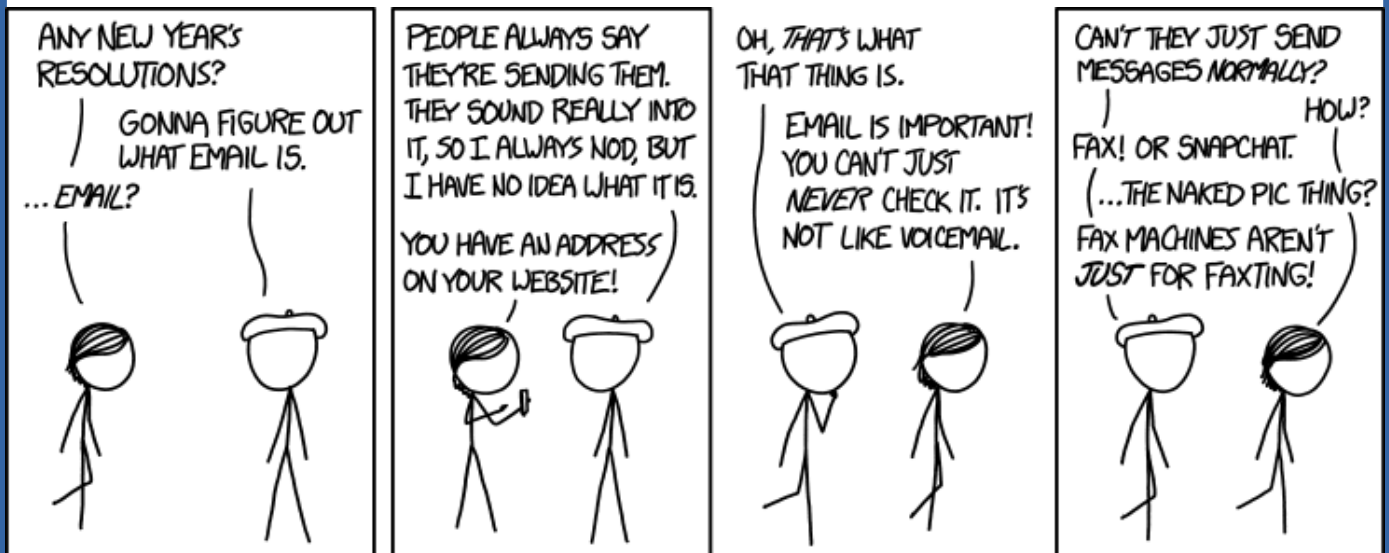


Serveur mail sous Linux



Certificateur de compétences

whoami

- Thomas Constans
- thomas@opendoor.fr
- 50 % sysadmin
- 50 % formateur
- <3 linux & logiciels libres

