

# Troubleshooting Mail

- Detilleux
- Bruno
- 01/01/2024
- 2TL1

## Situation 1

Rapport de Dépannage – Problème de permission et d'écoute de requêtes SMTP

### Outils / commandes

#### netstat

- Machine/Lien : Machine WWW dans la partie Serveur Postfix
- Commande : « netstat -nltpu »
- Cette commande est utilisée afin d'obtenir des informations sur les ports d'écoute ainsi que sur les ports et adresses sur lesquels il y a des connexions TCP et UDP. Il donne également les adresses Ip des appareils avec lesquels il est en relation. Dans ce cas-ci je l'utilise afin de connaître sur quel(s) port(s) les serveurs Postfix et Dovecot écoutent ainsi que les adresses Ip.

#### ls et cat

- Machine/Lien : Machine WWW dans la partie Serveur Postfix
- Commande : « ls /var/mail » et « cat toto »
- Ces deux commandes permettent d'afficher ce qui se trouve dans un répertoire pour la commande ls et afficher le contenu d'un fichier pour la commande cat.

#### nano

- Machine/Lien : Machine WWW dans la partie Serveur Postfix
- Commande : « nano main.cf »
- Cette commande permet d'ouvrir l'éditeur de texte/code intégré nativement dans Unix.

#### ps -A

- Machine/Lien : Machine WWW dans la partie Serveur Postfix
- Commande : « ps -A »

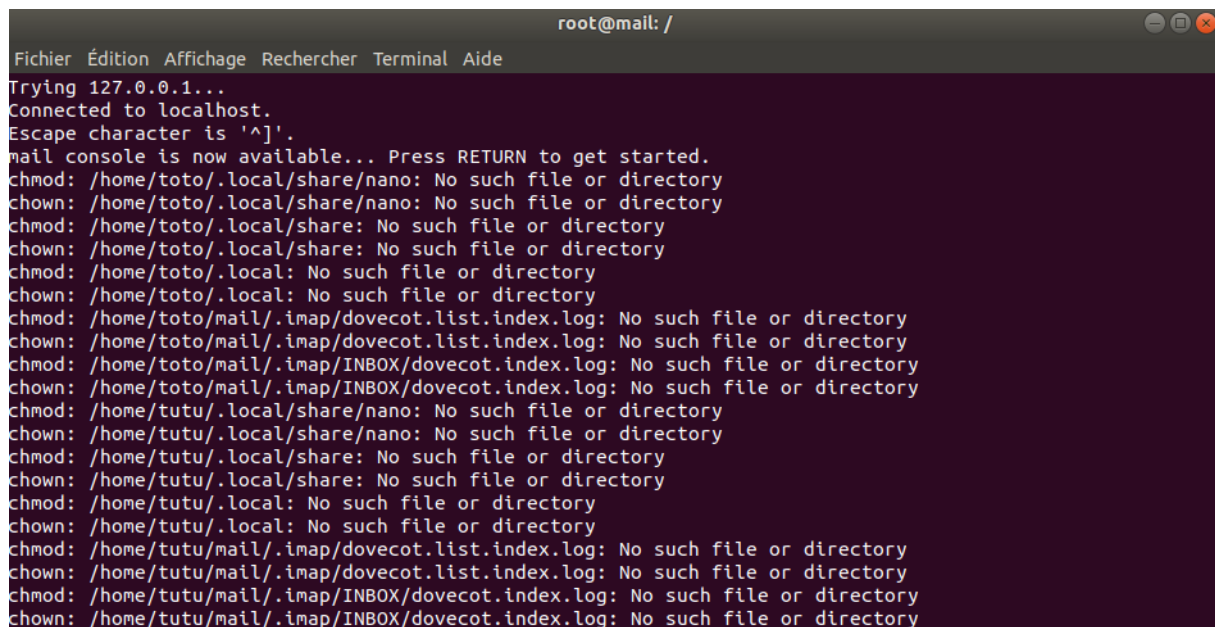
- Cette commande permet de lister tous les processus tournant sur le système en mentionnant les utilisateurs associés ainsi que le temps de fonctionnement et d'autres informations utiles.

