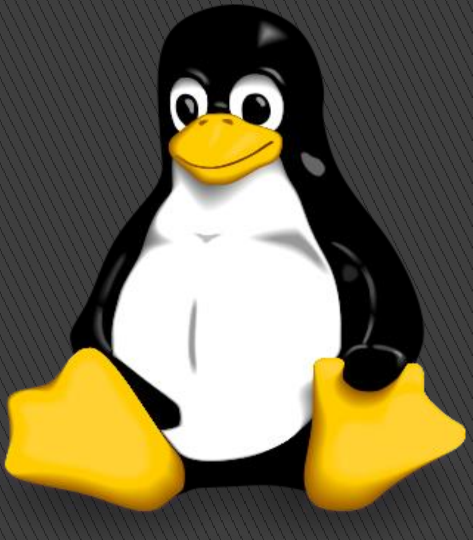
SELinux

Secure Enhanced Linux

What is SELinux

- SELinux gives that extra layer of security to the resources in the system.
- It is designed to protect the server against misconfigurations and compromised daemons.
- It put limits and instructs server daemons what files they can access and what actions they can take by defining a security policy.



Mode of SELinux

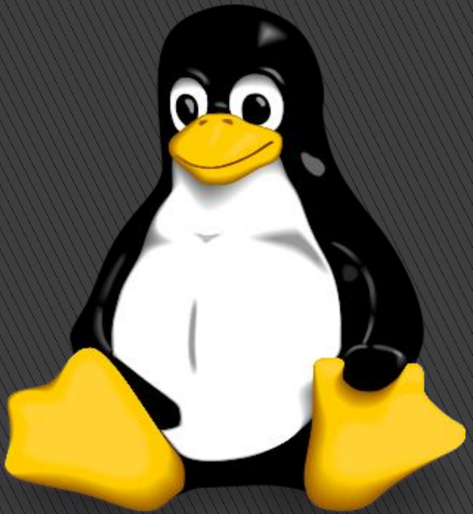
There are three mode

1. Enforcing
2. Permissive
3. Disabled

1. Enforcing

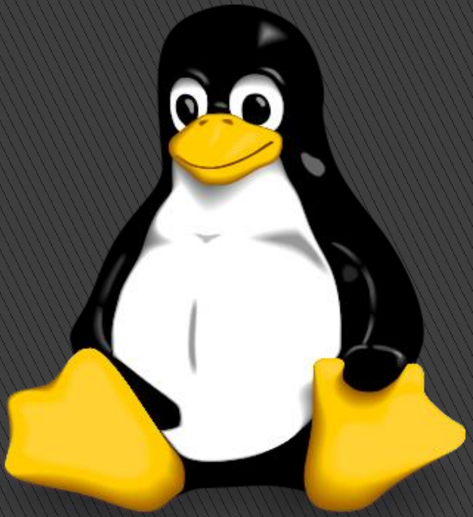
SELinux security policy is enforced.

IF this is set SELinux is enabled and will try to enforce the SELinux policies strictly



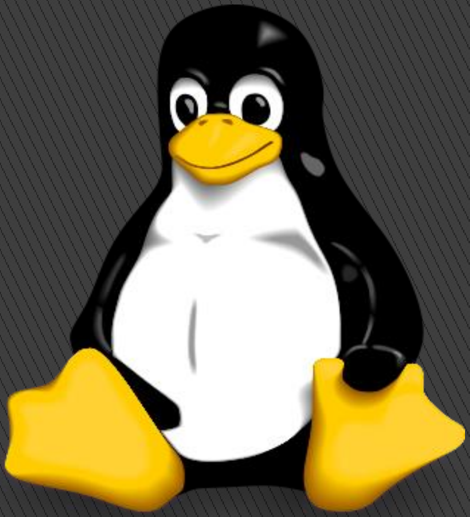
2. Permissive

SELinux prints warnings instead of enforcing. This setting will just give warning when any SELinux policy setting is breached



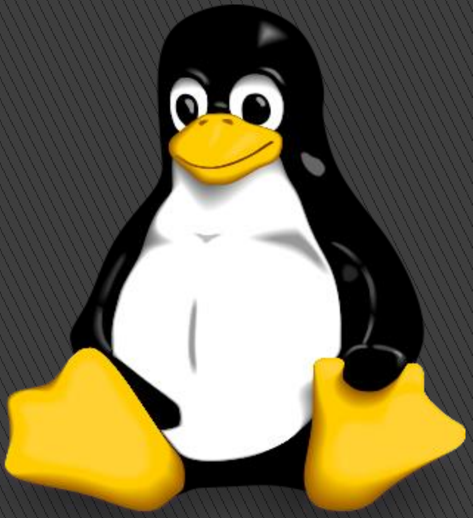
3. Disabled

No SELinux policy is loaded. This will totally disable SELinux policies.



For Check Current SELinux mode

```
#getenforce
```



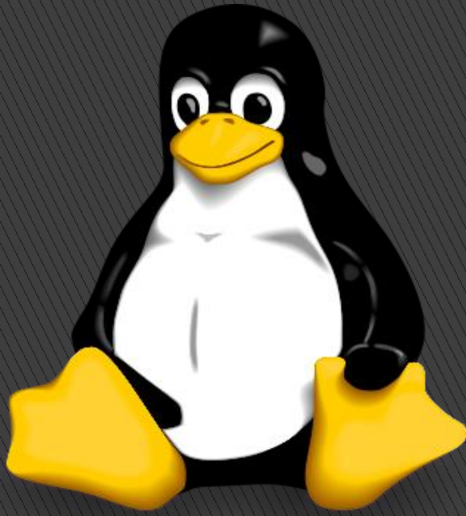
For Change SELinux Mode

```
#setenforce      0
      or
#setenforce      permissive
```

Note:

0 -for permissive

1 -for enforcing

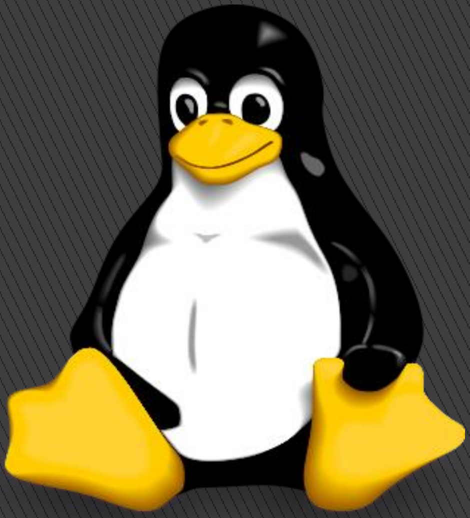


For Change SELinux mode permanently

```
#vim          /etc/selinux/config

        SELINUX=enforcing

:wq (for write & quit)
```



Exam Que on SELinux

Set your system to enforcing mode permanently