Mohamed Atef Elbitawy

Red Hat Enterprise Linux 9

2

شرح **Linux Admin 2** لكورس

Red Hat System Administration II

الموجود علي منصه **Mahara Tech** للباشمهندس

Karim Abd Elhamid

BY: Mohamed Atef Elbitawy

https://www.linkedin.com/in/mohamedelbitawy/

لا تنسونا من صالح الدعاء

- **Course Link**

  https://maharatech.gov.eg/enrol/index.php?id=2205r

- **Presentation Slides**

  https://drive.google.com/drive/folders/14x-f237P43_C9BUoSwSfAn58VP5upCZL?usp=sharing

- **Red Hat Enterprise Linux 9_RH134**

  https://drive.google.com/file/d/17rJovyJKthBHXoSCV4XAJzcB1W4qB5RA/view?usp=sharing

- **Red hat Admin 1 Explanation**

  https://www.linkedin.com/posts/mohamedelbitawy_linux-admin-1-v9-activity-7226626485799817218-JvWo?utm_source=share&utm_medium=member_desktop

  OR

  https://drive.google.com/file/d/19wnxrr12-i1dWV0DAGpS9WaCVF3NR8g6/view?usp=drive_link

- **RHCSA Exam**

  https://drive.google.com/drive/folders/11kxtwSi7fqhOefwRG3eZqh8TW3EBWwSU?usp=sharing

- **Interview Questions**

  https://drive.google.com/drive/folders/1qkfNakp_vSnLBMCZVhpCrUsJ0-UZ1hpO?usp=sharing

Content

CH01_Improving Command-line Productivity ……..... 4

CH02_Scheduling Future Tasks……..... 5

CH03_Tuning System Performance……... 19

CH04_Controlling Access to Files with ACLs……. 29

CH05_Managing SELinux Security…….… 39

CH06_Managing Basic Storage……... 56

CH07_ Managing Logical Volumes…… 81

CH08_ Implementing Advanced Storage Features…… 95

CH09_Accessing Network-Attached Storage…….. 107

CH10_Controlling the Boot Process…….. 118

CH11_Managing Network Security…… 129

CH12_Installing Red Hat Enterprise Linux……... 145

Chapter 1
Improving Command-line Productivity

اول شابتر بيتكلم عن ال Basics في ال Shell Scripting وده هيكون ليه شرح منفصل تماما عن باقي الكورس لان هيتم شرح ال Shell Scripting بالتفصيل باذن الله مع اضافه بعض المشاريع وباذن الله هيكون موجود علي الرابط التالي :-

https://drive.google.com/drive/folders/1PLU5V4LOxQ128jztjnoe3-yxx2Mzoix3?usp=sharing

Chapter 2
Scheduling Future Tasks

- مبدئيا كده ال scheduling في اللينكس عباره عن future مهمه جدا لأي system admin يقدر من خلالها انه ي automate ال execution بتاع اي task او script موجود عنده سواء عايز ي execute ال task دي مره واحده at specific time او repeated task عايز يعملها execution اكتر من مره علي سبيل المثال لو انا عندي health check script عاوز اعمله automation to be executed on a daily bases بمعني ان عايز كل يوم اعمل health check للسيستم بتاعي عايز for example اخد backups من ال system بتاعي اسبوعيا او كل اسبوع عايز مثلا اعمل maintenance للسيستم بتاعي today at midnight ف انا في الحاله دي بلجأ لل scheduling طبعا لو اتكلمنا عن مميزات ال scheduling هنلاقيه مثلا
  1- انه بيسمحلك انك ت automate ال repeated and routine operations بتاعتك وده طبعا بي save ال time وال offer بتاعك
  2- ان ال scheduling بيحسن ال productivity وبيسمح لل system admin انهم يركزو اكتر علي ال more critical tasks
  3- تالت ميزه مهمه هي ال error redaction ال scheduling بيقلل ال risk بتاع ال human errors اللي ممكن تحصل في حاله ال manual execution
  4- رابع ميزه هي ال resource optimization

• Scheduling one-time tasks with at command

- خلينا نتكلم عن ال Scheduling one-time tasks with at command مبدئيا كده انا ك سيستم ادمن ببقي محتاج أ run و execute task معينه at specific time مره واحده وخلاص ف علشان اعمل كده ف انا عندي services اسمها **atd** دي بتبقي install و enable by default وبيجي معاها مجموعه من ال command line tools زي ال **at command** اقدر ببساطه استخدم ال **at command** هقوله **at** وبعدين احددله ال time format اللي انا محتاج ان انا execute ال task بتاعتي عنده بمجرد ان انا عملت كده ودوست Enter بيدخلني في حاجه اسمها at prompt زي ماهنشوف كمان شويه . اقدر من خلال ال at prompt ادخل كل ال Commands اللي انا عايز اعملها execute عند ال time اللي انا حددته بمجرد ان انا دخلت كل ال commands بتاعتي ف علشان أ terminate ال at command بقوله CTRL+D خد بالك من حاجه بردك انا عندي ال time format اللي انا بحدده هنا بيكون very flexible او ممكن ي accept مني اي combinations يعني for example ممكن اقوله **at 02:00pm** بالفورمات ده هيقبلها مني كده انا عايز انفذ task معينه الساعه **02:00pm** او ممكن اقوله **now +5min** معناها ان كمان 5 دقائق روح نفذ ال task او ال job المطلوبه . ممكن اقوله **at noon +4days** يعني كمان 4 أيام الساعه 12pm روح نفذ ال task المطلوبه وممكن احددله ال time و ال date زي مثلا **at 5pm august 3 2021** . خلي بالك ان **teatime** يعني الساعه 16:00 او 4pm

Inspecting and managing deferred user jobs

- To get an overview of the pending jobs for the current user, use the command **atq** or the **at –l** commands.

```
[user@host ~]$ atq
❶28  ❷Mon Feb  2 05:13:00 2015 ❸a ❹user
29  Mon Feb  3 16:00:00 2014 h user
27  Tue Feb  4 12:00:00 2014 a user
```

In the preceding output, every line represents a different job scheduled to run in the future.

1. The unique job number for this job.
2. The execution date and time for the scheduled job.
3. Indicates that the job is scheduled with the default queue a. Different jobs may be scheduled with different queues.
4. The owner of the job (and the user that the job will run as).

- لو انا عايز اعرض كل ال jobs الموجوده عندي بستخدم command اسمه **atq** او **at -l** الاتنين بيطلعولي نفس ال output بمجرد ان قولتله **atq** وبعدين Enter بيطلعلي output بالمنظر ده

```
[user@host ~]$ atq
28    Mon May 16 05:13:00 2022   a   user
29    Tue May 17 16:00:00 2022   h   user
30    Wed May 18 12:00:00 2022   a   user
```

اول column بيكون عباره عن ال job ID

تاني column بيكون عباره عن execution data and time

تالت column بيكون موجود فيه حاله ال jobs اذا كانت active بيتم التعبير عنها بحرف a واذا كانت hold معلقه بيتم التعبير عنها بحرف h

واخر حاجه بيقولي مين هو ال owner بتاع ال job دي

Create at task

- **at +time** (to make a schedule for some commands to run in this time then enter.
- Time like now,1hour,6AM,tomorrow,4PM+3days , 10AM Jul 31, teatime ---> 4 pm).
- **at>** write the commands you want to execute in this time each command in one line then CTRL +d ---> to finish.
- **atq** ----------> show you all schedules created.
- **atrm + job** --------> to delete the schedule.
- **Time can be:**
  - HH:MM 23:15
  - Midnight 12:00 am
  - Noon 12:00 pm

- **خلينا نشوف ازاي ن create one time task باستخدام ال at command**

➢ اول حاجه بقوله at وبعدين بحددله ال time بتاعي وزي ماقولنا ال time format is very flexible وبي accept اي combination يعني ممكن اقوله ال time بتاعك now او 1hour او 6AM او tomorrow وهكذا ...

➢ ال **at>** بقدر من خلالها ان انا ادخله كل ال commands اللي انا عايز اعملها execute بمجرد ان انا دخلت كل ال commands بقوله CTRL+D علشان اطلع من ال at prompt

➢ لو انا عايز أ show او اعمل list لكل ال jobs اللي عندي بقوله atq

➢ لو انا عندي job وعايز اعملها remove هستخدم atrm وبعدين ال job id

علشان اتاكد ان ال atd معمول ليها install و enable و active هستخدم **systemctl status atd**

```
[root@MohamedAtef ~]# systemctl status atd
● atd. service - Deferred execution scheduler
    Loaded: loaded (/usr/lib/systemd/system/atd.service; enabled; preset: enabled)
    Active: active (running) since Thu 2024-06-06 03:26:05 EET; 3min 45s ago
      Docs: man:atd(8)
  Main PID: 1200 (atd)
     Tasks: 1 (limit: 5609)
    Memory: 304.0K
       CPU: 15ms
    CGroup: /system.slice/atd.service
            └─1200 /usr/sbin/atd -f
Jun 06 03:26:05 server systemd [1]: Started Deferred execution scheduler.
```

- تعال كده ن create اي Task نقوله مثلا at noon معناها ايه معناه وقت الظهيره يعني الساعه 12pm

```
[root@MohamedAtef ~]# at noon
warning: commands will be executed using /bin/sh
at>
```

- لما نفذت الامر ظهرلي ال prompt اللي اتكلمنا عليه قبل كده وهو ال **at>** وده من خلاله هكتب الامر اللي انا محتاج انفذه وقت الظهيره وليكن هقوله نفذلي echo “Hello” >>/tmp/hello.txt

```
[root@MohamedAtef ~]# at noon
warning: commands will be executed using /bin/sh
at> echo “Hello” >>/tmp/hello.txt
at>
```

- لو انت خلصت ال task هتقوله CTRL+D بمجرد ان انت ضغطت علي CTRL+D هيظهرلي ال job وال job ID اللي هو 6 وكمان هيظهرلي execution data and time ان يوم 6 يونيو الساعه 12pm نفذلي التاسك

```
[root@MohamedAtef ~]# at noon
warning: commands will be executed using /bin/sh
at> echo “Hello” >>/tmp/hello.txt
at> <EOT>
job 6 at Thu Jun  6 12:00:00 2024
[root@MohamedAtef ~]#
```

- تعال ناخد كمان مثال لو انا عايز اقوله كمان 3 ايام الساعه12pm انشئلي فولدر تحت /tmp/ باسم backup_system وكمان خدلي archive من /tmp/backup_system باسم etc.tar وخد كمان copy من ال archive اللي اسمه etc.tar تحت /etc

```
[root@MohamedAtef ~]# at noon+3days
warning: commands will be executed using /bin/sh
at> mkdir /tmp/backup_system
at> tar -cvf /tmp/backup_system/etc.tar /etc
at>
```

- لو انا عايز اعرض كل ال jobs اللي عندي هستخدم **atq** او **at -l**

```
[root@MohamedAtef ~]# atq
2	Sat Mar  9 14:13:00 2024 a Elbitawy
6	Thu Jun  6 12:00:00 2024 a root
7	Sun Jun  9 12:00:00 2024 a root
[root@MohamedAtef ~]# at -l
2	Sat Mar  9 14:13:00 2024 a Elbitawy
6	Thu Jun  6 12:00:00 2024 a root
7	Sun Jun  9 12:00:00 2024 a root
[root@MohamedAtef ~]#
```

- لو انا عايز اعمل remove لل job اللي ID بتاعها ب 6 هستخدم **atrm** وبعدين رقم ال ID

```
[root@MohamedAtef ~]# atrm 6
```

- طب لو انا عايز a pass command معين لل at من غير مأدخل جوه ال at prompt (at>) ممكن استخدم معاها ال pipeline (|)
- زي مثلا ممكن اقوله echo ان انا عايز ابعت ال command ده "data >> /home/mohamed/myjob.txt" ك input لل at command بمعني ان بمجرد ان انا نفذت الامر ده هيروح يطبعلي التاريخ ويحطهولي تحت /home/Mohamed/ في file اسمه myjob.txt وكمان نفذلي ال task دي حالا عن طريق ان انا هستخدم at now

```
[root@MohamedAtef ~]# echo "data >> /home/mohamed/myjob.txt" | at now
warning: commands will be executed using /bin/sh
job 8 at Thu Jun  6 05:06:00 2024
```

- وممكن اخد ال inputs بتاعتي من Script ان لو عندي اسكريبت معين فيه مجموعه من الcommands ممكن اقوله مثلا كمان 5 دقائق نفذلي الاسكربت ده

```
[root@MohamedAtef ~]#  at now+5min </home/mohamed/script.sh
```

- فيه عندي command اسمه **watch atq** بستخدمه لو انا عايز اعرض ال jobs بتاعتي في ال runtime

```
[root@MohamedAtef ~]#  watch atq
very 2.0s: atq                                        MohamedAtef: Thu Jun  6 19:21:35 2024
2     Sat Mar  9 14:13:00 2024 a Elbitawy
7     Sun Jun  9 12:00:00 2024 a root
```

- انا عندي by default ال jobs بتاعتي بتكون stored تحت /var/spool/at/ لو دخلنا تحت المسار ده هنلاقي عندي كذا اسكريبت created عندي ان كل job عندي ليه اسكريبت خاص بيه

```
[root@MohamedAtef ~]#  cd /var/spool/at/
[root@MohamedAtef at]# ls
a0000201b2df3d  a0000701b4e438  spool
[root@MohamedAtef at]#
```

- ولو فتحنا اي اسكربت هنلاقي ال output اللي طالعلك فيه مجموعه من ال environment variables هو بيعملها preparation الاول وبعد كده بيروح ي execute ال command اللي انت كنت حاططهوله

```
[root@MohamedAtef at]# cat a0000701b4e438
#!/bin/sh
# atrun uid=0 gid=0
# mail root 0
umask 22
SHELL=/bin/bash; export SHELL
HISTCONTROL=ignoredups; export HISTCONTROL
HISTSIZE=1000; export HISTSIZE
HOSTNAME=MohamedAtef; export HOSTNAME
GUESTFISH_OUTPUT=\\e[0m; export GUESTFISH_OUTPUT
PWD=/root; export PWD
LOGNAME=root; export LOGNAME
XDG_SESSION_TYPE=tty; export XDG_SESSION_TYPE
GUESTFISH_RESTORE=\\e[0m; export GUESTFISH_RESTORE
LS_COLORS=rs=0:di=01\;34:ln=01\;36:mh=00:pi=40\;33:so=01\;35:do=01\;35:bd=40\;33\;01:cd=40\;33\;01:or=40\;31\;01:mi=01\;37\;41:su=37\;41:sg=30\;43:ca=30\;41:tw=30\;42:ow=34\;42:st=37\;44:ex=01\;32:\*.tar=01\;31:\*.tgz=01\;31:\*.arc=01\;31:\*.arj=01\;31:\*.taz=01\;31:\*.
```

خلي بالك ان في اخر الاسكربت ده هتلاقي ال command اللي انت كاتبه علشان ال task تتنفذ اللي انت كتبته في ال at prompt

- وفيه طريقه اسهل اني اعرض الاسكربت اني اكتب **at** وبعدين **-c** وبعدين رقم ID الخاص بال job

```
[root@MohamedAtef ~]# at -c 7
```

At Job Important Files

- **/etc/at.allow** (the file which has the users who can use at commands).
- **/etc/at.deny** (the file which has the users who denied from using at commands).
- **/var/spool/at/** (Holds the jobs script files).

Notes

- If the both files not exists that is mean all users are denied.
- The default installation create **at.deny** and make as default all users allowed to use at commands so take care.

- خلينا دلوقتي نتكلم عن بعض ال Important Files اللي بتيجي مع ال at command

1- اول file تحت /etc/ وهو **at.allow** وده بيكون موجود فيه ال users اللي مسموح ليهم انهم يستخدموا ال at command
2- تاني file تحت /etc/ وهو **at.deny** وده بيكون موجود فيه ال users اللي ممنوع انهم يستخدموا ال at command
3- اما /var/spool/at/ بيكون موجود فيه كل ال jobs script files
4- وخلي بالك ان /etc/at.allow ده مبيكونش created عندي في السيستم يعني لو انا عملت create ل at.allow تحت /etc وكتبت جواه user معين وليكن Mohamed معني كده ان Mohamed هو اللي مسموح ليه انه يستخدم ال at command وباقي ال user معمولهم deny ولو انا عملت create لل file ده ومكتبتش جواه اي user يعني فاضي معناه ان by default كل ال users معمولهم deny

- اما /etc/at.deny ال file ده بيكون created عندي ولكن بيكون فاضي
- لو at.allow و at.deny اتمسحوا معني كده ان by default الusers كلهم معمولهم deny

- تعال نحط مثلا ال user اللي اسمه karim في ال at.deny

```
[root@MohamedAtef ~]# echo karim >/etc/at.deny
```

- وبعدين نجرب ان احنا نستخدم ال at command علي ال user اللي عملناله deny هيظهرلنا انه ملهوش permission انه يستخدم ال atq

```
[karim@MohamedAtef ~]$ atq
You do not have permission to use atq.
```

Describing recurring user jobs

- Jobs scheduled to run repeatedly are called recurring jobs. Red Hat Enterprise Linux systems ship with the **crond** daemon, provided by the cronie package, enabled and started by default specifically for recurring jobs. The **crond** daemon reads multiple configuration files: one per user (edited with the **crontab** command), and a set of system-wide files. These configuration files give users and administrators fine-grained control over when their recurring jobs should be executed.
- Fields in the **crontab** file appear in the following order:
  - Minutes.
  - Hours.
  - Day of month.
  - Month.
  - Day of week.
  - Command.

- خلينا دلوقتي نشوف لو انا عايز أ run ال tasks بتاعتي بشكل periodic او repeated فيه عندي service اسمها crond daemon السيرفز دي بتكون install و enable عندي ولو مش install بقدر اعملها install عن طريق package اسمها **cronie**
- السيرفز دي بينزل معاها مجموعه من ال command line tools اهمهم ال **crontab** وده اللي هنستخدمه علشان ن schedule اي repeated task موجوده عندي خلي بالك ان ال crontab بتتكتب ب format معين زي ماهنشوف في ال slide الجايه ولازم احددله ال Minutes وال Hours وال Day of month وال Month وال Day of week وال Command

Create crontab

```
# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
```

- **crontab -e** (to create a cron , you should enter the full path of the command which you want to execute it) which + command (to get the full path of the command).
- ***/3** (in the minutes field means every 3 minutes , in the hours field --> means every 3 hours ...etc).
- crontab -e -u +user (to edit in cron of specific user).
- **crontab -l** (to list cron scheduled).
- **crontab -l -u +user** (to list the crons of specific user).
- **crontab -r** (to remove your cron).

- علشان نعرف ال format الخاص بال crontab انا عندي file stored تحت /etc اسمه crontab لو انا عملت cat لل file ده هيظهرلي ال output بالمنظر ده

```
[root@MohamedAtef ~]# cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
# For details see man 4 crontabs
# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed
```

- ف ال file ده عباره عن مجموعه من ال command شارحلك بيهم لو انت عايز ت add job او ت add task في ال crontab بتاعتك ايه هي ال information اللي انت محتاجها ف انت اول حاجه محتاجها انك تظبطله الاول ال timing بتاعك ودي بتكون اول 5 استريك (* * * * *) زي اللي احنا شايفنهم فوق بالون الاحمر
  - اول استريك فيهم بيعبر عن ال minute ودي بتاخد value من 0 ل 59
  - تاني استريك بيعبر عن ال hour ودي بتاخد value من 0 ل 23
  - تالت استريك بيعبر عن ال day of month ودي بتاخد قيمه من 1 ل 31
  - رابع استريك بيعبر عن ال month ودي بتاخد value من 1 ل 12 وممكن اكتبله اول 3 حروف من كل شهر زي Jan او Feb او Mar وهكذاا
  - خامس استريك بيعبر عن ال day of week ودي بتاخد value من 0 ل 6 بعدد ايام الاسبوع
  - وبعد كده محتاج ان انا احددله ال user اللي انا ها execute من خلاله ال task ودي optional ممكن احطها او محطهاش
- انا عندي By Default كل ال Users بيكونو allowed انهم يستخدموا ال **crontab** command ال crontab معاه Three Option وهما ال **crontab -l** و **crontab -r** و **crontab -a**

Command	Intended use
crontab -l	بستخدمه لو انا عايز أ List كل ال Jobs بتاعتي
crontab -r	بستخدمه لو انا عايز اعمل remove لكل ال Jobs
crontab -e	بستخدمه لو انا عايز أ edit او Modify
crontab *filename*	بستخدمه لو انا مثلا واخد backup من ال crontab بتاعتي وعامله save ف file معين وعايز أ restore ال backup ده بقوله crontab filename هو هيروح ياخد كل ال jobs اللي stored في ال file ده وهيعملها replace بال current jobs الموجوده في ال crontab بتاعتي

- لو انا عايز اعمل edit ل crontab خاص ب user معين هستخدم **crontab -e -u username**
- انا عندي By Default ال crontab لكل الUsers بتبقي Stored تحت **/var/spool/cron/** وال root بس اللي عليه Full Access عليه

Example recurring user jobs

- The following job executes the command **/usr/local/bin/yearly_backup** at exactly 9 a.m. on February 2nd, every year.

```
0 9 2 2 * /usr/local/bin/yearly_backup
```

- The following job sends an email containing the word **Chime** to the owner of this job, every five minutes between 9 a.m. and 5 p.m., on every Friday in July.

```
*/5 9-17 * Jul 5 echo "Chime"
```

- The following job runs the command **/usr/local/bin/daily_report** every weekday at two minutes before midnight.

```
58 23 * * 1-5 /usr/local/bin/daily_report
```

- تعال نشرح بعض الامثله عن ال crontab من ال slide والامثله دي بيجي منها في امتحان RHCSA

1- اول مثال معانا زي ماهو واضح في ال slide اللي فوق ان بيقولك انه عنده اسكريبت yearly_backup ومن اسمه كده ده بياخد backup من السيستم بتاعك yearly وده موجود تحت /usr/local/bin/ ومديك ال path بتاعه وقالك انه عايزك تعمله execute او automate ان كل سنه يوم 2 فبراير الساعه 9 صباحا روح خد backup من ال system بتاعي طب دي هنعملها ازاي

- هقوله **crontab -e** علشان اعمل edit اول اما اضغط enter هيفتحلي بال VI text editor وبعدين اكتب جواه وزي ماحنا قولنا قبل كده ان اول عمود ده بيعبر عن الدقائق ف هحط مكان ال minute احط zeroعلشان هو قايلي الساعه 9a.m ومكان ال hour هكتب 9 وبعدين مكان يوم ايه في الشهر اكتب 2 علشان قايلي يوم 2 في شهر فبراير وبعد كده هكتب مكان الشهر هكتب 2 وهحط مكان يوم الاسبوع استريك * وبعد كده حط ال path بتاع ال script بتاعك .خلي بالك من حاجه مهمه جدا جداا الحاجه اللي مش هيجبلك سيرتهاا في ال example حط مكانها استريك * زي بالظبط يوم الاسبوع مجبش سيرته ف احنا حطيناه ب استريك*

```
0  9  3  2  * /usr/local/bin/yearly_backup
```

2- لو جينا بصينا علي تاني مثال هتلاقيه بيقولك انا عايزك تعملي automate ل command معين what ever ال command ده ايه المهم بالنسبالنا دلوقتي الTiming ان التركايه كلها في ال Timing قالك والله عايزك تعملي automate لل command ده to be executed every five minutes كل خمس دقائق هنا محددلك interval اللي هو كل خمس دقائق طب هنعمل ده ازاي هتقوله مكان ال minute استريك علي 5 (5/*) ده كده indication ان انت عايز تعمل interval وبعدين في ال hours قالك انه عايزك تعمل execute للcommand من الساعه 9a.m ل الساعه 5p.m هقوله 9-17 انا هنا مش هينفع احط 5p.m لا لازم احولها ل 24 hours وتبقي 17 .وطالما محددليش ال day of month يبقي هحط مكانها استريك * وبعد كده الشهر Jul وبعد كده ممكن اكتب اول 3 حروف من Friday او اكتب 5

```
*/5  9-17  *  Jul  5 echo “Chime”
```

هنتكلم عن بعض ال Files وال Directory المهمه الrelated لل cron

Cron Job Important Files

- **/etc/cron.d** (This is the path to put (your) cron files created).
- **/etc/cron.deny** (the file to put who users you want to deny them from creating cron).
- **/etc/cron.allow** (to put the users who allowed to create cron).
- **/var/spool/cron** (it contains all the crons of all users, so you can access any file you want).
- **/etc/crontab** (to see the syntax for writing a cron task).
- **/etc/anacrontab** (its a file contain all scripts runs in specific time , if you cat this file you will see all scripts which will run in future and time ...etc).
- **/etc/cron.daily** (list scripts which will be executed daily).
- **/etc/cron.monthly** (list scripts which will be executed every month).

/etc/cron.d	ده عباره عن Directory انت بتستخدمه علشان ت create فيه your customize crontab
/etc/cron.deny	ده بيكون created by default وبيكون فاضي ومعناها ان كل ال users بيكونوا allowed انهم يستخدمو ال cront وده بيكون نفس فكرت ال at.deny
/etc/cron.allow	ده مبيكونش created عندي .بمجرد ان انا عملتله create وحطتيط فيه user معين يبقي كده كل ال users معمولهم deny ماعدا ال user اللي انا حطتيطه في ال File
/etc/spool/cron	ده بيكون عباره عن Directory بيكون موجود فيه كل ال crontab الخاصه بكل ال users
/etc/crontab	ده بيكون عباره عن text file مكتوب جواه شويه comments بتفهمك ال syntax الخاص بال crontab
/etc/anacrontab	ميزه ال anacrontab ان انا لو عندي اي Task متعملهاش Execute last time بمجرد ان السيستم بتاعك اتعمله power on وبقي available ال anacrontab هتروح ت execute الاسكريبت ده
/etc/cron.daily	بحط فيه كل الاسكريبت اللي انا عايز اعملها execute daily
/etc/cron.monthly	بحط فيه كل الاسكريبت اللي انا عايز اعملها execute monthly

Managing temporary files

- Some applications (and users) use the **/tmp** directory to hold temporary data, Red Hat Enterprise Linux 7 and later include a new tool called **systemd-tmpfiles**, which provides a structured and configurable method to manage temporary directories and files.
- When systemd starts a system, one of the first service units launched is systemd-tmpfiles setup. This service runs the command **systemd-tmpfiles --create --remove**. This command reads configuration files from **/usr/lib/tmpfiles.d/*.conf, /run/tmpfiles.d/*.conf**, and **/etc/tmpfiles.d/*.conf**. Any files and directories marked for deletion in those configuration files is removed, and any files and directories marked for creation (or permission fixes) will be created with the correct permissions if necessary.
- To ensure that long-running systems do not fill up their disks with stale data, a **systemd** timer unit called systemd-tmpfiles-clean.timer triggers systemd-tmpfiles-clean. service on a regular interval, which executes the **systemd-tmpfiles --clean** command.

- احنا لحد دلوقتي اتكلمنا عن ال **at command** وال **crontab** خلينا دلوقتي نتكلم علي Schedule Function جديده اسمها **systemd timer unit** . بدايه من red hat 7 ومع ظهور systemd service ظهرتلنا systemd timer unit وقالك ان ال systemd timer عباره عن مجموعه من ال Timers او ال Counters وظيفتها انها تروح ت Activate units او service معينه علشان ال service دي تروح تعمل Task معينه مطلوبه منها

➢ لو انا عايز اعمل List لكل ال Timer Units الموجوده عندي في السيستم هستخدم ال command التالي

```
[root@MohamedAtef ~]# systemctl list-units --type=timer
  UNIT                          LOAD   ACTIVE SUB     DESCRIPTION
  dnf-makecache.timer           loaded active waiting dnf makecache --timer
  logrotate.timer               loaded active waiting Daily rotation of log files
  mlocate-updatedb.timer        loaded active waiting Updates mlocate database every day
  sysstat-collect.timer         loaded active waiting Run system activity accounting tool every 10 minutes
  sysstat-summary.timer         loaded active waiting Generate summary of yesterday's process accounting
  systemd-tmpfiles-clean.timer  loaded active waiting Daily Cleanup of Temporary Directories
  unbound-anchor.timer          loaded active waiting daily update of the root trust anchor for DNSSEC
LOAD   = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB    = The low-level unit activation state, values depend on unit type.
7 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

➢ لو لاحظت كده هتلاقي timer باسم logrotate.timer ده وظيفته انه بيروح يعمل activate لل service دي daily علشان تعمل التاسك المطلوبه منها اللي هي عمليه ال log rotation

- انا عندي باكدج او service اسمها **sysstat** وظيفتها ان هي ت collect statistic عن السيستم بتاعي كل 10 دقائق . الباكدج دي مبتكونش install عندي ف علشان اعملها install هستخدم ال command

```
[root@MohamedAtef ~]# dnf install sysstat
```

- بعد كده نشوف ال status هنلاحظ انها active بس exited مش running ليه علشان احنا قولنا ان الباكدج دي بت collect statistic عن السيستم بتاعي كل 10 دقائق

```
[root@MohamedAtef ~]# systemctl status sysstat
● sysstat.service - Resets System Activity Logs
   Loaded: loaded (/usr/lib/systemd/system/sysstat.service; enabled; preset: enabled)
   Active: active (exited) since Fri 2024-06-07 19:14:55 EET; 22min ago
  Process: 817 ExecStart=/usr/lib64/sa/sa1 --boot (code=exited, status=0/SUCCESS)
 Main PID: 817 (code=exited, status=0/SUCCESS)
      CPU: 15ms

Jun 07 19:14:55 MohamedAtef systemd[1]: Starting Resets System Activity Logs...
Jun 07 19:14:55 MohamedAtef systemd[1]: Finished Resets System Activity Logs.
```

- ال service دي بينزل معاها مجموعه من ال command line tools اهمهم command اسمه **sar**
- لو انا قولتله **sar -r** ده كده command بستخدمه لو انا عايز أ Display statistic عن ال memory utilization الموجوده عندي في السيستم

```
[root@MohamedAtef ~]# sar -r
Linux 5.14.0-284.11.1.el9_2.x86_64 (MohamedAtef)        06/07/2024        _x86_64_        (2 CPU)

12:33:31 PM       LINUX RESTART        (2 CPU)
12:40:04 PM kbmemfree   kbavail kbmemused  %memused kbbuffers  kbcached  kbcommit   %commit  kbactive   kbinact   kbdirty
12:50:04 PM    94400    214784    490296     51.14         4    232520   2068524     67.69    164484    363240         0
01:00:04 PM    87136    210092    495064     51.63         4    235028   2068572     67.69    167952    362696         0
01:10:04 PM    81028    204208    500896     52.24         4    235260   2068956     67.70    166944    364348         0
```

- طب لو انا عايز اغير بدل اما كل 10 دقائق يروح يعملي Collect statistic للسيستم اغيرها مثلا كل دقيقه لو انا روحت مثلا وعملت cat للtimer اللي اسمه sysstat-collect.timer باستخدام systemctl cat هنلاحظ ان موجود فيه الاعدادات الخاصه بالمهام من حيث اعدادات التوقيت والتشغيل

```
[root@MohamedAtef ~]#  systemctl cat sysstat-collect.timer
# /usr/lib/systemd/system/sysstat-collect.timer          ده المكان اللي فيه التايمر بتاعي
# /usr/lib/systemd/system/sysstat-collect.timer
# (C) 2014 Tomasz Torcz <tomek@pipebreaker.pl>
# sysstat-12.5.4 systemd unit file:
# Activates activity collector every 10 minutes
[Unit]
Description=Run system activity accounting tool every 10 minutes
[Timer]
OnCalendar=*:00/10
[Install]
WantedBy=sysstat.service
```

هنا لو انا عايز اغير بدل اما كل 10 دقائق يروح يعمل collect statistic هغيرها لدقيقه واحده هغير بدل 10 هكتب 1

- ف مش recommended انك تغير في ال file ده /usr/lib/systemd/system/sysstat-collect.timer الافضل ان انا اخد copy من ال Timerده /usr/lib/systemd/system/sysstat-collect.time تحت المسار ده /etc/systemd/system/ ويكون بنفس الاسم sysstat-collect.time وافتح ال file ده بال vi command واغير ال OnClender بدل ماهي ب 10 اغيرها ل 1

```
[root@MohamedAtef ~]# cp /usr/lib/systemd/system/sysstat-collect.timer  /etc/systemd/system/sysstat-collect.timer
```

- وبعد اما اغير في الملف لازم اعمل daemon -reload علشان السيستم يحس بالتغيير

```
[root@MohamedAtef ~]# systemctl daemon-reload
```

- خلينا دلوقتي نتكلم علي اخر Topic موجود معانا في الشابتر بتاع ال Scheduling اللي بيتكلم عن ال Temp File ونشوف ايه هي ال service اللي بن manage بيها ال Temp Files الموجوده عندنا في ال system مبدئيا كده لو فاكرين في ادمن 1 كنا اتكلمنا عن two directory واحد اسمه /tmp وواحد اسمه /var/tmp وقولنا ان دول عباره عن public ratable directories ال user و ال application بيستخدموهم علشان كل واحد ي create او ي restore ال temporary file او ال directory بتاعته في ال location دي وكنا قولنا الفرق بينهم ان /tmp اي file متعملوش access او modify او change لمده 10 ايام ال file ده هيتمسح اتوماتيك . اما ال /var/tmp ان لو فيه file متعملوش access او modify او change لمده 30 يوم ال file ده هيتمسح اتوماتيك . اللي بي manage الموضوع ده قالك بدايه من ريدهات 7 فيه عندي new service اسمها system-tmpfiles هي اللي بن manage بيها ال tmp files اللي created عندي في السيستم واول اما ال systemd ت start ال system بتاعك واحده من الservice المهمه اللي بيروح ال systemd يشغلها هي ال system-tmpfiles وال system-tmpfiles عندها مجموعه من ال tmp files موجوده تحت /usr/lib/tmpfiles.d/*.conf هتلاقي مجموعه من ال configuration file ال extension بتاعها .conf وهتلاقي كمان مجموعه من ال configuration files تحت /run/tmpfiles.d/*.conf وكمان تحت /etc/tmpfiles.d/*.conf . بمجرد ان ال systemd راح يشغل ال service دي ال service دي بتروح تقرا ال configuration files الموجوده في الاماكن اللي قولنا عليها وتشوف لو فيه اي file موجود في ال tmp location marked to be created هتعمله create ولو فيه اي file marked to be deleted هتعمله delete
- من ضمن المهام اللي بيعملها ال system-tmpfiles انه بيروح يعمل clean up لل temp files عن طريق انها بتنفذ command اسمه **system-tmpfiles-clean**
- انا علشان اعمل clean ل ال tmpfiles الموجوده عندي هتلاقي عندنا timer اسمه system-tmpfiles-clean.timerال timer ده وظيفته انه بيروح ي triggered ال service المسئوله عن ال clean up بتاع ال tmpfiles ال service دي اسمها **system-tmpfiles-clean.service** ولو جينا عملنا Display لل configuration بتاعت ال timer unit دي عن طريق ال command التالي

```
[root@MohamedAtef ~]# systemctl cat system-tmpfiles-clean.timer
```

هتلاقي ال timer ده عنده two parameters واحد اسمه OnBootSec=15min والتاني OnUnitActiveSec=1d الفرق بينهم ان ال parameters الاولاني ان لما ال server بتاعي يتعمله booted up ال timer ده هيعد 15 دقيقه اول اما 15 دقيقه يخلصوا هيروح ي trigger ال service اللي بتعمل clean up لل tmpfiles بتاعتك بمجرد ان عمل clean up ال next activation time او ال timer هيروح ي trigger ال service دي بعد one day بعد 24 ساعه

بعض الامثله اللي ممكن تحلها علي الشابتر

Exam Questions

- **Question 1: Scheduling a Task using at**

  1- Explain how to install and start the at service on a Red Hat system.

  2- Write the command to schedule a task that creates a text file containing "Hello, Exam!" in the path /tmp/exam.txt at 9:30 AM tomorrow.

  3- How can you display the list of scheduled tasks using at?

  4- How can you remove a scheduled task using at?

- **Question 2: Scheduling a Task using cron**

  1- Explain how to edit the crontab for the current user.

  2- Write a crontab entry to schedule a task that runs the backup.sh script located in /home/user/scripts/ every day at 2:00 AM.

  3- How can you display all scheduled tasks in the crontab for the current user?

  4- Write a crontab entry to schedule a task that sends the contents of /var/log/messages to the email admin@example.com every Monday at 5:00 PM.

- **Question 3**

  Schedule a cron job to run a script located at /home/user/backup.sh every day at 3:00 AM.

- **Question 4**

  How would you schedule a cron job to delete files from the /tmp directory every Sunday at midnight?

- **Question 5**

  Write a crontab entry that appends the current date and time to a file located at /home/user/timestamps.log every hour.

- **Question 6**

  Schedule a cron job to run a command that pings google.com and saves the output to /home/user/ping_results.txt every 15 minutes.

- **Question 7**

  Create a cron job that sends the content of /var/log/syslog to an email address admin@example.com every day at 6:30 PM

Chapter 3

Tuning System Performance

Tuning systems

- System administrators can optimize the performance of a system by adjusting various device settings based on a variety of use case workloads. The tuned daemon applies tuning adjustments both statically and dynamically, using tuning profiles that reflect particular workload requirements.
- **Configuring Static Tuning**
  Static tuning configures predefined kernel parameters in profiles that **tuned** applies at runtime. With static tuning, kernel parameters are set for overall performance expectations, and are not adjusted as activity levels change.
- **Configuring Dynamic Tuning**
  With dynamic tuning, the **tuned** daemon monitors system activity and adjusts settings depending on runtime behavior changes. Dynamic tuning is continuously adjusting tuning to fit the current workload, starting with the initial settings declared in the chosen tuning profile.

- مبدئيا كده احنا ك سيستم ادمن من ضمن المهام الاساسيه والمهمه عندنا هي اننا ن enhance ال performance بتاعت ال service عن طريق ان احنا بن adjusting ال settings بتاعت ال device بتاعنا according ال use case و ال workloads علشان ي enhance ال system performance . مثلا لو انت عندك لاب توب علشان تحافظ علي ال battery بتدخل علي ال settings بتاعت ال device وتدور علي اي اعدادات related للpower saving وتعملها adjust بحيث انك في الاخر ت optimize او ت enhance ال energy consumption. نفس الكلام عندنا بالظبط في اللينكس علشان كده ريدهات عملت service اسمها Tuned علشان تساعدنا اننا ن enhance ال performance بتاعت ال servers بتاعتنا نقدر نقول بكل بساطه ال Tuned وظيفتها انها بت monitors ال system بتاعك وت optimize ال performance علي حسب ال workload وال use case المختلفه
- ال Tuned service بيجي معاها مجموعه من ال predefined profiles بالاضافه ان ال Tuned عندها Two categories of system Tuning فيه عندي Static Tuning و Dynamic Tuning
- في حاله ال Static Tuning انت just بتختار profile معين according ال use case بتاعتك وال tuned service بتعملها apply at run time ومش بتتغير بعد كده الا لو انت غيرت البروفايل ده
- في حاله ال Dynamic Tuning ال Tuned service بتmonitors ال server activity زي ال Desk Utilization وال Network Utilization وال CPU Utilization وبتعمل apply لل Tuning Profile علي حسب ال workload و By default ال dynamic tuning بيبقي disable

Tuning systems

INSTALLING AND ENABLING TUNED

To install and enable the package manually:

```
[root@host ~]$ yum install tuned
[root@host ~]$ systemctl enable --now tuned
```

SELECTING A TUNING PROFILE

The Tuned application provides profiles divided into the following categories:

- Power-saving profiles.
- Performance-boosting profiles.

The performance-boosting profiles include profiles that focus on the following aspects:

- Low latency for storage and network.
- High throughput for storage and network.
- Virtual machine performance.
- Virtualization host performance.

➢ علشان اعمل install لل Tunedهستخدم ال command

```
[root@MohamedAtef ~]# yum install tuned
```

➢ لازم اعمل enable لل Tuned service

```
[root@MohamedAtef ~]# systemctl enable --now tuned
```

- وزي ماقولنا ان ال tuned بيجي معاها مجموعه من ال profiles نقدر نقول انها مقسموه ل two category

1- اول category عباره عن Power saving profiles ودي الهدف منها انها ت enhance ال energy consumption وتعملي power saving للسيستم بتاعي

2- تاني category اسمها performance-boosting profiles ودي بيكون موجود فيها مجموعه من ال profiles زي مثلا

- ال Low latency for storage and network وده بيكون عباره عن بروفايل بعمله apply والهدف منه انه بيقللي ال latency في السيرفر
- وعندي بروفايل كمان اسمه High throughput وده من اسمه كده بي enhance السيرفر بتاعي بطريقه معينه بحيث انه ي maximizeاو يديني اعلي Throughput ممكن
- فيه بروفايل تاني اسمه Virtual machine performance
- وعندي كمان بروفايل Virtualization host performance ده لو السيرفر بتاعي run ك KVM Host وحاطط عليه مجموعه من ال Virtual machines ف ساعتها بروح اعمل apply لبروفايل اسمه Virtualization host بحيث انه ي enhance ال performance بتاع ال Virtual host بتاعي

Tuning Profiles distributed with red hat enterprise Linux 9

- بعض من ال profiles المختلفه اللي بتيجي مع ال Tuned

Tuned Profile	Purpose
balanced	ده بيكون عباره عن Combination مابين ال power saving والperformance
desktop	ده بيستخدم عادتا مع ال desktop user او ال end user
throughput-performance	ده بي Tune السيستم بتاعك بطريقه معينه بحيث انه في الاخر ي ال maximize throughput بتاعك
latency-performance	الغرض من ال two profiles دول انهم ي tuned السيستم بتاعك بطريقه معينه بحيث ان هو ي minimize ال latency علي قد مايقدر في السيستم
network-latency	
network-throughput	ده بي Tune السيستم بتاعك بطريقه معينه وي apply شويه parameters بحيث انه في الاخر ي maximize ال network throughput
powersave	ده بي enhance ال power saving وال energy consumptions
virtual-guest	لو السيرفر بتاعك running as VM فقالك ف الاخر ال virtual-guest بيكون recommended ان انت تعمله apply لانه بي enhance السيستم بتاعك بطريقه معينه بيحيث انه يحسن اداء ال Virtual Machine
virtual-host	لو انت عندك مثلا KVM Host وعامل install ل VM علي السيرفر ده ف انت recommended ليك انك تعمل apply و activate لل virtual-host

Managing Profiles From The Command Line

- ال **Tuned service** بينزل معاها مجموعه من ال Command Line Tools اهمهم Command اسمه Tuned-adm وبنستخدمه علشان ن Manage بيه ال Profiles الخاصه بال Tuned

➢ اول command وهو **Tunned-adm active** وده بنستخدمه علشان ن list بيه ال current active profile الموجوده عندنا

```
[root@server~]# tunned-adm active
```

➢ تاني Command وهو **Tuned-adm list** وده بنستخدمه علشان ن List بيه كل ال Available profiles الموجوده عندي في السيستم وكمان بي Display ال Current active profile

```
[root@server~]# tuned-adm list
```

➢ تالت Command وهو **Tuned-adm profile** بستخدمه لو انا عايز اعمل active ل profile معين

```
[root@server~]# tuned-adm profile throughput-performance
```

➢ رابع command وهو **tuned-adm recommend** بستخدمه لو انا عايز اعرف ايه ال recommend a tuning profile للسيستم

```
[root@server~]# tuned-adm recommend
```

- اخر command وهو **tuned-adm off** وده بنستخدمه لو احنا عايزين نعمل turn off لل tuned servers

```
[root@server~]# tuned-adm off
```

هنشوف ازاي نستخدم ال commands اللي شرحناها

- تعال نشوف ازاي نعمل install و enable لل tuned service

```
[root@MohamedAtef ~]# dnf install tuned
[root@MohamedAtef ~]# systemctl enable --now tuned
[root@MohamedAtef ~]# systemctl status  tuned
● tuned.service - Dynamic System Tuning Daemon
   Loaded: loaded (/usr/lib/systemd/system/tuned.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-06-08 18:47:22 EET; 5s ago
     Docs: man:tuned(8)
           man:tuned.conf(5)
```

- اول مابنعمل install و start لل tuned هي by default بتروح ت select ال recommended profile وتعمله Active وعلشان نتاكد تعال نقوله **tuned-adm active** علشان ي list الاكتيف بروفايل هيقولك ال current active profile هو virtual-guest

```
[root@MohamedAtef ~]# tuned-adm active
Current active profile: virtual-guest
```

- تعال نشوف ال recommended profile هيقولي ال recommended هو ال virtual-guest ليه علشان انا شغال علي Virtual Machine

```
[root@MohamedAtef ~]# tuned-adm recommend
virtual-guest
```

- لو انا عايز أ List كل ال Available Profile الموجوده عندي دي نفس البروفايل اللي شرحناها في الاول

```
[root@MohamedAtef ~]#  tuned-adm list
Available profiles:
- accelerator-performance     - Throughput performance-based tuning with disabled higher latency STOP states
- aws                         - Optimize for aws ec2 instances
- balanced                    - General non-specialized tuned profile
- desktop                     - Optimize for the desktop use-case
- hpc-compute                 - Optimize for HPC compute workloads
- intel-sst                   - Configure for Intel Speed Select Base Frequency
- latency-performance         - Optimize for deterministic performance at the cost of increased power consumption
- network-latency             - Optimize for deterministic performance at the cost of increased power consumption,
focused on low latency network performance
- network-throughput          - Optimize for streaming network throughput, generally only necessary on older CPUs or
40G+ networks
- optimize-serial-console     - Optimize for serial console use.
- powersave                   - Optimize for low power consumption
- throughput-performance      - Broadly applicable tuning that provides excellent performance across a variety of common
server workloads
```

- سؤال هل دي كل ال profiles الموجوده عندي لا انت ممكن ت create و ت optimize profile علي حسب ال use case بتاعتك وممكن كمان ت search باستخدام dnf command زي مثلا **dnf search profiles**

```
[root@MohamedAtef ~]# dnf search profiles
Updating Subscription Management repositories.
Unable to read consumer identity
This system is not registered with an entitlement server. You can use subscription-manager to register.
Last metadata expiration check: 23:38:38 ago on Fri 07 Jun 2024 07:35:11 PM EET.
================================ Name & Summary Matched: profiles ================================================
power-profiles-daemon.x86_64 : Makes power profiles handling available over D-Bus
texlive-colorprofiles.noarch : Collection of free ICC profiles
================================== Name Matched: profiles ========================================================
tuned-profiles-atomic.noarch : Additional tuned profile(s) targeted to Atomic
tuned-profiles-cpu-partitioning.noarch : Additional tuned profile(s) optimized for CPU partitioning
tuned-profiles-mssql.noarch : Additional tuned profile(s) for MS SQL Server
tuned-profiles-oracle.noarch : Additional tuned profile(s) targeted to Oracle loads
tuned-profiles-postgresql.noarch : Additional tuned profile(s) targeted to PostgreSQL server loads
tuned-profiles-spectrumscale.noarch : Additional tuned profile(s) optimized for IBM Spectrum Scale
================================= Summary Matched: profiles ======================================================
authselect.x86_64 : Configures authentication and identity sources from supported profiles
```

- لما عملنا سيرش علي البروفايل ظهر عندنا مجموعه من ال profiles زي مثلا mssql و oracle و PostgreSQL
- يعني مثلا لو انت هتعمل install ل MS SQL Server ف قالك recommended انك تعمل اكتيفيت لل profiles ده tuned-profiles-mssql.noarch في حاله مثلا ال oracle فلازم تعمل اكتيفيت للبروفايل الخاص بيه
- تعال مثلا نعمل install لبروفايل ال oracle

```
[root@MohamedAtef ~]# dnf install tuned-profiles-oracle.noarch
```

- لما نعمل install لل oracle هيكون available مع باقي ال profilesالتانيه لو جينا عملنا tuned-adm list هنلاقي البروفايل انضاف مع كل الprofiles المتاحين عندي
- علشان نعمل active ل profile معين وليكن هنعمل اكتيف ل البروفايل الخاص بال oracle اللي احنا لسه عاملين ليه install هستخدم

```
[root@MohamedAtef ~]# tuned-adm profile oracle
[root@MohamedAtef ~]# tuned-adm active
Current active profile: oracle
```

هنا بعمل اكتيف للبروفايل اللي اسمه اوركال
وبستخدك الامر ده زي ماحنا عارفين علشان اعرض الاكتيف بروفايل
هنا هيقولي ان الاكتيف بروفايل هو الاوركال

- ممكن اننا نعمل اكتيفيت ل اكتر من بروفايل في نفس الامر زي مثلا انا عايز اعمل اكتيف للبروفايل اللي اسمه oracle والبروفايل throughput-performance

```
[root@MohamedAtef ~]# tuned-adm profile oracle throughput-performance
[root@MohamedAtef ~]# tuned-adm active
Current active profile: oracle throughput-performance
```

لو ملاحظ هتلاقي الاتنين اتعملهم اكتيف

- انا عندي ال main configuration file لل tuned تحت **/etc/tuned/** لو دخلنا تحت المسار ده وعملنا ls هنلاقي عندنا ملف اسمه active-profile ده بيكون جواه ال active profile بتاعك

```
[root@MohamedAtef ~]# cd /etc/tuned/
[root@MohamedAtef tuned]# ls
active_profile  bootcmdline  post_loaded_profile  profile_mode  recommend.d  tuned-main.conf
```

- تعال نعمل cat لل active_profile ونشوف ايه ال active profile بتاعنا

```
[root@MohamedAtef tuned]# cat active_profile
oracle throughput-performance
```

- فيه عندي ملف كمان مهم جدا اسمه tuned-main.conf ده بيكون ال main configuration file الخاص ب ال tuned service وده بيكون فيه مجموعه من ال parameters من ال parameters المهمه الموجوده في الملف ده ال dynamic_tuning = 0 ده معناه ان ال dynamic tuning بيكون disabled

```
[root@MohamedAtef tuned]# cat tuned-main.conf
# Global tuned configuration file.
# Whether to use daemon. Without daemon it just applies tuning. It is
# not recommended, because many functions don't work without daemon,
# e.g. there will be no D-Bus, no rollback of settings, no hotplug,
# no dynamic tuning, ...
daemon = 1
# Dynamicaly tune devices, if disabled only static tuning will be used.
dynamic_tuning = 0
```

- فيه عندي location بيكون stored جواه كل ال profiles الموجوده عندي في السيستم /usr/lib/tuned/ لو دخلت جوه المسار ده وعملت ls هيعرضلي كل ال profilesالموجوده عندي وكل profiles ليه Directory خاص بيه وبيكون جوه كل directory لكل ال profiles ملف باسم tuned.conf ده بيكون محدد جواه كل ال tuning parameters اللي هو بيستخدمها

```
[root@MohamedAtef tuned]# cd /usr/lib/tuned/
[root@MohamedAtef tuned]# ls
accelerator-performance   desktop   intel-sst   network-throughput   powersave   virtual-guest
aws   functions   latency-performance   optimize-serial-console   recommend.d   virtual-host
balanced   hpc-compute   network-latency   oracle   throughput-performance

[root@MohamedAtef tuned]# cd accelerator-performance/
[root@MohamedAtef accelerator-performance]# ls
tuned.conf
```

Create Custom Profile

- لو انا عايز اعمل Custom Profile عندي Two options
1- ي اما اعمل create لل custom profile في المكان ده /usr/lib/tuned/ وده مش recommended
2- ي اما ادخل جوه /etc/tuned/ وده ال recommended . واعمل فولدر للبروفيل بتاعي واحط جواه ال Tuned.conf
- تعال نعمل create لبروفايل معين مثلا اسمه web-server . ف احنا اول حاجه هنعملها هندخل جوه /etc/tuned/ وبعدين هنعمل create ل folder باسم ال web-server وبعدين ندخل جوه ال folder ده و نعمل create ل file باسم tuned.conf

```
[root@MohamedAtef tuned]# cd /etc/tuned/
[root@MohamedAtef tuned]# mkdir web-server
[root@MohamedAtef tuned]# cd web-server/
[root@MohamedAtef web-server]# touch tuned.conf
[root@MohamedAtef web-server]# ls
tuned.conf
```

- ونيجي مثلا نفتح ال tuned.conf باي editor عندي وليكن vim ونعمل جواه اي include ل اي بروفايل تاني انا كده كتبت جوه ال file وقولتله في ال main ان انا عايز أ include ال throughput-performance وعايز انفذ الاسكريبت اللي اسمه custom_script.sh

```
[main]
incluude=throughput-performance

[script]
script=custom_script.sh
```

- تعال نعمل create لملف الاسكريبت custom_script.sh ونديله permission Execute (+x)

```
[root@MohamedAtef web-server]# touch custom_script.sh
[root@MohamedAtef web-server]# chmod +x custom_script.sh
```

- وبعدين نكتب جوه الاسكريبت ان انا عايز ابعت الجمله دي "Custom tuned profile for web-server" في ال log file اللي اسمه custom_script.log تحت /var/log

```
#!/bin/bash
echo "Custom tuned profile for web-server" >>/var/log/custom_script.log
```

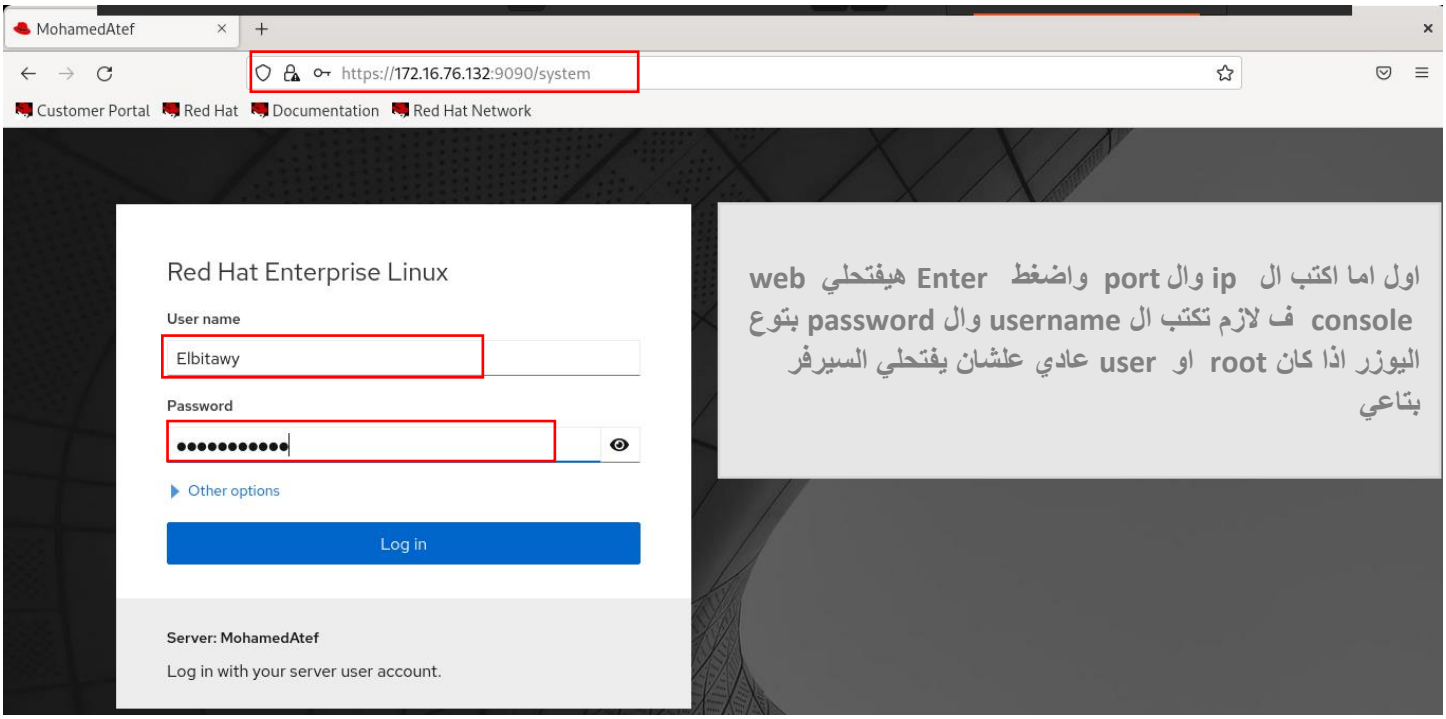
- انا كده عملت create ل ال custom profile بتاعي . علشان اتاكد انه create هقوله tuned-adm list هنلاقيه من ضمن ال profiles الموجوده عندي ولو روحت عملت active لل profile ده عن طريق الامر **tuned-adm profile web-server** هنلاقي الاسكريبت بتاعنا اتعمله create تحت /var/log/

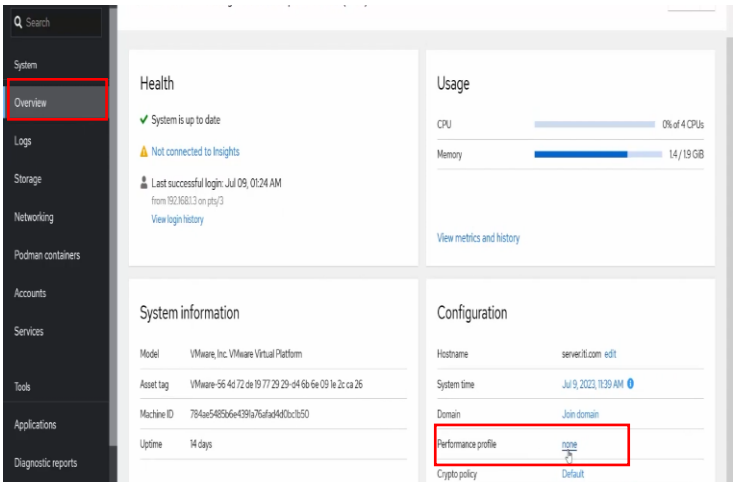
- فيه عندي طريقه تانيه اقدر من خلالها ان انا أ manage بيها ال Tuned بتاعتي عن طريقه service اسمها Cockpit وده عباره عن web interface او web console

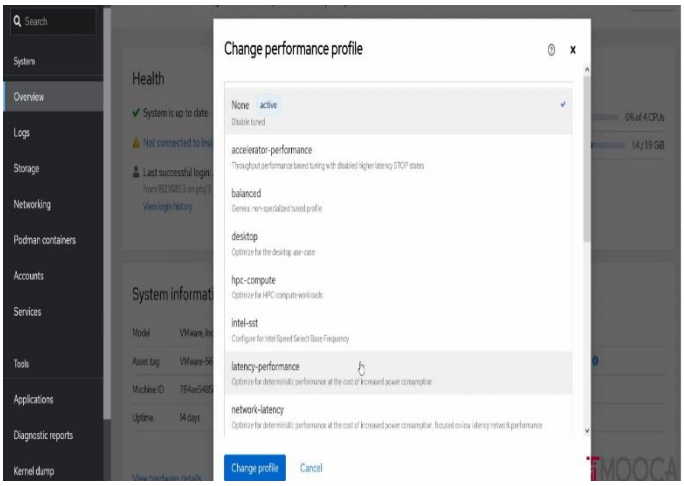
➢ تعال نعمل start لل service اللي اسماه Cockpitونشوف ال status بتاعتها

```
[root@MohamedAtef ~]# systemctl start cockpit
[root@MohamedAtef ~]# systemctl status cockpit
● cockpit.service - Cockpit Web Service
   Loaded: loaded (/usr/lib/systemd/system/cockpit.service; static)
   Active: active (running) since Sun 2024-06-09 01:02:03 EET; 5s ago
```

➢ علشان نعرف ن access ال cockpit عن طريق ال web console بفتح اي متصفح عندي واحط فيه IP السيرفر بتاعي واحط port 9090







Linux process scheduling and multitasking:

- The way Linux (and other operating systems) can run more processes is by employing a technique called time-slicing.
- The part of the Linux kernel that performs this switching is called the process scheduler.
- There are exactly 40 different levels of niceness a process can have (-20 to 19).
- By default, processes will inherit their nice level from their parent, which is usually 0.
- Higher nice levels indicate less priority, while lower nice levels indicate a higher priority.
- Only root is allowed to set negative nice levels and lower the nice level on existing processes.
- Un privileged users are only allowed to set positive nice levels, and they are only allowed to raise the nice level on their existing process but cannot lower them.

- هنتكلم عن ازاي ن manage ال priority of Linux process مبدئيا كده كل process بتكون running عندي ف السيستم بتكون ليها process ID وبيبقي ليها حاجه اسمها priority level أو nice level وزي ماحنا عارفين أن ال operating systems بيكون شغال ب Technique اسمه Time-slicing بمعني أن هو ب assign time slot لكل process علشان ت run فيها يعني بمعني لو انا عندي اكتر من process waiting to be executed جوه ال CPU بتاعي ف هو بي assign time slot لكل process علشان ت run فيها ويطلع ال process ويدخل process بعدها وهكذا الكلام ده اللي بي handle القصه دي بيكون ال kernel بتاعي ال kernel عنده حاجه اسمها process scheduler هي المسئوله انها ت switch مابين ال process وبعضها بس انت بالنسبالك علشان خاطر عمليه ال switching بتكون سريعه جدااا ف انت هتحس أن كل الprocess بتكون running at the same time انا عندي كل process بتكون running ف السيستم بت assign ليها nice level أو priority level وبتكون مابين -20 و 19 يعني من الاخر انا عندي40 different priority levels ف لو انا عندي two processes واحده منهم واخده priority -20 والprocess التانيه واخده priority 19 ف البروسيس اللي واخده priority -20 ليها ال highest priority عن البروسيس اللي واخده 19 و by default كل ال processes اللي running عندي ف السيستم بت inherit نفس ال nice level بتاعت ال parent بتاعهم اللي هو by default بيكون عاده ب 0 ف لو انت جيت عملت list لكل ال processes اللي شغاله عندك هتلاقي معظمهم واخدين 0 وطبعا الروت مسموح ليه أنه ي set negative nice levels او ي set lower the nice level - بينما الun privileged users أو regular user هو بس مسموح ليه أنه يت change ال priority بتاعت الprocess بتاعته في الpositive direction يعني لو عندي user اسمه Mohamed وعنده process معينه وعايز يغير ال priority بتاعتها وهي مثلا واخده 0 priority ف هل Mohamed يقدر يset الpriority بتاعتها ف ال negative direction ويخليها 5- أو 20- لا طبعا هو قالك أنه مش مسموح ليه أنه ي set في الnegative direction طب هو يقدر يخليها 5 أو 10 اه عادي مفيش مشكله طالما بي set ف الpositive direction طب لو ال regular user غير ال priority من zero خلاها 5 هل يقدر يرجعهاا تاني ل 4 أو 3 لا ميقدرش لو انت زودت ف الpositive direction متقدرش تقلل تاني.

How to set linux process priority using nice and renice commands

- Processes are scheduled according to priority.
- negative values are allowed only to root.

