Red Hat Enterprise Linux 9

شرح **Linux Admin 1** بالكامل لكورس

Red Hat System Administration I

الموجود علي منصه **Mahara Tech** للباشمهندس

Karim Abd Elhamid

BY: Mohamed Atef Elbitawy

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

- **رابط الكورس**

https://maharatech.gov.eg/course/view.php?id=2115&lang=ar

- **ال Slides المستخدمه في شرح الكورس**

https://drive.google.com/drive/folders/17MONm_cEdA95x2Oni9AkTn2gn-Mjoqly?usp=sharing

- **كتاب Red Hat Enterprise Linux 9_RH124**

https://drive.google.com/drive/folders/1H3Ke2iQuhlVP1Y8MWuDzsZKJY4jiom32?usp=sharing

- **دامب امتحان RHCSA**

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

- **أسئلة الانترفيو**

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

Content

CH01_Install RHEL 9 Step by Step

CH02_Accessing the Command Line

CH03_Managing Files From the Command Line

CH04_Getting Help in Red Hat Enterprise Linux

CH05_Creating, Viewing, and Editing Text Files

CH06_Managing Local Users and Groups

CH07_ Controlling Access to Files

CH08_Monitoring and Managing Linux Processes

CH09_Controlling Services and Daemons

CH10_Configuring and Securing SSH

CH11_Analyzing and Storing Logs

CH11_Analyzing and Storing Logs

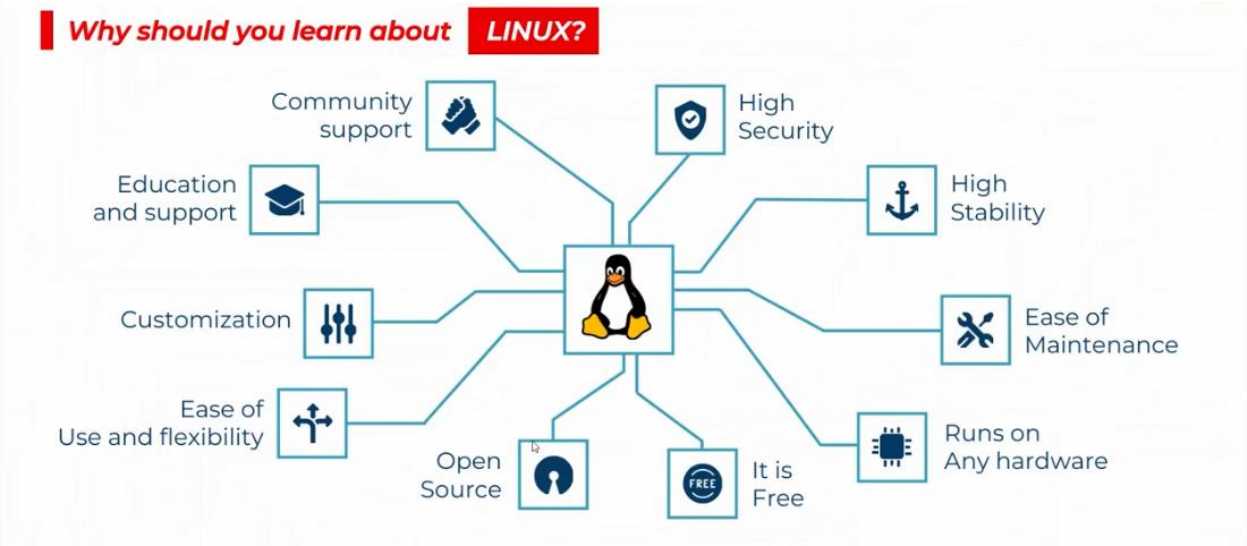
CH12_Managing Networking

CH13_Archiving and Transferring Files

CH14_Installing and Updating Software Packages

Chapter 1

Install RHEL 9 Step by Step

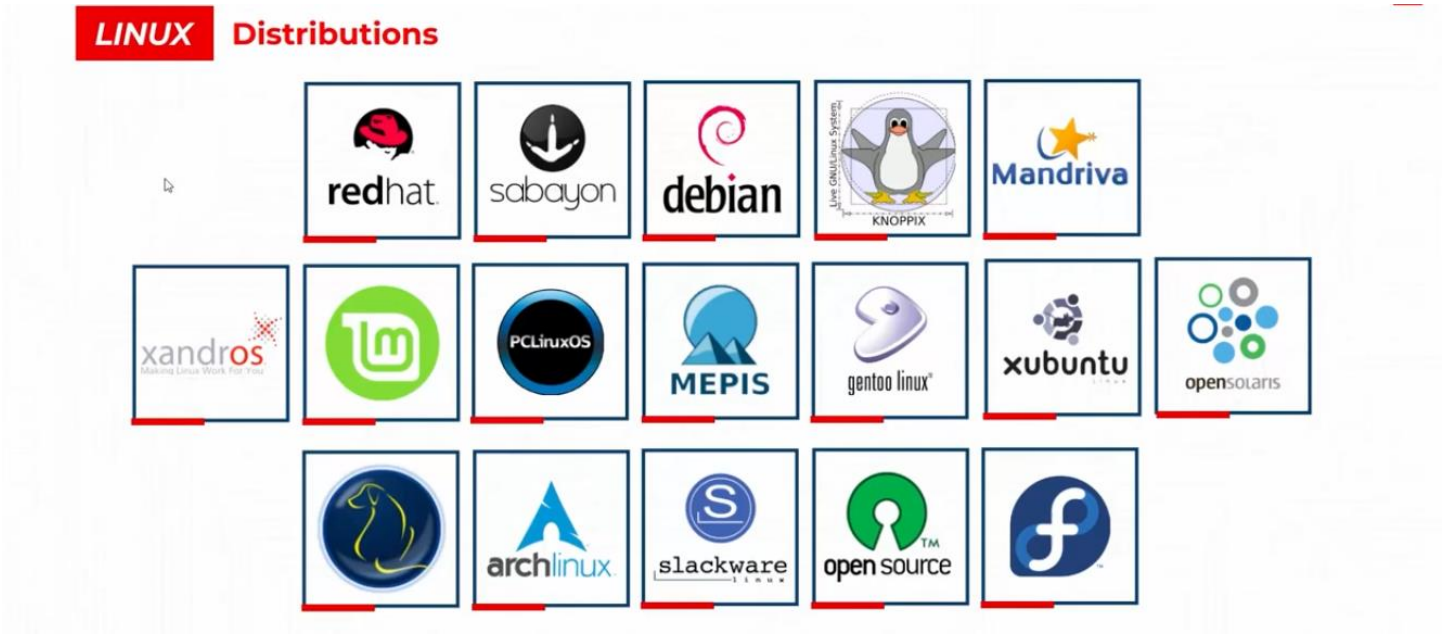


- مبدئيا اللينكس عباره عن Operating System بمعني if you are familiar with other operating systems like Microsoft windows, apple Mac, google android. Linux is also an operating system
- طبعا كلنا اول سؤال بيجي في بالنا ليه نتعلم لينكس وليه العالم كله دلوقتي بقي مهتم بيه ومش بس كده انت كمان ك IT Engineer محتاج تقدر تتعامل مع Linux operating system ببساطه علشان اللينكس بقي من اشهر ال OS المستخدمه حاليا ف ال market بمعني لو حضرتك بتستخدم Web Browser علشان ت Access اي web site هتبقي غالبا is interacting with Linux system كمان لو عندك smart tv هتلاقي ال OS اللي شغال عليه غالبا لينكس حتي في ال smart cars . حتي DNS الخاص بشركه جوجل اللي ال IP بتاعه 8.8.8.8 هتلاقيه شغال Linux operating system ف انت ك it engineer specially لو انت system admin او Network admin ف your career opportunities will be increased with Linux skills

➢ ايه المميزات اللي بتميز لينكس عن اي operating system تاني

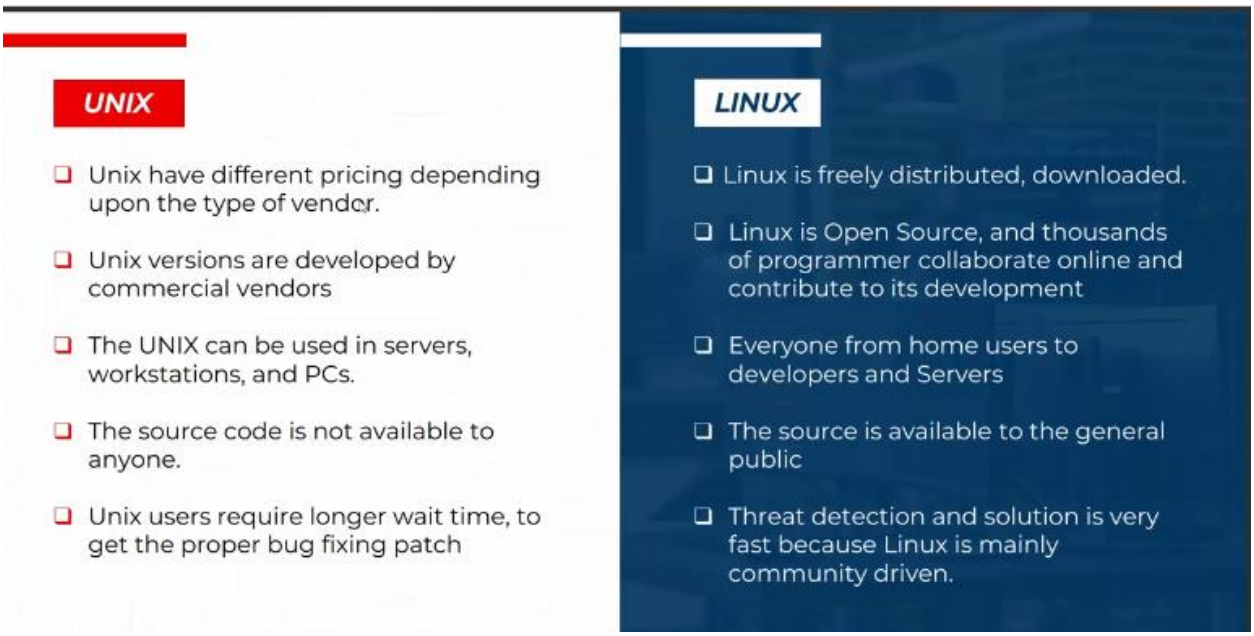
- اول حاجه اللينكس High security اكثر امانا عن ال windows بمعني ان انت لما تعمل Install ل ال windows اول حاجه بتعملها انك بتنزل برامج حمايه antivirus وده علي عكس اللينكس انك مبتعملش اي Install ل ا ي Antivirus
- من المميزات اللي بيتميز فيها اللينكس عن اي OS تاني وهي ال Stability علي سبيل المثال هتلاقي ال processing speed بتاعت اللينكس مش بتقل مع الوقت يعني انت لو جيت عملت Install ل اي Linux OS علي ال server وجيت بعد كذا سنه ف غالبا هتلاقي ال processing speed بتاعته محصلش فيها اي تاثير وده علي عكس الويندوز انك هتلاقي مع الوقت ال processing speed بيبدأ يبطي ويحصلش مشاكل

