acipia
Sécurité et Infrastructure Informatiques

Société : ACIPIA

Projet : Formations Intra-entreprise

Type de dossier : Catalogue

Référence dossier
Catalogue-formations-2018

Auteur : SM
Version : 1.0

Acipia
03 20 28 61 62
03 20 70 57 11
50 Grande Rue
59 100 Roubaix

Acipia Ouest
02 57 640 460
54 Rue du Grand Jardin
35 400 Saint-Malo

Sommaire

A PROPOS DES FORMATIONS ACIPIA

Afin de vous amener à une expertise et à une autonomie optimales sur les dernières technologies open source, Acipia fournit une gamme de **formations à haute valeur technologique**, portant sur plusieurs dizaines de scénarios et de solutions différents.

La **pédagogie Acipia** est basée sur un apprentissage à la fois théorique et pratique, où 50% du temps de formation est passée sur des mises en œuvre concrètes des enseignements dans des maquettes, pour une assimilation plus facile et plus efficace.

Acipia dispense ses formations exclusivement en intra-entreprise, c'est-à-dire en vos locaux. Dans ce fonctionnement, les scénarios sont adaptés à vos équipes et à vos projets, pour accroître encore la qualité de l'apprentissage et de l'assimilation.

Démarche pédagogique

Les prestations de formation dispensées par Acipia sont composées de 2 phases.

- **Préparation de la formation et rédaction du support pédagogique de la formation**
  Préalablement à chaque formation, le programme détaillé de la formation et des maquettes est établi conjointement avec vos équipes, afin de définir les éléments les plus importants pour vous, et d'adapter le scénario de la formation en conséquence.
  Concrètement, vous avez ainsi la possibilité de modifier et de remplacer certains points techniques du programme initial par d'autres éléments, généralement abordés dans d'autres formations du catalogue Acipia. Vous pouvez également allonger ou réduire la durée initiale de la formation, selon que vous souhaitez amplifier ou réduire certains points du programme.

- **Animation de la formation**
  Il s'agit de la phase de formation en elle-même, lors de laquelle le consultant formateur d'Acipia anime la formation et ses maquettes, en suivant le programme défini et détaillé dans le support de formation fourni.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

Infrastructure Réseau

Votre **infrastructure réseau** constitue le socle de votre production informatique. Elle est impliquée dans chaque échange de données, chaque communication. Ses performances et sa disponibilité ont un impact direct sur votre activité.

Dans cette optique, nous avons conçu une gamme de formations réseau dont le but est de vous rendre autonome dans la gestion de votre réseau, depuis sa conception et mise en oeuvre jusqu'à son exploitation, sa supervision et le troubleshoot.

FORMATION : INFRASTRUCTURE RÉSEAU

DR-151 : Concevoir et comprendre un réseau informatique (2 jours)

Matériels et logiciels utilisés

Linux, Windows, Wireshark

Présentation

Les réseaux informatiques occupent une place prépondérante dans les outils de production modernes. Une bonne conception amène un meilleur fonctionnement, et améliore la qualité du service fournit aux utilisateurs de manière globale, sur l'ensemble des applications.

Objectifs

Ce stage permet aux administrateurs réseaux et sécurité de concevoir un réseau informatique IP, et d'appréhender son fonctionnement. Le câblage, le plan d'adressage IP, les mécanismes de commutation, de filtrage et de routage sont notamment étudiés.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Notions sur Ethernet, IP et TCP.

Programme

JOUR 1 – Les réseaux ethernet et IP

Principes
- Rappel sur le modèle OSI
- Evolution des réseaux
- Les normes principales
- Les mécanismes de liaison

Ethernet
- Rôle et fonctionnement des réseaux filaires
- Les principaux constructeurs et équipements concernés

IP
- Rôle et fonctionnement
- Commutation et routage

JOUR 2 – Concevoir son réseau

Particularités des interfaces réseaux Wifi
Les normes principales

Sécurité
- Rôle et fonctionnement d'un firewall
- Principe du filtrage
- Les autres équipements de protection (proxy, IDS IPS …)
- L'authentification et le chiffrement

Maquette
- Conception d'un réseau multi-sites
- Analyse d'une communication HTTP avec Wireshark

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE RÉSEAU

DR-152 : Installer et administrer un réseau Cisco (2 jours)

Matériels et logiciels utilisés

Commutateurs Cisco 2960 Series, routeur Cisco 800 Series

Présentation

Cisco est l'équipementier leader des réseaux informatiques d'entreprise. Avec un R&D et des équipements particulièrement fonctionnels et performants, Cisco est à l'origine d'un grand nombre de protocoles et de normes aujourd'hui utilisés dans tous les réseaux. Cette formation s'intéresse aux commutateurs et aux routeurs de la gamme.

Objectifs

Ce stage permet aux administrateurs réseaux et sécurité d'installer, de configurer et de maintenir les commutateurs et les routeurs Cisco. Les fonctions de commutation, de VLAN, de spanning tree et de routage statique sont abordées. La prise en main et l'utilisation du CLI (Command Line Interface) sont également présentées.

Public Concerné

Administrateur réseaux / sécurité

Compétences nécessaires

Notions sur Ethernet, IP et TCP.

Programme

JOUR 1 – Commutation et routage avec Cisco

Rappel sur les réseaux IP
- Rappel sur le modèle OSI
- Evolution des réseaux
- Les normes principales
- Les mécanismes de liaison

Les équipements Cisco
- Les principaux équipements
- Architecture matérielle et logicielle
- Présentation de l'IOS

Configuration en CLI
- Rôle et fonctionnement
- Commutation et routage

JOUR 2 – Maquette

Prise en main du CLI
- Connexion en console, telnet et SSH
- Mise en réseau et configuration IP
- Mise en réseau d'un commutateur et d'un routeur avec VLANs et routage statique

Mise en réseau de plusieurs équipements
- Utilisation des stacks et des liens uplink
- Compréhension et utilisation d'un réseau hautement disponible : spanning tree, uplink fast, etc ...
- Supervision SNMP et troubleshoot des logs

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE RÉSEAU

DR-153 : Concevoir et comprendre un réseau IPv6 (2 jours)

Matériels et logiciels utilisés

Linux, Windows, Cisco

Présentation

Malgré 4,3 milliards d'adresses différentes, il n'existe plus d'adresses IP non attribuées. La dernière version du protocole le plus utilisé dans le monde, IPv6, règle ce problème mondial et devient incontournable. Pour autant, les intérêt d'IPv6, son fonctionnement et ses différences avec IPv4 sont encore méconnues. Avant d'appréhender une éventuelle migration, ces sujets doivent être appréhendés. C'est ce qui est proposé dans cette formation.

Objectifs

Ce stage permet aux administrateurs réseau de comprendre le protocole IPv6, en identifiant les bénéfices et les difficultés d'une migration éventuelle dans leur situation. Le fonctionnement du protocole et ses différences avec IPv4 sont largement abordés.

Public Concerné

Administrateurs réseaux/sécurité

Compétences nécessaires

Bonne compréhension des réseaux IPv4

Programme

JOUR 1 – Internet Protocol Version 6

Introduction et contexte
- Rappel sur IPv4 et présentation du contexte
- Etat des lieux des réseaux IP mondiaux
- Rôle et position des constructeurs / opérateurs

Présentation de IPv6
- Convention et notation
- Fonctionnement

IPv6 vs IPv4
- Principales différences entre les versions
- Intérêt et bénéficies d'IPv6
- Dois-je migrer ?

Préparer une migration
- Quels sont les impacts ?
- Tous les réseaux et OS sont-ils compatibles ?
- Comment se préparer ?

JOUR 2 – Déploiement et configuration

Les évolutions
- ICMPv6
- ARP / NDP
- Multicast
- QoS
- DNSv6
- Les tunnels Ipv4 / IPv6
- Les mécanismes d'auto-configuration IPv6

Maquette (Linux / Windows)
- Déploiement d'un réseau Ipv6 avec postes Linux et Windows
- Tests de connectivité, routage
- Auto-configuration
- Configuration d'autres équipements (firewall, cisco)

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE RÉSEAU

DS-123 : Utiliser Wireshark *(2 jours)*

Logiciels utilisés

Linux, Microsoft Windows, Wireshark, tcpdump, lib pcap

Présentation

Wireshark (anciennement Ethereal) est un puissant outil d'analyse de trafic réseau. Il déchiffre automatiquement la plupart des protocoles réseaux pour afficher lisiblement les en-têtes et contenu des trames Ethernet.. Il permet à un administrateur système et réseau de diagnostiquer tout problème réseau : lenteur applicative, perte de paquet.

