# SELinux

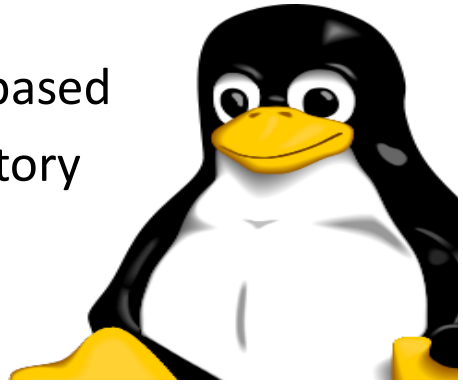
Secure Enhanced Linux

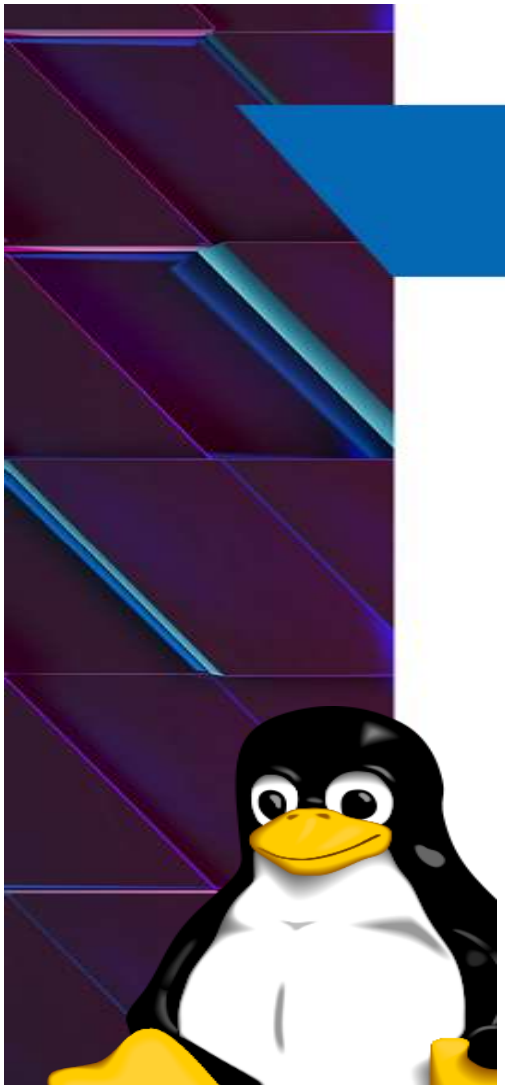
# What is SELinux

Security Enhanced Linux (SELinux) is an additional layer of system security. A primary goal of SELinux is to protect user data from system services that have been compromised.

Most Linux administrators are familiar with the standard user, group and other permission security model, known as Discretionary access control.

SELinux provide an additional layer of security that is object-based and controlled by more sophisticated rules, known as mandatory access control.





# Eg.

To allow remote anonymous access to a web server, firewall ports must be opened. However, this gives malicious people an opportunity to crack the system through a security exploit, and if they compromise the web server process, gain its permissions, the permission of the apache user and apache the group.

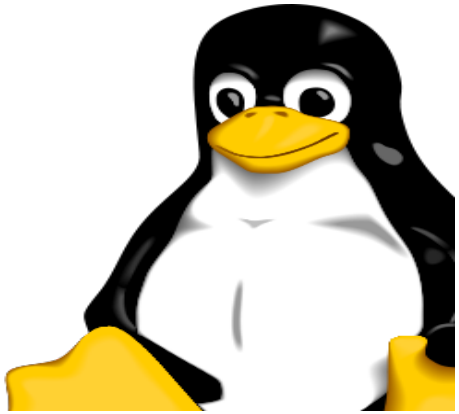
SELinux is a set of security rules that determine which process can access which files, directories and ports.

Every file, process, directory and port has a special security label called a SELinux context.

