

Mapping certification LPI Linux Essentials - Gérez les services Linux et déployez vos applications

Cette correspondance vous sera surtout utile si vous envisagez un jour de préparer la certification LPI Linux Essentials. Elle vous permet de situer ce cours dans le référentiel, mais ne remplace pas à elle seule une préparation complète à l'examen.

Thème 2 – Utiliser la ligne de commande

- Utiliser la ligne de commande pour observer et piloter un système Linux déjà installé.
- Lire et inspecter des fichiers de configuration système, notamment `sshd_config` et `compose.yml`.
- Utiliser des commandes de consultation et de diagnostic comme `cat`, `systemctl`, `journalctl`, `docker ps` et `docker compose logs`.
- Modifier un fichier texte en ligne de commande pour corriger une configuration.
- S'appuyer sur une méthode d'administration en terminal fondée sur l'observation, la vérification puis la correction.

Thème 3 : La puissance de la ligne de commande

- Exploiter les journaux d'un système pour diagnostiquer un service en échec.
- Utiliser des commandes de consultation de logs pour retrouver la cause probable d'un incident.
- Lire un fichier de déploiement texte (`compose.yml`) et relancer une application à partir d'une description structurée.
- Utiliser des outils de ligne de commande pour superviser l'état d'exécution de composants applicatifs.
- Mobiliser une logique de diagnostic proche de celle attendue par le référentiel : observer l'état, lire les journaux, identifier la cause, puis corriger.

Thème 4 – Le système d'exploitation Linux

- Comprendre qu'un serveur Linux ne se limite pas au système lui-même, mais repose aussi sur des services exécutés en arrière-plan.
- Comprendre ce qu'est un **service Linux** et son rôle dans le fonctionnement d'un serveur.
- Découvrir le rôle de **systemd** comme gestionnaire de services sur les distributions Linux modernes.
- Distinguer l'état actuel d'un service et son activation au démarrage du système.
- Comprendre qu'un service comme SSH ou Apache fournit une fonction continue indépendante de l'utilisateur connecté.
- Situer le rôle de la journalisation système dans l'exploitation et le dépannage.
- Comprendre la logique d'un déploiement applicatif natif par opposition à une approche conteneurisée.
- Comprendre que des applications peuvent être isolées dans des environnements dédiés afin de réduire les conflits de dépendances et d'améliorer la reproductibilité.
- Découvrir, à un niveau introductif, le rôle d'outils comme Docker, Podman et Docker Compose dans l'exploitation moderne d'un serveur Linux.

Thème 5 – Sécurité et permissions des fichiers

- Comprendre que SFTP repose sur l'infrastructure sécurisée de SSH et permet des transferts chiffrés.
- Appliquer le principe du moindre privilège à un accès de dépôt de fichiers.
- Configurer un confinement **chroot** pour limiter un utilisateur SFTP à un répertoire dédié.
- Comprendre que la sécurité d'un accès dépend à la fois de la configuration du service et des permissions du système de fichiers.
- Vérifier les propriétaires et permissions de répertoires impliqués dans un accès SFTP confiné.
- Diagnostiquer un refus de connexion lié à une erreur de permissions ou de propriétaire.
- Comprendre qu'une mauvaise configuration de droits peut rendre un service inutilisable même s'il est actif.
- Prendre en compte la persistance des données comme enjeu de sécurité et de fiabilité d'une application déployée.

- Comprendre l'intérêt de l'isolation, qu'elle soit mise en œuvre par un chroot ou par un conteneur, pour limiter les risques et mieux maîtriser un environnement d'exécution.

À noter

- Ce cours couvre surtout le Thème 4 : Le Système d'Exploitation Linux et le Thème 5 : Sécurité et Permissions des Fichiers.
- Il contribue aussi au Thème 2 : Se Repérer sur un Système Linux et, plus ponctuellement, au Thème 3 : La Puissance de la Ligne de Commande.
- Il ne couvre pas directement le Thème 1 : La Communauté Linux et une Carrière dans l'Open Source.