TP3 : Installation d'un serveur mail

Prérequis : avoir votre serveur DNS configuré (cf TP1).

Partie I : Configuration d'un serveur mail

I.1. Envoi d'emails avec un Mail Transfert Agent / SMTP

1. L'envoi et l'acheminement des emails se fait par le protocole SMTP qui est mis en œuvre par un Mail Transfert Agent (MTA). Nous utiliserons pour cela le démon **postfix**. Installer les paquets **postfix** et **mailutils**. L'installation se termine par l'interface de configuration. En cas de problème, *sudo dpkg-reconfigure nompkg* permet de reconfigurer. Choisir la configuration « Site Internet ». Renseigner votre sous-domaine comme « nom de courrier ».

2. Les fichiers de configuration de **postfix** sont stockés dans /etc/postfix/, en particulier *main.cf*. Configurer « myhostname » avec le nom renseigné dans l'entrée MX de votre zone. Ajouter la ligne suivante à la fin du fichier : « home_mailbox = Maildir/ » . Elle permet de définir où sont stockés les messages reçus. Redémarrer **postfix** avec la commande **service**.

3. Remarque: notre domaine étant inconnu, l'email risque d'être considéré comme un spam par le serveur de destination. Par ailleurs, certains FAI filtrent l'envoi de mails (le protocole SMTP) pour éviter d'être une source de SPAM. Il faut alors spécifier le serveur SMTP du domaine comme « relay_host » dans le fichier de configuration de postfix.

4. Si ce n'est pas déjà fait, créer une entrée « MX » dans votre zone DNS qui servira à identifier votre serveur comme serveur mail de la zone.

I.2. Réception d'emails avec un Mail Delivery Agent / IMAP

1. La réception des emails entre le serveur et le client mail (par exemple Thunderbird) se fait par le protocole IMAP qui est mis en œuvre par un Mail Delivery Agent (MDA). Nous utiliserons pour cela le démon **dovecot-imapd**.

2. Installer le paquet **dovecot-imapd**. Lors de l'installation, créer un certificat auto-signé en renseignant votre sous-domaine comme « commonName ». Les fichiers de configuration de **dovecot** sont stockés dans /etc/dovecot/conf.d/. Indiquer le répertoire de stockage des emails dans le home avec la commande : *maildirmake.dovecot ~/Maildir/* , ou renseigner dans le fichier *10-mail.conf : mail_location = maildir:~/Maildir* . Activer l'écoute du port 143 dans le fichier *10-master.conf*, ainsi que l'authentification plain dans *10-auth.conf*.

I.3. Test du service avec un Mail User Agent

1. L'envoi et la relève du courrier par l'utilisateur se fait grâce à un Mail User Agent (MUA). Vérifier que l'envoi de messages fonctionne avec un agent en ligne de commande :

mail *username@domain* < *fichier_texte*

2. Vérifier avec Wireshark la transmission du courrier en clair via le protocole SMTP. L'email doit avoir été transmis dans le répertoire Maildir. Les erreurs éventuelles sont enregistrées dans un fichier de log : *sudo tail /var/log/mail.log* .

3. Installer un client de messagerie : *sudo apt-get install thunderbird* sur le client. Le configurer pour qu'il envoie et récupère les emails grâce à votre serveur mail. L'authentification reprend pour l'instant celle du système (*login* et *password* unix). Dovecot utilise STARTTLS par défaut. Tester l'envoi et la réception de messages entre binômes.

Partie II : Sécurisation du serveur mail

L'objectif de cette seconde partie et de permettre une connexion à distance sécurisée aux serveur mail. Postfix ne fournit pas de service d'authentification mais peut se reposer sur un autre existant. Dovecot fournit quant à lui un service d'authentification via SASL (http://wiki2.dovecot.org/HowTo/PostfixAndDovecotSASL) que nous allons utiliser pour notre serveur mail.

1. Dans le fichier *10-ssl.conf* de dovecot, écrire ssl = required et relancer dovecot. Vérifier que votre courrier est récupéré à travers une connexion chiffrée.

2. Activer Postfix smtp-auth dans le fichier *10-master.conf* de dovecot.

3. Dans Postfix maintenant, activer l'authentification par le service SASL de Dovecot :
   smtpd_sasl_auth_enable = yes
   smtpd_sasl_type = dovecot
   smtpd_sasl_path = private/auth
   Envoyer un nouveau courrier. Vérifier que la connexion au serveur SMTP nécessite une authentification. Avec wireshark, vérifier que l'envoi du courrier est bien chiffré par TLS.

4. Remarque : une autre façon de procéder est d'utiliser SMTP/IMAP au dessus de TLS plutôt que STARTTLS. Dans ce cas, il faut également changer les ports : IMAP avec TLS utilise le port 993 et SMTP avec TLS le port 145.

5. Le mécanisme d'authentification utilisé jusque ici est le plus simple possible (plain text) et repose sur les utilisateurs du système. Dovecot permet cependant d'utiliser d'autres modes d'authentification (http://wiki2.dovecot.org/Authentication) et d'autres bases de données d'utilisateurs. Installer un annuaire LDAP et configurer Dovecot pour interroger cet annuaire lors de l'authentification.

Partie III : Pour aller plus loin

Beaucoup d'autres services sont généralement nécessaires au bon fonctionnement d'un réseau d'entreprise et n'ont pas pu être abordés lors de ces travaux pratiques par manque de temps. Parmi ceux-ci, les services suivants sont très répandus et bénéficient également d'implantations libres et performantes :

1. L'authentification des utilisateurs avec **LDAP** et **Kerberos**
2. La configuration du réseau avec un serveur **DHCP**
3. La connexion sécurisée à distance avec **OpenVPN**
4. Le partage réseau avec **NFS**, et la sauvegarde avec **rsync**
5. L'interopérabilité Linux-Windows avec **Samba**
6. Le serveur d'impression **CUPS**

S'il reste du temps en fin de séance et si les exercices des séances précédentes sont terminés, profitez des droits root de la salle E1.22 pour expérimenter les services listés ci-dessus. Ubuntu étant la distribution installée dans cette salle, les portails suivants peuvent être utiles :

http://doc.ubuntu-fr.org/entreprise et http://doc.ubuntu-fr.org/administration
http://doc.ubuntu-fr.org/serveur et http://doc.ubuntu-fr.org/systeme
http://doc.ubuntu-fr.org/reseau