# Mode of SELinux

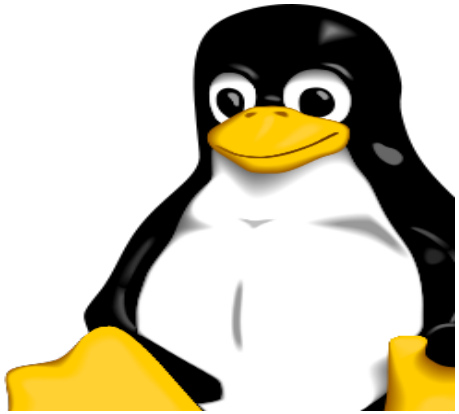
There are three mode

1. Enforcing
2. Permissive
3. Disabled



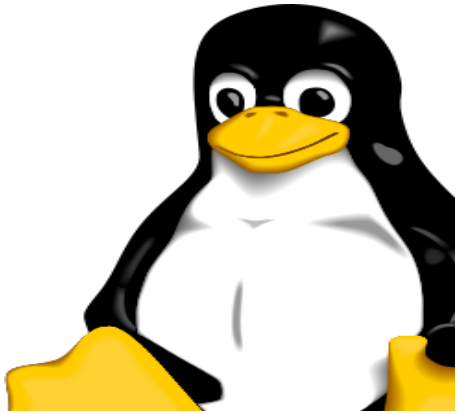
# 1. Enforcing

SELinux denies access based on SELinux policy rules, a set of guidelines that control the security engine.



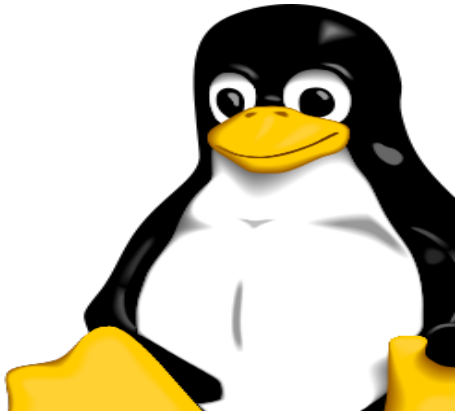
# 2. Permissive

SELinux does not deny access, but denials are logged for actions that would have been denied if running in enforcing mode.



# 3. Disabled

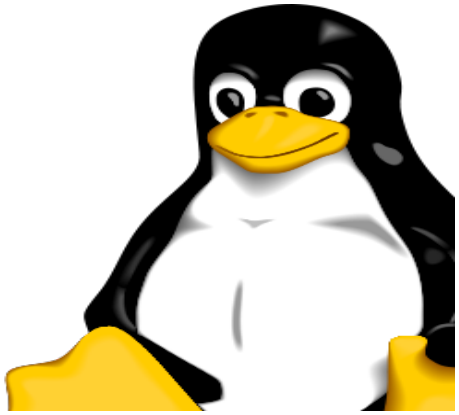
No SELinux policy is loaded. This will totally disable SELinux policies.



# For Check Current SELinux mode

#getenforce

#sestatus



# Set SELinux Mode Temporary

#setenforce 0

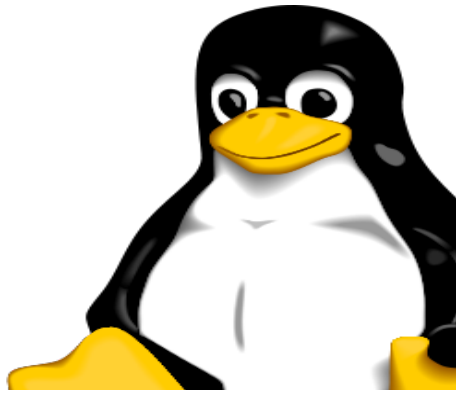
or

#setenforce Permissive

Note:

0 -for Permissive

1 -for Enforcing



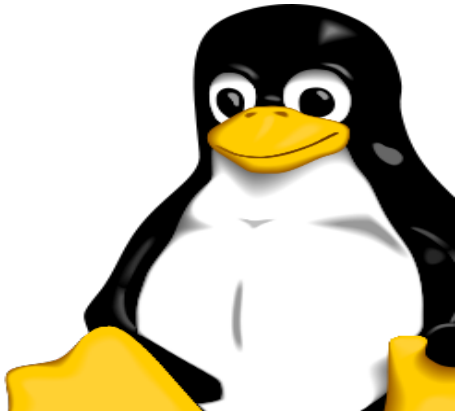
# Set SELinux mode permanently

#vim /etc/selinux/config

SELINUX=**enforcing**

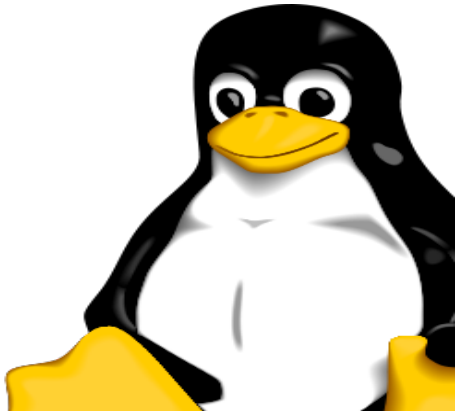
:wq (for write & quit)

#reboot



# SELinux File Labeling

- All files, directories, devices, and processes have a security context (or label) associated with them.
- For files, this context is stored in the extended attributes of the file system.