- وكمان Ease of Maintenance لو انت بتعمل software update في اللينكس انت مش محتاج انك كل شويه انك تعمل reboot للسيستم بتاعك علي عكس في الويندوز لو انت روحت عملت install ل اي software هتلاقي الويندوز بيطلب انك تعمل reboot للسيستم ولو انت عملت uninstall ل سوفت وير هتلاقيه بيطلب منك انك تعمل reboot حتي لو عملت ويندوز update هيطلب reboot اما في اللينكس قليل جدا لما بتحتاج انك تعمل reboot لل server بتاعك
- كمان من ضمن المميزات Runs on any hardware ودي معناها ان اللينكس can be installed and run on Old Hardware platform علي عكس الويندوز ساعات بتبقي محتاج تعمل upgrade او تعمل Install ل new windows version زي مثلا windows 11 علي لاب توب قديم عندك ف بتلاقي بيظهرلك بعض المشاكل اللي في الهارد وير ان مثلا امكانيات اللابت غير مسموح بيها ف ده بيتطلب منك انك تروح تعمل الاول upgrade للهارد وير بتاعك علشان تقدر انك تعمل install لل new windows version وده علي عكس اللينكس انك تقدر تعمله Install علي اي hardware موجود عندك
- ومن ضمن المميزات ان اللينكس بيكون free
- وومن ضمن اللميزات المهمه جدا في اللينكس ان هو بيكون open source معناها ان ال source code متاح ل اي حد يقدر يشوف ال source code ويعمل عليه change او modify واكيد بيجي سؤال طب طالما اللينكس free وopen source طب شركه زي red hat بتحقق ارباح ازاي شركه زي ريدهات بتقدم support و subscriptions وبتقدم مجموعه من ال training services لكل ال open source product بتاعتها ومجموعه من ال certificate ف بتحقق منها ارباح كويسه جداا
- ومن مميزات اللينكس انه ease of use and flexibility هتلاقي اللينكس flexible جدا و user friendly سهل جدا في التعامل
- Customizationاللينكس بيجي معاه command line interface او CLI اقدر من خلالها أ customizeاي task موجوده عندي واقدر اعمل automate لأي taskبمنتهي السهوله



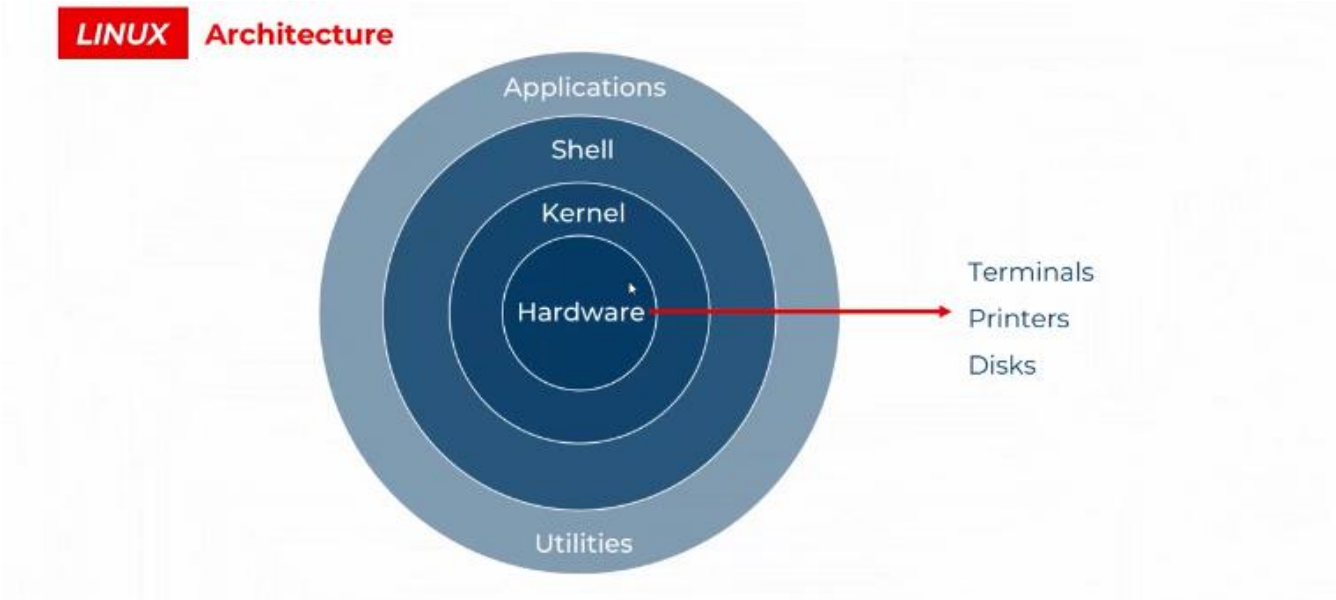
➢ هنتكلم عن ال Linux Distributions

- زي ماقولنا هو فكرت ان اللينكس Open Source ف اي حد يقدر انه هو ي modify في ال source code وي distribute ال Operating System او ال modification بتاعته في صوره distribution او في صوره Operating System ف دايما هتلاقي فيه مجموعه كبيره جدا من ال Linux Distributions ف احنا بنقسمها لمجموعه من ال Categories فيه category اسمها Desktop Distributions و category اسمها Server Distributions و category اسمها Embedded Distributions و category اسمها Specialize Distributions طب ايه الفرق مابينهم
  - ال Desktop Distributions دي بتبقي مصممه وموجهه لل Desktop User او ال End User ودي بتبقي دايما بتبقي جايه معاها features زي ال Graphical User Interface ومجموعه من ال applications وال tools اللي يقدر ال End User انه يستخدمها ومن ضمن الامثله اللي علي Desktop Distributions زي ال Ubuntu و Linux Mint و Fedora وال Debian
  - ال Server Distributions دي مجموعه من ال Operating System بتبقي موجهه ومصممه لل Servers وال Enterprises زي Red Hat Enterprise Linux و Centos و SUSE Linux Enterprise Server و Ubuntu Server
  - ال Embedded Distributions بتبقي موجهه ومصممه لل Embedded System زي مثلا ال Router فيه بعض ال Routers هتلاقي ال OS الموجود عليها هو لينكس واشهر مثال OS اسمه OpenWrt او open wireless router
  - ال Specialize Distributions ودي بتبقي OS مصممه لأستخدام محدد زي ال Gaming وال Security زي ال Kali Linux وال Development



➢ ايه الفرق بين ال UNIX , Linux

- احنا قولنا ان اللينكس بيكون completely free ان انت تقدر for free تعمله download و install وتستخدمة وده طبعا علي عكس ال Unix قالك ان ال Unix have different pricing وده ب depend علي ال vendor نفسه كل vendor ليه price معين
- تاني حاجه ان اللينكس بيكون open source معني ال open source ان ال source code available to any one علي عكس ال Unix ال Unix هنا بيكون closed source اللي يقدر ي modify او ي change ف الكود ده هو ال بس ال vendor اللي عمل create لل Unix OS
- تالت اختلاف ف اللينكس قالك ان اي حد يقدر يستخدم اللينكس بدايه من ال desktop users وال end users العاديه لحد ال servers وال workstation وال enterprises علي عكس ال Unix بيكون موجه اكتر لل enterprises وبيستخدم اكتر علي السيرفر وال workstation الكبيره
- اخر حاجه ف اللينكس ان فكره ال open source ده دايما بيخلي فكره ال solution او ال update بتكون اسرع كتير عن ال Unix

