TRAINUX
Nous faisons du libre notre métier

Linux Professional Institute

CONTENU PEDAGOGIQUE
LPIC-3 Spécialité Expert Sécurité
(LPI 301 et LPI 303)

La certification LPIC-3 est le point culminant du programme des certifications du LPI.
Elle valide les compétences nécessaires pour la gestion à un niveau "structure ou entreprise". Elle a été développée à partir de contributions de centaines de professionnels du monde entier ainsi que celles d'entreprises parmi les plus importantes du secteur des technologies. Il s'agit de la certification indépendante de la distribution Linux de plus haut niveau dans le monde de l'entreprise.

Cette certification comporte un examen commun associé à un ensemble d'examens de spécialité. Les différentes spécialités proposées sont les suivantes :

- Environnement hétérogéne
- Sécurité
- Haute disponibilité et virtualisation
- Web, intranet, messagerie

Prérequis :

Avoir obtenu la certification LPIC-2

Pour obtenir l'examen commun (LPI-301), il faut :

- Avoir de nombreuses années d'expérience dans l'installation et la maintenance de Linux sur de nombreuses machines pour des buts différents
- Avoir l'expérience de l'intégration de diverses technologies et de systèmes d'exploitation
- Avoir l'expérience professionnelle (ou avoir été formé pour cela) de Linux à un niveau entreprise (y compris avoir une expérience, même partielle, dans un autre rôle)
- Disposer de connaissances avancées de l'administration système sous Linux (installation, gestion, maintenance, régler les dysfonctionnements, sécurité)
- Etre à même d'utiliser des outils du monde libre pour effectuer des mesures de métrologie et détecter les dysfonctionnements
- Avoir une expérience de l'utilisation de LDAP dans un milieu mixte (Windows/Linux) comprenant les services Samba, PAM, Email, active directory
- Etre capable de planifier, concevoir, construire et mettre en oeuvre un environnement Samba associé à LDAP ainsi que d'évaluer sa sécurité et sa capacité à monter en charge
- Etre capable d'écrire des scripts en "bash" ou en "Perl" ou avoir la connaissance d'un ou plusieurs langages de programmation (par exemple C)

Pour obtenir l'examen de spécialité (LPI-302) «Expert Sécurité», il faut :

- Avoir l'expérience et les connaissances décrites pour l'examen commun (LPI-301)
- Disposer de l'expérience dans la mise en œuvre d'une politique de sécurité système et

réseau sous Linux

- Etre capable de planifier, concevoir, construire et mettre en oeuvre une politique de sécurité réseau sous Linux pour son Entrerise

Contenu détaillé :

Module	***Contenu du module***	***Durée prévue (en nombre d'heures)***
Programme LPI 301		
Module 301: Concepts, Architecture et Design	301.1 : LDAP : concepts et architecture	1h
	301.2 : Conception d'annuaires	
	301.3 : Schemas	
Module 302 : Installation et Développement	302.1 Compiler et installer OpenLDAP	1h
	302.2 Développer pour LDAP avec Perl/C++	
Module 303 : Configuration	303.2 : Access Control Lists dans LDAP	8h
	303.3 : Replication LDAP	
	303.4 : Sécuriser l'annuaire	
	303.5 : Paramétrage de la performance du serveur LDAP	
	303.6 : Configuration du démon OpenLDAP	
Module 304 : Utilisation d'OpenLDAP	304.1 : Chercher dans l'annuaire	1h
	304.2 : Outils LDAP en ligne de commande	
	304.3 : Pages Blanches	

Module 305 : Intégration et migration	305.1 :Integration LDAP avec PAM et NSS	6h
	305.2 : Migrer de NIS à LDAP	
	305.3 : Intégrer LDAP avec les services UNIX	
	305.4 :Intégrer LDAP avec Samba	
	305.5 : Intégrer LDAP avec Active Directory	
	305.6 : Intégrer LDAP avec les services de messagerie	
Module 306 : Planification des capacités	306.1 :Mesurer l'utilisation des ressources	3h
	306.2 : Dépanner les problèmes de ressources	
	306.3 : Analyser la demande	
	306.4 : Prévoir les besoins en ressources futurs	
Module T301 : Test de simulation pour la préparation à l'examen de certification LPI301		4h
Passage de l'examen de certification LPI301		1h30
Programme LPI303		
Module 320 : Cryptographie	320.1 OpenSSL	3h
	320.2 Cryptage GPG Avancé	
	320.3 Systéme de fichiers	

	cryptés	
Module 321: Contrôle d'accès	321.1 La gestion des utilisateurs et des droits d'accès	4h
	321.2 : Attributs de droits d'accès avancés et les ACLs	
	321.3 Le système SELinux	
	321.4 Autres systèmes mandataires pour le contrôle d'accès	
	322.1 DNS/BIND	
	322.2 Serveur de messagerie	
	322.3 Apache/HTTP/HTTPS	
	312.4 : Contrôle de domaine	
	322.4 FTP	
	322.5 OpenSSH	
	322.6 NFSv4	
	322.7 Syslog	
	323.1 Gestion de la configuration des machines clients avec RCS and Puppet	
	324.1 Détection des intrusions	
	324.2 Audit de la sécurité réseau	
	324.3 Les outils du supervision réseau	
	324.4 netfilter/iptables	
	324.5 OpenVPN	
Module T303 : Test de simulation pour la préparation à l'examen de certification LPI303		4h
Passage de l'examen de certification LPI303		1h30