Objectifs

Ce stage permet aux administrateurs réseaux et sécurité d'acquérir les bases pour utiliser efficacement l'outil d'analyse réseau Wireshark. En partant de la capture des trames jusqu'au filtrage des paquets, les stagiaires seront capable d'identifier rapidement la cause du problème rencontré.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Modèle OSI
Protocole Ethernet
Routage
Protocoles niveau 7

Programme

JOUR 1 – Théorie et captures simples

Principes
- Sniffing, méthode de capture des paquets
- Le mode Promiscous
- Capture locale
- Capture distante

Interface Graphique
- Navigation
- Options

Maquette
- Installation
- Analyse de flux

JOUR 2 – Utiliser les options avancées

Particularités des interfaces réseaux Wifi

Options d'affichage
- Filtres de sélection des paquets
- Coloration

Outils d'analyse
- Suivre un flux TCP
- Statistiques sur les données
- Graphiques de flux

Maquette
- Suivre une communication HTTP
- Afficher la bande passante consommée

Le programme ci-dessus présente le programme initial de la formation DS-123 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

Infrastructure Système

Les outils qui sont abordés dans les formations « Infrastructure système » concernent l'architecture des Systèmes d'Information. Chaque composant d'infrastructure est abordé sous son aspect théorique puis au travers d'un logiciel dédié à cette tâche. Le but de ces stages est d'être capable de déployer les composants majeurs d'un Système d'Information comme un serveur DNS, un relais de messagerie ou encore un serveur Web.

Les outils étudiés sont des « **logiciels libres** » dans leur très grande majorité. Ils permettent un déploiement aisé et peu coûteux sur tous types d'architecture. Certains de ces logiciels sont leaders sur leur segment. C'est par exemple le cas d'Apache qui détient 68% du marché des serveurs Web.

redhat ADVANCED PARTNER

FORMATION : INFRASTRUCTURE SYSTÈME

DI-101a : Installation et prise en main d'un système GNU/Linux *(2 jours)*

Logiciels utilisés

Une distribution GNU/Linux: Red Hat Enterprise Linux ou Debian

Présentation

Le noyau Linux est aujourd'hui le logiciel libre le plus connu et le plus répandu. Couplé au système GNU, il constitue une base fiable et robuste pour le déploiement d'applications critiques ou équiper votre infrastructure informatique (firewall, proxy, serveur de messagerie ...). Ce stage permet l'assimilation des notions essentielles à son déploiement et son exploitation .

Objectifs

Cette formation a pour but principal la découverte du noyau Linux en tant que base du système d'exploitation GNU. L'organisation du stage laisse une grande part à la pratique. Les maquettes permettront une mise en oeuvre immédiate des concepts étudiés.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un autre OS (Windows NT par exemple)

Bases techniques en administration système et réseau

Programme

JOUR 1

Principes
- Qu'est ce qu'un système d'exploitation
- L'histoire du noyau Linux
- Le système GNU

Le système de fichiers
- La couche d'abstraction
- Les différents filesystems
- Les permissions

Maquette – Préparation de l'installation
- Trouver le logiciel
- Gérer le matériel
- Utiliser l'éditeur de texte VI

JOUR 2

Maquette – Installation
- Installation complète du système
- Premier démarrage

Prendre la main
- Les différents shells
- Commandes usuelles
- Vérifier l'état physique du système
- Explorer les logs
- Quelques opérations courantes

Maintenir le système à jour
- Mises à jour de sécurité
- Mettre à jour le noyau

Le programme ci-dessus présente le programme initial de la formation DI-101a d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-101b : Administration d'un système GNU/Linux *(2 jours)*

Logiciels utilisés

Une distribution GNU/Linux: RedHat, Mandrake, Debian, ...

Présentation

Le noyau Linux est aujourd'hui le logiciel libre le plus connu et le plus répandu. Couplé au système GNU, il constitue une base fiable et robuste pour le déploiement d'applications critiques (firewall, proxy, serveur de messagerie ...). Ce stage permet l'assimilation des notions essentielles à son déploiement et son exploitation .

Objectifs

Cette formation permet de comprendre comment gérer avec efficacité des machines exploitées par un système GNU/Linux. Les enseignements sont complétés par des exemples pratiques sur machines. Les services les plus courants sous Linux sont abordés: serveur Web, routeur filtrant, proxy HTTP, ...

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation d'un système GNU/Linux (DI101a)

Bases techniques en système et réseau

Programme

JOUR 1

Principes importants
- Gérer les utilisateurs
- Gérer les permissions
- Surveiller les logs

Installation d'outils
- Par package
- Depuis les sources (patchs éventuels)
- Méthodes hybrides

Outils d'administration système
- Syslog
- Crontab
- Manipuler les disques et partitions

Surveiller les points vitaux d'une machine
- Localement
- A distance via SNMP

JOUR 2

Maquette avec quelques services
- Accès distant en SSH
- Routage/filtrage
- Serveur FTP
- Serveur SAMBA (SMB)
- Serveur Apache (HTTP) avec PHP
- Serveur MySQL (SGBD)

Adapter le noyau Linux
- Configurer un noyau à chaud
- Configurer et compiler un noyau « vanilla »
- « Patcher » un noyau « vanilla »

Quelques fonctionnalités avancées
- Agrégation de liens pour double attachement
- VRRP et heartbeat
- Filtrage niveau 7

Le programme ci-dessus présente le programme initial de la formation DI-101b d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-111a : Comprendre le protocole HTTP et utiliser Apache *(2 jours)*

Logiciels utilisés

Apache HTTP Server sur Linux

Présentation

Un serveur HTTP constitue le coeur d'un serveur de sites Web. Apache est le plus connu et le plus répandu d'entre eux avec plus de 68% de parts de marché. Ce chiffre tient tant à sa gratuité d'utilisation qu'à ses qualités propres : sécurité, performances et modularité.

Objectifs

Ce stage présente le projet Apache à des administrateurs systèmes et réseaux déjà familiarisés avec le système Linux. Le but est de parvenir à une complète autonomie sur la mise en place de plate-forme Web sécurisées et modulaires. La grande part prise par les maquettes permet aux stagiaires une assimilation totale des notions abordées.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Programme

JOUR 1

Principes
- Utilité d'un serveur HTTP
- Le projet Apache
- Historique d'Apache HTTP Server

Maquette - Installation
- Trouver le logiciel
- Installation par paquetages
- Configuration initiale
- Vérification du bon fonctionnement

Exploiter Apache
- Vérifier les ressources utilisées
- Configurer et surveiller les logs
- Superviser l'activité HTTP (voir DE-111)

JOUR 2

les virtualhosts
- Rappel sur HTTP
- Intérêt des virtualhosts
- Configuration et exemple

Configurer Apache
- Le mod_core
- Configuration TCP/IP
- Permissions
- SSL et certificats
- Créer des logs personnalisés

Architecture CGI – exemple

Troubleshoot des applications HTTP

Le programme ci-dessus présente le programme initial de la formation DI-111a d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-111b : Administration avancée et sécurisation d'Apache *(2 jours)*

Logiciels utilisés

Apache HTTP Server sur Linux

Présentation

Un serveur HTTP constitue le coeur d'un serveur de sites Web. Apache est le plus connu et le plus répandu d'entre eux avec plus de 68% de parts de marché. Ce chiffre tient tant à sa gratuité d'utilisation qu'à ses qualités propres : sécurité, performances et modularité.

Objectifs

Les administrateurs familiarisés au serveur HTTP Apache découvriront ici les possibilités offertes par ce logiciel libre. Apache dispose de nombreuses extensions qui se révèlent très intéressantes pour l'exploitation de serveurs de production. Les stagiaires pourront ensuite déployer des architectures évoluées basées sur Apache et notamment héberger des applications PHP.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Installation et configuration basique d'un serveur Apache (DI-111a)

Programme

JOUR 1

Rappels sur Apache
- Le protocole HTTP
- Architecture HTTP/CGI
- Les modules existants

Maquette
- Optimiser un serveur Apache
  - Mesurer les résultats
- Authentification
- Négociation dynamique

JOUR 2

Hébergement mutualisé
- Configuration par mod_userdir
- Configuration par VirtualHosts
- Permissions sur le filesystem

Maquette sur les modules d'Apache
- Ré-écriture d'url
- User tracking
- Expires / Headers

Extension d'Apache avec PHP (voir DI-112)
- Installation/Configuration
- Quelques scripts
- Adaptation à un hébergement mutualisé

Le programme ci-dessus présente le programme initial de la formation DI-111b d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-112 : Serveur d'applications PHP *(1 jour)*

Logiciels utilisés

Moteur applicatif PHP (Pre Hypertext Processor)

Présentation

PHP est une plate-forme de développement dédié aux applications relatives à Internet. PHP est clairement un outil de premier plan et on ne compte plus les plates-formes de premier plan qui ont choisi PHP, à commencer par facebook. PHP s'est imposé dans le monde des applications métiers et de l'Internet professionnel.

Objectifs

Ce module a pour objectif d'étendre les compétences d'administrateurs de serveurs Web. Ils découvriront comment installer et configurer leurs serveurs pour pouvoir déployer des applications développées en PHP. Ce stage approfondit également les notions relatives à la sécurité, aux performances et à l'hébergement mutualisé de sites Web.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Installation et configuration d'un serveur Apache (DI-111a et éventuellement DI-111b)

Programme

JOUR 1

Rappels sur l'architecture HTTP/CGI

Présentation de PHP
- Positionnement technique
- Historique
- Comparatif avec Perl/JSP/ASP

Maquette- Déployer PHP
- A partir de paquetages
- A partir des sources
- Architecture en module et en CGI

Configuration de PHP
- Les modules de PHP
- Sécurité en dédié / en mutualisé
- Maintenir PHP à jour

Les bibliothèques annexes : PEAR ...