```
[root@lab01 ~]# ps l (To show nice values)
Or)
[root@lab01 ~]# ps axo user,pid,nice,command
[root@lab01 ~]# ps axo user,pid,command,nice --sort=nice
[root@lab01 ~]# ps axo user,pid,command,nice --sort=user
```

- The nice command is used to start a process with a user defined priority.

```
[root@lab01 ~]# nice vim text & (Default is 10)
[1] 9182
[root@lab01 ~]# nice -n vim text &
```

- The renice command is used to change the priority of a currently running process.

```
[root@lab01 ~]# renice 19 9182 (19 is the new value)
[root@lab01 ~]#top (press r to renice a process)
```

TMOOCA MEDIA PRODUCTION

- علشان أ List ال priority بتاعت ال process ال running عندي . عندي command اسمه **ps l** هنلاقي فيه عمود عندي اسمه NI (nice) هنلاقي معظم ال process واخده قيمه 0 وبعض ال process واخده قيمه -20

```
[root@MohamedAtef ~]# ps l
F  UID  PID   PPID  PRI  NI   VSZ     RSS   WCHAN   STAT  TTY    TIME   COMMAND
0  0    1733  1729  20   0    224608  2436  do_wai  Ss    pts/0  0:01   -bash
0  0    1943  1733  0    -20  229496  600   do_sig  T     pts/0  0:00   vim tuned.conf
0  0    1972  1733  0    -20  229560  456   do_sig  T     pts/0  0:00   vim tuned.conf
```

- وممكن استخدم الامر **ps axo** وبعدين احددله يعرضلي ايه زي مثلا هخليه يعرضلي ال user وال pid وال nice وال command باستخدام **ps axo user,pid,nice,command**

```
[root@MohamedAtef ~]# ps axo user,pid,nice,command
USER    PID   NI   COMMAND
root    1     0    /usr/lib/systemd/systemd rhgb --switched-root --system --deserialize 31
root    2     0    [kthreadd]
root    3     -20  [rcu_gp]
root    4     -20  [rcu_par_gp]
```

- علشان اغير ال priority بتاعت اي بروسيس عندي فيه عند two command عندي command اسمه **nice** و command اسمه **renice**
- ال **nice** بستخدمه لو انا عايز اعمل start ل process معينه بي user defined. بقوله nice وبديله اسم ال command بتاعي زي مثلا **nice vim text** في الحاله دي لو انا محددتلهوش رقم ال priority بتاعتي ف هو ها assign رقم ال priority رقم 10 by default يعني هيعمل استارت للبروسيس دي وهيديها priority قيمتها 10
- ال **renice** بستخدمه لو انا عايز اعمل change لل priority عن طريق ان انا هستخدم **renice new_priority old_priority**

Chapter 4

Controlling Access to Files with ACLs

Access control list

- ACL provides an additional flexible permission mechanism for file system on a Linux system. It enhance the traditional UNIX file permissions for files & folder. With ACL, you can give permissions for any user or any group with fine-grained access rights.
- ACLs can be configured per user, per group or via the effective rights mask. These permissions then can be applying to an individual user or a group, and you can use the same as rwx (Read, Write, Execute) found in regular file/ folder permissions.

Check kernel for ACL support

- To check ACL Support for file system and **POSIX_ACL=Y** option (if there is **N** instead of **Y**, then it means Kernel doesn't support ACL and need to be recompiled).

```
[root@lab01 ~]# grep -i acl /boot/config*
CONFIG_EXT4_FS_POSIX_ACL=y
CONFIG_XFS_POSIX_ACL=y
CONFIG_BTRFS_FS_POSIX_ACL=y
```

- ال ACL(Access Control List) دي عباره عن futures في اللينكس بقدر استخدمها علشان أ control بيها ال permissions بتاعت اي file او directory موجوده عندي
- طب ايه الفرق مابينها ومبين ال standard او ال traditional permissions اللي احنا اخدناها في ادمن 1 نقدر نقول ان ميزه ال ACL انها more flexible بمعني اننا في ال standard permissions كنا بن apply ال permission علي three categories علي ال user owner وعلي ال group owner وعلي ال others . طب لو انا عندي special user في ال others وعايز اديله special permission علي special file او directory ف انا مش هقدر اعمل كده بال standard permissions العاديه ودي ميزه ال ACL ان انا اقدر اعمل apply او أ set special permissions ل special user او group علي special file or directory
- طب لو انا عايز اتاكد هل ال kernel بي support ال ACL هستخدم الامر grep -i acl /boot/config

```
[root@MohamedAtef ~]# grep -i acl /boot/config-5.14.0-284.11.1.el9_2.x86_64
CONFIG_EXT4_FS_POSIX_ACL=y
CONFIG_XFS_POSIX_ACL=y
CONFIG_FS_POSIX_ACL=y
```

هنلاقي كل ال kernel parameters بتساوي y معناها ان ال kernel بيدعم ال ACL

Viewing and interpreting ACL permissions

- The **ls -l** command only outputs minimal ACL setting details:

```
[user@host content]$ ls -l reports.txt
-rwxrw----+ 1 user operators 130 Mar 19 23:56 reports.txt
```

- The plus sign **(+)** at the end of the 10-character permission string indicates that an extended ACL structure with entries exists on this file.

- لو انا عايز اتاكد هل ال file عليه ACL هستخدم **ls -l filename** ف لو لاقيت **(+)** plus signجنب ال permissions معني كده ان ال file ده عليه ACL

```
[root@MohamedAtef tmp]# ls -l reports.txt
-rw-r--r--+ 1 root root 0 Jun  9 05:03 reports.txt
```

View File ACLs

- To display ACL settings on a file, use getfacl file:

```
[user@host content]$ getfacl reports.txt
```

```
[user@host content]$ getfacl reports.txt
# file: reports.txt
# owner: user
# group: operators
user::rwx
user:consultant3:---
user:1005:rwx        #effective:rw-
group::rwx           #effective:rw-
group:consultant1:r--
group:2210:rwx       #effective:rw-
mask::rw-
other::---
```

- لو انا عايز اعرف معلومات ازيد عن ال ACL بنستخدم command اسمه **getfacl** وبعدين اديله اسم ال file او ال directory يبقي ال **getfacl** انا بستخدمه علشان أ display بيه كل ال ACL entries ال configure علي اي file او directory عندي
- وزي ماحنا شايفين في ال slide اللي فوق شكل ال output لما استخدمنا ال **getfacl** علي ملف وده بيكون عباره عن مجموعه من ال entries اول entries بيكون اسمها comments entries وبعد كده ال user و ال group وال mask وال other هنعرف كل ده بالتفصيل

1- Commented entries

```
# file: reports.txt
# owner: user
# group: operators
```

1- اول section موجود عندي اسمه **Commented entries** ودول بيكونوا اول 3 سطور وبيكونوا عباره عن comment

- اول comment بيقولي ايه هو ال file name بتاعك
- تاني comment بيقولي ايه هو ال owner
- تالت comment بيقولي مين هو ال group owner بتاع ال file ده
- خلي بالك من حاجه لو انت عندك اي file او Directory عليه special permissions زي setuid او setgid او sticky bit هنلاقي عندنا comment رابع اسمه flags وهتلاقيه حاططلي ال permissions
- تعال نشوف مثال علي ال flags لو جيت طبقت ال getfacle علي three files مختلفين زي مثلا passwd وlocate و tmp علشان اشوف شكل ال special permissions عليهم

```
[root@MohamedAtef ~]# getfacl /usr/bin/passwd
# file: usr/bin/passwd
# owner: root
# group: root
# flags: s--
user::rwx
group::r-x
other::r-x
```

هنلاقي هنا line رابع اسمه flags وهنلاقي في اول بت فيه S ده كده
بيديك indication ان فيه setuid applied علي ال passwd

```
[root@MohamedAtef ~]# getfacl /usr/bin/locate
# file: usr/bin/locate
# owner: root
# group: slocate
# flags: -s-
user::rwx
group::--x
other::--x
```

هنلاقي هنا line رابع اسمه flags وهنلاقي في تاني بت فيه S ده كده
بيديك indication ان فيه setgid applied علي ال locate

```
[root@MohamedAtef ~]# getfacl /tmp/
# file: tmp/
# owner: root
# group: root
# flags: --t
user::rwx
group::rwx
other::rwx
```

هنلاقي هنا line رابع اسمه flags وهنلاقي في تالت بت فيه t ده كده
بيديك indication ان فيه applied sticky bit علي ال tmp

2- User entries

```
user::rwx                          ❶
user:consultant3:---               ❷
user:1005:rwx       #effective:rw- ❸
```

2- تاني section عندي اسمه **User entries** ودي بتكون عباره عن مجموعه من ال entries بتبدء بكلمه User

- لو جينا بصينا علي اول line هتلاقيه كاتبلك user::rwx ودي معناها ان ال owner بتاع ال file اللي اسمه user عليه كل ال permissions
- تاني line عندي قايلك ان ال named user اللي اسمه consultant3 معندهوش اي permissions
- تالت line قايلك ال user اللي UID بتاعه 1005 عنده rwx وكاتبلك قدامه comment قايلك خلي بالك ال effective permissions بتكون rw بس . ودي هنشوفها لما ناخد ال mask

3- Group entries

```
group::rwx          #effective:rw- ❶
group:consultant1:r--              ❷
group:2210:rwx      #effective:rw- ❸
```

3- تالت section اسمه **Group entries** ودي بتكون عباره عن مجموعه من ال entries بتبدء بكلمه group ودي نفس فكره ال User entries

- عندي اول line عباره عن ال permissions بتاعت ال group owner
- تاني Line قايلك ان ال named group اللي اسمه consultant1 عنده read permissions بس
- تالت line قايلك ال group اللي ال GID بتاعه 2210 عنده read و write و execute

4- Mask entry

```
mask::rw-
```

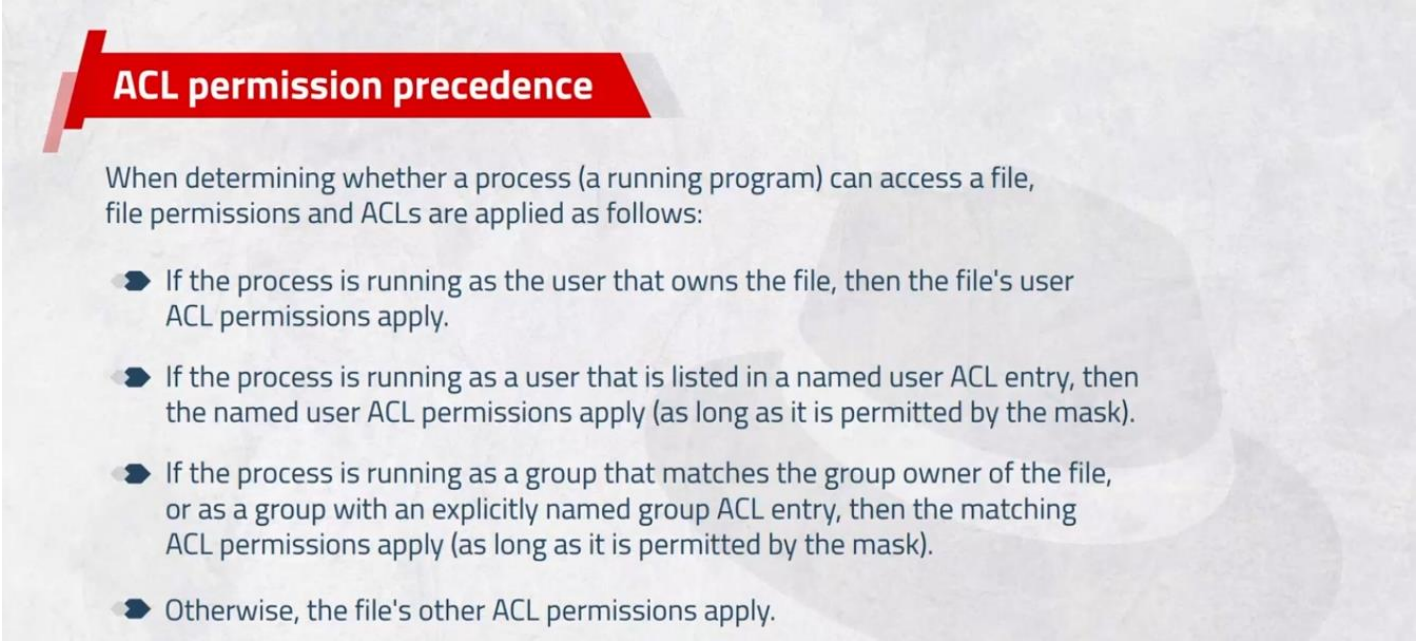
4- رابع section معانا وهو ال Mask entry ودي عباره عن entry بتبدء بكلمه mask:: وبعدين ال permissions . وظيفه ال mask ان انا بقدر أ control بيه اواقدر أ limit ال maximum permissions that be applied علي ال named users او ال group owner او ال named groups وملهوش اي effect علي ال user owner او others

- يعني بكل بساطه لو انا عندي named user معين وال UID بتاعه مثلا 1005 وكان واخد read و write و execute واخد permissions اعلي من ال mask سامح بيه هتلاقي ظاهر في ال ouput بتاعك comment بيقولك #effictive:rw- ان خلي بالك ان ال user اللي ال UID بتاعه 1005 عنده rwx ف ال user ده مش هيقدر انه يعمل execute علشان ال mask عمل limit علي ال permissions
- لو عايز اعمل list لل mask هستخدم الامر **getfacl**
- ولو عايز اعمل set لل mask هستخدم الامر **setfacl**

5- Other entry

```
other::---
```

5- خامس section وهو ال Other وده عباره عن entry بيبدي ب other:: وبعدين ال permissions . يعني مثلا عندي في المثال اللي فوق بيقولك other::--- معني --- انه معلهوش اي permissions ان لو عندي اي حد ملهوش explicit entry في ال ACL هيتطبق عليه ال other permissions بمعني ولا هو user owner ولا هو ال Group owner ولا حد من ال named user ولا ال named group ف في الاخر بيطبق عليه ال other



- ال ACL permission precedence دي معناها ان ال ACL بت follow order معين علشان تت check وت applied ال effect permissions علي ال users و ال groups يعني مثلا لو عندي user بي access ملف معين ف ممكن ال user وهو بي access يكون من ضمن الحالات دي

1- هل ال user اللي بي access هو ال owner بتاع ال file ساعتها ال permissions بتاعت ال user owner will be applied

2- لو ال user ده مش ال user owner طب هل هو listed في ال named user الموجودين في ال ACL ساعتها هياخد ال permissions بتاعت ال named user يعني لو عندي مثلا ال named use اسمه كريم وواخد rwx وال mask بتاعي rw بس ف ساعتها كريم ال effective permission بتاعته هتكون rw

3- لو ال user لا هو ال owner ولا هو listed في ال named user الموجودين عندنا . لو هو member في ال group owner ساعتها ال group owner permissions will be applied

4- طب لو ال user لا هو ال owner ولا listed في ال named user ولا listed في اي group من ال group entry الموجودين في ال ACl ساعتها ال other permissions will be applied

5- طب لو انا عندي user وال user ده member من two groups وال two groups موجودين عندي ليهم entries في ال ACL وكل جروب منهم ليه permission مختلف عن التاني ف ساعتها ال user ده هياخد انهي permission هياخد اعلي permission

How to set new ACLs

- Use the '**setfacl**' command for setting or modifying on any file or directory.

```
[root@lab01 ~]# setfacl -m u:karim:rw file.txt    (We can use UID or username)
[root@lab01 ~]# setfacl -m o::rw file.txt
[root@lab01 ~]# setfacl -m g:sales:rw dir1
[root@lab01 ~]# setfacl -R -m g:sales:rw dir1   (We can also use GID or group name)
```

- You can add multiple entries with the same command; use a comma-separated list of entries:

```
[root@lab01 ~]# setfacl -m u::rwx,g:consultants:rx,o::- file.txt
```

- You can use the output from getfacl as input to setfacl,In this case, file-B will have the same ACL settings as file-A

```
[user@host ~]$ getfacl file-A | setfacl --set-file=- file-B
```

MOOCA MEDIA PRODUCTION

- ال command اللي احنا هنستخدمه علشان ن set او ن modify او ن remove ال ACL بتاعت اي file او directory اسمه **setfacl**
- تعال مثلا ندخل تحت /tmp ونعمل touch ل file وليكن مثلا ال file ده اسمه reports.txt

```
[root@MohamedAtef ~]# cd /tmp
[root@MohamedAtef tmp]# touch reports.txt
```

- لو عملنا ls -l علي ال file هنلاقي ال default permission اللي واخدها rw لل owner و r ل group و r ل other والدوت . اللي جنب ال permission معناها ان مفيش ACL علي ال file

```
[root@MohamedAtef tmp]# ls -l reports.txt
-rw-r--r--. 1 root root 0 Jun 10 04:30 reports.txt
```

- او ممكن نستخدم getfacl

```
[root@MohamedAtef tmp]# getfacl reports.txt
# file: reports.txt
# owner: root
# group: root
user::rw-
group::r--
other::r--
```

- لو انا عايز ادي permission ل user علي ملف او فولدر هستخدم الامر **setfacl**
- تعال ندي ل user وليكن karim هنديله read permission علي ال file اللي اسمه reports.txt وبعدين نعمل ls -l علي الfile علشان نشوف هل فعلا اتطبق عليه ال ACL ولا لا او ممكن نستخدم الامر getfacl

```
[root@MohamedAtef tmp]# setfacl -m u:karim:r reports.txt
[root@MohamedAtef tmp]# ls -l reports.txt
-rw-r--r--+ 1 root root 0 Jun 10 04:30 reports.txt
[root@MohamedAtef tmp]# getfacl reports.txt
# file: reports.txt
# owner: root
# group: root
user::rw-
user:karim:r--
group::r--
mask::r--
other::r--
```

هنا استخدمت m- علشان اعمل modify

لو لاحظنا هنلاقي + ده كده بيديك indications ان فيه ACL

هنلاقي هنا new user entry ظهرت هنا في ال ACL ل Karim وفيه read permission

هنلاقيه علي طول بعد اما طبقنا ال ACL هنلاقيه زود entry بتاعت ال mask

- اكيد جه ف بالك في المثال السابق ال read permission اللي موجوده في ال mask ال permission ده اتحط علي اساس ايه في ال mask . احنا قولنا قبل كده ان ال mask ده وظيفته ان انا ب control بيه او بن limit ال maximum permission اللي هياخدها ال named user وال named groups وال group owner . بيتعملها recalculations كل مره بتعمل change او modify في ال ACL بتاعتك . بناءا علي ال permission اللي واخدها ال named user وال named groups وال group owner ان انا عندي اليوزر اللي اسمه كريم واخد read (user:karim:r--) والجروب واخد read (group::r--) لو انا عملت اتحاد (union) مابين ال permissions هيبقي ال permission الخاصه بال mask هي read
- مثال تاني علشان الفكره توضح تعال ندي write permission ليوزر تاني اسمه ali ونشوف ال mask هيكون ايه

```
[root@MohamedAtef tmp]# setfacl -m u:ali:w reports.txt
[root@MohamedAtef tmp]# getfacl reports.txt
# file: reports.txt
# owner: root
# group: root
user::rw-
user:karim:r--
user:ali:-w-
group::r--
mask::rw-
other::r--
```

هناخد ال permissions دي مع بعض ال read,write,read ونعملها اتحاد مع بعض هيطلع ال mask ب rw

Backup and Remove ACL

1- لو عايز اخد Backup من ال ACL الموجود علي file معين هستخدم ال

getfacl /path/to/directory > backup_acl.txt

- يعني لو انا عندي fileاسمه report.txt وعايز اخد backup منه ف انا هستخدم ال getfacl وبعدكده اكتب اسم ال file اللي انا عايز اخد منه ب backup وبعد كده اعمل redirect لل output في file تاني اسمه مثلا acl.txt زي ماهو واضح في المثال

```
[root@MohamedAtef tmp]# getfacl reports.txt >acl.txt
[root@MohamedAtef tmp]# cat acl.txt
# file: reports.txt
# owner: root
# group: root
user::rw-
user:karim:r--
user:ali:-w-
group::r--
mask::rw-
other::r--
```

- لو انا عايز اعمل restore للACL الموجود في file معين هستخدم

setfacl --set-file=acl.txt file1.txt

- تعال مثلا نعمل create ل file تاني اسمه file1.txt وانا عايز اعمل restore لل ACL الموجوده في ال fileاللي اسمه acl.txt علي ال file اللي اسمه file1.txt اني اعمل apply لل ACL علي ال file1.txt

```
[root@MohamedAtef tmp]# touch file1.txt
[root@MohamedAtef tmp]# setfacl  --set-file=acl.txt file1.txt
[root@MohamedAtef tmp]# getfacl file1.txt
# file: file1.txt
# owner: root
# group: root
user::rw-
user:karim:r--
user:ali:-w-
group::r--
mask::rw-
other::r--
```

- ملاحظه لو انا اخدت copy من file1 مثلا ل file2 وfile1 عليه ACL ال ACL مش هيتعملها apply علي file2 علشان اعمل copy بال ACL هستخدم p- مع ال copy زي مثلا cp -p file1 file2

```
[root@MohamedAtef tmp]# cp file1.txt file2.txt
[root@MohamedAtef tmp]# ls -l file1.txt file2.txt
-rw-rw-r--+ 1 root root 0 Jun 11 23:15 file1.txt
-rw-r--r--. 1 root root 0 Jun 11 23:25 file2.txt          لم يتم تطبيق ال ACL

[root@MohamedAtef tmp]# cp  -p file1.txt file2.txt
cp: overwrite 'file2.txt'? yes

[root@MohamedAtef tmp]# ls -l file1.txt file2.txt
-rw-rw-r--+ 1 root root 0 Jun 11 23:15 file1.txt
-rw-rw-r--+ 1 root root 0 Jun 11 23:15 file2.txt          تم تطبيق الACL
```

How to remove ACLs

For removing ACL from any file/ directory, we use **x** and **b** options as shown below.

```
[root@lab01 ~]# setfacl -x u:karim file.txt        (To remove ACL permissions for the user karim)
[root@lab01 ~]# setfacl -b file.txt                (roll back to the default ACL)
```

- **-n, --no-mask**
  - Do not recalculate the effective rights mask. The default behavior of setfacl is to recalculate the ACL mask entry, unless a mask entry was explicitly given. The mask entry is set to the union of all permissions of the owning group, and all named user and group entries. (These are exactly the entries affected by the mask entry).

```
[root@server home]# setfacl -n -m u:karim:rwx passwd
[root@server home]# setfacl -m u:karim:rw,m::r passwd
```

MOOCA

2- لو انا عايز اعمل **Remove** لل ACL فيه عندي Two options عندي اوبشن x واوبشن b

- اوبشن x لو انا عايز اعمل remove ل entry معينه من ال ACL من ال file بتاعي
- اما اوبشن b لو انا عايز اعمل roll back او أ remove كل ال ACL من ال fileبتاعي
- لو انا عايز اعمل remove لل named user اللي اسمه karim من علي ال file اللي اسمه report.txt هستخدم setfacl -x u:karim reports.txt

```
[root@MohamedAtef tmp]# getfacl reports.txt
# file: reports.txt
# owner: root
# group: root
user::rw-
user:karim:r—     remove  اللي هعمله name user  ده ال
user:ali:-w-
group::r--
mask::rw-
other::r--
```

→

```
[root@MohamedAtef tmp]# setfacl -x u:karim reports.txt
[root@MohamedAtef tmp]# getfacl reports.txt
# file: reports.txt
# owner: root
# group: root
user::rw-
user:ali:-w-
group::r--
mask::rw-
other::r--
```

- لو انا عايز اعمل remove لكل ال entry الموجوده هستخدم setfacl -b reports.txt هيرجع لل default

```
[root@MohamedAtef tmp]# getfacl reports.txt
# file: reports.txt
# owner: root
# group: root
user::rw-
user:ali:-w-
group::r--
mask::rw-
other::r--
```

→

```
[root@MohamedAtef tmp]# setfacl -b reports.txt
[root@MohamedAtef tmp]# getfacl reports.txt
# file: reports.txt
# owner: root
# group: root
user::rw-
group::r--
other::r--
```

- لو انا عايز وانا بت change ال ACL اقوله no mask متعملش recalculations لل mask بتاعك بزود اوبشن n-

```
[root@MohamedAtef tmp]# setfacl -n -m g:user1:rwx file1
```

Define default permissions and Apply rules recursively

- لو انا عايز اي file او directory هعمله create جوه ال directory يكون ليه نفس ال ACL بتاع ال directory بمعني اصح ان انا هعمل inherit علي مستوي ال file وال directory القديمه واللي هيتم انشائها حديثا فعلشان اعمل كده هستخدم اوبشن d مع ال command
- تعال نعمل create ل directory اسمه dir1 وبعدين نعمل set لل default permissions باستخدام الامر setfacl -m d:u:karim:rw- dir1 انا هنا زودت بس اوبشن d علشان اعمل inherit ل اي file او directory هيتعملهم create جوه ال dir1

```
[root@MohamedAtef tmp]# mkdir dir1
 [root@MohamedAtef tmp]# setfacl -m d:u:karim:rw- dir1
[root@MohamedAtef tmp]# getfacl dir1
# file: dir1
# owner: root
# group: root
user::rwx
group::r-x
other::r-x
default:user::rwx
default:user:karim:rw-
default:group::r-x
default:mask::rwx
default:other::r-x
```

هنلاقيه هنا حاطط مجموعه من ال default ACL معني كده ان اي file اتعمله create جوه ال dir1 هيتعمله inherit

- لو عايز اعمل remove ل default ACL هستخدم اوبشن -x

```
[root@MohamedAtef tmp]# setfacl -x d:u:karim:rw- dir1
```

- لو انا عايز اطبق علي مستوي directory وموجود جواه files هستخدم اوبشن -R

```
[root@MohamedAtef tmp]# setfacl -R -m u:karim:rw- dir1
```

Chapter 5

Managing SELinux Security

Why Use Security Enhanced Linux?

- Security Enhanced Linux (SELinux) is an **additional layer of system security**. The 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/other permission security model. This is a user and group based model known as discretionary access control. SELinux provides an additional layer of security that is **object-based** and controlled by more sophisticated rules, known as mandatory access control.

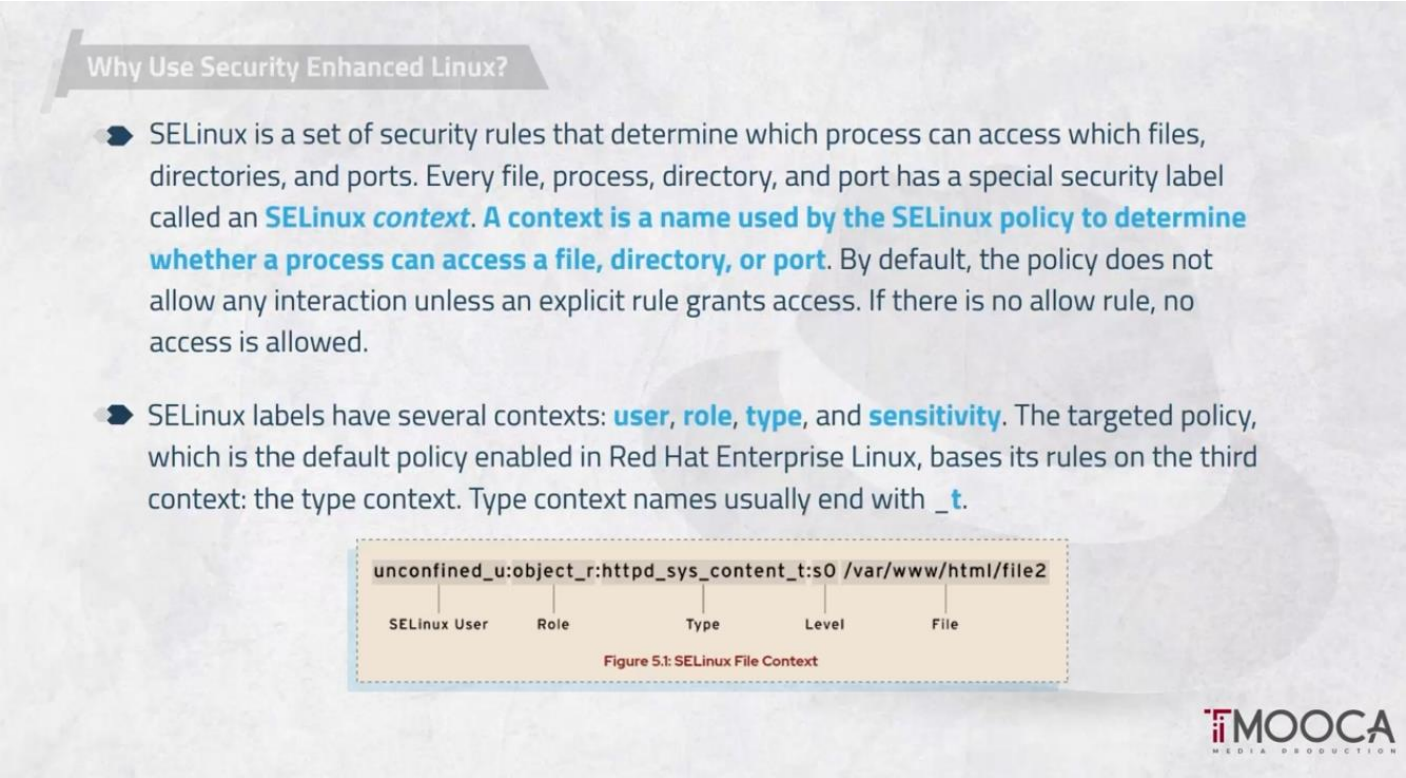
- To allow remote anonymous access to a web server, firewall ports must be opened. However, this gives malicious people an opportunity to crack the system through a security exploit. If they succeed in compromising the web server process they gain its permissions. Specifically, the permissions of the apache user and the apache group. That user and group has read access to the document root, **/var/www/html**. It also has access to **/tmp**, and **/var/tmp**, and any other files and directories that are world writable.

MOOCA

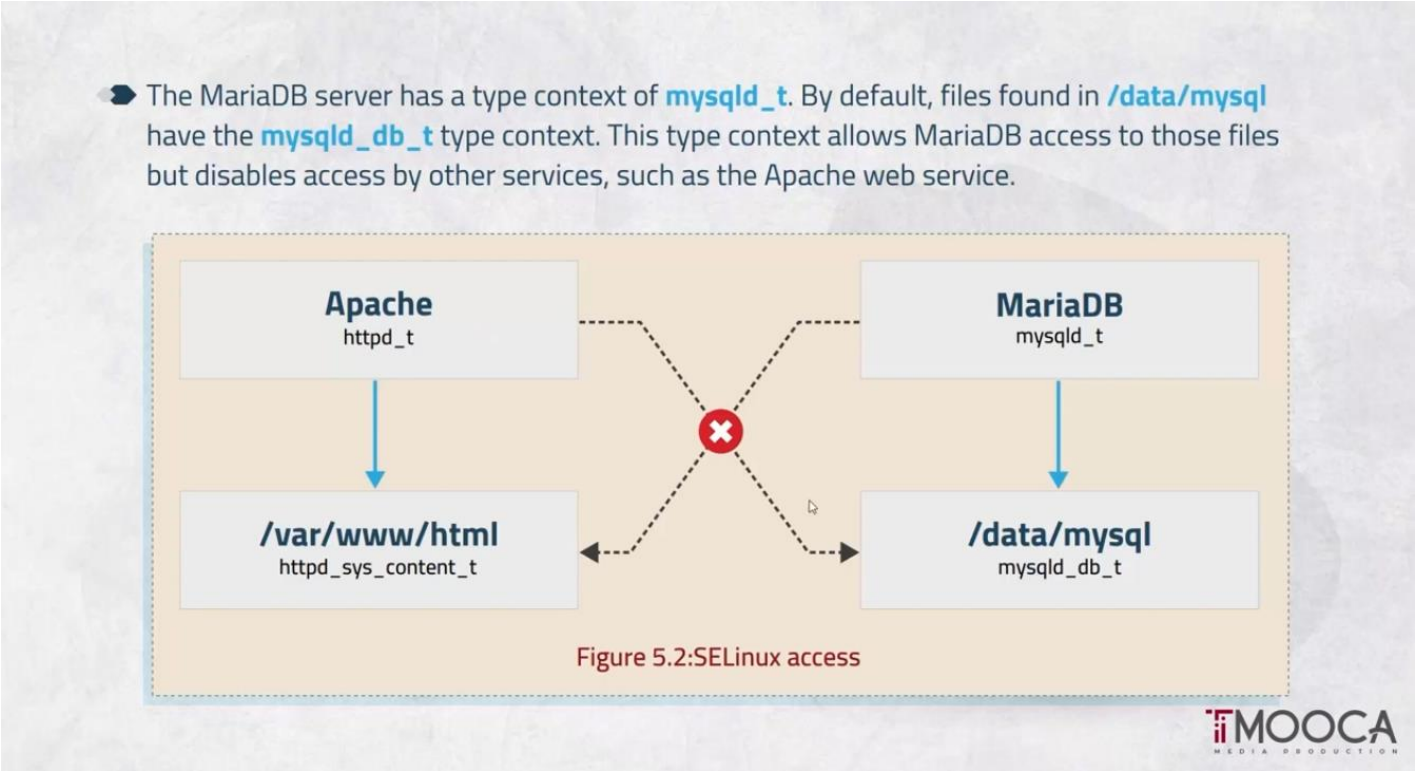
- ال **SELinux** عباره عن Additional layer of security بجانب ال traditional او ال standard permission
- قبل كده في admin 1 كنا اتكلمنا عن ال standard permission واخدنا حاجه اسمها special permission اللي هي كانت suid وال sgid وال sticky bit واخدنا في admin 2 ال ACL كل ال traditional permissions دي بيتقال عليها ال Discretionary Access Control (DAC) ودي بقدر من خلالها اني أ manage ال access بتاع ال files وبتكون based علي ال user وال group ownership بمعني ان في ال DAC ال owner او ال user هو اللي بي control ال permissions بتاعت ال files وال directors بتاعته وزي ماشوفنا قبل كده ان ال DAC عنده three level of access عنده حاجه اسمها read و write و execute وشوفنا تاثيرهم علي ال files وال directory وال permissions ودي بنعملها apply علي 3 categories علي ال owner وال group وال other ده كده بالنسبه لل DAC
- اما بالنسبه لل SELinux ده بيتقال عيلها ال Mandatory access control(MAC) ودي بقدر من خلالها اني أ control which subject ca access which object وال subject ده ممكن يكون process او service معينه او users سواء كان normal user او system user وال object ممكن يكون files او directory او ports او socket . وكمان ال selinux عندها مجموعه من ال roules او ال policy اللي بتكون stored عندها في حاجه اسمها SELinux policy database دي بيقدر من خلالها ياخد القرارسواء كان اي allow او ي grand او يdeny ال access . يعني من الاخر لو انا عندي في ال linux system ال selinux features معمولها enable كده هيكون عندي two later of security اول layer وهي ال MAC وتاني layer وهي ال DAC

- لو جينا شوفنا الفرق مابين ال DAC وال MAC هنلاقي ان في ال DAC ان ال owner او ال user هو اللي بي control ال Access بتاع ال files وطبعا لو ال user معندهوش ال experience الكافيه انه ي set ال permissions المظبوطه ده ممكن يسببلك security breaches في السيستم بتاعك علي عكس ال SELinux او الMAC وده بيكون عنده مجموعه من ال Rules المعقده اللي بتكون stored في الداتابيز وبيعملها enforce بشكل معين بحيث انه ي grant حاجه اسمها list privilege ومعناها انه هيدي ال process او ال user ال access اللي هو محتاجها بالظبط علي ال resources معينه بحيث انه من الاخر يعمل ال task المطلوبه منه وبيعمل restrict لل access بتاعته علي اي resources تانيه مش allowed ليه وده طبعا بيقللي ال impact بتاع ال security preaches علي عكس ال DAC
- وتاني حاجه ممكن نقولها ان ال DAC اسهل في التعامل وده بيخليه دايما ال default choice لأي system admin بس ده طبعا ال drawback بتاعه انه بيسبب security vulnerabilities

- علشان نفهم اكتر ال SELinux شغال ازاي خلينا ناخد مثال لنفرض مثلا ان عندك ويب سايت hosted عندك علي اي web server وليكن ال apache و by the way ال apache هو واحد من اشهر ال open source web servers المستخدمه حاليا وهنشوف كمان شويه ازاي هنعمله install ونستخدمه .فكره انك تكون فاتح public access لل web server بتاعك علشان ت allow وتخلي اي حد ي access ال website من اي مكان ده بيخليه دايما عرضه لل attacks فلو اي حد نجح انه ي compromise او يخترق ال webservers بتاعك عن طريق الاباتشي فساعتها هيقدر يوصل للسيستم بتاعك وهياخد ال permissions بتاعت ال apache user وال apache group ومش بس كده يقدر كمان يدخل علي ال location اللي بيبقي stored جواه ال files بتاعت ال web site ده اللي بتبقي stored by default تحت /var/www/html وكمان يقدر ان اي file او directory ليه permissions عليه زي مثلا /tmp و /var/tmp يقدر يدخل جواهم ويشوف ال files . ده في حاله لو ال SELinux معمول ليه disabled



- انا عندي كل file او process او directory او port موجود عندي في السيستم ال SELinux بت assign ليه حاجه اسمها security label او SELinux context وال context ده بيبقي عباره عن just name ال SELinux بتستخدمه علشان تحدد اذا كان انت هتعمل allow او deny لل access بتاعك و by default ال default behaver بتاع ال SELinux لو مفيش explicit rule بت allow او بت grants access هتعمل deny by default
- انا عندي ال context او ال labels بتتكون من 4 اجزاء . اول جزء وهو ال SELinux User تاني جزء وهو ال Role وتالت جزء وده الاهم بالنسبالنا وهو ال Type ورابع جزء وهو ال Level



- علشان نفهم ازاي ال SELinux بتعمل allow او deny لل access based علي ال context labels خلينا نشوف المثال ده لنفرض ان انا عندي server نازل عليه Apache webserver ونازل عليه كمان داتا بيز اسمها MariaDB وزي ماشوفنا ان اي process عندي او اي serves بيكون ليها context labels فلنفرض مثلا ان MariaDB ليها context label اسمها mysqld_t ودي بيكون ليها access علي ال files بتاعتها اللي بتبقي stored تحت /data/mysql وال context labels بتاعها اسمه mysqld_db_t طب لو جات البروسيس بتاعت ال mysql حاولت ت access ال files بتاعت ال apache اللي هي تحت /var/www/html ف هل فيه explicit rule عند ال SELinux انها مسموح ليها انها ت access ال files لا مفيش explicit rule عند ال SELinux ف ال access ده هيكون deny ونفس الكلام عند الاباتشي لو حد عمل compromise واخترق الاباتشي ويب سايت بتاعك ف ساعتها لو حاول انه ي access الداتا بيز الموجوده علي نفس السيرفر فساعتها ال SELinux هيعمله deny

- لو انا عايز أ List ال context labels الموجوده علي ال object بتاعتي سواء كان ال object ده process او service او file او directory بستخدم اوبشن upper case **Z** مع ps ax

```
[root@host ~]# ps axZ        لو انا عايز أ list كل process ال running عندي وأ list معاهم ال context labelالموجوده علي كل بروسيس
LABEL                                        PID TTY      STAT       TIME       COMMAND
system_u:system_r:init_t:s0                  1   ?        Ss         0:09       /usr/lib/systemd/...
system_u:system_r:kernel_t:s0                2   ?        S          0:00       [kthreadd]
system_u:system_r:kernel_t:s0                3   ?        S          0:00       [ksoftirqd/0]
...output omitted...
[root@host ~]# systemctl start httpd        لو عندي سيرفز زي الاباتشي وعايز اعرف ال label هستخدم ps -ZC httpd
[root@host ~]# ps -ZC httpd
LABEL                                        PID TTY      TIME       CMD
system_u:system_r:httpd_t:s0                 1608 ?       00:00:05   httpd
system_u:system_r:httpd_t:s0                 1609 ?       00:00:00   httpd
...output omitted...
[root@host ~]# ls -Z /home        لو عايز اعرض ال lables الموجوده علي ال directory
drwx------.        root      root      system_u:object_r:lost_found_t:s0 lost+found
drwx------.        student   student   unconfined_u:object_r:user_home_dir_t:s0 student
drwx------.        visitor   visitor   unconfined_u:object_r:user_home_dir_t:s0 visitor
[root@host ~]# ls -Z /var/www
drwxr-xr-x.        root      root      system_u:object_r:httpd_sys_script_exec_t:s0 cgi-bin
drwxr-xr-x.        root      root      system_u:object_r:httpd_sys_content_t:s0 error
drwxr-xr-x.        root      root      system_u:object_r:httpd_sys_content_t:s0 html
drwxr-xr-x.        root      root      system_u:object_r:httpd_sys_content_t:s0 icons
```

SELinux Modes

- **Enforcing mode**: In enforcing mode, SELinux enforces its policies and denies access to any actions or processes that violate those policies. When a violation is detected.
- **Permissive mode**: In permissive mode, SELinux logs any violations but does not enforce its policies. This mode is useful for testing and troubleshooting SELinux policies without affecting system security.
- **Disabled mode**: In disabled mode, SELinux is completely turned off and has no effect on the system.

Changing the current SELinux mode

- The SELinux subsystem provides tools to display and change modes. To determine the current SELinux mode, run the **getenforce** command. To set SELinux to a different mode, use the **setenforce** command:

- خلينا نتكلم عن ال SELinux وايه الفرق بينهم وازاي اسويتش مابين ال nodes وبعضها ال SELinux بيشتغل في 3 different modes

1- اول mode اسمه **Enforcing mode** وده يعتبر ال highest level of security ودي معناها ان ال SELinux بيبقي enable وبي enforce ال policies بمعني ان لو فيه اي access بي violated ال policy بتاعت ال SELinux ال SELinux هيعملها denyعلي طول

2- تاني Mode اسمه **permissive mode** وده شبه الenforcing mode شويه بمعني ان ال SELinux بتبقي enable بس الفرق الوحيد انه مش بي enforce ال policy بمعني انه مش هيعمل deny لأي access بي violated ال policy بتاعت ال SELinux وده بيستخدم في ال testing وال troubleshooting

3- اخر mode وهو ال **Disable Mode** وده معناه ان ال SELinux معمول ليه disable

CHANGING THE CURRENT SELINUX MODE

- انا لو عايز أ display او change ال current modes بتاعت ال SELinux فيه عندي Two command

1. **getenforce** ده بستخدمه علشان اعرض ال current mode بتاعي
2. **setenforce** ده بستخدمه لو انا عايز اسويتش مابين الmodes وبعضها

➢ خد بالك من حاجه لو انا عايز اسويتش من ال enforce ل ال permissive او العكس ده مبيحتجش اني اعمل reboot للسيستم الحاله الوحيده اللي بحتاج اني اعمل reboot لو انا عملت Disabled لل SELinux

➢ لو استخدمنا getenforce هنلاقيه قايلي ان ال current mode بتاعي هو Enforcing

```
[root@MohamedAtef ~]# getenforce
Enforcing
[root@MohamedAtef ~]#
```

➢ لو انا عايز اعرض معلومات اكتر عن ال status بتاعت ال SELinux بستخدم **sestatus**

```
[root@MohamedAtef ~]# sestatus
SELinux status:                 enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:             targeted
Current mode:                   enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:     actual (secure)
Max kernel policy version:      33
```

قالي هنا ان ال SELiuux enabled

ده بيكون stored جواه ال configuration file الخاص ب ال selinux

وهنا ان ال current mode بيكون enforcing

دي معناه ان لو عملت ريبوت للسيستم بتاعي السيستم هيقوم في ال enforcing mode

➢ لو انا عايز اسويتش من ال enforcing ل ال permissive mode لو انا قولتله setenforce هيعرضلي ال help بتاع ال command ده

```
[root@MohamedAtef ~]# setenforce
usage:  setenforce [ Enforcing | Permissive | 1 | 0 ]
```

➢ وبيقولي لو انت عايز تسويتش مابين ال modes وبعضها عندك two options ي اما تقوله **setenforce** وتقوله كلمه **permissive** وبعدين تضغط Enter او ممكن بدل permissive اكتبله **0** فيه حاله ال Permissiveو **1** في حاله ال **Enforcing**

```
[root@MohamedAtef ~]# setenforce permissive
[root@MohamedAtef ~]# getenforce
Permissive
[root@MohamedAtef ~]# setenforce 1
[root@MohamedAtef ~]# getenforce
Enforcing
```

➢ لو عايز اخلي ال mode يكون permanent هيكون عن طريق ال configuration file

```
[root@MohamedAtef ~]# vim /etc/selinux/config
```

لو انا فتحت ال file ده هلاقي فيه line اسمه SELINUX=enforcing لو انا عايز ال modeبتاعي مثلا permissive ويكون permanent هستخدم ال file ده وهكتب مكان ال enforcing اكتب permissive وهكذا بالنسبه للDisabled وخلي بالك وانت بتغير في ال file ده علشان لو كتبت اي حاجه غلط هيحصل مشكله عندك في السيستم والسيستم مش هيقوم

Initial SELinux Context

- On systems running SELinux, all processes and files are labeled. The label represents the security relevant information, known as the SELinux context.
- New files typically inherit their SELinux context from the parent directory, thus ensuring that they have the proper context.
- But this inheritance procedure can be undermined in two different ways. First, if you create a file in a different location from the ultimate intended location and then move the file, the file still has the SELinux context of the directory where it was created, not the destination directory. Second, if you copy a file preserving the SELinux context, as with the **cp -a** command, the SELinux context reflects the location of the original file.
- The following example demonstrates inheritance and its pitfalls. Consider these two files created in **/tmp**, one moved to **/var/www/html** and the second one copied to the same directory. Note the SELinux contexts on the files. The file that was moved to the **/var/www/html** directory retains the file context for the **/tmp** directory. The file that was copied to the **/var/www/html** directory inherited SELinux context from the **/var/www/html** directory.

TMOOCA MEDIA PRODUCTION

- **خلينا نتكلم عن ال Initial SELinux Context**
- زي ماقولنا قبل كده ان اي object موجود عندي في السيستم سواء كان file او directory او process او port بيكون ليه label
- وان اي new created file موجود عندي في السيستم بي inherit ال SELinux context بتاعت ال parent بتاعه لو جينا مثلا علي سبيل المثال دخلت تحت /var/www/html وعملت create ل file ف هتلاقيه بي inherit نفس ال context label بتاع الhtml directory ولو دخلت تحت /tmp وعملت create ل file او directory هتلاقيه بي inherit نفس ال context label بتاع ال tmp directory
- فيه هنا نقطه مهمه جدا لازم تخلي بالك منها ان لو انت جيت مثلا تحت /tmp وعملت create ل file معين وجيت نقلت ال file ده من /tmp و حطيته تحت /var/www/html باستخدام move command ف قالك ان ال move command بي maintain ال context label بتاع ال original file
- تاني حاجه لو جيت انقل ال file بال cp command ال cp command بي inherit ال context label بتاع ال destination
- ولو استخدمت ال cp -a ال command ده شبه ال mv انه بيحافظ علي ال context label بتاع ال original file
- علشان نفهم الكلام ده تعال ناخد مثال:-
- تعال نعمل install لل apache باستخدام dnf install httpd

```
[root@MohamedAtef ~]# dnf install httpd
```

- تاني خطوه ان انا اعمل enable و start للسيرفز دي

```
[root@MohamedAtef ~]# systemctl enable --now httpd
```

ال command ده بيعملي enable و start في نفس الوقت

- تالت خطوه انا عندي المسار ده /var/www/html ده بيكون ال default location بتاعك اللي بتحط فيه الويب سايت بتاعك تعال ندخل تحت /var/www/html/ ونعمل create ل fileاسمه مثلا index.html وخلي بالك الاسم ده مش حاجه عشوائيه لا هو هنا الاباتشي by default اول اما ت access الويب سايت بتاعك هو بيروح ي سيرش في ال default location علي file بالاسم ده لو لاقاه بيروح ي load ال web page الموجوده في ال index.html

```
[root@MohamedAtef ~]# cd /var/www/html/
[root@MohamedAtef html]# touch index.html
```

- لو جينا نفذنا ls -lZ index.html هنلاقي ال index.html واخد context label اسمه httpd_sys_content_t

```
[root@MohamedAtef html]# ls -lZ index.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 0 Jun 13 12:56 index.html
```

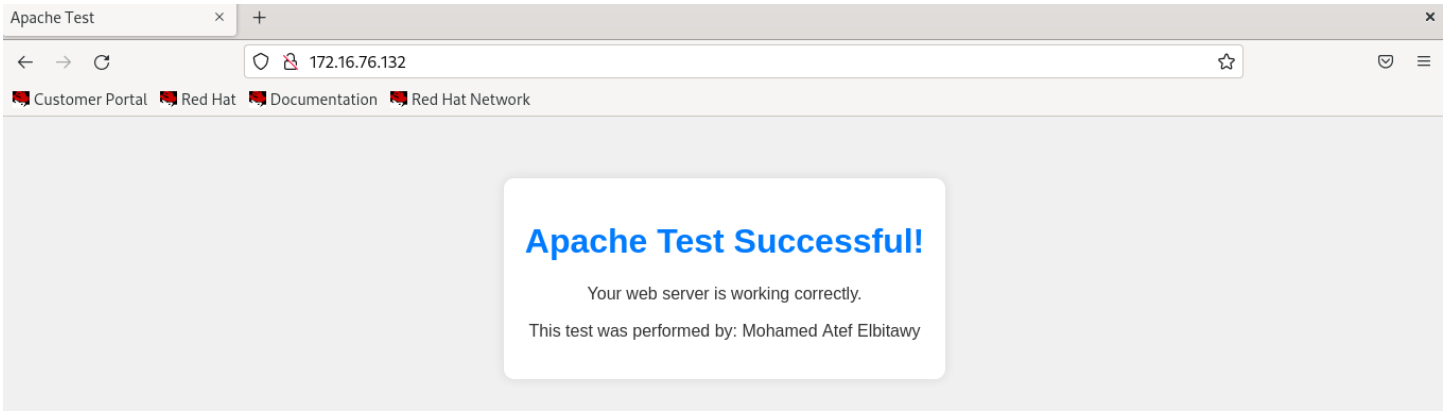
- ال context label ل ال file اللي اسمه index.html هو نفس ال context label بتاع ال parent لو عايزين نتاكد هنعمل ls -ldZ /var/www/html هنلاقيه نفس ال context label

```
[root@MohamedAtef html]# ls -ldZ /var/www/html/
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 24 Jun 13 12:56 /var/www/html/
```

- تعال بقي نفتح ال file اللي احنا عملناه ونحط فيه اي html code علشان بس ن access الويب سايت بتاعنا ف احنا هنكتب اي html code ف انا كتب مثلا

```
[root@MohamedAtef html]# vim index.html
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Apache Test</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f0f0f0;
            color: #333;
            text-align: center;
            padding: 50px;
        }
        .container {
            background-color: #fff;
            padding: 20px;
            border-radius: 10px;
            box-shadow: 0 0 10px rgba(0,0,0,0.1);
            display: inline-block;
        }
        h1 {
            color: #007bff;
        }
    </style>
</head>
<body>
    <div class="container">
        <h1>Apache Test Successful!</h1>
        <p>Your web server is working correctly.</p>
        <p>This test was performed by: Mohamed Atef Elbitawy</p>
    </div>
</body>
</html>
```

- بمجرد ان انت عملت install لل web server وعملت create لل html page بتاعتك تحت /var/www/html/ انت كده جاهز ان انت تعمل access للويب سايت بتاعك ف علشان ن access لازم نجيب ال ip الخاص بالسيرفر بتاعنا وبعد كده نفتح اي متصفح ونحط ال ip بتاعنا وبعدين Enter



- هنلاقيه هنا عمل access لل html page اللي احنا عملناهاا لو حصلت معاك اي مشكله ف لازم توقف ال firewall مؤقتاا
- تعال نجرب كذا حاجه ونشوف ال context label لو جينا عملنا create ل file1 و file2 و file3 وجيت عملت cp ل file1 تحت ال /var/www/html/ وعملت mv ل file2 تحت /var/www/html/ وعملت cp -a ل file3 تحت /var/www/html/

```
[root@MohamedAtef ~]# touch file1 file2 file3
[root@MohamedAtef ~]# cp file1 /var/www/html/ inherit
[root@MohamedAtef ~]# mv file2 /var/www/html/
[root@MohamedAtef ~]# cp -a file3 /var/www/html/
[root@MohamedAtef ~]# cd /var/www/html/
[root@MohamedAtef html]# ls -lZ
total 4
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0   0 Jun 13 13:58 file1
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0         0 Jun 13 13:58 file2
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0         0 Jun 13 13:58 file3
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 883 Jun 13 13:36 index.html
[root@MohamedAtef html]#
```

هنا زي ماقولنا ان ال cp بيخلي ال file ي inherit نفس ال label بتاع ال destination بتاع ال location الجديد

هنا زي ماقولنا ان ال mv بي maintain ال context label بتاع ال original file

هنا زي ماقولنا ان ال cp -a بي maintain ال context label بتاع ال original file

- تعال بقي نعمل cp ل index.html جوه ال file1 ,file2,file3

```
[root@MohamedAtef html]# cp index.html fiel1
[root@MohamedAtef html]# cp index.html fiel2
[root@MohamedAtef html]# cp index.html fiel3
```

- ف لو احنا عملنا access لل html page بتاعتنا عن طريق file1,file2,file3 وشوفنا مين اللي هيعمل access ومين لا . هفتح المتصفح واكتب ال ip وبعدين ال file1 زي مثلا 192.168.1.5/file1 هنلاقيه فتح معانا ال web page لان ال file1 عنده نفس ال context label الخاص بال index.html اما لو جربنا علي file2, file3 هيحصل مشكله عندي لان ال context label مختلف عن ال index.html

Changing The SELinux Context of a File

- Commands to change the SELinux context on files include **semanage fcontext**, **restorecon**, and **chcon**.
- The preferred method to set the SELinux context for a file is to declare the default labeling for a file using the **semanage fcontext** command and then applying that context to the file using the **restorecon** command. This ensures that the labeling will be as desired even after a complete relabeling of the file system.
- The **chcon** command changes SELinux contexts. **chcon** sets the security context on the file, stored in the file system. It is useful for testing and experimenting. However, it does not save context changes in the SELinux context database. When a **restorecon** command runs, changes made by the **chcon** command also do not survive. Also, if the entire file system is relabeled, the SELinux context for files changed using **chcon** are reverted.

- لو انا عايز أ change او أ modify ال context بتاع اي file او directory موجود عندي ف بيكون عندي three commands :-

1- اول command اسمه **semanage fcontext** بستخدمه علشان أ define او أ modify ال SELinux rules اللي بحدد بيها ال SELinux context بتاع اي file او directory وده بالمناسبه ال recommended command اللي بنستخدمه بالاخص لو انا عايز اغير اللي انا عملته يبقي permanent لان ال semanage بيروح يحفظ التغيرات اللي هو عملها في الداتابيز اللي في ال SELinux

2- تاني command اسمه **restorecon** وده بستخدمه علشان أ restore ال default context بتاع اي file او directory موجود عندي based علي ال rules الdefine عندي في SELinux database وده بستخدمه عادتا بعد ال semanage fcontext علشان نعمل apply لل context changes علي ال files بتاعتنا

3- تالت command اسمه **chcon** وده بستخدمه لو عايز اغير ال context بتاع اي file موجود عندي for tmp بس مش recommended اننا نستخدم ال command ده for long term solution لانه ببساطه مش بيحفظ الي هو عمله في الداتا بيز بستخدمه اكتر في ال Troubleshooting وال Testing

➢ لو انا عايز اغير ال context الخاص باي file هستخدم ال chcon وبعد كده **-t** علشان احددله ال context type بتاعي وبعد كده اديله ال context type اللي انا عايز اعمله apply علي ال file بتاعي وفي الاخر اديله اسم ال file

```
[root@MohamedAtef html]# ls -lZ
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0   0 Jun 13 13:58 file1
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0          0 Jun 13 13:58 file2

[root@MohamedAtef html]# chcon -t httpd_sys_content_t file2
[root@MohamedAtef html]# ls -lZ
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0   0 Jun 13 13:58 file1
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0   0 Jun 13 13:58 file2
```

هنا انا عايز اغير ال context type الخاص ب file2 اخليه نفس ال context type بتاع file1 ف انا عندي three command ف انا هستخدم ال chcon

- او ممكن استخدم ال restorecon وبعدين اسم ال file واحنا قولنا ال restorecon هيبص في الداتا بيز ويشوف هو ال file ده ال default context بتاعه ايه وي inherit ال context label بتاعه

```
[root@MohamedAtef html]# restorecon -v file3
Relabeled /var/www/html/file3 from unconfined_u:object_r:admin_home_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
```

استخدمت v- علشان بس اعرض الoutput علي الاسكرين

- ال SELinux عندها rules ان انت لو عملت create ل directory تحت / هياخد context اسمه default_t

```
[root@MohamedAtef ~]# ls -ldZ /virtual/
drwxr-xr-x. 2 root root unconfined_u:object_r:default_t:s0 6 Jun 13 21:46 /virtual/
```

Defining SELinux Default File Context Rules

- The following table is a reference for **semanage fcontext** options to add, remove or list SELinux file contexts.

OPTION	DESCRIPTION
-a, --add	Add a record of the specified object type
-d, --delete	Delete a record of the specified object type
-l, --list	List records of the specified object type

- To ensure that all files in a directory have the correct file context run the **semanage fcontext -l** followed by the **restorecon** command.

