Postfix, administrer un serveur de messagerie

★★★★★

SII-336 **2 Jours (14 Heures)**

Description

Après un rappel sur le fonctionnement global d'une messagerie d'entreprise, vous apprendrez à administrer un serveur Postfix, à en configurer les différents composants, à sécuriser son exploitation et à l'intégrer avec les logiciels applicatifs de votre environnement.

À qui s'adresse cette formation ?

Pour qui

Ingénieur système, ou décideur ayant des compétences techniques, devant choisir et mettre en oeuvre une solution open source pour la distribution, l'archivage, et la sécurité du courrier.

Prérequis

Bonnes connaissances de l'administration Linux et des réseaux d'entreprise.

Les objectifs de la formation

- Installer un serveur Postfix
- Configurer les différents composants : pop3, imap, smtp
- Mettre en œuvre des mesures antispam
- Assurer l'exploitation : vérifier les logs, les statistiques

Programme de la formation

Principes fondamentaux

- ? Les agents de transfert de courrier
- Sendmail, la solution historique mais complexe.
- Les alternatives Postfix ou Qmail.
- Xmail, un serveur de messagerie très complet.
- ? Envoi, routage et réception d'un courrier
- Format d'une adresse de messagerie.
- Paramétrage de base d'un poste client.
- ? Les acteurs
- Transport et relais des messages avec un MTA.
- Les agents de distribution de courrier.
- Les serveurs de messagerie.
- Les agents de gestion de courrier.

Installation et configuration de Postfix

- ? Installation
- Tour d'horizon des dernières versions.
- ? Configuration
- Configuration du DNS pour le courrier électronique.
- Les principaux paramètres de master.
- cf et main.
- cf.
- La configuration minimale.
- Le relayage (client, serveur).
- ? Les tables de correspondance
- Les tables de recherche de Postfix.
- Exemple d'utilisation de LDAP et MySQL avec Postfix.

Maîtriser les protocoles

- ? SMTP (Simple Mail Transport Protocol)
- SMTP c'est aussi un format de message.
- Les balises (EHLO, MAIL FROM, RCPT TO, DATA.
-).
- Les codes erreur (destinataire inconnu, refus.
-).
- SMTP et sécurité : notion de relais ouvert/fermé.
- Tolérance par mot de passe ou adresse IP.
- Cryptage.
- ? Le routage du courrier
- Le cycle MUA/MTA/MTA/.
- /MTA/MDA puis .
- MUA.
- Les relais MX et les frontaux entrants/sortants.
- ? POP et IMAP
- Les balises POP3 (USER, PASS, STAT, DELE, TOP.
-).
- Chiffrement du mot de passe (MD5).
- Limites de POP3 et apports de IMAP.

Exploitation de Postfix

- ? Au quotidien
- Les files d'attente de Postfix.
- Les logs de Postfix (paramétrage de syslog).
- Disposer de statistiques (pflogsumm.
- pl).
- ? Pour aller plus loin
- Lancer Postfix en environnement "chroot".
- La remontée d'incidents (notify_classes, spam).
- » Un environnement à sécuriser ? Blocage de courrier non sollicité
- Les différentes formes de spam.
- Les risques encourus par un système mal configuré.
- ? Authentification
- Limites de SMTP, apports de SASL.
- Choix de la méthode d'authentification.
- ? Cryptage
- Garantir la confidentialité du courrier.
- Les certificats TLS (Transport Layer Security).