## mutt

- Machine/Lien : Machine cliente
- Commande : « mutt »
- Cette commande lance un client de messagerie sous forme d'une interface en ligne de commande permettant d'envoyer, recevoir, lire, trier, transférer, ... des mails.

## Collecte des symptômes

- J'ai commencé en démarrant correctement les serveurs DHCP et DNS. Ensuite, en ouvrant la console de la machine 'www' j'ai obtenu les messages inhabituels suivants :



```

root@mail: /
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^['.
mail console is now available... Press RETURN to get started.
chmod: /home/toto/.local/share/nano: No such file or directory
chown: /home/toto/.local/share/nano: No such file or directory
chmod: /home/toto/.local/share: No such file or directory
chown: /home/toto/.local/share: No such file or directory
chmod: /home/toto/.local: No such file or directory
chown: /home/toto/.local: No such file or directory
chmod: /home/toto/mail/.imap/dovecot.list.index.log: No such file or directory
chown: /home/toto/mail/.imap/dovecot.list.index.log: No such file or directory
chmod: /home/toto/mail/.imap/INBOX/dovecot.index.log: No such file or directory
chown: /home/toto/mail/.imap/INBOX/dovecot.index.log: No such file or directory
chmod: /home/tutu/.local/share/nano: No such file or directory
chown: /home/tutu/.local/share/nano: No such file or directory
chmod: /home/tutu/.local/share: No such file or directory
chown: /home/tutu/.local/share: No such file or directory
chmod: /home/tutu/.local: No such file or directory
chown: /home/tutu/.local: No such file or directory
chmod: /home/tutu/mail/.imap/dovecot.list.index.log: No such file or directory
chown: /home/tutu/mail/.imap/dovecot.list.index.log: No such file or directory
chmod: /home/tutu/mail/.imap/INBOX/dovecot.index.log: No such file or directory
chown: /home/tutu/mail/.imap/INBOX/dovecot.index.log: No such file or directory

```

- Après avoir fait un « ps -A » j'ai remarqué que les processus des serveurs Postfix et Dovecot ne tournaient pas (voir image ci-dessous) :



```

root@mail:/# ps -A
  PID TTY          TIME CMD
    1 pts/0        00:00:00 bash
   648 pts/1        00:00:00 busybox
   672 pts/1        00:00:00 busybox
   718 pts/0        00:00:00 ps
root@mail:/#

```

- Après les avoir démarré j'ai donc essayé d'envoyer un mail à partir du 'client n°1' via l'utilisateur 'toto' et j'obtiens le message d'erreur suivant :

```
client-1
Fichier  Édition  Affichage  Rechercher  Terminal  Aide

y:Send q:Abort t:To c:CC s:Subj a:Attach file d:Descrip ?:Help
  From: toto@formation.lab
  To: tutu@formation.lab
  Cc:
  Bcc:
  Subject: Test de retablissement
Reply-To:
  Fcc: ~/sent
  Mix: <no chain defined>
Security: None

-- Attachments
- I      1 /tmp/mutt-client-1-1001-535-627717350300[text/plain, 7bit, us-ascii, 0

SMTP session failed: 554 5.7.1 <tutu@formation.lab>: Recipient address rejected:
```

## Analyse et explication du problème

- Le problème apparaissant dans ce troubleshooting est dû aux permissions de connexions SMTP qui acceptaient uniquement les connexions venant du réseau « 182.168.0.0/24 ». Or la machine n'est elle-même pas dans ce réseau, et le réseau en question n'existe tout simplement pas dans notre cas.

## Proposition de résolution

1. J'ai donc résolu le problème en procédant tout simplement au changement de l'adresse Ip du réseau accepté pour les connexions SMTP qui était « 182.168.0.0/24 » en l'adresse Ip du réseau réel et correct dans lequel la machine se trouve qui est « 192.168.0.0/24 ». Cette modification devant être faite dans le fichier de configuration du serveur Postfix (utilisant le protocole SMTP pour les envois de mail) nommé « main.cf » dans le répertoire « /etc/postfix ».