```
[root@host ~]# semanage fcontext -l
[root@host; ~]# restorecon -Rv /var/www/
```

- زي ماقولنا لو انا عايز اعمل add او modify او delete ويكون permanent هستخدم command اسمه semanage fcontext واديله اوبشن **-a** لو انا عايز اعمل add ل context rule و **-d** لو عايز امسح ال context rule و**-m** لو عايز اعدل في اي context rule و **-l** لو عايز اعمل list لكل ال context rules
- لازم بعد اما تعمل semanage fcontext تعمل run لل command ده **restorecon** علشان ت apply ال changes اللي انت عملتها علي ال file وال directory

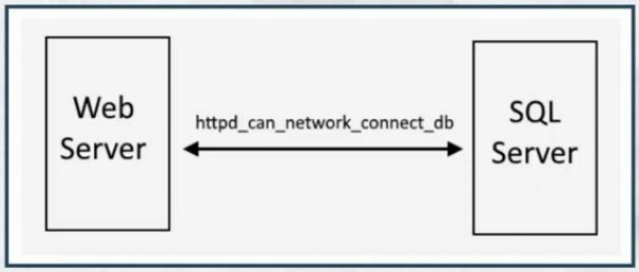
```
[root@host ~]# semanage fcontext -l
...output omitted...
/var/www(/.*)?          all files          system_u:object_r:httpd_sys_content_t:s0
```

انا عملت List لكل ال context rules فيه context كتير جدا بس احنا اختارنا ده

بيقولك هنا ان اي file او directory اتعمله create تحت /var/www/ هياخد ال context ده httpd_sys_content_t

SELinux Booleans

- SELinux booleans are switches that change the behavior of the SELinux policy. SELinux Booleans are rules that can be enabled or disabled. They can be used by security administrators to tune the policy to make selective adjustments.
- For example, let's say you have a Linux web server that will be using a SQL database, such as MySQL or MariaDB. One of the SELinux booleans is **httpd_can_network_connect_db**. If httpd_can_network_connect_db is off, the web server will be unable to connect to the SQL database. On the other hand, if httpd_can_network_connect_db is on, the web server will be able to connect to the SQL database.



- ال SELinux Boolean عباره عن switches بتت change ال behavior بتاعت ال SELinux policy بتاعتك بمعني ان ال SELinux عندها مجموعه من ال security features وكل feature بيكون ليها description وليها استخدام معين وممكن تعملها switch on وswitch off في ال run time علشان نفهم ال SELinux Booleans بتستخدم او بتعمل ايه تحديدا تعال نشوف المثال ده بيقولك ان for example لو عندك two servers سيرفر عامل عليه install ل web server وليكن apache web server وسيرفر تاني عامل عليه install ل اي داتابيزموجوده عندك سواء كان MySQL او MariaDB وعايز انت ال apache web server بتاعك ي reatch الداتابيز الموجوده علي سيرفر تاني من خلال النيتورك قالك في الحاله دي انت ممكن تبقي مظبط ال permissions وال SELinux علي السيرفر بتاع الاباتشي ونفس الكلام مع الداتا بيز لكن الاباتشي بتاعك مش قادر ي reatch الداتا بيز علي السيرفر التاني ده بيكون بسبب ان انا عندي SELinux Boolean اسمها httpd_can_network_connect_db دي by default بتكون switch off معناها ان الاباتشي ويب سيرفر بتاعك مش هيقدر انه يوصل للداتابيز بتاعتك عن طريق النيتورك علشان اخلي الاباتشي بتاعي يوصل للداتابيزمن خلال النيتورك لازم تعمل لل Boolean اللي اسمه httpd_can_network_connect_db تعمله enable او on

- Commands useful for managing SELinux booleans include **getsebool**, which lists booleans and their state, and **setsebool** which modifies booleans. **setsebool -P** modifies the SELinux policy to make the modification persistent. And **semanage boolean -l** reports on whether or not a boolean is persistent, along with a short description of the boolean.

- Non-privileged users can run the **getsebool** command, but you must be a superuser to run **semanage boolean -l** and **setsebool -P.**

```
[user@host ~]$ getsebool -a
[user@host ~]$ getsebool httpd_can_network_connect_db
httpd_can_network_connect_db --> off

[user@host ~]$ setsebool httpd_can_network_connect_db on
[user@host ~]$ semanage boolean -l | grep httpd_can_network_connect_db
httpd_can_network_connect_db   (on  ,  off)  Allow httpd to can network connect db
```

- علشان ن manage ال SELinux Booleans الموجوده عندنا انا عندي two command
1. Command اسمه getsebool ده بستخدمه علشان أ list بيه كل ال Booleans ال available عندي في السيستم وكمان بيعرضلي ال current state بتاعت كل واحده هل هي off او on
2. وعندي command تاني اسمه setsebool بستخدمه لو انا عايز switch ال state بتاعت اي Boolean عندي لو عايز ا switch on او off
- لو انا عايز التغير اللي عملته يكون permanent هستخدم مع ال setsebool اوبشن -P وال P هنا upper case
- وممكن استخدم semanage Boolean -l علشان ي list كل ال Booleans الموجوده عندي وبي list معاهم description عن كل Booleans

➢ تعال نعمل list لكل ال Booleans بال state بتاعتهم

```
[root@MohamedAtef ~]# getsebool -a
abrt_anon_write --> off
abrt_handle_event --> off
abrt_upload_watch_anon_write --> on
antivirus_can_scan_system --> off
```

➢ لو انا عارف ال Boolean وعايز اعرف ال state بتاعتها هل هي on ولا off هستخدم

```
[root@MohamedAtef ~]# getsebool httpd_can_network_connect_db
httpd_can_network_connect_db --> off
```

ممكن كمان اعمل grepعلي ال Boolean ده

```
[root@MohamedAtef ~]# getsebool -a | grep httpd_can_network_connect_db
httpd_can_network_connect_db --> off
```

فيه طريقه كمان ودي احسن طريقه علشان بيجبلك اسم ال Boolean بتاعك وبيجبلك descriptionعنه وجايبلك ال current state وال permanent state

```
[root@MohamedAtef ~]# semanage boolean -l | grep httpd_can_network_connect_db
httpd_can_network_connect_db      (off  ,  off)    Allow httpd to can network connect db
```

ده اسم ال Boolean — ده ال current state — ده ال permanent — ده ال description

➢ لو انا عايز اعمل switch او on او off ل Boolean معين هستخدم

```
[root@MohamedAtef ~]# semanage boolean -l | grep httpd_can_network_connect_db
httpd_can_network_connect_db        (off  ,  off)    Allow httpd to can network connect db
```

انا هنا لو عايز اسويتش لل boolean ده واعمله enable بمنتهي البساطه هقوله setsebool httpd_can_network_connect_db on

```
[root@MohamedAtef ~]# setsebool httpd_can_network_connect_db on
[root@MohamedAtef ~]# semanage boolean -l | grep httpd_can_network_connect_db
httpd_can_network_connect_db   (on   ,  off)  Allow httpd to can network connect db
```

هنلاقي هنا current state بقت on

هنلاقي هنا permanent state لسه off

لو انا عايز اغير ال permanent state بدل اما هي off اخليها on هزود P- ويكون upper case

```
[root@MohamedAtef ~]# setsebool httpd_can_network_connect_db  on  -P
[root@MohamedAtef ~]# semanage boolean -l | grep httpd_can_network_connect_db
httpd_can_network_connect_db   (on   ,   on)  Allow httpd to can network connect db
```

P- هنا علشان اخليه permanent

هنلاقي هنا current state بقت on

هنلاقي هنا permanent state بقت on

Troubleshooting SELinux Issues

- It is important to understand what actions you must take when SELinux prevents access to files on a server that you know should be accessible.
- Install the setroubleshoot-server package to send SELinux messages to **/var/log/messages.** **setroubleshoot-server** listens for audit messages in **/var/log/audit/audit.log** and sends a short summary **to /var/log/messages**. This summary includes unique identifiers (*UUID*) for SELinux violations that can be used to gather further information. The **sealert -l *UUID*** command is used to produce a report for a specific incident.
- Use **sealert -a /var/log/audit/audit.log** to produce reports for all incidents in that file.

```
[root@host ~]# ausearch -m AVC -ts recent
```

- مهم جدا تكون فاهم ال SELinux بيشتغل ازاي وتقدر ت troubleshooting لو فيه عندك اي مشكله SELinux وتقدر تاخد ال actions المظبوط بحيث انك ت fix المشكله دي .بالاخص المشاكل اللي دايما بنواجهاا بتبقي في الغالب incorrect context name موجوده علي ال file بتاعك وده غالبا بسبب انك عملت create ل file في location وجيت تنقله في location تاني ف استخدمت ال mv command وزي ماشوفنا قبل كده ال mv بي maintain ال original context بتاع ال file بتاعك فساعتها بيبقي انت محتاج علشان تحل المشكله ف لازم تظبط ال context label الموجود علي ال file بتاعك باستخدام اي command زي ماشوفنا قبل كده سواء كان chcon او restorcon وهكذا
- عندنا مجموعه من ال command line tools اللي بنستخدمهم علشان يساعدونا في ال Troubleshooting بتاع ال SELinux

➢ اول حاجه عندنا package اسمها **setroubleshoot-server** ودي بتكون Install by default دي وظيفتها انها بت audit ال audit.log بتاعك وت send a short summary عن ال violation اللي حصلت في /var/log/messages . طب ال summary ده بيكون فيه ايه بيكون فيه حاجه اسمها unique identifiers(UUID) عن كل violation عندي

➢ تقدر عن طريق الل UUID تستخدم command تاني اسمه **sealert -l** زي ماهنشوف مع بعض في ال CLI هتقوله **sealer -l** وتديله ال UUID علشان تشوف معلومات اكتر

➢ لو انا عايز تفاصيل اكتر عن كل المشاكل اللي حصلت عندي وكل ال reports الموجوده في audit.logهقوله **sealert -a /var/log/audit/audit.log**

➢ وفيه command تاني اسمه **ausearch -m AVC -ts recent** بستخدمه لو عايز اسيرش بيه علي الmessages اللي type بتاعها AVC او Access vector cache جوه ال audit.log file ال ts معناها timestamp و ال recent معناها انه هيروح يسيرش في ال audit.log علي اي massages ال type بتاعها AVC حصلت اخر 10 دقائق

- هنعمل install ل **setroubleshoot-server**

```
[root@MohamedAtef ~]# yum install setroubleshoot.x86_64
Installed:
```

- اللي احنا هنعمله هنعمل create ل file معين وبعدين هننقل ال file ده تحت الويب سيرفر اللي هو ال apache علشان نعمل access عليه من علي اي متصفح وبعدين هنشوف المشاكل اللي هتقابلنا و هنشوف كل الطرق اللي ممكن نستخدمها علشان نفهم سبب المشاكل دي ايه وحلها

- تعال نعمل create ل file اسمه myweb ونشوف ال context بتاعه

```
[root@MohamedAtef ~]# touch myweb
[root@MohamedAtef ~]# ls -lZ myweb
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 0 Jun 14 17:15 myweb
```

هنلاقيه واخد context اسمه admin_home_t

- هنعمل move ل myweb تحت /var/www/html/ ونشوف ال context بتاعه بعد اما عملنا ليه mv

```
[root@MohamedAtef ~]# mv myweb /var/www/html/
[root@MohamedAtef ~]# ls -lZ /var/www/html/myweb
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0 0 Jun 14 17:15 /var/www/html/myweb
```

هنلاقيه واخد نفس ال original context

- لو انا دلوقتي دخلت علي المتصفح وحاولت اني access علي ال file ده هيحصل مشكله و هيقولك forbidden او permissions deny
- فيه عندي command ظريف ممكن نستخدمه علشان اعمل http request عن طريق ال CLI بدل اما افتح المتصفح ال command اسمه **curl** وبعد كده تديله ال URL

```
[root@MohamedAtef ~]# curl  http://localhost/myweb
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
</head><body>
<h1>Forbidden</h1>
<p>You don't have permission to access this resource.</p>
</body></html>
```

انا هنا ممكن استخدم بدل ال localhost استخدم ال IP بتاعي

هنلاقيه هنا ظهرلي نفس ال output اللي علي المتصفح وهنلاقيه هنا ظهرلي error وبيقولك ان معندكش اي صلاحيه انك تعمل access علي ال file ده او الموقع محجوب ليه المشكله دي ظهرتلي علشان زي ماقولنا قبل كده ان ال context الخاص بال file مختلف عن ال context الخاص بال destination

- لو انا عايز اعرض معلومات عن المشكله اللي ظهرت ليا وانا بحاول اني ا access الfile علي المتصفح وازاي اعرف احل المشكله اللي حصلت وكمان لو انا عايز اعرف ال unique identifiers(UUID) فيه عندي كذا طريقه

1- اول طريقه اني افتح ال audit.log وده بيكون تحت /var/log/audit/

```
[root@MohamedAtef ~]#  tail /var/log/audit/audit.log
type=AVC msg=audit(1718381478.473:227): avc:  denied  { getattr } for  pid=1687 comm="httpd" path="/var/www/html/myweb"
dev="nvme0n1p2" ino=886109 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:admin_home_t:s0
tclass=file permissive=0
type=SYSCALL msg=audit(1718381478.473:227): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c a1=7f6c2803b7d8
a2=7f6c2dbf78b0 a3=0 items=0 ppid=1153 pid=1687 auid=4294967295 uid=48 gid=48 euid=48 suid=48 fsuid=48 egid=48 sgid=48
fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd" subj=system_u:system_r:httpd_t:s0
key=(null)ARCH=x86_64 SYSCALL=newfstatat AUID="unset" UID="apache" GID="apache" EUID="apache" SUID="apache"
FSUID="apache" EGID="apache" SGID="apache" FSGID="apache"
type=PROCTITLE msg=audit(1718381478.473:227): proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=AVC msg=audit(1718381478.476:228): avc:  denied  { getattr } for  pid=1687 comm="httpd" path="/var/www/html/myweb"
dev="nvme0n1p2" ino=886109 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:admin_home_t:s0
```

قالك هنا ان الsuccess=no معناها ان ال selinux منع الaccess

وجايبلك ال context label الخاص بال file

➢ تاني طريقه اني افتح ال file الخاص ب messages وده بيكون تحت /var/log/

```
[root@MohamedAtef ~]# tail /var/log/messages
Jun 14 18:29:02 MohamedAtef setroubleshoot[3135]: failed to retrieve rpm info for path '/var/www/html/myweb':
Jun 14 18:29:02 MohamedAtef systemd[1]: Started dbus-:1.4org.fedoraproject.SetroubleshootPrivileged@3.service.
Jun 14 18:29:04 MohamedAtef setroubleshoot[3135]: SELinux is preventing /usr/sbin/httpd from getattr access on
the file /var/www/html/myweb. For complete SELinux messages run: sealert -l b9229b89-3c0f-48ff-8d83-
aa602526b753
Jun 14 18:29:04 MohamedAtef setroubleshoot[3135]: SELinux is preventing /usr/sbin/httpd from getattr access on
the file /var/www/html/myweb.#012#012*****  Plugin restorecon (99.5 confidence) suggests
************************#012#012If you want to fix the label. #012/var/www/html/myweb default label should be
httpd_sys_content_t.#012Then you can run restorecon. The access attempt may have been stopped due to
insufficient permissions to access a parent directory in which case try to change the following command
accordingly.#012Do#012# /sbin/restorecon -v /var/www/html/myweb#012#012*****
```

بيقولك هنا لو انت عايز تجيب تفاصيل اكتر عن المشكله بتاعتك اعمل run لل command ده
SELinux messages run: sealert -l b9229b89-3c0f-48ff-8d83-aa602526b753

ده ال UUID

➢ هنفذ ال command ونشوف التفاصيل اللي هيعرضها

```
[root@MohamedAtef ~]# sealert -l b9229b89-3c0f-48ff-8d83-aa602526b753
SELinux is preventing /usr/sbin/httpd from getattr access on the file /var/www/html/myweb.
*****  Plugin restorecon (99.5 confidence) suggests   ************************

If you want to fix the label.
/var/www/html/myweb default label should be httpd_sys_content_t.
Then you can run restorecon. The access attempt may have been stopped due to insufficient permissions to access a parent
directory in which case try to change the following command accordingly.
Do
# /sbin/restorecon -v /var/www/html/myweb

allow this access for now by executing:
# ausearch -c 'httpd' --raw | audit2allow -M my-httpd
# semodule -X 300 -i my-httpd.pp

Additional Information:
Source Context                system_u:system_r:httpd_t:s0
Target Context                unconfined_u:object_r:admin_home_t:s0
Target Objects                /var/www/html/myweb [ file ]
Source                        httpd
Source Path                   /usr/sbin/httpd
Port                          <Unknown>
Host                          MohamedAtef
Source RPM Packages           httpd-core-2.4.53-11.el9_2.4.x86_64
Target RPM Packages
SELinux Policy RPM            selinux-policy-targeted-38.1.11-2.el9_2.noarch
Local Policy RPM              selinux-policy-targeted-38.1.11-2.el9_2.noarch
Selinux Enabled               True
Policy Type                   targeted
Enforcing Mode                Enforcing
Host Name                     MohamedAtef
Platform                      Linux MohamedAtef 5.14.0-284.11.1.el9_2.x86_64 #1
                              SMP PREEMPT_DYNAMIC Wed Apr 12 10:45:03 EDT 2023
                              x86_64 x86_64
Alert Count                   8
First Seen                    2024-06-14 17:38:04 EET
Last Seen                     2024-06-14 18:44:05 EET
Local ID                      b9229b89-3c0f-48ff-8d83-aa602526b753
```

اول description عندك بيقولك ان ال SELinux منعت ال /usr/sbin/httpd من انه ي access علي ال file ده /var/www/html/myweb/

ده ال source context الخاص بالسيرفز اللي بتحاول ت access ال resource بتاعك
السيرفز اللي ال context label بتاعها httpd_t بتحاول ت access ال target context بتاع ال fileاللي اسمه myweb اللي ال target context بتاعه اسمه admin_home_t

ده ال Object بتاعي

دي ال service

وجايبلي كمان ال source path الخاص ب ال service

وجايبيلي ال hostname الخاص بالسيرفر بتاعي

وهنا بيقولي هل ال SELinux معمول ليه enable ولا لا

- وممكن كمان اقوله روح اعمل سيرش علي اي messages ال type بتاعها AVC حصلت اخر 10 دقائق

جايبلي نفس ال output الموجود في ال audit.log file

```
[root@MohamedAtef ~]# ausearch -m AVC -ts recent
----
time->Fri Jun 14 19:43:25 2024
type=PROCTITLE msg=audit(1718387005.242:270):
proctitle=2F7573722F7362696E2F6874747064002D44464F524547524F554E44
type=SYSCALL msg=audit(1718387005.242:270): arch=c000003e syscall=262 success=no exit=-13 a0=ffffff9c
a1=7f6c28045828 a2=7f6c2d3f68b0 a3=0 items=0 ppid=1153 pid=1687 auid=4294967295 uid=48 gid=48 euid=48
suid=48 fsuid=48 egid=48 sgid=48 fsgid=48 tty=(none) ses=4294967295 comm="httpd" exe="/usr/sbin/httpd"
subj=system_u:system_r:httpd_t:s0 key=(null)
type=AVC msg=audit(1718387005.242:270): avc:  denied  { getattr } for  pid=1687 comm="httpd"
path="/var/www/html/myweb" dev="nvme0n1p2" ino=886109 scontext=system_u:system_r:httpd_t:s0
tcontext=unconfined_u:object_r:admin_home_t:s0 tclass=file permissive=0
```

- فيه طريقه كمان ان انا اروح اقوله **sealert -a** وبعدين اسم ال log file ف ال sealeart هيروح يسيرش علي كل ال violation اللي حصلت في ال file اللي اسمه audit.log ويجبلك معلومات عنها ويجبلك report عن كل violation حصل في ال file ده

```
[root@MohamedAtef ~]# sealert -a /var/log/audit/audit.log
```

- كده احنا عرفنا كل الطرق اللي ممكن نستخدمها علشان نت troubleshooting بيها المشكله دي
- ف احنا زي معرفنا ان سبب المشكله اللي معرفتش من خلالها اني أعمل Access لل file ان ال context label كان مختلف ف انا هعمل **restorecon** لل myweb علشان ياخد نفس ال context الخاص ب html

```
[root@MohamedAtef ~]# cd /var/www/html/
[root@MohamedAtef html]# ls -lZ
total 16
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 883 Jun 13 13:36 index.html
-rw-r--r--. 1 root root unconfined_u:object_r:admin_home_t:s0         0 Jun 14 17:15 myweb

[root@MohamedAtef html]# restorecon -v myweb
Relabeled /var/www/html/myweb from unconfined_u:object_r:admin_home_t:s0 to
unconfined_u:object_r:httpd_sys_content_t:s0
[root@MohamedAtef html]# ls -lZ
total 16
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 883 Jun 13 13:36 index.html
-rw-r--r--. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0   0 Jun 14 17:15 myweb
[root@MohamedAtef html]#
```

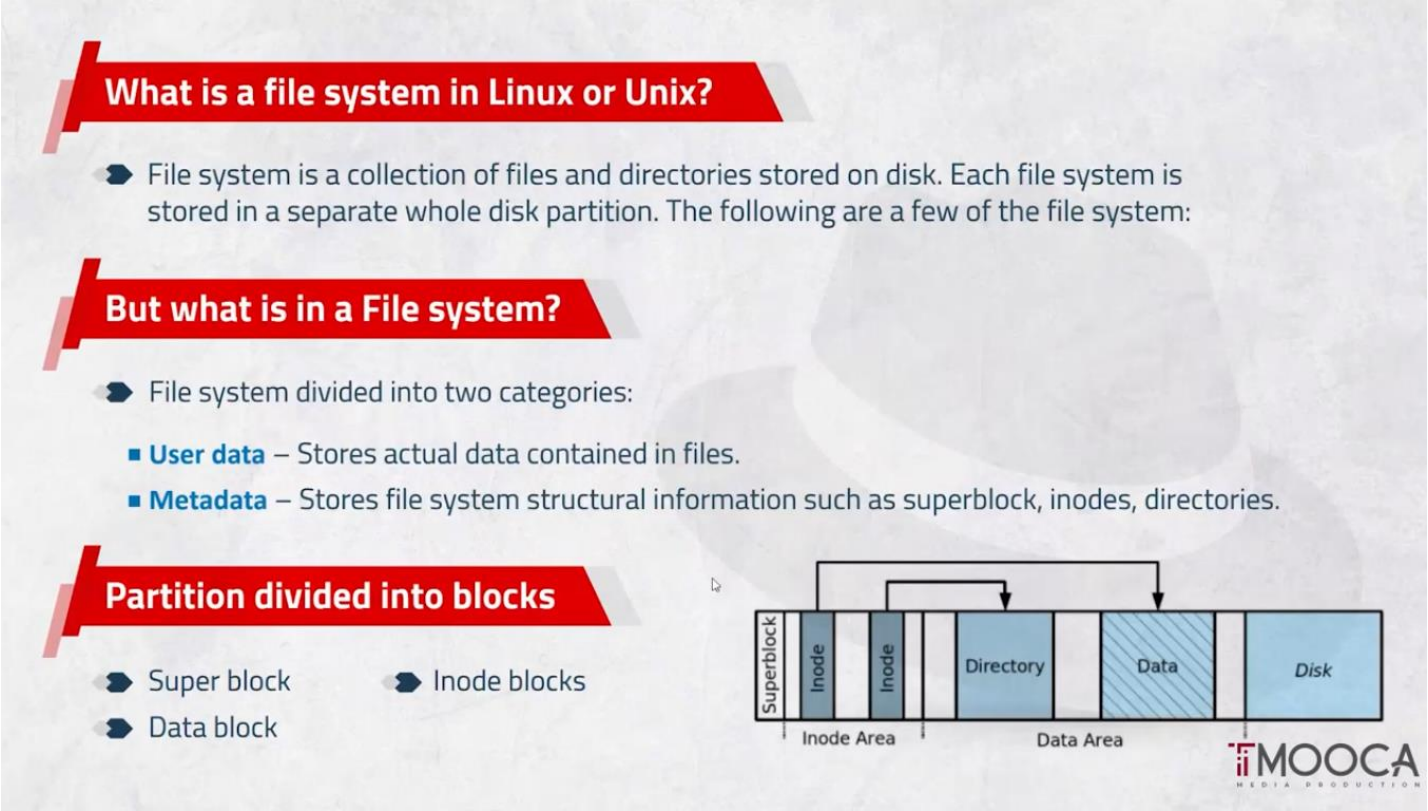
- **فيه عندي طريقه تانيه اقدر اني أ manage بيها ال SELinux issues من خلال ال cockpit web interface ف يفضل مشاهده الفيديو الخاص بيها علي مهاره تك**

Chapter 6
Manage Storage Stack

- خلينا الاول قبل ما نشوف ازاي ن manage ال Storage نعرف يعني ايه File Systems في اللينكس

➢ مبدئيا ال file system في اللينكس هي المسئوله انها ت manage وت organize الداتا الموجوده عندي علي ال storage devices بتاعتي وال storage devices فيه منها انواع كتيره فيه عندي مثلا HDD و SSD و NVMe وفيه انواع تانيه

➢ انا عندي لينكس بي support مجموعه من ال File Systems المختلفه وكل نوع منهم بيبقي ليه ال characteristic وال use cases بتاعته عندي مثلا نوع اسمه ext3 و ext4 و xfs و NTFS و FAT و exFAT وNFS



خلينا كده نتخيل لو عندنا بارتشن والبارتشن ده عملته فورمات بأي file system موجود عندي وليكن مثلا XFS file system لو جينا بصينا جوه البارتشن او ال file system بتاعنا هنلاقيه مقسوم ليه two categories

1- User data ودي بيكون stored جواها ال actual dataالموجوده في ال files بتاعتك زي مثلا ال textوال videoوال image وال application data وهكذا ودي كلها بتكون stored في ال Data Area

2- Metadata دي بيكون stored جواها information عن ال file system وال files بتاعتك زي مثلا ال Superblock وال inodes

What is Superblock?

- Each file system is different, and they have type like ext2, ext3 etc.
- Further each file system has size like 5 GB, 10 GB and status such as mount status. In short, each file system has a superblock, which contains information about file system such as:
  - File system type
  - Status
  - Size
  - Information about other metadata structures

- ال super block وده عباره عن block بيكون allocated في بدايه ال file system او بدايه ال partition وده بيكون stored جواه information عن ال file system زي مثلا ال file system type وال size وال status وهكذا

What is Inodes?

- **Metadata about the files**
  - File type (executable, block special etc)
  - Permissions (read, write etc)
  - Owner
  - Group
  - File size
  - File access, change and modification time
  - Number of links (soft/hard)
  - Access Control List (ACLs)

- ال Inode blocks ده عباره عن table او database بيبقي stored جواها معلومات عن الfiles وال directories و ال permissions وال file size وهكذا

Partitioning a Disk

- Disk partitioning allows system administrators to divide a hard drive into multiple logical storage units, referred to as partitions. By separating a disk into partitions, system administrators can use different partitions to perform different functions.
- **For example, disk partitioning is necessary or beneficial in these situations:**
  - Limit available space to applications or users.
  - Separate operating system and program files from user files.
  - Create a separate area for memory swapping.
  - Limit disk space use to improve the performance of diagnostic tools and backup imaging.

- خلينا نتكلم عن ال partitioning وال benefits بتاعته مبدئيا ال partitioning بيسمح للسيستم ادمن انهم يقسسموا ال disk لمجموعه من ال logical section بنقول عليها partitions وكل partition بيبقي ليه ال benefits بتاعته يعني من الاخر البارتشن ده حاجه logical مش physical والبارتشن ليه مجموعه من المميزات زي
  - ال data organization انه بيسمحلك انك ت organize ال data بتاعتك بطريقه efficient وت isolate ال operating system وال program files عن ال user files
  - تاني ميزه انه بيسملك انك ت limit ال space بتاعت ال application وال users
  - تالت ميزه وهي ال isolation ان لو عندك مثلا partition corrupted او running out of space ده مش هيأثر علي البارتشن التانيه وده بيخلي السيستم بتاعي more stable
  - وكمان ان البارتشن بيسمحلي اني اعمل create ل dedicated partition ل ال swap memory وده طبعا بي improve ال memory management

MBR Partitioning Scheme

- Since 1982, the Master Boot Record *(MBR)* partitioning scheme has dictated how disks are partitioned on systems. This scheme supports a maximum of **four primary partitions**. On Linux systems, with the use of extended and logical partitions, administrators can create a maximum of **15 partitions**. Because partition size data is stored as **32-bit values**, disks partitioned with the MBR scheme have a maximum disk and partition size of **2 TiB**.

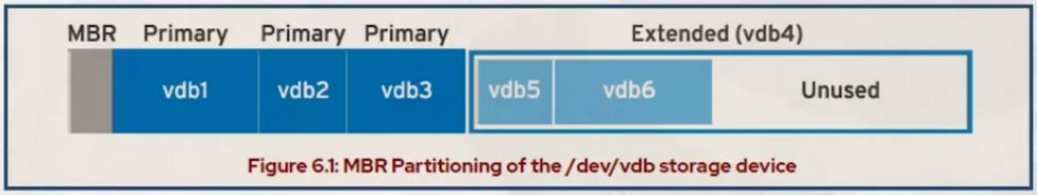


Figure 6.1: MBR Partitioning of the /dev/vdb storage device

- The **2 TiB disk** and partition size limit of the MBR partitioning scheme is no longer a theoretical limit but rather a real-world problem that system administrators encounter more and more frequently in production environments. As a result, the legacy **MBR scheme** is in the process of being superseded by the new ***GUID Partition Table (GPT)*** for disk partitioning.

MOOCA MEDIA PRODUCTION

- هنتكلم عن انواع ال partitioning scheme الموجوده عندنا في اللينكس مبدئيا ال partitioning scheme هي الطريقه اللي بستخدمها علشان اقسم ال storage device لمجموعه من ال logical partition عندنا نوعين نوع اسمه **MBR** ونوع تاني اسمه **GPT**

1- اول نوع هنتكلم عنه وهو ال **Master Boot Record(MBR)** النوع ده موجود من سنه ال 1982 ومستخدم لحد دلوقتي بس النوع ده فيه بعض ال limitations الموجوده فيه زي ان ال MBR بيسمحلك انك ت create لحد 4 primary partition بس بيكون متقسم ل 3 primary و 1 extended مقدرش اني اعمل create ل اكتر من extended واحد فقط وال extended اقدر اقسمه ل اكتر من partition بنسميهم logical partitions اقدر اقسم ال extended ل 63 logical partition واقصي مساحه في ال MBR هي 2 TiB

- لو جينا بصينا هنلاقي section موجود عندنا اسمه MBR ال MBR ده بيكون allocated في اول sector في ال Disk ال size بتاعه بيكون 512 byte وده بيكون متقسم ل 3 اجزاء
- اول جزء بيكون عباره عن 446 byte بيبقي stored جواهم حاجه اسمها Bootstrap code ووظيفته انه بيروح ي load ال boot loader اللي بيقوم ال operating system
- تاني جزء بيكون عباره عن 64 byte وده بيكون جواه information عن ال partitions اللي اتعملها create في ال disk زي ال size وال type وال status
- تالت جزء بيكون عباره عن 2 byte ده بيكون جوه حاجه اسمها magic number وده بيكون عباره عن number hexadecimal ال bios بيستخدمه علشان ي confirm هل ال MBR بتعاك valid ولا corrupted

GPT Partitioning Scheme

- A GPT provides a maximum of **128 partitions**. Unlike an MBR, which uses 32 bits for storing logical block addresses and size information, a GPT allocates **64 bits** for logical block addresses.
- Allows a GPT to accommodate partitions and disks of up to eight zebibytes (ZiB) or eight billion tebibytes.
- In addition to addressing the limitations of the MBR partitioning scheme, a GPT also offers some additional features and benefits. A GPT uses a ***globally unique identifier (GUID)*** to identify each disk and partition. In contrast to an MBR, which has a single point of failure, a GPT offers redundancy of its partition table information. The primary GPT resides at the head of the disk, while a backup copy, the secondary GPT, is housed at the end of the disk. A GPT uses a checksum to detect errors and corruptions in the GPT header and partition table.

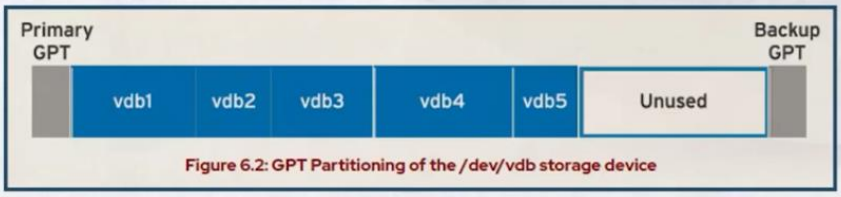


Figure 6.2: GPT Partitioning of the /dev/vdb storage device

- ال **GUID Partition Table(GPT)** النوع ده احدث من ال MBR وكمان بيحل كل مشاكل الlimitations اللي موجوده في ال MBR زي ان ال GPT بيسمحلك انك ت create up to 128 partitions علي عكس ال MBR وكمان بيسمحلي اني اعمل create ل partition ال size بتاعه بيوصل ل eight zebibytes
- فيه عندي redundancy علي مستوي ال GPT لو جينا بصينا علي ال Disk هنلاقي ال GPT موجود في بدايه ال Disk وبيبقي اسمها Primary GPT وفيه copy منه في نهايه ال Disk وبيكون اسمها Backup GPT لو ال GPT لأي سبب بقي corrupted تقدر بمنتهي السهوله انك ت restore ال GPT بتاعك من ال Backup GPT اللي بيكون موجود في نهايه ال Disk

Managing Partitions With Parted

- Partition editors are programs which allow administrators to make changes to a disk's partitions, such as creating partitions, deleting partitions, and changing partition types. To perform these operations, administrators can use the Parted partition editor for both the MBR and the GPT partitioning scheme.
- The **parted** command takes the device name of the whole disk as the first argument and one or more subcommands. The following example uses the **print** subcommand to display the partition table on the **/dev/vda** disk.

```
[root@host ~]# parted /dev/nvme0n1 print
```

- If you do not provide a subcommand, **parted** opens an interactive session for issuing commands.

```
[root@host ~]# parted /dev/nvme0n1
```

MOOCA MEDIA PRODUCTION

- انا عندي في red hat 9 مجموعه من ال command line tools اللي اقدر استخدمها علشان أ manage بيها البارتيشن الموجوده عندي سواء عايز أعمل creating partitions او deleting partitions او changing partition types ف انا عندي مجموعه من ال commands اهمهم اللي احنا هنركز عليه في الشابتر ده command اسمه **Parted** وهنشوف ال steps بتاعته ازاي نcreate new partition مره باستخدام ال MBR Partitioning Scheme ومره باستخدام ال GPT Partitioning Scheme
- علي قد ما Parted command سهل جدا و very straight forward في التعامل معاه الا ان في Point مهمه جدا تاخد بالك منها وانت شغال بال Parted command ان اي تغير بتعمله بال parted بيديك effect immediately فخد بالك وانت شغال لان اي خطأ ممكن تعمله ممكن يسبب انك تفقد الداتا بتاعتك كلها
- ال Syntax الخاص بال Parted انا عندي two option

1- اول طريقه ممكن اقوله parted واديله اسم ال Partition اللي انا عايز اعمل عليه operation معين وبعد كده اديله ال sub command اللي انا عايز اعمل عليها execute

- اول subcommand معانا اسمه Print وده just انه بي Print ال Partition اللي موجود في ال Disk

```
[root@MohamedAtef ~]# parted /dev/nvme0n1 print
```

- تاني طريقه بتكون interactive ان انا اقوله Parted وبعد كده اديله اسم ال Disk بتاعي واضغط Enter ساعتها هيفتحلي interactive session مع ال Parted Command اقدر من خلالها اني انفذ مجموعه من ال subcommands سواء عايز امسح بارتشن او انشئ بارتشن

```
[root@MohamedAtef ~]# parted /dev/nvme0n1
```

By default, **parted** displays all the sizes in powers of 10 (KB, MB, GB).
You can change that default with the **unit** subcommand which accepts the following parameters:

- **s** for sector
- **B** for byte
- **MB**, **GB**, or **TB** (powers of 10)

```
[root@host ~]# parted /dev/nvme0n1 unit s print
[root@host ~]# parted /dev/nvme0n1 unit B print
[root@host ~]# parted /dev/nvme0n1 unit MB print
[root@host ~]# parted /dev/nvme0n1 unit GB print
[root@host ~]# parted /dev/nvme0n1 unit TB print
```

- انا عندي by default ال print subcommand بي display ال sizes بتاع ال partition بال KB,MB,GB
- عندي subcommand تاني اسمه Unit بستخدمه لو انا عايز أ display ال Size بتاعت ال Partition ب Unit معينه زي مثلا لو عايزاعرض عدد ال Sector ف هقولها S ودي بتعبر عن ال Sector وال sector الواحد بيساوي 512 byte او ممكن اقوله B ودي بتعبر عن ال byte وهكذا

Writing the Partition Table on a New Desk

- اول step هعملها لو انا عندي new drive وعاوز اعملها partitioning لازم اول حاجه احدد حاجه اسمها ال disk labelاو ال Partitioning scheme واحنا عندنا Two Partitioning scheme وهما ال MBR والGPT
- انا علشان أ Select ال Partitioning scheme اللي انا هستخدمها بقوله Parted وبعدين اسم ال Disk وفيه عندي Subcommand اسمه mklabel وعندي two option لو انا عايز اشتغل MBR اوGPT

- لو هشتغل بال MBR هستخدم mklabel msdos

```
[root@server~]# parted /dev/nvme0n1 mklabel msdos
```

- ولو هشتغل GPT هستخدم mklabel gpt

```
[root@server~]# parted /dev/nvme0n1 mklabel gpt
```

- فيه ملاحظه مهمه جدا ان اول اما بتنفذ ال mklabel ده بيروح يمسح كل ال Partitions الموجوده في ال Disk ده .ف ال command ده احنا بنستخدمه مره واحده بس سواء انت عندك new hard drive وعاوز تبدأ تعمله Partitioning او عندك disk قديم فيه Partition وانت عايز ت reuse ال Disk ده ومش محتاج ال data اللي موجوده او ال Partition اللي جواه ف ساعتها اول اما انت بتختار ال Partitioning scheme اللي انت هتشتغل بيها هو بيروح يعمل Format لل Disk ده

➢ Create MBR Partitions

- علشان اعمل create ل new partition باستخدام ال MBR

1- اول step هقوله **parted** وبعدين اسم ال disk اللي انا عايز اعمله partitioning وبعدين اضغط Enter في الحاله دي هيفتحلي interactive session

```
[root@server~]# parted /dev/vdb
```

2- ال command اللي احنا هنستخدمه علشان ن Create بارتشن جديد اسمه **mkpart** ف انا هكتب ال command وبعدين اضغطEnter

- اول سؤال هيسألهولي في حاله ال MBR هيقولك حددلي ال partition type بتاعك انت عايزه primary ولا extended

```
(Parted) mkpart
Partition type? Primary/extended? Primary
```

3- تالت step هيقولك حددلي ال File system type اللي انت هتستخدمه علي ال Partition بتاعك انت هتستخدم مثلا xfs او ext4 براحتك . خلي بالك ال step دي هو مش هيروح يعمل create لل File system ده بس بي indicate ال File system اللي انت هتستخدمه بس هنعرف قدام شويه ايه ال command اللي هنستخدمه علشان نعمل create لFile system

```
File system type? [ext2]? xfs
```

- لو انا عايز اعرض كل File Systems الموجوده عندي هستخدم ال Command ده

```
[root@server~]# parted /dev/vdb help mkpart
```

4- رابع step ان انت هتحددله ال start وال End بتاعتك ان انت عايز ال size بتاع البارتشن ده بيبدأ منين وينتهي فين

```
Start? 2048s
```

5- بعد كده بحددله ال End بتاعتي انا هنا محددله لحد 1000 ميجا يعني 1 جيجا

```
End? 1000MB
```

6- لو انت خلصت وعايز تعمل Exit هتستخدم ال command ده quit

```
(parted) quit
Information: You may need to update /etc/fstab
```

7- ال command ده انا بستخدمه لو انا لاقيت ال partition اللي انا عملتله create لسه مش ظاهر تحت /dev ممكن تنفذ ال commandده **udevadm settle** ال command ده بيستني السيستم بتاعك لحد اما ي detect ال new partition وبعد كده بي return

```
[root@server~]# udevadm settle
```

في عندي طريقه بس مش interactive علشان اعمل MBR Partitions

- هقوله **parted** وبعدين اسم ال Disk اللي انا عايز اعمله Partitioning وبعدين ال subcommand ف انا عايز اعمل create ل new partition فهستخدم **mkpart** وبعد كده هحددله ال partition type ي اما primary او extended وبعد كده هحددله ال file system type وليكن في الحاله دي xfs وبعد كده بحددله ال start وال End

```
[root@server~]# parted /dev/vdb mkpart primary xfs 2048s 1000MB
```

Create GPT Partitions

1- نفس الكلام بالظبط لو انا عايز اعمل create ل new partitioning باستخدام ال GPT هيبقي هي هي نفس الخطوات اللي عملناها في ال MBR ولكن هتفرق في تاني step ان بعد اما اكتب parted واحددله ال disk علشان افتح interactive session مع ال parted command وبعدين اقوله mkpart علشان اعمل create وبعدين هيسالني عن اسم البارتشن بعكس ال MBR كان بيسالني اختار primary او extended

```
[root@server~]# parted /dev/vdb
```

2- الاختلاف هيكون في الخطوه دي لان زي ماقولنا قبل كده ان في ال GPT مفهوش extended partition ف هو بيتعامل ان كل ال partition بيكون primary ف هنا بيطلب مني اكتب اسم ال partition اللي هعمله create

```
(Parted) mkpart
Partition name? []? usersdata
```

3- بعد كده بحددله ال file system type اللي هعمل بيه create

```
File system type? [ext2]? xfs
```

8- بعد كده نفس الخطوات اللي عملناها في ال MBR هي هي مفيش اي اختلافي

- ان انت هتحددله ال start وال End بتاعتك ان انت عايز ال size بتاع البارتشن ده بيبدأ منين وينتهي فين
- وبعد كده لو انت خلصت وعايز تعمل Exit هتستخدم ال command ده quit
- بعد كده هستخدم **udevadm settle** لو انت لاقيت ال partition اللي انت عملتله create لسه مش ظاهر تحت /dev
- هي هي نفس خطوات ال MBR الاختلاف فقط في الخطوات اللي احنا ذكرناها فوق

Deleting Partitions

- The following steps apply for both the MBR and GPT partitioning schemes.

1- Specify the disk that contains the partition to be removed. [root@host ~]# **parted /dev/*vdb***

2- dentify the partition number of the partition to delete. (parted) **print**

3- Delete the partition. (parted) **rm1**

- The **rm** subcommand immediately deletes the partition from the partition table on the disk.

4- Exit **parted.** (parted) **quit**

- **هنفذ كل اللي احنا اتكلمنا عليه**

➢ لو انا عايز أ list كل ال blocks devices الموجوده عندي هستخدم الامر **lsblk**

```
[root@MohamedAtef ~]# lsblk
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sr0           11:0     1   8.9G  0  rom
sr1           11:1     1   8.9G  0  rom
nvme0n1       259:0    0   60G   0  disk
├─nvme0n1p1   259:1    0   512M  0  part   /boot
├─nvme0n1p2   259:2    0   20G   0  part   /
├─nvme0n1p3   259:3    0   20G   0  part   /home
├─nvme0n1p4   259:4    0   1K    0  part
└─nvme0n1p5   259:5    0   2G    0  part   [SWAP]
```

➢ لو انا استخدمت **lsblk -p** ده بيعرضلي المسار الخاص بال Disk

```
[root@MohamedAtef ~]# lsblk -p
NAME                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
/dev/sr0            11:0    1  8.9G  0 rom
/dev/sr1            11:1    1  8.9G  0 rom
/dev/nvme0n1        259:0   0   60G  0 disk
├─/dev/nvme0n1p1    259:1   0  512M  0 part /boot
├─/dev/nvme0n1p2    259:2   0   20G  0 part /
├─/dev/nvme0n1p3    259:3   0   20G  0 part /home
├─/dev/nvme0n1p4    259:4   0    1K  0 part
└─/dev/nvme0n1p5    259:5   0    2G  0 part [SWAP]
```

- لو انا عايز اعرض البارتشن وكمان ال file system ال created علي كل بارتشن منهم

```
[root@MohamedAtef ~]# lsblk -pf
NAME        FSTYPE FSVER LABEL                UUID                                 FSAVAIL FSUSE% MOUNTPOINTS
/dev/sr0    iso966 Jolie RHEL-9-2-0-BaseOS-x86_64
                                              2023-04-13-16-58-02-00
/dev/nvme0n1
├─/dev/nvme0n1p1
│           xfs                             89c6ad95-3330-4ca3-9eb2-5288ce7a231b  258.4M    49% /boot
├─/dev/nvme0n1p2
│           xfs                             86390f1a-b5d9-4684-8574-631d35fb87b2   14.5G    28% /
```

- هنعمل print لبارتشن باستخدام ال parted command

```
[root@MohamedAtef ~]# parted /dev/nvme0n1 print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n1: 64.4GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number  Start   End     Size    Type     File system     Flags
 1      1049kB  538MB   537MB   primary  xfs             boot
 2      538MB   22.0GB  21.5GB  primary  xfs
 3      22.0GB  43.5GB  21.5GB  primary  xfs
 4      43.5GB  64.4GB  20.9GB  extended                 lba
 5      43.5GB  45.6GB  2147MB  logical  linux-swap(v1)  swap
```

لما استخدم ال command ده هيجبلي معلومات عن البارتشن

اول حاجه جابيلك ال Model الخاص بالHard drive وقايلك انه عباره عن nvme

ده ال Disk name موجود تحت /dev/nvme0n1 وال size حوالي 64.4GB

وقايلك هنا ال Partition Table المستخدمه في ال disk هو msdos معناها انه ال مستخدم MBR Partitioning scheme

هنلاقي هنا معلومات عن رقم البارتشن وبدايه ونهايه كل بارتشن ونوع البارتشين ونوع ال file system

- هنعمل create ل مجموعه من البارتشن باستخدام MBR Partitions احنا ضيفنا Disk جديد اسمه nvme0n2 ده اللي احنا هتشتغل عليه

- قبل اما نعمل create هنعمل الاول print للبارتشين هقوله parted وبعدين اسم البارتشين وبعدين printهنلاحظ

```
[root@MohamedAtef ~]# parted /dev/nvme0n2 print
Error: /dev/nvme0n2: unrecognised disk label
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: unknown
Disk Flags:
```

هنلاقيه هنا مطلعلك error وبيقولك انه معلهوش اي Disk Label

وهنا بيقولك ال Partition Tableمش معروف

- علشان اضيف disk label هقوله parted وبعدين اسم البارتشين وبعدين mklabel msdos

```
[root@MohamedAtef ~]# parted /dev/nvme0n2 mklabel msdos
Information: You may need to update /etc/fstab.
```

- تعال نعمل print تاني ونشوف هل ال disk label انضاف ولا لا

```
[root@MohamedAtef ~]# parted /dev/nvme0n2 print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
```

هنلاقيه هنا قايلك ان ال Partiton table هو msdos او MBR

➢ علشان نعمل Create للبارتشين تعال ندخل جوه ال parted session عن طريق اني اقوله parted وبعدين اسم ال Disk

```
[root@MohamedAtef ~]# parted /dev/nvme0n2
GNU Parted 3.5
Using /dev/nvme0n2
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) mkpart
Partition type?  primary/extended? primary
File system type?  [ext2]? xfs
Start? 0%
End? 20%
(parted) print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number        Start        End        Size        Type        File system        Flags
 1            1049kB       4295MB     4294MB      primary     xfs
```

اول اما انفذ الامر ده هيفتحلي interactive session عن طريقه اقدر اني اعمل create للبارتشين بيكون عباره عن انه بيسالني وانا هكتب ال command اللي انا محتاج انفذه زي مثلا print او اني احدد بدايه ونهايه ال partition وهكذا

هنا هكتب mkpart علشان اعمل create

هنا بيسالني عن نوع ال file system type ف انا هنا هستخدم ال xfs

هنا بيسالني عن بدايه البارتشين ف انا عندي ال disk مساحته 20 جيجا ف انا هنا ممكن استخدم النسبه اني اقوله 0% معناها من بدايه الديسك عند 1 ميجا

هنا بيسالني عن نهايه البارتشين ف كاتبله 20% معناها اني عايز 20% من مساحه ال Disk اللي هو 20 جيجا ف هتكون المساحه حوالي 4 جيجا

هنا هعمل print وهشوف البارتشين اللي انا عملته create

هنا هنلاقي البارتشين اللي احنا عملناله create

رقم البارتشين | بدايه البارتشين اللي احنا حدددناها وهي 0% | نهايه البارتشين اللي احنا حدددناها وهي 20% | حجم البارتشين الكلي | نوع البارتشين | نوع ال file system

➢ هنضيف كذا بارتشين كمان

```
[root@MohamedAtef ~]# parted /dev/nvme0n2
GNU Parted 3.5
Using /dev/nvme0n2
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) mkpart primary ext4 20% 40%
(parted) print
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number   Start     End        Size       Type     File system  Flags
   1     1049kB    4295MB     4294MB     primary
   2     4295MB    8590MB     4295MB     primary  ext4

(parted) mkpart primary ext4 40% 60%
(parted) mkpart primary ext4 60% 80%
(parted) print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number  Start      End        Size       Type     File system  Flags
   1    1049kB     4295MB     4294MB     primary
   2    4295MB     8590MB     4295MB     primary  ext4
   3    8590MB     12.9GB     4295MB     primary  ext4
   4    12.9GB     17.2GB     4295MB     primary  ext4
```

ممكن اقوله في نفس الline اقوله mkpart وبعدين الtype اللي هنستخدمه هنكتب primary وبعدين نكتب ال file system هنكتب مثلا ext4 وبعدين بدايه البارتيشن ونهايه البارتشين خلي بالك ان بدايه البارتشين هي نهايه البارتشين اللي قابله وهكذا

هنا هعمل print وهشوف البارتشين اللي انا عملته create

ده البارتيشن اللي احنا لسه عاملينه

هنعمل بنفس الطريقه بارتشين تاني من بدايه 40% ل 60% ومن 60% ل 80%

هنلاقي هنا ال 4 بارتشين اللي احنا عملناهم وخلي بالك انهم كلهم primary يعني لو جيت عملت create ل بارتشين تاني primary او extended مش هيقبل وهيطلع ايرور لان احنا قولنا قبل كده في ال MBR مسموح ليا ب 4 بارتشين ي اما كلهم primary ي اما 3 منهم primary وواحد فقط extended وعن طريق ال extended اقدر اعمل create ل logical partitions 63

- لو عملنا ceate لبارتشين تاني هيحصل error زي ماقولنا

```
(parted) mkpart primary ext4 80% 100%
Error: Can't create any more partitions.
```

- طب لو انا عايز اضيف بارتشين تاني لازم امسح البارتشن رقم 4 ونعمله replace لبارتشين تاني نوعه extended والافضل والاحسن ان ال extended ياخد كل المساحه ال free
- علشان اعمل remove للبارتشين رقم 4 هقوله rm 4

```
(parted) rm 4
(parted) print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number  Start     End       Size     Type     File system  Flags
  1     1049kB    4295MB    4294MB   primary
  2     4295MB    8590MB    4295MB   primary  ext4
  3     8590MB    12.9GB    4295MB   primary  ext4
```

هنا هكتب rm 4 علشان اعمل remove للبارتشين رقم 4

هنلاقي هنا البارتشين رقم 4 مش موجود

- هنعمل create لبارتشين رابع نوعه extended هنسخدم زي ماحنا عارفين mkpart

```
(parted) mkpart
Partition type?  primary/extended? extended
Start? 60%
End? 100%
(parted) print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Disk Flags:
Number  Start     End       Size     Type     File system  Flags
  1     1049kB    4295MB    4294MB   primary
  2     4295MB    8590MB    4295MB   primary
  3     8590MB    12.9GB    4295MB   primary
  4     12.9GB    21.5GB    8590MB   extended             lba
```

هنا هحدد نوع البارتيشن ف احنا هنختار extended

في ال extended يفضل انك تحدد المساحه ال free كلها يعني احنا هنا اخر بارتشين احنا عاملين ليه create بارتشين رقم 3 احنا حددنا نهايه المساحه بتاعته ل 60% ف اللي فاضي 40% لحد اما توصل ل 100% ف يفضل اني احدد المساحه الفاضيه كلها اللي هتكون من 60% ل 100%

ضافلي هنا البارتشين رقم 4 ال extended

- لو انا عايز اعرض ال size بالنسبه % percentage هستخدم امر unit وبعدين %

```
(parted) unit %
(parted) print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 100%
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number  Start    End      Size    Type     File system  Flags
  1     0.00%    20.0%    20.0%   primary
  2     20.0%    40.0%    20.0%   primary
  3     40.0%    60.0%    20.0%   primary
  4     60.0%    100%     40.0%   extended             lba
```

استخدمت unit % علشان اعرض ال size بال %

هنا اصبحت ال size بال % percentage

- بعد اما ضيفنا بارتشين رابع نوعه extended هنعمل create لبارتشين تاني نوعه logical

```
(parted) mkpart
Partition type?  [logical]?  logical
File system type?  [ext2]? ext3
Start? 60%
End? 80%
(parted) print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 100%
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number  Start  End    Size   Type     File system  Flags
 1      0.00%  20.0%  20.0%  primary
 2      20.0%  40.0%  20.0%  primary
 3      40.0%  60.0%  20.0%  primary
 4      60.0%  100%   40.0%  extended             lba
 5      60.0%  80.0%  20.0%  logical   ext3
```

هنا انا لما كتبت mkpart جابلي علي طول logical مجبليش ولا primary ولا extended
لان انا لما انا حددت extended اي بارتشين هيتعمله create هيكون logical

دايما بدايه ال size الخاص بال logical بيكون بدايه حجم ال extended وليس النهايه

ده ال logical partition اللي احنا عملناه لو خدت بالك هتلاقي بدايه ال extended نفس ال logical

- تعال نشوف الطريقه ال no interactive اللي بقدر من خلالها اني اعمل create او remove وهكذا
- لو انا عايز اعمل remove ل partition معين هستخدم parted وبعدين اسم البارتشين وبعدين rm ورقم البارتشين

```
[root@MohamedAtef ~]# parted /dev/nvme0n2 rm 5
Information: You may need to update /etc/fstab.
```

هنا عملنا remove للبارتشين رقم 5

- علشان اعمل print

```
[root@MohamedAtef ~]# parted /dev/nvme0n2 print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: msdos
Disk Flags:
Number  Start   End     Size    Type     File system  Flags
 1      1049kB  4295MB  4294MB  primary
 2      4295MB  8590MB  4295MB  primary
 3      8590MB  12.9GB  4295MB  primary
 4      12.9GB  21.5GB  8590MB  extended             lba
```

- علشان اعمل create ل بارتشين من بره هستخدم

```
[root@MohamedAtef ~]# parted /dev/nvme0n2 mkpart logical xfs 60% 80%
Information: You may need to update /etc/fstab.
```

- علشان اغير ال Disk بتاعي من ال MBR ل GPT هستخدم

```
[root@MohamedAtef ~]# parted /dev/nvme0n2 mklabel gpt
Warning: The existing disk label on /dev/nvme0n2 will be destroyed and all data on this
disk will be lost. Do you want to continue?
Yes/No? yes
Information: You may need to update /etc/fstab.

[root@MohamedAtef ~]# parted /dev/nvme0n2 print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:
Number  Start  End  Size  File system  Name  Flags
```

خلي بالك لما تستخدم الامر لما تغير من ال MBR ل GPT او العكس الامر ده هيعملك format لل Disk بكل حاجه جواه علشان كده اداك تحذير انه هيعمل format وانك هتفقد كل الداتا الموجوده

لما جينا عملنا print هنلاقيه هنا مسح كل الداتا ومسح كل البارتشين اللي احنا كنا عملينها في حاله الMBR

- هنعمل create ل new partition باستخدام ال GPT

```
[root@MohamedAtef ~]# parted /dev/nvme0n2
GNU Parted 3.5
Using /dev/nvme0n2
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) mkpart
Partition name?  []? nvme0n2p1
File system type?  [ext2]? xfs
Start? 0%
End? 50%
(parted) print
Model: VMware Virtual NVMe Disk (nvme)
Disk /dev/nvme0n2: 21.5GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Disk Flags:
Number  Start    End    Size    File system    Name  Flags
 1      1049kB  10.7GB  10.7GB    xfs         nvme0n2p1
```

الاختلاف الوحيد زي ماقولنا قبل كده ان في ال MBR بيسالني علي نوع البارتيشن ي اما primary او extended اما في الGPT هو بيعتبر كل البارتشين بتكون primary ف هو هنا بيسالني علي اسم البارتشين اللي هيتعمله create ف انا هسميه علي سبيل المثال nvme0n2p1

Managing Partitions With fdisk, gdisk Command

- فيه عندي Two Command اقدر استخدمهم ان انا اعمل manage لل partition غير ال **parted** command وهما ال **fdisk** و ال **gdisk**

➢ هنستخدم ال **fdisk command**

➢ لو انا عايز اعرف معلومات عن الهارد هستخدم ال command ده **fdisk -l**

```
[root@MohamedAtef ~]# fdisk -l
Disk /dev/nvme0n1: 60 GiB, 64424509440 bytes, 125829120 sectors
Disk model: VMware Virtual NVMe Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xd04d129c
Device        Boot    Start       End  Sectors  Size Id Type
/dev/nvme0n1p1 *       2048   1050623  1048576  512M 83 Linux
/dev/nvme0n1p2      1050624  42993663 41943040   20G 83 Linux
/dev/nvme0n1p3     42993664  84936703 41943040   20G 83 Linux
/dev/nvme0n1p4     84936704 125829119 40892416 19.5G  f W95 Ext'd (LBA)
/dev/nvme0n1p5     84938752  89133055  4194304    2G 82 Linux swap / Solaris
```

➢ لو انا عايز اعرف معلومات علي مستوي disk معين هستخدم **fdisk -l** وبعدين اسم البارتشن

```
[root@MohamedAtef ~]# fdisk -l /dev/nvme0n2
Disk /dev/nvme0n2: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual NVMe Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: gpt
Disk identifier: A4D6D3DC-5408-47F3-A29B-A3BBEA3B481D
Device        Start      End  Sectors Size Type
/dev/nvme0n2p1  2048 20971519 20969472  10G Linux filesystem
```

➢ لو انا عايز اعمل create لبارتشين جديد هستخدم الامر fdisk /dev/nvme0n2 وبعدين هيفتحلي interactive session

```
[root@MohamedAtef ~]# fdisk /dev/nvme0n2
Welcome to fdisk (util-linux 2.37.4).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
Command (m for help): m
Help:
  GPT
   M   enter protective/hybrid MBR
  Generic
   d   delete a partition
   F   list free unpartitioned space
   l   list known partition types
   n   add a new partition
   p   print the partition table
   t   change a partition type
   v   verify the partition table
   i   print information about a partition
```

هنا فتحلي interactive session زي الموجوده في ال parted ولكن بشكل مختلف

هنا بيسالني عن ال command اللي هستخدمه ولو انت عايز تعرض كل ال command استخدم m

لما تستخدم ال m هيعرضلك كل ال command اللي ممكن تستخدمها زي مظاهر قدامك فيه commands تانيه غير دول

➢ احنا هنعمل create ل new partition ف هنستخدم ال n command

```
Command (m for help): n
Partition type
   p   primary (0 primary, 0 extended, 4 free)
   e   extended (container for logical partitions)
Select (default p): primary
Partition number (1-4, default 1): 1
First sector (2048-41943039, default 2048):
Last sector, +/-sectors or +/-size{K,M,G,T,P} (2048-41943039, default 41943039): +10G
Created a new partition 1 of type 'Linux' and of size 10 GiB.

Command (m for help): p
Disk /dev/nvme0n2: 20 GiB, 21474836480 bytes, 41943040 sectors
Disk model: VMware Virtual NVMe Disk
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xe0aca04f
Device       Boot      Start     End       Sectors  Size  Id  Type
/dev/nvme0n2p1         2048    20973567  20971520  10G   83  Linux

Command (m for help): w
The partition table has been altered.
Syncing disks.
[root@MohamedAtef ~]#
```

انا استخدم ال n علشان هعمل new partition

بيقولك هنا اختار نوع البارتشن وهنا قايلك ال default هو p اختصار ل primary

هنا قايلك اختار رقم البارتشن ومحددلك ان الdefault هو 1

وهنا عايزك تحددله بدايه ال sector وهو by default محددهالك ب 2048

وهنا نهايه ال sector ف انا محدد 10GB

علشان اعمل print هستخدم p علشان يعرضلي معلومات عن البارتشين

لو انا عايز اعمل save واخرج بره ال session هقوله w

Creating File Systems

- After the creation of a block device, the next step is to add a file system to it. Red Hat Enterprise Linux supports many different file system types, but two common ones are **XFS** and **ext4** , the installer for Red Hat Enterprise Linux, uses **XFS** by default.
- As root, use the **mkfs.xfs** command to apply an XFS file system to a block device. For ext4, use **mkfs.ext4**.

```
[root@host ~]# mkfs.xfs /dev/vdb1
```

Mounting File Systems

- After you have added the file system, the last step is to mount the file system to a directory in the directory structure. When you mount a file system onto the directory hierarchy, user can access or write files on the device.

```
[root@host ~]# mount /dev/vdb1 /mnt
[root@host ~]# cat /etc/fstab
```

- When you add or remove an entry in the **/etc/fstab file**, run the **systemctl daemon-reload** command, or reboot the server, for systemd to register the new configuration.

MOOCA MEDIA PRODUCTION

- بمجرد اننا عملنا create ل new partition الخطوه اللي بعدها ان احنا نبدأ ن create file system علي ال new created partition
- انا عندي مجموعه من ال file system الموجوده في اللينكس زي ال XFS وال ext4 وهكذا
- وعندي مجموعه من ال commands بنستخدمها علشان ن apply ال file system المختلفه علي ال partitions بتاعتنا
- وليكن في حاله ال XFS File System عندي command اسمه mkfs.xfs وبعدين اديله اسم البارتشن علشان يعمل add او apply ل XFS File system علي البارتشن
- وعندي في حال ال ext4 عندي command اسمه mkfs.ext4 وبعدين اديله اسم البارتشن علشان يعمل add او apply ل ext4 File system علي البارتشن
- بعد اما اعمل add او apply لل file system اخر step بنعملها علشان تبدأ انك ت access البارتشين وتبدأ تستخدمه ان انا اعمل mount لل partition علي mounting point ان انا بقوله mount وبعدين اسم البارتشين وبعدين اسم ال directory اللي هعمل mount تحتيه
- بعد كده علشان اخلي ال mount بتاعي يكون permanent في حاله لو عملت reboot لل system ان انا احط ال mount في ال configuration file اللي اسمه **/etc/fstab**
- وبعد اما اعدل في ال **/etc/fstab** لازم اعمل **systemctl daemon-reload** علشان يحس بكل التغييرات اللي حصلت

- تعال في الاول نعرض كل البارتشين الموجوده عندي بال file system الخاص بيها

```
[root@MohamedAtef ~]# lsblk -pf
NAME                FSTYPE  FSVER      LABEL          UUID           FSAVAIL FSUSE%      MOUNTPOINTS
/dev/nvme0n2
├─/dev/nvme0n2p1
├─/dev/nvme0n2p2
├─/dev/nvme0n2p3
├─/dev/nvme0n2p4
└─/dev/nvme0n2p5
```

- لو انا جيت قولت **mkfs** وبعدين ضغط علي Tab مرتين هيعرضلي كل ال file system اللي ممكن استخدمها

```
[root@MohamedAtef ~]# mkfs
mkfs          mkfs.ext2   mkfs.ext4   mkfs.minix   mkfs.vfat
mkfs.cramfs   mkfs.ext3   mkfs.fat    mkfs.msdos   mkfs.xfs
```

- لو جيت عملت add ل file system علي بارتشين وليكن /dev/nvme0n2p1

```
[root@MohamedAtef ~]# mkfs.ext4 /dev/nvme0n2p1
mke2fs 1.46.5 (30-Dec-2021)
Creating filesystem with 1048320 4k blocks and 262144 inodes
Filesystem UUID: 65c10360-1dd8-40c3-ad43-6f8e4b740f9d
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912, 819200, 884736
Allocating group tables: done
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
```

- لو جينا نفذنا الامر **lsblk -pf** هنلاحظ

```
[root@MohamedAtef ~]# lsblk -pf
NAME                FSTYPE      FSVER      LABEL      UUID                    FSAVAIL    FSUSE%    MOUNTPOINTS
/dev/nvme0n2
├─/dev/nvme0n2p1    ext4    1.0                    65c10360-1dd8-40c3-ad43-6f8e4b740f9d
├─/dev/nvme0n2p2
├─/dev/nvme0n2p3
├─/dev/nvme0n2p5
└─/dev/nvme0n2p4
```

هنلاقيه هنا كتبلي اسم ال file system اللي احنا عملناه

بمجرد ان انا عملت create ل file system هنلاقي عملي UUID ده رقم Hexadecimal بنستخدمه لو عايز اعمل mount للبارتشين

- وهكذا لباقي البارتشين بنفس الطريقه ممكن اضيف ليهم file system

- تاني step هنعمل Mount لل partitions

➢ ممكن نستخدم ال df -h علشان اعرض ال file system الموجوده عندي وكل ال partitions اللي معمول ليها Mount

```
[root@MohamedAtef ~]# df -h
Filesystem      Size   Used  Avail   Use%   Mounted on
devtmpfs        4.0M   0     4.0M    0%     /dev
tmpfs           469M   0     469M    0%     /dev/shm
tmpfs           188M   5.9M  182M    4%     /run
/dev/nvme0n1p2  20G    5.6G  15G     28%    /
/dev/nvme0n1p1  507M   249M  259M    49%    /boot
/dev/nvme0n1p3  20G    179M  20G     1%     /home
```

هنلاقي بس ال 3 partitions دول بس اللي معمول ليهم mount

➢ علشان اعمل mount لازم اعمل New Directory علشان اعمل mount تحت ال Directory ده

➢ ف هنعمل create ل directory وليكن اسمه data1 تحت ال /

```
[root@MohamedAtef ~]# mkdir /data1
```

➢ بعد كده هنعمل mount لل /dev/nvme0n2p1 تحت ال /data

```
[root@MohamedAtef ~]# mount /dev/nvme0n2p1   /data1
```

➢ لو عملنا df -h هنلاقي البارتشين اتعمله mount تحت /data1

```
[root@MohamedAtef ~]# df -h
Filesystem      Size   Used  Avail   Use%   Mounted on
devtmpfs        4.0M   0     4.0M    0%     /dev
tmpfs           469M   0     469M    0%     /dev/shm
tmpfs           188M   5.9M  182M    4%     /run
/dev/nvme0n1p2  20G    5.6G  15G     28%    /
/dev/nvme0n1p1  507M   249M  259M    49%    /boot
/dev/nvme0n1p3  20G    179M  20G     1%     /home
/dev/nvme0n2p1  3.9G   24K   3.7G    1%     /data1
```

البارتشين اتعمله mount تحت /data1 ف انا حاليا اقدر استخدم البارتشين ده

➢ ممكن كمان اعمل mount عن طريق ال UUID الخاص بالبارتشن بدل اسم البارتشن

```
[root@MohamedAtef ~]# mount UUID="65c10360-1dd8-40c3-ad43-6f8e4b740f9d"   /data1
```

➢ علشان اعرض ال UUID الخاصه بكل بارتشين ممكن استخدم **blkid** او ال **lsblk -pf**

```
[root@MohamedAtef ~]# blkid
/dev/nvme0n1p5: UUID="c225b2df-568e-497d-889f-198d33b98efe" TYPE="swap" PARTUUID="d04d129c-05"
/dev/nvme0n1p3: UUID="7dd0042b-6f80-4dc7-9fe9-17612d15f429" TYPE="xfs" PARTUUID="d04d129c-03"
/dev/nvme0n1p1: UUID="89c6ad95-3330-4ca3-9eb2-5288ce7a231b" TYPE="xfs" PARTUUID="d04d129c-01"
/dev/nvme0n1p2: UUID="86390f1a-b5d9-4684-8574-631d35fb87b2" TYPE="xfs" PARTUUID="d04d129c-02"
/dev/sr0: UUID="2023-04-13-16-58-02-00" LABEL="RHEL-9-2-0-BaseOS-x86_64" TYPE="iso9660"
PTUUID="d3d1f9a5" PTTYPE="dos"
/dev/nvme0n2p3: PARTUUID="d2aa7a6c-03"
/dev/nvme0n2p1: UUID="65c10360-1dd8-40c3-ad43-6f8e4b740f9d" TYPE="ext4" PARTUUID="d2aa7a6c-01"
```

- علشان اخلي الmount يكون permanent هنفتح ال /etc/fstab بال vim ونضيف جواه ال mount بالطريقه التاليه

```
[root@MohamedAtef ~]# vim  /etc/fstab
```

هنفتح ال file بال vim وهنكتب فيه الاتي

```
UUID=86390f1a-b5d9-4684-8574-631d35fb87b2   /        xfs     defaults   0 0
UUID=89c6ad95-3330-4ca3-9eb2-5288ce7a231b   /boot    xfs     defaults   0 0
UUID=7dd0042b-6f80-4dc7-9fe9-17612d15f429   /home    xfs     defaults   0 0
UUID=c225b2df-568e-497d-889f-198d33b98efe   none     swap    defaults   0 0
/dev/nvme0n2p1                              /data1   ext4    defaults   0 0
```

هنكتب هنا اسم البارتشن

وهنا هنكتب الDirectory اللي انا عملت mount للبارتشين تحتيه

هنا هنكتب نوع ال file system اللي احنا عملنا ليه add علي البارتشن ده

ودول ال default نكتبهم زي مهما

- وبعد كده هنعمل mount -a علشان يعمل reread تاني للconfiguration file ويشوف هل انا كاتب جوه ال fstab صح ولا غلط لو مظهرليش اي حاجه معناه كده ان ال configuration مفهوش اي مشكله

```
[root@MohamedAtef ~]# mount -a
```

- اخر حاجه طالما غيرت في ال configuration file لازم اعمل reload علشان يحس بكل التغييرات اللي احنا عملناها في ال configuration file ف هستخدم ال command

```
[root@MohamedAtef ~]# systemctl daemon-reload
```

MANAGING SWAP SPACE

INTRODUCING SWAP SPACE CONCEPTS

- خلينا نتكلم عن اهم topic عندنا في red hat admin 2 هو ال swap memory ونشوف ايه هي اهميته وايه المميزات الخاصه بيه
- فكره ال swap ببساطه هي عباره عن space بتعملها create علي الهارد ديسك بحيث ان ال operating system يستخدمها ك virtual memory في حاله لو ال physical memory كانت full utilized
- وده ليه مجموعه من المميزات اولهم ان ال swap memory بيساعدك انك ت extend ال virtual memory بتاعتك وال Virtual memory هنا المقصود بيها ال total size او ال combination مابين ال Physical swap space + RAM Size
- تاني ميزه انه بي support ال Hibernation
- انا عندي ال kernel هو المسئول انه ي handle وي manage ال swap memory ال kernel عنده sub system اسمه memory management هو المسئول لو ال physical RAM عدت limit معين مثلا عدت 90% فساعتها ال Kernel هيروح يفضي مكان ليها في الميموري عن طريق انه هيروح ي search علي اي inactive pages في ال physical Ram ويروح يعملها save او write علي ال swap area بتاعتك for temp ويروح يعمل reassigned لل pages دي ل ال new process اللي محتاجه الميموري

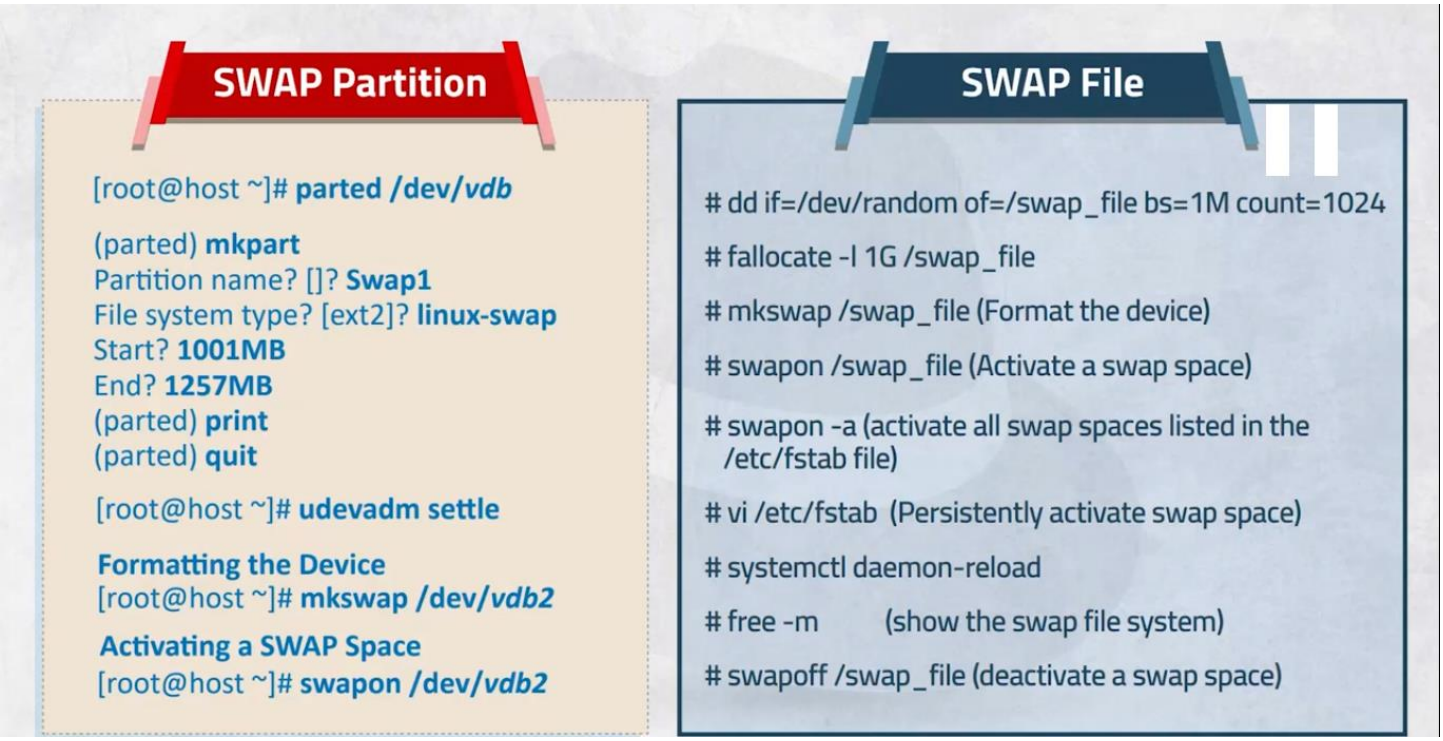
Sizing the Swap Space

- علشان نعمل Sizing ل swap space فيه عندي كذا option ممكن انا ك سيستم ادمن ممكن اعمل sizing based علي ال workload الموجود علي السيرفر بتاعي يعني انا ك سيستم ادمن aware دايما بال memory utilization علي السيرفر ف وانا بعمل sizing بعمله sizing بال level اللي يحافظ علي ال stability علي السيرفر بتاعي
- او ممكن يجي vendor معين يديك مجموعه من ال recommendations من ضمنها يقولك انا عايزك تعمل ال swap area تخلي ال size بتاعها مثلا 8 جيجا ف ساعتها انت بت follow ال recommendation بتاعت ال vendor
- انا ك سيستم ادمن لو مش عارف اعمل sizing ازاي فيه عندك red hat حطالنا table في ال documents بتاعتها بيساعدك انك تعمل sizing علي حسب ال physical memory يعني لو الرام بتاعتك مساحتها 2 جيجا يبقي تخلي ال swap area مساحته ضعف الرام. ولو هي في الرينج من 2 ل8 جيجا يبقي تخلي ال swap area نفس حجم الميموري وهكذا

RAM and Swap Space Recommendations

RAM	Swap space	Swap space if allowing for hibernation
2 GB or less	Twice the RAM	Three times the RAM
Between 2 GB and 8 GB	Same as RAM	Twice the RAM
Between 8 GB and 64 GB	At least 4 GB	1.5 times the RAM
More than 64 GB	At least 4 GB	Hibernation is not recommended

CREATING A SWAP SPACE



- فيه عندي طريقتين علشان اعمل create ل new swap space عندي طريقتين

1- اول طريقه وهي ال swap partition وفي الطريقه دي انا بعمل create لبارتشين مخصص لل swap area عن طريق اي command من اللي احنا اخدناها زي مثلا parted command بقوله parted واديله اسم ال Disk وبعمل create ل بارتشين عادي جدا اني اقوله mkpart وبعدين احددله ال partition name وليكن swap1 وبعدين احددله ال file system ف اقوله linux-swap وبعدين احددله ال start وال End وبعدين اقوله print وبعدين quit بنفس الطريقه اللي بنعمل بيها create ل partition جديد

- تاني step كنا بنعملها اننا بنعمل create ل file system في حاله ال swap علشان ن create ال file system عندنا command بنستخدمه اسمه mkswap وبعدين اديله اسم البارتشن انا كده عملت formatting للبارتشين

- علشان اعمل Activating لل swap space علشان ال kernel يلاحظ ان فيه new swap space انه يقدر انه يستخدمها بستخدم command اسمه swapon وبعدين اديله اسم البارتشين

2- تاني طريقه لو انا مثلا معنديش اي مساحه فاضيه اقدر اعمل بيها create لبارتيشن لل swap area بتاعتي او انا وصلت لل limitations ان انا مثلا مستخدم MBR Partitioning scheme وعامل create ل 4 primary partitions وال 4 بستخدمهم ف في الحاله دي انا بلجئ لطريقه تانيه اسمها SWAP File. ان انا بعمل create ل file ب size معين وبتعامل ان ال file ده كانه بارتشين بعمل عليه SWAP File system وبعمله activate وال kernel بيتعامل معاه كانه بارتشين موجود في السيستم

- في عندي two command بستخدمهم لو انا عايز أ create new swap file ب size معين
- اول commandاسمه dd وده بيكون عباره عن

```
#dd if=/dev/random  of=/swap_file  bs=1M  count=1024
```

- ال command اسمه dd
- بعد كده بقوله if=/dev/random ده بيكون special file تحت /dev بيكون فيه random number file ال if معناها ال input file
- وبخلي ال of اللي هو ال output file بيساوي /swap_file
- وبعد كده بحددله ال block size بقوله bs=1M
- وبعد كده بحددله ال count

- تاني command اسمه **fallocate** ان انا بقوله fallocate وبعدين اوبشن l- وبعدين 1G علشان يعمل create تحت ال / ويكون ال size بتاعه 1 جيجا

```
fallocate  -l 1G /sawp_file
```

- بعد اما نعمل create ل ال file هتعامل معاه كأنه Partitions موجود عندي ف هروح اعمله format باستخدام **mkswap** واحددله اسم ال file

```
mkswap /swap_file
```

- بعد كده اعمل activate لل swap باستخدام **swapon** وبعدين اديله اسم ال file

```
swapon /swap_file
```

- علشان اخلي ال swap تكون permanent في حاله لو السيستم اتعمله reboot ف بحط record ليها في ال **/etc/fstab** عن طريق ان انا بفتح ال fstab file باستخدم ال vim واحط فيه ال record الخاص بال swap
- وبعد كده علشان السيستم يحس بكل التغييرات اللي حصلت هعمل reload باستخدام

```
systemctl daemon-reload
```

- لو انا عايز اعمل deactivate لل swap space هستخدم swapoff وبعدين اسم ال file الخاص بال swap

```
swapoff  /swap_file
```

- لو انا عايز أ display ال memory utilization هستخدم commad اسمه free ولو انا عايز أ display ال size بالميجا هضيف m-

```
free  -m
```

Setting the Swap Space Priority

Setting the SWAP Space Priority

- By default, the system uses swap spaces in series, meaning that the kernel uses the first activated swap space until it is full, then it starts using the second swap space. However, you can define a priority for each swap space to force that order.
- To set the priority, use the pri option in /etc/fstab. The kernel uses the swap space with the highest priority first. The default priority is -2.
- The following example shows three swap spaces defined in /etc/fstab.
  The kernel uses the last entry first, with pri=10. When that space is full, it uses the second entry, with pri=4. Finally, it uses the first entry, which has a default priority of -2.
- Use swapon --show to display the swap space priorities.
- When swap spaces have the same priority, the kernel writes to them in a round-robin

```
UUID=af30cbb0-3866-466a-825a-58889a49ef33   swap   swap   defaults   0 0
UUID=39e2667a-9458-42fe-9665-c5c854605881   swap   swap   pri=4      0 0
UUID=fbd7fa60-b781-44a8-961b-37ac3ef572bf   swap   swap   pri=10     0 0
```

- انا عندي by default ال kernel بيستخدم ال swap area الcreated عندي في السيستم علي التوالي معني انه يبدا يستخدم ال first activated swap space لحد اما يتملي بعد كده يدخل علي تاني واحد لحد اما يتملي وهكذا علشان نفهم هو ليه بيعمل كده قالك ان كل swap area بتعملها create و activate في السيستم بتاخد priority واول واحد بتعمله create بياخد ال default priority اللي هي 2- . وتاني واحد بتعمله create و activate بياخد 3- واللي بعديه ياخد 4- وهكذا . وقالك ان priority ال highest in number بمعني ان الswap area اللي واخده 2- الpriority بتاعتها اعلي مالي واخد 3- وهكذا

- هل فيه طريقه اني اغير ال priority الخاصه بأي swap area موجود عندي اه في طريقه عن طريقه ال fstab file الموجود في /etc/fstab فيه اوبشن اسمه pri موجود في ال fstab بقدر من خلاله اني اغير ال priorty اني مثلا لو عايز اغيرها ل 10 مثلا هقوله pri=10 او ممكن اسبها default وال default هنا هياخد 2-
- علشان اعرض ال swap area ال activated عندي بال priority هستخدم

```
[root@MohamedAtef ~]# swapon -s
Filename                        Type        Size        Used    Priority
/dev/nvme0n1p5                  partition   2097148     78336     -2
```

Chapter 7
Managing Logical Volumes

Logical Volume Management (LVM) Concepts

- ال LVM عباره عن Tool بقدر من خلالها اني أ manage ال Storage Devices الموجوده عندي في ال system بطريقه فعاله بالاضافه ان ال LVM عنده مجموعه من المميزات من ضمنها ان ال LVM بيدعم انك ت resized ال Logical Volume بمعني لو عندي Logical Volume شغاله فسهل جدا اني اعمل extend لل size بتاعه ونفس الكلام لو عندي Logical Volume حجمه كبير سهل جداا انك ت reduce او ت shrink ال size بتاعه بالاضافه لو انت عندك physical volume وكان corrupted سهل جداا انك ت replace ال Physical Volume من غير ماتفقد الداتا الخاصه بيك

LVM Definitions

➢ Physical Devices

- ال **Physical Devices** عباره عن ال Storage Devices او ال Block Devices اللي بيتخزن فيها ال actual data بتاعتك زي ال Hard Drive بأنواعها والبارتشين وال RAID arrays وال SAN disk

➢ Physical Volumes (PVs)

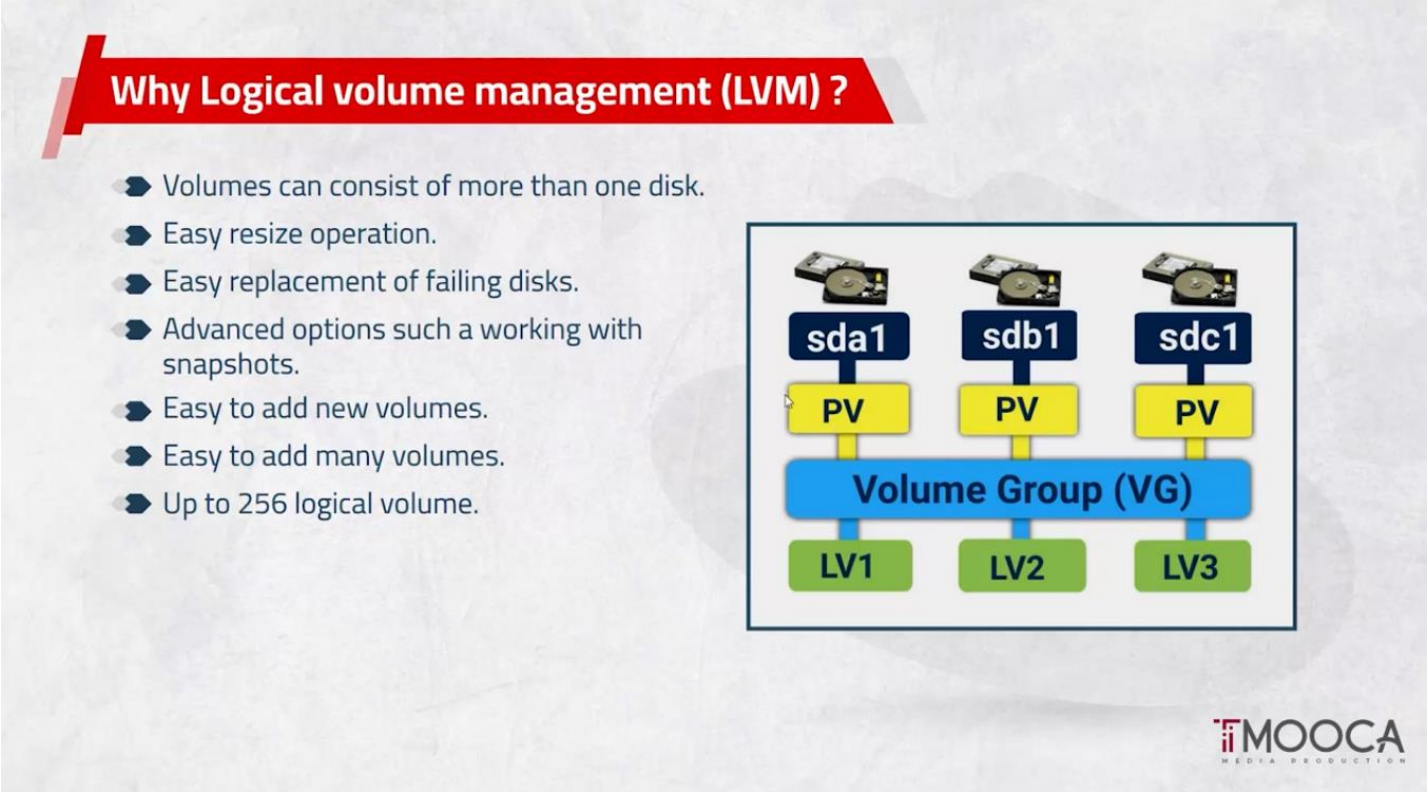
- ال **Physical Volumes** احنا بنعملها created علشان ن initialize ال Physical Devices وبمجرد اننا عملنا create لل Physical Volumes ال LVM بتروح تقسم ال Physical Volumes لمجموعه من ال blocks وال block الواحد اسمه physical extend وال size بتاعه بيكون by default 4MB

➢ Volume Groups (VGs)

- ال **Volume Groups** ودي بتكون ال storage pools . ال size بتاعها بيكون equal لل total size بتاع ال Physical Volumes اللي allocated فيها يعني مثلا لو ال Volume Group ده انت allocated فيه 3 Physical Volumes كل واحد فيه مساحه 1 جيجا ف ال Volume Groups size هيكون 3 جيجا يعني كان عندك هارد ديسك واحد مساحته 3 جيجا تقدر من خلاله انك ت create مجموعه من ال Logical Volumes

➢ Logical Volumes (LVs)

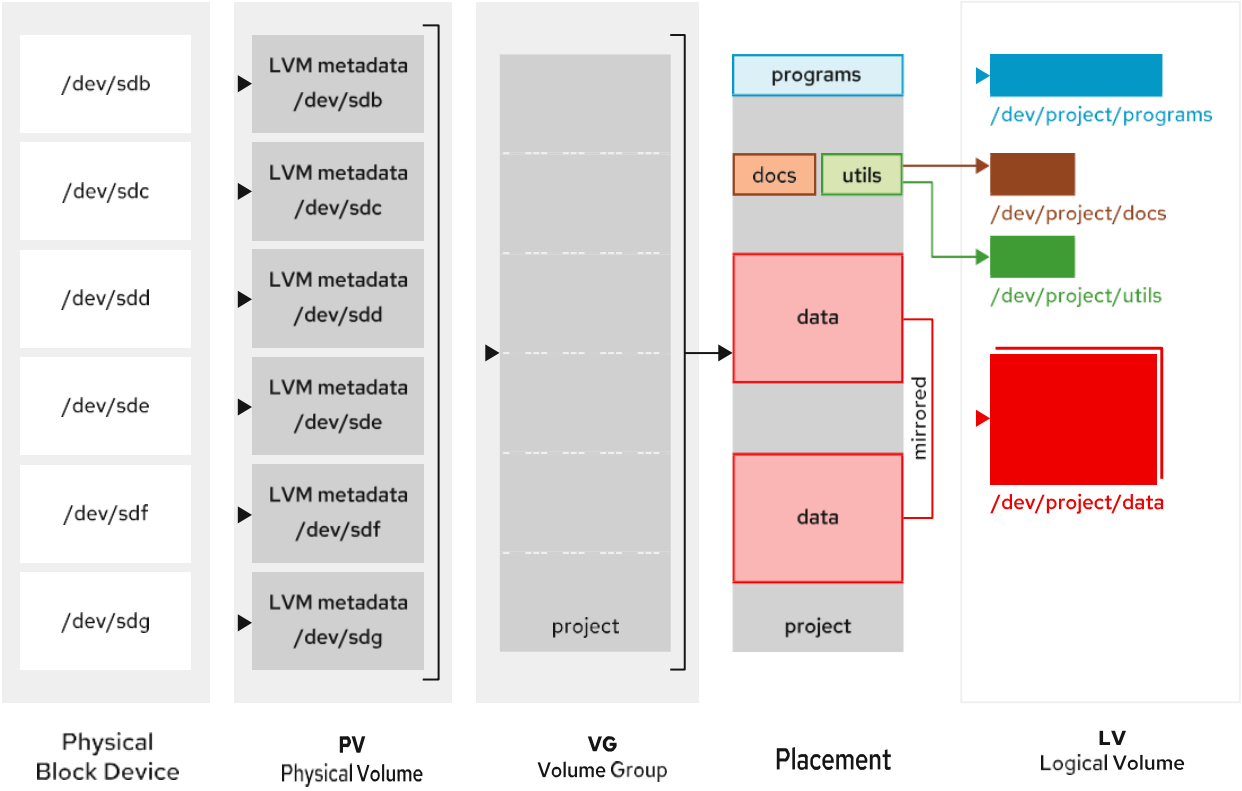
- ال **Logical Volumes** ده اللي هنتعامل معاه كانه ال Partition بتاعك هتروح ت format ال Logical Volume ده باي file system وبعد كده تعمله mount وبعدين تحط ال mount ده في ال fstab file تاني حاجه ان ال logical volumes بتكون مقسومه ل مجموعه من ال blocks ال block الواحد بيتقال عليه Logical Extents(LEs) وال size بتاعه بيكون 4 MB



- زي ماقولنا ان ال LVM عنده مجموعه من المميزات المختلفه اهمهم :-

- volumes can consist of more than one disk يعني ان انا ممكن يكون عندي اكتر من physical devices وليكن 3 physical devices وبعدين عملت create ل PV علشان اعملهم initialize وبعد كده من ال PV بعمل create ل VG ال size بتاعه بيساوي ال total بتاع ال 3 physical devices وبقدر من خلال ال VG اعمل create ل LV
- وكمان Easy resize operation ان لو مثلا عندك LV1 شغاله عندي او اتملي علي اخره سهل جدا لو انت عندي مساحه فاضيه في ال VG انك ت extend LV
- و Easy replacement of failing disks ان لو عندك disk حصله مشكله سهل جدا انك ت replace ل disk ده ب disk تاني من غير ماتفقد الداتا بتاعتك
- و بي support ال snapshots ان انت تقدر تاخد نسخه من ال file system بتاعك وال snapshots ميزتها انك بتستخدمها في حاله ال backup وال recovery
- وسهل جدا ان اعمل add ل new logical volumes
- واقدر كمان اعمل create ل 256 logical volume

Logical Volume Manager Workflow



- دي كده عباره workflow هيفهمنا اكتر ال components او ال Layers الخاصه بال LVM
- اول Layer هي ال Physical Storage او ال Physical Block Device ودي بتبقي عباره عن مجموعه من ال Hard Drives او ال Partitions او ال Disk Array او ال SAN Disk وهكذا
- تاني Layer وهي ال Physical Volume ودي بتعمل initialize لل Physical Devices
- تالت Layer وهي ال Volume Group بمجرد انك عملت create لل Physical Volume الخطوه اللي بعد كده انك تعملcreate لل Volume Group ودي بتكون عباره عن مجموع ال Physical Volume
- رابع layer وهو ال Logical Volume بمجرد انك عملت create لل Volume Group الخطوه اللي بعد كده انك تعمل create لل Logical Volume
- بعد اما عملت create ل Logical Volume لازم تعمل format لل LV باستخدام ال file system وبعد كده تعمله mount

- **هنشوف ال steps اللي هنمشي عليها علشان نعمل create ل LVM**

1-Create a Physical Volume

- اول Step بعملها اني بعمل create ل Physical Volume او PV علشان نعمل create ال command اللي احنا بنستخدمه هو **pvcreate** وبعد كده بديله ال Physical devise بمجرد ان انا عملت create لل PV هو هيروح يقسم ال PV لمجموعه من ال Physical extend(PEs) ال Physical extendالواحد حجمه 4 MB ممكن ان انا اعمل create ل اكتر من PV في نفس الوقت عن طريق اني اقوله pvcreate وبعدين اديله ال Physical devise الاولاني وبعدين Physical devise التاني وهكذا

2-Create Volume Group

- تاني step اني بعمل create ل ال Volume Group او VG فبنستخدم command اسمه **vgcreate** ف بقوله vgcreate وبعدين اديله اسم ال Volume Group بتاعي وليكن مثلا vg01 وبعدين بديله ال Physical Volume اللي انا عايز احطها في ال Volume Group

```
[root@server~]# vgcreate vg01 /dev/vdb2 /dev/vdb1
```

3-Create a Logica Volume

- تالت step اني بعمل create ل ال Logical Volume او LV فبنستخدم command اسمه **lvcreate** ف بقوله lvcreate بعد كده في 3 معلومات لازم اضيفهم بعد ال lvcreate اول معلومه بتديله اسم ال LV اللي هتعمله create ب اوبشن **-n** تاني معلومه بتحددله ال size علشان تحددله ال size عندك two option ي اما تقوله اوبشن **-l** وال **L** بتكون Uppercase ي اما تقوله **-l** وال**l** بتكون lowercase تالت معلومه اضيف ال VG

```
[root@server~]# lvcreate -n lv01 -L 700M vg01
```

- الفرق مابين ال -L وال -l
- لو انا قولتله -L معني كده ان انا بديله ال size بتاعي بالميجا بايت او الجيجا بايت او التيرا بايت وهكذا
- لو انا قولتله -l معني كده انك بتديله ال size بتاعك ب number of extent وال extent الواحد بيساوي 4 MB يعني لو قولتله مثلا 128 -l كاني عايز اعمل create ل LV ال size بتاعه 128 extent وال extent الواحد بيساوي 4 MB ف اضرب ال 128 في 4 هيطلع ال size بيساوي 512 MB
- لازم اتاكد وانا بحدد ال size ان ال size ده free في ال VG

4-Add The File System

- رابع step ان احنا نعمل create ل file system عن طريق اني اقوله mkfs -t وبعدين احددله نوع ال file system اذا كان xfs او ext4 او اين كان وبعدين اديله ال path الخاص ب ال LV ال path بتاع ال LV تحت dev/ هنلاقيه م create folder باسم ال VG وجوه ال VG هنلاقيه عامل create لل LV جواه

```
[root@server~]# mkfs -t xfs /dev/vg01/lv01
```

- بعد اما عملنا format لل LV باستخدام ال file system ال step اللي بعد كده اننا نعمل create ل directory ونعمل mount لل LV عليه علشان الدا اعمل ا Access عليه واقدر استخدمه لازم اعمله mount

```
[root@server~]# mkdir /mnt/data
```

- وبعد كده علشان اخلي ال mount بتاعي permanent لازم اضيف ال record الخاص بال mount في ال fstab file زي ماستخدمناه في الشابتر اللي فات ان انا احط record شبه ده

```
/dev/vg01/lv01 /mnt/data xfs defaults 1 2
```

- وبعد كده نعمل mount لل LV باستخدام امر mount

```
[root@server~]# mount /mnt/data
```

Removing a Logical Volume

- علشان نعمل remove ل LV هنبدا بالعكس بمعني ان وانا بعمل create اول حاجه عملت Physical volumes وبعدين Volume Group وبعدين Logical Volume وبعدين file system في ال remove هنبدأ بالعكس

  - **Prepare The File system.**

```
[root@server~]# umount /mnt/data
```

  - **Remove The Logical Volume.**

```
[root@server~]# lvremove /dev/vg01/lv01
```

  - **Remove The Volume Group.**

```
[root@server~]# vgremove vg01
```

  - **Remove The Physical Volumes.**

```
[root@server~]# pvremove /dev/vdb2 /dev/vdb1
```

• هنفذ اللي احنا شرحناه هنعمل create ل LVM

➢ هنعرض ال Disks الموجوده عندي باستخدام امر lsblk -p ف انا ضايف 4 Disks مساحه كل Disk بتكون 5 جيجا زي ماموجود ف المثال التالي

```
[root@MohamedAtef ~]# lsblk -p
NAME            MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
/dev/nvme0n2    259:6    0    5G  0 disk
/dev/nvme0n3    259:7    0    5G  0 disk
/dev/nvme0n4    259:8    0    5G  0 disk
/dev/nvme0n5    259:9    0    5G  0 disk
```

موجود هنا 4 Disk ومساحته كل Disk بتكون 5G

- تعال نعمل LVM وننشوف ال Steps مع بعض

1- اول Step هنعمل create ل Physical Volume باستخدام **pvcreate** وبعدين احنا هنعمل PV ل Two Disks اللي هما /dev/nvme0n2 و /dev/nvme0n3

```
[root@MohamedAtef ~]# pvcreate /dev/nvme0n2 /dev/nvme0n3
  Physical volume "/dev/nvme0n2" successfully created.
  Physical volume "/dev/nvme0n3" successfully created.
```

قالك هنا ان هما اتعملهم created

➢ لو انا عايز اعمل Display ل Physical Volume فيه عندي two command . command اسمه **pvs** وcommand اسمه **pvdisplay** لو انا عايز more details

```
[root@MohamedAtef ~]# pvs
  PV         VG Fmt  Attr PSize PFree
  /dev/nvme0n2   lvm2 ---  5.00g 5.00g
  /dev/nvme0n3   lvm2 ---  5.00g 5.00g
```

2- تاني step هنعمل create ل Volume Group باستخدام **vgcreate** واديله اسم الVG اللي هعمله create ف احنا هنسميه vg01 وبعد كده اديله ال PV اللي احنا عملنالها create

```
[root@MohamedAtef ~]# vgs
  VG   #PV #LV #SN Attr   VSize VFree
  vg01   2   0   0 wz--n-  9.99g 9.99g
```

➢ علشان اعمل Display ل VG هستخدم command اسمه **vgs** او **vgdisplay** لو عايز more details

```
[root@MohamedAtef ~]# vgcreate  vg01  /dev/nvme0n2  /dev/nvme0n3
  Volume group "vg01" successfully created
```

3- ال step اللي بعد كده ان احنا نعمل create ل Logical Volume باستخدام ال **lvcreate** واحنا قولنا ان ال LV بياخد 3 معلومات اول حاجه اقوله n- وبعد كده اديله اسم ال LV وليكن هنسميه lv01 وبعد كده نديله الsize ف هقوله اوبشن L- وبعدين احنا عايزين ن create LV ال size بتاعه 5G ف احنا هنديله 5G وبعد كده اديله ال VG اللي انا عايزه ي allocate منها

```
[root@MohamedAtef ~]# lvcreate -n lv01 -L 5G vg01
  Rounding up size to full physical extent 5.000 GB
  Logical volume "lv01" created.
```

➢ لو انا عايز اجيب معلومات عن ال LV هستخدم lvs او lvdisplay لو انا عايز more details

```
[root@MohamedAtef ~]# lvs
```

4- ال step اللي بعد كده بعد اما عملنا create ل LV هنعمل create ل ال file system ف هنستخدم **mkfs -t**
وبعدين نوع ال file system وبعدين ال LV Path

- علشان اجيب ال logical volume path هستخدم امر **lvdisplay**

```
[root@MohamedAtef ~]# lsdisplay
--- Logical volume ---
  LV Path            /dev/vg01/lv01          هنلاقي هنا ال LV Path
  LV Name            lv01
  VG Name            vg01
```

- هنعمل create للfile system

```
[root@MohamedAtef ~]# mkfs -t xfs /dev/vg01/lv01
```

5- ال step اللي بعد كده هعمل create ل Directory علشان اعمل mount

```
[root@MohamedAtef ~]#  mkdir /data_lv01
```

6- بعد كده هعمل **mount**

```
[root@MohamedAtef ~]# mount   /dev/vg01/lv01   /data_lv01/
```

- لو عايزين نتاكد هنستخدم **df -h**

```
root@MohamedAtef ~]# df -h
Filesystem                Size  Used Avail Use% Mounted on
devtmpfs                  4.0M     0  4.0M   0% /dev
tmpfs                     469M     0  469M   0% /dev/shm
tmpfs                     188M    6.0M  182M   4% /run
/dev/nvme0n1p2            20G     5.6G   15G  28% /
/dev/nvme0n1p1            507M   249M  259M  49% /boot
/dev/nvme0n1p3            20G     179M   20G   1% /home
/dev/mapper/vg01-lv01     5.0G    68M  5.0G   2% /data_lv01          هنلاقي هنا ال LV اتعمله create تحت /data_lv01
```

7- بعد كده علشان اخلي ال mount بتعاي permanent هضيف ال record الخاص بيه ف ال fstab file

```
[root@MohamedAtef ~]#vim  /etc/fstab
/dev/vg01/lv01                /data_lv01          xfs       defaults        0   0
```

8- بعد كده هنعمل mount -a وبعدين هنعمل **systemctl daemon-reload**

```
[root@MohamedAtef ~]# mount -a
[root@MohamedAtef ~]# systemctl daemon-reload
```

Extend Logical Volumes

Extending Logical Volumes (no down time):

```
# pvcreate /dev/sde1
# vgextend data-vg /dev/sde1
# lvextend -L +3G /dev/data-vg/data-lv
# xfs_growfs /dev/data-vg/data-lv        (update the file system for XFS file systems)

# resize2fs /dev/data-vg/data-lv         (update the file system for other file systems)
```

Or:

```
# lvextend -r -L +3G /dev/data-vg/data-lv   (extend and update in one step)
```

- لو انا عايزاعمل extend ل Logical Volumes ف قالك no down time معناها لو انت مستخدم ال LV تقدر انك تعمله extend وهو شغال يعني لو عندك Logical Partition معموله mounting انت مش محتاج انك تعمل unmount للlogical volume علشان تعمله extend ولكن في حاله ال swap لو انت عامل swap area بال logical volume فساعتها الحاله الوحيده اللي انت هتسخدمها علشان ت extend swap area لازم تعمل deactivate لل swap area وتروح تعملها extend وبعدين ترجع تعملها activate تاني

- الخطوات اللي هستخدمها علشان اعمل Extend
- بتعمل اول حاجه Physical Volume ل new partition

```
Pvcreate /dev/sde1
```

- وبعدين بالPhysical volume اللي عملناه نعمل extend ل Volume Group عن طريق ان هقوله **vgextend** وبعد كده ال VG اللي هعمله extend وبعد كده PV اللي عملناله

```
Vgextend data-vg  /dev/sde1
```

- بعد اما عملنا extend لل volume group هنعمل extend لل Logical Volume عن طريق اني اقوله **lvextend** وبعدين اوبشن L- وبعد كده احددله ال size اللي انا عايز اعمله extend وليكن انا عايز اضيف 3G ف انا هقول 3G+ وبعد كده بحددله ال path الخاص بال VG

```
lvextend -L +3G /dev/data-vg/data-lv
```

- بعد كده لازم اعمل update لل file system عندي two command فيه command اسمه xfs_growfs وبعد كده تديله اسم ال LV ده في حاله لو انت مستخدم file system علي ال LV نوعه XFS

```
xfs_growfs    /dev/data-vg/data-lv
```

- اما لو انا مستخدم اي نوع تاني من ال file system غير ال xfs هستخدم command اسمه resize2fs وبعد كده

```
resize2fs /dev/data-vg/data-lv
```

تديله اسم ال LV

- فيه عندي اوبشن تاني افضل ان انا اعمل extend و update لل file system في خطوه واحده في نفس الوقت عن طريق وانا بعمل extend لل LV هزود بس اوبشن r-

```
lvextend -r -L +3G /dev/data-vg/data-lv
```

- تعال نطبق اللي شرحناه هنعمل create ل 3 Logical Volume واحد هنعمل عليه file system نوعه xfs والتاني ext4 والتالت هنعملهswap وبعد كده هنعمل extend ل XFS file system و ext4 file system و swap file system ف الخطوات اللي هنعملها هنعمل create ل PV وبعدين نعمل create ل VG وبعدين نعملcreate ل LV وبعدين نعمل create ل file systems وبعد كده نعمل mount ل ال LV

```
[root@MohamedAtef ~]# lsblk -p
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
/dev/nvme0n2    259:6    0    5G  0 disk
/dev/nvme0n3    259:7    0    5G  0 disk
/dev/nvme0n4    259:8    0    5G  0 disk
/dev/nvme0n5    259:9    0    5G  0 disk
```

هنعمل PV ل 2 Disks

```
[root@MohamedAtef ~]# pvcreate /dev/nvme0n2  /dev/nvme0n3
 Physical volume "/dev/nvme0n2" successfully created.
 Physical volume "/dev/nvme0n3" successfully created.
```

هنا عملنا PV ل two Disks وهما /dev/nvme0n2 و dev/nvme0n3/

```
[root@MohamedAtef ~]# pvs
 PV         VG     Fmt  Attr PSize  PFree
 /dev/nvme0n2 myvg01 lvm2 a--  <5.00g 1020.00m
 /dev/nvme0n3 myvg01 lvm2 a--  <5.00g   <3.00g
```

عملنا display ل PV علشان نشوف ال PV اللي احنا عملناه الموجودين عندي ف هنلاقي ال 2 Desks اللي عملانهم ومساحه كل disk بتكون 5G

```
[root@MohamedAtef ~]# vgcreate myvg01 /dev/nvme0n2 /dev/nvme0n3
 Volume group "myvg01" successfully created
```

بعد كده هنعمل create ل VG

```
[root@MohamedAtef ~]# vgs
 VG     #PV #LV #SN Attr   VSize VFree
 myvg01   2   0   0 wz--n-  9.99g 9.99g
```

عملنا display ل VG علشان نشوف ال VG اللي عملناه هنلاقي myvg01 اللي احنا عملناله create و الsize حوالي 10G

```
[root@MohamedAtef ~]# lvcreate -n lv01-xfs -L 2G myvg01
 Logical volume "lv01-xfs" created.

[root@MohamedAtef ~]# lvcreate -n lv02-ext4 -L 2G myvg01
 Logical volume "lv02-ext4" created.

