Formation SELinux donné par RedHat

KB – mai 2014

1 FORMATION RHS429

http://fr.redhat.com/training/courses/rhs429/

1.1 CLASSROOM TRAINING

Red Hat propose des sessions de formation en salle de classe dans plus de 25 centres de formation en Europe. Les cours sont dispensés par des instructeurs certifiés Red Hat qui encouragent les étudiants à participer activement à des activités impliquant des tâches concrètes, à vérifier leurs connaissances en laboratoire et à dialoguer ouvertement.

Durée:4 days , 1st course day: 10.00-17.30 All other days: 09.00-17.30

Prix:€ 2,880

Unités de formation: 12

1.1.1 Public

- Administrateurs de systèmes Linux expérimentés responsables de la sécurité basée sur le contrôle MAC (Mandatory Access Control) ou souhaitant renforcer la sécurité de leurs services mis en réseau ou de leurs systèmes Linux existants
- Titulaires d'une certification RHCE désireux d'obtenir un certificat d'expertise Red Hat ou la certification Red Hat Certified Security Specialist (RHCSS)

1.1.2 Contenu cours

1.1.3 Introduction à SELinux

Contrôle d'accès discrétionnaire et contrôle d'accès obligatoire

- Présentation de l'historique de SELinux et de son architecture
- Éléments du modèles de sécurité de SELinux : rôles et identités des utilisateurs ; domaine et type ; sensibilité et catégories ; contexte de sécurité
- Politiques SELinux
- Configuration de politiques avec valeurs booléennes
- Archivage
- Configuration et affichage d'attributs étendus

1.1.4 Utilisation de SELinux

- Contrôle de SELinux
- Contexte des fichiers
- Ré-étiquetage des fichiers et systèmes de fichiers
- Options de montage

1.1.5 Politiques ciblées de Red Hat

- Identification et activation/désactivation des services protégés
- Contextes de sécurité Apache et valeurs booléennes de configuration
- Contextes de services de noms et valeurs booléennes de configuration
- Contextes de client NIS
- Autres services
- Contexte de fichiers pour arborescences d'annuaires spéciaux
- Résolution des problèmes et messages de refus avc
- Résolution et journalisation des problèmes liés à SE

1.1.6 Présentation des politiques

- Présentation et organisation des politiques
- Compilation et chargement des politiques monolithiques et des modules de politiques
- Syntaxe des modules d'application des types de politiques
- Classes d'objets
- Transition d'un domaine à un autre

1.1.7 Utilitaires de développement de politiques

- Outils disponibles pour manipuler et analyser des politiques : apol, seaudit et seaudit_report, checkpolicy, sepcut, sesearch, sestatus, audit2allow et audit2why, sealert, avcstat, seinfo, semanage et semodule, pages de manuel

1.1.8 Sécurité utilisateurs et rôles

- Contrôle des accès en fonction des rôles
- Sécurité multicatégorie
- Définition d'un administrateur de sécurité
- Sécurité multiniveau
- Politiques strictes
- Identification et déclaration d'utilisateurs
- Identification et déclaration de rôles
- Rôles utilisés dans les transitions
- Dominance des rôles

1.1.9 Anatomie d'une politique

- Macros des politiques

- Attributs et alias de types
- Transitions de type
- Étiquetage des fichiers
- restorecond
- Types personnalisables

1.1.10 Manipulation des politiques

- Installation et compilation des politiques
- Langage des politiques
- Vecteur d'accès
- Journaux SELinux
- Identificateurs de sécurité (SID)
- Comportement de l'étiquetage des systèmes de fichiers
- Contexte pour les objets réseau
- Création et utilisation des nouvelles valeurs booléennes
- Exemple de manipulation des politiques
- Macros
- Enableaudit

1.1.11 Projet

- Meilleures pratiques
- Création de contextes de fichiers, de types et d'alias de types
- Modification et création de contextes réseau
- Modification et création de domaines

Comprend :

- 4 jours de formation intensive sur Red Hat Enterprise Linux
- Des travaux pratiques et des exercices
- Repas du midi
- Une station de travail par étudiant
- Un manuel, des aides à l´étude, divers documents
- Articles promotionnels Red Hat

Toutes les autres dépenses et indemnités journalières sont à la charge de l´étudiant.

http://www.flane.fr/course/rh-s429#schedule

1.2 A QUI S'ADRESSE CETTE FORMATION

RHS429 est conçu pour les **experts en sécurité informatique** et autres **administrateurs systèmes** responsables de la définition et de l´implémentation des règles de sécurité sur un

ordinateur Linux. Les **programmeurs** d'applications peuvent également envisager de suivre ce cours afin de comprendre comment doter des applications tierces d'un ensemble de règles SELinux. Les participants ne doivent pas nécessairement avoir une connaissance approfondie de SELinux, mais doivent avoir des connaissances de base de la couche de sécurité SELinux. Par exemple, les informations SELinux apportées par le cours RH133 ou RH300 se révèlent suffisantes.

