



# Administration Réseau Avancée sous GNU/Linux

Mohammed Madiafi

Département Informatique, Réseaux et Télécoms

# Plan de la 4<sup>ème</sup> partie

- Serveur Web
- Messagerie électronique
- Connexion à distance par SSH
- Pare-Feu

# Serveur Apache

- Caractéristiques :
  - Popularité
  - Stabilité
  - Structure modulaire

# Installation

- Côté serveur :
  - apt-get install apache2
- Côté client :
  - apt-get install iceweasel
  - ou
  - apt-get install lynx

# Configuration (côté serveur)

- Configurations générales
  - /etc/apache2/apache2.conf
- Configurations spécifiques pour chaque site web
  - /etc/apache2/sites-available/\*
- Configurations spécifiques pour chaque module
  - /etc/apache2/mods-available/\*

# Configuration (côté serveur)

## Exemple

- ServerRoot /etc/apache2
- ErrorLog /var/log/apache2/error.log
- Listen 80
- DocumentRoot /var/www
- <Directory /var/www>  
allow from all  
</Directory>

# Site web par défaut

- /etc/apache2/sites-available/default
- <VirtualHost \*:80>

ServerAdmin root@localhost

DocumentRoot /var/www

<Directory /var/www>

allow from allow

</Directory>

...

</VirtualHost>

# Plusieurs sites/une seule adresse IP

## Hôtes virtuels

- /etc/apache2/sites-available/site1

- <VirtualHost \*:80>

    ServerName  nom.domaine

    DocumentRoot /var/www/site1

</VirtualHost>

- a2ensite  site1



# Sites web personnels

- Chargement du module « userdir »
  - `a2enmod userdir`
- Création du répertoire « public\_html » sous `/home/$USER`
  - Peut modifié dans `/etc/apache2/mods-available/userdir.conf`
- Consultation à l'aide de l'adresse `serveur.domaine/~$USER`

# Serveur de messagerie

- MTA (MAil Transfer Agent) : Agent de Transfert de Mails
  - Envoi et réception de messages électroniques
- MDA (Mail Delivery Agent) : Agent de délivrance de Mails
  - Remise des messages
- MUA (Mail User Agent) : Client de messagerie

# Protocole SMTP

- SMTP (Simple Mail Transfer Protocol)
  - Protocole utilisé par un MTA
  - Pour le transfert de messages électroniques vers les serveurs de messagerie.

# Postfix

- Postfix
  - C'est un MTA open-source
  - utilisé par de nombreux hébergeurs et fournisseurs d'accès.
  - Se caractérise par sa simplicité de configuration

# Postfix

## Comptes de messagerie

- Comptes unix créés sur le serveur
  - user@domaine
- Alias
  - /etc/alias
    - webmaster : root
    - hostmaster : root
- Génération de la base à partir de /etc/alias
  - postalias /etc/alias

# Postfix

## Configuration

- /etc/postfix/main.cf
  - myorigin = domaine vu de l'extérieur
  - mydestination = domaine à destination
  - mynetwork = réseau/masque
  - home\_mailbox = Maildir/

# Postfix

## Domaines virtuels

- /etc/postfix/main.cf
  - virtual\_alias\_domain domaine1, domaine2
- Affectation des boîtes aux lettres aux différents comptes :
  - virtual\_alias\_maps=hash:/etc/postfix/virtual
- /etc/postfix/virtual
  - adresse\_mail compte\_unix
- postmap /etc/postfix/virtual

# IMAP4

- IMAP4
  - L'un des protocoles utilisés par les MDA
  - Télécharge les en-têtes des messages et donne au client le choix de consulter, effacer, déplacer, etc.



# Courier-IMAP

- Courier-IMAP
  - Suite logicielle fournissant un ensemble de services de gestion de courriers électroniques.

# Courier-IMAP

- Configuration
    - /etc/courier/imapd
- MAILDIRPATH = Maildir

# Installation

- Côté serveur :
  - apt-get install postfix
  - apt-get install courier-imap
- Côté client
  - apt-get install evolution

# Client de messagerie

Bienvenue

Restaurer à partir de l'archive

## Identité

Réception du courrier

Options de réception

Envoi du courrier

Résumé du compte

Terminé

Saisissez vos nom et adresse électronique ci-dessous. Les champs « optionnels » ci-dessous n'ont pas besoin d'être remplis, à moins que vous ne désiriez inclure ces informations dans les messages que vous envoyez.