Gérer les performances d'un serveur Apache/PHP

Maquette interconnexion
- avec MySQL (DI-113a) ou
- avec PostgreSQL (DI-113b)

Le programme ci-dessus présente le programme initial de la formation DI-112 d'une durée d'une journée. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-113a : Administration du serveur et des bases de données MySQL *(2 jours)*

Logiciels utilisés

Serveur de base de données MySQL

Présentation

MySQL est un serveur de base de données solide et fiable. Il dispose de la plupart des fonctionnalités nécessaires à l'exploitation de base de données relationnelles. Grâce à des performances exceptionnelles, MySQL est particulièrement adapté au stockage de données destinées à des sites Internet.

Objectifs

Le stage permet à des administrateurs expérimentés d'acquérir les compétences nécessaires à la mise en place de serveurs de bases de données MySQL. Les aspects les plus évolués seront abordés comme le fonctionnement en redondance, l'optimisation des performances ou encore la récupération sur incident.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Bonnes connaissances des bases de données relationnelles et du langage SQL (DD-111)

Programme

JOUR 1

Rappels sur les SGBD relationnelles et le SQL

Présentation de MySQL
- Positionnement technique
- Historique
- Comparatif avec SQL Server, Oracle et pgSQL

Maquette – Déployer MySQL
- A partir de paquetages
- A partir des sources

Maquette – Administration
- Création de bases de données
- Définition des permissions
- Surveillance de l'activité

JOUR 2

Les clients pour MySQL
- Ligne de commande
- Maquette avec PHP (voir DI-112)
- Bibliothèques C, C++, java ...

Fonctionnalités avancées
- Procédures stockées
- Backup/Restore à chaud
- Index fulltext

Les performances de MySQL

MySQL en redondance
- Création d'une grappe de serveurs
- Mode de réplication
- Bascule sur incident

Le programme ci-dessus présente le programme initial de la formation DI-113a d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-113b : Administration du serveur et des bases de données PostgreSQL *(2 jours)*

Logiciels utilisés

Serveur de base de données PostgreSQL

Présentation

PostgreSQL est le serveur de bases de données libre le plus abouti fonctionnellement. Il dispose de la majorité des outils et technologies que l'on peut trouver dans les produits leaders comme Oracle ou DB2. Doté d'une structure solide et complète, PostgreSQL permet le déploiement d'applications complexes et performantes.

Objectifs

Le stage permet à des administrateurs expérimentés d'acquérir les compétences nécessaires à la mise en place de serveurs de bases de données PostgreSQL. Les aspects les plus évolués seront abordés comme les procédures stockées, l'écriture d'extension en C, les notions objet ou encore les classes polymorphes.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Bonnes connaissances des bases de données relationnelles et du langage SQL (DD-111)

Programme

JOUR 1	JOUR 2
Rappels sur les SGBD relationnelles et le SQL Présentation de PostgreSQL ● Positionnement technique ● Historique ● Comparatif avec SQL Server/Oracle/MySQL ... Maquette – Déployer PostgreSQL ● A partir de paquetages ● A partir des sources Maquette – Administration ● Création de bases de données ● Définition des permissions ● Surveillance de l'activité	Les clients pour PostgreSQL ● Ligne de commande ● Maquette avec PHP (voir DI-112) ● Bibliothèques C, C++, java ... Fonctionnalités avancées ● Procédures stockées ● Backup/Restore à chaud ● MCD et notions objets Écriture de procédures stockées en C Classes polymorphes et héritage

Le programme ci-dessus présente le programme initial de la formation DI-113b d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-121a : Serveur SMTP avec Postfix *(2 jours)*

Logiciels utilisés

Serveur SMTP Postfix

Présentation

Deux tiers des messages électroniques échangés aujourd'hui passent au moins une fois par un relais SMTP basé sur un logiciel libre. Postfix est l'un d'eux. Il s'agit d'un serveur extrêmement robuste, fiable et performant. Il peut être couplé à d'autres produits à forte valeur ajoutée comme des solutions antivirus et antispam.

Objectifs

Ce premier module sur Postfix aborde les notions théoriques essentielles à une bonne compréhension des architectures de messagerie. Les interactions avec les hiérarchies DNS et le protocole SMTP sont mis en avant. Une partie pratique concerne l'installation d'un serveur Postfix complet sur un OS Linux.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Bonnes connaissances des réseaux TCP/IP

Programme

JOUR 1

Rappels sur la messagerie électronique
- le protocole SMTP
- les différents noeuds
- interaction avec DNS

Présentation de Postfix
- Positionnement technique
- Historique
- Comparatif avec Sendmail, Exim,...

Maquette – Déployer Postfix
- A partir de paquetages
- A partir des sources

Maquette – Administration
- Configuration initiale
- Surveillance des logs
- Validation du fonctionnement

JOUR 2

Les composants de Postfix
- Les différents processus
- Les transports

Positionnement de Postfix
- en relais entrant
- en relais sortant
- en serveur final

Création de boîtes pour des utilisateurs locaux
- format mbox / format Maildir

Opérations supplémentaires
- Création d'alias et de listes
- Gestion de quotas
- Vérification du protocole SMTP
- Configuration sécurisée

Le programme ci-dessus présente le programme initial de la formation DI-121a d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-121b : Serveur SMTP avancé avec Postfix *(2 jours)*

Logiciels utilisés

Serveur SMTP Postfix – Logiciels connexes OpenLDAP, MySQL, Amavis, ClamAV et Spam Assassin

Présentation

Deux tiers des messages électroniques échangés aujourd'hui passent au moins une fois par un relais SMTP basé sur un logiciel libre. Postfix est l'un d'eux. Il s'agit d'un serveur extrêmement robuste, fiable et performant. Il peut être couplé à d'autres produits à forte valeur ajoutée comme des solutions antivirus et antispam.

Objectifs

Ce second module sur Postfix aborde les thèmes les plus poussés de ce serveur SMTP. Ainsi l'hébergement de domaines virtuels, la centralisation de la base utilisateur ou encore l'authentification SMTP sont couverts. La maquette mettra en avant l'administration avancée de la queue de message ainsi que l'adjonction de modules tiers comme spam assassin ou clamAV.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Installation d'un serveur SMTP avec Postfix (DI-121a)

Programme

JOUR 1

Virtual hosting
- Hébergement de domaines multiples
- Virtual mailbox

Centralisation de la base de données
- Utilisation d'un annuaire LDAP
- Utilisation d'une base MySQL

Maquette – Postfix + OpenLDAP
- Configuration du schéma LDAP
- Intégration de données
- Configuration de Postfix
- Tests

JOUR 2

Vérification du contenu
- Configuration de Postfix en back-to-back
- Amavis et ClamAV (antivirus)
- Amavis et Spam Assassin (antispam)

Maquette Postfix + Amavis + ClamAV + SA

Fonctionnalités avancées
- Authentification sur SMTP
- SMTP over TLS/SSL
- Gestion de la queue et des performances
- Troubleshooting

Le programme ci-dessus présente le programme initial de la formation DI-121b d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-131 : Déployer un serveur DNS *(2 jours)*

Logiciels utilisés

ISC **Bind Server** sur système GNU/Linux

Présentation

Bind est l'implémentation du protocole DNS le plus répandu. Ce protocole est désormais indissociable des réseaux IP et des services associés. Développé par l'Internet Software Consortium (ISC), Bind équipe la majorité des serveurs DNS publics. Ce module permet d'acquérir les connaissances nécessaires au déploiement et à l'administration de tels serveurs DNS, qu'il soit à usage interne ou externe.

Objectifs

Ce stage permet la découverte de l'implémentation libre du protocole DNS au travers du serveur Bind. Après une présentation de l'architecture DNS et son implication dans les réseaux IP, les stagiaires réaliseront une maquette complète d'une telle architecture. Les mécanismes plus poussés offerts par Bind seront également abordés : mise à jour automatique, chiffrement, délégation, partage de charge ...

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Bonnes connaissances des réseaux TCP/IP

Programme

JOUR 1

Présentation de Domain Name Server (DNS)
- Le protocole DNS
- Hiérarchie DNS
- Clients, servers et resolvers

Le logiciel ISC Bind
- Historique
- Positionnement technique
- Plate-formes supportées

Maquette installation
- A partir de paquetages
- A partir des sources

Configuration initiale

JOUR 2

Les différentes zones
- La zone racine
- Les zones d'autorité (master/slave)
- Les zones déléguées

Maquette générale – Internet
- Les « root servers »
- Les serveurs autoritaires
- Les resolvers
- Les clients

Fonctionnalités avancées
- Synchronisation
- Update par le client / par DHCP
- Chiffrement / Authentification

Le programme ci-dessus présente le programme initial de la formation DI-131 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-131b : Administration DNS avancée et sécurité *(3 jours)*

Logiciels utilisés

ISC **Bind Server** sur système GNU/Linux

Présentation

Bind est l'implémentation du protocole DNS le plus répandu. Ce protocole est désormais indissociable des réseaux IP et des services associés. Développé par l'Internet Software Consortium (ISC), Bind équipe la majorité des serveurs DNS publics. Ce module permet d'acquérir les connaissances nécessaires au déploiement et à l'administration de tels serveurs DNS, qu'il soit à usage interne ou externe.
Cette formation complète la formation DI-131 (Déployer un serveur DNS) en traitant de la messagerie, de la sécurité, du partage de charge, ...

