

RHS429 Red Hat Enterprise SELinux Policy Administration

Goal:

Among the most significant features of Red Hat Enterprise Linux is SELinux (Security Enhanced Linux), a powerful, kernel-level security layer that provides fine-grained control over what users and processes may access and execute on a system. By default, SELinux is enabled on Red Hat Enterprise Linux systems, enforcing a set of mandatory access controls that Red Hat calls the targeted policy. These access controls substantially enhance the security of the network services they target, but can sometimes affect the behavior of third-party applications and scripts that worked under previous versions of Red Hat Enterprise Linux.

RHS429 provides a four day tutorial on SELinux and SELinux policy writing. The first day of the course provides a introduction to SELinux, how it operates within the Red Hat targeted policy, and the tools used to manipulate it. The class then will spend the remaining days learning how policies are written, compiled, and debugged.

This culminates in a project in which participants will create a set of policies from scratch for a previously unprotected service. The class will 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.

Audience:

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.

Note that [RHS427](#) is **not** a prerequisite to this course; rather, that one day introduction to SELinux constitutes the first day of this course: the remaining three days cannot be taken separately.

Contents

- ➔ Introduction to SELinux
- ➔ Using SELinux
- ➔ The Red Hat Targeted Policy
- ➔ Introduction to Policies
- ➔ Policy Utilities
- ➔ User and Role Security
- ➔ Anatomy of a Policy
- ➔ Manipulating Policies