2. On peut dès lors faire le test d'envoi d'un mail via le 'client n°1' et voir que celui-ci a envoyé le mail :

```
client-1
Fichier Édition Affichage Rechercher Terminal Aide
q:Quit d:Del u:Undel s:Save m:Mail r:Reply g:Group ?:Help
---Mutt: =INBOX [Msgs:0 Post:2]---(threads/date)----- (all)---
Mail sent.
```

Le 'client n°2' reçoit bien le mail envoyé par le 'client n°1' :

```
client-2
Fichier Édition Affichage Rechercher Terminal Aide
i:Exit -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Help
Date: Thu, 4 Jan 2024 15:21:59 +0000
From: toto@formation.lab
To: tutu@formation.lab
Subject: Test de retablissement

Ceci est un mail de test de retablissement

-N +- 1/1: toto@formation.lab Test de retablissement -- (all)
```

- Et puis vérifier sur le serveur les processus tournants ainsi que les ports d'écoute via la commande « `netstat -nltpu` » et la commande « `ps -A` » (qui ici les indique bien) :

```
root@mail: /etc/dovecot
Fichier Édition Affichage Recherche Terminal Aide
postfix/postfix-script: starting the Postfix mail system
root@mail:/etc/postfix# cd /etc/dovecot
root@mail:/etc/dovecot# ls
conf.d               dovecot-dict-sql.conf.ext  dovecot.conf
dovecot-dict-auth.conf.ext  dovecot-sql.conf.ext      dovecot.conf_bck
root@mail:/etc/dovecot# ps -A
  PID TTY          TIME CMD
    1 pts/0        00:00:00 bash
   648 pts/1        00:00:00 busybox
   672 pts/1        00:00:00 busybox
   813 ?            00:00:00 master
   814 ?            00:00:00 pickup
   815 ?            00:00:00 qmgr
   819 ?            00:00:00 dovecot
   820 ?            00:00:00 anvil
   821 ?            00:00:00 log
   822 ?            00:00:00 config
   823 pts/0        00:00:00 ps
root@mail:/etc/dovecot# netstat -nltpu
bash: netstat: command not found
root@mail:/etc/dovecot# netstat -nltpu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:110             0.0.0.0:*                LISTEN      819/dovecot
tcp        0      0 0.0.0.0:143             0.0.0.0:*                LISTEN      819/dovecot
tcp        0      0 0.0.0.0:25              0.0.0.0:*                LISTEN      813/master
tcp6       0      0 :::110                  :::*                    LISTEN      819/dovecot
tcp6       0      0 :::143                  :::*                    LISTEN      819/dovecot
tcp6       0      0 :::25                   :::*                    LISTEN      813/master
root@mail:/etc/dovecot#
```

## Résultats attendus

Dans le cas présent on aimerait voir, en tapant la commande « `mutt` » sur le client n°1 ou n°2, les mails échangés entre les 2 machines. On peut également vérifier cela directement dans le serveur en allant dans les fichiers contenant les mails échangés pour chaque utilisateur, ici « `toto` » et « `tutu` ». Ils sont dans le répertoire « `/var/mail` » et les 2 fichiers sont respectivement les noms d'utilisateur « `toto` » et « `tutu` ».

Exemple de mail envoyé de « `toto@formation.lab` » correspondant au 'client n°1' à « `tutu@formation.lab` » correspondant au 'client °2' (vu depuis le récepteur : « `tutu` ») :

```
root@mail: /var/mail
Fichier Édition Affichage Rechercher Terminal Aide
GNU nano 4.8 tutu
From toto@formation.lab Thu Jan  4 15:21:59 2024
Return-Path: <toto@formation.lab>
X-Original-To: tutu@formation.lab
Delivered-To: tutu@formation.lab
Received: from client-1 (unknown [192.168.0.28])
        by mail.formation.lab (Postfix) with SMTP id 33D328A981
        for <tutu@formation.lab>; Thu,  4 Jan 2024 15:21:59 +0000 (UTC)
Date: Thu, 4 Jan 2024 15:21:59 +0000
From: toto@formation.lab
To: tutu@formation.lab
Subject: Test de retablissement
Message-ID: <20240104152159.GA595@client-1>
MIME-Version: 1.0
Content-Type: text/plain; charset=us-ascii
Content-Disposition: inline
Ceci est un mail de test de retablissement

[ Read 18 lines ]
^G Get Help  ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^  Go To Line  M-E Redo
```

