Hewlett Packard Enterprise

RHEL SELinux Policy Administration (GL429) H8PB2S

This advanced security course takes a deep dive into the complexities and nuances of SELinux. The course discusses security threats posed to today's computing resources and mitigating them through network and host protections. Students will review SELinux technology through understanding SELinux's goals, how it has evolved including its features and limitations.

Students will gain hands-on experience in working with SELinux modes, virtualization, and container security. The core of the course is learning and understanding SELinux policy through choosing, managing, and studying policy examples. Once students have an understanding of the SELinux policy, the course will cover writing policy modules. The course is capped off with multiple discussions on case studies that explore building SELinux policies. This SELinux course covers one of the major challenges faced by administering SELinux, SELinux troubleshooting.

HPE course number	H8PB2S
Course length	3 Days
Delivery mode	ILT, VILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

Why HPE Education Services?

- IDC MarketScape leader 5 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and SUSE
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

Prerequisites

The U8583S "Linux Fundamentals" and H7091S "Enterprise Linux Systems Administration courses.

Supported distributions

Red Hat Enterprise Linux 7

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, October 2017

Detailed course outline

Module 1: Computing Security & SELinux Overview	• Security Threats • Network and Host Protection • Shortcomings of Traditional Unix Security • DAC vs. MAC • SELinux Goals • SELinux Evolution • SELinux Features and Limitations • SELinux Context	• Labels • Access Decisions • Transition Decisions: Processes • SELinux Example Lab Tasks • System Preparation • Contexts
Module 2: Working with SELinux	• SELinux Modes • Gathering SELinux Information • SELinux Virtual Filesystem • Core Commands and SELinux • SELinux Management Utilities • Context and File Operations • Managing File Context Database • Managing Contexts • Booleans • SELinux Mount Options • Virtualization Security	• Container Security • Securing Networked Services • Managing Port Contexts Lab Tasks • Exploring SELinux Modes • Gathering Information • Managing SELinux Booleans • Managing Contexts • Mounting Filesystems • Manual Relabel • GUI Utilities
Module 3: Policies	• The SELinux Policy • Choosing an SELinux Policy • Policy Layout • Examining Policy • Managing Policies • Targeted Policy • Targeted Policy Example: Apache	• Targeted Policy Example: Other Contexts • Minimum Policy • MLS Policy Overview • MCS Translation • Polyinstantiated Directories
Module 4: Users & Roles	• Overview of Roles • Roles • User Mappings • Kiosk User (xguest) • Controlling Application Execution	Lab Tasks • SELinux Identities and Roles • Kiosk User
Module 5: Troubleshooting SELinux	• Access Denied. Now what? • AVC Denied Examples • Incorrect File Context	• Permissive Domains • Using audit2allow Lab Tasks • Troubleshooting using Permissive Domains • Using audit2why and audit2allow to create policy

Module 6: Writing Policy Modules	• SELinux Policy Tools • SELinux Policy Source • Reference Policy Source Exploration • Process Transitions • Object classes • Policy Macros • Creating Booleans • Using Booleans in Policies • Other Policy Commands	• Writing Policy Modules Lab Tasks • Domain Transition Exploration • Exploring SELinux Modes • Writing a Simple Module • Defining and using booleans • Creating & Compiling Policy from Source • Using seplogen
Module 7: Case Study: Securing an Application	• SELinux Policy Building: Case Study 1	
Module 8: Case Study: Securing an Application	Lab Tasks • SELinux Policy Building: Case Study 2	
Module 9: Bonus Labs:	Lab Tasks • Installing and Switching Policies • Minimum policy	• MCS Exploration • MCS Restrictions • Polyinstantiated Directories

Learn more at

hpe.com/ww/learnlinux

Follow us:

a00037766enw, December 2017, H8PB2S A.00

Hewlett Packard Enterprise