Objectifs

Ce stage permet la découverte de l'implémentation libre du protocole DNS au travers du serveur Bind. Après une présentation de l'architecture DNS et son implication dans les réseaux IP, les stagiaires réaliseront une maquette complète d'une telle architecture. Les mécanismes plus poussés offerts par Bind seront également abordés : mise à jour automatique, chiffrement, délégation, partage de charge, messagerie, sécurité avancée, ...

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)
Bonnes connaissances des réseaux TCP/IP

Programme

JOUR 1

DNS et la messagerie
- Les pointeurs MX
- Les enregistrements inverses (PTR)
- DNS et les protections Antispam
- DNS et les blacklists (RBL)
- Le "Sender Policy Framework" (SPF) et « sender-id »

Sécurisation d'une installation DNS
- Connaître les principales failles et erreurs de configuration
- Étude de la faille de Juillet 2008
- Tester la sécurité d'un serveur
- Récursivité, transfert de zone
- Utilisation des « vues »

JOUR 2

Maquette générale :

Utilisation de DNSSEC
- Présentation du mécanisme
- Impacts sur la sécurité du protocole DNS
- Mise en oeuvre avec Bind

Sécurisation d'une installation DNS
- Redondance
- Sécurisation
- Tests

JOUR 3

Load-balancing avec DNS
- Partage de charge entre serveurs DNS
- DNS pour répartir la charge entre serveurs HTTP
- Les enregistrements SRV

Multicast DNS
- Présentation du mécanisme
- Implémentations Avahi, Bonjour et Zeroconf
- Active Directory et DNS

Maquette

Le programme ci-dessus présente le programme initial de la formation DI-131b d'une durée de 3 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin. Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-132 : Déployer un serveur NNTP *(1 jour)*

Logiciels utilisés

ISC INN Server sur système GNU/Linux

Présentation

INN est l'implémentation du protocole NNTP le plus répandu. Développé par l'Internet Software Consortium (ISC), INN équipe la majorité des serveurs NNTP publics. Ce module permet d'acquérir les connaissances nécessaires au déploiement et à l'administration de tels serveurs, qu'il soit à usage interne ou externe.

Objectifs

Ce stage permet la découverte de l'implémentation libre du protocole NNTP au travers du serveur INN. Après une présentation de l'architecture NNTP, les stagiaires réaliseront une maquette d'installation d'un serveur INN.

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Bonnes connaissances des réseaux TCP/IP

Programme

JOUR 1

Présentation du Network News Transport Protocol
- Le protocole NNTP
- Hiérarchie des serveurs de news
- Clients, local servers et feed servers

Le logiciel ISC INN
- Historique
- Positionnement technique
- Plateformes supportées

Maquette installation
- A partir de paquetages
- A partir des sources

Configuration initiale

Le programme ci-dessus présente le programme initial de la formation DI-132 d'une durée d'une journée. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-134 : Administration d'un annuaire LDAP avec OPENLDAP *(2 jours)*

Logiciels utilisés

Linux, OpenLDAP

Présentation

OpenLDAP est le serveur d'annuaire Opensource le plus utilisé dans les réseaux d'entreprise, des FAI et des opérateurs. Ses performances, son interopérabilité, sa robustesse et sa grande fiabilité en font un logiciel de choix pour les projets d'annuaire, d'identity management, de sécurité et d'authentification.

Au delà du rôle d'annuaire, il est un élément essentiel d'une infrastructure, où il occupe les fonctions d'authentification centralisée, d'accounting et de gestion des droits.

Objectifs

Ce stage permet aux administrateurs réseau, système et sécurité de connaître le rôle et le fonctionnement d'un serveur d'annuaire et de maîtriser le procotole LDAP et le serveur OpenLDAP

Public Concerné

Administrateurs réseau, système ou sécurité

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Programme

Introduction
- Présentation
- Fonctionnalités
- Installation et configuration de base

Utilisation du registrar SIP
- Notion de registrar
- Implémentation
- Création des comptes téléphoniques et du 'dialplan'

Enregistrements SRV
- Communication entre domaines
- Création de DNS et configuration Asterisk
- Mise en œuvre et tests

Plan de numérotation
- Définitions : contextes, applications
- Configuration /etc/asterisk/extensions.conf
- Syntaxe générale
- Contextes
- Extensions
- Priorités
- Configuration des Applications
- Dial(), Record(), CDR (Call Details Record)
- Syntaxe détaillée
- Les opérateurs
- Les expressions
- Les motifs
- Les branchements conditionnels
- Les fonctions et macros

Fonctionnalités supplémentaires
- Mail-to-Fax / Fax-to-Mail
- Serveur Vocal Interactif (SVI)
- Couplage Téléphonie-Informatique (CTI)
- G722 (son haute définition)

Le programme ci-dessus présente le programme initial de la formation DI-133 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : INFRASTRUCTURE SYSTÈME

DI-141 : Orchestration avec Puppet *(2 jours)*

Matériels et logiciels utilisés

Linux, Puppet 4 – Version Opensource

Présentation

La gestion quotidienne d'un parc de serveurs est une activité délicate et chronophage. Afin de fiabiliser les déploiements et **la gestion du changement** il est nécessaire d'industrialiser les procédures. Cette phase commence par une bonne conception, un choix judicieux des composants et une tenue stricte des documentations. Mais au-delà d'une dizaine de serveurs, l'automatisation devient nécessaire pour garantir la conformité des opérations. Puppet est la solution de référence **pour l'orchestration de la gestion des configurations système**.

Objectifs

Ce stage permet aux administrateurs système de découvrir **Puppet** (v4) et son puissant langage de configuration. La formation repose dans un premier temps sur l'usage de modules existants et sur leur déploiement au sein d'un architecture de grande envergure à l'aide du **Puppet Server** (v2.6). Ensuite le développement de modules personnalisés est abordé pour permettre de couvrir les besoins les plus spécifiques.

Public Concerné

Administrateur système, réseau et sécurité

Compétences nécessaires

Notions sur le chiffrement SSL/TLS.
Bases en système Unix : édition de fichiers, démarrage de processus.

Programme

JOUR 1 – Puppet et son environnement

Principes
- L'agent Puppet
- Programmation déclarative
- Le Puppet Server
- Hiera / Facter

Modules Puppet
- Modules apt, ntp, rpm etc
- Modules spécifiques
- La forge Puppet

Maquette en mode autonome
- Installation de Puppet
- Définition d'une configuration
- Mode « apply »

JOUR 2 – Puppet en environnements larges

Maquette en mode « Server »
- Installation du « server » et de PuppetDB
- Enrôlement des agents
- Contrôle de l'activité de Puppet

Séparer les variables avec Hiera
- Présentation de Hiera
- Créer une hierarchie de configuration
- Déclarer les IDP

Créer des modules personnalisés
- Création d'un module vierge
- Déclaration de ressources
- Le langage Puppet

Base PuppetDB
- Stocker les données collectées par Puppet
- Analyser et présenter les données

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

Supervision des Systèmes d'Information

Les formations relatives à l'exploitation concernent les administrateurs de systèmes informatiques et réseaux. Elles permettent d'acquérir les compétences nécessaires à l'amélioration de l'exploitation des Systèmes d'Information. Sont notamment regroupés dans ce domaine la **supervision** et le **reporting** d'activité des équipements.

Les outils étudiés sont des « **logiciels libres** » dans leur très grande majorité. Ils permettent un déploiement aisé et peu coûteux sur tous types d'architecture.

FORMATION : SUPERVISION

DE-101 : Supervision consolidée *(2 jours)*

Logiciels utilisés

MRTG/Cacti sous environnement GNU/Linux

Présentation

Les contraintes de production des infrastructures informatiques obligent les décideurs à mettre en place des solutions de supervision fiables. Il faut disposer d'une visibilité complète sur l'architecture. La création de rapports détaillés quant à la disponibilité et à la charge de chaque équipement permet d'anticiper les évolutions.

Objectifs

Cette formation permet d'acquérir les compétences nécessaires à la supervision complète d'un SI. Les stagiaires découvriront notamment comment définir les indicateurs pertinents par famille d'équipement ainsi que les méthodes pour leur récupération et leur mise en forme.

Public Concerné

Administrateurs système ou réseaux soucieux de mettre en place des outils de surveillance de leurs infrastructures techniques.

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Installation et administration d'un système GNU/Linux (ref: DI-101)

Programme

JOUR 1 - Techniques de monitoring

Commun DE-101/DE-102

Qualifier l'état d'une architecture
- Indicateurs de disponibilité
- Indicateurs de charge

Le protocole SNMP
- Organisation
- Structure
- Déploiement

Mise en œuvre
- Définir les indicateurs pertinents
- Collecter les données (push / pull)
- Agréger les données

JOUR 2 - Supervision consolidée

Maquette avec MRTG/Cacti
- Installation
- Configuration initiale

Création de rapports de charge
- pour routeurs
- pour commutateurs
- pour serveurs

Supervision personnalisée
- Définir des indicateurs complexes
- Collecter et agréger ces indicateurs
- Produire des rapports adéquats

Superviser des serveurs applicatifs
- Serveur de messagerie
- Serveur de fichiers
- Serveur proxy

Le programme ci-dessus présente le programme initial de la formation DE-101 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SUPERVISION

DE-102 : Monitoring temps-réel *(2 jours)*

Logiciels utilisés

Nagios sous environnement GNU/Linux

Présentation

Afin d'améliorer la disponibilité du Système d'Information. Différents outils de supervision ont été développés. Certains d'entre eux sont spécialisés dans le monitoring « temps-réel » qui permet de surveiller en permanence les éléments critiques du SI. Ainsi, même lorsque la panne d'un composant n'est pas immédiatement critique (grâce à la redondance par exemple), les équipes techniques peuvent être informées instantanément par différents moyens : mails, console visuelle, SMS ...