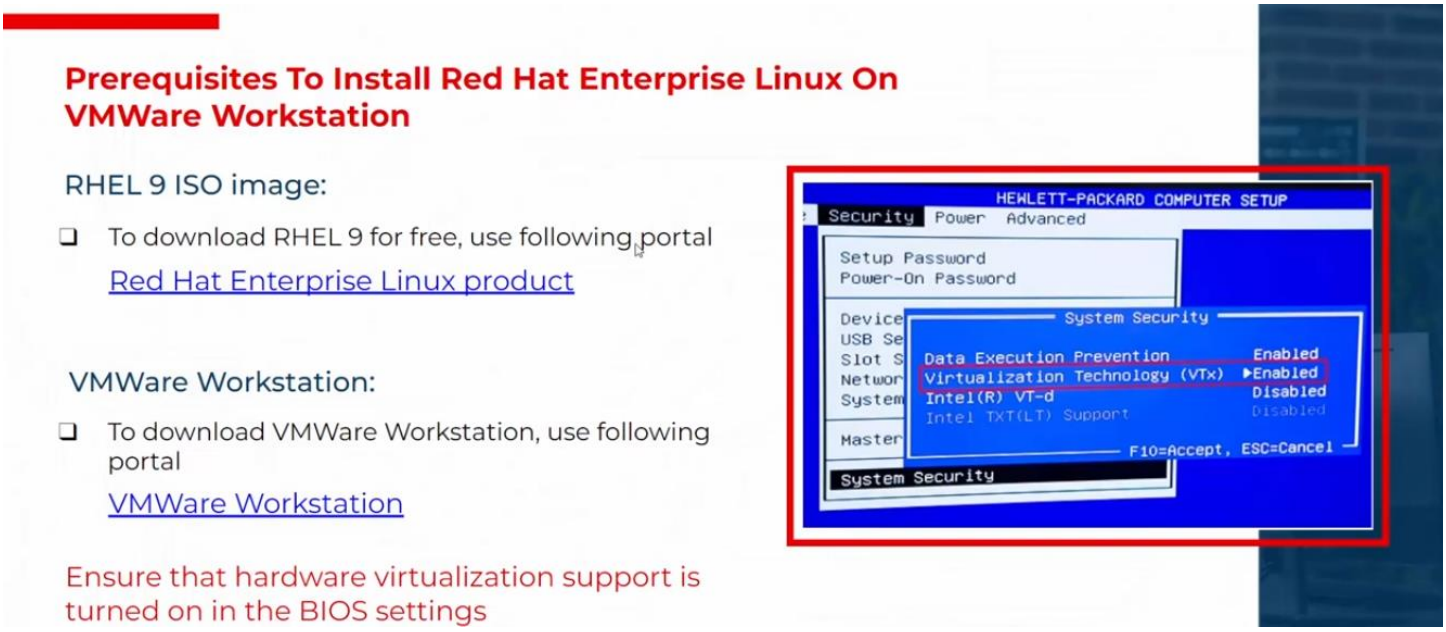


➢ ايه هو ال Linux architecture

- اول حاجه عندي هي ال Hardware وده بيكون عباره عن ال physical devices ال attached للسيستم بتاعي زي الهارد درايف و الرام و ال mother board و ال terminals و printers انا علشان امنج الهارد وير بتاعي محتاج سوفت وير اللي هو ال kernel
- وال kernel ده هو ال core OS المسئول عن الهارد وير مانجمينت والريسورس مانجمينت بس ال kernel ده علشان نتعامل معاه انا ك end user هيبقي صعب جدا علشان ال kernel حاجه معقده جداا وانا مش kernel engineer وانا ف الحاله دي هبقي محتاج وسيط اقدر اتعامل معاه بين اليوزر وال kernel الوسيط ده اسمه shell
- ال shell دي لو عايز احطلها تعريف هي عباره عن command interpreter او مترجم اوامر وظيفته الاساسيه انها تاخد ال inputs من ال users تترجمها لل kernel علشان ت manage الهارد وير بتاعي

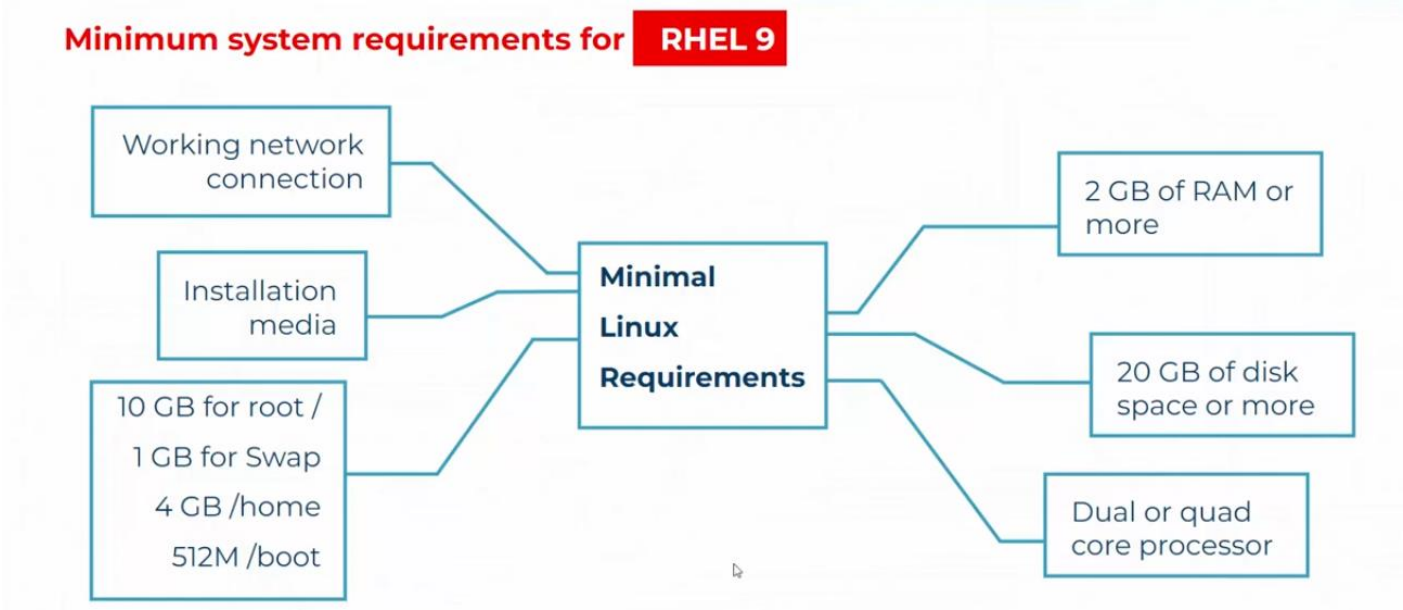
وفي نفس الوقت بتاخد ال outputs من ال kernel وتعرضلي ال result علي ال shell او ال root عندي
انا عندي ال shell في عندي منها شكلين اول شكل بيكون GUI وتاني شكل بيكون CLI

- اخر حاجه عندي هي ال application و ال utilities ودي بتكون عباره عن الابلكيشن ال installed عندي علي ال OS زي مثلا ال web browser ال text editor ال media player

