RHS429-Bundle: Red Hat Enterprise SELinux Policy Administration + EX429

Duration: 5 Days **Course Code: RH430**

Overview:

Security-enhanced Linux® (SELinux) is a powerful, kernel-level security layer that provides fine-grained control over which users and processes may access which resources and execute which programs on a system. Red Hat® Enterprise SELinux Policy Administration (RHS429) introduces senior system administrators, security administrators, and application programmers to SELinux policy writing. Students will learn how SELinux works and how to manage, write, compile, and debug an SELinux policy. This class culminates in a major project to analyze, determine the security needs of, and design and implement a set of net new policies for a service previously unprotected by SELinux.
A Red Hat Certified Engineer (RHCE®) who successfully completes this course is prepared to take the Red Hat Enterprise SELinux Policy Administration Expertise Exam (EX429). Exam sold separately.

Target Audience:

Experienced Linux system administrators responsible for Mandatory Access Control-based (MAC) security, or who want to harden their existing Linux system or networked services security and RHCEs interested in earning a Red Hat Certificate of Expertise or a Red Hat Certified Security Specialist (RHCSS) certification.

Objectives:

- 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

Prerequisites:

- The essential elements of how to configure the services covered, as this course focuses on more advanced topics
- RHCE certification or equivalent experience

Testing and Certification

- Red Hat Enterprise SELinux Policy Administration Expertise Exam (EX429) Hands-on, performance-based, 4-hour exam with 2 sections.
- This course prepares you for these credentials:
- Certificates of Expertise
- Red Hat Certified Security Specialist — RHCSS

Follow-on-Courses:

- RHS333, Red Hat Enterprise Security Network Services
- RH423, Red Hat Enterprise Directory Services and Authentication

Content:

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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- SELinux history and architecture overview
- Elements of the SELinux security model:

Introduction to policies

- Policy overview and organization
- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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

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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- Apache security contexts and configuration

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- SELinux history and architecture overview
- Elements of the SELinux security model: user identity and role; domain and type;

- Archiving
- Setting and displaying extended attributes
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

Manipulating policies

- Installing and compiling policies

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- Apache security contexts and configuration booleans

booleans
- Name service contexts and configuration booleans
- NIS client contexts
- Other services
- File context for special directory trees
- Troubleshooting and avc denial messages
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax

sensitivity and categories; security context
- SELinux policy and Red Hat's targeted policy
- Configuring policy with booleans
- Archiving
- Setting and displaying extended attributes
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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

Name service contexts and configuration booleans
- NIS client contexts
- Other services
- File context for special directory trees
- Troubleshooting and avc denial messages
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases

- Setting and displaying extended attributes
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

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

User and role security

- Role-based access control

- SELinux history and architecture overview
- Elements of the SELinux security model:

- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions

- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

Using SELinux

- Controlling SELinux

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Edit and create network contexts
- Edit and create domains

- Archiving
- Setting and displaying extended attributes
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options

- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- Apache security contexts and configuration booleans
- Name service contexts and configuration booleans
- NIS client contexts
- Other 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

The Red Hat® targeted policy

- Identifying and toggling protected services
- 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
- File contexts
- Relabeling files and file systems
- Mount options
- Apache security contexts and configuration booleans
- Name service contexts and configuration booleans

- File context for special directory trees
- Troubleshooting and avc denial messages
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes

- Name service contexts and configuration booleans
- NIS client contexts
- Other services
- File context for special directory trees
- Troubleshooting and avc denial messages
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- NIS client contexts
- Other services
- File context for special directory trees
- Troubleshooting and avc denial messages
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security

- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions

- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond

- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond

- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit

- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector

- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

Project

- Best practices

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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

- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

Anatomy of a policy

- Policy macros

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts

policy
- Configuring policy with booleans
- Archiving
- Setting and displaying extended attributes
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- Apache security contexts and configuration booleans
- Name service contexts and configuration booleans

- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit

- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- NIS client contexts
- Other services
- File context for special directory trees
- Troubleshooting and avc denial messages
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

- 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
- File contexts
- Relabeling files and file systems
- Mount options
- 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
- SE troubleshooting and logging
- Compiling and loading the monolithic policy and policy modules
- Policy type enforcement module syntax
- Object classes
- Domain transition
- Multicategory security
- Defining a security administrator
- Multilevel security
- The strict policy
- User identification and declaration
- Role identification and declaration
- Roles in use in transitions
- Role dominance
- Type attributes and aliases
- Type transitions
- When and how files get labeled
- restorecond
- Customizable types
- The policy language
- Access vector
- SELinux logs
- Security Identifiers - SIDs
- File system labeling behavior
- Context on network objects
- Creating and using new booleans
- Manipulating policy by example
- Macros
- Enableaudit
- Create file contexts, types, and typealiases
- Edit and create network contexts
- Edit and create domains

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.qa

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar