

Course Description: RHS429 introduces advanced system administrators, security administrators, and applications programmers to SELinux policy writing. Participants in this course will learn how SELinux works; how to manage SELinux; and how to write an SELinux policy. This class culminates in a major project to scope out and then write policies for previously unprotected services.

Who Should Attend: RHS429 is designed for computer security specialists and other system administrators responsible for setting and implementing security policies on a Linux computer. Applications programmers also may consider taking the course to understand how to provide a set of SELinux policies for third party applications. Participants need not have indepth knowledge of SELinux, but should have a basic understanding of the SELinux security layer. For example, SELinux information as taught in RH133 or RH300 is sufficient.

Prerequisites: RHS429 requires RHCE-level skills. Prerequisite skills can be shown by passing the RHCE Exam in either RH302 or RH300, or by taking RH253 or by possessing comparable skills and knowledge.

Benefits of Attendance: Upon completion of this course, students will be able to:

- Understand how SELinux operates within the Red Hat targeted policy.
- Understand how policies are written, compiled, and debugged.
- Create a set of policies from scratch for a previously unprotected service.
- Analyze the service, determining its security needs.
- Design and implement a set of policies.
- Test and fix the policies.
- Document the service's new policies so that others can effectively administer the service.