## Conclusion

En conclusion un serveur de mail Postfix utilise des configurations pouvant contenir des restrictions de réseaux ou de machines bien précises bloquant alors tout échange d'informations possible avec celle-ci excepté les messages d'erreurs provenant du serveur et allant au client.

## Situation 2

### Rapport de Dépannage – Problème d'accès au serveur de messagerie

#### Outils / commandes

Voir commande mentionnée plus haut.

#### Collecte des symptômes

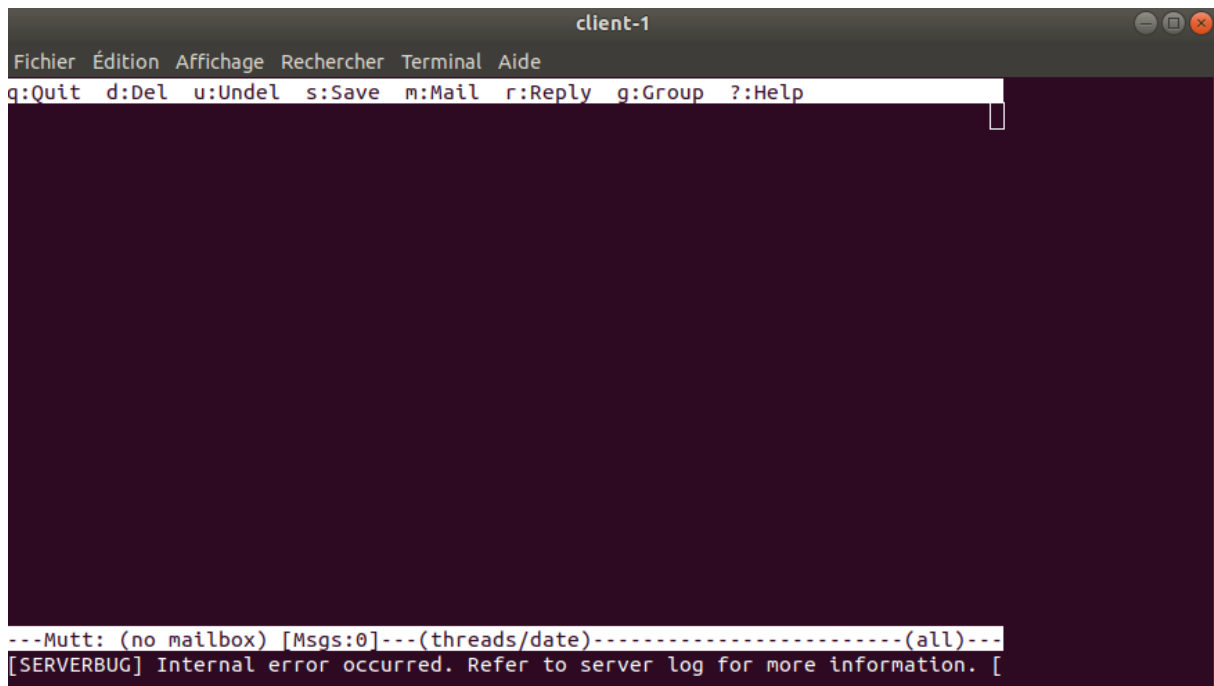
- Après avoir démarré les serveur DHCP et DNS j'ouvre le terminal de commande de la machine 'www' et j'observe déjà plusieurs messages d'erreurs qui sont les suivants :

```
root@mail: /
Fichier Édition Affichage Rechercher Terminal Aide
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
mail console is now available... Press RETURN to get started.
chmod: /home/toto/mail/.imap/dovecot.list.index.log: No such file or directory
chown: /home/toto/mail/.imap/dovecot.list.index.log: No such file or directory
root@mail:/#
```

