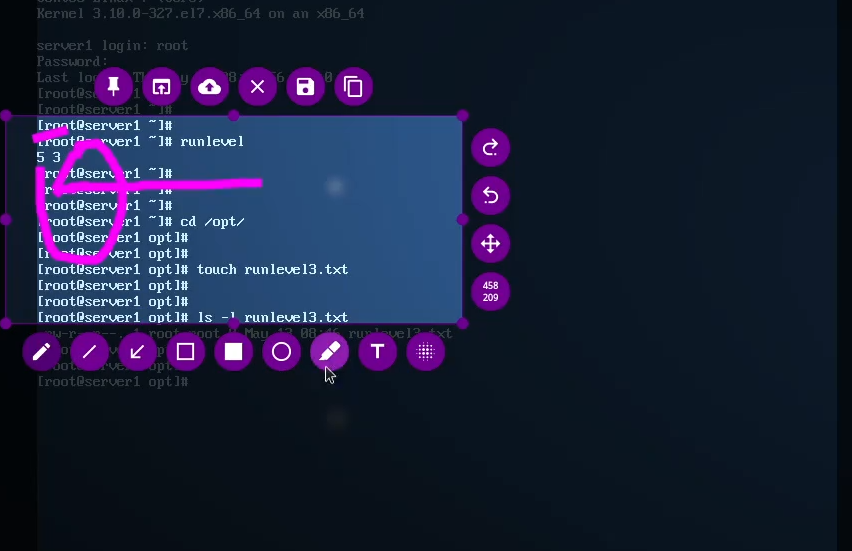
Lecture 07

Run Levels

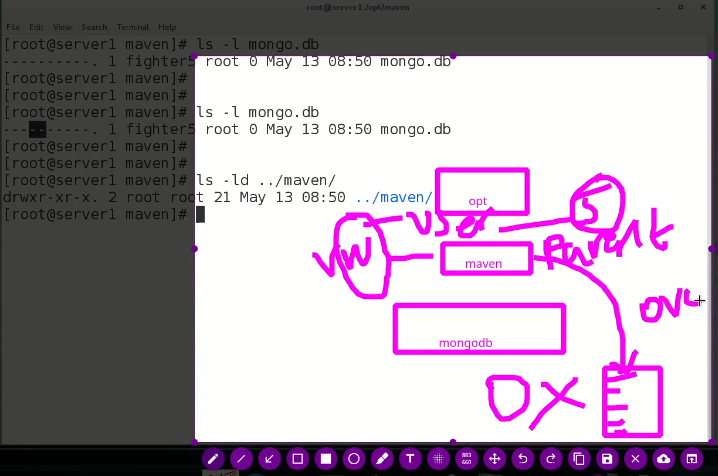
* Total 7 levels (0-6)
* To check run level command is
  + $ runlevel
* It will never exceed 6
* To switch level command is “init”, init is like a lift which carries us towards different floors
* $ init 3 🡪 it is runlevel 3
* Infact runlevels are like floors and init command is just like a lift
* 
* In this figure 5 is last runlevel and 3 is current runlevel
* There would becases when previous runlevel shows “n” means nothing

**Permissions and ownership**

* In the scenario below owner/user has no permissions
* 

But owner/user can still dele this file and root user can also delete this file. But others cant do anything in this file