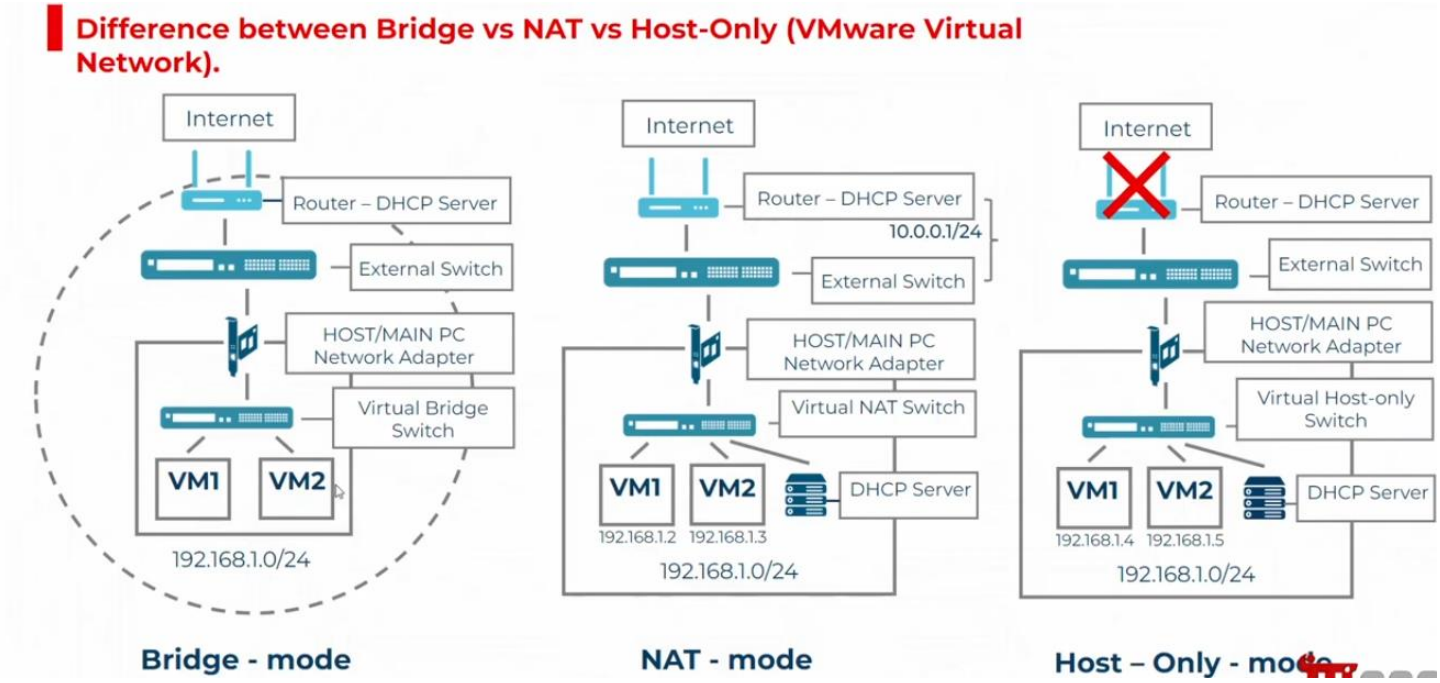


- طبعا علشان اعمل install لل Virtual Machine محتاج يكون عندي حاجتين

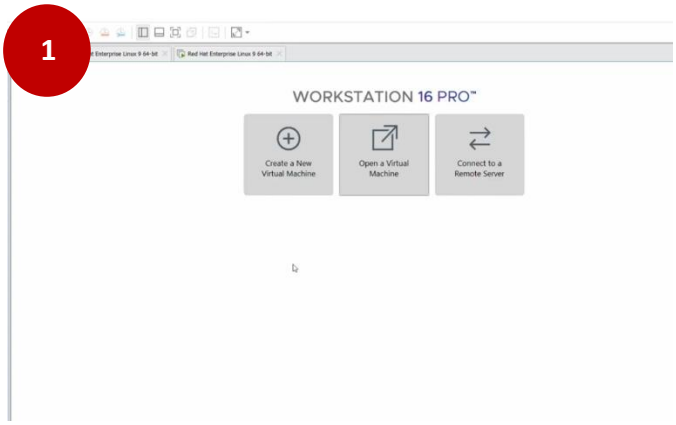
- اول حاجه ايه هي ال ISO Image اللي انا هستخدمها علشان اعمل Install ل OS ودي احنا هنشتغل في الكورس علي Red Hat 9 واقدر ببساطه ان اعمل download لل ISO Image مجانا عن طريق ان احنا هندخل علي الرابط ده Download Red hat 9 ونعمل download لل ISO
- تاني حاجه محتاج اني اعمل Download للابلكيشن اللي انا عن طريقه اقدر اتعامل مع الهارد وير بتاعي انا عندي كذا option ممكن انزل VMWare Workstation او Virtual Box او Oracle Virtual Box ف انت اشتغل علي اللي انت عايزه بس الافضل والاحسن انك تشتغل علي ال VMWare Workstation وهنعمل Download ليه عن طريق الضغط علي الرابط ده Download VMWare Workstation
- انا كده جاهز اني اعمل install لأي VM فيه ملحوظه مهمه ساعات فيه laptops القديمه جدا بيبقي ال Virtualization Technology بتبقي disable by default في الحاله دي هتبقي محتاج انك تدخل علي ال BIOS Settings وهتلاقي حاجه اسمها Security وهتدخل عليSecurity وهتلاقي في الSystem Security فيه حاجه اسمها Virtualization Technology(VTx) ودي بتبقي معمول ليها Disable هتعملها Enable وتعمل reboot هتلاقي كل حاجه شغاله معاك



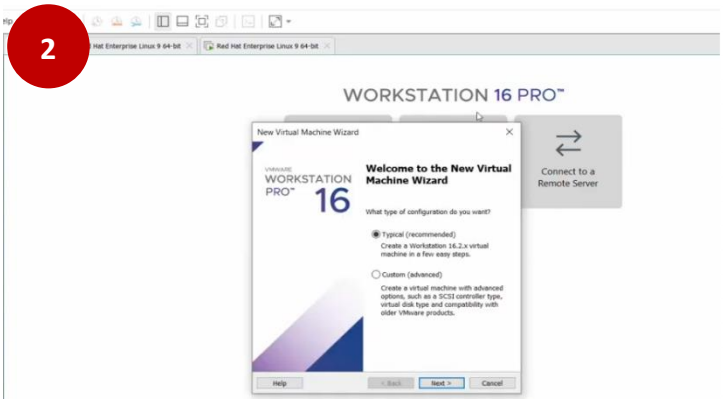
- انا علشان اعمل install لل VM عندي محتاج بعض ال Minimal requirements علشان اقدر اعمل Install زي مثلا محتاج علي الاقل 2 جيجا للرام او ازيد وبالنسبه لل Disk محتاجين 20 جيجا او ازيد وبالنسبه لل processor محتاجين Dual or quad core processor ومحتاجين ال Network Interface Card او Working network connection ومحتاجين ال Installation media اللي احنا عملنا ليها download مع علي Red Hat ومحتاجين ان احنا نعمل Partitions انا عندي 20 جيجا في ال Disk ف ال 20جيجا احنا هنعمل create لمجموعه من البارتشن هعمل create ل 10 جيجا ل root file system و 1 جيجا لل swap memory و 4 جيجا لل home directory و 512 ميجا لل boot وهنعرف كل ده بالتفصيل في الكورس



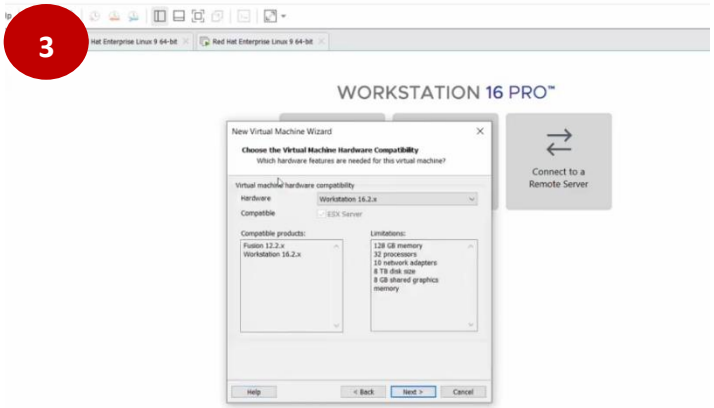
1


WORKSTATION 16 PRO™
Create a New Virtual Machine
Open a Virtual Machine
Connect to a Remote Server

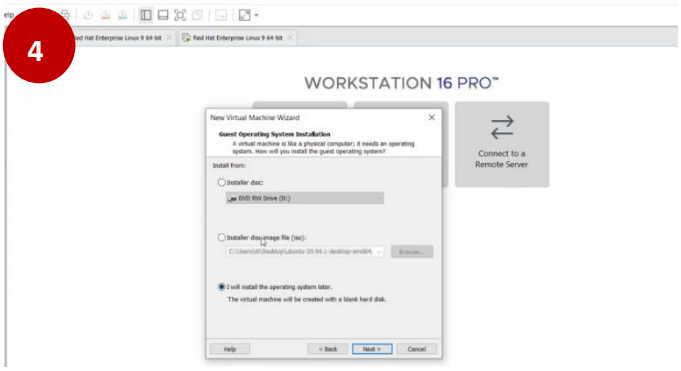
2


WORKSTATION 16 PRO™
New Virtual Machine Wizard
Welcome to the New Virtual Machine Wizard
WORKSTATION PRO™ 16
Connect to a Remote Server

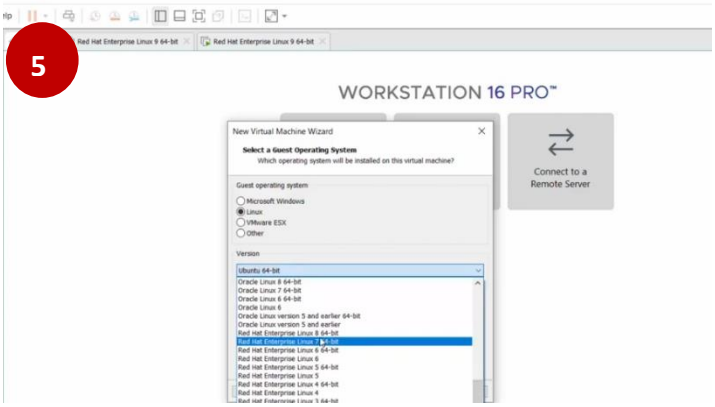
3


WORKSTATION 16 PRO™
New Virtual Machine Wizard
Choose the Virtual Machine Hardware Compatibility
Connect to a Remote Server

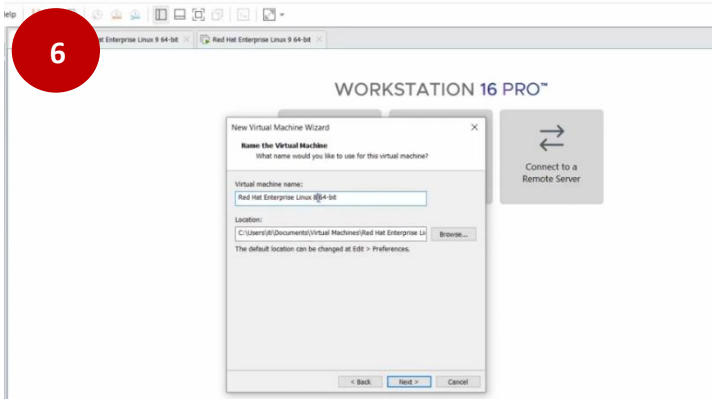
4


WORKSTATION 16 PRO™
New Virtual Machine Wizard
Guest Operating System Installation
Connect to a Remote Server

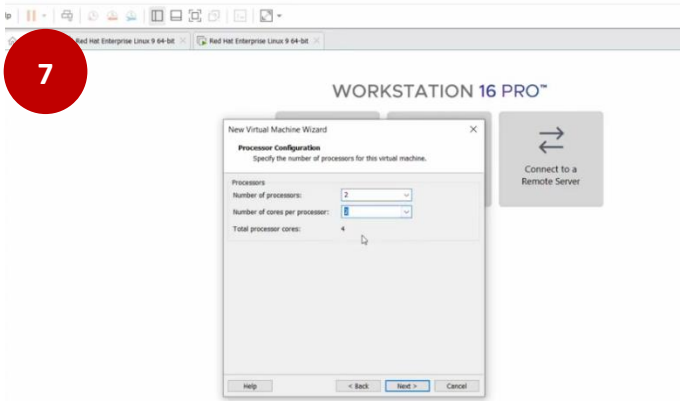
5


WORKSTATION 16 PRO™
New Virtual Machine Wizard
Select a Guest Operating System
Connect to a Remote Server

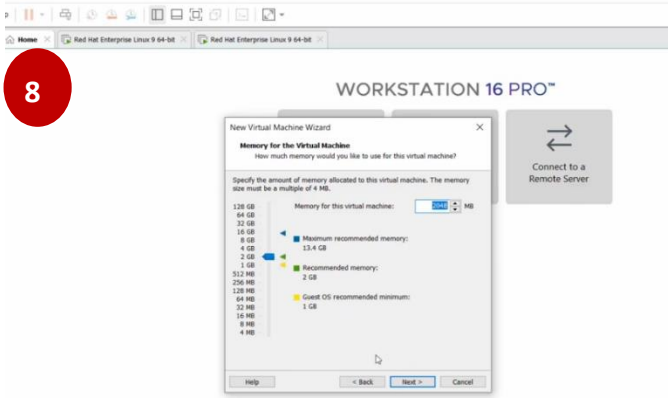
6


WORKSTATION 16 PRO™
New Virtual Machine Wizard
Name the Virtual Machine
Connect to a Remote Server