# Viewing SELinux context information

**View SELinux context information about files**

To view the file system context information from the command line, use the "**ls –Z**" command:

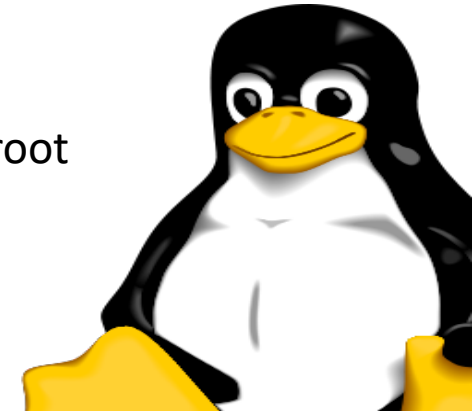
#ls -ldZ /india

#ls -lZ note.txt

**Eg.**

#ls -ldZ /root

dr-xr-xr-x. root root system_u:object_r:admin_home_t:s0 /root



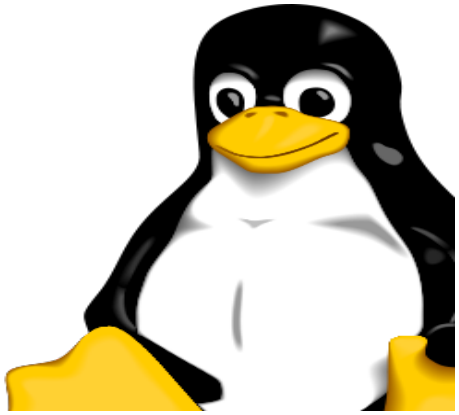
# Viewing SELinux context information

**View SELinux default context information**

```
#ls     -ldZ     /root
#ls     -ldZ     /home/student
#ls     -ldZ     /var
#ls     -ldZ     /etc
#ls     -ldZ     /tmp
```

**View SELinux default context for file or directory**

```
#mkdir    /root/data
#mkdir    /database
#ls     -ldZ     /root/data
#ls     -ldZ     /database     (it got default label)
```



# SELinux context http process

**View SELinux default context information  for httpd process**

#ps -efZ | grep httpd

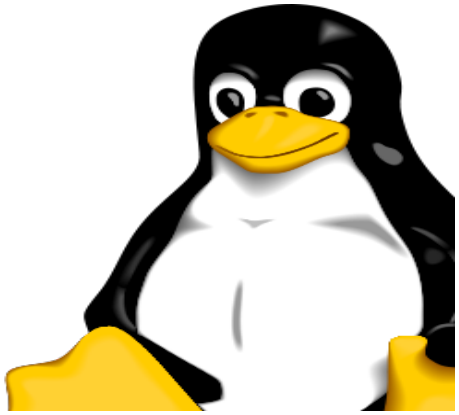
**httpd process can access**

#ls -ldZ /var/www

#ls -ldZ /etc/www/html

#ls -ldz /etc/httpd

#ls -ldz /var/log/httpd



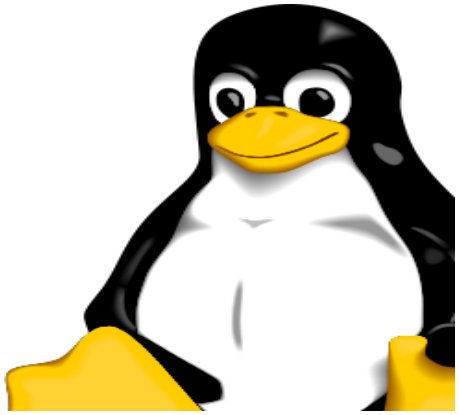
# Apache web hosting default directory

#systemctl start httpd
#systemctl enable httpd
#echo “Sample web page” > /var/www/html/index.html

#systemctl restart httpd

**Open Firefox and verify web page open or not**
http://192.168.1.10

#ls -ldZ /var/www/html
#ls -ldZ /var/www/html/index.html



# Apache web hosting different directory

#mkdir /usr/local/web

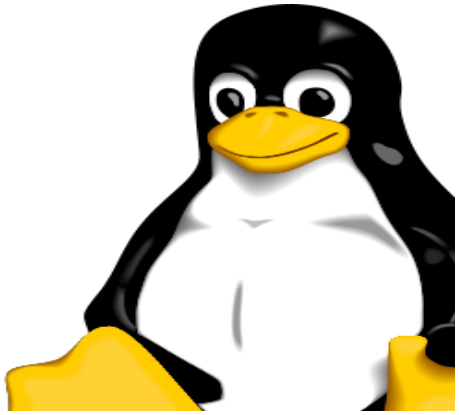
#echo "Web hosting on manual directory" > /usr/local/web/index.html