1.3 PRÉ-REQUIS

RHS429 nécessite des compétences de niveau RHCE. Les compétences préalables peuvent être mises en évidence par la réussite à l´examen RHCE par le cours RH-302 ou Accès rapide à RHCE (300), en suivant le cours RH-253 ou encore en possédant des connaissances et compétences comparables.

Prépare à :

Red Hat Enterprise SELinux Policy Administration Exam (EX429)

1.4 OBJECTIFS DE LA FORMATION

Parmi les fonctions les plus significatives de Red Hat Enterprise Linux, SELinux (Security Enhanced Linux) est une couche de sécurité puissante au niveau du noyau, qui permet un contrôle minutieux des accès des utilisateurs et des processus sur un système. SELinux est actif par défaut sur les systèmes Red Hat Enterprise Linux, ce qui permet de mettre en œuvre un ensemble de contrôles d'accès obligatoires que Red Hat qualifie de politique ciblée. Ces contrôles d'accès améliorent de façon substantielle la sécurité sur les services de réseau qu´ils ciblent, mais peuvent parfois altérer le comportement des applications tierces et des scripts qui fonctionnaient sous des versions précédentes de Red Hat Enterprise Linux.

RHS429 fournit une formation de quatre jours sur SELinux et sur l´écriture de règles SELinux. Le premier jour de cours présente une introduction à SELinux, son fonctionnement au sein de la politique ciblée de Red Hat et les outils utilisés pour le manipuler. Les jours restants sont ensuite consacrés à l'apprentissage de l'écriture, de la compilation et du débogage des règles.

Ceci se termine par un projet dans lequel les participants doivent créer entièrement un ensemble de règles destinées à un service jusqu´à présent dénué de protection. Les étudiants analysent le service et déterminent ses besoins en matière de sécurité, ils conçoivent et mettent en œuvre un ensemble de règles, testent et fixent les règles, documentent les nouvelles règles du service afin que d´autres personnes puissent administrer efficacement le service.

1.5 CONTENU DE LA FORMATION

Note: Technical content subject to change without notice. Reload this page regularly to insure up-to-date information.

1.5.1.1 Unit 1 - Introduction to SELinux

- Discretionary Access Control vs. Mandatory Access Control
- SELinux History and Architecture Overview
- Elements of the SELinux security model:
    - user identity and role
    - domain and type
    - sensitivity and categories
    - security context

- SELinux Policy and Red Hat´s Targeted Policy
- Configuring Policy with Booleans
- Archiving
- Setting and Displaying Extended Attributes
- Hands-on Lab: Understanding SELinux

1.5.1.2 Unit 2 - Using SELinux

- Controlling SELinux
- File Contexts
- Relabeling Files and Filesystems
- Mount options
- Hand-on Lab: Working with SELinux

1.5.1.3 Unit 3 - The Red Hat Targeted Policy

- Identifying and Toggling Protected Services
- Apache Security Contexts and Configuration Booleans
- Name Service Contexts and Configuration Booleans
- NIS Client Contexts
- Other Services
- File Context for Special Directory Trees
- Troubleshooting and avc Denial Messages
- setroubleshootd and Logging
- Hands-on Lab: Understanding and Troubleshooting the Red Hat Targeted Policy

1.5.1.4 Unit 4 - Introduction to Policies

- Policy Overview and Organization
- Compiling and Loading the Monolithic Policy and Policy Modules
- Policy Type Enforcement Module Syntax
- Object Classes
- Domain Transition
- Hands-on Lab: Understanding policies

1.5.1.5 Unit 5 - Policy Utilities

- Tools available for manipulating and analyzing policies
    - apol
    - seaudit and seaudit_report
    - checkpolicy
    - sepcut
    - sesearch
    - sestatus
    - audit2allow and audit2why
    - sealert
    - avcstat
    - seinfo
    - semanage and semodule
    - Man pages

- Hands-on Lab: Exploring Utilities

1.5.1.6 Unit 6 - User and Role Security

- Role-based Access Control
- Multi Category Security
- Defining a Security Administrator
- Multi-Level Security
- The strict Policy
- User Identification and Declaration
- Role Identification and Declaration
- Roles in Use in Transitions
- Role Dominance
- Hands-on Lab: Implementing User and Role Based Policy Restrictions

1.5.1.7 Unit 7 - Anatomy of a Policy

- Policy Macros
- Type Attributes and Aliases
- Type Transitions
- When and How do Files Get Labeled
- restorecond
- Customizable Types
- Hands-on Lab: Building Policies

1.5.1.8 Unit 8 - Manipulating Policies

- Installing and Compiling Policies
- The Policy Language
- Access Vector
- SELinux logs

- Security Identifiers - SIDs
- Filesystem Labeling Behavior
- Context on Network Objects
- Creating and Using New Booleans
- Manipulating Policy by Example
- Macros
- Enableaudit
- Hands-on Lab: Compiling Policies

1.5.1.9 Unit 9 - Project

- Best practices
- Create File Contexts, Types and Typealiases
- Edit and Create Network Contexts
- Edit and Create Domains
- Hands-on Lab: Editing and Writing Policy