[root@MohamedAtef ~]# lvcreate -n lv03-swap -L 2G myvg01
 Logical volume "lv03-swap" created.
```

بعد كده نعمل create ل 3 LV مساحه كل واحد فيهم 2G علشان نعمل علي كل واحد فيهم files system مختلف هنسمي بس كل lv باسم ال file system علشان بس نكون فاهمين واحنا بنطبق هنعمل LV اسمه lv01-xfs و lv02-ext4 وlv03-swap

```
[root@MohamedAtef ~]#lvs
 LV       VG     Attr       LSize Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
 lv02-ext4 myvg01  -wi-a-----  2.00g
 lv03-swap myvg01 -wi-a-----  2.00g
 lv01-xfs  myvg01  -wi-a-----  2.00g
```

هنلاقي هنا ال LV اللي عملنالهم create

```
[root@MohamedAtef ~]# mkfs -t xfs /dev/myvg01/lv01-xfs
[root@MohamedAtef ~]# mkfs -t ext4 /dev/myvg01/lv02-ext4
[root@MohamedAtef ~]# mkswap /dev/myvg01/lv0-swap
```

وبعد كده هنعمل create ل file system علي كل LV

هنا عملنا create ل xfs file system علي اول LV

هنا عملنا create ل ext file system علي تاني LV

هنا عملنا create ل swap file system علي تالت LV

```
[root@MohamedAtef ~]# mkdir /lv01-xfs
[root@MohamedAtef ~]# mount /dev/myvg01/lv01-xfs /lv01-xfs/
[root@MohamedAtef ~]# mkdir /lv01-ext4
[root@MohamedAtef ~]# mount /dev/myvg01/lv01-ext4 /lv01-ext4
[root@MohamedAtef ~]# swapon /dev/myvg01/lv01-swap
```

بعد كده هنعمل mount ف هنعمل directory تحت ال / اسمه lv01-xfs علشان نعمل mount لل LV الاول تحتيه وبعد كده هنعمل directory تاني تحت ال / اسمه lv01-ext4 علشان نعملmount لل LV التاني تحتيه

اما بالنسبه لل swap ف هنعمله activate

➢ احنا كده عملنا create ل 3 Logical Volume تعال نشوف ازاي نعمل extend

- احنا قولنا ان ال extend لل normal file systems بتكون now down time is needed يعني مبحتجش اني اعمل unmount لل file system . ولكن في حاله ال swap لو انت عايز تعمله extend لازم تعمل الاول deactivate لل swap وتروح تعملها extend وبعدين ترجع تعملها activate تاني ف تعال نعمل اول extend معانا وهو ال extend xfs file system

1- Extend XFS File System

➢ تعال كده قبل اما نعمل extend نشوف ال LV اللي احنا عملناها باستخدام امر df -h

```
root@MohamedAtef ~]# df -h
Filesystem                      Size  Used Avail Use%  Mounted on
/dev/nvme0n1p2                  20G    5.6G  15G  28%   /
/dev/nvme0n1p1                  507M  249M  259M  49% /boot
/dev/nvme0n1p3                  20G    179M  20G  1%   /home
/dev/mapper/myvg01-lv01--xfs    2.0G  47M  2.0G  3%    /lv01-xfs
/dev/mapper/myvg01-lv01--ext4   2.0G  24K  1.8G  1%    /lv01-ext4
```

هنلاحظ هنا ال LV اللي عملنالهم create وكل واحد فيهم مساحته 2G

➢ لازم نعمل display لل VG علشان نتاكد هل فيه مساحه فاضيه اقدر استخدمها اني اعمل extend ولا لا

```
[root@MohamedAtef ~]# vgdisplay
  --- Volume group ---
  VG Name               myvg01
  System ID
  Format                lvm2
  MAX LV                0
  Cur LV                3
  Open LV               3
  Max PV                0
  Cur PV                2
  Act PV                2
  VG Size               9.99 GiB
  PE Size               4.00 MiB
  Total PE              2558
  Alloc PE / Size       1536 / 6.00 GiB
  Free  PE / Size       1022 / 3.99 GiB
  VG UUID               iNovXf-31Lh-RXvJ-aWFR-3TXu-JWeE-BQvt4o
```

هنلاحظ هنا المساحه ال free حوالي 4G ف انا اقدر اعمل extend

➢ هنعمل extend لل logical Volume الاولاني lv01 الخاص ب xfs هنزود عليه 2G

➢ علشان اعمل extend للLV هقوله **lvextend** وبعدين احددله ال LV اللي عايز اعمله extend وهو /dev/myvg01/lv01-xfs وبعد كده اوبشن -L واديله ال size اللي عايز اضيفه ف احنا هنضيف 2G

```
[root@MohamedAtef ~]# lvextend   /dev/myvg01/lv01-xfs   -L   +2G
  Size of logical volume myvg01/lv01-xfs changed from 2.00 GiB (512 extents) to 4.00 GiB (1024 extents).
  Logical volume myvg01/lv01-xfs successfully resized.
```

بيقولك هنا ان ال مساحه ال LV ذات من 2G ل 4G

➢ لو جينا عملنا df -h علشان نشوف مساحه ال LV هل اصبحت 4G ولا لا هنلاقيها لسه المساحه زي ماهي 2G ف كده فاضل خطوه علشان ال file system يحس بال size الجديد ويعمل update هستخدم في حاله لو انا مستخدم xfs file system امر xfs_growfs وبعد كده ال LV

```
[root@MohamedAtef ~]# xfs_growfs   /dev/myvg01/lv01-xfs
```

2- Ext4 File System

- هنعمل extend ل LV رقم 2 الخاص ب ext4 بس لو جينا نشوف فيه مساحه فاضيه ولا لا في ال VG هنلاقي ان مفيش مساحه تسمحلي اني اعمل extend ل 2G لان المساحه اقل من 2G
- هنعمل display ل VG علشان نشوف ال size

```
[root@MohamedAtef ~]# vgdisplay
  --- Volume group ---
  VG Name               myvg01
  Alloc PE / Size       2048 / 8.00 GiB
  Free  PE / Size       510 / 1.99 GiB
  VG UUID               iNovXf-31Lh-RXvJ-aWFR-3TXu-JWeE-BQvt4o
```

هنلاقي مساحه ال VG اقل من ال 2 جيجا اللي انا محتاجهم علشان اعمل extend ف الحل ان انا ازود مساحه ال VG عن طريق اني اضيف disk كمان في ال VG

- ف احنا ف الاول هنعمل extend ل VG عن طريق ان احنا هناخد Hard Disk مالي موجودين ونعمله PV وبعد كده نعمل extend ل ال VG
- هنشوف الDisks اللي عندي ونختار Disk منهم

```
[root@MohamedAtef ~]# lsblk
NAME            MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
nvme0n2         259:6    0    5G  0 disk
├─myvg01-lv01--xfs  253:0    0    4G  0 lvm  /lv01-xfs
└─myvg01-lv02--ext4 253:1    0    2G  0 lvm  /lv02-ext4
nvme0n3         259:7    0    5G  0 disk
├─myvg01-lv01--xfs  253:0    0    4G  0 lvm  /lv01-xfs
└─myvg01-lv03--swap 253:2    0    2G  0 lvm  [SWAP]
nvme0n4         259:8    0    5G  0 disk
nvme0n5         259:9    0    5G  0 disk
```

هنلاحظ هنا هنلاقي عندي Two Disks رقم 4 و 5 مش مستخدمين ف احنا هنختار اي Disk منهم ف احنا هشتغل علي ال Disk ده nvme0n4

- هنعمل PV ل nvme0n4

```
[root@MohamedAtef ~]# pvcreate /dev/nvme0n4
  Physical volume "/dev/nvme0n4" successfully created.
```

- بعد كده اعمل extend لل VG عن طريق ان انا احددله ال VG بتاعي وبعدين ال PV

```
[root@MohamedAtef ~]# vgextend myvg01  /dev/nvme0n4
  Volume group "myvg01" successfully extended
```

- لو جينا نشوف حجم ال VG هنلاقيه اتعمله extend ل تقريبا 7G

```
[root@MohamedAtef ~]# vgdisplay
VG Size               <14.99 GiB
  PE Size               4.00 MiB
  Total PE              3837
  Alloc PE / Size       2048 / 8.00 GiB
  Free  PE / Size       1789 / <6.99 GiB
  VG UUID               iNovXf-31Lh-RXvJ-aWFR-3TXu-JWeE-BQvt4o
```

هنلاقي هنا ال size بقي 6.99 يعني حوالي 7 جيجا

- احنا كده جاهزين اننا نعمل extend لل LV وزي ماقولنا ان طالما ال LV معمول باي file system تاني غير ال xfs ف هنستخدم الامر lvextend مع اوبشن r- علشان يعمل extend ويعمل update في نفس الوقت

```
[root@MohamedAtef ~]# lvextend -r -L +2G /dev/myvg01/lv02-ext4
  Size of logical volume myvg01/lv01-ext4 changed from 2.00 GiB (512 extents) to 4.00 GiB (1024 extents).
```

3- Swap Space in Logical Volume

- اخر حاجه هنعمل extend لل swap logical volume
- هنعمل اول حاجه deactivate لل swap

```
[root@MohamedAtef ~]# swapoff  /dev/myvg01/lv01-swap
```

- وبعدين هنعمل mount -a علشان نشوف حصل تغيير ولا لا في حجم ال swap

```
[root@MohamedAtef ~]# free  -m
              total        used        free      shared  buff/cache   available
Mem:            936         733          70           5         284         203
Swap:          2047         152        1895
```

هنلاقي هنا ال size 2047M

- بعد كده هنعمل extend لل swap logical volume

```
[root@MohamedAtef ~]# lvextend  /dev/myvg01/lv01-swap  -L  +1G
  Size of logical volume myvg01/lv01-swap changed from 2.00 GiB (512 extents) to 3.00 GiB (768 extents).
  Logical volume myvg01/lv01-swap successfully resized.
```

- بعد كده هنعمل mkswap علشان يعمل format ويحس بال change

```
[root@MohamedAtef ~]# mkswap  /dev/myvg01/lv01-swap
mkswap: /dev/myvg01/lv01-swap: warning: wiping old swap signature.
Setting up swapspace version 1, size = 3 GiB (3221221376 bytes)
no label, UUID=44a2bba3-0bbb-4d2f-ac5f-4fa1912614a5
```

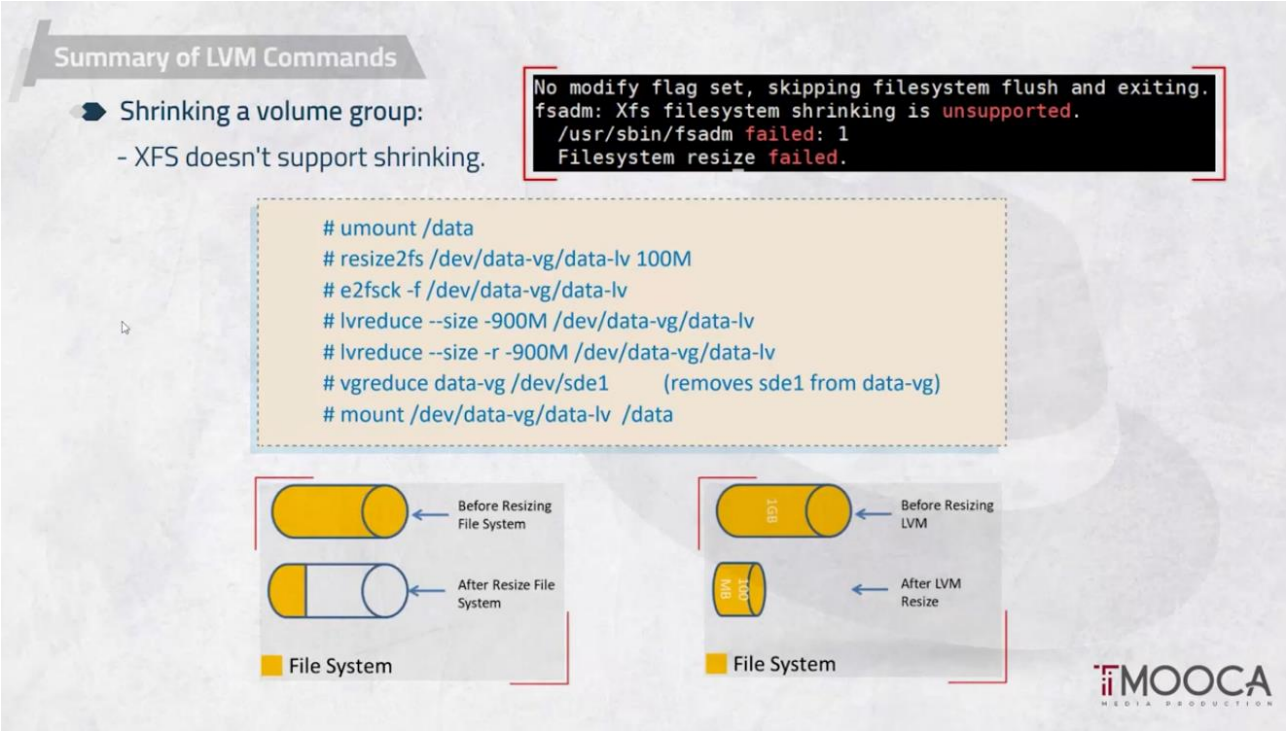
- بعد كده هنعمل activating باستخدام swapon

```
[root@MohamedAtef ~]# swapon  /dev/myvg01/lv01-swap
```

- كده احنا عملنا extend لل swap وعلشان نتاكد هنستخدم mount -a علشان نشوف حجم ال swap

```
[root@MohamedAtef ~]# free -m
              total        used        free      shared  buff/cache   available
Mem:            936         733          70           5         284         203
Swap:          5119         152        4967
```

Shrinking a volume group



- في حاله ال shrinking لو انت عايز تعمل reduce ل Logical Volume لازم تعمل unmount لل Logical Volume يعني في حاله ال reduce او shrinking ال down time is needed وكمان XFS File System مبيدعمش ال shrinking يعني لو انت عندك Logical Volume وانت عامل لل Logical Volume ده create او format بال XFS file system انت مش هتعرف تعمل reduce لل Logical Volume
- ال steps اللي المفروض اعملها علشان اعمل reduce

1- تعمل umount لل logical volume باستخدام امر umount

```
Umount /data
```

2- وبعد كده تعمل reduce لل file system عن طريق انك تقوله resize2fs وبعد كده تديله اسم ال LV وبعد كده تديله ال new size اهم حاجه تخلي بالك وانت بتنفذ ال command ده علشان لو فيه اي مشكله في ال command ممكن تفقد الداتا اللي علي ال LV ف خلي بالك

```
resize2fs /dev/data-vg/data-lv 100M
```

3- وبعد كده تعمل check هل السيستم ده corrupted ولالا عن طريق اني استخدم e2fsck -f وبعد كده اسم ال LV

```
e2fsck -f /dev/data-vg/data-lv
```

4- وبعد كده بت reduce ال size بتاع ال LV باستخدام ال lvreduce وبعدين --size او ممكن بدل ال --size احط -L وبعدين احددله ال size اللي انا عايز اطرحه وليكن -900M خلي بالك انا حطيت – علشان انا هنا بعمل reduce لما كنا بنعمل extend كنا بنحط + وبعد كده ال LV

```
lvreduce --size -900M /dev/data-vg/data-lv
```

5- فيه طريقه افضل واحسن ان انا ممكن ا reduce ال file system وال size في خطوه واحده وفي نفس الوقت يعني ممكن اعمل من اول مره الخطوه رقم 2 و 4 في command واحد عن طريق ان انا ازود اوبشن r- في الخطوه رقم 4

```
lvreduce –size  -r  -900M /dev/data-vg/data-lv
```

6- بعد كده لو انت عايز ت remove ال PV من ال VG هستخدم

```
vgreduce  data-vg  /dev/sde1
```

7- اخر خطوه تعمل تاني mount لل LV تحت ال directory اللي كنت عامل mount فيه

```
mount  /dev/data-vg/data-lv  /data
```

- **تعال نطبق اللي شرحناه**

➢ هنعمل reduce ل LV اللي موجود عليه xfs file system ونشوف هينفع نعمله reduce ولا لا احنا عارفين ان ال shrinking مبيدعمش ال xfs بس احنا هنجرب ونشوف شكل ال error

➢ اول خطوه هنعمل umount لل LV اللي موجود عليه xfs file system

```
[root@MohamedAtef ~]# umount  /lv01-xfs
```

➢ بعد كده هنعمل reduce ف زي مقولنا ان الافضل انك تستخدم ال command اللي تقدر من خلاله انك تعمل reduce ل file system وال size في خطوه واحده ف هنستخدم

```
[root@MohamedAtef ~]# lvreduce -r -L -2G /dev/myvg01/lv01-xfs
  File system xfs found on myvg01/lv01-xfs.
  File system size (4.00 GiB) is larger than the requested size (2.00 GiB).
  File system reduce is required and not supported (xfs).
```

زي مظهر معانا ان قالك ال xfs not supported

➢ هنعمل reduce ل LV باستخدام file system مختلف وليكن ext4

➢ هنعمل umount لل LV اللي موجود عليه ext4 file system

```
[root@MohamedAtef ~]# umount   /lv02-ext4
```

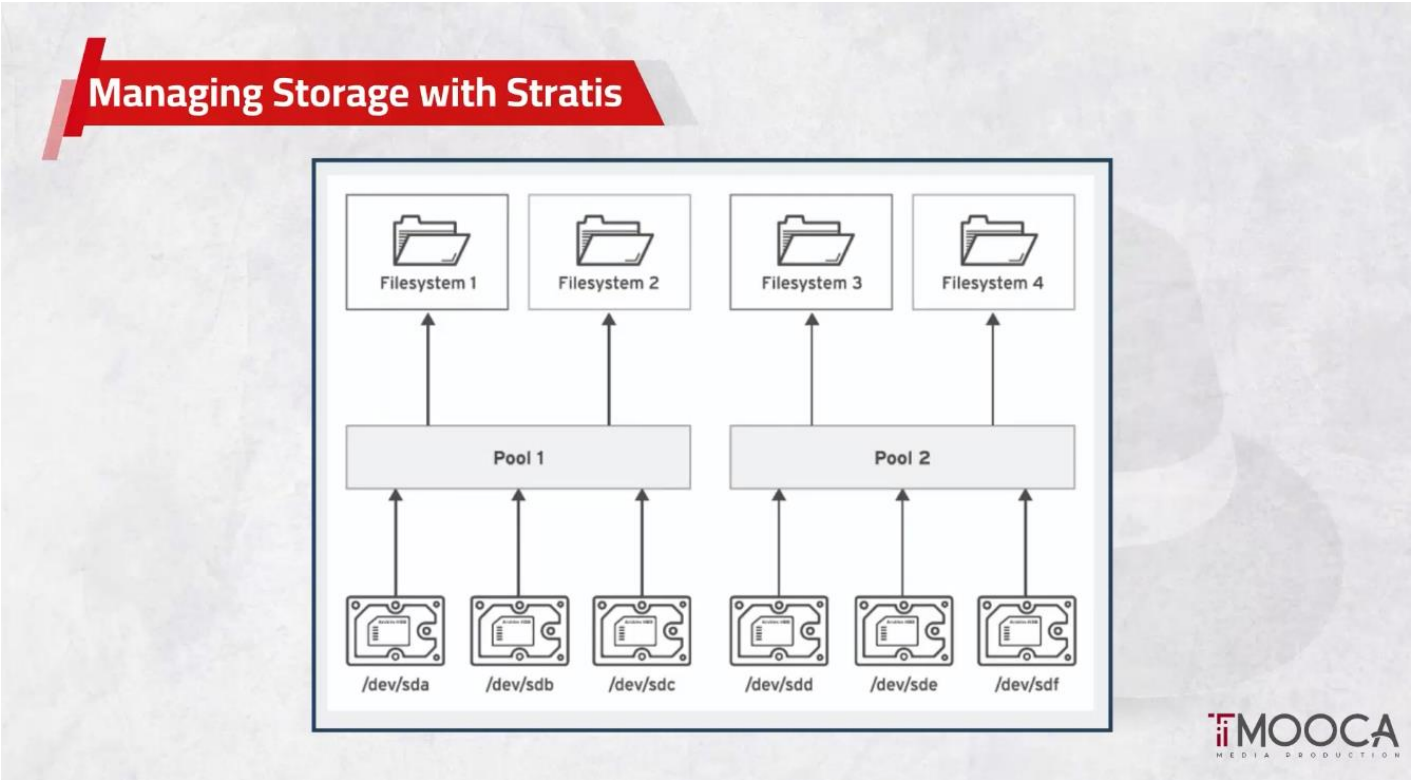
➢ بعد كده هنعمل reduce

```
[root@MohamedAtef ~]# lvreduce -r -L -2G /dev/myvg01/lv02-ext4
  File system ext4 found on myvg01/lv01-ext4.
  File system size (4.00 GiB) is larger than the requested size (2.00 GiB).
  File system reduce is required using resize2fs.
  File system fsck will be run before reduce.
  Reducing file system ext4 to 2.00 GiB (2147483648 bytes) on myvg01/lv01-ext4...

resize2fs done
  Reduced file system ext4 on myvg01/lv02-ext4.
  Size of logical volume myvg01/lv02-ext4 changed from 4.00 GiB (1024 extents) to 2.00 GiB (512 extents).
  Logical volume myvg01/lv02-ext4 successfully resized.
```

➢ اخر step هنعمل mount تاني لل LV

```
[root@MohamedAtef ~]# mount /dev/myvg01/lv01-ext4 /lv01-ext4
```

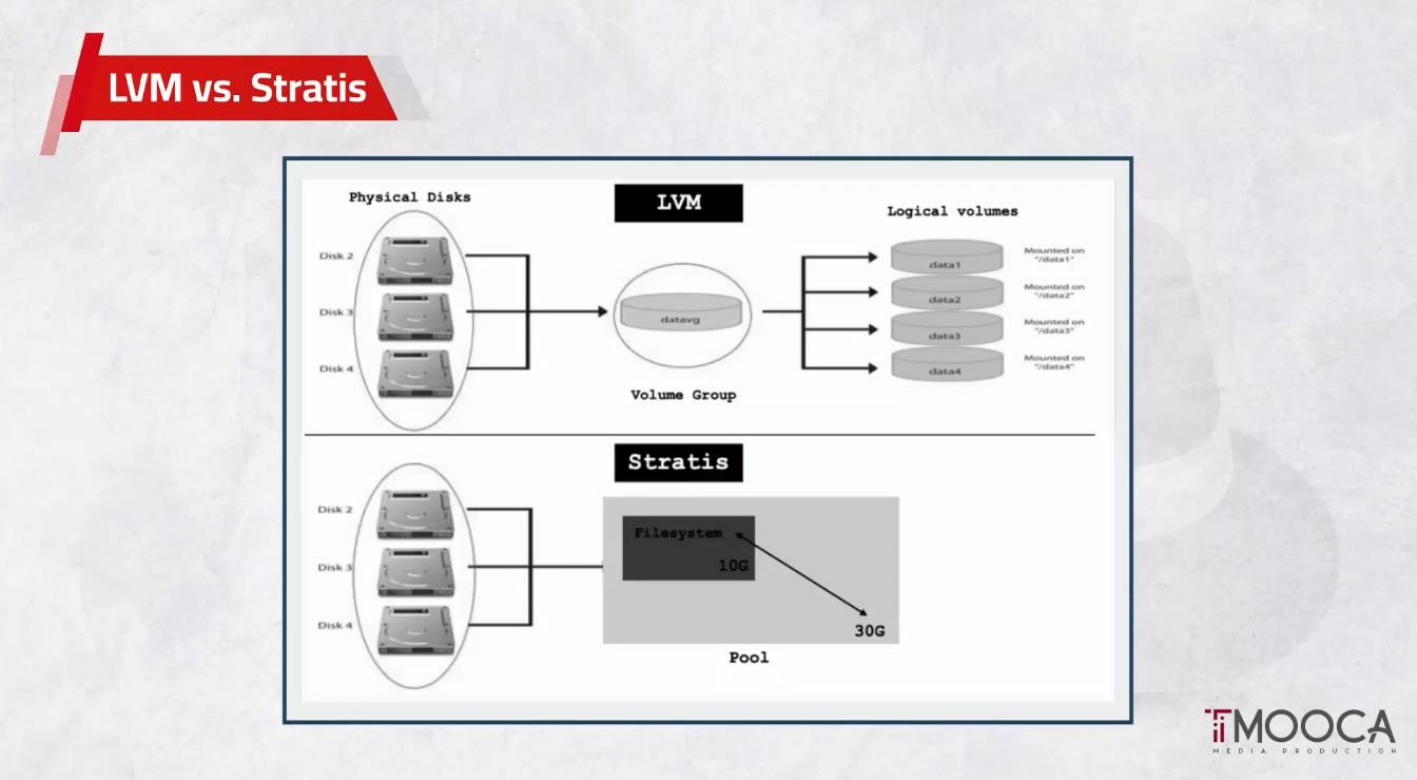
Chapter 8
Implementing Advanced Storage Features



- ببساطه ال **Stratis** عباره عن service بتبقي not install احنا بنعملها install باستخدام dnf وبنستخدمها علشان ن manage بيها ال Local storage devices عن طريق ان انا ب create pool من مجموعه من ال block devices المختلفه وال block devices دي ممكن تبقي hard drives بانوعها ممكن تبقي partitions ممكن تبقي RAID array او SAN Disk وال pool size بيكون equal للtotal size بتاع ال block devices اللي member فيها او allocated فيها
- Once انك عملت create ل Stratis pool تقدر من خلالها انك ت create file system او مجموعه من ال file system المختلفه و ممكن ت create اكتر من pool علي نفس ال system بتاعك باستخدام deferent block devices
- يعني عندك في المثال اللي فوق عملت create لل Stratis pool 1 من ال block devices دي /dev/sda و /dev/sdb و /dev/sdc وعملت create لل Stratis pool 2 من ال block devices دي/dev/sdd و /dev/sde و /dev/sdf ومن pool1 عملت create ل file system 1 و file system 2 ومن pool 2 عملت create ل file system 3 و file system 4

- **فيه عندي كذا ميزه لل Stratis**

- اول حاجه انه شغال ب concept اسمه Thin Provisioning يعني وانت بت create ال file system هو بي allocate ال space ل file system بتاعتك بطريقه dynamic مش بي allocate fixed size لل file system يعني كل اما تضيف more data لل file system بتاعك هو بي extend ال file system لو احتاج
- تاني ميزه ان انت بمجرد انك عملت create لل file system باستخدام ال Stratis هو بي format ال file system بطريقه dynamic بال XFS من غير مانت تعمل format
- تالت ميزه انه بي support ال snapshots انك ت create snapshot من ال file system المختلفه وبنستخدمها في حاله ال Backup and recovery operation



- **الفرق مابين ال LVM وال Stratis**

- الاتنين عباره عن storage management solutions وكل نوع ليه مميزاته وانت ك سيستم ادمن بتختار اي نوع based علي ال use cases بتاعتك. بس دايما هتلاقي ال Stratis اسهل في التعامل وال setup بتاعه مقارنتا بال LVM. ان ال setup بتاعة ال LVM بتكون more complex وفيه layers و steps كتير يعني في ال LVM علشان نعمل create ل LV كنا بنعمل create ل PV وبعدين VG وبعدين LV وبعدين نعمل format باستخدام file system وبعدين نعمل mount ف هنلاقي فيه steps كتير جدا بنعملها علشان نcreate ل LV علي عكس ال Stratis ان ال setup وال layers بتاعته قليله جدا انت بيبقي عندك ال physical devices بتاعتك وبتعمل create منهم ل Stratis pool ومن ال pool دي بت create علي طول file system وزي ماقولنا ان ال file system بتبقي شغاله في ال Stratis ب concept ال Thin Provisioning
- ال steps اللي بنعملها في ال LVM علشان نعمل create ل file system بتكون manual يعني انت اللي بتعملها ب ايدك في ال Stratis هو اللي بي format ال file system بتاعك بال XFS
- بالنسبه لل snapshot الاتنين بي support ال snapshot

➢ Removing a Logical Volume

- زي ماقولنا ال stratis service بتبقي not installed by default ف لازم علشان نستخدمها نعملها الاول installعلشان نعمل install عندنا two packages
  1- عندي package اسمها Stratis-cli ودي بت provide ال command line اللي هتعامل بيه مع ال Stratis service
  2- ال package التانيه اسمها stratisd ودي ال service بتاعت ال Stratis ذات نفسها

➢ Installing and Enabling Stratis

- هعمل install عن طريق ان انا هقوله yum او dnf واديله ال two packages اللي انا هعملهمinstall

```
[root@server~]# yum install stratis-cli stratisd
```

- بعد اما اعمل Install بعمل enable و start للسيرفز الخاصه بال stratisd

```
[root@server~]# systemctl enable --now stratisd
```

➢ Assmbling Block Storage into Stratis Pools

- اول step بعملها علشان اعمل create ل file system باستخدام ال stratis اول حاجه بعمل create pool علشان اعمل pool بستخدم command اسمه stratis pool create وبعد كده بديله اسم ال pool وليكن pool1 واحط فيها ال physical devices اللي اسمه مثلا /dev/vdb

```
[root@server~]# stratis pool create pool1 /dev/vdb
```

- علشان اعمل list ل more details عن ال pool بتاعتي بقوله stratis pool list

```
[root@server~]# stratis pool list
```

- لو انا عايز اعمل add new block devices لل pool هقوله stratis pool add-data بعد كده اديله اسم ال pool وبعد كده أ add new block device

```
[root@server~]# stratis pool add-data pool1 /dev/vdc
```

- لو انا عايز اعمل list لل block devices ال member في pool معينه هقوله stratis blockdev list وبعد كده اسم ال pool اللي عايز اعمل List ليها

```
[root@server~]# stratis blockdev list pool1
```

➢ Managing Stratis File Systems

- بمجرد ان انا عملت create لل pool ال step اللي بعد كده ان انا اعمل create file system ف بقوله stratis file system create وبعدين اديله اسم ال pool وبعد كده اديله اسم ال file system اللي هنعمله create

```
[root@server~]# stratis filesystem create pool1 fs1
```

- علشان اعمل list لكل ال available stratis file system ال created عندي بقوله stratis filesystem list

```
[root@server~]# stratis filesystem list
```

- علشان اعمل create ل snapshot هقوله stratis filesystem snapshot وبعد كده اديله اسم ال pool اللي جواها ال file system ف هقوله مثلا pool1 fs1 وبعد كده اسم ال snapshot بتاعتي

```
[root@server~]# stratis filesystem snapshot pool1 fs1 snapshot1
```

➢ Persistently Mounting Stratis File Systems

- اخر step زي ماقولنا ان انا بعمل mount لل file system علشان ابدا استخدمه وعلشان اخلي ال mount بتاعي يكون permanent بضيف ليه record في /etc/fstab وعلشان اعمل mount في عندي two options ي اما تعمل mount باسم ال file system نفسه او بال path بتاعه او بال UUID عن طريق ان انا هاخد ال UUID واحطه في الfstab file. وعلشان اعمل display لل UUID ممكن اقوله lsblk --output=UUID وبعد كده اديله ال path بتاع ال file system

```
[root@server~]# lsblk --output=UUID /stratis/pool1/fs1
```

- فيه عندي ملاحظه مهمه جدا وانا بضيف ال record في ال fstab file لازم تاخد بالك منها انك بعد ال default تقوله comma , وبعد كده تزود الاوبشن ده x-systemd.requires=stratisd.service

```
UUID=31b9363b-add8-4b46-a4bf-c199cd478c55 /dir1 xfs defaults,xsystemd.requires=stratisd.service 0 0
```

- طب ايه معني الاوبشن ده x-systemd.requires=stratisd.service معناه ان السيستم بتاعك وهو بي boot up بيروح يعمل mount لكل ال record الموجوده في ال fstab file ف انت كانك بتقوله متعملش mount لل record او ال file system ده لحد اما ال systemd تقوم ال stratis service لان لو محطتش ال record ده هيحصل مشكله والسيستم بيشتغل

- تعال نشوف ازاي نعمل install لل stratis service لو انت مش عارف اسم ال package ممكن تستخدم yum او dnf علشان تعمل serach عن ال package عن طريق انك هتقوله dnf search stratis

```
[root@MohamedAtef ~]# dnf search stratis
Last metadata expiration check: 6 days, 10:44:47 ago on Fri 14 Jun 2024 08:54:22 PM EET.
============================== Name & Summary Matched: stratis ==============================
stratis-cli.noarch : Command-line tool for interacting with the Stratis daemon
stratisd-dracut.x86_64 : Dracut modules for use with stratisd
============================== Name Matched: stratis ==============================
stratisd.x86_64 : Daemon that manages block devices to create filesystems
```

طب احنا هنعمل install ل انهي package هنعمل ل ال stratis-cli و stratisd

1- هنعمل install ل two packages

```
[root@MohamedAtef ~]# dnf  install  stratis-cli  stratisd
```

2- ال step اللي بعد كده اننا نعمل start و enable لل Package علشان نبدا نستخدمهم ونشوف ال status بعد اما نعمل enable

```
[root@MohamedAtef ~]#  systemctl  enable  --now  stratisd
[root@MohamedAtef ~]#  systemctl status stratisd
● stratisd.service - Stratis daemon
   Loaded: loaded (/usr/lib/systemd/system/stratisd.service; enabled; preset: enabled)
   Active: active (running) since Fri 2024-06-21 07:35:42 EET; 32min ago
     Docs: man:stratisd(8)
```

3- احنا كده جاهزين اننا نعمل create ل stratis pool وال file systems

- تعال نشوف ال block devices اللي هنشتغل عليهم

```
[root@MohamedAtef ~]# lsblk -p
NAME          MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
/dev/nvme0n2    259:6    0    5G  0 disk
/dev/nvme0n3    259:7    0    5G  0 disk
/dev/nvme0n4    259:8    0    5G  0 disk
/dev/nvme0n5    259:9    0    5G  0 disk
```

عندي هنا 4 block devices كل واحد فيهم مساحته 5 جيجا دول اللي هنستخدمهم

- هنعمل create لل stratis pool اسمها stratispool1 زي مشرحنا قبل كده

```
[root@MohamedAtef ~]# stratis  pool  create  stratispool1  /dev/nvme0n2
```

ده ال command اللي هستخدمه علشان اعمل create

بعد كده بديله اسم ال stratis pool اللي عايزين نعمله create احنا هنا في المثال هنستخدم اسم strtispool1

بعد كده بحددله ال blook devices اللي هضيفها في ال pool اللي احنا هنعملها اللي هي stratispool1 ف احنا هنضيف ال block رقم 2 في ال stratispool1

- مساحه ال stratispool1 هي نفسها مساحه الblock device اللي موجوده فيها
- هنعمل list لل stratis pool

```
[root@MohamedAtef ~]# stratis pool list
Name            Total / Used / Free          Properties        UUID                                  Alerts
stratispool1    5 GiB / 524.81 MiB / 4.49 GiB   ~Ca,~Cr, Op    2dc175ff-02e1-4c44-8b7d-8113f4ab2a38   WS001
```

قايلك هنا ان عند stratis pool اسمها stratispool1 ومساحتها 5 GiB

4- هنعمل add ل new block devices ل stratis pool

```
[root@MohamedAtef ~]# stratis  pool  add-data  stratispool1  /dev/nvme0n3
```

➢ لو عملنا list لل stratis pool

```
[root@MohamedAtef ~]# stratis  pool  list
Name              Total / Used / Free    Properties                    UUID                                  Alerts
stratispool1   10 GiB / 531.37 MiB / 9.48 GiB   ~Ca,~Cr, Op    2dc175ff-02e1-4c44-8b7d-8113f4ab2a38      WS001
```

هتلاقي مساحه stratispool اصبحت بدل مكانت 5GiB بقت 10GiB لان انت بقي عندك 2 block devices في ال stratispool1

➢ لو انا عايز اعمل List ل كل ال block devices ال member من ال pool

```
[root@MohamedAtef ~]# stratis blockdev list
Pool Name      Device Node    Physical Size   Tier
stratispool1   /dev/nvme0n2        5 GiB      DATA
stratispool1   /dev/nvme0n3        5 GiB      DATA
```

هتلاقي عندك two block devices والاتنين member من ال pool الي اسمها stratispool1

➢ لو انا عندي اكتر من pool وعايز اعمل List ل pool معينه هستخدم نفس ال commandواديله اسم ال pool

```
[root@MohamedAtef ~]# stratis blockdev list  stratispool1
```

5- بعد كده هنعمل create ل Thin Provisioning file system باستخدام ال stratis

```
[root@MohamedAtef ~]# stratis  filesystem  create  stratispool1   stratis-filesystem1
```

➢ لو انا عايز اعمل create ل اكتر من file system عادي مفيش اي مشكله هستخدم نفس ال command

➢ لو عايز أ check و list ال file system

```
root@MohamedAtef ~]# stratis filesystem list
Pool          Filesystem          Total / Used / Free          Created          Device                                UUID
stratispool1   stratis-filesystem1   1 TiB / 546 MiB / 1023.47 GiB   Jun 21 2024 10:41
/dev/stratis/stratispool1/stratis-filesystem1   dfc34f29-a7d7-45bb-8eca-6e97e2ebabb9
```

➢ احنا كده عملنا create لل file system علشان نبدا بعد كده نستخدمه لازم تعمله mount

6- هنعمل create ل Directory تحت ال / بنفس اسم ال file system

```
[root@MohamedAtef ~]#  mkdir /stratis-filesystem1
```

7- هنعمل mount لل file system

```
[root@MohamedAtef ~]# mount  /dev/stratis/stratispool1/stratis-filesystem1  /stratis-filesystem1
```

By default اول اما تعمل create ل اي pool هتلاقي تحت /dev فيه folder اسمه stratis هتلاقيه عمل create جواه ل directory باسم ال pool بتاعتك وحط جواهم ال file systems اللي انت عملتلها create

➢ لو عملنا df -h

```
[root@MohamedAtef ~]# df -h
Filesystem                                                  Size  Used  Avail  Use%   Mounted on
/dev/mapper/stratis-1-2dc175ff8b72a38-thin-fs-dfc34f29ae2ebabb9   1.0T   7.2G   1017G   1%   /stratis-filesystem1
```

هتلاقيه هنا عمل mount بس خد بالك من حاجه لو جيت بصيت علي Size هتلاقيه 1 تيرا بايت واحنا كنا عملين ال pool ب 10 طب ايه ال 1 تيرا دي معانها ان انت معندكش fixed size هو هنا بي allocate ال size بتاعك بصوره dynamic ف انت تجاهل خالص ال 1 تيرا اللي بتظهرلك لو انت عايز تعرف ال size الفعلي فيه عندي two command ي اما تستخدم stratis pool ي اما تستخدم stratis filesystem

8- اخر step معانا ان احنا نخلي ال mount بتاعنا يكون permanent وده عن طريق ان احنا هنضيف record جوه ال fstab file باستخدم ال UUID

- علشان اجيب ال UUID ممكن استخدم اكتر من command ممكن استخدم stratis filesystem وممكن استخدم lsblk فقط . الافضل اننا نستخدم ال command ده ان انا اقوله lsblk وبعد كده بقوله انا عايز ال output يكون UUID بس وبعد كده اديله ال path الخاص بال file system

```
[root@MohamedAtef ~]# lsblk  --output=UUID  /dev/stratis/stratispool1/stratis-filesystem1
UUID
dfc34f29-a7d7-45bb-8eca-6e97e2ebabb9
```

- هفتح ملف fstab وابدا اكتب جواه ال record

```
[root@MohamedAtef ~]# vim fstab
UUID=dfc34f29-a7d7-45bb-8eca-6e97e2ebabb9  /stratis-filesystem1  xfs  defaults,x-systemd.requires=stratisd.service 0 0
```

اول حاجه بنكتب الUUID او ال path الخاص بال file system

تاني حاجه بنكتب ال mounting point

تالت حاجه بنكتب ال file system وال stratis بي support ال xfs file system

رابع حاجه بنكتب الاوبشن ده زي ماهو بالنص مابين ال defaults وباقي الاوبشن فيه علامه coma ,
defaults,x-systemd.requires=stratisd.service

- طالما عملنا تعديل في ال fstab لازم نعمل reload علشان السيستم يحس بالتتغير

```
[root@MohamedAtef ~]# systemctl daemon-reload
```

- علشان نتاكد ان السيستم بتاعك هيعمل mount بعد اما تعمل reboot automatic للfile system لازم تعمل reboot لل machine بتاعتك

- تعال نبدأ ن access ال file system اللي عملنا ليه create اللي ال type بتاعها Thin Provision ونشوف هل لو احنا عملنا create لاي new data هل ال size بتاعت ال file system دي هيتعمله extend بطريقه dynamic ولا لا . تعال نعمل الاول list لل file system اللي عندنا هنلاقي ال file system ال size ال used عليه حوالي 546MiB

```
root@MohamedAtef ~]# stratis filesystem list
Pool        Filesystem              Total / Used / Free        Created        Device                    UUID
stratispool1   stratis-filesystem1   1 TiB / 546 MiB / 1023.47 GiB   Jun 21 2024 10:41
/dev/stratis/stratispool1/stratis-filesystem1   dfc34f29-a7d7-45bb-8eca-6e97e2ebabb9
```

- هنعمل create ل اي file جوه ال file system هندخل تحت مسار ال mount ده stratis-filesystem1 علشان نعمل create ل اي file

```
[root@MohamedAtef ~]# cd /stratis-filesystem1
[root@MohamedAtef stratis-filesystem1]# echo "Hello World!" >file1
[root@MohamedAtef stratis-filesystem1]# dd if=/dev/urandom of=file2 bs=1M count=1024
1024+0 records in
1024+0 records out
1073741824 bytes (1.1 GB, 1.0 GiB) copied, 10.9872 s, 97.7 M
```

هدخل تحت ال stratis-filesystem1 / ونعمل create ل ملفين

هنعمل file ونكتب جواه Hello world

هنعمل create ل file باستخدام ال command ده ميزه ال command ده انه بيعمل create ل file بمساحه كبيره بمعني انا بقوله انا عايز اعمل create ل file2 ال size بتاعه 1G ف ال command ده هيفضل ياخد random values من ال special file ده / dev/urandom يقعد يملي بيها file2 لحد اما ال size بتاعه يكون 1G

- لو جينا شوفنا حجم ال file system بعد اما ضفنا فيه ال files

```
root@MohamedAtef ~]# stratis filesystem list
Pool        Filesystem              Total / Used / Free        Created        Device                    UUID
stratispool1   stratis-filesystem1   1 TiB / 1.53 GiB/ 1023.47 GiB   Jun 21 2024 10:41  /dev/stratis/stratispool1/stratis-filesystem1   dfc34f29-a7d7-45bb-8eca-6e97e2ebabb9
```

هنلاقي هنا بصوره automatic ال file system اتعمله grow up للsize بتاعه

Create Snapshot of file system

- زي مقولنا ال snapshot عباره عن at specific point in time بتاخد copy من اللي موجود في ال filesystem وت create منه snapshot وقولنا ال snapshot بتستخدم في حاله ال backup وال recovery operations لو انت ال file system حصل فيه مشكله لاي سبب تقدر انك ترجع للstatus اللي انت كنت فيها او ت restore
- هنشوف ازاي ن create snapshot لل file system

➢ علشان اعمل create لل snapshot بقوله stratis filesystem snapshot وبعدين اديله اسم ال pool وبعدين اسم ال file system اللي هاخد منه ال snapshot وبعد كده اسم ال snapshot

```
[root@MohamedAtef ~]# stratis filesystem snapshot  stratispool1  stratis-filesystem1  stratis-filesystem1-snap
```

ال command اللي هستخدمه لعمل ال snapshot

اسم ال pool اللي موجود فيها ال filesystem اللي هاخد منه snapshot

اسم ال filesystem اللي هاخد منه snapshot

اسم ال snapshot اللي انت عايزه اي اسم عادي

➢ احنا كده عملنا snapshot لل stratis-filesystem1

➢ لو جينا احنا مسحنا اي file موجود في ال file system ونشوف هل فعلا الfile ده اقدر اعمله restore

➢ احنا كنا عاملين create ل file1 و file2 احنا هنمسح file1 وهنعمل mount لل snapshot اللي لسه عاملينه ونشوف هل موجود file2 ولالا

```
[root@MohamedAtef stratis-filesystem1]# rm -f file1
```

عملت remove ل file1 من ال file system

```
[root@MohamedAtef stratis-filesystem1]# ls
file2
```

بعد اما عملت ls هتلاقي file واحد بس وهو file2

بعد كده عملنا directory علشان نعمل mount لل snapshot

```
[root@MohamedAtef stratis-filesystem1]# mkdir  /stratis-filesystem1-snap
```

بعد كده عملنا mount لل snapshot

```
[root@MohamedAtef stratis-filesystem1]# mount  /dev/stratis/stratispool1/stratis-filesystem1-snap  /stratis-filesystem1-snap
```

بعد اما عملنا mount هندخل علي ال directory اللي عملنا mount فيه

```
[root@MohamedAtef stratis-filesystem1]# cd /stratis-filesystem1-snap
[root@MohamedAtef stratis-filesystem1-snap]# ls
file1  file2
```

لما نعمل ls ونشوف محتوي ال directory هتلاقي موجود ال files اللي كانت موجوده في ال file system وهتلاقي كمان ال file1 اللي عملناله remove

➢ طب لو انا عندي ال file system حصله corrupted بكل حاجه في الحاله دي هنعمل restore لل file system بالكامل عن طريق ان انا هاخد snapshot من ال snapshot اللي كنا واخدينه بس بنفس اسم ال file system اللي حصله corrupted

Destroy pools

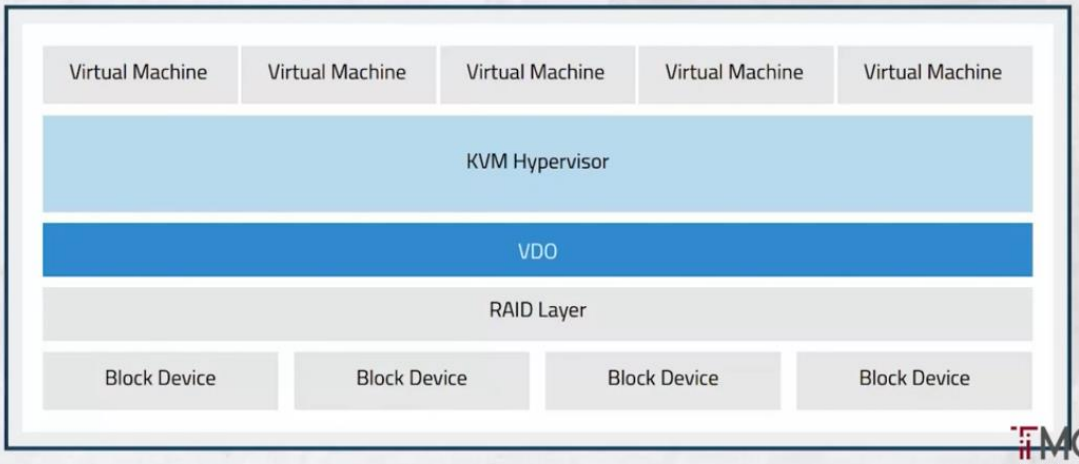
➢ لو انا عايز اعمل destroy لل file system والpool بتاعتي

➢ اول حاجه لازم تعمل umont الاول لل file system قبل ال Destroy وبعد كده بتعمل destroy عن طريق انك تقوله stratis filesystem destroy وبعد كده اسم ال pool وبعدين اسم ال file system اللي هتعمله destroy

```
[root@MohamedAtef ~]# umount  /stratis-filesystem1
[root@MohamedAtef ~]# stratis filesystem destroy stratispool1 stratis-filesystem1
```

Compressing and Deduplicating Storage with VDO

- The Virtual Data Optimizer (VDO) is a storage optimization technology developed by Red Hat. It is designed to reduce storage costs and improve efficiency by using data deduplication and compression techniques. VDO operates at the block level and is primarily used for reducing the amount of storage space required for storing data.



- ال VDO(The Virtual Data Optimizer) عباره عن Storage Optimization Technology الهدف الاساسي انها ت reduce ال storage space اللي انت محتاجها علشان ت store الداتا بتاعتك وتenhace ال performance بتاع ال Storage devices بتاعتك
- يعني من الاخر بتوفرلك في المساحه التخزينيه اللي محتاجها علشان تخزن الدتا بتاعتك وده بيسمحلك انك تخزن داتا كتير علي نفس مساحه التخزين وبيوفرلك في ال cost بتاعت ال storage
- علشان ال VDO ي reduce ال space اللي انت محتاجها علشان ت store الداتا بتاعتك بيعمل 3 حاجات

1- بيعمل Zero Block Elimination يعني لو عندي blocks فيها zeros بيعملها eliminates او remove
2- بمجرد انه عمل Zero Block Elimination تاني حاجه بيعملها Data Compression عنده مجموعه من ال compression algorithms بيعمل compress بيها للداتا بتاعتك قبل اما يعملها store علي ال storage device وده طبعا بيقلل في المساحه التخزينيه اللي انت محتاجها علشان ت store الداتا دي
3- تالت حاجه بيعملها بيعمل Deduplication ان لو عندي كذا copy من الداتا بتاعتي stored علي نفس ال disk هو بي store بس one single instance من الداتا دي

- **ملاحظه مهمه جدا**

➢ ال VDO بيسستخدم في Red Hat 9 مع ال LVM فقط واحنا بنعمل create ل Logical Volume بنستخدم معاه ال VDO
➢ فيه command واحنا بنعمل create مبقاش مستخدم في redhat9 وهو

ال command ده لا يستخدم في Red Hat 9 لعمل create ل VDO

Creating a VDO Volume

- To create a VDO volume, run the **vdo create** command.

```
[root@host ~]# vdo create --name=vdo1 --device=/dev/vdd --vdoLogicalSize=50G
```

Create & Change compression deduplication of VDO

- تعال نشوف ازاي نعمل create لل VDO مع ال LVM

➢ اول حاجه نعمل install ل VDO وعلشان اعمل install لازم عمل install ل Two Packages وهما ال vdo وال kmod-kvdo

```
[root@MohamedAtef ~]# dnf install  vdo   kmod-kvdo
```

➢ احنا قولنا كذا مره ان ال VDO بيستخدم مع الLVM بس

➢ ف احنا هنعمل create ل Physical Volume(PV) وبعدين هنعمل Volume Group(VG)

```
[root@MohamedAtef ~]# pvcreate /dev/nvme0n2 /dev/nvme0n3
  Physical volume "/dev/nvme0n2" successfully created.
  Physical volume "/dev/nvme0n3" successfully created.
[root@MohamedAtef ~]# vgcreate vdo_vg /dev/nvme0n2 /dev/nvme0n3
  Volume group "vdo_vg" successfully created
[root@MohamedAtef ~]# vgs
  VG     #PV #LV #SN Attr   VSize VFree
  vdo_vg   2   0   0 wz--n- 9.99g 9.99g
```

عملنا PV ل Two Disks

وبعد كده عملنا VG وهنسميه مثلا vdo_vg

علشان نتاكد هنعمل display لل VG هنلاقي انه بيقولك ان في 2 PV

➢ الخطوه اللي بعد كده ان احنا نعمل create للLV نوعه VDO ف علشان اعمل create هستخدم ال command التالي

```
[root@MohamedAtef ~]# lvcreate --type vdo  -n  vdo_lv   -l   +100%FREE   vdo_vg
```

اول حاجه بقوله lvcreate

تاني حاجه بحددله ال typeعن طريق ان انا اقوله type- وبعد كده vdo

بعد كده بقوله اوبشن n- علشان اديله اسم ال lv اللي هيكون نوعه vdo ف هسميه vdo_lv

بعد كده بحدد ال size عن طريق ان انا اقوله اوبشن l- وبعدين ال size انا هنا قولتله +100%FREE معناها كاني بقوله روح allocate ال free space اللي موجوده في ال VG اللي اسمه vdo_vg في ال LV ده vdo_lv

➢ كده احنا عملنا create ل LV نوعه VDO

➢ الخطوه اللي بعد كده علشان نبدا نaccess ونستخدم ال LV نعمل create ل file system ونبدأ نستخدمه

```
[root@MohamedAtef ~]#  mkfs -t xfs /dev/vdo_vg/vdo_lv
```

➢ بعد كده هنعمل create ل director اسمه vdo_lv علشان نعمل mount تحتيه

```
[root@MohamedAtef ~]#  mkdir /vdo_lv
[root@MohamedAtef ~]# mount /dev/vdo_vg/vdo_lv /vdo_lv
```

➢ لو عملنا df -h هنلاقيه اتعمله mount

```
[root@MohamedAtef ~]# df -h
Filesystem                 Size   Used  Avail  Use%  Mounted on
devtmpfs                   4.0M   0     4.0M   0%    /dev
tmpfs                      469M   0     469M   0%    /dev/shm
tmpfs                      188M   6.2M  182M   4%    /run
/dev/nvme0n1p2             20G    6.6G  14G    33%   /
/dev/nvme0n1p1             507M   249M  259M   49%   /boot
tmpfs                      1.0M   0     1.0M   0%    /run/stratisd/ns_mounts
/dev/mapper/vdo_vg-vdo_lv  6.0G   75M   6.0G   2%    /vdo_lv
```

هنلاقيه اتعمله Mount تحت /vdo_lv كده اقدر استخدمه

- تعال نجرب نضيف فيه داتا ونشوف تاثير ال VDO علي الداتا دي عامل ازاي
- انا عندي command اسمه vdostats ده بيجبلك ال status بتاعت ال VDO Volume

```
[root@MohamedAtef vdo_lv]# vdostats
Device              1k-blocks     Used Available Use% Space saving%
vdo_vg-vpool0-vpool 10477568   4190664   6286904  40%          98%
```

- لو انا عايزه يجبلي ال size بال GiB هستخدم vdostats --human-readable

```
[root@MohamedAtef vdo_lv]# vdostats --human-readable
Device                    Size     Used Available Use% Space saving%
vdo_vg-vpool0-vpool      10.0G     4.0G     6.0G   40%          98%
```

قايلك هنا ان المساحه ال available=6 والمستخدمه 4G

- هندخل جوه ال vdo_lv ونحاول نعمل file مساحته كبيره

```
[root@MohamedAtef vdo_lv]#  dd if=/dev/urandom of=urandom_file bs=1M count=1024
1024+0 records in
1024+0 records out
1073741824 bytes (1.1 GB, 1.0 GiB) copied, 12.3358 s, 87.0 MB/s
```

استخدمنا ال command اللي استخدمناه قبل كده علي اعمل file مساحته كبيره

- ممكن استخدم الcommand ده علشان اشوف مساحه ال file اللي عملناه

```
[root@MohamedAtef vdo_lv]# du -sh urandom_file
1.0G  urandom_file
```

هنلاقيه عملي create ل file مساحته 1G

- لو جينا عملنا تاني vdostats --human-readable ونشوف ال size بعد اما انشئنا file مساحته 1G

```
[root@MohamedAtef vdo_lv]# vdostats --human-readable
Device                    Size     Used   Available Use% Space saving%
vdo_vg-vpool0-vpool      10.0G     5.0G     5.0G    50%          5%
```

هنلاقي ان ال size اصبح المستخدم 5 والمتاح 5 لان احنا ضفنا ملق مساحته 1G

- تعال ناخد كذا نسخه من نفس الملف

```
[root@MohamedAtef vdo_lv]# cp urandom_file urandom_file1
[root@MohamedAtef vdo_lv]# cp urandom_file urandom_file2
[root@MohamedAtef vdo_lv]# cp urandom_file urandom_file3
[root@MohamedAtef vdo_lv]# cp urandom_file urandom_file4
[root@MohamedAtef vdo_lv]# du -sh *
1.0G  urandom_file
1.0G  urandom_file1
1.0G  urandom_file2
1.0G  urandom_file3
1.0G  urandom_file4
```

انا اخدت 4 نسخ من ال file فيهم نفس الداتا وكل حاجه

استخدمت du -sh* علشان يعرضلي حجم كل ملف ف ذي مظاهر كده عندك 5 ملفات كل واحد مساحته 1G

- لو جينا عملنا تاني vdostats --human-readable ونشوف ال size بعد اما اخدنا copy من ال file وعملنا 4 file

```
[root@MohamedAtef vdo_lv]# vdostats --human-readable
Device                    Size     Used   Available Use% Space saving%
vdo_vg-vpool0-vpool      10.0G     5.0G     5.0G    50%          5%
```

هنلاقي ال size لسه زي ماهو المستخدم والمتاح 5 جيجا طب ليه واحنا ضفنا 4 ملفات يعني المفروض المساحه المتاحه 1 جيجا علشان ال VDO بيعمل deduplication انه بي store بس one single instance من نفس ال data

- احنا قولنا ان اي داتا هتحطها في ال Logical Volume ال VDO بيعملها Compression و deduplication علشان ي reduce ال storage space اللي انت محتاجها علشان تخزن الداتا بتاعتك وي enhance ال performance بتاعت ال storage devices

➢ طب لو عايز اتاكد لو compression و deduplication معمول ليها enable ولا لا عليال LV بتاعي هستخدم command

```
[root@MohamedAtef ~]# lvs -o lv_name,vdo_compression,vdo_deduplication
  LV     VDOCompression VDODeduplication
  vdo_lv       enabled        enabled
  vpool0       enabled        enabled
```

➢ علشان اعمل disable ليهم هستخدم lvchange --compression وبعدين n معناه no وبعدين ال path

```
[root@MohamedAtef ~]# lvchange  --compression  n  /dev/vdo_vg/vdo_lv
  Logical volume vdo_vg/vdo_lv changed.
```

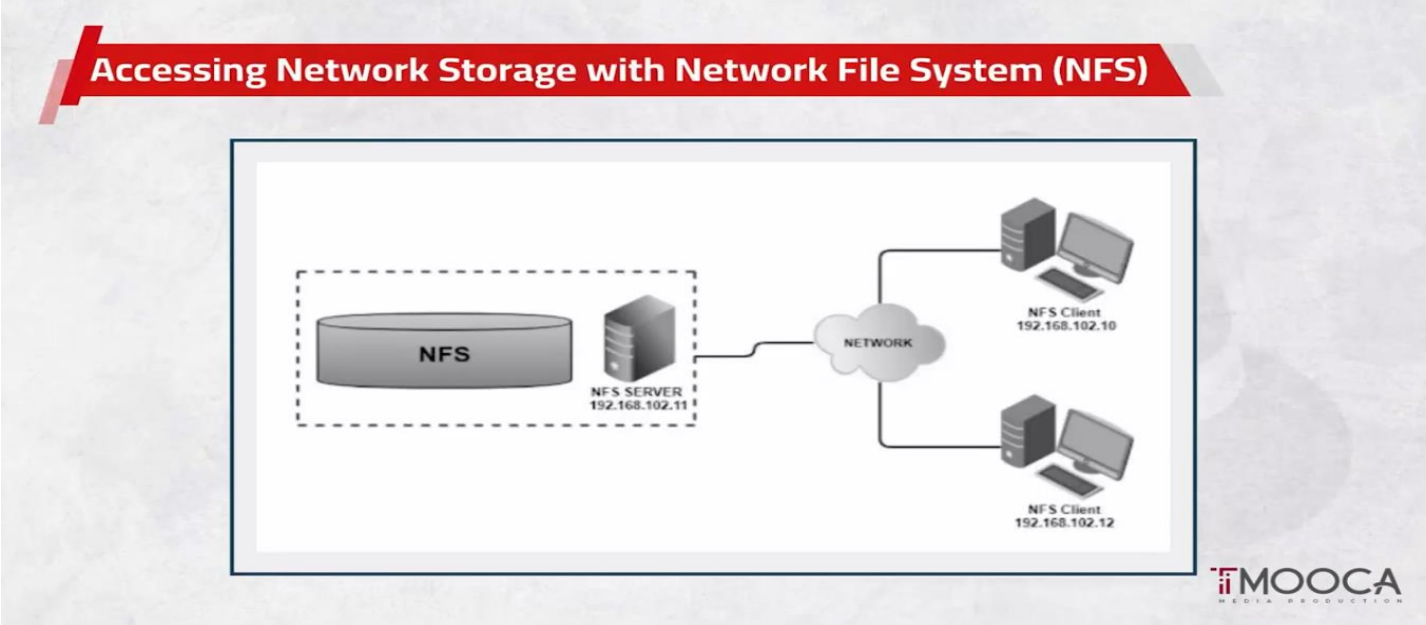
لو عايز اعمل enable هستخدم y بدل n

➢ وبالنسبه للdeduplication لو عايز اعمله disable هستخدم

```
[root@MohamedAtef ~]# lvchange  --deduplication n  /dev/vdo_vg/vdo_lv
  Logical volume vdo_vg/vdo_lv changed.
```

لو عايز اعمل enable هستخدم y بدل n

Chapter 9
Accessing Network-Attached Storage



- ببساطه ال NFS عباره عن network file sharing protocol بيستخدم في ال Network File Sharing بين Linux و Unix operating system فيه عندي protocols تانيه بتسمحلك انك تعمل network file sharing بين ال Linux وال Windows زي ال SMB Protocol و ال CIFS Protocol
- احنا عندنا مجموعه من ال versions المختلفه ل NFS زي NFSv2و NFSv3 و NFSv4 ال default version المستخدمه في red hat 9 هي NFSv4.2 وعندنا NFSv3 مازالت مستخدمه في red hat 9 . احنا عندنا كذا ميزه في NFSv4 مقارنتا بال old versions زي انها more secure والحاجه التانيه انها بتستخدم ال TCP Protocol علي عكس ال old versions اللي كانت بتستخدم ال TCP او ال UDP تالت ميزه ان ال old versions مكنتش ليها dedicated port
- **اما مميزات ال NFS**

- ال NFS بي allow local access to remote files عن طريق ال Network
- تاني ميزه مش شرط ال two machines يكونوا عليهم نفس ال operating system او نفس ال versions ممكن تعمل file sharing مابين اللينكس وال Unix بشرط ان الاتنين بي support ال NFS Protocol
- ال NFS بيساعدك ان يكون عندك centralize storage solutions وده بيساعدك في ال data management وال security
- كمان ال NFS Client تقدر تجيب الداتا بتاعتها بغض النظر عن ال Physical location انا في الاخر ك client مش فارق معايا الداتا بتاعتي موجوده في انهي physical location انا فارق معايا ان لما احتاج الداتا بتاعتي الاقيها
- كمان ال NFS بيساعدك انك ت add more storage لل clients بتاعتك

Setup and Configure NFS Mounts on Linux Server

- To setup NFS mounts, we'll be needing at least two Linux/Unix machines.
  - ✓ NFS Server
  - ✓ NFS Client

Installing NFS Server and NFS Client

- We need to install NFS packages on our NFS Server as well as on NFS Client machine.