Objectifs

Ce stage a pour but la découverte et la prise en main de l'outil libre Nagios. Ce dernier permet une grande diversité de test réseau et applicatif. Les stagiaires découvriront comment mettre en place et exploiter Nagios dans un environnement de production.

Public Concerné

Administrateurs système ou réseaux soucieux de mettre en place des outils de surveillance de leurs infrastructures techniques.

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Installation et administration d'un système GNU/Linux (ref: DI-101)

Programme

JOUR 1 – Techniques de monitoring

Commun DE-101/DE-102

Qualifier l'état d'une architecture
- Indicateurs de disponibilité
- Indicateurs de charge

Le protocole SNMP
- Organisation
- Structure
- Déploiement

Mise en œuvre
- Définir les indicateurs pertinents
- Collecter les données (push / pull)
- Agréger les données

JOUR 2 - Monitoring temps-réel

Maquette avec Nagios
- Installation
- Configuration initiale

Création d'un rapport réseau/système
- Supervision de routeurs
- Supervision de commutateurs
- Supervision de liens (Internet ...)
- Supervision de serveurs

Définir des vecteurs d'alerte
- Mail
- SMS
- Log

Le programme ci-dessus présente le programme initial de la formation DE-102 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SUPERVISION

DE-111 : Analyse de trafic Web / Mail / FTP *(2 jours)*

Logiciels utilisés

Webalizer, AWStats et Mailgraph sous environnement GNU/Linux

Présentation

Les serveurs publics constituent aujourd'hui un élément fondamental du Système d'Information. Ils collectent une quantité phénoménale de données sur leurs utilisateurs. Il convient d'archiver et de synthétiser ces informations. Leur analyse permet d'accroître significativement la qualité du service rendu.

Objectifs

Le but de cette formation est de découvrir les principaux outils libres qui permettent de collecter et de synthétiser les données de logs des principaux serveurs SMTP, FTP et HTTP. Le stagiaire sera ainsi capable de produire des rapports d'activité des différents services dont il a la charge dans son activité quotidienne.

Public Concerné

Administrateur système ou réseaux en charge d'architecture Web

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Installation et administration d'un système GNU/Linux (ref: DI-101)

Programme

JOUR 1

Informations disponibles
- sur un serveur HTTP
- sur un serveur FTP
- sur un proxy
- sur un serveur Mail

L'agrégation des données

Maquette avec Webalizer / Apache (HTTP)
- répartition hits/visites/visiteurs
- analyse horaire
- analyse des referers
- répartition des navigateurs
- ...

JOUR 2

Maquette avec Webalyser / Squid (proxy)
- installation/configuration
- analyse du trafic web sortant
- répartition horaire

Maquette avec AWStats / Postfix (SMTP)
- Installation/configuration
- analyse du trafic SMTP
- répartition horaire
- analyse par destination
- présentation de Mailgraph

Exportation et présentation des rapports

Le programme ci-dessus présente le programme initial de la formation DE-111 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SUPERVISION

DE-201 : Découverte de SmartReport *(1 jour)*

Logiciels utilisés

Client et serveur SmartReport

Présentation

SmartReport est une appliance de supervision de l'infrastructure IP basée sur une solution logicielle ouverte. Il facilite et améliore l'exploitation des infrastructures en se basant sur trois briques fonctionnelles : la gestion des performances, la gestion des incidents et le reporting d'activité.

Objectifs

Cette formation permet d'acquérir les compétences nécessaires à la prise en main de SmartReport pour la supervision d'un SI. Les stagiaires découvriront notamment comment installer et configurer l'appliance SmartReport et le client logiciel, puis comment intégrer les équipements dans SmartReport pour démarrer la supervision.

Public Concerné

Administrateurs système ou réseaux soucieux de mettre en place des outils de surveillance de leurs infrastructures techniques.

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Programme

JOUR 1

Mise en place de l'appliance SmartReport :
- Installation
- Configuration

Découverte du client logiciel :
- Installation
- Configuration
- Prise en main de l'interface

Démarrer la supervision des équipements :
- Intégration dans SmartReport
- Création de graphes de performance selon des modèles pré-définis et les appliquer à un équipement
- Création de tests de bon fonctionnement selon des modèles pré-définis et les appliquer à un équipement.

Le programme ci-dessus présente le programme initial de la formation DE-201 d'une durée d'une journée. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SUPERVISION

DE-202 : Gestion des performances avec SmartReport *(1 jour)*

Logiciels utilisés

Client et serveur SmartReport

Présentation

SmartReport est une appliance de supervision de l'infrastructure IP basée sur une solution logicielle ouverte. Il facilite et améliore l'exploitation des infrastructures en se basant sur trois briques fonctionnelles : la gestion des performances, la gestion des incidents et le reporting d'activité.

Objectifs

Cette formation permet d'acquérir les compétences nécessaires à l'élaboration de stratégies de gestion des performances d'un SI, puis à leur mise en place à l'aide de SmartReport. Les stagiaires découvriront notamment comment choisir et déployer les indicateurs de performance pertinents par famille d'équipement, en utilisant les technologies SNMP, Netflow / sFlow et IP/SLA.

Public Concerné

Administrateurs système ou réseaux soucieux de mettre en place des outils de surveillance de leurs infrastructures techniques.

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Découverte de SmartReport (ref: DE-201)

Programme

JOUR 1

Qualifier la charge d'une infrastructure
- Indicateurs de performances

Le protocole SNMP
- Organisation et structure
- Déploiement sur les équipements

Le protocole Netflow/sFlow
- Principe de fonctionnement
- Pertinence d'utilisation
- Déploiement sur les équipements

Le protocole IP/SLA
- Principe de fonctionnement
- Pertinence d'utilisation
- Déploiement sur les équipements

Mise en œuvre des indicateurs dans SmartReport
- Définir les indicateurs pertinents
- Collecter les données (push / pull)
- Agréger les données sur des graphes de performance

Le programme ci-dessus présente le programme initial de la formation DE-202 d'une durée d'une journée. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SUPERVISION

DE-203 : Gestion des incidents avec SmartReport *(1 jour)*

Logiciels utilisés

Client et serveur SmartReport

Présentation

SmartReport est une appliance de supervision de l'infrastructure IP basée sur une solution logicielle ouverte. Il facilite et améliore l'exploitation des infrastructures en se basant sur trois briques fonctionnelles : la gestion des performances, la gestion des incidents et le reporting d'activité.

Objectifs

Cette formation permet d'acquérir les compétences nécessaires à l'élaboration de stratégies de gestion des incidents d'un SI, puis à leur mise en place à l'aide de SmartReport. Les stagiaires découvriront notamment comment choisir et déployer les tests de bon fonctionnement d'un équipement ou d'un service, définir des indicateurs de disponibilité, créer des alertes et intercepter des évènements extérieurs tels que des trappes SNMP.

Public Concerné

Administrateurs système ou réseaux soucieux de mettre en place des outils de surveillance de leurs infrastructures techniques.

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Découverte de SmartReport (ref: DE-201)

Programme

JOUR 1

Qualifier la disponibilité d'une infrastructure à partir de tests de bon fonctionnement :

- Choix
- Mise en place
- Synthèse

Créer des cartes de réseau

Intercepter des traps SNMP

Créer des alertes à partir des évènements

Le programme ci-dessus présente le programme initial de la formation DE-203 d'une durée d'une journée. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

Sécurité des Systèmes d'Information

La sécurité du Système d'Information est devenu un enjeu crucial. Avec ces formations, les administrateurs pourront déployer avec efficacité les outils correspondant à leurs besoins. Lors des exercices pratiques, l'accent est mis sur la sécurité des solutions déployées. Cela implique en premier lieu une résistance aux **tentatives d'intrusion** mais également une **haute disponibilité** face aux problèmes de charge ou de pertes matérielles.

Les outils étudiés sont des « **logiciels libres** » dans leur très grande majorité. Ils permettent un déploiement aisé et peu coûteux sur tous types d'architecture.

FORMATION : SÉCURITÉ

DS-101 : Déployer un IDS Snort *(2 jours)*

Logiciels utilisés

IDS Snort

Présentation

Les IDS sont les dernières innovations en matière de sécurité informatique. Elles permettent de détecter et d'enregistrer les attaques survenant sur le réseau. En « écoutant » de manière permanente le trafic échangé à un endroit clef de votre système d'information, cet équipement est capable de détecter les événements caractéristiques d'une attaque. L'IDS utilise un dictionnaire de signatures qui sont mises à jour régulièrement pour faire face aux nouvelles attaques.

