

# RedHat Certified System Administrator (RHEL 9)

## SUMMARY

### SELinux Context

- SELinux uses contexts to label files, processes, ports, and so on.
- SELinux contexts are composed of three parts:
  - User
  - Role
  - Type: The only part that is relevant to the RHCSA exam.
- Check the SELinux context of a file with the following command:
  - `ls -Z file`
- Change the SELinux context of a file with two methods:
  - chcon: Change the SELinux context of a file temporarily. (Never use it)
  - semanage: Change the SELinux context of a file permanently. (More in the man page `man semanage-fcontext`)
    - `semanage fcontext -m -t type file`
    - `restorecon -v file`
- Check the SELinux context of a process with the following command:
  - `ps -eZ | grep process`
- Check the SELinux context of a port with the following command:
  - `semanage port -l | grep port`
- Change the SELinux context of a port with the following command:
  - `semanage port -m -t type -p protocol port`

## SELinux Booleans

- SELinux booleans are used to enable or disable SELinux features.
- Check the SELinux booleans with the following command:
  - ``semanage boolean -l``
  - ``getsebool -a``
- Change the SELinux booleans with the following command:
  - ``setsebool -P boolean on``
  - -P: Make the change permanent.
  - You can check if the change is permanent: ``semanage boolean -l | grep boolean``

## SELinux Troubleshooting

- Check the SELinux logs with the following command:
  - ``grep -i avc /var/log/messages``
    - avc: Access Vector Cache
  - ``sealert -a /var/log/audit/audit.log``