```
[root@master ~]# yum install nfs-utils
[root@master ~]# systemctl start nfs-server
[root@master ~]# systemctl enable nfs-server
[root@master ~]# systemctl stop firewalld
```

- علشان نعمل setup ون configure ال NFS service علشان نستخدمها محتاج علي الاقل يكون عندي two Linux او Unix machines ان واحده منهم يكون عليها NFS Server والتانيه NFS Client
- عندنا مجموعه من الsteps هنعملهم علي ال server وال client
- اول حاجه هنعملها علي ال server وال client ان احنا نعمل install لل NFS packages عن طريق ان انا اقوله yum install nfs-utils ال step دي بعملها علي ال two server ال client وال server
- بعد اما نعمل Install باجي علي ال NFS Server بعمل start و enable ل service اسمها nfs-server ال start وال enable بعملهم علي الNFS Server مش بعملهم علي ال NFS Client
- بعد كده بعمل allow لل NFS Service جو ال firewall او اعمل stop لل firewall

Setting Up the NFS Server

```
[root@master ~]# mkdir /data
[root@master ~]# vim /etc/exports
/data        192.168.1.0/24(ro)
/data     192.168.1.101(rw)
[root@master ~]# systemctl restart nfs-server      (terminates all open sessions)
[root@master ~]# exportfs -r                (re-read the config file without termination of open sessions)
[root@master ~]# exportfs -f                (force re-read the config file)
```

علشان اعمل export ل اي Directory بعمل create ل directory اسمه مثلا data تحت ال / هقوله mkdir /data وبعد كده عندي ال main config file اللي احنا هنستخدمه علي ال NFS Server علشان ن add record لل shared directories اسمه export تحت /etc ف بفتح ال export file بال vim وبحط فيه record بالشكل ده /192.168.1.0/24(ro) data ان انا بقوله انا عايز أ share ال directory اللي تحت / اسمه data مع ال subnet دي 192.168.1.0/24 وبين قوسين بحطله option او مجموعه من ال options وليكن ro ف كده انا مديله subnet معينه. ف اي IP او اي client واخد IP من ال subnet دي هيقدر ان هو ي access ال shared directory عن طريق ال network بس هياخد permissions read and only بمجرد ان انا عملت update في ال export لازم اخلي ال nfs services تحس بال change اللي حصل فيه عندي two options علشان اعمل كده ي اما اقوله systemctl restart nfs-server بس في الحاله دي هو بيعمل terminates لكل ال open sessionsومش recommended انك تعمل كده علشان لو فيه عندك اي client تانين فاتحين sessions مع ال NFS Server ف انت ساعتها ممكن تعمل impact لل sessionدي . ال option التاني اللي احنا بنستخدمه دايما اسمه export -r او export -f

Setting Up the NFS Client

```
[root@client ~]# showmount -e 192.168.1.100
[root@client ~]# mount 192.168.1.100:/data /root/data
[root@client ~]# df -hT                    (nfs4)
[root@client ~]# mount -t nfs 192.168.1.100:/data /root/data
[root@client ~]# vim /etc/fstab

192.168.1.100:/data     /root/data     nfs     defaults     0     0
```

ال steps اللي علي ال NFS Client ان انا بعمل بكل بساطه ان انا بعمل mount لل shared directory معايا. علشان اعمله mount عندي كذا طريقه اول طريقه هي ان انا اقوله mount واديله ال ip بتاع ال NFS server واقوله : colon وبعد كده ال directory اللي هو shared معايا وبعد كده احددله ال directory اللي هيتعمله shared وهيتعمل mount فين
او ممكن اقوله mount وبعدين -t واحددله ال file system بتاعي وليكن nfs وبعد كده نفس ال commands اللي استخدمناها
او ممكن استخدم الطريقه ال permanent ان انا افتح ال fstab file واكتب جواه record بنفس الشكل اللي فوق
او ممكن نستخدم سيرفز اسمها autofs وهنشرح الطريقه دي بالتفصيل
لو انا علي ال client وعايز أ List ال shared directories اللي سيرفر معين عامل sharedليها هستخدم showmount -e وبعدين ip ال NFS Server

هنطبق اللي احنا شرحناه

- اول حاجه اننا هنشتغل علي ال NFS Server وال NFS Client وكل واحد وليه ال steps الخاصه بيه
- هنشتغل الاول علي NFS Server

➢ اول حاجه هنعمل install ل NFS Server

```
root@MohamedAtef ~]# dnf install nfs-utils
```

➢ بعد كده هنعمل start و enable

```
[root@MohamedAtef ~]# systemctl start nfs-server
[root@MohamedAtef ~]# systemctl enable nfs-server
```

➢ تعال نشوف ال status الخاصه بال nfs-server

هنلاقي ال service اتعملها start و enable

```
[root@MohamedAtef ~]# systemctl status nfs-server
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; enabled; preset: disabled)
   Active: active (exited) since Sat 2024-06-22 11:00:50 EET; 3h 40min ago
```

➢ بعد كده هنعمل add لل service في ال firewall علشان ميحصلش معايا مشكله وانا بعمل shared ف احنا هنستخدم ال command الاتي وهيتم شرح ال command ده بالتفصيل ف الشابتر الخاص بيه

```
[root@MohamedAtef ~]# firewall-cmd  --permanent  --add-service=nfs
success
```

➢ بعد كده هنعمل reload لل firewall باستخدام

```
[root@MohamedAtef ~]# firewall-cmd --reload
success
```

- بعد كده هنعمل create ل directory تحت ال / باسم data

```
[root@MohamedAtef ~]# mkdir  /data
```

- بعد كده هنعمل mount لل shared directory عن طريق ان انا هفتح ملف ال export بال vim علشان نضيف ال record فيه عندي كذا طريقه اني اكتب ال record هنشوفها في المثال

```
[root@MohamedAtef ~]# vim /etc/exports
/data    192.168.2.132(rw)
/data    192.168.2.0/24(ro)
/data    *(rw)
/data    mohamedatef.client.com (ro, sync)
/data    *.client.com(rw,sync)
```

بعد اما فتحنا ال export هكتب جواه ال record وفيه طرق كتيره علشان اكتب ال record

اول حاجه بحددله ال directory اللي هعمله share وبعد كده بضيف IP ال Client وبعدين بضيف بين قوسين اي اوبشن

او ممكن اقوله ان عايز اعمل share لل directory لل subnet كلها بالمنظر ده

او ممكن اقوله ان انا عايز أشارك share مع كل الناس عن طريق ان انا اقوله استريك *

او ممكن اقوله ان انا عايز أشارك share مع الHostname معين

او ممكن اقوله ان انا عايز أشارك share مع الدومين

ف انت علي حسب انت عايز تدي ل مين ال acces علي ال directory اللي هعمله شير

- طالما عملنا update في ال export file لازم اعمل exportfs -r

```
[root@MohamedAtef ~]# exportfs -r
```

- لو انا عايز اتاكد هل ال data/ اتعمله share ولا لا هستخدم exportfs

```
[root@MohamedAtef ~]# exportfs
/data                192.168.2.132
```

هتلاقيه هنا جايبلك ال directory ومتشير لانهي IP

- فيه عندي command تاني اسمه exportfs -a بنستخدمه ساعات لو انت عندك مجموعه من ال shares او مجموعه من ال export جوه ال exports file وعايز تعملهم export في نفس الوقت ف بتقولهم exportfs -a ف هو هيروح يعمل share لكل ال record الموجوده في ال exports file

```
[root@MohamedAtef ~]# exportfs -a
```

- لو انا عايز اعمل unexport لكل ال record وال share اللي عندي بقوله exportfs -ua

```
[root@MohamedAtef ~]# exportfs -ua
```

- لو انا عايز اجيب كل ال default options هقوله exportfs -v

```
[root@MohamedAtef ~]# exportfs -v
/data          172.16.76.133(sync,wdelay,hide,no_subtree_check,sec=sys,rw,secure,root_squash,no_all_squash)
```

دي كده كل ال options اللي عندي

- لو انا عايز معلومات اكتر عن كل option هستخدم ال man وبعدين exports

```
[root@MohamedAtef ~]# man 5 exports
```

- احنا كده عملنا كل steps في الجزء الخاص بال NFS Server هنعرف دلوقتي ال Steps الخاصه بال NFS Client علشان ال share يكون موجود عند ال client

هنشتغل علي ال client

- هنروح علي جهاز ال client ونعمل install ل NFS

```
[root@client ~]#dnf install nfs-utils
```

- بعد كده ال step الوحيده اللي بتعملها علي جهاز ال client انك بتعمل Mount لل shared directory
- وزي ماقولنا علشان اعمل mount عندي 3 طرق اول طريقه وهي الطريق ال manual اللي بنستخدم فيها ال mount command الطريقه التانيه ال permanent اللي بنستخدم فيها ال fstab file والطريقه التالته اللي هي ال on demand و بنستخدم فيها ال autofs service ودي هنشرحها بالتفصيل كمان شويه

هنشوف ال 3 طريق اللي اقدر اعمل بيها mount لل shared directory

1- اول طريقه وهي ان انا هستخدم **mount**

```
[root@client ~]# mkdir /mnt/data
[root@client ~]# mount  -t  nfs  172.16.76.132:/data  /mnt/data/
```

هنا انا كتبت ال command الخاص بال mount

بعد كده قولته اوبشن -t وحددلته ال file system ال nfs

بعد كده ال ip ال server بعد كده بضيف: colun وبعدين اضيف مسار ال directory اللي عامله share

بعد كده بضيف المسار اللي هعمل عليه mount

- كده احنا عملنا mount علشان نتاكد هنستخدم **df -hT**

```
[root@client ~]# df -hT
Filesystem          Type     Size  Used Avail Use% Mounted on
/dev/nvme0n1p2      xfs      20G  4.3G   16G  22% /
/dev/nvme0n1p3      xfs      20G  179M   20G   1% /home
172.16.76.132:/data   nfs4     20G  6.6G   14G  33% /mnt/data
```

هنلاقيه عمل mount وتحت /mnt/data وال file system نوعه nfs4

- الطريقه دي مش permanent يعني لو عملت reboot ال mount مش هيبقي موجود

2- تاني طريقه وهي ال permanent هنفتح ال fstab file وهنضيف ال record فيه

```
[root@client ~]# vim /etc/fstab
nfs  172.16.76.132:/data        /mnt/external          nfs       rw,sync          0  0
```

هنا انا كتبت جوه ال fstab ال record ده

- وبعد كده هتعمل **systemctl daemon-reload**

```
[root@client ~]# systemctl daemon-reload
```

- لو انا عايز اعمل list لل shared directory الموجوده علي السيرفر استخدم ال command ده **showmount -e** علشان استخدم ال command ده لازم اضيف كذا سيرفز في ال firewall عند ال NFS Server ف احنا هنروح علي ال server ونضيف السيرفز دي mountd , nfs, rpc-bing لازم تضيف السيرفز دي في ال firewall علشان يشتغل

```
[root@MohamedAtef ~]# firewall-cmd --permanent --add-service=mountd
[root@MohamedAtef ~]# firewall-cmd --permanent --add-service=rpc-bind
```

- بعد كده بعمل reload لل firewall

```
[root@client ~]# firewall-cmd --reload
```

- بعد كده هنستخدم ال command ده **showmount -e** وبعد كده هضيف IP ال server

```
[root@client ~]# showmount -e 172.16.76.132
Export list for 172.16.76.132:
/data 172.16.76.133
```

اول اما استخدمت ال command ده قالك ان السيرفر ده 172.16.76.132 عامل share معاك لل directory ده /data

Automounting Network-Attached Storage

Mounting NFS Shares with the Automounter

- The automounter is a service (**autofs**) that automatically mounts NFS shares "on-demand," and will automatically unmount NFS shares when they are no longer being used.

Automounter Benefits

- Users do not need to have root privileges to run the **mount** and **umount** commands.
- NFS shares configured in the automounter are available to all users on the machine, subject to access permissions.
- NFS shares are not permanently connected like entries in **/etc/fstab**, freeing network and system resources.
- The automounter is configured on the client side; no server-side configuration is required.

Mount NFS Exports with the Automounter

- هنتكلم عن تاني service موجوده معانا في ال topic ده وبيجي عليها سؤال في ال exam بتاع ال RHCSA بعنوان autofs او Automounter
- ببساطه ال autofs عباره عن service الهدف الاساسي منها انها تعمل mount لل NFS Shares بطريقه automatic او on-demand يعني من الاخر لما تيجي تستخدم ال NFS shares يتعملها mount بطريقه automatic ولما متستخدمهوش لفتره معينه بي time out ويتعمله unmount بطريقه automatic علي عكس ماشوفنا من شويه احنا كان عندنا علي ال NFS Client كان عندنا 3 طرق بنعمل بيهم mount اول طريقه وهي الطريقه ال manual اللي بنستخدم فيها ال mount command تاني طريقه وهي ال permanent اللي بنستخدم فيها ال fstb file وتالت طريقه وهي اللي on-demand وهي اللي بنشرحها دي اننا بنستخدم ال autofs

Automounter Benefits

- لو هنتكلم عن ال benefits بتاعت ال autofs او automounter هنلاقي اول ميزه انه بيقولك ان ال normal user مش محتاج يبقي عندها root permissions علشان ت execute ال mount وال unmount commands بمعني لو انت عايز تعمل mount ل NFS file system عندك 3 طرق اول طرقتين وهما ال manual وال permanent دول ال root هو اللي ليه الصلاحيه ان هو ي execute ال commands دي ولكن باستخدام ال autofs ال normal users تقدر ان هي تعمل mount لل file systems on-demand
- تاني ميزه ان ال NFS shares ال configured عندك بال automounter او autofs بتبقي available لكل ال users الموجودين عندك علي ال machines علي حسب ال permissions بتاعتهم
- تالت ميزه مهمه بما ان ال mount بيبقي on-demand مش permanent زي ال entries اللي بتبقي في ال fstab file ف ده بي reduce جدا ال network وال system resource بتاعتك

- رابع ميزه ال autofs كل ال configuration بتتعامل من ناحيه ال client فبيتقال عليها client side service مش server side يعني انت مش محتاج من ناحيه ال server تعمل اي configurations لل auto mounter او ال autofs بتاعتك
- واخر حاجه ال autofs بي support نوعين من ال mount نوع اسمه direct mount ونوع تاني indirect وهنشوف الفرق مابينهم

Steps for Automounting NAS Using Autofs

1. Install the autofs package.

-Ensure Autofs is installed on your RHEL 9 system

```
[user@host ~]# dnf install autofs
```

2. Add a master map file to /etc/auto.master.d. This file identifies the base directory used for mount points and identifies the mapping file used for creating the automounts.

```
[user@host ~]# vim /etc/auto.master.d/demo.autofs
```

-Add the master map entry, in this case, for indirectly mapped mounts:

```
/shares /etc/auto.demo
```

3. Create the mapping files. Each mapping file identifies the mount point, mount options, and source location to mount for a set of automounts.

```
[user@host ~]# vim /etc/auto.demo
```

-The mapping file-naming convention is /etc/auto.name, where name reflects the content of the map

```
work -rw,sync serverb:/shares/work
```

4. Start and enable the automounter service.

-Use systemctl to start and enable the autofs service.

```
[user@host ~]$ sudo systemctl enable --now autofs
```

- علشان نعمل implement ل autofs service

1- اول step بروح اعمل install ل autofs service عن طريق ان انا بقوله `dnf install autofs`

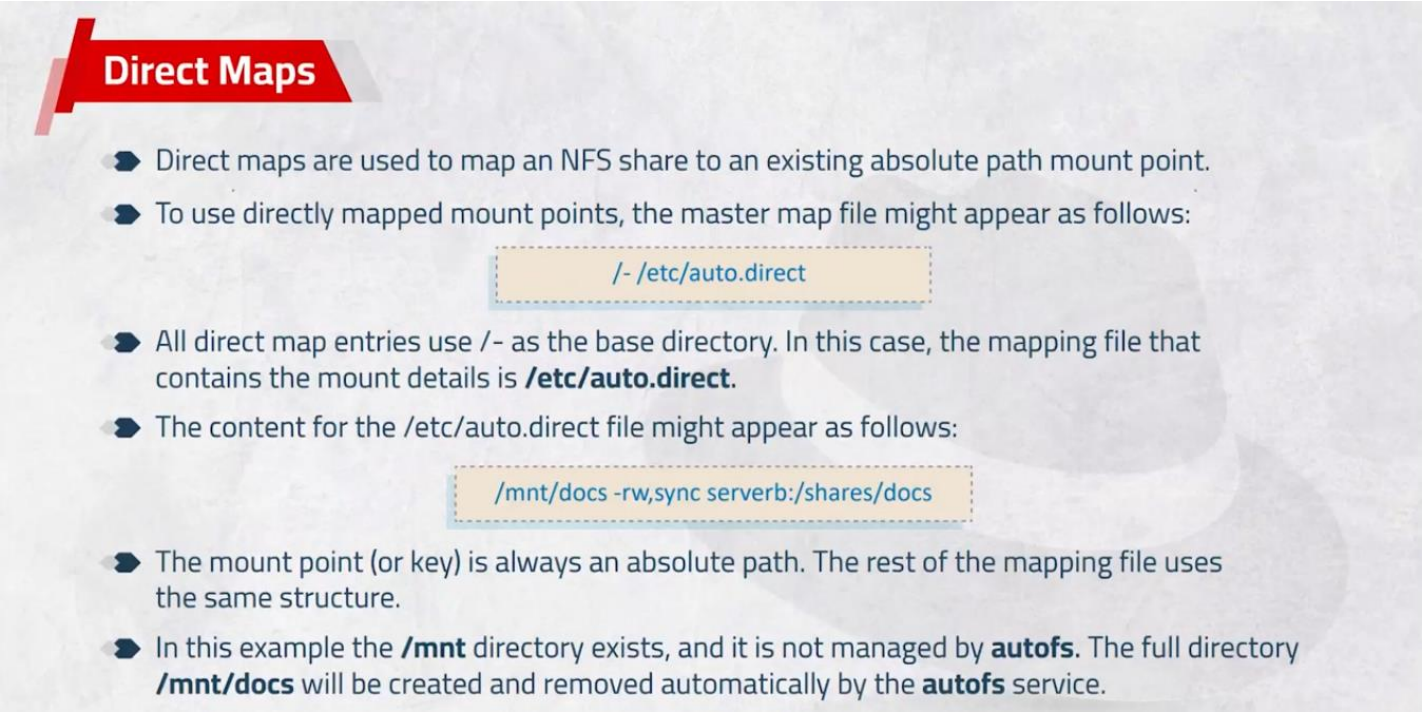
2- تاني step بعمل create لحاجه اسمها master map file تحت المكان ده `/etc/auto.master.d` وبعمل create ل master map file عباره عن text file عادي جدا بسميه باي اسم بس اهم حاجه اخلي ال extension بتاعه يكون `.autofs` وبعد كده نفتح ال file ده بال vim وبحط فيه entry بالشكل ده `/shares /etc/auto.demo` وال entry بتختلف علي حسب انت هتشتغل بال direct map ولا بال indirect يعني مثلا ف حاله ال indirectly mapping بحط record اول حاجه بحددله ال based directory زي ماموجود في ال مثال `/shares` وتاني حاجه بحددله ال map file اللي انت هتحط جواه ال

mount details بتاعتك كلها يعني تحت ال /etc/ هعمل create ل file اسمه auto.demo والاسم بتاعه مش شرط اسم معين اي اسم عادي ومش شرط يكون ليه اي extension زي ال master map file ال file اللي عملنا ليه create هنحط جواه كل ال mount details سواء كان ال mount point او ال mount option او ال source location وهكذا

3- ال step اللي بعد كده ان انا بروح اعمل create ل ال map file تحت ال /etc/ وبفتح ال file ده بال vim command زي vim /etc/auto.demo ده ال file اللي انا حاطه في ال master map file وبحط entry بالمنظر ده work -rw,sync serverb:/shares/work

4- ال step اللي بعد كده ات انا اعمل start و enable لل autofs باستخدام sudo sysyemctl enable --now autofs

- **زي ماقولنا انا عندي نوعين من ال mapping نوع اسمه direct maps ونوع اسمه indirect maps**



- ال **direct maps** عباره عن طريقه سهله و very straight forward وبستخدمها في حاله لو عندي NFS Share وعايز اعمله map ل absolute path mount point موجود عندي عن طريق ان بروح اعمل create ل master map file وبحط فيه entry بالشكل ده /- /etc/auto.direct اول حاجه بقوله ال path directory بحطها forward slash /- وبحددله بعد كده ال map file اللي انا هحط فيه ال mount details بتاعتي وليكن تحت /etc/auto.direct وبعد كده ال auto.direct هعمله create واحط جواه entry بالشكل ده /mnt/docs -rw,sync serverb:/shares/docs واهم حاجه في ال direct map ان انا بحط في ال Mount Point بحطله ال absolute path وليكن /mnt/docs وبعد كده احط ال mount option وال source location بتاع ال NFS Location وبعد كده بحددله ال directory ال shared معايا وبعد كده بروح اعمل restart لل autofs service

تعال نشوف مثال علي ال Direct Maps

- زي ماقولنا انا عندي ال autofs بتبقي عباره عن client side service ال configuration بتاعتها بتتعمل من ناحيه ال Client كل اللي احنا بنعمله من ناحيه ال server ان احنا بنعمل export ل اي directory مع ال Client بتاعنا
- هعمل directory واعمله share مع ال client

```
[root@client ~]# mkdir -p /shares/direct/external
```

- هعمل share لل directory ده مع ال client عن طريق ان انا هفتح ملف exports واكتب فيه ال record

```
[root@server ~]# vim /etc/exports
/shares/direct/external        172.16.76.133(rw,sync,no_root_squash)
```

بحط اول حاجه مسار ال Directory اللي عامله share

وبعدين احط ال IP ال Client اللي هعمل معاه share لل directory ده وبديله بين قوسين ال options اللي عايز اطبقها علي ال client

- وبعد كده اقوله `exportfs -r` علشان ال nfs ت read ال config file وتديني effect

```
[root@server ~]# exportfs -r
```

- علشان نتاكد انه عمل share لل directory مع ال client هنستخدم `exportfs`

```
[root@server ~]# exportfs
/shares/direct/external
                172.16.76.133
```

هتلاقيه هنا بيقولك ان هو عمل share لل directory مع ال IP ده 172.16.76.133

- كده احنا عملنا الجزء الخاص بال server هنشتغل علي ال client

- اول step هنعمل install ل autofs علي ال client

```
[root@client ~]# dnf install autofs
```

- تاني step هنعمل create ل master map file عن طريق ان احنا هندخل تحت المسار ده `/etc/auto.master.d/` وهنعمل create تحتيه باسم direct.autofs وبعدين هنفتح ال file ده واكتب ال entry بقوله ال path directory بحطها forward slash /- وبحددله بعد كده ال map file اللي انا هحط فيه ال mount details بتاعتي وليكن تحت `/etc/` هيكون ال file اسمه `auto.direct`

```
[root@client ~]# cd /etc/auto.master.d/
[root@client auto.master.d]# vi direct.autofs
/-              /etc/auto.direct
```

- بعد كده هنعمل create ل ال map file هنعمل create لل file ده auto.direct واحط جواه ال mount details بتاعي

```
[root@client auto.master.d]# vim /etc/auto.direct
/external      -rw,sync,fstype=nfs4    172.16.76.132:/shares/direct/external
```

اول حاجه بحط ال absolute path mount الموجوده عندي علي ال client وليكن هقوله /external

بعد كده بحط ال - وبعدين ال mount option وليكن - rw,sync,fstype=nfs4

وفي الاخر بحطله ال source location ان انا بجيب ال ip ال server وبعدين colon: وبعدين ال path بتاع ال share directory

- اخر step ان احنا نعمل start و enable لل autofs service

```
[root@client ~]# systemctl enable --now autofs
```

- لو عملنا df -h هنلاقيه لسه متعملهوش mount لان ال autofs بيعمل mount اتوماتيك بيعمل mount لما تستخدم ال directory وبعد 5 دقائق بيعمل umount
- هنعمل create ل اي file ونشوف اتعمله mount ولا لا

```
[root@client ~]#  echo testing-direct > /external/testing.txt
[root@client ~]# df -h
Filesystem                          Size  Used Avail Use% Mounted on
/dev/nvme0n1p2                      20G  4.3G  16G  22%        /
/dev/nvme0n1p1                      507M  248M  260M  49%      /boot
/dev/mapper/vg01-lv01               3.0G  54M  3.0G  2%        /data_lv01
/dev/nvme0n1p3                      20G  179M  20G  1%         /home
172.16.76.132:/shares/direct/external  20G  6.6G  14G  33%      /external
```

هنلاقيه هنا عمل Mount وقدرت استخدم ال directory ده

- كده احنا اخدنا مثال علي ال direct maps هنشوف دلوقتي ال indirect maps ونشوف مثال عليها

Indirect Wildcard Maps

- When an NFS server exports multiple subdirectories within a directory, then the automounter can be configured to access any one of those subdirectories using a single mapping entry.
- Continuing the previous example, if serverb:/shares exports two or more subdirectories and they are accessible using the same mount options, then the content for the **/etc/auto.demo** file might appear as follows:

```
* -rw,sync serverb:/shares/&
```

- The mount point (or key) is an asterisk character (*), and the subdirectory on the source location is an ampersand character (&). Everything else in the entry is the same.
- When a user attempts to access **/shares/work,** the key * (which is **work** in this example) replaces the ampersand in the source location and serverb:/shares/ is mounted. As with the indirect example, the **work** directory is created and removed automatically by autofs.

- نقدر نقول ان ال **indirect maps** بتكون more dynamic مقارنتا بال direct mapping ودي بستخدمها لو عندي for example ال NFS Server عاملي export او share لمجموعه من ال subdirectories تحت نفس ال directory . وليكن تحت `/share` عاملي share لمجموعه من ال subdirectories ف انت ممكن تستخدم الطريقه دي علشان خاطرتحط one single entry بالشكل ده
  `* -rw,sync server:/shares/&` لكل ال shares وليكن هتقوله في الاول * وبعد كده ال mount option وبعد كده هتقوله `serverb:` وبعدين ال directory وهتقوله في الاخر `&`
- ال & معناه لما تيجي ت access اي subdirectory موجود تحت shares directory هيعملها mount عند بنفس ال name بتاع ال directory

مثال علي ال Indirect Maps

- هنعمل create ل directory تحت ال /shares باسم indirect و هنعمل جواه مجموعه من ال subdirectory

```
[root@server ~]# mkdir /shares/indirect
[root@server ~]# cd /shares/indirect/
[root@server indirect]# mkdir center west east
```

- هنعمل ل subdirectory اللي عملناهم هنعملهم export هفتح ملف ال export واكتب ال entry

```
[root@server ~]# vim /etc/exports
/shares/direct/          172.16.76.133(rw,sync,no_root_squash)
```

- بعد كده هعمل exportfs -r علشان غيرنا في ملف ال export

```
[root@server ~]# exportfs -r
```

- بعد كده هنروح علي ال client ون configure ال autofs
- اول step هعملها علي ال client هعمل create ل ال master map file عن طريق ان احنا هندخل تحت المسار ده /etc/auto.master.d/ وهنعمل create ل file تحتيه باسم indirect.autofs وبعدين هنفتح ال file ده واكتب ال entry بقوله ال path directory وليكن /internal وبحددله بعد كده ال map file اللي انا هحط فيه ال mount details بتاعتي وليكن تحت /etc/ هيكون ال file اسمه auto.indirect

```
[root@client ~]# cd /etc/auto.master.d/
[root@client auto.master.d]# vim indirect.autofs
/internal                /etc/auto.indirect
```

- بعد كده هنعمل create ل ال map file هنعمل create لل file ده auto.indirect واحط جواه ال mount details بتاعي

```
[root@client auto.master.d]# vim /etc/auto.indirect
*      -rw,sync,fstype=nfs4    172.16.76.132:/shares/indirect/&
```

- بعد كده هنعمل restart لل autofs

```
[root@client ~]# systemctl restart autofs
```

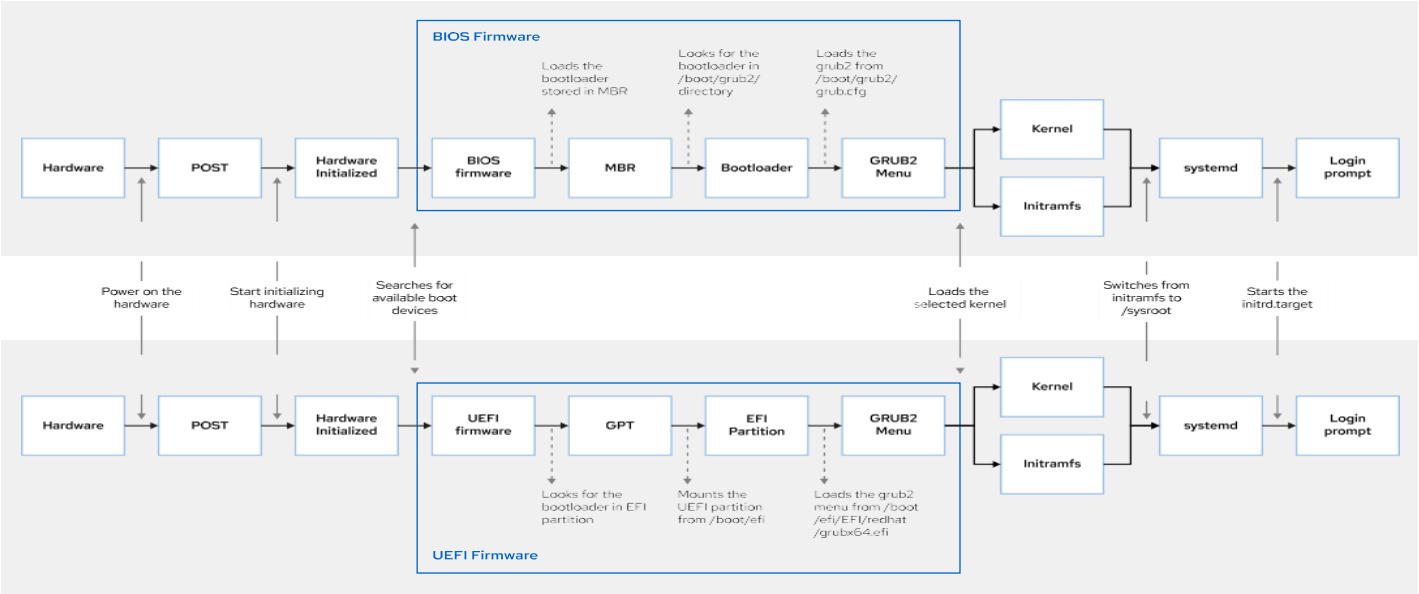
- هنعمل create ل اي file ونشوف اتعمله mount ولا لا

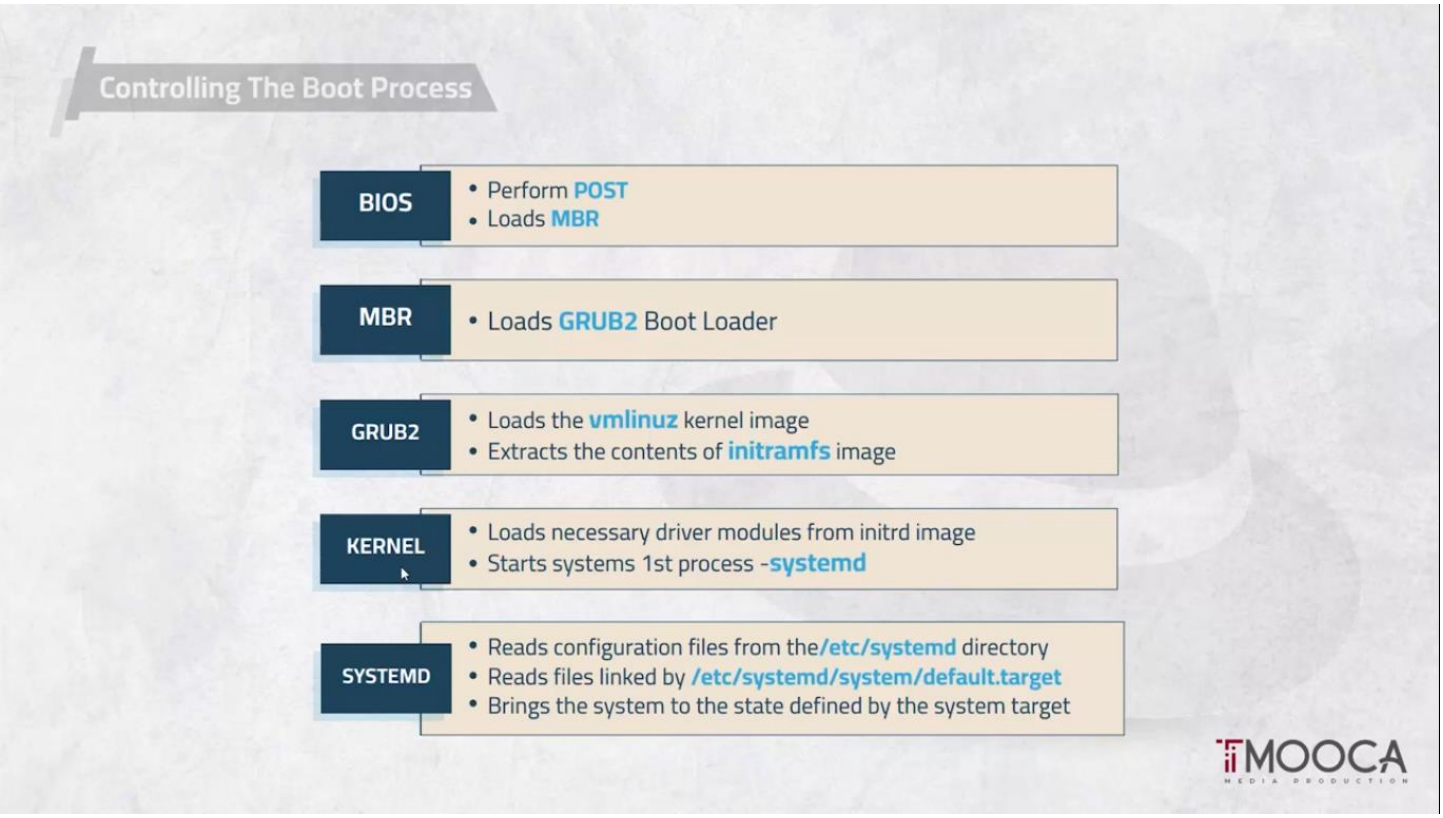
```
[root@client ~]#  echo testing-1 > /internal/west/testing-1.txt
[root@client ~]# df -h
Filesystem                          Size  Used Avail Use% Mounted on
/dev/nvme0n1p2                      20G  4.3G   16G  22%          /
/dev/nvme0n1p1                      507M  248M  260M  49%       /boot
/dev/mapper/vg01-lv01               3.0G   54M  3.0G   2%        /data_lv01
/dev/nvme0n1p3                      20G  179M   20G   1%         /home
172.16.76.132:/shares/indirect/west   20G  6.6G   14G  33% /internal/west
```

هنلاقيه هنا عمل Mount وقدرت استخدم ال directory ده

Chapter 10

Controlling the Boot Process





- **خطوات ال Boot Process في ال Linux**

➢ مبدئيا كده انا عندي السيستم بيمر بمجموعه من ال steps أو المراحل من اول مبعمل power on لل machine بتاعي لحد اما ال system بتاعي يقوم ويظهرلي ال login page اللي بدخل عليها ال username وال password علشان أ login علي ال machine ال steps دي بنقول عليها Boot Process أو Boot sequence .

1. اول step في ال Boot Process هي انك تروح تعمل power on لل machine
2. تاني step في عندنا small software بيكون stored في ال room الموجود عندك في ال motherboard ال software ده اسمه Firmware نقدر نقول إن ال Firmware ده هو ال interface بين الهاردوير و ال software احنا عندنا نوعين من ال Firmware نوع قديم شويه اسمه BIOS ونوع تاني modern و more advanced اسمه UEFI ووظيفه ال firmware أنه بيعمل حاجتين اول حاجه بيروح يعمل checks علي main hardware components الstep دي بنقول عليها POST ودي اختصار ل power on self-test وonce أن ال Firmware عمل post بيروح بعد كده ي initialize ال hardware components دي اول step ال Firmware بيعملها سواء كان ال type بتاعه BIOS أو UEFI . تاني حاجه بيعملها بيروح يعمل search ويعمل load لل MBR ودي اختصار ل master boot record

وال MBR زي ماحنا عارفين انه بيكون عباره عن 512 بت وبيبقي allocated في أول sector في الDrive وبيكون متقسم ل 3 اجزاء

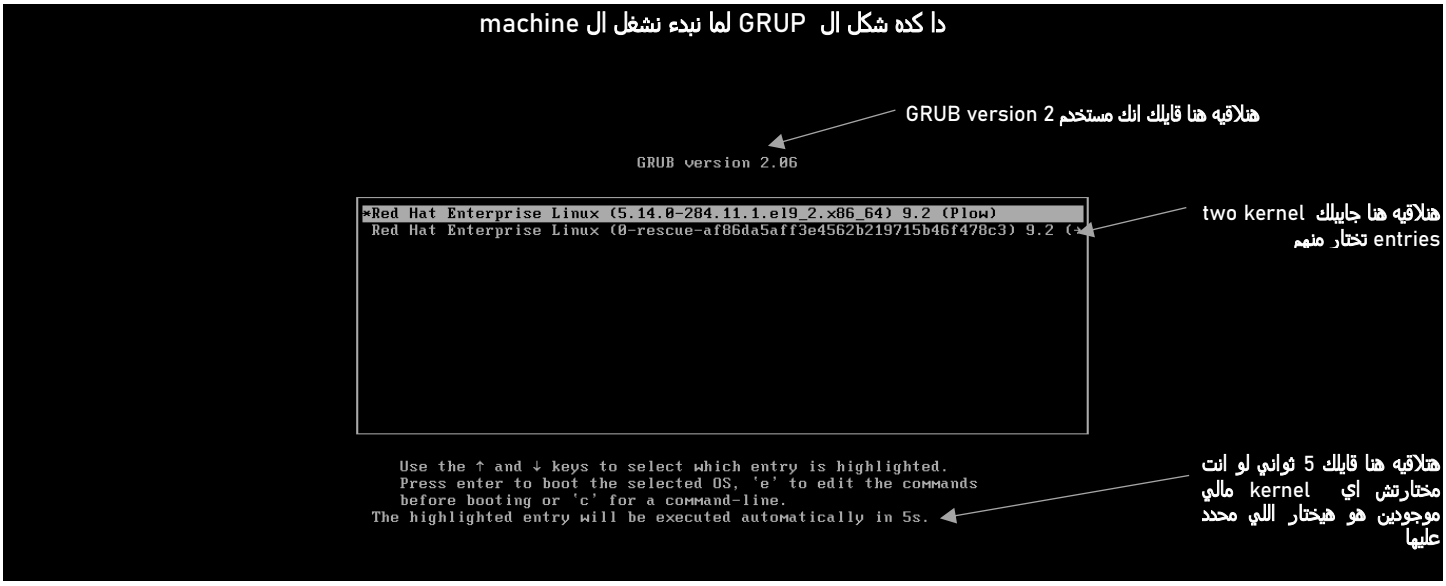
- اول جزء بيكون الsize بتاعه عباره عن 446 بت وبيكون stored جواه ال boot loader
- تاني جزء في ال MBR هو ال partition table ال size بتاعه بيكون 64 بت وده بيكون جواه معلومات عن partition اللي عندك علي الdisk زي ال size وال type وال status
- تالت جزء في ال MBR ال size بتاعه بيكون 2 بت واسمه magic number وده عباره عن number hexadecimal ال Firmware أو ال BIOS بيستخدمه علشان ي confirm هل ال MBR بتاعك valid ولا corrupted
- و once أن ال Firmware أو BIOS عمل load لل MBR ال MBR بعد كده بيروح يشاور ويعمل load لل main boot loader اللي هو اسمه GRUB2

3. بعد كده ال GRUB2 بتاخد الcontrol والهدف الأساسي منه أنه بيروح يعمل load لل kernel في الmemory وبيروح ي extracts ال contents بتاعت ال initramfs في ال memory وال initramfs عباره عن archive بيبقي stored جواه مجموعه من ال modules وال drivers اللي ال kernel بيستخدمها
4. و once أن ال GRUB2 عملت loads لل kernel في الميموري بعد كده ال kernel بياخد ال control وبيروح بعد كده ي initialize ال hardware وبيقوم ال first process اللي بتقوم عندي ف السيستم اسمها systemd ودي اول بروسيس بتقوم عندي
5. وonce أن ال kernel قوم ال systemd service ال systemd بتاخد ال control وتروح بعد كده تقرأ ال configuration بتاعتها تحتetc/systemd/ وتشوف ال link ده
/etc/systemd/system/default.target بيشاور علي انهي target وتروح تقوملك كل الunits وكل الservices اللي توصل ف الآخر لل target ده يعني مثلا لو ال default target بيشاور علي target اسمه grafical.target يبقي كده ال systemd هتفهم انها هتروح تقوملك كل السيرفيز وال units اللي توصلك لل GUI وال Login Page اللي بتكتب فيها الusername والباسورد . دي كده كل خطوات ال Boot Process.

Examine GRUB 2 configuration file, grub.cfg

- هنتكلم عن ال main boot loader او ال GRUP2 احنا قولنا ان الهدف الاساسي من ال GRUP 2 ان هي بتعمل load لل kernel في ال memory وبيروح ي extracts ال contents بتاعت ال initramfs في ال memory عن طريقه ان في الاول بت display menu وبتديك ال option انك بتختار ال kernel اللي انت عايز ت boot ال system بتاعك منه وممكن يكون عندك اكتر من kernel version وساعتها هي بتديك ال option انك تختار اي kernel بطريقه manual وتضغط enter علشان هو يروح ي load ال kernel اللي انت اختارته في الميموري او بيكون عنده timer بيكون 5 ثواني لو انت مختارتش بطريقه manual هو بي expires ال 5 ثواني ويختار ال kernel اللي بي selected عنده في ال menu

- علشان نشوف شكل ال GRUP menu لازم نعمل reboot لل system



- انا عندي by default كل ملفات ال kernel وال interamfs وال configuration بتاعت ال GRUP بتبقي stored تحت /boot
- هندخل تحت `/boot` ونعمل ls -lh علشان ن list كل المحتوي اللي تحت `/boot`

```
[root@MohamedAtef ~]# cd /boot/
[root@MohamedAtef boot]# ls -lh
-rw-r--r--. 1 root root 211K Apr 12  2023 config-5.14.0-284.11.1.el9_2.x86_64
drwxr-xr-x. 3 root root   17 Mar  5 19:21 efi
drwxr-xr-x. 2 root root 4.0K May 30 10:39 extlinux
drwx------. 5 root root   97 Jun  9 01:25 grub2
-rw-------. 1 root root 126M Mar  5 19:35 initramfs-0-rescue-af86da5aff3e4562b219715b46f478c3.img
-rw-------. 1 root root  53M Mar  5 19:43 initramfs-5.14.0-284.11.1.el9_2.x86_64.img
drwxr-xr-x. 3 root root   21 Mar  5 19:28 loader
lrwxrwxrwx. 1 root root   52 Mar  5 19:31 symvers-5.14.0-284.11.1.el9_2.x86_64.gz -> /lib/modules/5.14.0-284.11.1.el9_2.x86_64/symvers.gz
-rw-------. 1 root root 5.7M Apr 12  2023 System.map-5.14.0-284.11.1.el9_2.x86_64
-rwxr-xr-x. 1 root root  12M Mar  5 19:33 vmlinuz-0-rescue-af86da5aff3e4562b219715b46f478c3
-rwxr-xr-x. 1 root root  12M Apr 12  2023 vmlinuz-5.14.0-284.11.1.el9_2.x86_64
```

ف علشان نعرف فين ملفات ال kernel هنلاقي اي file بيبدأ ب vmlinuz ده كده بيكون ملف ال kernel الخاص بيك وبيكون عندنا ملفين لل kernel ملف انت بت boot منه علشان السيستم وملف تاني خاص ب ال rescue وبيستخدم في حاله ال troubleshooting

ال main config file الخاص بال grup هنلاقيه تحت ال directory ده grub2 في حاله لو ال firmware بتاعك ال type بتاعه UEFI

ال main config file الخاص بال grup هنلاقيه تحت ال directory ده grub2 في حاله لو ال firmware بتاعك ال type بتاعه BIOS

وكل kernel بيبقي ليه ال interamfs img بتاعته

وده ملف ال kernel الخاص ب ال rescue اللي انت بت boot منه في حاله لو انت عايز تدخل في mode اسمه rescue mode علشان تعمل troubleshooting

ده ملف ال kernel اللي انت بت boot منه السيستم بتاعك

- ملفات ال grup بتكون موجوده في `/boot/grup2` دي في حاله ال BIOS لو دخلنا تحت المسار ده هنلاقي فيه مجموعه من ال files هنلاقي ال main configuration file الخاص بال grup2 اسمه grub.cfg

```
[root@MohamedAtef boot]# cd grub2/
[root@MohamedAtef grub2]# ls
device.map  fonts  grub.cfg  grubenv  i386-pc  locale
```

- اما في حاله لو ال firmware بتاعك ال type بتاعه UEFI هنلاقي ال configuration file بتاع ال grup تحت `/boot/efi/EFI/redhat` ف علشان ال default firmware بتاعنا BIOS ف هنلاقي ال folder ده فاضي

```
[root@MohamedAtef ~]# cd /boot/efi/EFI/redhat/
```

- لو فتحنا ال config file الخاص ب ال grup هنلاقيه عباره عن script فيه مجموعه من ال if statement ومجموعه من ال functions و بيعمل insert لمجموعه من ال modules وهكذا

```
[root@MohamedAtef ~]# vim /boot/grub2/grub.cfg
```

- مش recommended ان احنا نعدل في ال grub.cfg ف لو انت عايز تعمل اي change في ال grup ف recommended انك تعدل في ال file ده `/etc/default/grub`
- لو فتحنا ال file ده هنلاقيه فيبه مجموعه من ال parameters

```
[root@MohamedAtef ~]# vim /etc/default/grub
GRUB_TIMEOUT=5
GRUB_DISTRIBUTOR="$(sed 's, release .*$,,g' /etc/system-release)"
GRUB_DEFAULT=saved
GRUB_DISABLE_SUBMENU=true
GRUB_TERMINAL_OUTPUT="console"
GRUB_CMDLINE_LINUX="resume=UUID=c225b2df-568e-497d-889f-198d33b98efe rhgb quiet"
GRUB_DISABLE_RECOVERY="true"س
GRUB_ENABLE_BLSCFG=true
```

ده كده ال timer اللي بيكون في ال grup menu وبيكون 5 ثواني ف احنا ممكن نغيره زي ماحنا عايزين

دا لو انا عندي اكتر من kernel في ال menu وانا عايز أختار kernel معين يكون معمول عليه select في الاول علشان أ boot السيستم منه ف علشان اغير ده لازم اغير بدل كلمه saved بالرقم بتاع ال kernel entry والارقام بتبدأ من 0 وبعدين 1 وهكذا

- بعد اما نعدل في ال`/etc/default/grub` لازم نعمل regenerate لل configuration بتاعت ال grup عن طريق ال command اللي اسمه grub2-mkconfig

```
[root@master ~]# grub2-mkconfig
```

Rebooting And Shutting Down

- To power off or reboot a running system from the command line, you can use the **systemctl** command.
- **systemctl poweroff** stops all running services, unmounts all file systems (or remounts them read-only when they cannot be unmounted), and then powers down the system.
- **systemctl reboot** stops all running services, unmounts all file systems, and then reboots the system.
- You can also use the shorter version of these commands, **poweroff** and **reboot**, which are symbolic links to their **systemctl** equivalents.

- لو انا عايز اعمل shut down او reboot للسيستم من ال cli ف عندنا مجموعه من ال commands
- اول command وهو اني بقوله `systemctl poweroff` ساعتها هو هيعمل stop لكل ال running services وهيعمل unmount للfile system ال mount عندي ولو فيه اي file system معرفش يعمله unmount هيعمله remount في ال read-only بحيث وهو بي power off السيستم ميحصلش corruption لل file system

```
[root@master ~]# systemctl poweroff
```

- تاني command ممكن استخدم `systemctl repoot` هيعمل stop لكل ال running services وهيعمل unmount للfile system وبعدين هيعمل reboot لل machine

```
[root@master ~]# systemctl repoot
```

- تالت command ممكن استخدم `poweroff` او `reboot` دول عباره عن symbolic link بيشاورو علي systemctl

```
[root@master ~]# poweroff
[root@master ~]# reboot
```

- رابع command وهو اني استخدم shutdown

```
[root@master ~]# shutdown
```

Selecting a Systemd Target

A **systemd** target is a set of systemd units that the system should start to reach a desired state. The following table lists the most important targets:

TARGET	PURPOSE
`graphical.target`	System supports multiple users, graphical- and text-based logins.
`multi-user.target`	System supports multiple users, text-based logins only.
`rescue.target`	**`sulogin`** prompt, basic system initialization completed.
`emergency.target`	**`sulogin`** prompt, **`initramfs`** pivot complete, and system root mounted on **/** read only.

- هنتكلم عن systemd target المختلفه مبدئيا ال target عباره عن ال state اللي انت عايز توصلها او ت boot ليها بمعني ان ال systemd service بتروح ت start او ت stop مجموعه من ال service وال units المختلفه علشان توصلك لل target اللي انت عايز تboot ليه
- عندنا مجموعه من systemd target المختلفه

- فعندي target مثلا اسمه graphical.target معناه ان هو هيعمل start لكل ال services وال Units اللي توصلك في الاخر لل GUI وال target ده بي support ال multiple users وال graphical وال text-based logins
- عندي target تاني اسمه multi-user.target وده كده شبه ال graphical.target بس من غير ال GUI وبي support ال multiple users وال text-based logins only
- وعندي target تاني اسمه rescue.target دهtarget احنا بندخل عليه بيقوملك زي minimum environment بنستخدمه في ال troubleshooting لو انا عندي مشكله في ال boot process او لو عندك اي مشكله في ال file system
- وعندي target تاني اسمه emergency.target بنستخدم ال targe ده في ال critical situation لو انت عندك مشكله ف انت بتدخل علي emergency.target وقالك في ال target ده ان هو بيروح يعمل mount لل file system بتاعك لل root file system بيعمله read only

➢ Selecting a Systemd Target

- عندنا target ممكن يكون جزء من target تاني علي سبيل المثال ال target اللي اسمه graphical.target ده عباره عن multiuser.target زائد + ال GUI services ونفس الكلام ال multiuser.target بي depend علي target تاني اسمه basic.target وهكذا
- لو عايز أ list ال dependencies الخاصه بأي target ممكن استخدم ال command ده

```
[root@server~]# systemctl list-dependencies graphical.target | grep target
```

```
[user@host ~]$ systemctl list-dependencies graphical.target | grep target
graphical.target
* └multi-user.target
*   ├basic.target
*   | ├paths.target
*   | ├slices.target
*   | ├sockets.target
*   | ├sysinit.target
*   | | ├cryptsetup.target
*   | | ├local-fs.target
*   | | └swap.target
```

- لو عايز أ List كل ال available target الموجوده عندي هستخدم ال command ده

```
[root@server~]# systemctl list-units --type=target --all
```

```
[user@host ~]$ systemctl list-units --type=target --all
  UNIT                      LOAD      ACTIVE   SUB    DESCRIPTION
  ------------------------------------------------------------------------------
  basic.target              loaded    active   active Basic System
  cryptsetup.target         loaded    active   active Local Encrypted Volumes
  emergency.target          loaded    inactive dead   Emergency Mode
  getty-pre.target          loaded    inactive dead   Login Prompts (Pre)
  getty.target              loaded    active   active Login Prompts
  graphical.target          loaded    inactive dead   Graphical Interface
```

Selecting a Target at Runtime

- On a running system, administrators can switch to a different target using the systemctl isolate command.

```
[root@host ~]# systemctl isolate multi-user.target
```

- Isolating a target stops all services not required by that target (and its dependencies), and starts any required services not yet started.
- Not all targets can be isolated. You can only isolate targets that have AllowIsolate=yes set in their unit files.
- For example, you can isolate the graphical target, but not the cryptsetup target.

```
[user@host ~]$ systemctl cat graphical.target | grep AllowIsolate
AllowIsolate= yes
```

- علشان أ switch مابين ال target وبعضها at runtime عن طريق ان انا بقوله systemctl isolate وبعدين اديله اسم ال target يعني for example لو ال current target بتاعي graphical.target وعايز اروح ل multi-user.target ف بقوله systemctl isolate multi-user.target ف ساعتها ال systemd هتروح ت stop كل ال services ال not required by that target service
- فيه نقطه مهمه بيقولك not all target can be isolated يعني مش كل ال target ينفع ان انت ت isolate او ت switch ليها والسيستم بتاعك شغال هو هيعمل switch بس لل target اللي عندها ال AllowIsolate بيكون بي yes
- لو انا عايز أ display ال AllowIsolate ل اي target مثلا لل graphical.target هستخدم ال command ده systemctl cat graphical.target | grep AllowIsolate

Setting a Default Target

- When the system starts, systemd activates the **default.target** target. Normally the default target in **/etc/systemd/system/** is a symbolic link to either graphical. target or multiuser. target. Instead of editing this symbolic link by hand, the **systemctl** command provides two subcommands to manage this link: **get-default** and **set-default**.