### Informations requises

Nom complet :

Adresse électronique :

### Informations optionnelles

☐ En faire mon compte par défaut

Répondre à :

Organisation :

Annuler

Précédent

Continuer

# Client de messagerie

Bienvenue

Identité

**Réception du courriel**

Options de réception

Envoi du courriel

Terminé

Résumé du compte

Restaurer à partir de l'archive

Configurez les paramètres de compte suivants.

Type de serveur : IMAP

Description : Pour lire et stocker les courriels sur des serveurs IMAP.

## Configuration

Serveur : 192.168.1.10 Port: 143

Nom d'utilisateur : user1

## Sécurité

Utiliser une connexion sécurisée : Sans chiffrement

## Type d'authentification

Mot de passe Vérifier les types pris en charge

☐ Mémoriser le mot de passe

Annuler

Précédent

Continuer

# Client de messagerie

Bienvenue

Identité

Réception du courriel

Options de réception

**Envoi du courriel**

Terminé

Résumé du compte

Restaurer à partir de l'archive

Saisissez les informations nécessaires pour envoyer le courriel. En cas de doute, adressez-vous à votre administrateur système ou à votre fournisseur d'accès Internet.

Type de serveur : SMTP

Description : Pour la distribution du courriel via un serveur de courriel distant utilisant SMTP.

