Organisme de formation professionnelle continue
Numero agrément 91 30 03332 30
France : +33 (0)188 24 70 33 / 34
Site : www.oo2.fr
Mail : contact@oo2.fr

Red Hat Linux – Sécurité Avancée

Date et durée

Code formation : RH143
Durée : 4 jours
Nombre d'heures : 28 heures

Formation avec préparation à la certification

Red Hat Certified Architect

Description

Le renforcement de serveur est un ensemble d'opérations et de techniques ayant pour objectif de **renforcer la sécurité d'un système en réduisant les sources de vulnérabilité**. Cette formation vous apprendra à maîtriser les pratiques de renforcement de la sécurité avec Red Hat Enterprise Linux. Elle fait partie de la préparation à l'examen de **certification Red Hat** « Expertise en renforcement de serveur » et du **cursus de certification Red Hat Certified Architect (RHCA)**.

Objectifs

Cette formation a pour objectif de vous apporter les connaissances pour comprendre le renforcement de la sécurité de Red Hat Enterprise Linux, en conformité avec les exigences des politiques de sécurité. Il existe effectivement un certain nombre de normes de sécurité, qui imposent à l'administrateur système de savoir agir et renforcer la protection d'un large choix de domaines (authentification des utilisateurs, mises à jour, audit du système, journalisation, intégrité des systèmes de fichiers, etc.). Ce cours vous apportera donc l'ensemble des compétences et savoirs pour maîtriser le durcissement de la sécurité d'un serveur Red Hat. Il se compose à la fois de modules théoriques et d'expériences pratiques pour exercer vos compétences en situation concrète. Cette formation prépare à **l'examen de certification Red Hat** – Expertise en renforcement de serveur (EX413), elle fait également partie du cursus de **certification Red Hat Certified Architect (RHCA)**.
A l'issue de cette formation, vous saurez :

- Réviser les errata et les appliquer à Red Hat Enterprise Linux.
- Utiliser les permissions spéciales et les listes de contrôle des accès aux systèmes de fichiers.
- Gérer les politiques de renouvellement de mots de passe et d'utilisateurs.
- Installer et configurer les outils de Red Hat Identity Management.
- Assurer l'audit du système.

Pré-requis

La participation à cette formation implique d'être **certifié RHCE ou RHCSA**, ou de maîtriser des connaissances de niveau égal.

Les formations ci-dessous sont recommandées.

Red Hat System Administration I

Public

Cette formation s’adresse aux professionnels IT impliqués dans l’amélioration et le maintien de la **sécurité des systèmes Red Hat Enterprise Linux.**

Cette formation s'adresse aux profils suivants

Administrateur système
Ingénieur système

Programme

- **Suivre les mises à jour de sécurité :** Ce module vous aide à comprendre le fonctionnement des mises à jour Red Hat Enterprise Linux et comment utiliser yum pour identifier les errata disponibles.
- **Administrer les mises à jour de logiciel :** Gestion et application des mises à jour du système.
- **Créer des systèmes de fichiers :** Ce module vous explique comment allouer un affichage avancé du système de fichier et comment le crypter.
- **Gérer les systèmes de fichiers :** Utilisez les options de sécurité et les attributs des systèmes de fichiers pour ajuster leurs propriétés.
- **Administrer les permissions spéciales :** Maîtrisez les permissions sticky (SVTX), set user ID (SUID) et set group ID (SGID), et localisez les fichiers équipés de ces permissions.
- **Administrer les contrôles des accès aux fichiers additionnels :** Utilisez les listes de contrôle d’accès aux fichiers et modifiez les permissions par défaut appliquées aux fichiers et répertoires.
- **Surveiller les changements de système de fichiers :** Configurez la surveillance logicielle des changements de fichiers.
- **Administrer les comptes utilisateurs :** Ce module vous apprend à paramétrer le renouvellement des mots de passe et à auditer les comptes utilisateurs.
- **Administrer les Pluggable Authentication Modules (PAMs) :** Renforcez les différents types de règles des utilisateurs grâce aux PAMs.
- **Sécuriser l’accès à la console :** Ajustez les propriétés des services de la console pour activer ou désactiver les paramètres de sécurité.
- **Installer l’authentification centrale :** Apprenez à installer et configurer le serveur et client Red Hat Identity Management.
- **Administrer l’authentification centrale :** Ce module explique comment configurer les règles de Red Hat Identity Management pour contrôler l’accès utilisateur aux systèmes clients, et les privilèges supplémentaires de ces utilisateurs.
- **Configurer la journalisation du système :** Configurer la journalisation à distance pour utiliser le cryptage de couche transport et gérer les logs supplémentaires générés par les systèmes distants.
- **Configurer l’audit du système :** Activez et configurez l’audit du système.
- **Contrôler l’accès aux services de réseau :** Apprenez à gérer les règles du pare-feu pour limiter la connectivité aux services de réseau.