7

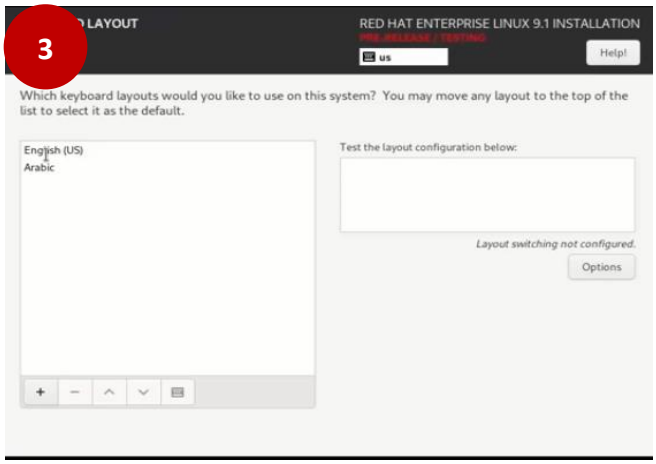

WORKSTATION 16 PRO™
New Virtual Machine Wizard
Processor Configuration
Connect to a Remote Server

8

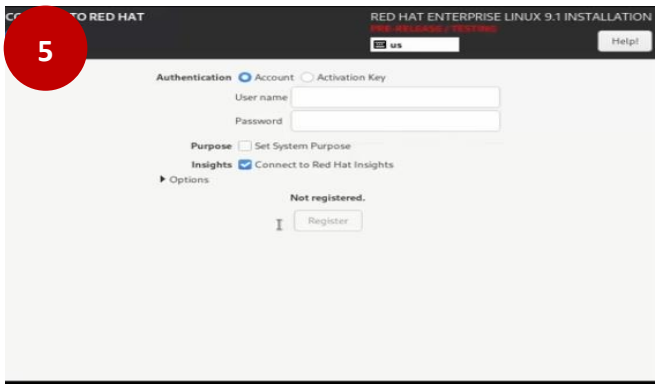

WORKSTATION 16 PRO™
New Virtual Machine Wizard
Memory for the Virtual Machine
Connect to a Remote Server

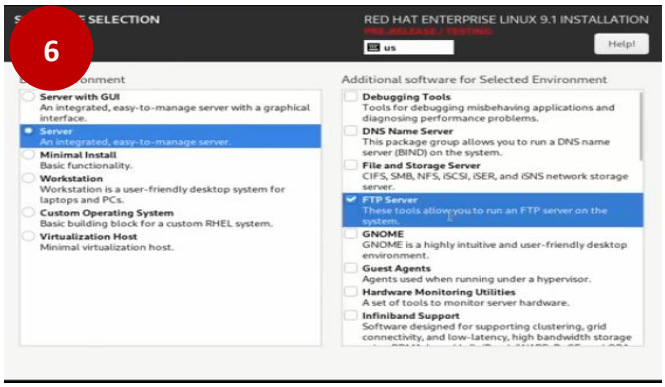
1
Red Hat
مرحبًا بكم في RED HAT ENTERPRISE LINUX 9.1.
ما اللّغة التي تودّ استخدامها أثناء عمليّة التثبيت؟
العربية (مصر)
العربية (السودان)
العربية (الجزائر)
العربية (المغرب)
العربية (العراق)
العربية (المملكة العربية السعودية)
العربية (اليمن)
العربية (سوريا)
العربية (تونس)
العربية (ليبيا)
Arabic
English
French
German
Japanese
Mandarin Chin...
Russian
Spanish
Afrikaans
Continue
Quit

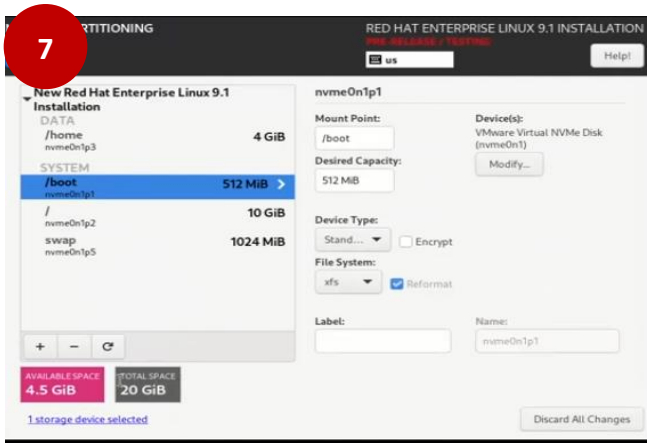
2
INSTALLATION SUMMARY
RED HAT ENTERPRISE LINUX 9.1 INSTALLATION
PRE-RELEASE / TESTING
Help!
LOCALIZATION
Keyboard
English (US)
Language Support
English (United States)
Time & Date
Africa/Cairo timezone
SOFTWARE
Connect to Red Hat
Not registered.
Installation Source
Local media
Software Selection
Server with GUI
SYSTEM
Installation Destination
Automatic partitioning
KDUMP
Kdump is enabled
Network & Host Name
Wired (ens160) connected
Security Profile
No profile selected
USER SETTINGS
Root Password
Quit
Begin Installation
We won't touch your disks until you click 'Begin Installation'.
Please complete items marked with this icon before continuing to the next step.

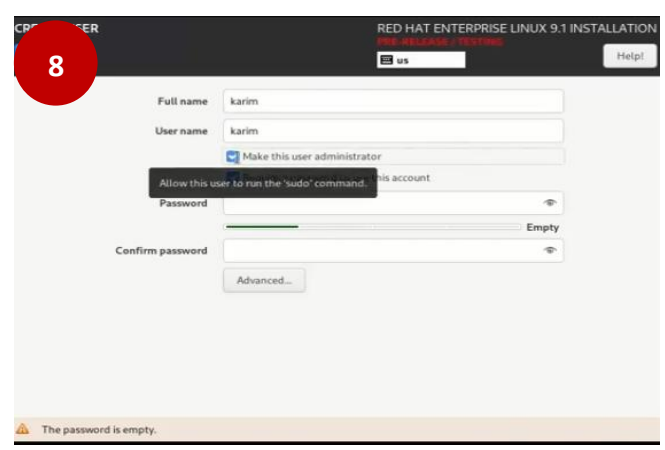

3
LAYOUT
RED HAT ENTERPRISE LINUX 9.1 INSTALLATION
Help!
Which keyboard layouts would you like to use on this system? You may move any layout to the top of the list to select it as the default.
English (US)
Arabic
Test the layout configuration below:
Layout switching not configured.
Options

4
INSTALLATION SUMMARY
RED HAT ENTERPRISE LINUX 9.1 INSTALLATION
PRE-RELEASE / TESTING
Help!
LOCALIZATION
Keyboard
English (US), Arabic
Language Support
English (United States)
Time & Date
Africa/Cairo timezone
SOFTWARE
Connect to Red Hat
Not registered.
Installation Source
Local media
Software Selection
Server with GUI
SYSTEM
Installation Destination
Automatic partitioning
KDUMP
Kdump is enabled
Network & Host Name
Wired (ens160) connected
Security Profile
No profile selected
USER SETTINGS
Root Password
Quit
Begin Installation
We won't touch your disks until you click 'Begin Installation'.
Please complete items marked with this icon before continuing to the next step.


5
TO RED HAT
RED HAT ENTERPRISE LINUX 9.1 INSTALLATION
Help!
Authentication
Account
Activation Key
User name
Password
Purpose
Set System Purpose
Insights
Connect to Red Hat Insights
Options
Not registered.
Register


6
SELECTION
RED HAT ENTERPRISE LINUX 9.1 INSTALLATION
Help!
Server with GUI
An integrated, easy-to-manage server with a graphical interface.
Server
An integrated, easy-to-manage server.
Minimal Install
Basic functionality.
Workstation
Workstation is a user-friendly desktop system for laptops and PCs.
Custom Operating System
Basic building block for a custom RHEL system.
Virtualization Host
Minimal virtualization host.
Additional software for Selected Environment
Debugging Tools
Tools for debugging misbehaving applications and diagnosing performance problems.
DNS Name Server
This package group allows you to run a DNS name server (BIND) on the system.
File and Storage Server
CIFS, SMB, NFS, iSCSI, iSER, and iSNS network storage server.
FTP Server
These tools allow you to run an FTP server on the system.
GNOME
GNOME is a highly intuitive and user-friendly desktop environment.
Guest Agents
Agents used when running under a hypervisor.
Hardware Monitoring Utilities
A set of tools to monitor server hardware.
Infiniband Support


7
RTITIONING
RED HAT ENTERPRISE LINUX 9.1 INSTALLATION
Help!
New Red Hat Enterprise Linux 9.1 Installation
DATA
/home
nvme0n1p3
4 GiB
SYSTEM
/boot
nvme0n1p1
512 MiB
/
nvme0n1p2
10 GiB
swap
nvme0n1p5
1024 MiB
nvme0n1p1
Mount Point:
/boot
Desired Capacity:
512 MiB
Device(s):
VMware Virtual NVMe Disk (nvme0n1)
Modify...
Device Type:
Stand...
Encrypt
File System:
xfs
Reformat
Label:
Name:
nvme0n1p1
AVAILABLE SPACE
4.5 GiB
TOTAL SPACE
20 GiB
1 storage device selected
Discard All Changes


8
RED HAT ENTERPRISE LINUX 9.1 INSTALLATION
Help!
Full name
karim
User name
karim
Make this user administrator
Allow this user to run the 'sudo' command.
Password
Empty
Confirm password
Advanced...
The password is empty.