#vim /etc/httpd/conf.d/server1.conf

```
<VirtualHost *:80>
ServerAdmin root@server1.example.com
ServerName server1.example.com
DocumentRoot /usr/local/web/
</VirtualHost>
<Directory "/usr/local/web/">
Require all granted
</Directory>
```

:wq

#systemctl restart httpd

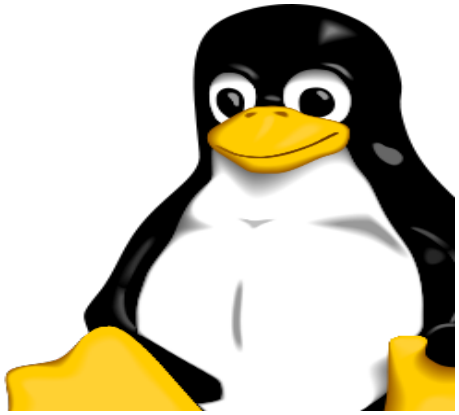


# Verify Web site open or not

#vim /etc/hosts
192.168.1.10 server1.example.com
:wq

Open Firefox and verify web page open or not
http://server1.example.com

#ls -ldZ /usr/local/web
#ls -ldZ /var/www/html/index.html
#getenforce
#setenforce 0
#getenforce
Now verify again in Firefox

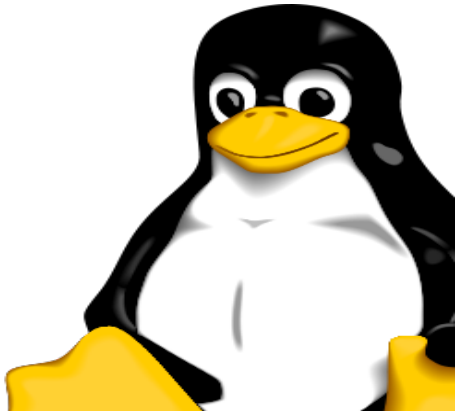


# Check SELinux Log messages

#cat /var/log/messages | grep httpd

For Detail Info

#sealert -l a4f6a-abc123re-kh235k-2ilg76i



# Change SELinux lable

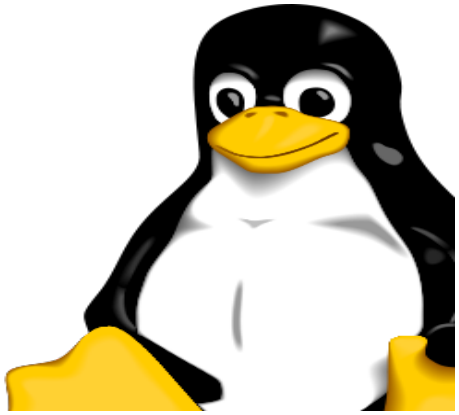
```
#chcon   -t   httpd_sys_content_t     /usr/local/web

#chcon   -t   httpd_sys_content_t     /usr/local/web/index.html

#ls    -ldZ        /usr/local/web
#ls    -ldZ        /usr/local/web/index.html
```

**Open Firefox and verify web page open or not**

http://server1.example.com



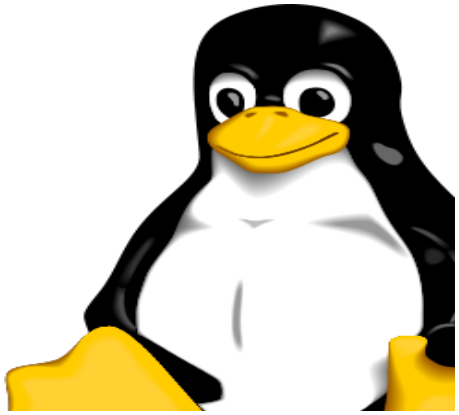
# Relabel default label using restorcon

Restorcon command is uses to set default file context.

```
#ls        -ldZ     /usr/local/web
#ls        -ldZ     /usr/local/web/index.html
#restorecon     -Rv    /usr/local/web/
```

**Verify SELinux label again**

```
#ls        -ldZ     /usr/local/web
#ls        -ldZ     /usr/local/web/index.html
```



# Chcon work temporary

Chcon command set label temporary means after restore default label, label reset and change as per the default policy like above example

Label will be change after relabel in following conditions

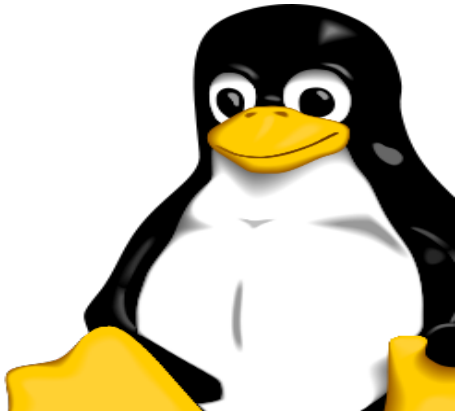
#restorecon

Or

#touch /.autorelabel

#reboot

After above commands default label will be applied.