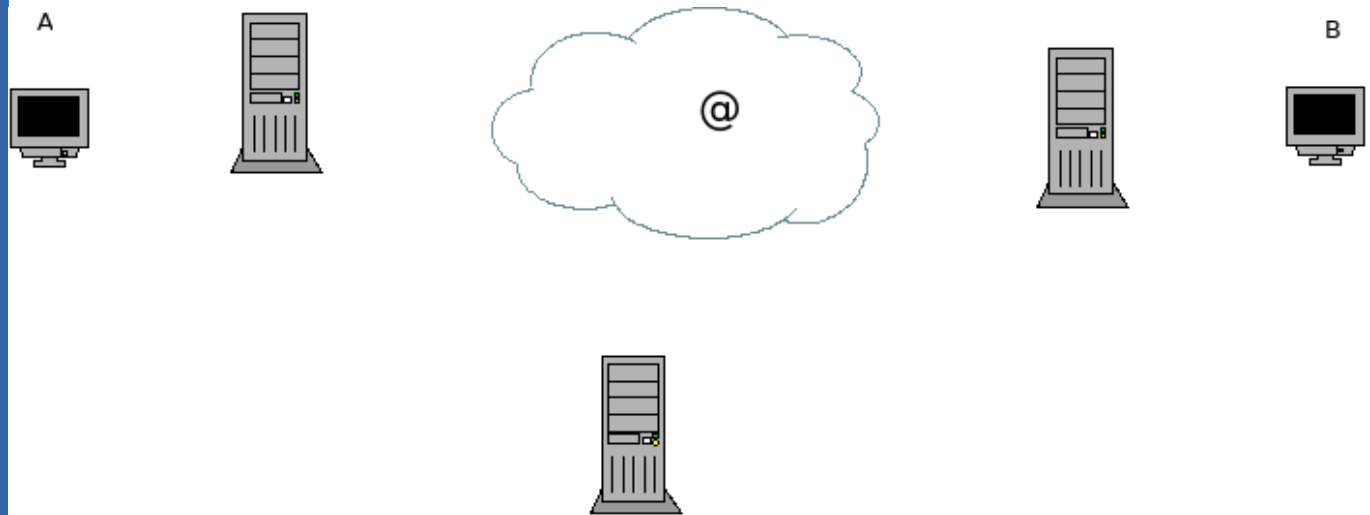
Rappel : Vi

lancer vi	vim
changer de mode	i(nsert) / Esc
se déplacer	G pour aller à la fin du fichier Gg pour aller au début \$ pour aller en fin de ligne 6G pour aller à la ligne 6 Marche aussi avec les commandes : dG : supprime tout jusqu'à la fin
annuler / répéter une commande	u(ndo) / control+r (redo)
rechercher et remplacer	:%s/foo/bar/g # remplace toutes les occurrences de foo par bar dans tout le fichier
rechercher dans le fichier	/aiguille puis n pour prochaine occurrence, N pour précédente occurrence
enregistrer	:w
quitter	:q /:q!

Plan

- 1) Principes du mail
- 2) Installer un serveur postfix
- 3) Installer un serveur cyrus
- 4) Communiquer avec l'extérieur
- 5) Authentification smtp
- 6) Antivirus et Antispam
- 7) Exploitation et MCO

Principes



Utilisateur "a@client1.opendoor.fr"
envoie un email à "b@foobar.org"
Complétez le schéma avec un
maximum de détails.

DNS

- Donnez la commande permettant d'obtenir le MX du domaine *opendoor.fr*
- Quel sont les serveurs mails légitimes du domaine *opendoor.fr* ?
- Quels sont les 5 premiers caractères de la clé utilisée pour signer les messages en provenance de *opendoor.fr*

Dialoguer avec un serveur SMTP)

- Remettez dans l'ordre les étapes de soumission d'un mail à un MTA via telnet/netcat :

helo foobar.org

quit

rcpt to: client1@client1.opendoor.fr

mail from: toto@test.fr

telnet localhost 25

```
data
subject: mail de test
hello world !
```

▪

Postfix

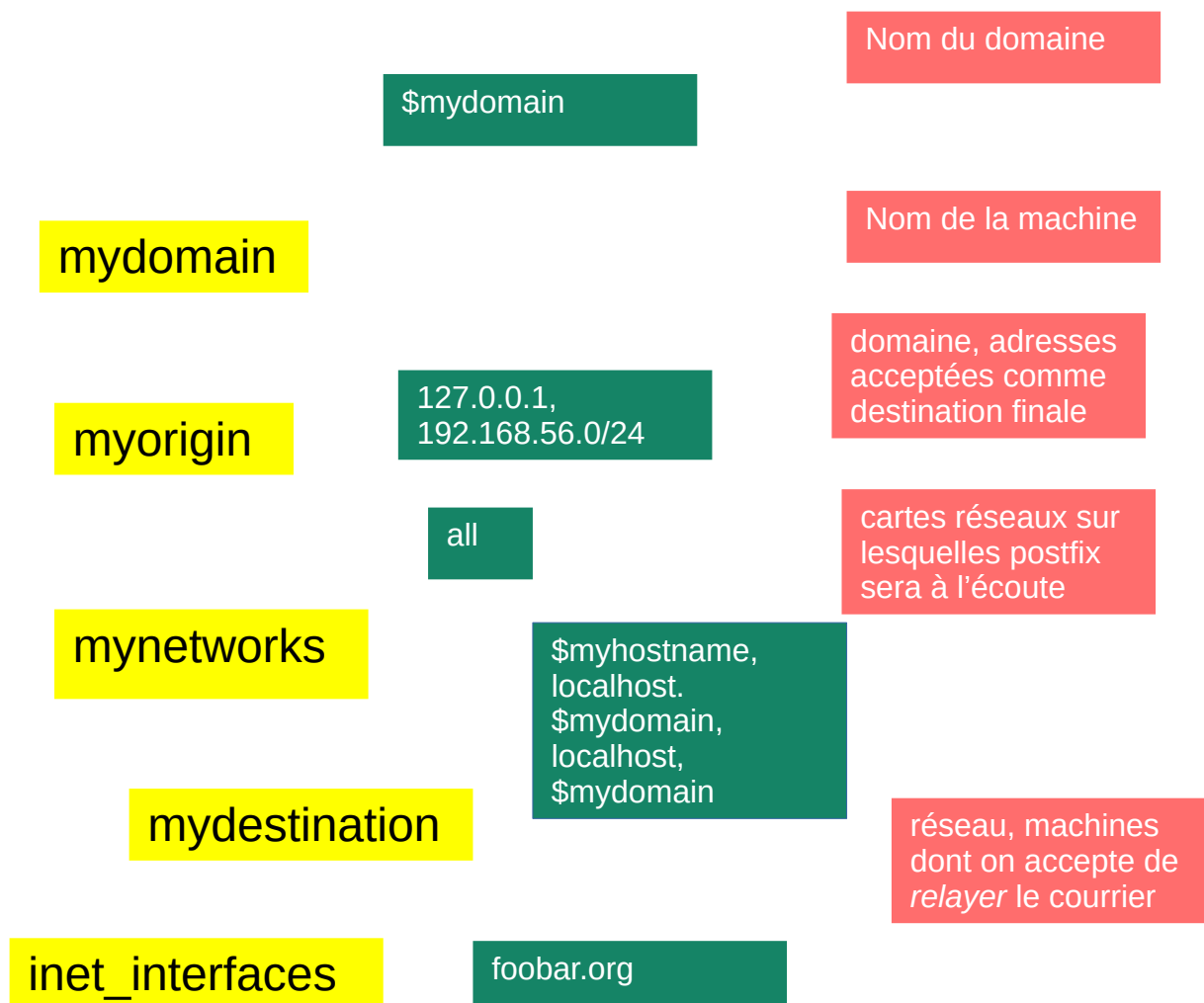
- postfix peut faire office de :
 - MDA
 - MUA
 - MTA
- Liste des paquets à installer :
- 2 choses à faire une fois le paquet installé :
- Où se trouve le (principal) fichier de conf ?:
- Quels sont les ports d'écoute standard du protocole SMTP ?