- Je lance donc les serveurs Postfix et Dovecot afin de vérifier s'ils démarrent correctement et je vérifie à l'aide des commandes « netstat -nltpu » et « ps -A » que les processus tournent bien :

```
root@mail: /
Fichier Édition Affichage Rechercher Terminal Aide
postfix: See http://www.postfix.org/COMPATIBILITY_README.html for details
postfix: To disable backwards compatibility use "postconf compatibility_level=2" and "postfix reload"
postfix/postfix-script: starting the Postfix mail system
root@mail:/# dovecot
root@mail:/# ps -A
  PID TTY          TIME CMD
    1 pts/0        00:00:00 bash
   439 pts/1        00:00:00 busybox
   464 pts/1        00:00:00 busybox
   791 ?            00:00:00 master
   792 ?            00:00:00 pickup
   793 ?            00:00:00 qmgr
   794 ?            00:00:00 postlogd
   796 ?            00:00:00 dovecot
   797 ?            00:00:00 anvil
   798 ?            00:00:00 log
   799 ?            00:00:00 config
   800 pts/0        00:00:00 ps
root@mail:/# netstat -nltpu
bash: netstat: command not found
root@mail:/# netstat -nltpu
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:110             0.0.0.0:*               LISTEN      796/dovecot
tcp        0      0 0.0.0.0:143             0.0.0.0:*               LISTEN      796/dovecot
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      791/master
tcp6       0      0 :::110                  :::*                    LISTEN      796/dovecot
tcp6       0      0 :::143                  :::*                    LISTEN      796/dovecot
tcp6       0      0 :::25                   :::*                    LISTEN      791/master
root@mail:/#
```

- Ensuite je tente de lancer le client de messagerie 'mutt' sur le 'client n°1' et je remarque que celui-ci (tout comme sur le 'client n°2') m'affiche l'erreur suivante :



```
client-1
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
q:Quit  d:Del  u:Undel  s:Save  m:Mail  r:Reply  g:Group  ?:Help

---Mutt: (no mailbox) [Msgs:0]---(threads/date)-----all)---
[SERVERBUG] Internal error occurred. Refer to server log for more information. [
```

