

LINUX : MAÎTRISER LES SERVICES RÉSEAUX

Durée : 4 jours (28 heures)

CONNAISSANCES PREALABLES

- Connaissances de base de Linux en ligne de commande.
- Connaissances fondamentales des réseaux TCP/IP.
- Expérience de l'administration Linux ou formation Linux Installation et Administration équivalente.

PROFIL DES STAGIAIRES

- Administrateurs systèmes Linux.
- Administrateurs réseaux.
- Ingénieurs systèmes et infrastructures.
- Techniciens d'exploitation.
- Responsables de plateformes Linux.

OBJECTIFS

À l'issue de la formation, les participants seront capables de :

- Comprendre l'architecture des services réseaux sous Linux.
- Configurer et administrer les principaux services d'infrastructure.
- Déployer des services DNS, DHCP, Web et FTP.
- Mettre en œuvre des services de partage de fichiers.
- Sécuriser les services réseaux Linux.
- Superviser et maintenir les services en production.
- Diagnostiquer et résoudre les incidents courants..

CERTIFICATION PREPAREE

Aucune

METHODES PEDAGOGIQUES

- Apports théoriques.
- Démonstrations techniques.
- Travaux pratiques sur serveurs Linux.
- Études de cas d'exploitation.
- Ateliers de configuration.
- Mise en situation de résolution d'incidents..

FORMATEUR

- Consultant formateur expert Unix/Linux disposant d'une expérience significative dans l'administration, l'exploitation et le support de systèmes Linux en environnement de production.

METHODE D'EVALUATION DES ACQUIS

- Exercices pratiques.
- Quiz de validation.
- Études de cas.
- Atelier fil rouge.
- Évaluation pratique finale.

CONTENU DU COURS

Jour 1 – Fondamentaux réseau et services d'infrastructure

Module 1 : Architecture réseau sous Linux (2h)

Objectifs

- Comprendre le fonctionnement des services réseaux Linux.
- Identifier les composants de l'infrastructure réseau.

Contenu

- Architecture TCP/IP.
- Rappels réseau.
- Modèle client/serveur.
- Ports et protocoles.
- Services réseaux Linux.
- Gestion des interfaces réseau.
- Outils de diagnostic.

Mises en pratique

- Analyse de la configuration réseau d'un serveur.
- Utilisation des outils de diagnostic.
- Exercices de connectivité et de dépannage.

Module 2 : Configuration avancée du réseau Linux (2h)

Objectifs

- Administrer les paramètres réseau d'un serveur Linux.

Contenu

- Configuration IPv4 et IPv6.
- Routage.
- Résolution DNS.
- Gestion des interfaces.
- Paramétrage persistant.
- Outils NetworkManager.

Mises en pratique

- Configuration manuelle d'interfaces réseau.
- Mise en place de routes statiques.
- Tests de résolution réseau.

Module 3 : Déployer et administrer un serveur DNS (3h)

Objectifs

- Mettre en œuvre un service DNS sous Linux.

Contenu

- Principes du DNS.
- Architecture DNS.
- Installation de BIND.
- Zones directes et inverses.
- Enregistrements DNS.
- Délégation.
- Sécurisation du service.

Mises en pratique

- Installation d'un serveur DNS.
- Création de zones DNS.
- Validation et dépannage des résolutions.

Jour 2 – Services DHCP, FTP et partage de fichiers

Module 4 : Déployer un serveur DHCP (2h)

Objectifs

- Automatiser l'attribution des adresses IP.

Contenu

- Fonctionnement DHCP.
- Installation du service.
- Configuration des pools d'adresses.
- Réservations.
- Gestion des options DHCP.
- Haute disponibilité.

Mises en pratique

- Déploiement d'un serveur DHCP.
- Configuration de réservations.
- Validation du fonctionnement client.

Module 5 : Mettre en œuvre un serveur FTP/SFTP (2h)

Objectifs

- Fournir un service sécurisé de transfert de fichiers.

Contenu

- Protocoles FTP, FTPS et SFTP.
- Installation de VSFTPD.
- Authentification.
- Gestion des accès.
- Chroot et confinement.
- Sécurisation des échanges.

