15.8.3 SELinux Facts

This lesson covers the following topics:

- Mandatory Access Control
- SELinux policies
- Security context
- Commands

Mandatory Access Control

Security-Enhanced Linux (SELinux) is a Linux kernel security module that provides a strong and flexible, mandatory access control (MAC) system for the Linux kernel. It can be used to enforce access control on resources based on variables, such as users and applications. Standard Linux uses access controls, such as granting permission using read, write, and execute, that can be modified by users and also by applications. SELinux enhances security by using policies to restrict access based on variables, such as user, role, type, and, optionally, level.

With SELinux, access controls are determined by an SELinux policy. Using this type of implementation, SELinux access controls:

- Can only be added, deleted, or changed by an administrator. This prevents users or applications from making access changes.
- Provides finer granularity in permission, such as the ability to unlink, append only, and move a file.
- Extends access control to many resources, such as network resources and interprocess communication (IPC).

> SELinux is designed to enhance existing security solutions, not replace them. It is not a replacement for antivirus software, passwords, firewalls, or other security systems. It is not an all-in-one security solution.

SELinux Policies

When SELinux is enabled, policies are used to determine how and what items are protected. Policies are a set of rules that guide the SELinux security engine.

There are two types of policies:

- Targeted policies apply access controls to certain (targeted) processes. Targeted processes run in a confined domain. Processes that are not targeted run in an unconfined domain.
- Multi-level Security (MLS) policies specify multiple levels of access. MLS applies labels to files, processes and other system objects to control the flow of information between security levels. Each level has different rules for user access. Labels for security levels might range from top secret to unclassified.

In addition to types of policies, SELinux uses modes to control how policies are applied and how access is granted or denied. There are two modes:

- Enforcing mode allows or denies access based on policy rules. Any attempted action that occurs on the system that is against the defined policy is blocked and logged.
- Permissive mode allows access even if the access violates SELinux policy rules. However, it does log any action that violates policy rules.

> Use permissive mode to troubleshoot or test a new SELinux system, or one that you've changed. You can switch between the two modes without a system reboot.

Security Context

SELinux uses a *security context,* also referred to as a *security label*, to classify resources, such as processes and files. This context specifies how and by whom a given resource can be accessed. The security context of files and processes are listed in the /etc/sestatus.conf file.

A security context is typically shown as a string of three or four words. Each word specifies a different component of the security context, namely the user, role, type, and level of that file or process. Each word is separated by a colon as shown:

Commands

The following table identifies commands you use with SELinux.

Command	Function	Example
sestatus	Displays status of a system running SELinux. The information it displays includes: • SELinux status: enabled or disabled	**sestatus** displays status of SELinux system

	• Loaded policy type: targeted or MLS • Current mode: permissive or enforcing	
getenforce	Displays the current SELinux mode: Enforcing, Permissive, or Disabled.	**getenforce** displays mode of SELinux system
setenforce	Switches between permissive and enforcing mode. The command syntax is **setenforce** *mode value.* You must have root level permission to run this command. Change the /etc/sestatus.conf to permanently change the mode or disable SELinux.	**setenforce Enforcing 1** turns on Enforcing mode **setenforce Permissive 1** turns on Permissive mode
getsebool	Displays a list of booleans. Booleans allow you to change part of the SELinux policy at run time without reloading or recompiling the SELinux policy. Enter: • **getsebool -a** to view the value of all booleans. • **getsebool** *boolean* to view the value of the specified boolean.	**getsebool -a** lists all booleans **getsebool allow_console_login** to view the status of the allow_console_login boolean
setsebool	Changes the current state of an SELinux boolean. • **setsebool** *boolean_name switch* turns the specified boolean on or off. • Add **-P** to make the change permanent. the command.	**setsebool allow_console_login --> off** turns off the allow_console_login boolean **setsebool -P allow_console_login --> on** permanently turns on the allow_console_login boolean
ls	Displays the SELinux context for a specified file by using the -Z parameter. **ls -Z** *filename*.	**ls -Z /user/bin/pkexec** displays the context of the /user/bin/pkexec file.
ps	Displays the SELinux context for all active processes by using the **-eZ** parameter.	**ps -eZ** displays all active processes **ps -eZ | grep ibus** displays the active processes for ibus