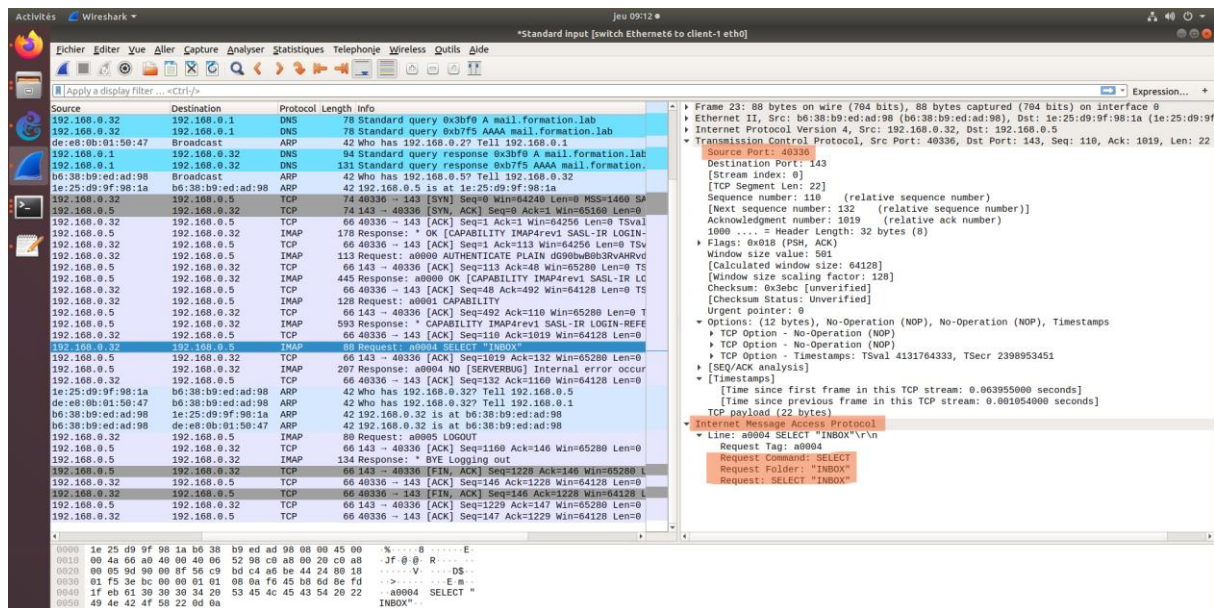
## Analyse et explication du problème

Le problème survenu ici est un problème dû au fait qu'un répertoire important utilisé par le serveur n'est pas existant. Le serveur Dovecot, faisant appel au répertoire « /var/mail », stocke les mails échangés par les différents utilisateurs pour chacun des utilisateurs. Chacun des utilisateurs se voit attribuer un fichier répertoriant tous les mails échangés. Ce fichier ayant le nom de l'utilisateur. Les protocoles IMAP et POP utilisent tous deux ce répertoire pour stocker de manière provisoire ou permanente les mails échangés. Sans ce répertoire le serveur ne sait pas où les conserver.

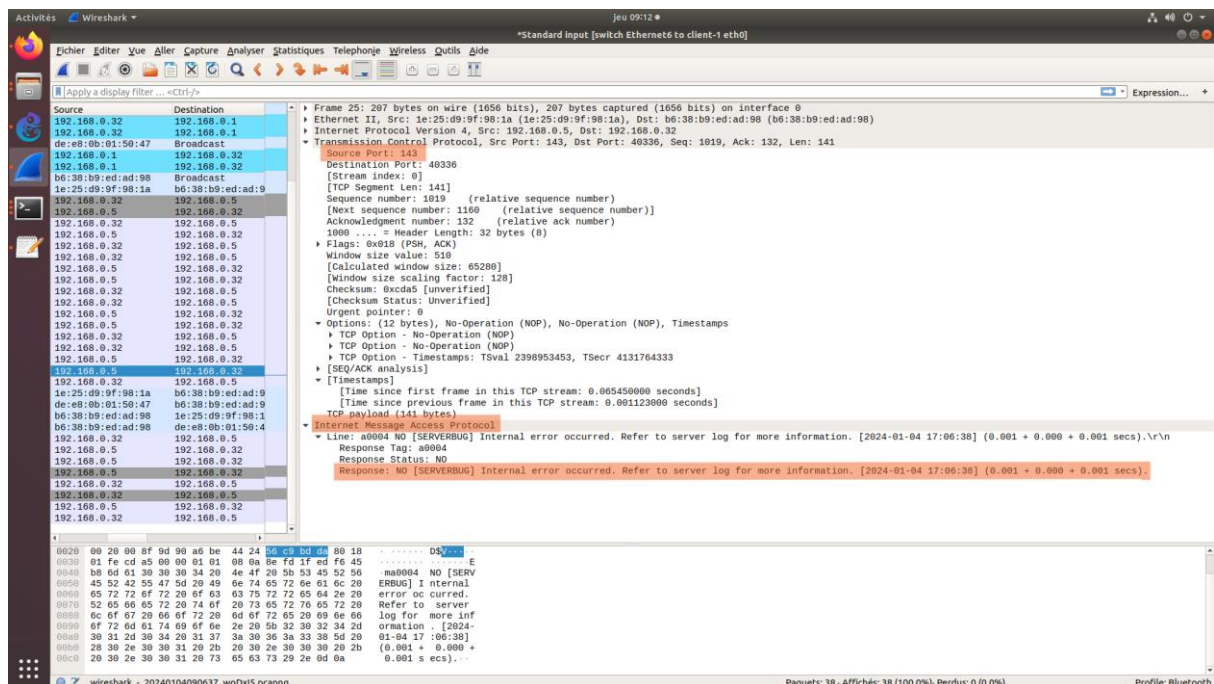
## Proposition de résolution

1. Afin de résoudre le problème j'ai commencé par effectuer une capture Wireshark afin d'en savoir plus sur l'erreur indiquée et de savoir quelle requête a échoué. J'ai découvert que la requête pour la boîte aux lettres (INBOX) a été refusée :