Troubleshooting postfix

- Penser à relancer postfix !
- Configurer postfix pour qu'il écrive ses logs dans un fichier (postconf -e maillog_file=/var/log/mail.log)
- Vérifier ces logs
- Vérifier la file d'attente :
 - `postqueue -p #` afficher le contenu de la file d'attente
 - `postqueue -f #` forcer le traitement de la file d'attente
 - `postsuper -d ID #` supprimer un message de la file
 - `postsuper -d ALL #` vider la file de message

Configuration de postfix

En vous aidant de la documentation* et des commentaires du fichier /etc/postfix/main.cf, remettez dans l'ordre les 6 directives suivantes, et reliez-les à leur valeur et leur rôle :



* http://www.postfix.org/BASIC_CONFIGURATION_README.html

Postfix : 1ère mise en oeuvre

- Utilisez http://www.postfix.org/BASIC_CONFIGURATION_README.html pour configurer un serveur postfix:
 - reçoit les mails pour le domaine *client1.opendoor.fr*
 - sert de relais pour les machines du réseau local
 - est accessible depuis l'extérieur
- Créez une boîte mail "augustine@client1.opendoor.fr"
- Envoyez un mail (en utilisant telnet) à cette adresse.
- Retrouvez la boîte mail dans lequel le message a été distribué
- Transférez les mails à destination de root soient transférée à augustine.
- Envoyez un mail à root. Celui-ci doit se retrouver dans la boîte mail de augustine

Postfix : utilisateurs virtuels

- Qu'est-ce qu'un utilisateur virtuel ?
- En vous aidant de http://www.postfix.org/VIRTUAL_README.html, implémentez la partie "*Postfix virtual MAILBOX example: separate domains, non-UNIX accounts*" en respectant les contraintes suivantes :
 - domaines hébergés : `client1.opendoor.fr` et `client2.opendoor.fr`
 - emplacement des boîtes mails : `/srv/mail/NOM_DU_DOMAINE`
 - format maildir
 - distribution du courrier avec l'identité de l'utilisateur "facteur", à créer.
- Testez en envoyant un mail à l'attention de `augustine@client1.opendoor.fr` le mail doit arriver dans le dossier `/srv/mail/client1.opendoor.fr/augustine/new`

Postfix : utilisateurs virtuels avec ldap

- Qu'est-ce que LDAP ?
- Quels sont ses avantages et inconvénients ?
- Rajouter la directive *virtual_alias_maps* = ldap://etc/postfix/ldap_alias.cf
- *En vous basant sur https://www.postfix.org/LDAP_README.html#config, mettez au point le fichier ldap_alias.cf*
- Testez en envoyant un mail à l'attention de augustine@client1.opendoor.fr
- Vérifier dans les logs que le mail a été correctement distribué en utilisant le relay *virtual*

Dovecot

- dovecot peut faire office de :
 - MDA
 - MUA
 - MTA
- nom des paquets :
- 2 choses à faire une fois le paquet installé :
- Quel est le principal fichier de configuration ?
- Quels sont les ports d'écoute standard des protocoles POP et IMAP?

