

# 15.8.5 Practice Questions

**Candidate:** Ethan Bonavida (suborange)

**Date:** 12/9/2022 12:30:00 am • **Time Spent:** 00:21

**Score: 100%**

Passing Score: 80%

▼ **Question 1:**      ✓ Correct

You are a network administrator for your company. A user calls to complain that his Firefox browser is not working as it did the day before. Knowing that you recently updated the SELinux profile for Firefox, you suspect the change you made is causing the issue. You want to troubleshoot the issue by switching the profile to permissive mode.

Which of the following is the BEST command to use in this situation?

- ☐ **setsebool**
- ☐ **sestatus**
- ☐ **getenforce**
- ➡ ☒ **setenforce**

## Explanation

**setenforce** switches between permissive and enforcing mode. The command syntax is **setenforce mode value**.

**setsebool** changes the current state of an SELinux boolean.

**sestatus** displays the status of a system running SELinux.

**getenforce** displays the current SELinux mode (Enforcing, Permissive, or Disabled).

## References

 15.8.3 SELinux Facts

q\_selinux\_lp5\_setenforce.question.fex


## ▼ Question 2:

✓ Correct

You were recently asked to manage the SELinux implementation at your company. Since you are still coming up to speed on this technology, you have not yet mastered the process of creating or making major changes to SELinux policies.

However, an employee has just called you complaining that they don't seem to be able to accomplish a task with a particular application. After scanning through the SELinux policy for that application, you notice that there is a method that can be used to enable the desired function.

Which of the following is the BEST command for enabling that feature without editing the policy?

- ☐ **sestatus**
- ☐ **ls -Z *application\_name***
-  ☒ **setsebool**
- ☐ **setenforce**
- ☐ **getenforce**

**Explanation**

**setsebool** changes the current state of an SELinux boolean. This command is used to make the change immediately. But unless the **-P** switch is used, at the next boot, it will revert back to the defaults.

**setenforce** switches between permissive and enforcing mode. The command syntax is **setenforce mode value**.

**sestatus** displays the status of a system running SELinux.

**getenforce** displays the current SELinux mode (Enforcing, Permissive, or Disabled).

**ls -Z *application\_name*** displays the SELinux context for a specified file by using the **-Z** parameter.


**References** **15.8.3 SELinux Facts**

q\_selinux\_lp5\_setsebool.question.fex

**▼ Question 3:**      **✓ Correct**

As the network administrator, one of your responsibilities is to analyze and troubleshoot SELinux context violations.

In which directory are the SELinux violations recorded?

- ☐ /var/log/firewalld
-  ☒ /var/log/audit
- ☐ /var/log/secure
- ☐ /var/log

**Explanation**

/var/log/audit is the directory where SELinux violations are recorded as Access Vector Cache (AVC) event errors. The entries are stored in the audit.log files.

/var/log/secure contains information related to authentication and authorization privileges.

/var/log/firewalld contains information related to the local firewall.

/var/log is the main folder where logs are stored.

**References**

 **15.8.4 SELinux Troubleshooting Facts**

q\_selinux\_lp5\_avc.question.fex

## ▼ Question 4:

✓ Correct

Which of the following is the BEST command for viewing SELinux errors?

- ➡ ☒ **sealert**
- ☐ **semanage**
- ☐ **getenforce**
- ☐ **getsebool**

#### Explanation

**sealert** is used to view SELinux errors. If not run from the GUI interface, you would run `sealer -a /var/log/audit/audit.log`.

**semanage** is used to configure certain elements of SELinux policy without requiring modification to or recompilation from policy sources.

**getenforce** displays the current SELinux mode (Enforcing, Permissive, or Disabled).

**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.

#### References

 15.8.4 SELinux Troubleshooting Facts

q\_selinux\_lp5\_sealert.question.fex

Copyright © 2022 TestOut Corporation All rights reserved.