Objectifs

Ce module permet à un administrateur de sécurité de découvrir le logiciel Snort ainsi que le module Acid (reporting). Le but est de savoir déployer la sonde sur un environnement de production et de pouvoir en retirer les informations pertinentes. Le stage met l'accent sur l'aspect pratique en proposant à chaque stagiaire de manipuler sa propre sonde.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Programme

JOUR 1

Présentation du concept d'IDS

Intrusions, attaques et trafic suspect

Placer une sonde en mode passif
- Hub
- Port mirroring
- VLAN mirroring

Le logiciel libre Snort
- Historique
- Fonctionnalités
- Comparatif avec d'autres IDS

Maquette – Déployer Snort
- A partir de paquetages
- A partir des sources

JOUR 2

Configuration
- Modifier la configuration manuellement
- Administration via Webmin
- Les paramètres importants
- Le fichier de signatures
- Stockage des résultats
  - Fichiers
  - Base de données

Maintenir et exploiter la sonde
- Centraliser l'activité des sondes
- Mettre à jour et créer des signatures
- Comprendre les résultats
- Quelques outils d'aide à l'analyse
- Survol d'ACID (voir DS-102)

Le programme ci-dessus présente le programme initial de la formation DS-101 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-102 : utiliser ACID avec un IDS *(1 jour)*

Logiciels utilisés

IDS Snort

Présentation

Les IDS sont les dernières innovations en matière de sécurité informatique. Elles permettent de détecter et d'enregistrer les attaques survenant sur le réseau. En « écoutant » de manière permanente le trafic échangé à un endroit clef de votre système d'information, cet équipement est capable de détecter les événements caractéristiques d'une attaque. L'IDS utilise un dictionnaire de signatures qui sont mises à jour régulièrement pour faire face aux nouvelles attaques.

Objectifs

Ce stage permet aux administrateurs Snort de déployer l'outil d'analyse ACID (Analysis Console for Intrusion Databases). Celui-ci permet une gestion centralisée de l'analyse des journaux Snort. Il produit également des rapports graphiques de l'activité des différents IDS déployés sur le Système d'Information.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Déploiement et administration de Snort (DS-101)

Programme

JOUR 1

Rappel sur l'IDS

Installation d'ACID
- Architecture IDS/base de données
- Pré-requis applicatifs
- Installation rapide LAMP (Apache, Mysql et PHP)

Configuration d'ACID
- Récupération et centralisation des données
- Intégration avec MySQL et Snort
- Contôles d'accès et sécurité

Modules additionnels
- Librairie GD pour tracer des graphiques

Le programme ci-dessus présente le programme initial de la formation DS-102 d'une durée d'une journée. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-111a : Déployer un proxy-cache Squid *(2 jours)*

Logiciels utilisés

Proxy-cache Squid

Présentation

Squid est un logiciel libre dont la vocation est de servir d'intermédiaire (proxy) entre un utilisateur et un serveur de site Web. Le but est de contrôler de manière très fine l'accès au Web en termes d'horaires, de type de contenu, de profil d'utilisateur etc. Squid dispose également d'une fonction de caching qui permet de conserver en mémoire les sites Web les plus demandés. La mise en place du caching accélère notablement l'accès aux sites Web tout en optimisant l'utilisation de la bande passante.

Objectifs

Ce module permet à un administrateur réseau et système de découvrir le logiciel Squid et toutes ses possibilités. Il saura déployer une hiérarchie de serveurs proxy-cache dédiés à la production. Le stage met l'accent sur l'aspect pratique en proposant à chaque stagiaire de manipuler son propre serveur Squid.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Bonnes connaissances des réseaux TCP/IP

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Programme

JOUR 1

Rappels sur les protocoles HTTP et FTP

Théorie du proxy-cache
- Intérêts
- Fonctionnement
- Positionnement
- Hiérarchie de caches

Le logiciel libre Squid
- Historique
- Fonctionnalités
- Comparatif avec Bluecoat/ISA Server/...

Maquette – Déployer Squid
- A partir de paquetages
- A partir des sources

JOUR 2

Administration
- Modifier la configuration manuellement
- La configuration via Webmin
- Gestion et rotation des fichiers logs
- Authentification locale des clients
- Gestion des horaires d'accès
- Filtrer sur des critères d'en-têtes

Gestion du déploiement
- Mode transparent
- Automatisation par fichiers PAC
- Distribution par DHCP

Paramétrer Squid
- Algorithme de caching
- Hiérarchie de caches
- Définir des peers

Le programme ci-dessus présente le programme initial de la formation DS-111a d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-111b : Sécuriser un proxy-cache Squid *(2 jours)*

Logiciels utilisés

Proxy-cache Squid

Présentation

Squid est un logiciel libre dont la vocation est de servir d'intermédiaire (proxy) entre un utilisateur et un serveur de site Web. Le but est de contrôler de manière très fine l'accès au Web en termes d'horaires, de type de contenu, de profil d'utilisateur etc. Squid dispose également d'une fonction de caching qui permet de conserver en mémoire les sites Web les plus demandés. La mise en place du caching accélère notablement l'accès aux sites Web tout en optimisant l'utilisation de la bande passante.

Objectifs

Squid dispose de fonctionnalités extrêmement poussées concernant le reverse proxy, l'authentification sur bases externes ou encore la supervision en SNMP. Ce module permet de découvrir les caractéristiques les plus intéressantes de ce logiciel libre.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Déploiement d'un proxy-cache Squid de type client (DS-111a)

Programme

JOUR 1

Positionnement d'un Squid en reverse proxy
- Caching d'un serveur web local
- ACL sur les adresses URL
- Protection contre les vers et DOS

Maquette reverse Squid / Apache

Authentification sur bases externes
- NTLM
- Domaine Windows
- LDAP

JOUR 2

Administration avancée
- Supervision SNMP d'un serveur Squid
- Rapports d'activité
- Access-lists évoluées
- Manipulation d'entêtes

Positionnement de produits tiers
- back-to-back
- ICAP

Couplage de Squid à d'autres produits
- Anti-virus
- Filtrage d'url
- Filtrage de contenu

Le programme ci-dessus présente le programme initial de la formation DS-111b d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-121 : Sécurité des serveurs GNU/Linux *(2 jours)*

Logiciels utilisés

Une distribution GNU/Linux : RedHat Linux, Mandrake Linux, Debian ...

Présentation

Le système GNU associé au noyau Linux forme aujourd'hui la base de nombreux serveurs d'entreprise. Dans le cas d'infrastructures fortement exposées comme le Web ou la messagerie, il devient nécessaire de « durcir » la configuration standard de ces équipements pour garantir une sécurité optimale.

Objectifs

Ce module s'adresse à des administrateurs Linux avancés qui souhaitent développer leur compétences en matière de sécurité système et réseau. A l'issue du stage, les participants sont à même de déployer des serveurs critiques en toute sérénité.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Bases techniques en système et réseau

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Bonne approche des notions propres à la sécurité informatique

Programme

JOUR 1

Principes généraux
- Les risques
- Les ennemis
- Élaborer une défense

Aspects réseaux, la DMZ
- Le réseau comme vecteur d'attaque
- Firewalls, DMZ et routage
- Les architectures possibles

Sécurisation de la couche réseau de Linux
- Iptables / netfilter
- Se protéger des attaques ICMP et ARP
- Les protocoles à bannir

JOUR 2

La sécurité interne du noyau avec Grsecurity
- Durcissement TCP/IP
- Sécurisation des process
- Sécurisation des buffers et cache

Les failles applicatives
- Focus sur le SMTP
- Focus sur le HTTP
- Focus sur le DNS

Prévenir, détecter et corriger les failles
- Veille technologique
- L'outil Nessus
- Définir sa politique de mise à jour

Le programme ci-dessus présente le programme initial de la formation DS-121 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-122 : Sécuriser un réseau WiFi à la norme 802.11i *(2 jours)*

Logiciels utilisés

Linux, FreeRadius, OpenLDAP et OpenSSL

Présentation

La sécurité est un aspect à ne pas négliger lors du déploiement d'un réseau sans fil. Afin de préserver la confidentialité des données de l'entreprise, il est nécessaire de mettre en place un système d'authentification qui n'autorise que les personnes habilitées à se connecter en WiFi, et un système de chiffrement qui assure l'intégrité des données échangées par le client.

Les protocoles pouvant être mis en place sont nombreux, mais peu remplissent ces deux objectifs.