2. La requête fut refusée et le serveur fournissait une erreur proposant d'aller voir dans les logs du serveur :



3. Après avoir vu cela j'ai donc été voir dans les logs et c'est là que j'ai découvert que le serveur ne parvenait pas à créer le répertoire « mail » dans « etc » pour l'INBOX car celui-ci n'avait pas les permissions pour le faire. Ce qui est normal car il n'est pas possible pour lui d'écrire dans ce répertoire protégé et en plus ce n'est pas du tout le bon répertoire :

```
root@mail: /var/log
Fichier Édition Affichage Rechercher Terminal Aide
dovecot.log
GNU nano 4.8
Jan 04 16:20:01 auth: Debug: shadow(toto,192.168.0.30,<Uj94GLE0LK/AqAAe>): Finished passwd lookup
Jan 04 16:20:01 auth: Debug: auth(toto,192.168.0.30,<Uj94GLE0LK/AqAAe>): Auth request finished
Jan 04 16:20:01 auth: Debug: client passwd out: OK 1 user=toto
Jan 04 16:20:01 auth-worker(836): Debug: shadow(toto,192.168.0.30,<Uj94GLE0LK/AqAAe>): Finished passwd lookup
Jan 04 16:20:01 auth-worker(836): Debug: conn unix:auth-worker (pid=827,uid=106): auth-worker<1>: Finished
Jan 04 16:20:01 auth: Debug: master ln: REQUEST 567934977 835 1 e8efb693376275b9df3a29cd0ab8ffae session_pid=837 request_auth_token
Jan 04 16:20:01 auth: Debug: passwd(toto,192.168.0.30,<Uj94GLE0LK/AqAAe>): Performing userdb lookup
Jan 04 16:20:01 auth-worker(836): Debug: conn unix:auth-worker (pid=827,uid=106): auth-worker<2>: Handling USER request
Jan 04 16:20:01 auth: Debug: passwd(toto,192.168.0.30,<Uj94GLE0LK/AqAAe>): Performing userdb lookup
Jan 04 16:20:01 auth-worker(836): Debug: passwd(toto,192.168.0.30,<Uj94GLE0LK/AqAAe>): lookup
Jan 04 16:20:01 auth: Debug: passwd(toto,192.168.0.30,<Uj94GLE0LK/AqAAe>): Finished userdb lookup
Jan 04 16:20:01 auth: Debug: master userdb out: USER 567934977 toto system_groups.user=toto uid=1000 gid=1000 home=/home/toto auth_token=51cada64ff128c278cf9accb77
Jan 04 16:20:01 auth-worker(836): Debug: passwd(toto,192.168.0.30,<Uj94GLE0LK/AqAAe>): Finished userdb lookup
Jan 04 16:20:01 auth-worker(836): Debug: conn unix:auth-worker (pid=827,uid=106): auth-worker<2>: Finished
Jan 04 16:20:01 lnep-login: Info: Login: user=<toto>, method=PLAIN, rip=192.168.0.30, lip=192.168.0.5, mpid=837, session=<Uj94GLE0LK/AqAAe>
Jan 04 16:20:01 lnep(toto)<837><Uj94GLE0LK/AqAAe>: Debug: Effective uid=1000, gid=1000, home=/home/toto
Jan 04 16:20:01 lnep(toto)<837><Uj94GLE0LK/AqAAe>: Debug: fs: root=/home/toto/mail, index=, indexpvt=, control=, inbox=/etc/mail/toto, alt=
Jan 04 16:20:01 lnep(toto)<837><Uj94GLE0LK/AqAAe>: Debug: Mailbox INBOX: Mailbox opened because: SELECT
Jan 04 16:20:01 lnep(toto)<837><Uj94GLE0LK/AqAAe>: Debug: Namespace : Using permissions from /home/toto/mail: mode=0755 gid=default
Jan 04 16:20:01 lnep(toto)<837><Uj94GLE0LK/AqAAe>: Debug: Namespace : /etc/mail/toto doesn't exist yet, using default permissions
Jan 04 16:20:01 lnep(toto)<837><Uj94GLE0LK/AqAAe>: Debug: Namespace : Using permissions from /home/toto/mail: mode=0755 gid=default
Jan 04 16:20:01 lnep(toto)<837><Uj94GLE0LK/AqAAe>: Error: Mailbox INBOX: mkdir_parents(/etc/mail) failed: Permission denied
Jan 04 16:20:08 lnep(toto)<837><Uj94GLE0LK/AqAAe>: Info: Logged out ln=96 out=1187 deleted=0 expunged=0 trashed=0 hdr_count=0 hdr_bytes=0 body_count=0 body_bytes=0
Jan 04 16:21:01 auth-worker(836): Debug: conn unix:auth-worker (pid=827,uid=106): Disconnected: Connection closed (fd=1)
```