Chapter 2

Accessing the Command Line

Introduction to the bash shell

- A command line is a text-based interface which can be used to input instructions to a computer system.
- The default shell for users in Red Hat Enterprise Linux is the GNU Bourne-Again Shell (**bash**).
- When a shell is used interactively, it displays a string when it is waiting for a command from the user. This is called the shell prompt.
- When a regular user starts a shell, the default prompt ends with a **$** character, as shown below.

```
[karim@RHEL9 ~]$
```

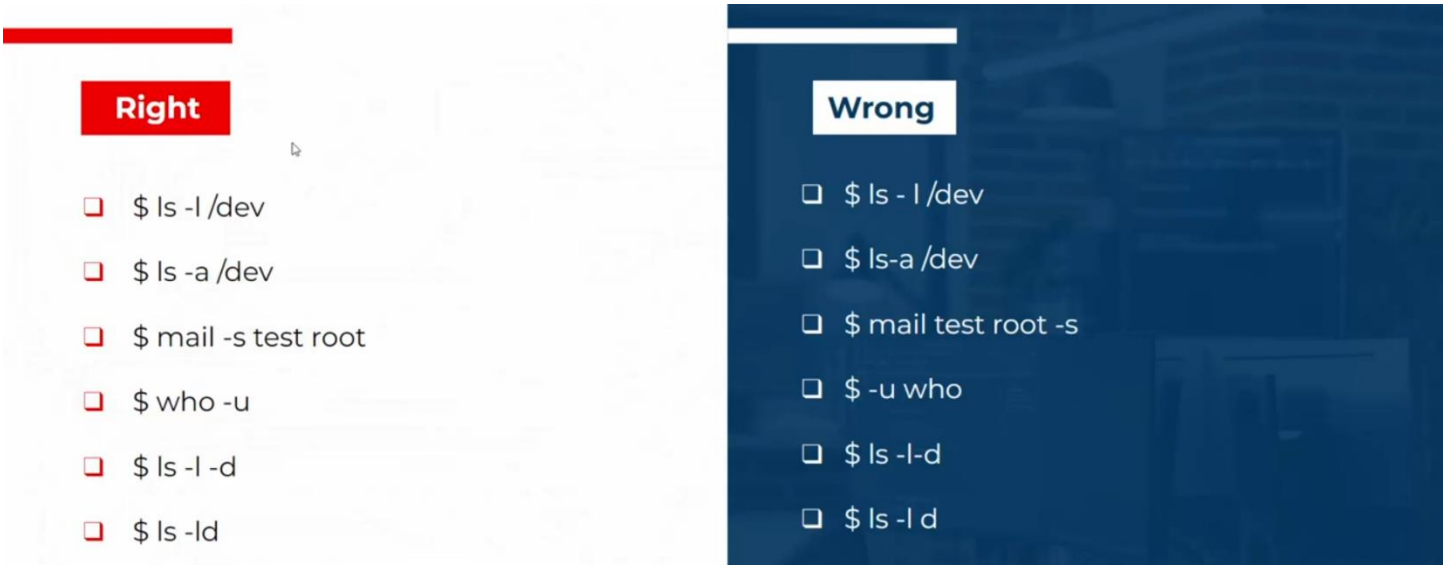
- The **$** character is replaced by a **#** character if the shell is running as the superuser, root.

```
[root@RHEL9 ~]#
```

- قبل اما نبدأ ازاي ن Access ال CLI او ال Command Line Interface عايزين ناخد Introduction عن ال Bash Shell

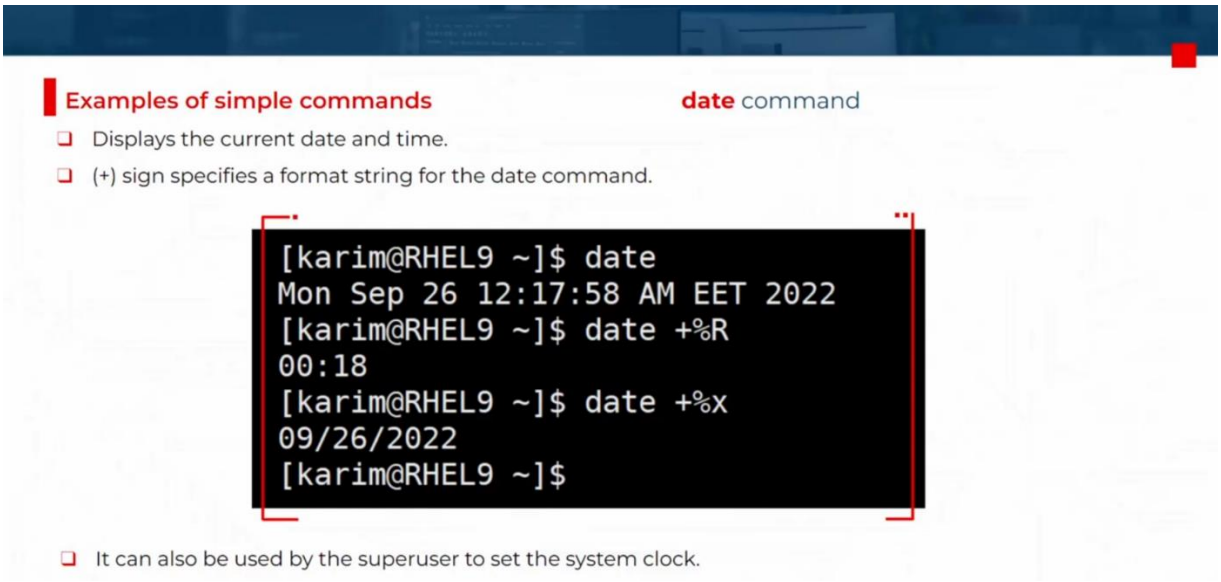
- اول حاجه ايه هي ال Bash هي عباره عن Command Interpreter بيكون هو ال Interface مابين ال user وال Kernel اللي انت من خلال ال Shell ان انت ت Pass اوامر و تبعتها لل Kernel علشان ينفذها ويرجعلك بال Output
- طب ايه هو ال Command Line هو عباره عن Text based interface Which can be used to input instructions to a computer system
- في Red Hat Enterprise Linux ال default shell بتاعتنا هي الBash
- اول اما تفتح ال Command Line Interface بيظهرلك في ال CLI شكل كده Prompt بيتقال عليها Shell Promptال Shell Prompt زي ماحنا شايفين هنا `[karim@RHEL9 ~]$` تقدر تطلع منها بكذا معلومه اول معلومه مين هو ال user name اللي هو logged in دلوقتي ال interactive user زي Karim وبعدين @ وبعدين ال Hostname الخاص ب ال Virtual machine بتاعتك زي ال RHEL9 وبعدين علامة التيلدا ~ معناها انت واقف في ال Home Directory بتاع اليوزر اللي اسمه karim وهنشوف الكلام ده بالتفصيل قدام شويه وفي الاخر الdollar sign $
- خد بالك من حاجة لو انت عامل Logging ب Normal User او Regular User هتلاقي هنا ف ال Shell Promptاللي طلعالك هتلاقي ف الاخر $ Doller Sign `[karim@RHEL9 ~]$`
- لو انت عامل Logging ب ال Super User او ال Root او ال Administrator هتلاقي حاططلك ف الاخر # زي `[root@RHEL9 ~]#` ف من شكل ال Prompt تقدر تعرف من خلال ال $ و # انت Super user ولا Regular user
-

- قبل اما نبدأ بال command syntax حابب اعرفكم حاجه احنا طول الكورس بتاعنا في red hat admin1,2 بنسبه 90% هنتعامل مع ال CLI احنا مش هنتعامل مع ال GUI غير في حالات قليله جدا جدا وبردك خد بالك ان انت في ال market بعد كده لو انت شغال في اي مكان هتتعامل بال CLI لان في معظم الاوقات ال Servers اللي هتتعامل معاها بتبقي موجوده في مكان اسمه Data Center وانت بتـ Access كل السيرفرات دي remotely ف علشان تبدأ تكتب Command علي ال CLI لازم تعرف ال Syntax بتاع ال Command عامل ازاي اولا ال Command بيتكون من 3 اجزاء
  1- اول حاجه ال Command او الامراللي انت عايز تعمله Run
  2- تاني حاجه الOption دي حاجه بتعدل في ال behavior بتاع ال Command بتاعك عايز تعدل في شكل ال output عايز ال Command يعمل حاجه معينه ف بتزودله Option معين
  3- وتالت حاجه ال Argument
- في المثال اللي فوق في Command عندي اسمه **Usermod** ده لو انا عايز اعمل Modify لـuser معين ف ال Command في ال option لازم احط قبلهاا داش – ف هو حاطط **-L** ده ال Option بتاعنا وال **-L** ده بيعمل Lock وبعد كده ال Argument اللي هو اسم ال User اللي عندي اللي اسمه user01. ف كده ببساطه ال Command ده الهدف منه انك تعمل lock للباسورد بتاعت ال user01 ده كده مثال عن ال Command syntax

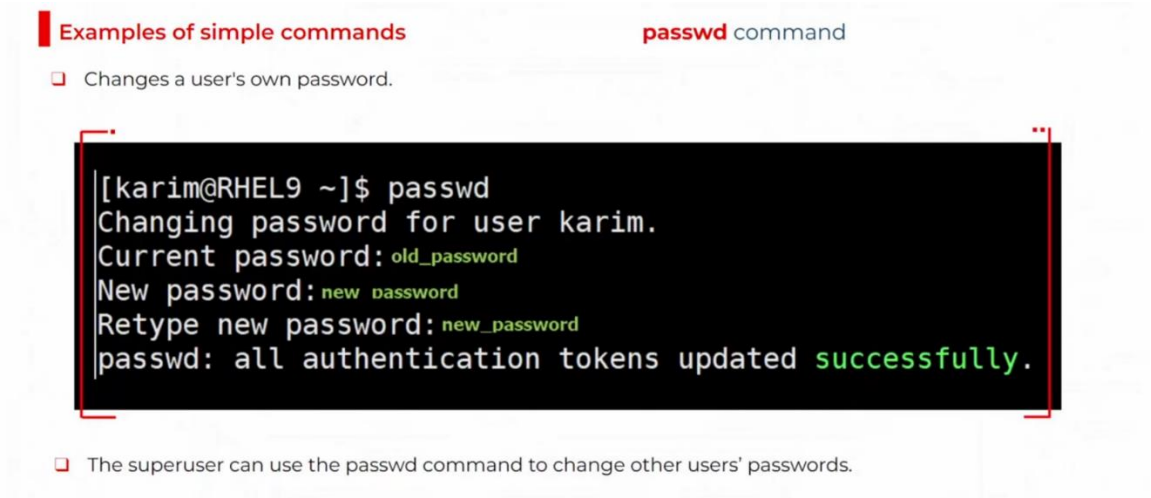


- هنيجي هنا ن Practice هنلاقي علي الشمال ال Commands مكتوبه بال Right Syntax وعلي اليمين مكتوبه بال Wrong syntax تعال نشوف كل Command ونشوف ايه الصح وايه الغلط كل ال Commands هنشوفها بالتفصيل اثناء الكورس