## Configuration du serveur

Serveur : 192.168.1.10 Port : 25

☐ Le serveur requiert une authentification

## Sécurité

Utiliser une connexion sécurisée : Sans chiffrement

## Authentification

Type : CLAIR

Vérifier les types pris en charge

Nom d'utilisateur : user1

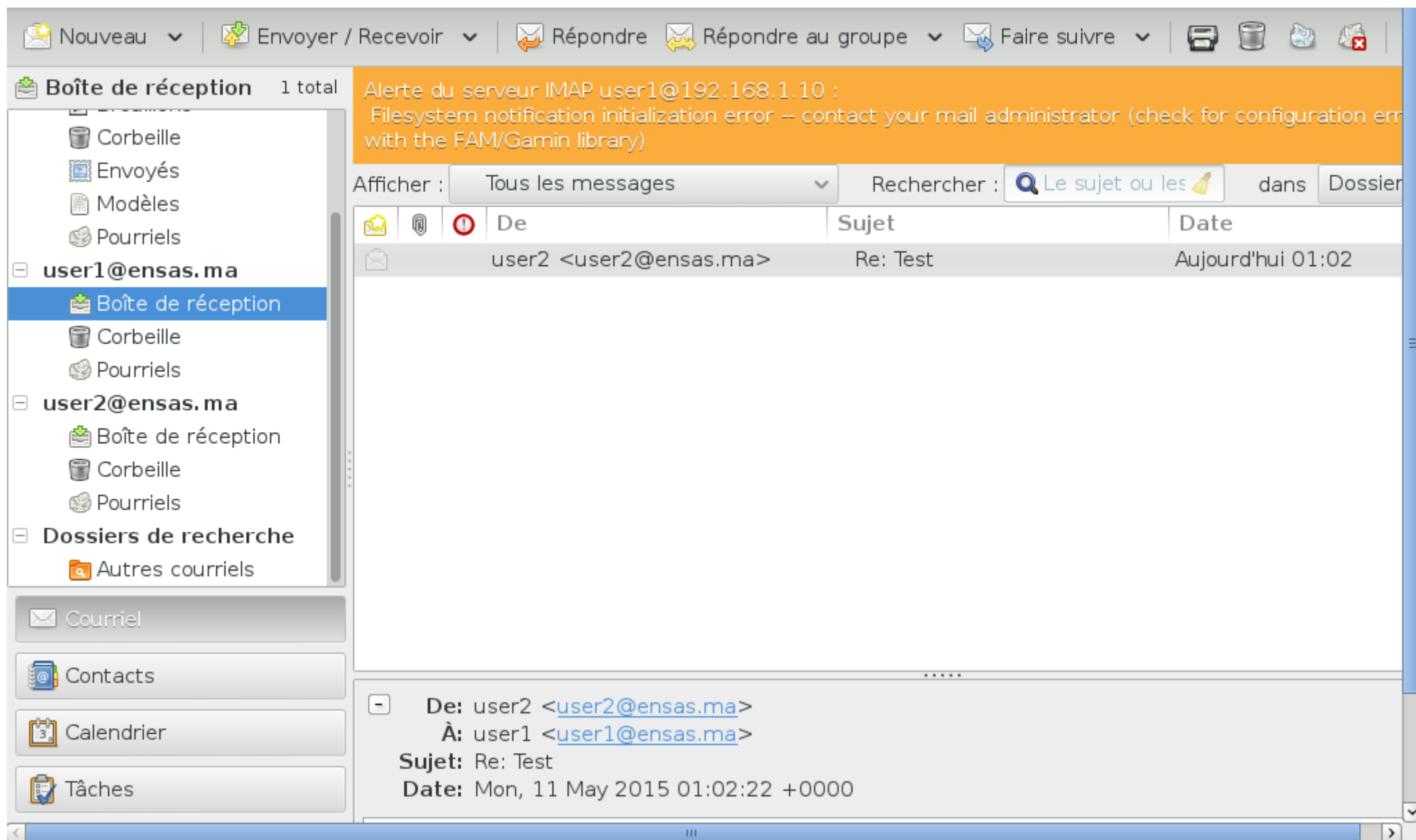
☐ Mémoriser le mot de passe

Annuler

Précédent

Continuer

# Client de messagerie



# Connexion à distance par SSH

- SSH :
  - Protocole de connexion à distance à l'aide d'un compte unix local au serveur
  - Apporte des services d'authentification et de confidentialité
  - Considéré comme « telnet sécurisé »



# Installation

- Côté serveur :
  - `apt-get install openssh-server`
- Côté client :
  - `apt-get install openssh-client`

# Authentication par mot de passe

- `ssh user@serveur`
  - Vérification de la clé ECDSA affichée avec celle stockée sur le serveur
  - `ssh-keygen -l` (côté serveur)
- Une fois c'est vérifié, la clé est stockée cryptée dans `~/.ssh/known_hosts`

# Authentication par mot de passe

- `ssh user@serveur`
  - Vérification de la clé ECDSA affichée avec celle stockée sur le serveur
  - `ssh-keygen -l` (côté serveur)
- Une fois c'est vérifié :
  - la clé est stockée cryptée dans `~/.ssh/known_hosts`
  - Le mot de passe de user est demandé

# Authentification par clés

- Utilisation de clés stockées sur le client
- Création d'une clé publique et une clé privée (côté client) :
  - `ssh-keygen -t rsa`
  - `.ssh/id_rsa` et `.ssh/id_rsa.pub`
- Copie de la clé publique dans `.ssh/authorized_keys` du serveur

# Copie de fichiers par SCP

- Copie à l'aide du protocole SSH.
- Copie d'un fichier local vers le serveur :
  - `scp user@server : /fichier_distant  
fichier_local`
- Téléchargement d'un fichier distant :
  - `scp fichier_local user@server :  
/fichier_distant`

# Tunnels SSH

- Utilisation de SSH pour sécuriser une communication client-serveur basée sur un protocole peu sécurisé
  - `ssh -L port : cible_trafic : port_cible user@serveur`

# Pare-Feu

- Gestion de filtrage de paquets IP
- Peut fonctionner selon deux modes :
  - Tout ce qui n'est pas autorisé est interdit
  - Tout ce qui n'est pas interdit est autorisé
- Utilise l'outils « iptables »
- Iptables filtre le trafic en transit dans un routeur, le trafic entrant et le trafic sortant.

# Politique par défaut

- Affichage de la politique par défaut :
  - iptables -S
- Modification de la politique par défaut :
  - iptables -P chaine action

Chaine = INPUT, OUTPUT ou FORWARD

Action = ACCEPT ou DROP



# Ajout de règles iptables

- iptables -A chaine -s ip\_source -d ip\_destination -p protocole --dport port -j action
- Exemple :
  - iptables -A FORWARD -s 192.168.9.0/24 -d 192.168.8.9/32 -p icmp -j DROP

# Gestion des règles

- Suppression de toutes les règles
  - iptables -F
- Affichage des numéros des règles :
  - iptables -L chaine --line-numbers -n
- Suppression d'une règle :
  - iptables -D chaine numéro
- Insertion d'une règle :
  - iptables -I chaine numéro condition  
action

# Gestion des flux retours

- Autoriser les flux retours qui sont des réponses à un flux en sortie explicitement autorisé.
  - iptables -A chaine -m state --state ESTABLISHED,RELATED -j ACCEPT
- ESTABLISHED : paquets en réponse à un flux aller autorisé
- RELATED : paquets issus d'une nouvelle connexion établie à l'initiative d'une connexion autorisée.