Objectifs

Ce stage permet aux administrateurs réseaux et sécurité de comprendre l'ensemble des spécificités de la sécurité des réseaux sans fil en terme de chiffrement des données et d'authentification des utilisateurs.
Ils pourront ensuite appréhender la mise en place d'un réseau sans fil sécurisé à la norme 802.11i en ayant recours à des certificats numériques côté serveur et côté client.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Notions sur le chiffrement informatique et sur les certificats numériques (ex: SSL)

Installation et configuration de réseaux sans fil en mode WEP (point d'accès et client)

Programme

JOUR 1 – Théorie des réseaux sans fil

Définition, terminologie et rappels lexicaux
- WiFi
- 802.11b/g, 802.1x
- 802.11i

Authentification et chiffrement sur WiFi
- Études comparatives : WEP, WPA, WPA2, WPA-PSK, TKIP, EAP-TLS, EAP-TTLS, LEAP
- Principes de fonctionnement
- Bénéfices et contraintes

Maquette
- Mise en place d'un réseau sans fil sécurisé à la norme WPA/WPA2 basé sur des certificats

JOUR 2 – Utiliser EAP-TLS et EAP-TTLS

Maquette - PKI
- Installer et configurer une infrastructure à clés publiques (PKI), gestion et déploiement de certificat

Maquette – EAP-TTLS avec Freeradius
- Configurer un serveur RADIUS 802.1x
- Installer et configurer un point d'accès en mode authentification EAP
- Installer et configurer un client WiFi WPA
  - TKIP ou AES pour le chiffrement
  - EAP-TTLS pour l'authentification

Le programme ci-dessus présente le programme initial de la formation DS-122 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-124 : Installer et configurer Freeradius *(1 jour)*

Logiciels utilisés

Linux, FreeRadius, OpenLDAP et OpenSSL

Présentation

Le protocole Radius s'est imposé dans le domaine des réseaux comme la solution la plus pertinente aux besoins de contrôle d'accès. Un serveur Radius permet de centraliser toutes les demandes de connexion des utilisateurs et ce quel que soit le média utilisé. Radius est ainsi disponible pour l'établissement de connexions WiFi comme de tunnels VPN ou encore de connexions GSM/3G. De par sa position centrale, le serveur Radius devient le point de contrôle idéal de toutes les communications avec les nomades.

Objectifs

Ce stage permet aux administrateurs réseaux et sécurité de découvrir le protocole Radius au travers de son implémentation opensource Freeradius. A l'issue de la session, l'administrateur est capable d'installer et de configurer un serveur Radius qui corresponde aux besoins de son système d'information. Un accent particulier est porté sur la sécurisation des accès WiFi pour les nomades et les invités.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Notions sur le chiffrement informatique et sur les certificats numériques (ex: SSL)

Programme

JOUR 1 – Radius et Freeradius Fonctionnalités du protocole Radius ● Rappel historique ● « AAA : Authorization, Authentication, Accounting » ● Radius vs Tacacs ● Fonctionnement du protocole ● Limites de Radius Le serveur Freeradius ● Installation et configuration ● Déclaration des clients ● « Backends » disponibles ● Ajout des comptes	Maquette ● Installation d'un serveur Freeradius ● Configuration initiale en PEAP ● Configuration d'un access-point Wifi ● Connexion d'un client Wifi WPA

Le programme ci-dessus présente le programme initial de la formation DS-124 d'une durée d'une journée. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.
Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-125 : Sécuriser un réseau à la norme 802.1x *(2 jours)*

Logiciels utilisés

Linux, FreeRadius, OpenLDAP et OpenSSL

Introduction

La simplicité des réseaux Ethernet rend la connexion et l'accès aux ressources informatiques possible par le simple branchement d'une prise. Mais ce qui est souhaitable pour vos utilisateurs ne l'est pas forcément pour les autres. La norme **IEEE 802.1X** est le standard qui définit le contrôle d'accès aux réseaux Ethernet. A la différence de la plupart des autres mécanismes de protection, le 802.1X intervient dès la **connexion physique** sur le port du commutateur. L'authentification est ainsi effectuée avant tout autre service, y compris les services d'auto-configuration du réseau (DHCP, PXE, Active Directory, etc ...). On obtient ainsi une protection beaucoup plus fiable que les restrictions basées sur du filtrage par adresses IP ou par adresses MAC.

L'authentification des équipements ou des utilisateurs est généralement basée sur le protocole RADIUS. En plus d'autoriser ou de refuser l'accès au réseau, il est possible de **définir des droits d'accès** et des **groupes d'utilisateurs**, afin d'assigner des droits différents aux différentes populations d'utilisateurs. Sur un même port réseau, ou sur une même connexion WiFi, on distingue ainsi les visiteurs ponctuels des salariés (par exemple). Certains équipements réseau permettent d'aller plus loin. Il est notamment possible de contrôler la présence de certains logiciels sur le poste de travail (comme par exemple un anti-virus à jour) avant de donner accès au réseau.

Objectifs

Ce stage permet aux administrateurs réseaux et sécurité de comprendre l'ensemble des spécificités de la sécurité des réseaux filaires et sans fil, en terme de contrôle d'accès et d'authentification des utilisateurs.
Ils pourront ensuite appréhender la mise en place d'un réseau filaire sécurisé à la norme 802.1x en ayant recours à un serveur Radius, une base d'utilisateur LDAP et des certificats numériques.

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Installer et configurer FreeRadius
Installation et configuration de réseaux filaires Ethernet

Programme

JOUR 1 – Sécurité des réseaux locaux et présentation de 802.1x

Définition, terminologie et rappels lexicaux
- Les enjeux de la sécurité du LAN
- Présentation et comparaison des différents modes de protection des accès (libre accès, portail captif, 802.1x)
- Principe du 802.1x

Contrôle d'accès et authentification avec 802.1x
- Principes de fonctionnement
- Bénéfices et contraintes
- Rappels sur Radius
- Présentation et comparaison des différents modes d'authentification
- Compatibilité des différents OS avec 802.1x
- Exemples de déploiement et bonnes pratiques

JOUR 2 – Maquettes en environnement CISCO

Maquette – FreeRadius simple
- Installation et configuration d'un serveur FreeRadius pour 802.1x
- Configuration du 802.1x sur commutateurs réseau pour authentification sur adresse MAC

Maquette – FreeRadius + OpenLDAP
- Installation et configuration d'un serveur FreeRadius pour 802.1x avec base d'utilisateur LDAP
- Configuration du 802.1x sur commutateurs réseau pour authentification sur login / mot de passe
- Gestion de groupes d'utilisateurs

Le programme ci-dessus présente le scénario initial de la formation DS-122 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin. Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-126 : Sécuriser un réseau par un portail captif *(2 jours)*

Logiciels utilisés

Linux, FreeRadius, OpenLDAP et OpenSSL

Introduction

Un portail captif est un équipement de sécurité réseau. Il se place le plus souvent comme un routeur, juste devant le firewall. Le rôle d'un portail captif est précisément d'intercepter les communications afin d'authentifier les utilisateurs, d'enregistrer les accès et de bloquer les trafic illégitimes.

Objectifs

Ce stage permet aux administrateurs réseaux et sécurité de mettre en place un portail captif au sein de leur réseau, afin de donner un accès sécurisé à tout ou partie de leur réseau à des populations d'utilisateurs différentes (visiteurs, salariés, VIP …) et via des modes de connexion différents (WiFi, VPN, filaires …).

Public Concerné

Administrateur réseaux/sécurité

Compétences nécessaires

Installer et configurer FreeRadius

Installation et configuration de réseaux filaires Ethernet

Programme

JOUR 1 – Contrôle d'accès avec un portail captif

Rôle et fonctionnement d'un portail captif
- Présentation
- Exemple de fonctionnement et bonnes pratiques
- Mise en oeuvre en complément d'un réseau 802.1x

Maquette – Mise en oeuvre d'un portail captif avec Chilispot
- Installation et configuration du portail captif
- Authentification avec backend FreeRadius / OpenLDAP
- Gestion des droits d'accès et des groupes d'utilisateurs

JOUR 2 – Suite portail captif / Présentation de Netflow

Maquette – Utilisation du portail captif pour sécuriser un réseau WiFi
- Introduction à la norme 802.11i
- Différents modes d'authentification et chiffrement
- Maquette : mise en oeuvre d'un portail captif pour une population « invité »
- Maquette : mise en oeuvre d'un portail captif pour plusieurs populations différentes

Le programme ci-dessus présente le scénario initial de la formation DS-122 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin. Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : SÉCURITÉ

DS-131 : Infrastructure SSO avec SAML (2 jours)

Matériels et logiciels utilisés

Linux, simpleSAMLphp, Apache mod_auth_mellon

Présentation

La multiplication des applications hébergées (SaaS) oblige les DSI à proposer des solutions pour garantir la confidentialité des informations internes. A ce titre l'authentification des utilisateurs est un sujet majeur. En effet il est impossible de demander à chaque utilisateur de retenir un mot de passe pour chaque application. Pour autant il n'est pas pensable d'ouvrir à des applications externes un accès à la base d'authentification interne (souvent un Active Directory). C'est à cette problématique que les mécanismes SSO permettent de répondre, en autorisant un échange standard et sécurisé des informations d'identité entre des entités distinctes.

Objectifs

Ce stage permet aux administrateurs système, réseau et sécurité de découvrir les mécanismes de SSO disponibles avec un **focus sur SAML**. Ce protocole est le plus standard, il est disponible sur de nombreux systèmes et tend à remplacer les autres mécanismes existant. Des maquettes permettent de concevoir de A à Z un système basé sur SAML. Les **deux modes principaux (IDP et SP) sont couverts**, permettant d'appréhender l'intégralité des échanges nécessaires au bon fonctionnement. Un accent particulier est placé sur la phase d'analyse des dysfonctionnements propres au SSO.

Public Concerné

Administrateur système, réseau et sécurité

Compétences nécessaires

Notions sur le chiffrement SSL/TLS.
Notions sur HTTP/HTTPS.
Bases en système Unix : édition de fichiers, démarrage de processus.