Mises en pratique

- Installation et configuration d'un serveur FTP.
- Mise en œuvre de SFTP sécurisé.
- Tests d'accès utilisateurs.

Module 6 : Services de partage de fichiers NFS et Samba (3h)

Objectifs

- Mettre à disposition des espaces de partage réseau.

Contenu

- Architecture NFS.
- Exportation de ressources.

- Gestion des droits.
- Architecture Samba.
- Intégration Windows/Linux.
- Authentification et sécurité.

Mises en pratique

- Mise en œuvre d'un partage NFS.
- Configuration d'un serveur Samba.
- Tests d'accès multi-utilisateurs.

Jour 3 – Services Web et sécurisation**Module 7 : Déployer un serveur Web Apache (3h)****Objectifs**

- Héberger des applications et sites web.

Contenu

- Architecture Apache.
- Installation et configuration.
- Hôtes virtuels.
- Gestion des modules.
- Journaux de fonctionnement.
- Optimisation des performances.

Mises en pratique

- Installation d'Apache.
- Création de plusieurs sites virtuels.
- Analyse des journaux.

Module 8 : Sécuriser les services Web avec TLS/SSL (2h)**Objectifs**

- Sécuriser les communications réseau.

Contenu

- Certificats numériques.
- Infrastructure PKI.
- HTTPS.
- Génération de certificats.
- Configuration SSL/TLS.
- Bonnes pratiques de sécurité.

Mises en pratique

- Création d'un certificat.
- Activation HTTPS sur Apache.
- Validation de la configuration sécurisée.

Module 9 : Introduction aux serveurs Proxy et Reverse Proxy (2h)**Objectifs**

- Comprendre les architectures intermédiaires.

Contenu

- Proxy et Reverse Proxy.
- Cas d'usage.
- Introduction à Nginx.
- Répartition de charge.
- Sécurisation des accès.

Mises en pratique

- Configuration d'un Reverse Proxy simple.
- Publication sécurisée d'un service Web.

Jour 4 – Sécurisation, supervision et exploitation

Module 10 : Administrer les services SSH et les accès distants (2h)

Objectifs

- Sécuriser l'administration distante.

Contenu

- Fonctionnement SSH.
- Authentification par clés.
- Renforcement de la sécurité.
- Contrôle des accès.
- Tunnels SSH.

Mises en pratique

- Configuration sécurisée d'OpenSSH.
- Mise en œuvre d'une authentification par clés.
- Création d'un tunnel sécurisé.

Module 11 : Sécuriser les services réseaux Linux (2h)

Objectifs

- Renforcer la sécurité globale de l'infrastructure.

Contenu

- Pare-feu Linux.
- Filtrage réseau.
- Contrôle des ports.
- Gestion des mises à jour.
- Durcissement des services.

Mises en pratique

- Configuration du pare-feu.
- Restriction des accès aux services.
- Vérification de l'exposition réseau.

Module 12 : Supervision et diagnostic des services réseaux (2h)

Objectifs

- Surveiller les services en production.

Contenu

- Journaux système.
- Analyse des performances.
- Contrôle de disponibilité.
- Outils de supervision.
- Diagnostic des incidents.

Mises en pratique

- Analyse de journaux d'incidents.
- Recherche de causes de dysfonctionnement.
- Résolution de problèmes réseau.

Module 13 : Atelier fil rouge – Déploiement d'une infrastructure de services Linux (2h)

Objectifs

- Mettre en œuvre l'ensemble des compétences acquises.

Contenu

- Mise en place d'une infrastructure complète :
 - DNS
 - DHCP
 - Apache
 - Samba ou NFS
 - SSH sécurisé
- Documentation de l'architecture.

Mises en pratique

- Étude de cas complète d'entreprise.
- Déploiement et validation des services.
- Diagnostic d'incidents simulés.
- Évaluation pratique finale et débriefing collectif.

Notre référent handicap se tient à votre disposition au [01.71.19.70.30](tel:01.71.19.70.30) ou par mail à <mailto:referent.handicap@edugroupe.com> pour recueillir vos éventuels besoins d'aménagements, afin de vous offrir la meilleure expérience possible.