Stage pratique de 2 jour(s)
Réf : POF

Participants

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

Pré-requis

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

Dates des sessions

Modalités d'évaluation

L'évaluation des acquis se fait tout au long de la session au travers des multiples exercices à réaliser (50 à 70% du temps).

Compétences du formateur

Les experts qui animent la formation sont des spécialistes des matières abordées. Ils ont été validés par nos équipes pédagogiques tant sur le plan des connaissances métiers que sur celui de la pédagogie, et ce pour chaque cours qu'ils enseignent. Ils ont au minimum cinq à dix années d'expérience dans leur domaine et occupent ou ont occupé des postes à responsabilité en entreprise.

Moyens pédagogiques et techniques

• Les moyens pédagogiques et les méthodes d'enseignement utilisés sont principalement : aides audiovisuelles, documentation et support de cours, exercices pratiques d'application et corrigés des exercices pour les stages pratiques, études de cas ou présentation de cas réels pour les séminaires de formation.

• A l'issue de chaque stage ou séminaire, ORSYS fournit aux participants un questionnaire d'évaluation du cours qui est ensuite analysé par nos équipes pédagogiques.

• Une feuille d'émargement par demi-journée de présence est fournie en fin de formation

Postfix, administrer un serveur de messagerie

OBJECTIFS

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.

Travaux pratiques

Ils vous présenteront de manière progressive toutes les étapes, ainsi que les composants, nécessaires à la mise en oeuvre d'un serveur de messagerie "professionnel" (installation, exploitation, sécurité, antivirus, antispam, Webmail, logs, MySQL, LDAP...).

1) 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.

2) 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.

3) 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.

4) Exploitation de Postfix

Au quotidien

- Les files d'attente de Postfix.
- Les logs de Postfix (paramétrage de syslog).
- Disposer de statistiques (pflogsumm.pl).

ainsi qu'une attestation de fin de formation si le stagiaire a bien assisté à la totalité de la session.

Pour aller plus loin

- Lancer Postfix en environnement "chroot".
- La remontée d'incidents (notify_classes, spam).

5) 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).