# Set selinux label permanently

Show label list

#semanage fcontext -l

#semanage fcontext -a -t httpd_sys_content_t /usr/local/web/

#semanage fcontext -a -t httpd_sys_content_t /usr/local/web/index.html

**Or**

Instead of one by one file we can all recursively on all content using following command.

The most common extended regular expression use in fcontext rule is (/.*)? Which means optionally match a / followed by any number or characters.

#semanage fcontext -a -t httpd_sys_content_t '/usr/local/web/(/.*)?'

#ls -ldZ /usr/local/web/

# Restore default label

This command change default label for “/usr/local/web/” in configuration file

So need to run relabel command

```
#restorcon      -Rv      /usr/local/web
#ls    -ldZ          /usr/local/web/
```

# selinux label store in file_contexts_local

**Show available file context**

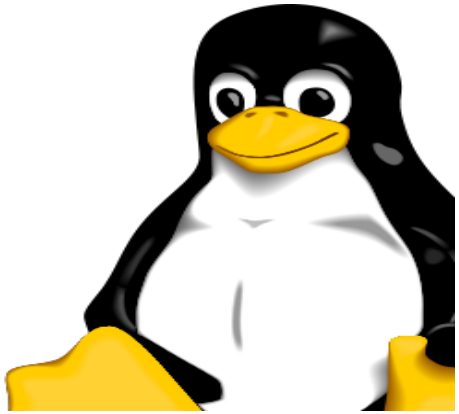
#cat /etc/selinux/targated/contexts/files/file_contexts

**After set manual directory context the it show**

#semanage fcontext -C -l

or

#cat /etc/selinux/targated/contexts/files/file_contexts.local



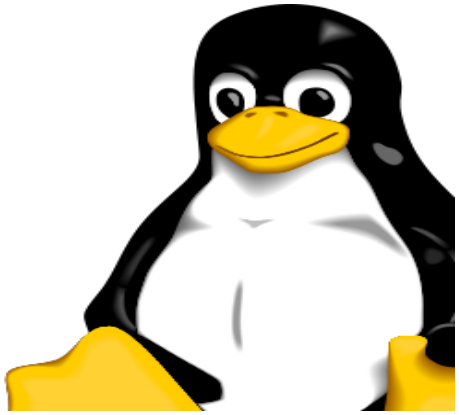
# Remove Selinux label

**Show available file context**

#semanage fcontext -d “/usr/local/web(/.*)?”

#restorcon -Rv /usr/local/web

#ls -ldZ /usr/local/web/



# Checking default selinux context with matchpathcon

#touch /var/www/html/file{1..3}

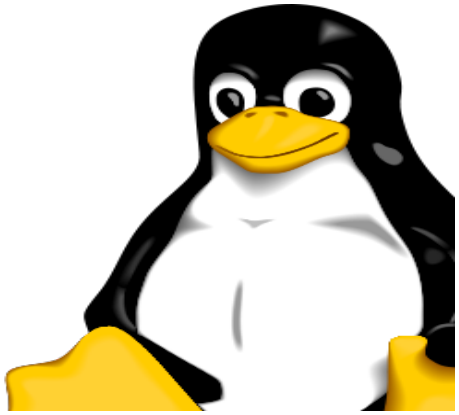
#ls -lz /var/www/html/file*

These file inherit the httpd_sys_content_t type from /var/www/html

**Now change manualy label:**

#chcon -t samba_share_t /var/www/html/file1

#matchpathcon -V /var/www/html/*



# SELinux booleans

A given SELinux policy can be customized by enabling or disabling a set of policy Booleans. Booleans allow parts of SELinux policy to be changed at run time, without any knowledge of SELinux policy writing. This allows changes without reloading or recompiling SELinux policy.

SELinux booleans are show the rule that can be enabled or disabled.

Getsebool command use to show selinux current value

#getsebool -a

Or

# getsebool ftpd_anon_write

Setsebool command use to set selinux policy

# setsebool ftpd_anon_write on

OR

# setsebool ftpd_anon_write 1

# getsebool ftpd_anon_write