4. J'ai donc été dans le dossier de configuration du serveur Dovecot qui se nomme « dovecot.conf » et j'y ai changé la directive pour situer où les INBOX peuvent être créées et où les mails peuvent être stockés (dans la ligne de commande il suffit de changer « mail\_location = mbox:~/mail:INBOX=/etc/mail/%u » par « mail\_location = mbox:~/mail:INBOX=var/mail/%u ») :

```
root@mail: /etc/dovecot
Fichier Édition Affichage Rechercher Terminal Aide
dovecot.conf
GNU nano 4.8
protocols = pop3 imap
#Utilisation des utilisateurs systeme et des shadow password
passwd {
  driver = shadow
}
userdb {
  driver = passwd
}
#Indiquer a Dovecot ou sendmail stocke les mails et ou eut creer ses INBOX
mail_location = mbox:~/mail:INBOX=/etc/mail/%u
#Pas de ssl par facilite dans le cadre du TP
ssl=no
disable_plaintext_auth = no
#Configuration des logs : On veut un maximum d'information
log_path=/var/log/dovecot.log
auth_verbose = yes
auth_verbose_passwords = yes
auth_debug = yes
auth_debug_passwords = yes
mail_debug = yes
[ Read 20 lines ]
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos M-U Undo
^X Exit ^R Read File ^_ Replace ^U Paste Text ^T To Spell ^_ Go To Line M-E Redo
```

## Résultats attendus

Le résultat attendu serait donc le suivant pour le client n°1 qui n'a reçu encore aucun mail :

```
client-1
Fichier Édition Affichage Rechercher Terminal Aide
q:Quit d:Del u:Undel s:Save m:Mail r:Reply g:Group ?:Help

---Mutt: =INBOX [Msgs:0]---(threads/date)------(all)---
There are no messages.
```

Ou bien le suivant pour le client n°2 qui lui a reçu le mail provenant du client n°1 :

```
client-2
Fichier Édition Affichage Rechercher Terminal Aide
i:Exit -:PrevPg <Space>:NextPg v:View Attachm. d:Del r:Reply j:Next ?:Help
Date: Thu, 4 Jan 2024 16:38:43 +0000
From: toto@formation.lab
To: tutu@formation.lab
Subject: Test de retablissement

Ceci est un petit mail de test de retablissement du serveur

-N +- 1/1: toto@formation.lab    Test de retablissement    -- (all)
```

## Conclusion

Pour conclure on peut dire que le serveur Dovecot ne pouvait fournir au client de messagerie ce qu'il désirait (c'est-à-dire les mails déjà échangés etc) car celui-ci n'avait pas le bon répertoire renseigné dans son fichier de configurations. Donc les mails ne pouvaient être sauvegardés et les INBOX créées. Le serveur Dovecot utilisant les protocoles IMAP (qui stocke les mails sur le serveur et permet aux clients de venir les consulter directement dessus) et POP (qui stocke les mails de manière temporaire sur le serveur permettant aux clients de les télécharger et les supprimant ainsi du serveur) a besoin d'un répertoire dédié pour faire ses manipulations.