



Objectifs

Ce cours vous apprend à effectuer les tâches principales d'administration de sécurité avec SUSE Linux Enterprise Server 10 dont le chiffrement des données, les considérations à prendre en compte pour développer une politique de sécurité d'entreprise, ainsi que la configuration des services AppArmor, des filtres paquets, des passerelles et des réseaux privés virtuels.

Public

Ce cours s'adresse à des administrateurs certifiés Novell Certified Professional (CLP 10) ou équivalent, souhaitant préparer la certification Novell Certified Linux Engineer 10 (CLE 10).

Pré-requis

Avant de suivre ce cours, vous devez avoir suivi le cursus CLP (C3071, C3072 et C3073) ou avoir des connaissances équivalentes. Ce cours, associé à la formation C3074 constitue le cursus CLE 10.

Durée et Tarifs

5 jours soit 35 heures
2.400,00 €HT
Support de cours & déjeuners inclus

FORMATION C3075 SUSE LINUX ENTERPRISE SERVER 10 SECURITE



1. Considérations générales et définitions

- Créer un concept de sécurité,
- Comprendre la terminologie usuelle

2. Sécurité de la machine hôte

- Limitier l'accès physique aux serveurs,
- Les partitions et la sécurité du système de fichiers,
- Limitier l'installation de logiciels,
- Configurer les paramètres de sécurité avec YaST,
- Rester informé sur les questions de sécurité,
- Appliquer les mises à jour de sécurité,
- Tester et documenter la configuration,
- Utiliser les logs et la surveillance des comptes.

3. AppArmor

- Améliorer la sécurité des applications avec AppArmor,
- Créer et gérer des profils AppArmor,
- Contrôler AppArmor,
- Suivre et maintenir AppArmor.

4. Chiffrement : Bases et applications pratiques

- Les bases du chiffrement des données,
- Créer une autorité de certification (CA) et utiliser les outils CLI,
- Utiliser YaST pour créer une autorité de certification (CA) et gérer les certificats,
- GNU Privacy Guard (GPG)

5. Sécurité réseau

- Comprendre les services et les protocoles,
- Sécuriser les accès avec TCP Wrapper,
- Utiliser SSL pour sécuriser un service,
- Sécuriser les clients.

6. Architecture Générale d'un pare feu

- Comprendre les concepts de pare feu,
- Décrire les composants d'un pare feu,
- Comprendre les avantages et les inconvénients de différentes configurations.

7. Filtres de paquets

- Comprendre les filtres de paquets,
- Les bases d'iptables,
- Les fonctionnalités avancées d'iptables,
- Comprendre la translation d'adresse (NAT).

8. Les passerelles au niveau application

- Décrire les passerelles au niveau application,
- Configurer et utiliser SQUID,
- Configurer et utiliser Dante,
- Configurer et utiliser rinetd.

9. Réseau privé virtuel (VPN)

- Les bases du VPN et IPSec,
- Configurer et établir une connexion IPSec,
- Comprendre le filtrage de paquets du trafic VPN.

10. Détection d'intrusion et réponse aux incidents

- Les fichiers de log et leur analyse,
- Détection des intrusions sur la machine hôte,
- Détection des intrusions sur le réseau,
- Réponse aux incidents.

11. Exercices sur des cas pratiques

- Configurer une passerelle applicative,
- Configurer un « Screening Router »,
- Configurer un serveur Web en DMZ,
- Configurer un serveur de messagerie sur le réseau,
- Configurer une passerelle VPN.