- اول Command بيقولك **ls -l /dev** ده مكتوب بال Syntax المظبوط اما ال command الغلط مكتوب **ls – l /dev** علشان لازم ال option يكون لازق في الداش **-** مينفعش اكتب داش وبعدين مسافه
- تاني Command مكتوب **ls-a /dev** هنا لازم ال command يكون مفصول عن ال Option
- ال Command اللي بعد كده مكتوب **mail test root -s** اهم حاجه الترتيب مينفعش اكتب ال argument وبعدين ال option
- لو انا عايز اديله اكتر من option ممكن اقوله داش الاوبشن الاولاني مسافه داش الاوبشن التاني زي **ls -l -d** او ممكن احط داش واحده وبعدين الاوبشن كلها اللي انا عايزها زي ال **ls -ld**



- خلينا بقي هنا ن Go through بعض ال Basic Commands ونشوف ايه هو ال syntax بتاعهاا وازاي نعملها Runعلي ال CLI اول Command معانا هو command اسمه date انا بستخدمه لو انا عايز أ displays ال current date and timeطبعا ال command نفسه ممكن اكتبه بس date وبعدين Enter فالحاله دي ه displayال current date وال time بتاعي زي `[karim@RHEL9 ~]$ date` `Mon Sep 26 12:17:58 AM EET 2022` او ممكن احط عليه مجموعه من الا options ممكن اكتبله date +%R ال + هنا لو انا عايز اعدل في ال format بتاع ال Output بتاعي هنا +%R هنا هيعرضلي الساعه كام دلوقتي بس زي `[karim@RHEL9 ~]$ date +%R` `00:18` او استخدم ال +%X هنا هيعرضلي التاريخ زي `[karim@RHEL9 ~]$ date +%x` `09/26/2022`



- تاني Command معانا هو Command اسمه Passwd بستخدمه لو انا عايز اعمل Change للباسورد بتاعتي يبقي انا هنا ك يوزر اسمه Karim ممكن اغير الباسورد بتاعتي ف اي وقت باستخدام امر passwd بقوله Passwd وبعدين enter وهدخله ال old password بتاعتي وبعدين ال new password طب هل انا ك يوزر Karim اقدر اني اغير باسورد اي يوزر تاني لا مقدرش ال superuser او ال root هو اللي مسموح ليه انه يغيرالباسورد بتاعت اي يوزر تاني

Examples of simple commands — file command

- Scans the beginning of a file's contents and displays what type it is.
- The files to be classified are passed as arguments to the command.

```
[karim@RHEL9 ~]$ file /etc/passwd
/etc/passwd: ASCII text
[karim@RHEL9 ~]$ file /home
/home: directory
```

- فيه Command اسمه file بيعمل scan لل file contents ويقولي ال type بتاع ال fileده ايه خدهاا قاعده احنا عندنا ف اللينكس everything is a file يعني لينكس بيتعامل مع كل حاجه كانها file بيتعامل مع الهارد ديسك كانه file وبيتعامل مع ال ISO كانه file وبيتعامل مع الميموري كانهاا file وال directory عباره عن file طب لو انا عايز اعرف ال type بتاع ال file هستخدم command اسمه file
- ف مثلا لو نفذنا ال command اللي فوق **file /etc/passwd** الpasswd ده stored جواه كل اليوزر الcreated عندي في ال system

Examples of simple commands — cat command

- View the contents of files.

```
[karim@RHEL9 ~]$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
```

- Concatenate the contents from multiple files.
- Redirect contents of the file to a terminal or files.
- Display the contents of multiple files.

```
[karim@RHEL9 ~]$ cat file1 file2
Hello Mahara-Tech
Introduction to Linux commands.
```

- نيجي بعد كده لو انا عندي text file وعايز a Display ال content بتاعت text file هستخدم command اسمه cat

- لو هنفذ الامر cat /etc/passwd هيظهرلي كل ال content الموجوده ف ال passwd

```
[root@MohamedAtef ~]# cat /etc/passwd
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin
gnome-initial-setup:x:981:980::/run/gnome-initial-setup/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
Elbitawy:x:1000:1000:Elbitawy:/home/Elbitawy:/bin/bash
```

- ممكن استخدم نفس ال Command ان انا a Display ال content بتاعت اكتر من file زي مثلا اعرض محتوي ال passwd و محتوي ال redhat-release ده file بيكون موجود فيه الversion بتاعت ال operating system بتاعي ف ال command اللي انا كتبته هيعرضلي كل اللي موجود في ال passwd وف الاخر هيعرضلي ال version

```
[root@MohamedAtef ~]# cat /etc/passwd /etc/redhat-release
cockpit-ws:x:983:982:User for cockpit web service:/nonexisting:/sbin/nologin
cockpit-wsinstance:x:982:981:User for cockpit-ws instances:/nonexisting:/sbin/nologin
gnome-initial-setup:x:981:980::/run/gnome-initial-setup/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/usr/share/empty.sshd:/sbin/nologin
chrony:x:980:979:chrony system user:/var/lib/chrony:/sbin/nologin
dnsmasq:x:979:978:Dnsmasq DHCP and DNS server:/var/lib/dnsmasq:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
Elbitawy:x:1000:1000:Elbitawy:/home/Elbitawy:/bin/bash
Red Hat Enterprise Linux release 9.2 (Plow)
```

ده محتوي /etc/passwd

ده محتوي /etc/redhat-release

Examples of simple commands **less** command

- Displays **one page** of a file at a time and lets you scroll at your leisure.

```
[karim@RHEL9 ~]$ less /etc/passwd
```

- المشكله في الcat command ان هو بيعرضلي ال output كله at once في ال CLI بتاعتك ف لو انت عندك file حجمه كبير جدا ف كده مش هيكون human readable ليك انك عايز تشوف محتوي ال text file ده page by page ف cat مش بي support الحته دي ف هنا في command تاني اسمه less ده بيعرضلي ال content بتاع ال text file بتاعك one page at a time زي مهنشوف لو نفذنا الامر التالي **less /etc/passwd** ده هيعرضلي اول صفحه من الملف اللي اسمه Passwd واقدر من خلاله اني اتحكم ف عرض الملف من خلال اني استخدم الاسهم اللي عندي ف الكيبورد اني اعمل scroll up و scroll down وفيه option اني اقدر اعمل search علي pattern معين او كلمه معينه عن طريق ان بدوس علي forward slash / واكتب بعديها ال pattern اللي عايز اسيرش عليه

Examples of simple commands — head and tail commands

- Display the beginning and end of a file, respectively (10 lines of the file)
- -n option allows a different number of lines to be specified

```
[karim@RHEL9 ~]$ head -n 2 /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
[karim@RHEL9 ~]$ tail -n 3 /etc/passwd
tcpdump:x:72:72::/:/sbin/nologin
systemd-oom:x:978:978:systemd Userspace OOM Killer:/:/usr/sbin/nologin
karim:x:1000:1000:Karim:/home/karim:/bin/bash
```

- عندنا command تاني اسمه **tail** و**head** دول شبه ال cat شويه بس الفرق مابينهم ومابين ال cat ان الcat بي display ال content بتاع ال file كله علي الاسكرين طب **head** بيعمل ايه لو انت حطلته اسم الفايل بس by default بيعمل display اول 10 سطور في الفايل و**tail** العكس بيعمل display ل اخر 10 سطور في الفايل بتاعك وممكن تحطله **-n** option وتحددله عدد السطور اللي انت عايزه يعرضها

Examples of simple commands — history command

- Displays a list of previously executed commands prefixed with a command number.
- (**!**) is a metacharacter that is used to expand previous commands without having to retype them.

```
[karim@RHEL9 ~]$ history
   50  history
   51  history | tail
   52  ls
   53  pwd
   54  date
   55  cal
   56  who
   57  uptime
   58  ls
   59  history
[karim@RHEL9 ~]$ !54
date
Mon Sep 26 01:11:09 AM EET 2022
[karim@RHEL9 ~]$ !ls
ls
Desktop  Documents  Downloads  file1  file2  Music  Pictures
```

- نيجي دلوقتي ل command اسمه **history** ال history بي List كل ال commands اللي انا نفذتها في ال CLI
  - لو انا قولتله history هيعرضلي كل ال commands زي مظاهر ف الصوره فوق
  - طب لو انا عايز انفذ command معين كان في ال history اقوله علامه تعجب ! وفيه علي الشمال ارقام ال command نفسه وليكن عايز انفذ الامر اللي اسمه date هكتب هكتب علامه تعجب وبعدين رقم ال command زي **!54**
  - طب لو عايز انفذ اخر command انا نفذته هستخدم علامه التعجب مرتين **!!**
  - لو انا عايز اسيرش جوه ال history هضغط علي **CTRL+R**

Terminal shortcuts — TAB completion

- Allows a user to quickly complete commands or file names after they have typed enough at the prompt to make it unique.
- If the characters typed are not unique, pressing the tab key twice displays all commands that begin with the characters already typed.

```
[user@host ~]$ pas❶Tab+Tab
passwd        paste        pasuspender
[user@host ~]$ pass❷Tab
[user@host ~]$ passwd
Changing password for user user.
Current password:
```

```
[user@host ~]$ ls /etc/pas❶Tab
[user@host ~]$ ls /etc/passwd❷Tab
passwd    passwd-
```