```
[root@host ~]# systemctl get-default
graphical.target
```

```
[root@host ~]# systemctl set-default multi-user.target
Removed /etc/systemd/system/default.target.
Created symlink /etc/systemd/system/default.target -> /usr/lib/systemd/system/multi-user.target
```

```
[root@host ~]# systemctl get-default
multi-user.target
```

- علشان اتحكم في ال default target عندي two command في عندي command اسمه systemctl get-default ده كده بي display ال default target بتاعك وهو بيكون by default graphical.target لو انت عامل Install ل OS بتاعك ك GUI
- في حاله لو انا عايز اغير ال default target فيه command اسمه systemctl set-default وبعدين اديله اسم ال target الجديد وليكن انا عايز ال default target يكون multi-user.target هستخدم systemctl set-default multi-user.target

Selecting a Different Target at Boot Time

This configuration change only affects a single boot, making it a useful tool for troubleshooting the boot process.To use this method of selecting a different target, use the following procedure:

1. Boot or reboot the system.
2. Interrupt the boot loader menu countdown by pressing any key (except **Enter** which would initiate a normal boot).
3. Move the cursor to the kernel entry that you want to start.
4. Press **e** to edit the current entry.
5. Move the cursor to the line that starts with **linux**.This is the kernel command line.
6. Append **systemd.unit=target.target.** For example,**systemd.unit=emergency.target.**
7. Press **Ctrl+x** to boot with these changes.

- لو انا عايز اختار target مختلف والسيستم بتاعي بيشتغل فيه عندي كده option بزوده علي ال kernel command line من ال grup الاوبشن ده systemd.unit في حاله مثلا لو انا عايز ادخل علي ال resuce.target علشان أ troubleshooting لو عندي مشكله ف بضيف الاوبشن ده systemd.unit=rescue.target علي ال kernel command line وعلشان اضيف الاوبشن ده فيه عندي مجموعه من ال steps اللي لازم اعملها

1- اول step ان انت هتعمل reboot للسيستم بتاعك
2- تاني step والسيستم بي boot up اول اما يظهرلك ال grup menu اضغط علي اي key ماعدا ال enter
3- تالت step علشان تبدء ان انت تعمل edit هتضغط علي حرف e في الكيبورد
4- رابع step هتلاقي عندك Line بيبدء بكلمه linux ال line ده بيتقال عليه kernel command line بتروح لنهايه ال line ده وت append عليه الاوبشن اللي هتضيفه وليكن هتضيف الاوبشن ده systemd.unit=rescue.target
5- اخر step ان انت بعد اما هتضيف الاوبشن هتضغط علي CTRL +X

- لو انا بالغلط عملت ال default target بتاعي reboot.target ال reboot.target معناه ان لو عملت reboot للسيستم ال systemd كل اما تيجي تقوم هتبص علي ال default target تلاقيه reboot.target ف هتعمل reboot للسيستم ف علشان نحل المشكله دي هنستخدم طريقه ال selecting a deferent target at a boot time عن طريق ان السيستم و هو بيشتغل هضيف اوبشن في ال kernel command line من ال grub ف هنعمل ال steps اللي شرحناها

او step ان انا بدخل علي ال grup

```
GRUB version 2.06

*Red Hat Enterprise Linux (5.14.0-284.11.1.el9_2.x86_64) 9.2 (Plow)
 Red Hat Enterprise Linux (0-rescue-af86da5aff3e4562b219715b46f478c3) 9.2 (→

   Use the ↑ and ↓ keys to select which entry is highlighted.
   Press enter to boot the selected OS, 'e' to edit the commands
   before booting or 'c' for a command-line.
The highlighted entry will be executed automatically in 5s.
```

تاني step ان انا اضغط علي اي key في الكيبورد وبعدين اضغط علي حرف e علشان اعمل edit

```
 Red Hat Enterprise Linux (5.14.0-284.11.1.el9_2.x86_64) 9.2 (Plow)
*Red Hat Enterprise Linux (0-rescue-af86da5aff3e4562b219715b46f478c3) 9.2 (→

   Use the ↑ and ↓ keys to select which entry is highlighted.
   Press enter to boot the selected OS, 'e' to edit the commands
   before booting or 'c' for a command-line.
```

بعد اما اضغط علي حرف e هيظهرلي kernel command line بالشكل ده وبعدين اروح علي ال line اللي بيبدء بكلمه linux

```
load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-0-rescue-af86da5aff3e4562b219715b46f478c3 root=UUID=8\
6390f1a-b5d9-4684-8574-631d35fb87b2 ro resume=UUID=c225b2df-568e-497d-889f-\
198d33b98efe rhgb quiet
initrd ($root)/initramfs-0-rescue-af86da5aff3e4562b219715b46f478c3.img

   Minimum Emacs-like screen editing is supported. TAB lists
   completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
   a command-line or ESC to discard edits and return to the GRUB menu.
```

بعد اما روحنا علي ال line اللي بيبدء بكلمه linux هضيف في اخر ال line ده الاوبشن وليكن احنا في حالتنا هنضيف systemd.unit=graphical.target بعد اما نضيف الاوبشن هنضغط علي CTRL+X

```
load_video
set gfxpayload=keep
insmod gzio
linux ($root)/vmlinuz-0-rescue-af86da5aff3e4562b219715b46f478c3 root=UUID=8\
6390f1a-b5d9-4684-8574-631d35fb87b2 ro resume=UUID=c225b2df-568e-497d-889f-\
198d33b98efe rhgb quiet systemd.unit=graphical.target_
initrd ($root)/initramfs-0-rescue-af86da5aff3e4562b219715b46f478c3.img

   Minimum Emacs-like screen editing is supported. TAB lists
   completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
   a command-line or ESC to discard edits and return to the GRUB menu.
```

Resetting The Root Password From The Boot Loader

- One task that every system administrator should be able to accomplish is resetting a lost root password. If the administrator is still logged in, either as an unprivileged user but with full sudo access, or as root, this task is trivial. When the administrator is not logged in, this task becomes slightly more involved.

- **To access that root shell, follow these steps:**

1. Reboot the system.
2. Interrupt the boot loader countdown by pressing any key, except **Enter**.
3. On the GRUB2 boot screen, use the down arrow key on your keyboard to select rescue mode.
4. Move the cursor to the kernel entry to boot.
5. Press **e** to edit the selected entry.
6. Move the cursor to the kernel command line (the line that starts with **linux**).
7. Append **rd.break.** With that option, the system breaks just before the system hands control from the **initramfs** to the actual system.
8. Press **Ctrl+x** to boot with the changes.

MOOCA MEDIA PRODUCTION

- **To Reset the Root Password From This Point, Use the Following Procedure:**

1. Remount **/sysroot** as read/write.

```
switch_root:/# mount -o remount,rw /sysroot
```

2. Switch into a chroot jail, where /sysroot is treated as the root of the file-system tree.

```
switch_root:/# chroot /sysroot
```

3. Set a new root password.

```
sh-4.4# passwd root
```

4. Make sure that all unlabeled files, including **/etc/shadow** at this point, get relabeled during boot.

```
sh-4.4# touch /.autorelabel
```

5. Type **exit** twice. The first command exits the **chroot** jail, and the second command exits the **initramfs** debug shell.

At this point, the system continues booting, performs a full SELinux relabel, and then reboots again.

MOOCA MEDIA PRODUCTION

Chapter 11

Managing Network Security

Introducing Firewalld

- **Firewalld** is a dynamic firewall manager, used to classify all network traffic into zones.
  Based on criteria such as the source IP address of a packet or the incoming network interface, traffic is diverted into the firewall rules for the appropriate zone.
  Each zone has its own list of ports and services that are either open or closed.

- **Firewalld** checks the source address for every packet coming into the system.
  If that source address is assigned to a specific zone, the rules for that zone apply.
  If the source address is not assigned to a zone, firewalld associates the packet with the zone for the incoming network interface and the rules for that zone apply.
  If the network interface is not associated with a zone for some reason, then firewalld associates the packet with the default zone.

- ال firewalld عباره عن service بقدر من خلالها أ control او أ limit ال Network Connection مع ال Servers نقدر نقول ان ال firewalld عباره عن additional layer of security علي مستوي ال network لو فاكرين قبل كده احنا اخدنا كذا موضوع متعلق بال security الموجوده عندنا في ال Linux كنا اخدنا في ادمن 1 ال standard permissions واخدنا بعدها ال special permissions وفي ادمن 2 اتكلمنا عن ال ACL وبعد كده اتكلمنا عن ال SELinux كل دي عباره عن security features علي مستوي ال file وال object الموجوده عندي علي السيرفر بتاعي لكن انا علشان اوصل لل servers من خلال ال network سواء عن طريق ال SSH او ال HTTP او ال FTP ف انا محتاج الاول ان ال firewall يكون عامل allow لل network connection علشان اقدر اوصل للسيرفر عن طريق ports او services معينه
- ببساطه ال firewalld عباره عن dynamic firewall manager بيستخدم علشان يclassify ال network traffic لمجموعه مختلفه من ال zones بتكون based علي criteria معينه
- علشان نفهم ال firewalld بيشتغل ازاي ال firewalld عنده مجموعه من ال predefined zones المختلفه بتبقي نازله معاها by default وانت ممكن بعد كده ت customize ال zones دي او تعمل create ل zones معينه كل zone من ال zones دي بتبقي فيها مجموعه من ال rules المختلفه اللي بتعمل allow او deny لأي services او port
- ال criteria اللي ال firewalld بيشتغل بيها ان اول حاجه ال firewalld بيعملها بيروح ي check علي ال source address اللي جاي منه ال traffic لل system بتاعي هل هو assigned او defined ف zone معينه ولا لا لو defined ساعتها هيروح ي apply ال rules الموجوده في ال Zone دي علي ال traffic
- تاني حاجه في حاله لو ال source address بيكون not assigned في zone معينه ساعتها هيروح يشوف ال traffic ده جاي علي انهي network interface ويشوف هل ال interface ده associated ل zone معينه ساعتها هيروح ي apply ال rules اللي في ال zone علي ال traffic

- تالت حاجه لو ال source address بيكون not defined في zone معينه وال network interface is not associated ل اي zone ساعتها هيستخدم ال default zone وهيروح ي apply الrules اللي علي ال traffic ده

Introducing firewalld

- The default zone is not a separate zone, but is a designation for an existing zone. Initially, **firewalld** designates the public zone as default, and maps the lo loopback interface to the trusted zone.
- Most zones allow traffic through the firewall, which matches a list of particular ports and protocols, such as **631/udp**, or pre-defined services, such as ssh. If the traffic does not match a permitted port and protocol or service, it is generally rejected.
(The trusted zone, which permits all traffic by default, is one exception to this.)

- ال firewall عنده حاجه اسمها default zone بيستخدمها وال default zone اسمها Public Zone و initially ال firewalld بيروح ي map كل ال network interface الموجوده عندك في ال system في ال public zone يعني من الاخر لو فيه اي traffic جاي علي ال system بتاعك علي ال interface ال firewalld هيروح ي route ال traffic ده لل public zone وساعتها هيروح ي apply عليه كل ال rules الموجوده في ال public zone سواء كان ه allow او ي deny

Pre-defined Zones

- **Firewalld** has pre-defined zones, each of which you can customize. By default, all zones permit any incoming traffic which is part of a communication initiated by the system, and all outgoing traffic. The following table details these initial zone configuration.

ZONE NAME	DEFAULT CONFIGURATION
trusted	Allow all incoming traffic.
home	Reject incoming traffic unless related to outgoing traffic or matching the ssh, mdns, ipp-client, samba-client, or dhcpv6-client pre-defined services.
internal	Reject incoming traffic unless related to outgoing traffic or matching the ssh, mdns, ipp-client, samba-client, or dhcpv6-client pre-defined services (same as the home zone to start with).
work	Reject incoming traffic unless related to outgoing traffic or matching the ssh, ipp-client, or dhcpv6-client pre-defined services.
public	Reject incoming traffic unless related to outgoing traffic or matching the ssh or dhcpv6-client pre-defined services. *The default zone for newly added network interfaces.*

MOOCA MEDIA PRODUCTION

- هنتكلم عن ال pre-defined zones المختلفه اللي بتبقي نازله by default مع ال firewalld services ونشوف ال main characteristic بتاعت كل zone فيهم

- كل ال zones الموجوده by default بت allow كل ال outgoing traffic واي incoming traffic متعلق بالoutgoing traffic

- طب ايه الفرق مابين ال outgoing traffic وال incoming traffic

- لو انت عندك مثلا server وال server ده اي traffic initiated من ال server بتاعك طالع بره ده بيتقال عليه uplink traffic او outgoing traffic بالنسبه ل outgoing traffic ال firewalld by default مش بيعمل اي limitation او control علي ال outgoing traffic يعني من الاخر كل ال outgoing traffic بيبقي allowed by default

- بالنسبه ل incoming traffic بيتقال عليه downlink traffic وده ال traffic اللي جاي للسيرفر بتاعك من بره ال incoming traffic فيه منه جزئين فيه جزء منه بيبقي جايلك as response علي ال outgoing traffic بتاعك وفيه جزء تاني بيبقي originated من ال destination وجاي من السيرفر بتاعك

- ال table ده بيعبر عن بعض ال pre-defined zones المختلفه وال initial configuration الموجوده علي كل واحده فيهم

Zone name	Default configuration
trusted	دي بت allow كل ال incoming traffic ان اي traffic بي match علي ال trusted zone ال firewall هيعملها allow
home	ال home zone بت reject كل ال incoming traffic unless ان هو related لل outgoing traffic او بي match علي اي service من ال pre-defined services زي ال ssh, mdns, ipp-client, samba-client, or dhcpv6-client,
internal	ال intial configuration شبه ال home بالظبط
work	ال work بت reject كل ال incoming traffic unless ان هو related لل outgoing traffic او بي match علي اي service من ال pre-defined services زي ال ssh, ipp-client, or dhcpv6-client
public	ودي بتكون ال default zone عندنا وال public zone بت reject كل ال incoming traffic unless ان هو related للtraffic outgoing او بي match علي اي service من ال pre-defined services زي ال ssh or dhcpv6-client
dmz	ال *work* بت *reject* كل ال *incoming traffic unless* ان هو *related* لل *outgoing traffic* او بي *match* علي اي *service* من ال *pre-defined services* زي ال *ssh* كانك جوه ال *dmz zone* عامل *allow* بس لل *ssh*
block	بتعمل *reject* لكل ال *incoming traffic unless* ان هو *related* للtraffic *outgoing* بس هنا هي *respond* لل *server* بال *error*
drop	في ال *drop* هتعمل *drop* للtraffic *incoming* ومش هت *respond*

Pre-defined Services

- Firewalld has a number of pre-defined services. These service definitions help you identify particular network services to configure. Instead of having to research relevant ports for the **samba-client** service, for example, specify the pre-built **samba-client** service to configure the correct ports and protocols. The following table lists the pre-defined services used in the initial firewall zones configuration.
- Use **firewall-cmd --get-services** to list them

SERVICE NAME	CONFIGURATION
ssh	Local SSH server. Traffic to 22/tcp
dhcpv6-client	Local DHCPv6 client. Traffic to 546/udp on the fe80::/64 IPv6 network
ipp-client	Local IPP printing. Traffic to 631/udp.
samba-client	Local Windows file and print sharing client. Traffic to 137/udp and 138/ udp.
mdns	Multicast DNS (mDNS) local-link name resolution. Traffic to 5353/udp to the 224.0.0.251 (IPv4) or ff02::fb (IPv6) multicast addresses.

- من ضمن ال features المهمه الموجوده في ال firewalld services ان بيبقي نازل معاها مجموعه من ال pre-defined services المختلفه اللي بتساعدك و بتسمحلك انك ت allow سيرفز معينه باستخدام ال pre-defined services

- احنا عارفين ان كل services عندنا بت listen علي port معين او ممكن يكون عندك service بتستخدم اكتر من protocol او port ف انت علشان ت allow سيرفز معينه في ال firewall عندك two options ي اما تعمل search علي كل ال relevant port وال protocols اللي السيرفز دي بتستخدمها و تروح تعملها allow في ال firewall او ببساطه عندك مجموعه من pre-defined services بتبقي موجوده عند ال firewall ممكن تستخدمها علشان تعمل allow لل traffic بتاع ال service عندك مثلا service اسمها samba-client دي ال service المسئوله عن ال windows file sharing ال service دي بتعتمد علي two ports بتعتمد علي port 137/udp و port 138/udp ف قالك بدل اما تعمل allow لل two ports او تعمل search علي ال ports اللي ال samba-client بتستخدمها علي طول انت ممكن تستخدم built in pre-defined services ان انت ت allow عن طريقها ال traffic بتاع ال samba-client

- علشان اجيب معلومات اكتر وأ list كل ال pre-defined services الموجوده عند ال firewall فيه command احنا بنستخدمه اسمه firewall-cmd --get-services ف احنا عندنا بعض ال pre-defined services زي

Service name	Configuration
ssh	Local SSH server. Traffic to 22/tcp.
dhcpv6-client	Local DHCPv6 client. Traffic to 546/udp on the fe80::/64 IPv6network.
ipp-client	Local IPP printing. Traffic to 631/udp.
samba-client	Local Windows file and print sharing client. Traffic to 137/udp and 138/ udp.
mdns	Multicast DNS (mDNS) local-link name resolution. Traffic to 5353/udpto the 224.0.0.251 (IPv4) or ff02::fb (IPv6) multicast addresses.

Configuring The Firewall

- System administrators interact with **firewalld** in three ways:
  - Directly edit configuration files in **/etc/firewalld/** (not discussed in this chapter)
  - The graphical interface
  - The **firewall-cmd** command-line tool

- علشان نبدء ن manage ال firewalld service عندنا 3 طرق

1- اول طريقه عن طريق ان احنا ن edit ال directly في ال files بتاعت ال firewalld وعندنا ال files بتاعت ال firewalld بتبقي stored في two different location اول location بيبقي stored جواه ال default configuration بتاعت ال firewall بتبقي stored تحت /usr/lib/firewalld وال location ده مش recommended انك ت edit فيه علشان ده بيستخدم في حاله لو انت عايز ت roll back او ت restore ال default configuration بتاعتك اما لو انت عايز ت edit هت edit في ال location ده تحت /etc/firewalld/ ده ال location اللي انت recommended انك ت edit فيه

2- تاني طريقه عن طريق ال graphical tools عندنا two tools عندنا tool اسمها firewall-config دي بتعملها install وتقدر من خلالها ت configure ال firewall وعندنا طريقه تانيه عن طريق services اسمها Cockpit

3- تالت طريقه ودي اللي هنركز عليها عن طريق ال CLI Tool الي اسمها firewall-cmd

Configuring the Firewall from the Command Line

- The **firewall-cmd** command interacts with the **firewalld** dynamic firewall manager. It is installed as part of the main firewalld package and is available for administrators who prefer to work on the command line, for working on systems without a graphical environment, or for scripting a firewall setup.

- The following table lists a number of frequently used **firewall-cmd** commands, along with an explanation. Note that unless otherwise specified, almost all commands will work on the runtime configuration, unless the **--permanent** option is specified.
  If the **--permanent** option is specified, you must activate the setting by also running the **firewall-cmd -reload** command, which reads the current permanent configuration and applies it as the new runtime configuration.

- الطريقه اللي هنركز عليها وهي ال firewall-cmd وال command بيبقي installed by default مع ال firewalld package وال command ده هو ال most common used في شغلنا بالاخص لو انت بتتعامل مع systems without a graphical environment ف انت ساعتها مش هتعرف تستخدم ال GUI Tool وكمان لو انت عايز تعمل automation او عايز تعمل script ل firewall setup ف انت بتستخدم معاها ال firewall-cmd
- اي change او اي command بتعمله execute بال firewall-cmd بيتعمله execute في ال runtime بمجر انك عملت reload لل service او عملت restart او عملت full system reboot ف ساعتها ال

runtime configuration هتطير ولا كانها موجوده الا لو انت بتعمل execute ل اي command زودت الاوبشن ده permanent-- فساعتها هيخلي اي change يكون permanent بس ف حاله لو انت استخدمت الاوبشن ده permanent-- لازم تعمل firewall-cmd --reload علشان ت reload ال firewall بتاعك وت activate ال permanent configuration بتاعتك

Configuring the Firewall from the Command Line

FIREWALL-CMD COMMANDS	EXPLANATION
`--get-default-zone`	Query the current default zone.
`--set-default-zone=ZONE`	Set the default zone. This changes both the runtime and the permanent configuration.
`--get-zones`	List all available zones.
`--get-active-zones`	List all zones currently in use (have an interface or source tied to them), along with their interface and source information.
`--add-source=CIDR [--zone=ZONE]`	Route all traffic coming from the IP address or network/netmask to the specified zone. If no `--zone=` option is provided, the default zone is used.
`--remove-source=CIDR [--zone=ZONE]`	Remove the rule routing all traffic from the zone coming from the IP address or network/ netmask network. If no `--zone=` option is provided, the default zone is used.
`--add-interface=INTERFACE [--zone=ZONE]`	Route all traffic coming from *INTERFACE* to the specified zone. If no `--zone=` option is provided, the default zone is used.

`--change-interface=INTERFACE [--zone=ZONE]`	Associate the interface with *ZONE* instead of its current zone. If no `--zone=` option is provided, the default zone is used.
`--list-all [--zone=ZONE]`	List all configured interfaces, sources, services, and ports for *ZONE*. If no `--zone=` option is provided, the default zone is used.
`--list-all-zones`	Retrieve all information for all zones (interfaces, sources, ports, services).
`--add-service=SERVICE [--zone=ZONE]`	Allow traffic to *SERVICE*. If no `--zone=` option is provided, the default zone is used.
`--add-port=PORT/PROTOCOL [--zone=ZONE]`	Allow traffic to the *PORT/PROTOCOL* port(s). If no `--zone=` option is provided, the default zone is used.
`--remove-service=SERVICE [--zone=ZONE]`	Remove *SERVICE* from the allowed list for the zone. If no `--zone=` option is provided, the default zone is used.

- ال table ده بيوضح مجموعه من ال most common used options اللي احنا بنستخدمها كتير مع ال firewall-cmd command و description عن كل option فيهم وزي ماحنا شايفين ال options كلها بتبدء بي - - وعندنا category بيبدء ب get - - وcategory تانيه بتبدء ب set - - و category بتبدء ب add - - وهكذا
- وفي option عندي بيكون في ال command وهو [- -zone=ZONE] ده بستخدمه لو انا عايز ال command يتطبق علي zone معينه وده option ممكن تستخدمه او متستخدمهوش زي ماهنشوف في ال table

firewall-cmd commands	Explanation
`--get-default-zone`	بستخدمه لو عايز اعمل display لل current default zone وال default zone بيكون public الا لو انا غيرتها
`--set-default-zone=ZONE`	بستخدمه في حاله لو عايز اعمل change لل default zone
`--get-zones`	بستخدمه لو انا عايز أ list كل ال available zones
`--get-active-zones`	بستخدمه لو عايز اعمل display لكل ال active zones اللي هي مستخدمه حاليا
`--add-source=CIDR [--zone=ZONE]`	بستخدمه لو انا عايز اعمل add ل source address معين في zone
`--remove-source=CIDR [--zone=ZONE]`	بستخدمه لو انا عايز اعمل remove ل source address معين في zone
`--add-interface=INTERFACE [--zone=ZONE]`	بستخدمه لو انا عايز اعمل add ل interface في zone معينه ف بستخدم ال command ده
`--change-interface=INTERFACE [--zone=ZONE]`	لو انا عندي ال Interface مثلا added في zone معينه وعايز ان انت ت migrate او ت move ال interface ده ل new zone ف بستخدم ال command ده

`--list-all [--zone=ZONE]`	الcommand ده لو انا محددتلهوش اي zone هيروح ي list كل ال configuration بتاعت ال default zone لو انا عايزه يعمل List ل zone معينه هستخدم الاوبشن =zone-- واحددله ال zone
`--list-all-zones`	بستخدمه لو انا عايز اعمل display لكل ال information بتاعت كل ال zones ال defined عندي في السيستم من حيث ال interfaces وال sources وال ports وال services
`--add-service=SERVICE [--zone=ZONE]`	بستخدمه لو انا عايز اعمل add ل service معينه
`--add-port=PORT/PROTOCOL [--zone=ZONE]`	بستخدمه لو انا عايز اعمل add ل port معين
`--remove-service=SERVICE [--zone=ZONE]`	بستخدمه لو انا عايز اعمل remove ل service معينه
`--remove-port=PORT/PROTOCOL [--zone=ZONE]`	بستخدمه لو انا عايز اعمل remove ل port معين

- **تعال نطبق اللي احنا شرحناه ونشوف ازاي نتعامل مع ال firewall من خلال ال CLI**

- اول حاجه علشان اتاكد هل ال firewall معمول ليه running او not running هستخدم systemctl status firewalld.service

```
[root@MohamedAtef ~]# systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset>
```

- او ممكن استخدم firewall-cmd –state هيعرضلي هل ال firewall معمول ليه enable ولا disable

```
[root@MohamedAtef ~]# firewall-cmd --state
running
```

- لو ال firewall معمول ليه disable وانا عايز اعمله enable و start هستخدم

```
[root@MohamedAtef ~]# systemctl enable --now firewalld.service
```

- في حاله لو عايز اعمل List لكل ال supported options اللي مع ال firewall-cmd command هقوله firewall-cmd -- وبعدين اضغط علي tab مرتين ف هو هيعرضلك كل ال options اللي ممكن تستخدمها

```
[root@MohamedAtef ~]# firewall-cmd --
Display all 101 possibilities? (y or n)
```

بعد اما اكتب firewall-cmd – واضغط علي tab مرتين هيعرضلي كل ال options وعددهم تقريبا 101

- لو انا عايز اعمل List لكل ال available zones الموجوده عندي في ال system

```
[root@MohamedAtef ~]# firewall-cmd --get-zones
block dmz drop external home internal libvirt libvirt-routed nm-shared public trusted work
```

- لو انا عايز اعرف ال active zones الموجوده عندي

```
[root@MohamedAtef ~]# firewall-cmd --get-active-zones
public
  interfaces: ens160
```

- لو عايز اعرف ال default zone

```
[root@MohamedAtef ~]# firewall-cmd --get-default-zone
public
```

- لو انا عايز أ list كل ال pre-defined services الموجوده عندي ان انا لو عايز اعمل allow ل services معينه وعايز اتاكد هل ال service دي موجوده عند ال firewall ولا لا هستخدم

```
[root@MohamedAtef ~]# firewall-cmd --get-services
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit
ausweisapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd
ceph ceph-mon cfengine checkmk-agent cockpit collectd condor-collector cratedb ctdb dhcp dhcpv6 dhcpv6-
client distcc dns dns-over-tls docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-
server finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp
galera ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs
ipp ipp-client ipsec irc ircs iscsi-target isns jellyfin jenkins kadmin kdeconnect kerberos kibana klogin kpasswd
```

- ممكن تستخدم ال grep علشان تتاكد ان service معينه موجوده علي ال firewall وليكن مثلا هعمل allow ل HTTP Service ممكن استخدم ال grep ولما استخدم ال grep command بي حددلي كل ال key word او pre-defined services الخاصه بال HTTP

```
[root@MohamedAtef ~]# firewall-cmd --get-services | grep http
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit
ausweisapp2 bacula bacula-client bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd
finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera
ganglia-client ganglia-master git gpsd grafana gre high-availability http http3 https ident imap imaps ipfs ipp -
murmur mysql nbd netbios-ns netdata-dashboard nfs nfs3 nmea-0183 nrpe ntp nut openvpn ovirt-imageio ovirt-
ssdp ssh steam-streaming svdrp svn syncthing syncthing-gui synergy syslog syslog-tls telnet tentacle tftp tile38
tinc tor-socks transmission-client upnp-client vdsm vnc-server wbem-http wbem-https wireguard ws-
```

- لو انا عايز اعرف ال location بتاعت ال zones وال services وال files الخاصه بيهم موجوده فين هنلاقي كل ال files تحت /usr/lib/firewalld/ هنلاقي عندنا two folders هنلاقي folder اسمه services و folder اسمه zones ولو دخلنا علي اي folder هنلاقي جواه مجموعه من ال xml file لكل service او ال zone وجوه ال xml file هنلاقي فيه information عن ال service او ال zone

```
root@MohamedAtef ~]# cd /usr/lib/firewalld/
[root@MohamedAtef firewalld]# ls
helpers  icmptypes  ipsets  policies  services  zones
```

- في حاله لو عايز اعمل display لكل ال enable features او ال configuration بتاعت zone معينه عندي option تاني اسمه -list-all - لو انا استخدت الاوبشن ده بدون ماحددله اي zone هو هيعمل display لل default zone وهي ال public zone

```
[root@MohamedAtef ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client mountd nfs rpc-bind ssh
  ports: 3260/tcp
  protocols:
```

هنلاقي هنا قايلك ان ال default zone هي ال public ومعمول ليها active

وقايلك هنا ان ال target هو ال default

وقايلك ال interfaces ال added عندك في ال public zone هي ens160

وكمان قايلك ان ال services ال allowed هي ال cockpit وال dhcpv6 وال nfs وال ssh وrpc-bind

- لو انا عايز أdisplay ال enable futures او ال initial configuration بتاعت zone معينه بيبقي نفس ال command بس بزود zone-- وبعدين يساوي وبعدين احددله اسم ال zone بتاعتي وليكن انا عايز أ display ال initial configuration بتاعت ال zone اللي اسمها internal

```
[root@MohamedAtef ~]# firewall-cmd --list-all --zone=internal
internal
  target: default
  icmp-block-inversion: no
  interfaces:
  sources:
  services: cockpit dhcpv6-client mdns samba-client ssh
  ports:
  protocols:
```

- لو انا عايز أ display كل ال enable futures بتاعت كل ال pre-defined zones الموجوده عندي

```
[root@MohamedAtef ~]# firewall-cmd --list-all --zone=internal
```

- لو انا عندي interface وليكن ens160 وعايز اعرف ال interface ده منضاف في zone معينه ولالا بستخدم

```
[root@MohamedAtef ~]# firewall-cmd --get-zone-of-interface=ens160
public
```

هنلاقي هنا قايلك ان ال ens160 منضاف في ال public zone

- لو انا عايز اعمل add ل new interface هستخدم

```
[root@MohamedAtef ~]# firewall-cmd --add-interface=ens160
success
```

- لو انا عندي interface معمول ليه add في zone معينه وجيت عملت add لنفس ال interface هيطلعلك error ويقولك ان ال interface ده موجود وليكن انا عامل add ل ens160 في ال zone وعايز اضيف ال interface ده في ال نفس ال zone هيطلعلك warning

```
[root@MohamedAtef ~]# firewall-cmd --add-interface=ens160
Warning: ZONE_ALREADY_SET: 'ens160' already bound to ''
success
```

- لو انا عايز اعمل add ل new interface علي zone معينه هستخدم

```
[root@MohamedAtef ~]# firewall-cmd --add-interface=ens124 --zone=public
success
```

- لو انا عايز اعمل remove ل interface موجود علي zone معينه

```
[root@MohamedAtef ~]# firewall-cmd --remove-interface=ens124 --zone=public
success
```

- لو انا عايز اعرف هل ال interface موجود في zone ولا لا هستخدم اوبشن اسمه query-interface- - وليكن انا عايز اعرف هل ال interface ده ens160 موجود في Zone ولا لا

```
[root@MohamedAtef ~]# firewall-cmd --query-interface=ens160
yes
```

قالك yes هو فعلا معمول ليه add في zone

- طب هل ال interface اللي اسمه lo موجود في zone

```
[root@MohamedAtef ~]# firewall-cmd --query-interface=lo
no
```

قالك no هو مش معمول ليه add في اي zone

- لو عايز اعرف كل ال services الموجوده في zone معينه

```
[root@MohamedAtef ~]# firewall-cmd --list-services --zone=public
cockpit dhcpv6-client mountd nfs rpc-bind ssh
```

- علشان اعمل reload لل firewall علشان يعمل roll back لكل ال changes اللي عملناها في ال runtime

```
[root@MohamedAtef ~]# firewall-cmd --reload
success
```

- لو انا عايز اضيف service معينه في ال firewall وليكن عايز اعمل add ل ال http

```
[root@MohamedAtef ~]#  firewall-cmd --add-service=http
success
```

- لو هعمل remove ل service معينه

```
[root@MohamedAtef ~]#  firewall-cmd --remove-service=http
success
```

- لو انا عايز اعمل add ل service من خلال ال port وليكن هعمل add ل ال http من خلال ال port وانا بحدد ال port لازم احددله هل ال port ده tcp ولا udp

```
[root@MohamedAtef ~]#  firewall-cmd --add-port=80/tcp
success
```

- علشان اتاكد هل ال port اتعمله add ولا لا هستخدم

```
[root@MohamedAtef ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client mountd nfs rpc-bind ssh
  ports: 3260/tcp 80/tcp
```

هنلاقيه هنا عمل add لل port 80/tcp

- زي ماقولنا لو انا عايز ايchange انا بعمله يكون دائم لو عملت reboot للسيستم يكون موجوده ف انا هستخدم الاوبشن ده permanent-- في نهايه ال command وليكن مثلا لو انا هضيف نفس ال port الخاص بال http ويكون دائم هستخدم

```
[root@MohamedAtef ~]#  firewall-cmd --add-port=80/tcp --permanent
```

- زي ماقولنا في حاله ال runtime mode اي ت change انت بتعمله مبيكونش permanent بمجرد انك عملت reload او start لل firewalld service ال change اللي انت عملتها في ال runtime بيتعملها delete اتوماتيك . لو انا عايز اعمل enable ل service او port معين في ال runtime لوقت معين وبمجرد ان الوقت ده خلص يتعمل delete لل change ده هستخدم اوبشن timeout-- وبعدين ال number of second وليكن مثلا انا عايز اعمل add ل http service في ال zone اللي اسمها public ويكون ال timeout يكون 60 ثانيه ان بعد 60 ثانيه هيعمل delete لل http service

```
[root@MohamedAtef ~]#  firewall-cmd --add-service=http --zone=public --timeout=60
success
```

- علشان اعمل create ل new custom service او zoneعن طريق ان انا ادخل تحت ال Location ده /etc/firewalld/ واعمل create ل اي customize configuration انا عايزها
- تعال ندخل تحت ال location ده /etc/firewalld/ ونعمل list ونشوف اللي تحتيه هنلاقي عندنا folders من ضمنها two folders وهما ال services وال zones لو هعمل create ل custom service هعمل create جوه ال folder اللي اسمه services ولو عمل custom zone هعمل create جوه ال folder اللي اسمه zones

```
[root@MohamedAtef ~]# cd /etc/firewalld/
[root@MohamedAtef firewalld]# ls
firewalld.conf  icmptypes  lockdown-whitelist.xm  services  helpers  ipsets  policies  zones
```

- علشان اعمل custom service عن طريق ان انا هدخل تحت المسار ده /etc/firewalld/services/ وهعمل copy ل file معين من الfiles الموجوده في ال Location ده /usr/lib/firewalld/services/ واحنا قولنا ان ال Location ده مش recommended ان اعدل فيه وبعد اما اخد copy من ال file الموجوده في ال services هسميه باي اسم انا عايزه وبعدين اعدل في ال file زي منا عايز . وليكن مثلا عايز اعمل new services اسمها myssh واحط جواها ال port الجديد ف انا هاخد copy من ال file اللي اسمه ssh.xml الموجوده في المسار ده /usr/lib/firewalld/services/ وبعدين اسميه مثلا myssh.xml

```
[root@MohamedAtef services]# cp /usr/lib/firewalld/services/ssh.xml myssh.xml
```

- ف انا ممكن افتح ال file ده myssh.xml واعدل فيه وبعد اما نعدل لازم نعمل reload لل firewall
- لو انا عايز اعمل new custom zone فيه عندي طريقتين اول طريقه ان انا انا اقوله اوبشن new-zone-- وبعدين اضيف اسم ال zone الجديده وليكن هنسميها mgmt_zone

```
[root@MohamedAtef zones]# firewall-cmd --permanent --new-zone=mgmt_zone
success
```

- بعد كده هنعمل reload لل firewall علشان يحس بالتغيير

```
[root@MohamedAtef zones]# firewall-cmd --reload
success
```

- لو جينا دخلنا تحت /etc/firewalld/zones/ وعملنا ls هنلاقي ال zone اللي احنا عملنا ليها create

```
[root@MohamedAtef zones]# ls
mgmt_zone.xml  public.xml  public.xml.old
```

- تاني طريقه ان انا هدخل تحت ال location ده /etc/firewalld/zones/ وهعمل copy ل zone موجوده عندي بال zone الجديده وبعدين هعدل في ال file

```
[root@MohamedAtef zones]# cp public.xml services_zone.xml
```

- في حاله لو عندي critical situation او attack قدر انه يوصل علي ال servrer بتاعي وعايز اعمل block لكل ال incoming وال outgoingtraffic الموجوده عندي لحد اما المشكله تتحل ف فيه عندي اوبشن اسمه panic-on بعمله enable

```
[root@MohamedAtef ~]# firewall-cmd --panic-on
```

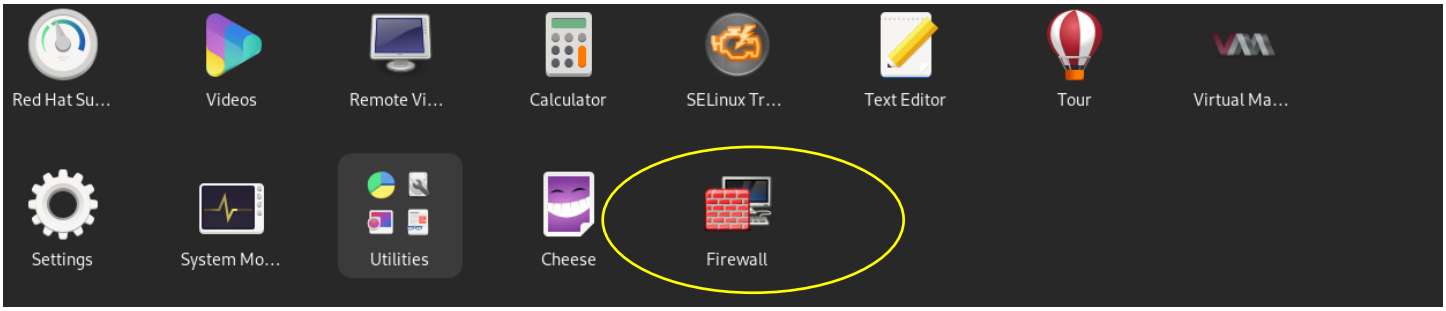
- لو انا عايز اعمل disable لل panic بقوله اوبشن panic-off--

Interact with firewalld using graphical interface

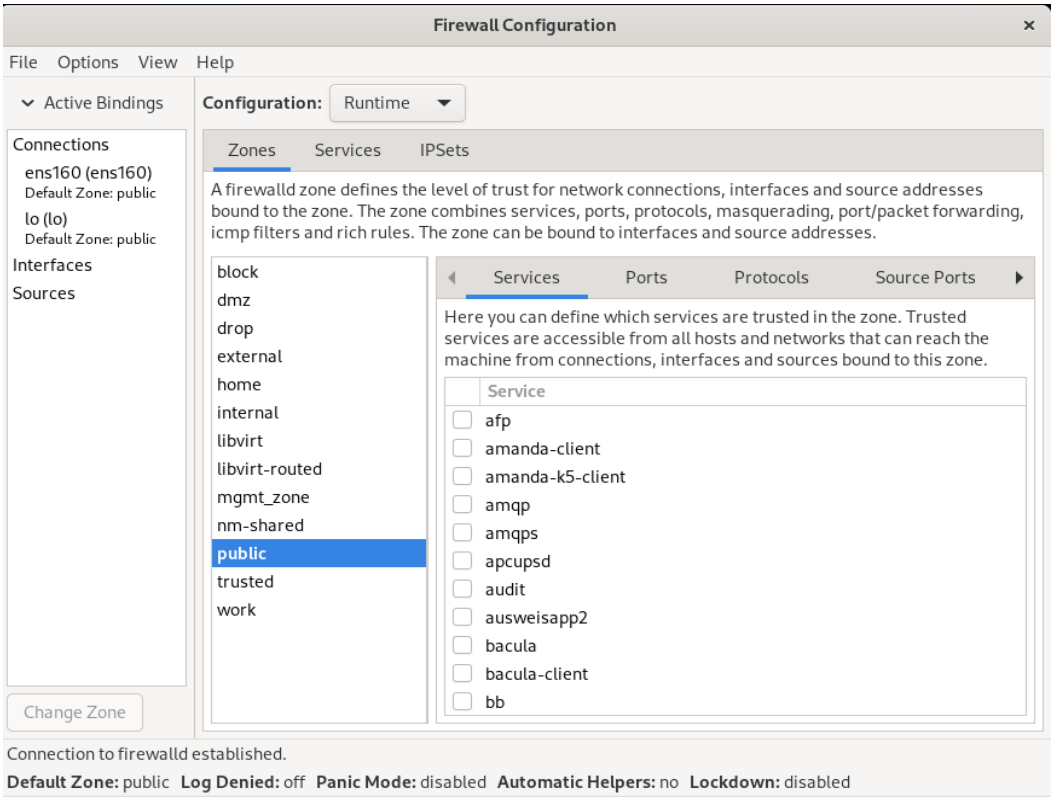
- احنا شوفنا لحد دلوقتي ازاي نmanage ون configure الfirewall عن طريق ال CLI باستخدم ال firewall-cmd وشوفنا كمان بعض ال configuration file وازاي ن edit فيها وازاي ن create new zones وازاي ن create new services عن طريق ال configuration file اللي stored تحت /etc/firewalld/. الطريقه التالته ان احنا نconfigure او ن manage ال firewall عن طريق ال GUI وزي ماقولنا احنا عندنا two GUI tools عندنا tool اسمها firewall-config ودي مبتكونش installed by default انت بتعملها Install وتقدر من خلال ال application ده انك ت manage وconfigure ال firewall . وفيه عندنا tool تانيه اسمها Cockpit ودي عباره عن web interface بت manage منه ال server بتاعك وفيه عنده feature من ضمن ال features انه بيسمحلك انك ت manage وت configure ال firewall
- هنعمل install ل اول tool وهي ال firewall-config

```
[root@MohamedAtef ~]# dnf install firewall-config-1.2.1-1.el9.noarch
```

- بمجرد ان احنا عملنا install هنلاقي عمل create ل application علي ال GUI بتاعتك اسمه firewall



- لو شغلنا ال application هنقدر من خلاله اننا ن manage ال firewall



Interact with firewalld using Cockpit

- الطريقه التانيه اللي بقدر من خلالها أ manage ال firewall عن طريق service اسمها Cockpit وال service دي بتبقي install by default

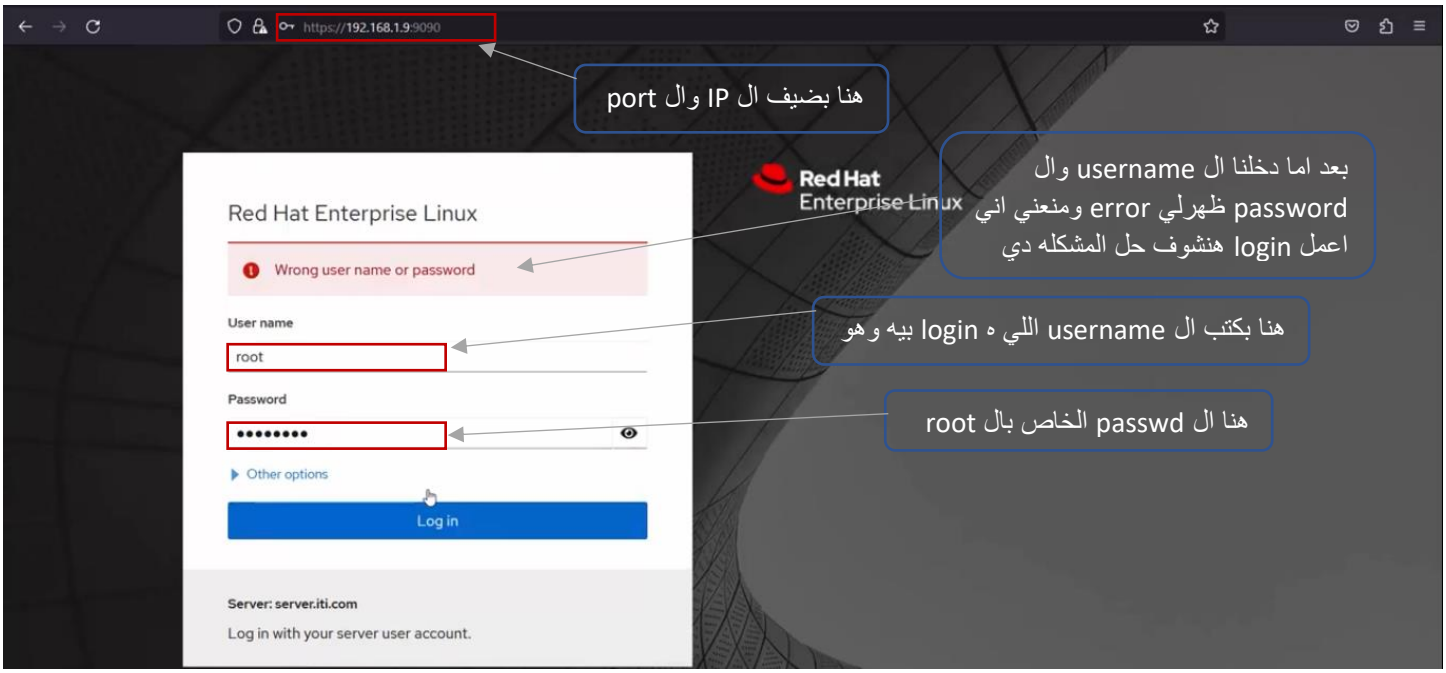
```
[root@MohamedAtef ~]# dnf install firewall-config-1.2.1-1.el9.noarch
```

- علشان أ access ال Cockpit عن طريق ال browser بحط ip ال server وبحط ال port بتاع ال Cockpit
- علشان اعرف ال Cockpit بت listen علي انهي port فيه عندي طريقه ان انا ادخلت تحت ال location ده /usr/lib/firewalld/services/ واعمل cat ل xml الخاص بال Cockpit

```
[root@MohamedAtef ~]# cd /usr/lib/firewalld/services/
 [root@MohamedAtef services]# cat cockpit.xml
<?xml version="1.0" encoding="utf-8"?>
<service>
  <short>Cockpit</short>
  <description>Cockpit lets you access and configure your server remotely.</description>
  <port protocol="tcp" port="9090"/>
</service>
```

هنلاقيه هنا قايلك ال port ال cockpit بتlisten عليه هو 9090

- هندخل علي ال browser ونكتب في ال URL ال ip وبعدين احط البورت 9090



- ال Cockpit by default بتبقي عامله deny لل root access ف قالك wrong user name or password
- فيه عند file تحت /etc/cockpit/ اسمه disallowed-users ال disallowed-users بيبقي حاطط فيه ال users اللي هما not allowed ان هما يدخلوا علي ال Cockpit web interface ف انا هفتح ال file ده واعمل هاش او comment لل line اللي فيه ال root وبعد كده لو عملت login هيدخل ومش هيحصل اي مشكله

```
[root@MohamedAtef ~]# vim /etc/cockpit/disallowed-users
# List of users which are not allowed to login to Cockpit
# root
```

هعمل للline اللي فيه ال root هعمله # او comment

student@
servera.lab.example....

Administrative access | Help | Session

Search

System
Overview
Logs
Networking
Accounts
Services

Kbps Transmitting

Kbps Receiving

Firewall

1 active zone

Edit rules and zones

student@
servera.lab.example....

Administrative access | Help | Session

Search

System
Overview
Logs
Networking
Accounts
Services
Tools
Applications

Networking > Firewall

Firewall

Add zone

public zone Interfaces eth0

Add services

Service	TCP	UDP
ssh	22	

Secure Shell (SSH) is a protocol for logging into and executing commands on remote machines. It provides secure encrypted communications. If you plan on accessing your machine remotely via SSH over a firewalled interface, enable this option. You need the openssh-server package installed for this option to be useful.

dhcpv6-client		546
cockpit	9090	

Add services to public zone

Services Custom ports

Filter services

- RH-Satellite-6
  TCP: 5000, 5646-5647, 5671, 8000, 8080, 9090, 8140 UDP: 68
- RH-Satellite-6-capsule
  TCP: 8443, 5000, 5646-5647, 5671, 8000, 8080, 9090
- amanda-client
  TCP: 10080 UDP: 10080
- amanda-k5-client

Add services Cancel

- اخر point هنشرحها وهي حاجه اسمها rich rules ودي من ضمن ال enable futures بتسمحلك ال rich rules انك تعمل add more complex و more flexible rules في ال firewall وليكن عندك specific IP عايز تفتحله specific service

- لو عملنا display لل default zone هنلاقي من ضمنها ال rich rules

```
[root@MohamedAtef ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client mountd nfs rpc-bind ssh
  ports: 3260/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

هنلاقي هنا ال rich rules

- علشان اعمل add ل new rich rules بيبقي command طويل شويه بالمنظر ده

```
[root@MohamedAtef ~]# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.8/32" service name="http" accept'
```

ال command بيكون عباره عن ان انا بقوله firewall-cmd ان انا عايز اعمل add في ال public zone ف بقوله zone=public– وعايز اعمل new rich rule ف بقوله add-rich-rule= – وبعدين بين ' ' single quotes بحطله كل ال configuration بتاعت ال rich rule ان انا عايز اعمل create ل rule ال family بتاعتها ipv4 وال source address اللي هو ال ip بتاع ال client ان انا عايز اعمله allow لل http وفي الاخر اضيف الاكشن ان انا عايز اعمل drop او reject او accept ف انا عايز أ accept ان اي incoming traffic من ال source address اللي احنا حددناه اعمله allow لل http

- لو عملنا تاني display لل default zone علشان نشوف ال rich rules

```
[root@MohamedAtef ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client mountd nfs rpc-bind ssh
  ports: 3260/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
      rule family="ipv4" source address="192.168.1.8/32" service name="http" accept
```

هنلاقي عمل add ل new rich rules

- لو انا عايز اعمل rich rules تعمل drop مثلا لinterface معين وليكن ل 192.168.1.9 ان اي incoming traffic جاي من ال interface ده اعمله drop

```
[root@MohamedAtef ~]# firewall-cmd --zone=public --add-rich-rule='rule family="ipv4" source address="192.168.1.9/32" drop'
```

- لو عملنا تاني display لل default zone علشان نشوف ال rich rules

```
[root@MohamedAtef ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client mountd nfs rpc-bind ssh
  ports: 3260/tcp
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
        rule family="ipv4" source address="192.168.1.9/32" drop
        rule family="ipv4" source address="192.168.1.8/32" service name="http" accept
```

هنلاقي عمل drop ل new rich rules اللي Interface بتاعه 192.168.1.9

- لو عايزين نعمل roll back عن كل اللي عملناه هقوله firewall-cmd --reload

```
[root@MohamedAtef ~]# firewall-cmd --reload
success
```

Chapter 12

Installing Red Hat Enterprise Linux

Automating Installation with Kickstart

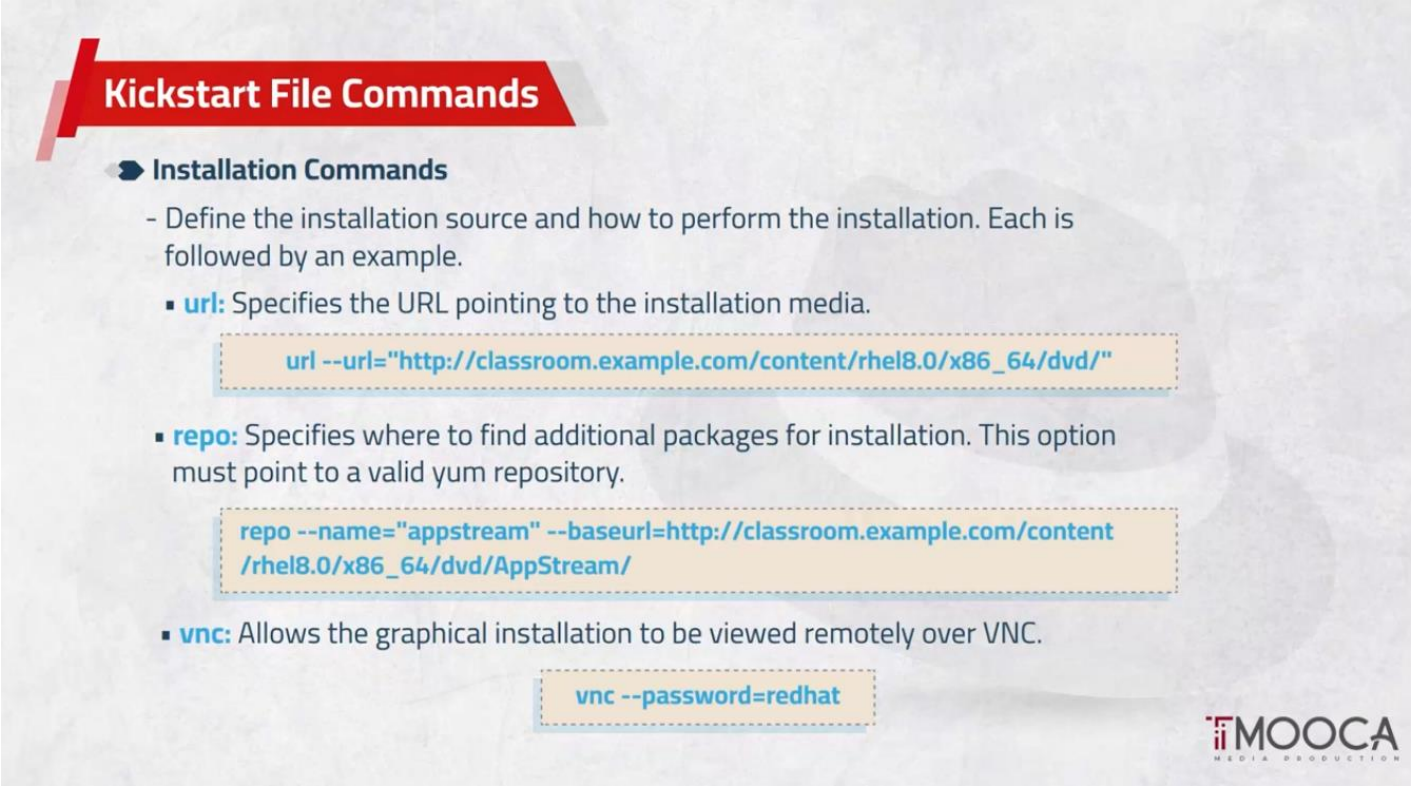
Automating Installation With Kickstart

- You can automate the installation of Red Hat Enterprise Linux using a feature called ***Kickstart***. Using Kickstart, you specify everything **Anaconda** needs to complete an installation, including disk partitioning, network interface configuration, package selection, and other parameters, in **a Kickstart text file**. By referencing the text file, Anaconda performs the installation without further user interaction.
- Kickstart files begin with a list of commands that define how to install the target machine. Lines starting with **#** characters are comments to be ignored by the installer. Additional sections begin with a directive, recognized by a **%** first character, and end on a line with the **%end** directive.
- The **%packages** section specifies the software to be installed on the target system. Specify individual packages by name (without versions). Package groups, specified by name or ID, are recognized by beginning them with an @ character. Environment groups (groups of package groups) are recognized by beginning them with the **@^** characters. Specify modules, streams, and profiles with **@** module:stream/profile syntax.