Intégration avec postfix

- Suivre la procédure décrite à la section "[Non-Postfix mailbox store: separate domains, non-UNIX accounts](https://www.cyrusimap.org/quickstart.html?highlight=postfix#install-postfix)", en vous aidant de la doc : "<https://www.cyrusimap.org/quickstart.html?highlight=postfix#install-postfix>"
- Testez et validez en envoyant un mail à `augustine@client1.opendoor.fr`

Dovecot

- Quelles directives permettent :
 - de définir l'emplacement des boîtes mail ?
 - De définir le compte utilisé pour distribuer le courrier
 - De définir la liste des dossiers automatiquement créés
 - De vérifier l'existence des boîtes utilisateurices
 - D'authentifier les utilisateurices
- Qui peut utiliser cette commande ?
- Quelle commande de cette interface permet d'afficher toutes les boîtes mails existantes.
- Quelle commande de cyradm permet de donner les droits de lecture (voir <https://www.cyrusimap.org/imap/reference/admin/access-control/combining-rights.html>)
- Créez une boîte mail pour client1@client1.opendoor.fr
- Dans quel répertoire se trouvent les boîtes mail ainsi créées ?

Coté client

- À ce stade, il est possible de configurer un client mail (thunderbird par exemple) se connectant sur notre serveur IMAP et utilisant notre service postfix pour l'envoi de mail.
- Récapitulatif des paramètres de connexion :
 - serveur entrant :
 - numéro de port :
 - utilisateur :
 - mot de passe :

Postfix : authentification SMTP

- Qu'est-ce qu'un *open-relay* ?
- Pourquoi, quand on est sur un réseau "free" ne peut-on pas utiliser les smtp de "orange" ?
- Donnez les n° des 2 lignes à décommenter dans `/etc/postfix/master.cf` pour que postfix écoute sur les ports 465 et 587 ?
- Implémentez les instructions décrites dans ce document : https://postfix.traduc.org/index.php/SASL_README.html#server_sasl
- Créer un compte utilisateur

SSL

- Installez et utiliser wireshark pour capturer le trafic réseau circulant entre le client et le serveur imap lors d'une connexion. Effrayant non ?
- Récupérez <https://formation.opendoor.fr/AUX120/certificates.tar> et décompressez l'archive dans le répertoire /etc/postfix/ssl
- Configurez vos serveurs postfix et cyrus pour qu'ils utilisent ces certificats.
- Recapturez le trafic avec wireshark, ça devrait être moins clair.
- Quel est le service communautaire permettant d'avoir des certificats SSL gratuits **ET** reconnus par les principaux navigateurs du marché ?

DKIM, SPF, DMARC

- À l'aide de votre moteur de recherche favori, définissez en 1 phrase chaque acronyme du titre :
 - SPF :
 - DKIM :
 - DMARC :
- Quel sont les serveurs mails légitimes du domaine opendoor.fr ?
- Quels sont les 5 premiers caractères de la clé utilisée pour signer les messages en provenance de opendoor.fr

La lutte contre le spam

- intégrer spamassassin
 - implémenter en suivant la doc suivante :
<https://blog.microlinux.fr/spamassassin-centos/#config-postfix>
 - Quel est le principe de fonctionnement de *spamassassin* ?
- greylisting
 - Quel est le principe de fonctionnement du greylisting ?
 - Implémentez en suivant <https://wiki.centos.org/HowTos/postgrey>
- Renfort des contrôles postfix (https://wiki.centos.org/HowTos/postfix_restrictions)

Exploitation

- **fetchmail**
- **imapsync**
- **mxttoolbox.com & Co**

(Web|Biblio)graphie

- [Bash Beginner Guide](#)
- [Vim tutorial](#)
- [Common administrative commands in Red Hat Enterprise Linux 5, 6, and 7](#)
- [RedHat 7 System Administrators guide](#)
- <https://wiki.centos.org/HowTos>
- [POSTFIX documentation](#)
- [Cyrus imapd quickstart](#)

Notes personnelles

Notes personnelles