

Configuring SELinux in Centos

Topics : Centos Server **Written on** March 05, 2024

SELinux (Security-Enhanced Linux) is a mandatory access control (MAC) security mechanism built into the Linux kernel that provides fine-grained access control policies and enhances system security by enforcing access restrictions based on security policies. Here's how you can configure SELinux on CentOS:

1. Check SELinux Status:

• Before configuring SELinux, check its current status using the following command:

sestatus

• This command will display whether SELinux is enabled, disabled, or in permissive mode.

2. Enabling or Disabling SELinux:

- To enable or disable SELinux, you can edit the /etc/selinux/config file and set the SELINUX parameter to enforcing, permissive, or disabled.
- For example, to enable SELinux in enforcing mode:

SELINUX=enforcing

• After making changes, reboot the system for the changes to take effect.

3. Changing SELinux Modes:

- Enforcing mode: In this mode, SELinux policies are enforced, and violations are logged and denied.
- Permissive mode: In this mode, SELinux policies are not enforced, but violations are logged for analysis.
- Disabled mode: In this mode, SELinux is completely disabled, and no security policies are applied.

4. Setting SELinux Contexts:

- SELinux assigns security contexts (labels) to files, processes, and network ports to enforce access controls.
- Use commands like ls -Z, ps -Z, or netstat -Z to view SELinux contexts.
- Use choon or restorecon commands to change or restore SELinux contexts for files and directories.

5. Managing SELinux Booleans:

- SELinux booleans are tunable parameters that modify SELinux policies to allow or deny specific behaviors.
- Use the getsebool and setsebool commands to view and modify SELinux booleans, respectively.
- For example, to allow Apache to connect to network services, use:

setsebool -P httpd can network connect on

6. Auditing and Troubleshooting:

- Use audit tools like auditd and ausearch to monitor SELinux audit logs for policy violations and security incidents.
- Analyze audit logs to troubleshoot SELinux-related issues and refine security policies.

7. Configuring SELinux Policy Modules:

- Customize SELinux policies using policy modules to define access controls for specific applications or services.
- Use tools like semodule to manage SELinux policy modules.

8. SELinux Management Tools:

- CentOS provides utilities like sestatus, semanage, setroubleshoot, and audit2allow for managing and troubleshooting SELinux.
- Use these tools to monitor SELinux status, configure SELinux policies, troubleshoot policy violations, and generate policy exceptions.

© Copyright Aryatechno. All Rights Reserved. Written tutorials and materials by Aryatechno