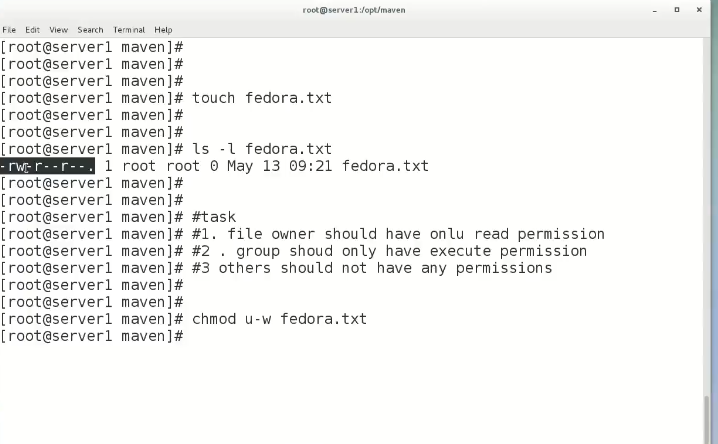
Inherit permission



In above scenario maven is the parent folder of file mongo.db

* Initially the permissions for file mongo.db are not permitted to any user but the user which have access to its parent folder “maven” can over write (in vim editor :wq! Feature “!” sigh means forcefully doing the edit in a specific file) this mongo.db file and perform tasks. This is called inherit permission. (because parent folder has read and write permission which are inherited to the users who have access to maven directory or folder.)

Task



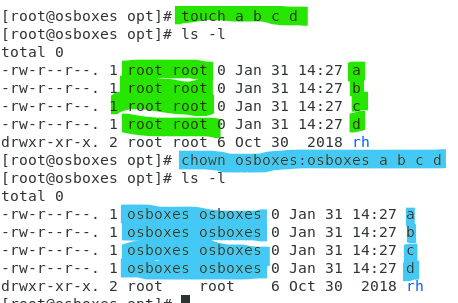
Recursion

-changing permission of all the files in a directory at once

$ chmod -Rv 777 <directory\_name>

-it will change permission for all the files in the directory.