Programme

JOUR 1 – Principes du SSO

Principes
- Présentation des mécanismes SSO
- Rappels sur HTTP
- Rappels sur Digest et Kerberos

Protocoles d'échange
- SAML
- OAuth
- Shiboleth

Les parties prenantes
- Identity Provider (IDP)
- Service Provider (SP)

Organisation
- Echange d'informations
- La fédération d'identité
- Clefs et certificats

JOUR 2 – Architecture SSO avec SAML

Définir son projet SSO et choisir les composants

Créer un IDP
- Maquette avec simpleSAMLphp
- Configurer les backends d'authentification
- Déclarer les SP

Créer un SP
- Maquette avec simpleSAML ou mod_mellon
- Configurer la délégation d'identité
- Déclarer les IDP

Diagnostiquer les incidents
- Méthodologie
- Comprendre les échanges
- Vérifications importantes

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

Communications Unifiées

Les outils qui sont abordés dans les formations «Communications Unifiées» concernent les solutions techniques liées à la téléphonie sur IP. Chaque brique est abordée sous son aspect théorique puis au travers d'un logiciel dédié à cette tâche. Le but de ces stages est d'être capable de configurer et d'intégrer aux systèmes d'information une téléphonie opérationnelle rapidement et évolutive.

Les outils étudiés sont des « **logiciels libres** » dans leur très grande majorité. Ils permettent un déploiement aisé et peu coûteux sur tous types d'architecture. Certains de ces logiciels sont leaders sur leur segment.

Avencall Partner
XiVO Gold certified

FORMATION : COMMUNICATIONS UNIFIÉES

DT-101 : Administration IPBX XiVO *(2 jours)*

Matériels, logiciels et protocoles

Logiciels : Linux, Asterix, XiVO
Protocole : SIP

Présentation

XiVO est un IPBX basé sur Asterisk et largement adopté par les entreprises. Il fournit l'ensemble des fonctionnalités de téléphonie professionnelle et de centre d'appels, complété par de nombreux services de couplage téléphonie informatique.

Objectifs

Ce stage permet aux administrateurs de système téléphonique de se familiariser à XiVO en comprenant son fonctionnement et les différentes fonctionnalités.

Public Concerné

Administrateur système, réseau et sécurité

Compétences nécessaires

Réseau, Protocole Sip,

Notions sur le routage d'appels

Programme

JOUR 1 – Présentation & Installation de XiVO

Introduction

- Présentation générale de XiVO

Initialisation et paramètres de base

- Configuration réseau dans XIVO
- Les contextes
- Serveur d'approvisionnement
- Les greffons
- Modèles de lignes
- Modèles de terminaisons
- Choix des codecs
- Création des utilisateurs
- Comptes d'administration
- Approvisionnement des téléphones

JOUR 2 – Fonctionnalités classiques

Fonctionnalités classiques

- Extensions téléphoniques
- Fichiers sons
- Musiques d'attente
- Groupements
- Messagerie vocale
- Chambres de conférence
- Le filtrage patron-secrétaire
- Interception d'appel
- Horaires
- Interphonie
- Droits d'appels
- Annuaires
- Journaux d'appels
- Introduction au Dialplan avec un SVI

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : COMMUNICATIONS UNIFIÉES

DT-102 : Administration Avancée IPBX XiVO *(2 jours)*

Matériels, logiciels et protocoles

Logiciels : Linux, Asterix, XiVO
Protocole : SIP

Présentation

XiVO est un IPBX basé sur Asterisk et largement adopté par les entreprises. Il fournit l'ensemble des fonctionnalités de téléphonie professionnelle et de centre d'appels, complété par de nombreux services de couplage téléphonie informatique.

Objectifs

Ce stage permet aux administrateurs de système téléphonique de gérer le XiVO avec l'ensemble des fonctionnalités avancées.

Public Concerné

Administrateur système, réseau et sécurité

Compétences nécessaires

Réseau, Protocole Sip,

Notions sur le routage d'appels

Exploitation et administration quotidienne XiVO

Programme

JOUR 1 – Gestion des communications	JOUR 2 – Maintenance
Interconnexions ● Interconnexions SIP ● Interconnexion IAX ● Interconnexion RNIS ● Boucle locale ● Appels sortants ● Appels entrants	**Maintenance** ● CLI Asterisk ● Sauvegarde ● Restauration ● Mise à jour ● Les logs du système ● Mise en HA

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : COMMUNICATIONS UNIFIÉES

DT-103 : Administration passerelle Patton SmartNode *(2 jours)*

Matériels, logiciels et protocoles utilisés

Matériel : Passerelle Patton SmartNode avec connectique TDM (T0 et T2)
Logiciels : OS SmartWare et Trinity
Protocoles : SIP, TDM (q921, q931)

Présentation

Les passerelles Patton SmartNode sont les équipements de référence pour connecter des réseaux de téléphonie sur IP aux installations téléphoniques dites « traditionnelles », en numérique TDM.

Objectifs

Cette formation apporte aux administrateurs de systèmes téléphoniques les notions et enseignements nécessaires pour administrer une passerelle Patton SmartNode, choisir les modèles adéquats, comprendre le fonctionnement, analyser et modifier une configuration en CLI, surveiller l'activité téléphonique et comprendre les dysfonctionnements.

Public Concerné

Administrateur réseau, administrateur de systèmes téléphoniques PABX et IPBX
Les maquettes sont réalisées avec les modèles SN4638, SN4970 et SN4971, mais les notions abordées et les configurations produites sont valables pour tous les modèles de la gamme SmartNode.

Compétences nécessaires

Les notions abordées nécessitent de disposer des notions de base sur les réseaux IP (routage, adressage IP) et téléphoniques (câblage, SIP et TDM).

Programme

JOUR 1 – Principes de fonctionnement

Principes
- Rappel sur les protocoles IP, SIP et TDM
- Cas d'utilisation et modèles
- Fonctionnalités et documentation
- Installation physique et câblage

Fonctionnement et configuration
- Concepts basiques du fonctionnement
- Gestion des comptes administrateurs
- Gestion du système et accès aux outils d'administration
- Mise en réseau, mise à niveau logicielle, configuration de base

Diagnostics
- Voir la configuration
- Voir l'état des connexions
- Voir l'activité téléphonique
- Debug et troubleshooting

JOUR 2 – Configurations et maquettes

Configuration TDM (maquette)
- Configurer les ports T0 et T2 pour connexion à un opérateur européen
- Configurer les ports T0 et T2 pour connexion à un PABX
- Interfaces ISDN

Configuration SIP (maquette)
- Configurer un trunk SIP pour connexion à un opérateur
- Configurer un trunk SIP pour connexion à un IPBX
- Interfaces SIP

Configuration téléphonique avancée
- Gestion des tonalités
- Gestion des interfaces
- Utilisation des tables et des services
- Utilisation des location-service

Gestion du plan d'appels (maquette)
- Modifier les numéros présentés et composés
- Routage sélectif et haute disponibilité

Le programme ci-dessus présente le scénario initial de la formation d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.

FORMATION : COMMUNICATIONS UNIFIÉES

DT-104 : Installer et configurer Asterisk *(2 jours)*

Logiciels utilisés

Linux, Asterisk, Hylafax

Présentation

Asterisk est un IPBX open source pour systèmes UNIX. Mettre en place une solution Asterisk dans votre entreprise vous permettra de profiter de toutes les fonctionnalités de la TOIP (téléphonie sur IP) : la messagerie vocale, les conférences, les files d'attente, les musiques d'attente et les mises en garde d'appels, la distribution des appels...

Objectifs

Ce stage permet aux administrateurs réseaux de découvrir la téléphonie sur IP à travers l'installation et la configuration de l'IPBX open source Asterisk. Nos spécialistes TOIP, vous expliqueront les principes de base de la voix sur IP (VOIP), puis ils vous présenteront plusieurs installations et configurations suivant les types d'infrastructures réseaux et les fonctionnalités souhaitées .

Public Concerné

Administrateur système ou réseau

Compétences nécessaires

Les connaissances de bases sur les réseaux et la téléphonie sont le minimum requis pour suivre cette formation.
Optionnel : Installation et administration d'un système GNU/Linux (DI-101a et DI-101b)

Programme

Introduction
- Présentation
- Fonctionnalités
- Installation et configuration de base

Le protocole SIP

Utilisation du registrar SIP
- Notion de registrar
- Implémentation
- Création des comptes téléphoniques et du 'dialplan'

Enregistrements SRV
- Communication entre domaines
- Création de DNS et configuration Asterisk
- Mise en œuvre et tests

Plan de numérotation
- Définitions : contextes, applications
- Configuration /etc/asterisk/extensions.conf
- Syntaxe générale
- Contextes
- Extensions
- Priorités
- Configuration des Applications
- Dial(), Record(), CDR (Call Details Record)
- Syntaxe détaillée
- Les opérateurs
- Les expressions
- Les motifs
- Les branchements conditionnels
- Les fonctions et macros

Fonctionnalités supplémentaires
- Mail-to-Fax / Fax-to-Mail
- Serveur Vocal Interactif (SVI)
- Couplage Téléphonie-Informatique (CTI)
- G722 (son haute définition)

Le programme ci-dessus présente le programme initial de la formation DI-133 d'une durée de 2 jours. La durée de la formation et les points à traiter peuvent être modifiés suivant votre besoin.

Toutes nos formations sont réalisées en intra-entreprise et peuvent faire l'objet de financement par votre OPCA.