:: epMMSWVBUfWiLopMMbbRXBrYURKVWc=
- **icsnMailPath: /Mail/albertd** }
- **icsnMailHost: agni** }

Champs rajoutés

Postfix sur Mailhost

#myorigin = /etc/mailname (doit être commentédans une config avec des comptes virtuels)

myhostname = mail.xxxx.yyy.fr

alias_maps = hash:/etc/aliases

alias_database = hash:/etc/aliases

mydestination = mail.xxxx.yyy.fr, localhost.xxxx.yyy.fr, localhost

relayhost = [smtp.yyy.fr]

fallback_relay = [smtp-1.yyy.fr]

mynetworks = 127.0.0.0/8, 192.168.1.0/24, 192.168.2.0/23, 192.168.3.0/24

message_size_limit = 20240000

mailbox_transport = dovecot

mailbox_size_limit = 0

recipient_delimiter = +

inet_interfaces = all

header_checks = regexp:/etc/postfix/header_checks (pour Mailscanner)

la réception d'un mail en provenance d'un expéditeur unique avec plusieurs destinataire ne fonctionnerais pas sans cette option

dovecot_destination_recipient_limit = 1

Postfix sur Mailhost – comptes virtuels

virtual_uid_maps = static:3000

virtual_gid_maps = static:3000

virtual_mailbox_base = /Mail

virtual_transport = dovecot

virtual_mailbox_domains = xxxx.yyy..fr

virtual_mailbox_maps = ldap:/etc/postfix/ldap_virtual_mailbox_maps.cf

virtual_alias_maps = proxy:ldap:/etc/postfix/ldap_virtual_alias_maps.cf,proxy:ldap:/etc/postfix/ldap_virtual_lists_maps.cf

Postfix sur Mailhost – comptes virtuels

smtpd_reject_unlisted_recipient = yes

smtpd_client_restrictions= permit_inet_interfaces, permit_mynetworks, permit_sasl_authenticated,permit

smtpd_delay_reject = yes

smtpd_helo_required = yes

smtpd_helo_restrictions = permit_mynetworks, reject_invalid_hostname, reject_unknown_hostname

smtpd_sender_restrictions = hash:/etc/postfix/access, reject_unknown_sender_domain

smtpd_restriction_classes = insiders_only

insiders_only = check_sender_access hash:/etc/postfix/insiders, reject

smtpd_recipient_restrictions =

permit_mynetworks,

permit_sasl_authenticated,

hash:/etc/postfix/protected_destinations,

reject_unauth_destination

Les fichiers ldap qui vont bien -1 -

#cat ldap_virtual_mailbox_maps.cf

server_host = ldaps://ldaps.xxxx.yyy.fr

port = 636

version = 3

search_base = ou=people,dc=xxxx,dc=yyy,dc=fr

query_filter = (&(objectClass=InetOrgPerson)(|(mail=%s)(uid=%u)(mailLocalAddress=%u)))

result_attribute = uid

#postmap –q mathilde.rousseau@xxxx.yyy.fr ldap:/etc/postfix/ldap_virtual_mailbox_maps.cf

mrouss

#postmap -q mrouss ldap:/etc/postfix/ldap_virtual_mailbox_maps.cf

mrouss

#postmap -q mathilde.rousseau ldap:/etc/postfix/ldap_virtual_mailbox_maps.cf

mrouss

Les fichiers ldap qui vont bien -2 -

#cat ldap_virtual_alias_maps.cf

version = 3

server_host = ldaps://ldaps.xxxx.yyy.fr

port = 636

search_base = ou=Alias,dc=icsn,dc=cnrs-gif,dc=fr

query_filter = (&(objectClass=nisMailAlias)(cn=%u))

result_attribute = rfc822MailMember

#postmap -q mrousseau@xxxx.yyy..fr ldap:/etc/postfix/ldap_virtual_alias_maps.cf

mrouss

Les fichiers ldap qui vont bien -3 -

```
# cat ldap_virtual_lists_maps.cf
# Listes de diffusions
version = 3
server_host = ldaps://ldaps.xxxx.yyy.fr
port = 636
search_base = ou=Lists,dc=icsn,dc=cnrs-gif,dc=fr
scope = sub
query_filter = (&(objectClass=extensibleObject)(mail=%s))
result_attribute = rfc822MailMember
#postmap -q staff@xxxx.yyy.fr ldap:/etc/postfix/ldap_virtual_lists_maps.cf
Mrouss,dle,jmartin,gloire,jmichel
```

dovecot

Utilisation de dovecot-deliver comme MDA

```
protocol lda {
  postmaster_address = staff@xxxx.yyy..fr
   hostname = mail.xxxx.yyy.fr
   mail_plugins = sieve
   mail_plugin_dir = /usr/lib/dovecot/modules/lda
  deliver_log_format = msgid=%m: %$
  sendmail_path = /usr/sbin/sendmail
  rejection_subject = Rejected: %s
  # UNIX socket path to master authentication server to find users.
  auth_socket_path = /var/run/dovecot/auth-master
}

mail_location = maildir:~/Maildir:INDEX=~/indexes
```

Fichier dovecot.conf

```
mail_uid = vmail
mail_gid = vmail

mail_privileged_group = mail

verbose_proctitle = no
first_valid_uid = 3000
last_valid_uid = 3000

first_valid_gid = 3000
last_valid_gid = 3000
```

Dovecot.conf – 2

```
auth default {
 mechanisms = plain login
 passdb ldap {
   args = /etc/dovecot/dovecot-ldap.conf
 }
 userdb ldap {
   args = /etc/dovecot/dovecot-ldap.conf
 }
  socket listen {
   master {  # gère l'authentification, socket qui a accès à userdb
     path = /var/run/dovecot/auth-master
     mode = 0600
     user = vmail
     group = vmail
   }
```

Dovecot.conf - 3

```
client { # permet de faire du smtp authentifié
    path = /var/spool/postfix/private/auth
    mode = 0660
    user = postfix
    group = postfix
  }
}
```

Dovecot-ldap.conf

uris = ldaps://ouessant.icsn.cnrs-gif.fr/

dn = cn=administrator, dc=xxxx,dc=yyy,dc=fr

dnpass = secret

ldap_version = 3

base = dc=xxxx,dc=yyy,dc=fr

user_attrs = icsnMailPath=home, =uid=vmail, =gid=vmail

#icsnMailPath=home <- On va chercher dans ldap la valeur du homedir #pour dovecot

user_filter = (&(objectClass=posixAccount)(|(mailLocalAddress=%u) (mail=%u)(uid=%u)))

pass_attrs = uid=user,userPassword=password

default_pass_scheme = CRYPT