- to change owner and group of multiple files at once



* Similarly to change owner and group of a directory
* 

**Advance permissions (Access Control List ACL)**

**If we have a large no of users than the normal way of assigning permissions is not a suitable one,**

**User wise permission are job requirement in industry**

For specific user

$ setfacl -m u:<user>:rwx <file\_Name>



\*m flang means modify



The “+” sign means there is user specific ACL is applied

To check which users are given permission through ACL

$ getfacl <fine\_name>

To remove the user specific permissions

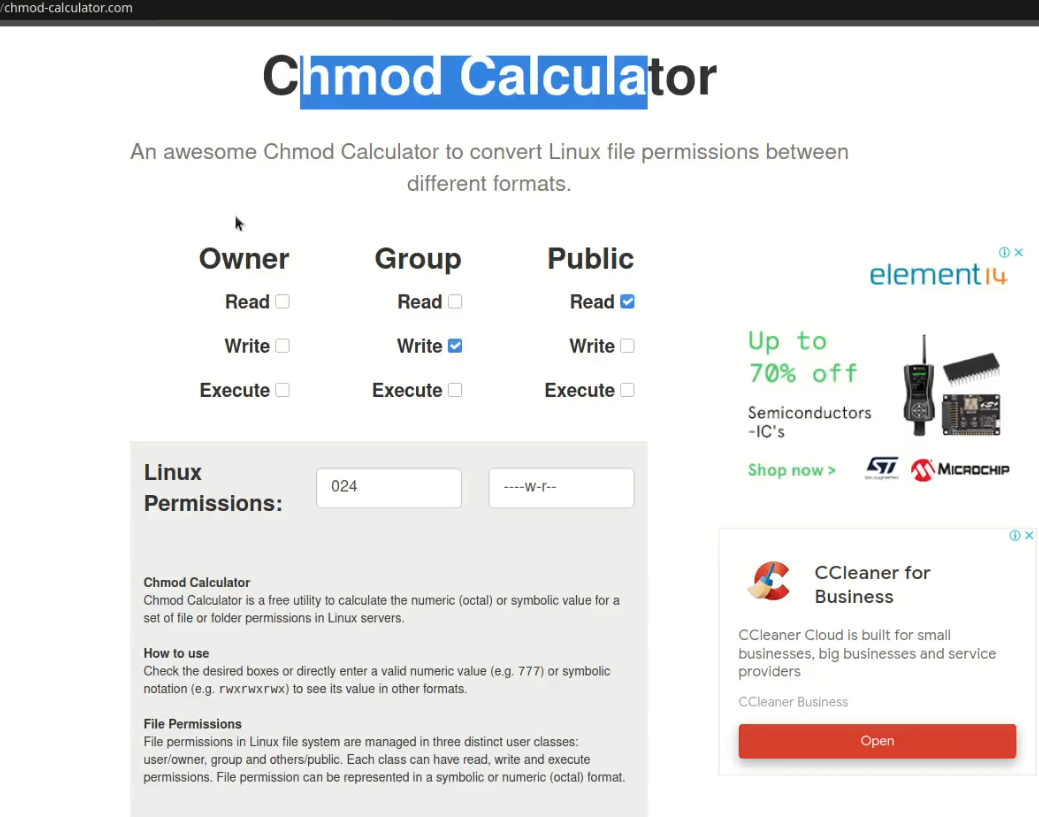
$ sefacl -x u:<user\_name> <file\_name>



-

In case of confusion an online calculator is available for reference

Chmod-calculator-com



-

-

Runlevels further explaines

Just likw MS Windows Linux als has modes or levels

* In RHL6 its called “runlevels” but in RHL 7/8 its called “targets”
* The command is
* $ init 3 <0-6>
* runlevel 0 🡪 is HALT
* runlevel 1 🡪 **single user mode (or safe mode) here no password is required (here root password can be reset if required)**
* runlevel 2🡪
* runlevel 3🡪 CLI more or terminal mode
* runlevel 4🡪
* runlevel 5🡪
* runlevel 6🡪 reboot

\*init means “initialize”

Password resetting

In this example RHL 6 is used

Its root password is forgotten

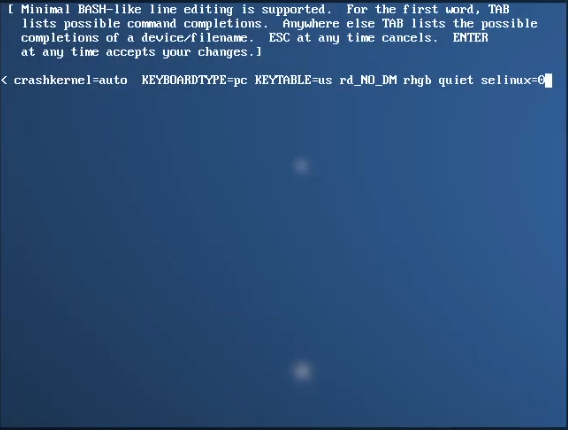
Steps,

1. on startup (splash screen) press arrow key to interrupt

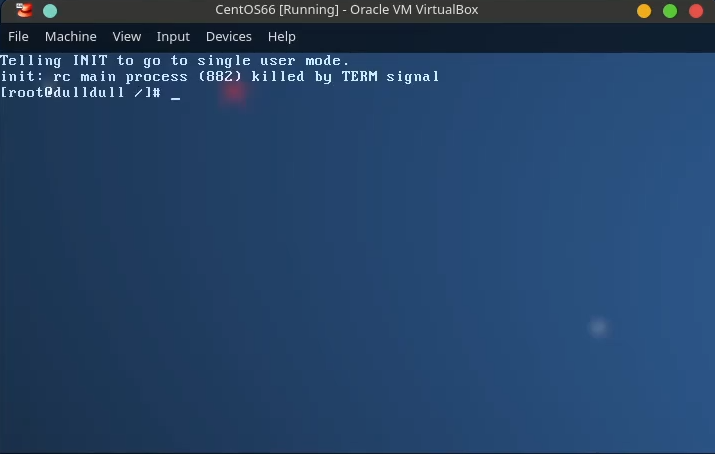
A picture containing graphical user interface

Description automatically generated

1. here against rhgb quiet (Red Hat graphical boot quite) put 1 in front and press <ENTER>
   * it means take me to the runlevel “1”



1. it will take to loginprompt



1. here reset password with command
   1. $ passwd root <ENTER>

Now, $ init 5 <ENTER>

It will take to runlevel 5 which is GUI