- ببساطه ال kickstart عباره عن features موجوده في اللينكس بقدر من خلالها أ automate ال installation process بتاعت red hat operating system

- كنا اتكلمنا قبل كده في admin 1 عن ال manual installation ازاي اعمل install ل red hat 9 بطريقه manual باستخدام VMware workstation وكان بيطلعلنا حاجه اسمها installation summary او بنقول عليها anaconda program وكان بيبقي فيها مجموعه من ال settings ومجموعه من ال configuration المختلفه اللي بظبطها بأيدي زي ال disk partitioning زي ال network configuration زي ال package selection وال installation media وهكذا كل الحاجات دي كنا بنجاوب عليها manual لل anaconda علشان ابدا اعمل install لل OS
- في حاله ال kickstart بيبقي عندي configuration file بنقول عليه kickstart file وال kickstart file بيبقي عباره عن pure text file مكتوب ب syntax معين هنشوف كمان شويه ازاي نعمله create و generate وبحط فيه كل ال configurations وكل ال settings بتاعت ال OS و بعد كده once ان انا عملت create لل kickstart file ب syntax معين بعمله بعد كده publish في location يبقي reachable لل server اللي بعمل install منه لل OS وبعد كده once ان انا عملت create و publish لل kickstart file بخلي ال anaconda تروح تقرأ كل ال configuration وكل ال answer بتاعتها من ال file ده بطريقه automatic من غير اي interaction مني

- انا عندي ال kickstart file بيبقي مكتوب ب syntax معين هنشوفه مع بعض كمان شويه ازاي نعمله create و generate وبيبقي فيه مجموعه من ال commands وال directives اللي بقدر من خلالها احدد ازاي اعمل install لل OS وخد بالك من حاجه ان اي Line في kickstart file بيبدء ب # ده بيبقي عباره عن comment
- عندي مثلا section او directory اسمه packages% بقدر جوه ال section ده احدد كل ال packages او كل ال groups او كل ال modules اللي انا عايز اعملها install بطريقه automatic باستخدام ال kickstart



- زي ماقولنا ان ال kickstart file بيبقي فيه مجموعه من ال commands المختلفه اللي ال anaconda program بيستخدمها علشان يعمل عمليه install لل OS بطريقه automatic من غير اي user interaction زي ال installation commands ده كده بحددله فيها ال Installation media اللي هو هيعمل Install لل OS من خلالها ف علشان احددله ال Installation media فيه عندي command بحطه جوه ال file اسمه url وبديله اوبشن =url-- وبين " " double quotes بحطه ال url بتاع ال Installation media بتاعتي سواء كان ال Installation media موجوده في http server او موجوده في NFS او FTP بحطه ال url اللي هيعمل Install من خلاله

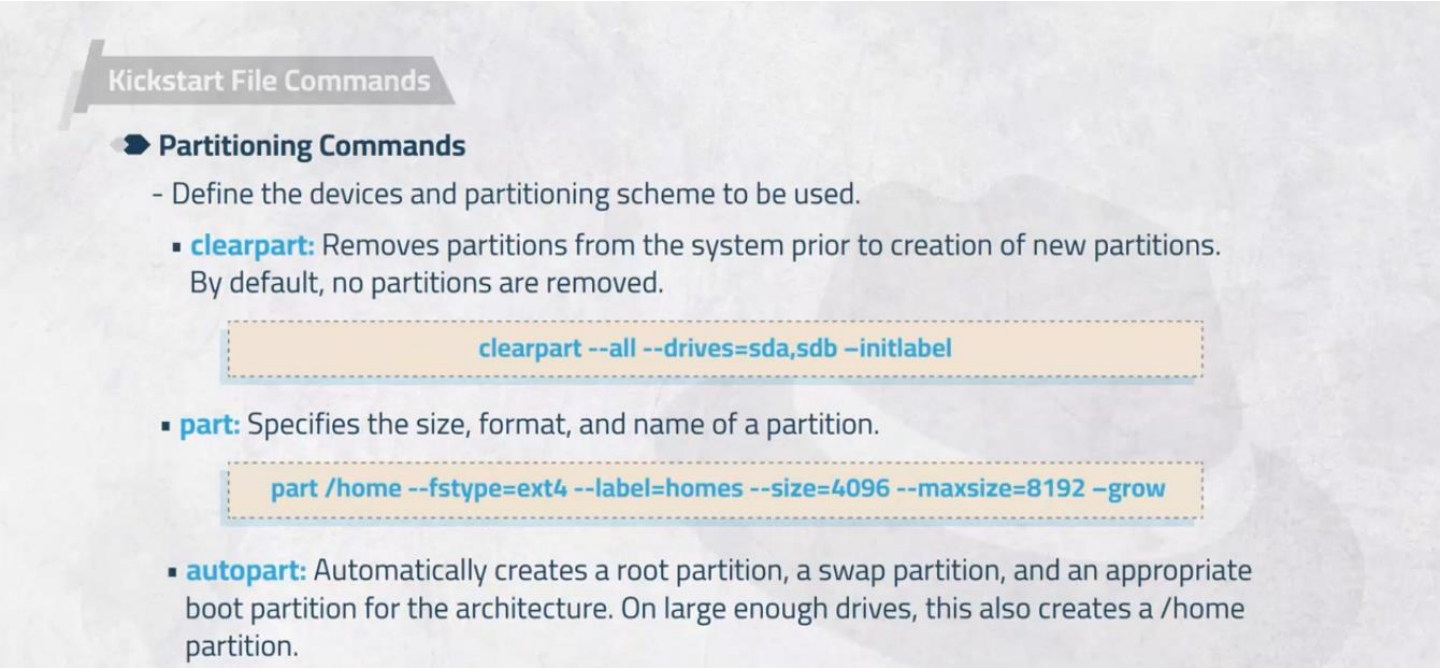
```
url --url="http://classroom.example.com/content/rhel8.0/x86_64/dvd/"
```

- اما لو انا عايز اعمل install ل اي additional packages ف في الحاله دي لازم احددله ال repository اللي هو هيدور جواه علي الباكدج بتاعته ويعملها install عندي two repository عندي ال AppStream وال BaseOS فعلشان احددله repository عندي command اسمه repo وبعدين اديله الاوبشن =name-- ومابين " " double quotes بحطه ال AppStream او ال name بتاع ال repository بتاعي وبعدين اديله ال -baseurl=

```
repo --name="appstream" --baseurl=http://classroom.example.com/content /rhel8.0/x86_64/dvd/AppStream/
```

- فيه عندي command تاني اسمه VNC ده كده بيسمحلك انك تشوف ال graphical instillation process بتاعتك remotely عن طريق ال VNC Service حاجه كده شبه ال remote desktop الموجوده عندنا في الwindows ف علشان انت ت access ال graphical instillation بتاعك remotely عن طريق ال VNC لازم تعمل set password لل VNC عن طريق ال command ده vnc --password= وبعدين تديله الباسورد

```
vnc --password=redhat
```



- عندنا section تاني اسمه Partitioning Commands وده بيكون فيه كل ال commands اللي بتكون related لل Partitioning زي command clearpart ده بنستخدمه علشان ن remove بيه كل ال Partitions الموجوده علي الهارد قبل اما نعمل create ل new partitions لان by default هو مش بيمسح ال partitions دي ف لازم تقول لل anaconda ان هي تعمل remove لكل الpartitions الموجوده علي الهارد قبل اما تعمل create ل new partitions علشان اعمل كده بستخدم

```
clearpart --all --drives=sda,sdb –initlabel
```

- علشان ابدء اعمل create ل new partition عندي كذا طريقه عندي الطريقه ال manual اوالطريقه ال standard وعندي الطريقه ال automatic وعندي الطريقه التالته وهي اني استخدم ال LVM
- ف لو انا عايز اعمل create ل new partition بالطريقه ال standard العاديه بستخدم command اسمه part عن طريق ان انا بقوله part وبعدين اديله اسم البارتشن بتاعي وليكن home/ وبعدين اديله ال file system وليكن ext4 وبعدين ال label وبعد كده بحدله ال size وعندي اوبشن كمان ان انا احددله ال maxsize

```
part /home --fstype=ext4 --label=homes --size=4096 --maxsize=8192 –grow
```

- لو انا عايز اعمل create ل new partition بالطريقه ال automatic بستخدم command تحت ال clearpart اسمه autopart ان اول اما ال anaconda يلاقي autopart هيفهم منه انك عايز تعمل automatic creation

للبارتشن بتاعتك ف هو هيروح يعمل create لل root partition وال swap partition وال /boot partition
ولو عندك مساحه فاضيه هيعملكcreate ل /home partition

Kickstart File Commands

Partitioning Commands

- Define the devices and partitioning scheme to be used.

- **ignoredisk:** Controls Anaconda's access to disks attached to the system.

```
ignoredisk --drives=sdc
```

- **bootloader:** Defines where to install the bootloader.

```
bootloader --location=mbr --boot-drive=sda
```

- **volgroup, logvol:** Creates LVM volume groups and logical volumes.

```
part pv.01 --size=8192
volgroup myvg pv.01
logvol / --vgname=myvg --fstype=xfs --size=2048 --name=rootvol --grow
logvol /var --vgname=myvg --fstype=xfs --size=4096 --name=varvol
```

MOOCA MEDIA PRODUCTION

- فيه command تاني اسمه ignoredisk لو انت عايز ال anaconda تعمل ignore ل disk معين ف بقوله ignoredisk –drives= وبعدين اسم ال disk

```
ignoredisk --drives=sdc
```

- فيه عندي command تاني اسمه bootloader ده بنستخدمه احنا عايزين نعمل install لل bootloader علي هارد درايف معين

```
bootloader --location=mbr --boot-drive=sda
```

- اما لو انا عايز اعمل create ل new partition عن طريق ال LVM زي ماحنا عارفين اول حاجه بعملها في ال LVM ان انا بعمل create ل Physical Volume ف ال syntax بتاع ال kickstart مختلف ف انا هقوله part وبعدين اديله اسم ال Physical Volume وبعدين اديله ال size بعد كده هعمل create ل Volume Group عن طريق ان انا اقوله volgroup وبعدين اديله اسم ال Volume Group وبعدين اديله اسم ال Physical Volume بعد اما عملت create لل Volume Group بعمل create ل مجموعه من ال Logical Volume عن طريق ان اقوله logvol / وبعدين احددله ال Volume Group وبعدين ال file system وبعدين ال size وبعدين اديله اسم ال Logical Volume

```
part pv.01 --size=8192
volgroup myvg pv.01
logvol / --vgname=myvg --fstype=xfs --size=2048 --name=rootvol --grow
logvol /var --vgname=myvg --fstype=xfs --size=4096 --name=varvol
```

Kickstart File Commands

Network Commands

-Define the network features used by the host.

- **network:** Configures network information for target system. Activates network devices in installer environment.

```
network --device=eth0 --bootproto=dhcp
```

- **firewall:** Defines the firewall configuration for the target system.

```
firewall --enabled --service=ssh,http
```

- فيه عندي section تاني اسمه Network Commands بحددله فيها ال network features او ال configuration بتاعت ال Network ان لو عندي interface معين وعايز ال interface ده أ configure ليه static IP او انا اقوله ال bootproto هو ال dhcp ان يسحب IP automatic ف بعملها عن طريق command اسمه network

```
network --device=eth0 --bootproto=dhcp
```

- عندي command تاني لل firewall ان انا ممكن اعمل enable او disable ل service معينه او port معين

```
firewall --enabled --service=ssh,http
```

Kickstart File Commands

Location and Security Commands

-Configure settings related to security, language, and regions.

- **lang:** Sets the language to use during installation and the default language of the installed system. Required.

```
lang en_US.UTF-8
```

- **firewall:** Defines the firewall configuration for the target system.

```
firewall --enabled --service=ssh,http
```

- **keyboard:** Sets the system keyboard type. Required.

```
keyboard --vckeymap=us --xlayouts=''
```

- فيه عندي section تاني لل Location and Security Commands ان انت من خلاله تقدر ت configure ال settings ال related لل security وال language وال regions وهكذا

- زي مثلا لو انت عايز تحددله ال installation language بتاعتك تخليها مثلا English ف جوه ال kickstart بحطله command اسمه lang وبعدين ال language بتاعتك

```
lang en_US.UTF-8
```

- وعندي command اسمه keyboard بستخدمه لو انا عايز احدد ال layout او ال type بتاع ال keyboard

```
keyboard --vckeymap=us --xlayouts=''
```

- عندنا command تاني اسمه timezone بنحدد فيه ال time zone

- **timezone:** Defines the timezone, NTP servers, and whether the hardware clock uses UTC.

```
timezone --utc --ntpservers=time.example.com Africa/Cairo
```

- ال root password من الحاجات الالزاميه عند ال anaconda مش هينفع يبدأ ال installation الا لما تحددله ال root password عن طريق command اسمه rootpw

- **rootpw:** Defines the initial root password.

```
rootpw --plaintext redhat
```

- فيه عندي command تاني اسمه selinux لو انا عايز احدد ال mode بتاع ال selinux عايزه enforcing ولا permissive ولا disable

- **selinux:** Sets the SELinux mode for the installed system.

```
selinux –enforcing
```

- فيه عندي command تاني اسمه services بستخدمه لو انا عايز اعمل enable او disable ل service معينه

- **services:** Modifies the default set of services to run under the default systemd target.

```
services --disabled=network,iptables,ip6tables --enabled=NetworkManager,firewalld
```

- لو عايز اعمل create ل new user او group

- **group, user:** Create a local group or user on the system.

```
rgroup --name=admins --gid=10001
user --name=jdoe --gecos="John Doe" --groups=admins --password=changeme –plaintext
```

➢ Example Kickstart File

- ده كده مثال علي ال kickstart file شكله بالمنظر ده
- هنلاقي مجموعه من ال comment بتبدء ب # ده كده بيكون عباره عن وصف عن كل command بيعمل ايه وال file بيكون مقسوم ل مجموعه من ال sections

1- اول section فيه بيكون فيه ال installation commands زي ال disk partitioning وال installation source

```
#version=RHEL9
ignoredisk --only-use=vda
# System bootloader configuration
bootloader --append="console=ttyS0 console=ttyS0,115200n8 no_timer_check net.ifnames=0
crashkernel=auto" --location=mbr --timeout=1 --boot-drive=vda
# Clear the Master Boot Record
zerombr
# Partition clearing information
clearpart --all --initlabel
# Use text mode install
text
repo --name="Appstream" --baseurl=http://classroom.example.com/content/rhel8.0/x86_64/dvd/AppStream/
# Use network installation
url --url="http://classroom.example.com/content/rhel8.0/x86_64/dvd/"
# Keyboard layouts
# old format: keyboard us
# new format:
keyboard --vckeymap=us --xlayouts="
# System language
lang en_US.UTF-8
# Root password
rootpw --plaintext redhat
# System authorization information
auth --enableshadow --passalgo=sha512
# SELinux configuration
selinux --enforcing
firstboot --disable
# Do not configure the X Window System
skipx
# System services
services --disabled="kdump,rhsmcertd" --enabled="sshd,rngd,chronyd"
# System timezone
timezone America/New_York --isUtc
# Disk partitioning information
part / --fstype="xfs" --ondisk=vda --size=10000
```

ال ignoredisk ده لو انا عايز ال anaconda ت ignore disk معين متجيش جنبه

عندنا command تاني اسمه boot loader لو انا عايز اعمل install لل MBR علي هارد درايف معين

لو انا عايز اعمل clear لل master boot record هستخدم zerombr

لو انا عايز اعمل clear لكل ال patitions اللي عندي هستخدم clearpart

لو انا عايز اعمل install لباكج معينه عن طريق ال repo

لو عايز احددله ال installation media

لو انا عايز احدد ال keyboard

لو عايز اخدد ال root password

1- تاني section وال section ده بيبدء ب %packages وبينتهي ب %end وده بتحددله جواه كل اسامي ال packages اللي انت عايز تعملها Install

- وكمان لو انت مش عايز تعمل install ل package معينه هتحط – قبل ال package زي مثلا -plymouth
- خلي بالك من حاجه لو انت ال package اللي انت مش عايز تعملها Install فيه package تانيه بت depend عليها ال anaconda هتعملها Install عادي جدا

```
%packages
@core
chrony
cloud-init
dracut-config-generic
dracut-norescue
firewalld
grub2
kernel
rsync
tar
-plymouth

%end
```

2- اخر section معانا اسمه pre and post installation scripts وبيبدء ال section ده ب %post وبينتهي ب %end وجواه بحط اي script انا عايز اعمله execute وال script ده باي لغه برجمه زي مثلا ال python

```
%post --erroronfail

# For cloud images, 'eth0' _is_ the predictable device name, since
# we don't want to be tied to specific virtual (!) hardware
rm -f /etc/udev/rules.d/70*
ln -s /dev/null /etc/udev/rules.d/80-net-name-slot.rules

# simple eth0 config, again not hard-coded to the build hardware
cat > /etc/sysconfig/network-scripts/ifcfg-eth0 << EOF
DEVICE="eth0"
BOOTPROTO="dhcp"
ONBOOT="yes"
TYPE="Ethernet"
USERCTL="yes"
PEERDNS="yes"
IPV6INIT="no"
EOF

%end
```

Kickstart Installation Steps

- To successfully automate installation of Red Hat Enterprise Linux, follow these steps:
  1. Create a Kickstart file.
  2. Publish the Kickstart file to the installer.
  3. Boot Anaconda and point it to the Kickstart file.

Creating a Kickstart File

- TUse either of these methods to create a Kickstart file:
  - Use the Kickstart Generator website.
  - Use a text editor.

- علشان نبدء نعمل automate لل installation باستخدام ال kickstart فيه عندنا 3 steps
  1- اول step ان احنا نعمل create لل kickstart file وقولنا ال kickstart file بيبقي عباره عن pure text file مكتوب ب syntax معين بحط جواه كل ال configuration وكل ال answer اللي ال anaconda محتاجاها علشان تعمل automate لل installation بتاع ال OS بتاعك
  2- تاني step انك تعمل publish للkickstart file
  3- تالت step انك تبدء ال installation process وتخلي ال anaconda تروح تقرا ال configuration بتاعتها من ال kickstart file
- علشان تبدء تعمل create لل kickstart file عندنا كذا طريقه
  1- اول طريقه علشان ال syntax بتاع ال kickstart file بيبقي more complex ف صعب ان انت تكتبه from scratch بأيدك ف red hat بتوفلك website tool تقدر من خلالها انك ت generate ال kickstart file عن طريق ان انا هدخل علي ال url ده
  https://access.redhat.com/labs/kickstart.config/
  2- تاني طريقه عن طريق ال cli انك ت create text file وعن طريق ال VI editor تفتح ال file ده وتبدء انك ت edit فيه و by default لما تيجي تعمل install لOS هتلاقي تحت ال /root عاملك create ل file اسمه anaconda-ks.cfg وحاططلك جواه كل ال kickstart configuration اللي انت احتجتها علشان تعمل install لل OS ف ال file ده انت ممكن تستخدمه انك تاخد نسخه منه وتعدل فيه وتستخدمه علشان تعمل Install من خلاله

Creating a Kickstart File

- **ksvalidator** is a utility that checks for syntax errors in a Kickstart file. It ensures that keywords and options are properly used, but it does not validate that URL paths, individual packages,or groups, nor any part of %**post** or %**pre** scripts will succeed. For instance, if the **firewall -- disabled** directive is misspelled, **ksvalidator** could produce one of the following errors: **yum install pykickstart**.

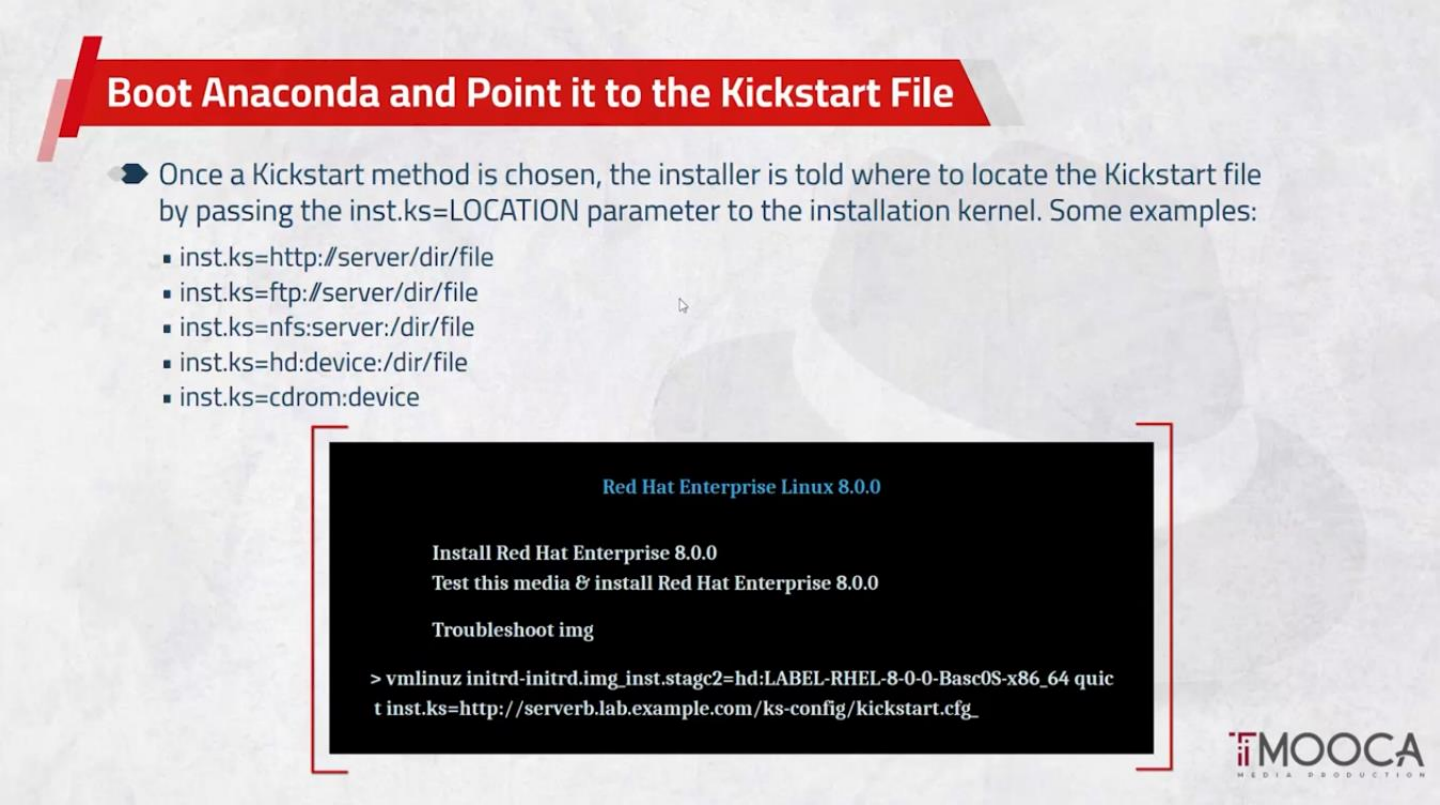
```
[user@host ~]$ ksvalidator /tmp/anaconda-ks.cfg
The following problem occurred on line 10 of the kickstart file:

Unknown command: frewall

[user@host ~]$ ksvalidator /tmp/anaconda-ks.cfg
The following problem occurred on line 10 of the kickstart file:

no such option: --dsabled
```

- بمجرد انك عملت create لل kickstart file عندنا tool اسمها ksvalodator بنستخدمها علشان نت check ال syntax بتاع ال kickstart file علشان لو فيه اي errors او فيه اي commands او option انت كاتبه مش مظبوط ف ساعتها هو هيقولك ان فيه في ال Line كذا error
- ال command مبيكونش install by default علشان تعمله Install هتقوله yum install pykickstart بعد اما عملنا Install وبعد اما عملنا edit و create لل kickstart file بقوله ksvalodator واديله اسم ال file ف هو هيعمل check لل syntax اللي انا كاتبه ف لو مثلا كاتب ال firewall غلط ف هو هيقولي مثلا ان في ال line رقم 10 عندك unknow command او لو انت كاتب اوبشن disabled غلط ف هيطلعلك error ويقولك ان المشكله في ال line كذا

Publish the Kickstsart File to Anaconda

- Make the Kickstart file available to the installer by placing it in one of these locations:
  - A network server available at install time using FTP, HTTP, or NFS.
  - An available USB disk or CD-ROM.
  - A local hard disk on the system to be installed.
- The installer must access the Kickstart file to begin an automated installation. The most common automation method uses a network server such as an FTP, web, or NFS server. Network servers facilitate Kickstart file maintenance because changes can be made once, and then immediately used for multiple future installations.
- Providing Kickstart files on USB or CD-ROM is also convenient. The Kickstart file can be embedded on the boot media used to start the installation. However, when the Kickstart file is changed, you must generate new installation media.
- Providing the Kickstart file on a local disk allows you to quickly rebuild a system.

- تاني step ان انا اعمل publish لل kickstart file سواء كان هن create مثلا HTTP Server او FTP او NFS او عن طريق ال CD-ROM او ال USB



- اخر step ان انا اعمل boot لل anaconda وتديها ال location بتاع ال kickstart file
- علشان ادي ال anaconda ال location بتاع ال kickstart file انت بتبدء ال installation بتاعك عادي جدا واول اما يجيلك ال iso image بت load ال menu بتروح دايس في الكيبورد علي tab وبتزود Line من ال lines دي علي حسب ال protocol اللي انا مستخدمه يعني لو انت من الاخر لو عامل publish لل kickstart file علي http ف بتقوله ال command ده inst.ks=http://server/dir/file ولو علي FTP ف هيكون ال line بالشكل ده inst.ks=://server/dir/file وهكذا

- **هنطبق اللي احنا شرحناه**

Create a Kickstart file using text editor

- اول اما تعمل Install لل operating system بيبقي فيه file زي ماقولنا اسمه anaconda-ks.cfg بيبقي موجود تحت /root/
- لو جينا فتحنا ال file ده بال vim editor هنلاقيه بيحتوي علي كل ال kickstart configuration اللي انت احتجتها علشان تعمل install لل OS زي ماحنا شايفين

```
[root@MohamedAtef ~]# vim anaconda-ks.cfg
# Generated by Anaconda 34.25.2.10
# Generated by pykickstart v3.32
#version=RHEL9
# Use graphical install
graphical
repo --name="AppStream" --baseurl=file:///run/install/sources/mount-0000-cdrom/AppStream
%addon com_redhat_kdump --disable
%end
# Keyboard layouts
keyboard --xlayouts='us','ara'
# System language
lang en_US.UTF-8
# Network information
network  --bootproto=dhcp --device=ens160 --ipv6=auto --no-activate
network  --hostname=server.iti.com
# Use CDROM installation media
cdrom
%packages
@^graphical-server-environment
%end
# Run the Setup Agent on first boot
firstboot --enable
# Generated using Blivet version 3.6.0
ignoredisk --only-use=nvme0n1
# Partition clearing information
clearpart --none --initlabel
# Disk partitioning information
part / --fstype="xfs" --ondisk=nvme0n1 --size=20480
part /home --fstype="xfs" --ondisk=nvme0n1 --size=20480
part swap --fstype="swap" --ondisk=nvme0n1 --size=2048
# System timezone
timezone Africa/Cairo --utc
# Root password
rootpw --iscrypted --allow-ssh
$6$MQWzokEPeyZKD7m0$MEHEnFEqTj0MR5nXV6lYoYEv2CCOnExkrM0oJqiaXepNfmtFGWIpqI.QSebCew9ZFJk9DPijvXKljMgMT
gTWn1
user --name=Elbitawy --
password=$6$3D8debSVPevkSD6v$bql2Hxqk7AqLRbEjnyQkVFHOkqq2QY0TcrXJn86KGWBr3fjE/nEPetFxktX/hwfm56Tt4Xe6O8a
E9KFmhlMsq0 --iscrypted --gecos="Elbitawy"
```

- ممكن اخد copy من ال file ده وابدء اعمل edit فيه وليكن هاخد copy واسمي ال file اللي هعمل عليه edit علشان اعمل install من خلاله اسمه ks.cfg

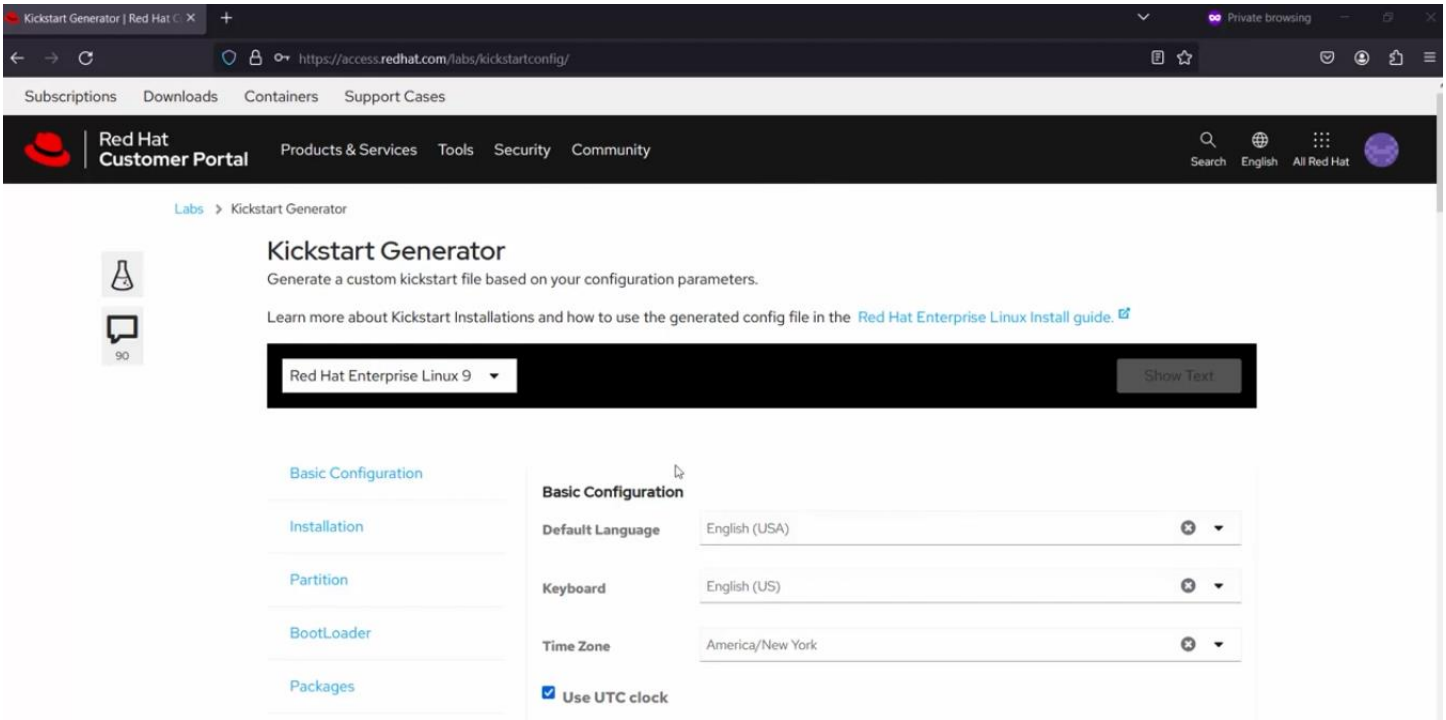
```
[root@MohamedAtef ~]# cp anaconda-ks.cfg  ks.cfg
```

- بعد كده افتح ال file ده ks.cfg بال vi editor وبعدين اعمل edit جواه

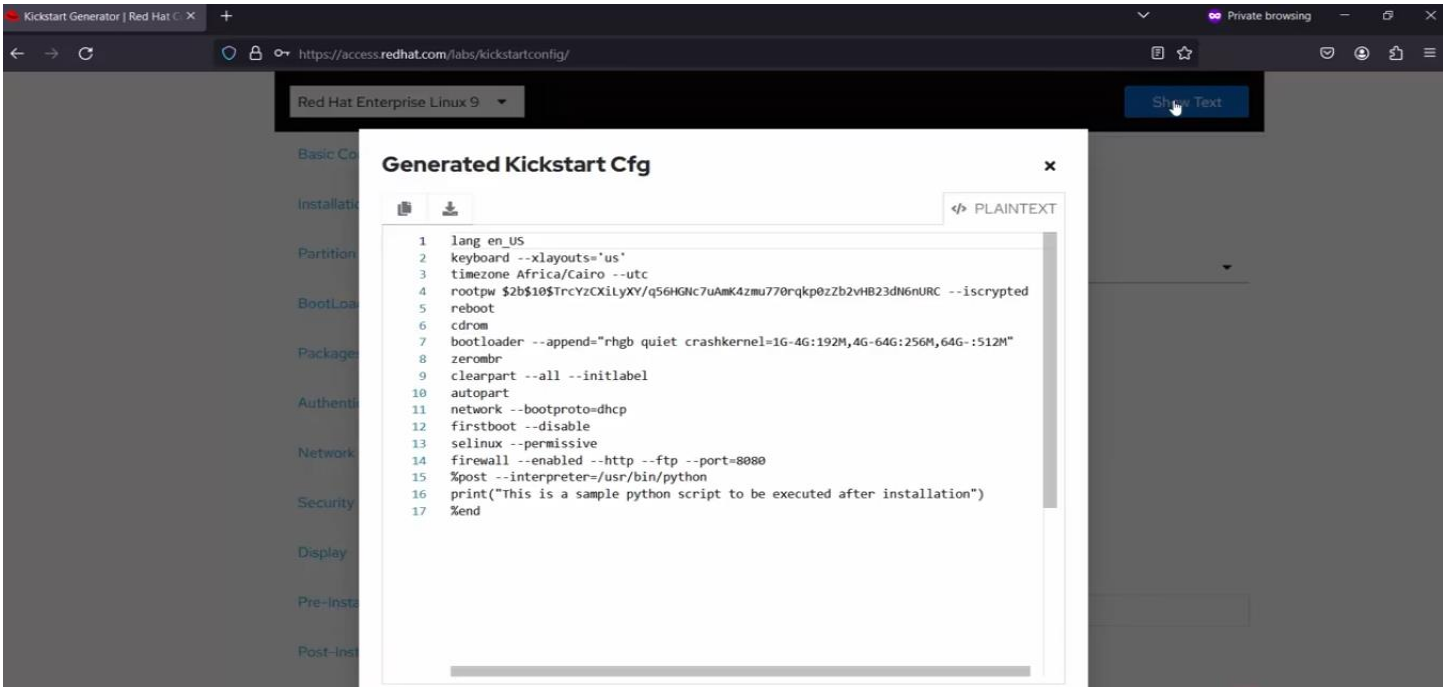
```
[root@MohamedAtef ~]# vi   ks.cfg
```

Create a Kickstart file using Kickstart Generator

- الطريقه التانيه زي ماقولنا عن طريق ال Kickstart Generator اللي هو ب provided by red hat ان احنا ندخل علي ال url ده https://access.redhat.com/labs/kickstart.config/ ون login هيطلعلنا tool بالمنظر دا كده نقدر اننا ن select كل ال options اللي احنا محتاجينها



- بعد اما نختار كل ال options اللي احنا محتاجينهاا علشان نعمل Install هنضغط علي show text وبعدين هيظهرلي ال kickstart file بتاعي بالشكل ده وبعدين اعمل download لل file ده



Verify Kickstart file is valid using ksvalidator

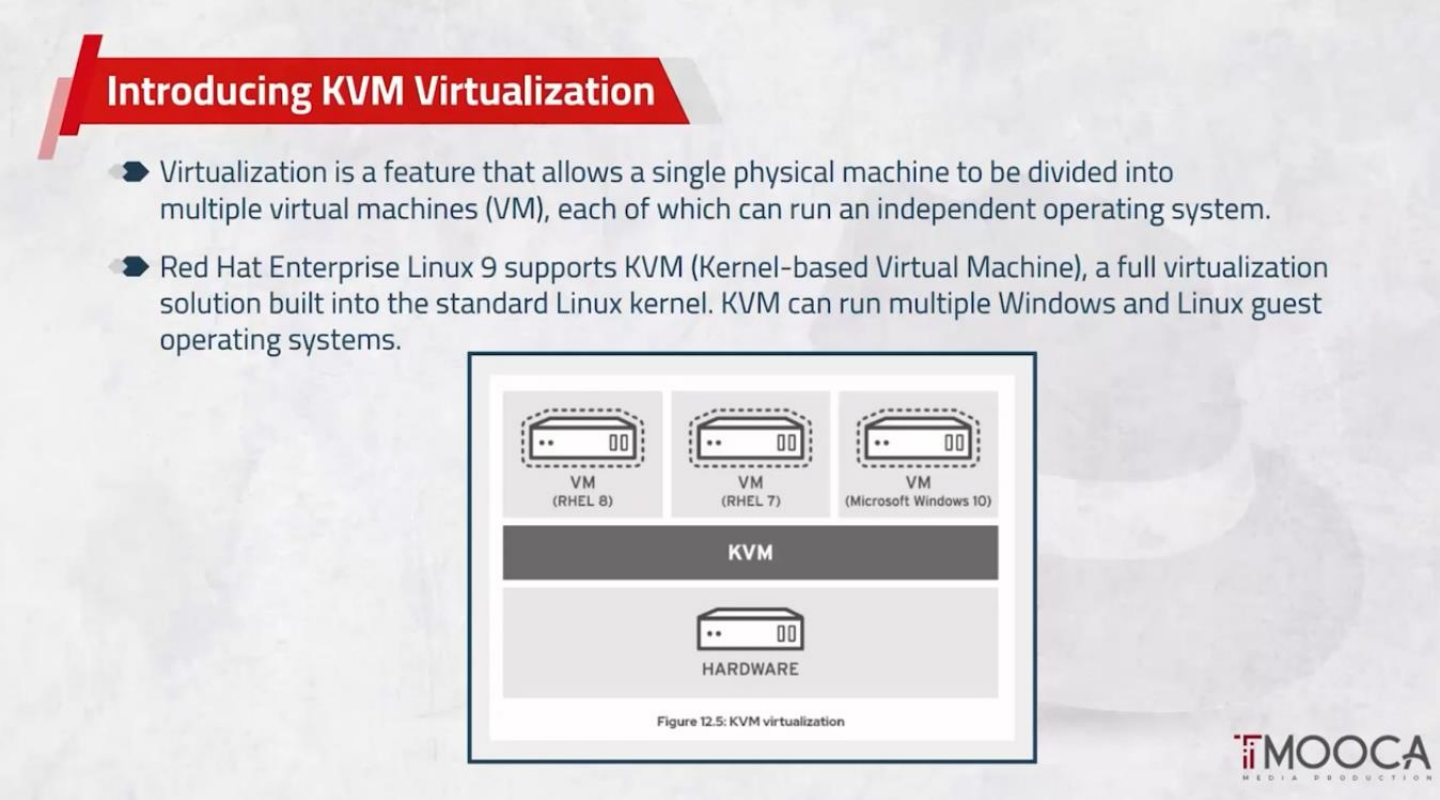
- بعد اما عملنا create لل kickstart file الا step اللي بعد كده ان انت تبدأ ت verify ان انت عامل ال syntax بتاع ال kickstart file بتاعك مظبوط ومفيش اي errors فيه علشان نعمل كده فيه command اسمه ksvalodator ودي مبتكونش install عندي
- علشان اعمل Install هقوله

```
[root@MohamedAtef ~]# dnf install pykickstart
```

- بعد كده علشان أ verify ال kickstart file هقوله ksvalodator وبعدين اسم ال file ساعتها هو لو فيه اي مشكله في ال syntax هيطلعلك error ويحددلك ال error ده فين

```
[root@MohamedAtef ~]# ksvalodator ks.cfg
```

- الافضل ان انت تشوف الفيديوهات الخاصه بالجزئيه دي علشان فيه تطبيق عملي لل install
- **Publish the Kickstart File to Anaconda**
- **Boot Anaconda and point it to the Kickstart file (HTTP)**
- **Boot Anaconda and point it to the Kickstart file (FTP)**
- الفيديوهات موجوده في شابتر 12 الفيديو رقم 7 و 8 و 9 في كورس مهاره تك



- مبدئيا كده ال virtualization عباره عن features بتسمحلك ان لو عندك single physical machine تقدر ت create مجموعه من ال virtual machines علي ال physical machine بتاعتك وكل virtual machines منهم بتبقي ليها ال resources بتاعتها زي ال CPU وال RAM وال Storage وبيكونو منفصلين عن بعضهم
- ريدهات عندها ال virtualization solutions بتاعها اللي اسمه KVM(Kernel-based Virtual Machine) وده كده ال hyper visor اللي من خلاله تقدر ان انت ت virtualize ال Linux OS يعني لو انت عندك server running عليه red hat OS تقدر بمنتهي السهوله انك تعمل install لل KVM علي السيرفر ده ومن خلال ال KVM تقدر انك ت virtualize ال HARDWARE بتاعك وت create مجموعه من VM وكل VM ليها ال OS version بتاعتها سواء كان red hat 7 او red hat 8 او windows 10
- علشان تعمل create ل مجموعه من ال VM علي ال KVM لازم ال KVM يكون فيه resources كافيه

- علشان نتاكد هل ال CPU بي support ال VTX او ال Virtualization عندي كذا command ممكن استخدمهم
- اول command عن طريق ان انا اعمل grep لل vmx تحت /proc/cpuinfo

```
[root@MohamedAtef ~]# grep vmx /proc/cpuinfo
flags                    : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca cmov pat pse36 clflush mmx fxsr sse sse2 syscall nx rdtscp lm constant_tsc arch_perfmon nopl xtopology tsc_reliable nonstop_tsc cpuid tsc_known_freq pni pclmulqdq vmx ssse3 cx16 pcid sse4_1 sse4_2 x2apic popcnt tsc_deadline_timer aes xsave avx hypervisor lahf_lm pti ssbd ibrs ibpb stibp tpr_shadow vnmi ept vpid tsc_adjust arat md_clear flush_l1d arch_capabilities
vmx flags     : vnmi invvpid ept_x_only tsc_offset vtpr mtf ept vpid unrestricted_guest
```

لو ظهر معانا vmx بالشكل ده يبقي ال cpu بي support ال Virtualization

- عندي command تاني اسمه lscpu ده بيجبلي more details عن ال CPU بتاعي وهنلاقي من ضمن ال features بتاعت ال CPU بيقولك ان الfeatures Virtualization معمول ليها enable

```
[root@MohamedAtef ~]# lscpu
Virtualization features:
Virtualization:          VT-x
Hypervisor vendor:       VMware
Virtualization type:     full
```

- علشان نتاكد ان ال KVM modules معمول ليها loaded عندي في ال kernel هستخدم command اسمه lsmod وبعدين اعمل grep لل KVM

```
[root@MohamedAtef ~]# lsmod | grep kvm
kvm_intel          409600  0
kvm               1134592  1 kvm_intel
irqbypass           16384  1 kvm
```

هنلاقيه ظاهر معانا KVM ده كده اشاره ان ال KVM modules loaded عندي

- كده انا جاهز اني اعمل installation لل KVM Packages
- لو انا عملت dnf group list هنلاقيه جايبلي مجموعه من ال Available Environment Groups وال group ده بيبقي عباره عن مجموعه من ال Packages بتبقي موجوده تحت group معين وهنلاقي من ضمن ال groups جروب اسمه Virtualization Host وده اللي احنا بنستخدمه لو انت عايز تعمل install علي طول لكل ال KVM Tools بتاعتي

```
[root@MohamedAtef ~]# dnf group list
Available Environment Groups:
  Server
  Minimal Install
  Workstation
  Custom Operating System
Installed Environment Groups:
  Server with GUI
  Virtualization Host
```

- لو عايز اعرف معلومات عن الجروب اللي اسمه Virtualization Host هقوله

```
[root@MohamedAtef ~]# dnf group info "Virtualization Host"
```

- لو انا عايز اعمل install لل KVM هقوله

```
[root@MohamedAtef ~]# dnf group install "Virtualization Host"
```

- بعد اما عملنا install لل KVM لازم نعمل enable ل service اسمها libvirtd

```
[root@MohamedAtef ~]# systemctl enable --now libvirtd
```

- علشان نبدء نعمل create لمجموعه من ال VM علي ال KVM عندي كذا طريقه
  - اول طريقه عن طريقه ال web عن طريق ال service اللي اسمها cockpit
  - تاني طريقه عن طريق ال CLI
  - تالت طريقه عن طريق GUI

1- Create virtual machine through cockpit

- علشان نبدأ ان احنا نعمل create لمجموعه من ال VM سواء كان بال web او بال CLI او بال GUI عندنا مجموعه من ال packages الاضافيه اللي احنا محتاجين نعملهم install

```
[root@MohamedAtef ~]# dnf install cockpit-machines virt-install virt-manager virt-viewer
```

ال package دي هتنزلك module او menu في ال cockpit web console بتعاك تسمحلك انك ت create مجموعه من ال VM عن طريق ال web browser بتاعت ال cockpit

ال package دي مسئوله ان هي تنزلي ال command اللي هستخدمه علشان اعمل create لل kvm vm عن طريق ال CLI

ال package دي بتنزلي GUI تقدر من خلال ال Desktop بتاع ال OS بتاعك تعمل create ل VM

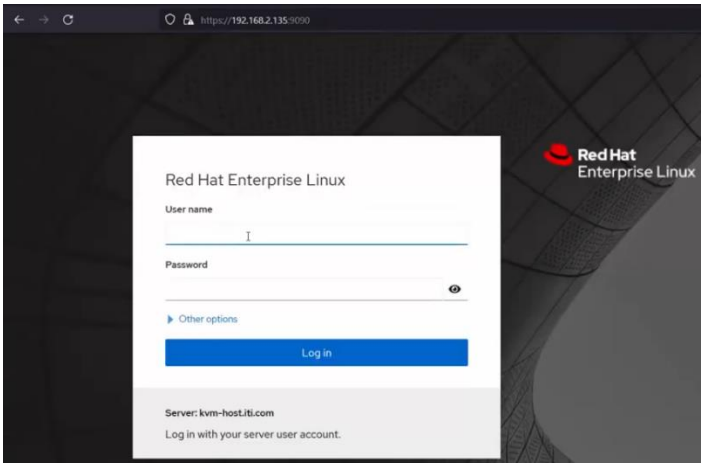
ال package دي عباره عن command او application بنقدر من خلاله نفتح ال VM ونقدر نستخدمها

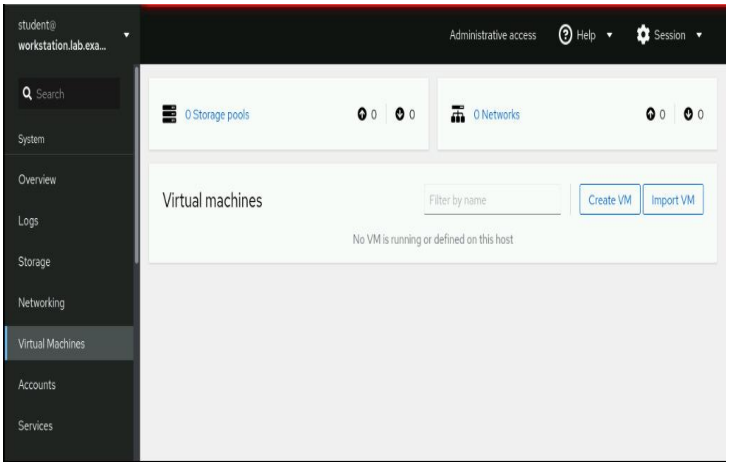
- هنشوف ازاي نعمل create عن طريق ال cockpit

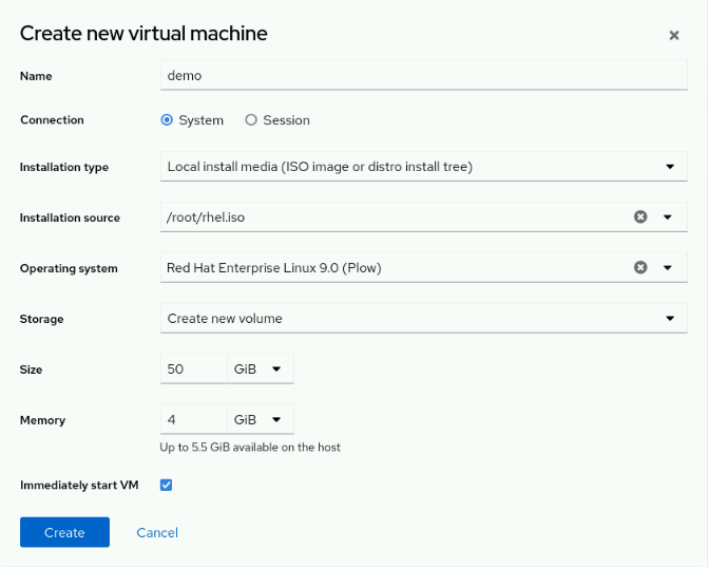
- اول حاجه بعد اما عملنا Install لل package الخاصه بال cockpit وهي cockpit-machines هنعمل enable و start لل cockpit

```
[root@MohamedAtef ~]# systemctl enable --now cockpit.socket
```

- بعد كده هنفتح ال Browser ونكتب في ال url ال IP الخاص بال server وبعدين نكتب الport الخاص بال cockpit وهو 9090 وبعدين هنكتب ال username وال password وبعدين هيفتحلنا ال cockpit اقدر من خلاله ان اعمل create ل VM وسهل جدا في التعامل زي ال vmware workstation الخاص بال windows







2- Create virtual machine through CLI

- علشان نبدأ ان احنا نعمل create لل VM عن طريق ال CLI في command بنستخدمه اسمه virt-install هو command طويل شويه بس سهل هقسم ال command ده في الشرح للتبسيط

1- اول حاجه بستخدم command اسمه virt-install وبعدين اديله كل الاوبشن بتاعتي
2- بعد كده بحددله اسم ال VM ف هستخدم --name= وبعدين احددله الاسم
3- بعد كده بحدد cpu ال VM اللي هعملها create عن طريق اني هستخدم --vcpus=
4- بعد كده بحددله ال memory اللي هستخدمها عن طريق اني هستخدم --memory
5- بعد كده بحددله ال location الموجود فيه ال ISO بتاعتي اللي هعمل Install من خلالها عن طريق --location=
6- بعد كده بحددله ال disk بتاعي اللي هعمل install عليه عن طريق --disk path= وبعد كده بحددله اسم ال virtual disk اللي هيعمله create يكون زي RHEL9_CLI.qcow2 وبعدين بحدد ال size بتاعي
7- بعد كده بضغط enter واعمل install عن طريق ان انا هعمل ال steps اللي هتتطلب مني في ال install

```
[root@MohamedAtef ~]# virt-install --name=RHEL9_CLI --vcpus=2 --memory=2048 --
location=/var/lib/libvirt/images/RHEL9.3.iso --disk path=/var/lib/libvirt/images/RHEL9_CLI.qcow2,size=10 --
nograpgics --os-variant=rhel9.9
```

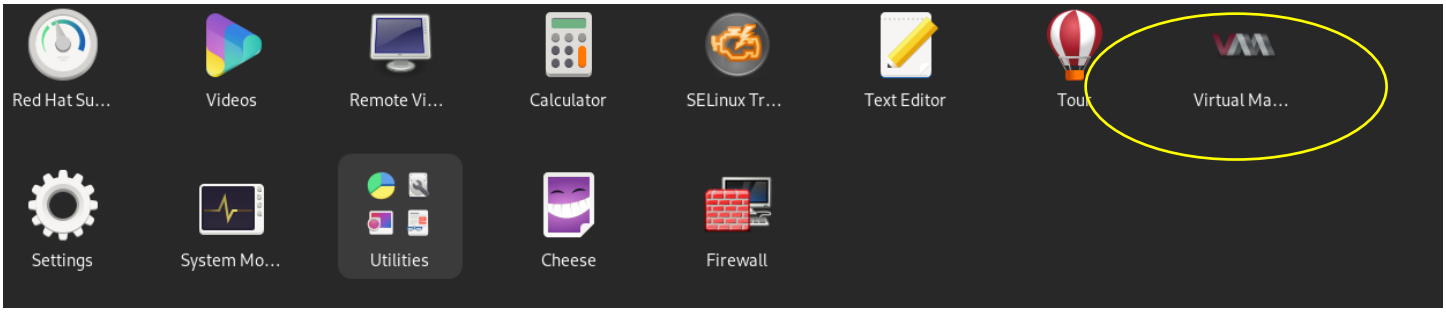
- في عندي طريقه تانيه عن طريق ال virt-install تخليه يروح يقرا عن طريق ال kickstart file ان انت ت automate ال installations process بتاعت ال KVM Virtual Machine عن طريق ان انا ممكن اعمل create ل kickstart file عن طريق ان انا اخد copy من ال anaconda-ks.cfg ل file جديد اسمه مثلا ks.cfg وافتح ال file ده واعمل edit فيه وبعد اما تعمل edit وتحفظ .الخطوه اللي بعد كده انك هتستخدم نفس ال command الخاص بال virt-install ونفس ال options بس هزود في نهايه ال commandالاوبشن ده

```
[root@MohamedAtef ~]# virt-install --name=RHEL9_CLI --vcpus=2 --memory=2048 --
location=/var/lib/libvirt/images/RHEL9.3.iso --disk path=/var/lib/libvirt/images/RHEL9_CLI.qcow2,size=10 --
nograpgics --os-variant=rhel9.9 --initrd-inject ks.cfg --extra-args "inst,ks=file:/ks.cfg console=tty0
console=ttyS0,115200n8"
```

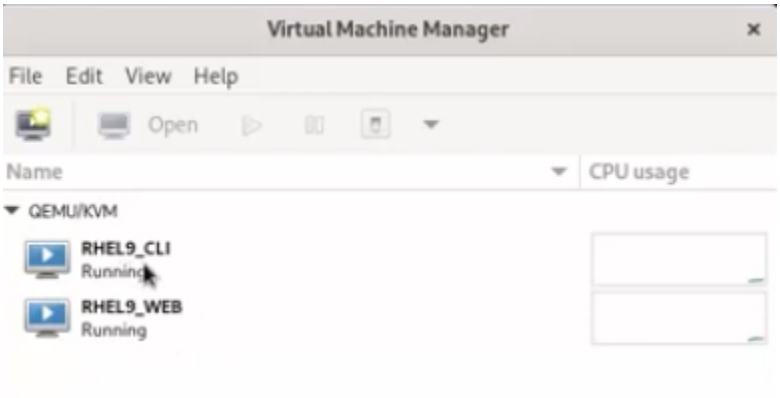
- وبعد كده اضغط Enter وهيعمل installation

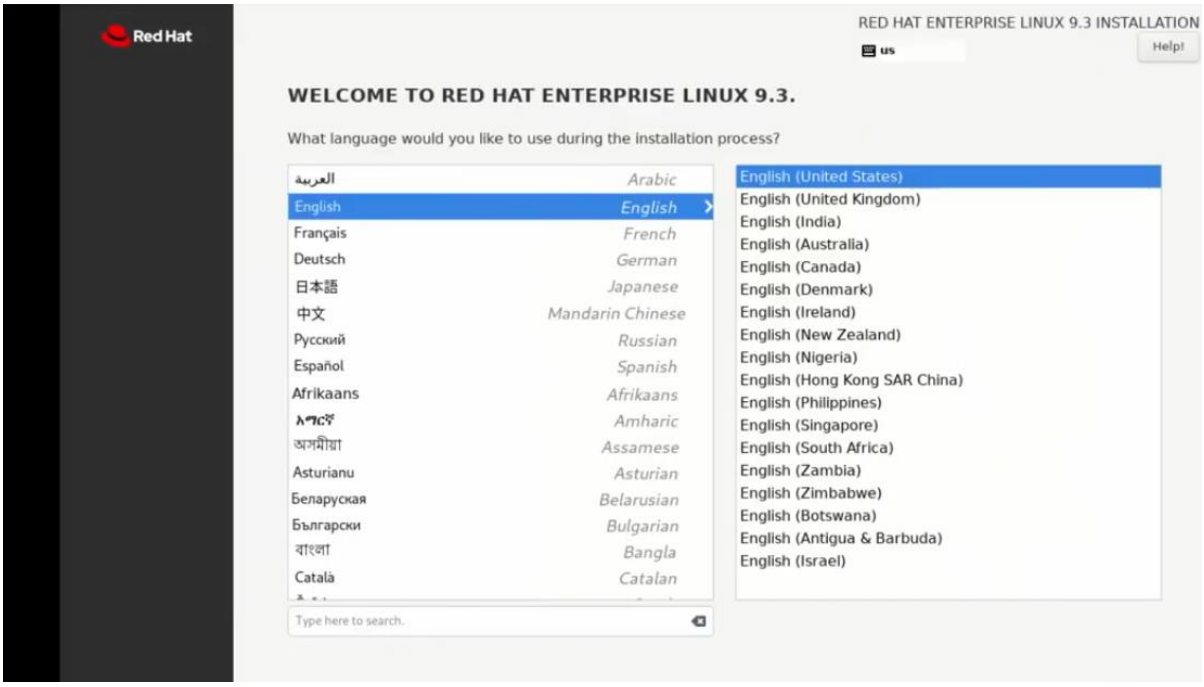
3- Create virtual machine through GUI

- الطريقه الاخيره وهي ال GUI ان انا عملت Install ل package اسمها virt-manager هنلاقيها منزله application علي ال OS بتاعي هنلاقي application اسمه Virtual Machine Manager لما نفتح ال application ده كاننا بالظبط فاتحين VMware workstation



- هنفح ال application ده هنلاقي موجود فيه ال VM اللي احنا كنا عاملين ليهم create عن طريق ال CLI وال WEB ف انا هستخدم الابلكيشن ده وابدء اعمل install





Manage virtual machine using virsh command

- اخر حاجه هنتكلم عنها في ال KVM علشان خاطر اني أ manage ال VM اللي انا عملتها create عندي عن طريق ال CLI بنستخدم command اسمه virsh
- لو انا عايز أ list كل ال VM ال running عندي بستخدم virsh list

```
[root@MohamedAtef ~]# virsh list
 Id    Name          State
----------------------------
 4     RHEL9_CLI     running
 5     RHEL9_WEB     running
 6     RHEL9_GUI     running
```

- لو انا عايز أ list كل ال VM ال running وال not running بستخدم virsh list –all

```
[root@MohamedAtef ~]# virsh list --all
 Id    Name          State
----------------------------
 4     RHEL9_CLI     running
 5     RHEL9_WEB     running
 6     RHEL9_GUI     running
```

- لو انت عايز ت access عن طريق ال CLI ال console بتاع اي VM منهم ف بستخدم virsh console وبعدين اسم ال VM

```
[root@MohamedAtef ~]# virsh console RHEL9_CLI
Connect to domain 'RHEL9_CLI'
Escape character is ^] (Ctrl + ])
[root@RHEL9_CLI ~]#
```

علشان ت Escape لل server قالك اضغط علي [+ Ctrl

كده انا دخلت جوه ال VM

- لو انا عايز اعمل reboot ل اي VM هستخدم virsh reboot وبعدين اسم ال VM

```
[root@MohamedAtef ~]# virsh reboot RHEL9_CLI
```

- لو انا عايز اعدل في ال settings الخاصه بال VM عندي command اسمه virsh edit وبعدين اسم ال VM

```
[root@MohamedAtef ~]# virsh edit RHEL9_CLI
```

- ولو انا عايز اعرف كل options المستخدمه مع ال virsh هستخدم help–

```
[root@MohamedAtef ~]# virsh --help
```

- لو انت عايز ت destroy وت remove ال VM اللي احنا عملنالها create هستخدم virsh destroy واديله اسم ال VM ال command ده لما بستخدمه ال VM بيتعملها shut off بس مبتتعملهاش remove

```
[root@MohamedAtef ~]# virsh destroy RHEL9_CLI
```

- علشان اعمل remove خالص لل VM هستخدم virsh undefine وبعدين اسم ال VM

```
[root@MohamedAtef ~]# virsh undefine RHEL9_CLI
```

- ف زي ماقولنا علشان تعمل remove لل VM لازم تعمل destroy الاول وبعدين تعمل remove

Red Hat Enterprise Linux 9

Mohamed Atef

BY: Mohamed Atef Elbitawy

https://www.linkedin.com/in/mohamedelbitawy/