- تعال بقي نتكلم علي بعض ال Shortcuts

➢ اول terminal shortcuts موجوده معانا هي ال **TAB** بستخدمها لو انا مش عارف ال command اللي انا عايز انفذه بس عارف اول 3 حروف منه ف انا بكتب مثلا اول 3 حروف من ال command ده واضغط tab ممكن يكملي ال command ده طب لو مكملش بضغط علي tab مرتين ف بيظهرلي كل ال command اللي بتبدأ بأول 3 حروف دول

Terminal shortcuts

- (\ ) Continuing a long command on another line

```
[karim@RHEL9 ~]$ head -n 3 \
> /usr/share/dict/words \
> /usr/share/dict/linux.words
==> /usr/share/dict/words <==
1080
10-point
10th

==> /usr/share/dict/linux.words <==
1080
10-point
10th
```

- احيانا ساعات وانا بكتب في ال CLI ال Command بتاعي بيكون طويل جدا لو عايز اكتب command طويل جدا علي كذا سطر ف انا هكتب \ وبعدين اضغط علي Enter ف هو هيفتحلي prompt جديده اكمل فيها باقي ال command بتاعي وبمجرد اني اضغط Enter هينفذلي الامر ده زي مظاهر ف المثال اللي فوق ف انا لازم اكتب باك اسلاش \ علشان ال bash تفهم ان انت عايز تقسم ال command بتاعك علي كذا سطر

Terminal shortcuts

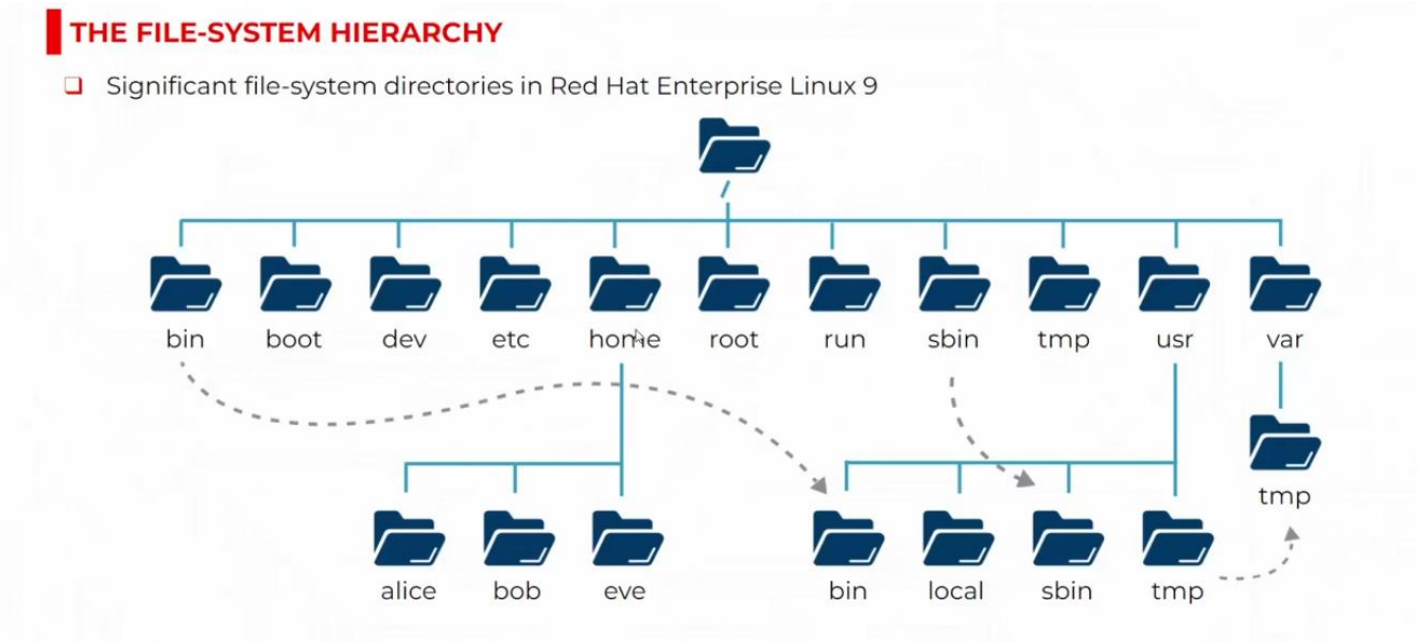
Ctrl+A	Jump to the beginning of the command line.
Ctrl+E	Jump to the end of the command line.
Ctrl+U	Clear from the cursor to the beginning of the command line.
Ctrl+K	Clear from the cursor to the end of the command line.
Ctrl+LeftArrow	Jump to the beginning of the previous word on the command line.
Ctrl+RightArrow	Jump to the end of the next word on the command line.
Ctrl+R	Search the history list of commands for a pattern.

- عندي مجموعه من ال shortcuts اللي هتسهل علينا التعامل مع ال Terminal عن طريق الكيبورد

- لو انا مثلا كاتب command ف طبيعي المؤشر هيكون في نهايه ال Line طب لو انا عايز المؤشر يكون في بدايه ال Line هضغط علي **CTRL+A**
- لو المؤشر في بدايه ال Line و عايز المؤشر يكون في نهاية ال Line هضغط علي **CTRL+E**
- لو ضغط علي **CTRL+U** ده هيمسح من اول ال Line ل بدايه المؤشر واقف فين
- لو ضغط علي **CTRL+K** هيمسح من بدايه المؤشر ل نهايه ال Line
- لو ضغط علي **CTRL+LeftArrow** يعني لو ضغط علي CTRL وسهم شمال المؤشر هيتنقل من كلمه ل كلمه ناحيه الشمال
- لو ضغط علي **CTRL+RightArrow** يعني لو ضغط علي CTRL وسهم يمين المؤشر هيتنقل من كلمه ل كلمه ناحيه اليمين
- اما **CTRL+R** لو انا عايز اعمل search في ال History بتاعي

Chapter 3

Managing Files from the Command Line



- دلوقتي هنتكلم عن ال File System Hierarchy

- مبدئيا انا عندي ال files في اللينكس هي stored و organized بطريقه معينه according لل types وال purpose بتاع كل file في ال Directories الموجوده في ال tree اللي قدامنا
- لو جينا في بدايه ال tree من فوق او في بدايه ال file system من فوق هنلاقي فيه كده Directory مكتوب تحتيه (/) forward slash وده بيتقال عليه slash file system او root file system وده بيبقي بدايه ال file system hierarchy نقدر نقول ان ال directory ده شبه كده My Computer في الويندوز
- لو دخلنا جوه ال slash file system او ال root directory هنلاقي جواه مجموعه من ال directory وال sub directory كل directory منهم بيبقي stored جواه مجموعه من ال files وليه purpose معين هنشوفه كمان شويه
- لو جينا بصينا هنلاقي كده فيه سهم معمول من bin ل directory تاني اسمه bin وسهم كمان معمول من sbin ل directory تاني اسمه sbin طب السهم ده معناه ايه معناه ان ده عباره shortcut علشان توصل لل data بتاعتك بكل سهوله ف انت مثلا عندك ال directory اللي اسمه bin الموجود في اسفل ال hierarchy ال directory ده ال Parent بتاعه directory تاني اسمه usr وال Parent بتاع ال usr هو ال root directory ف انا لو عايز أ access ال directory اللي اسمه bin عندي طريقتين ي اما اقوله **/usr/bin** خلي بالك من حاجه ال separated مبين ال directory وال subdirectory هو ال / slash ف انا هقول **/usr/bin** يعني انا لو دخلت علي **/bin** ده كاني دخلت علي محتوي **/usr/bin**

➢ خلينا نشوف ال purpose بتاع كل Directory من ال Directories الموجوده

Location	Purpose
/boot	➢ ده بيبقي جواه ال bootable file اللي السيستم بيحتاجها وهو بي boot up او بي restart up
/dev	➢ بيبقي stored جواه كل ال special device الموجوده عندك يعني اللينكس بيتعامل مع ال Hardware devices ال connected بال server علي انها files وال files دي بتبقي عباره عن special file يعني بيتعامل مع الهارد وير كانه special file وبيتعامل مع ال memory كانه special file وبيتعامل مع الكيبورد والماوس كانها files وكل ده بيبقي stored تحت /dev
/etc	➢ وده بيبقي فيه ال system configuration file يعني معظم ال configuration file الموجوده عندي في اللينكس بتبقي stored في /etc وده بيبقي من ال directories المهمه جدا لو انت مثلا عايز تاخد backup للسيستم بتاعك في /etc من ال directories المهمه اللي المفروض تاخد منها backup
/home	➢ اي local user اتعمله create عندي في السيستم بيت create ليه home directory باسمه تحت /home
/root	➢ ده ال home directory بتاع ال root
/run	➢ بيتقال عليها runtime data ده بيبقي stored جواه ال runtime data لكل البروسيس الشغاله عندي علي السيستم اللي هي started since the last boot
/tmp	➢ ده عباره عن public writable directory كل ال user ليها full access علي ال directory ده علشان ت create فيه اي files او directories for temp خد بالك من نقطه مهمه في /tmp ايه اللي يمنع اي user انه يدخل يعمل download او upload ل files حجمها كبير جدا وكل ده بياكل من ال file system بتاعك ف قالك في service مسئوله ان هي ت keep audit او تفضل ت audit علي /tmp وتقولك لو في اي file متعملهوش access او change او modify لمده 10 ايام هتمسحه علي طول ده علشان احافظ علي ال storage بتاعتي. ➢ هنلاقي directory تاني تحت /var اسمه tmp طب ده ايه الفرق مابينه ومابين ال /tmp هما الاتنين عباره عن public writable directory والاتنين بيستخدموا for temp بس الفرق الوحيد مابين الاتنين ان في /var/tmp لو فيه file متعملهوش access او change او modify لمده 30 يوم هيمسحه. ➢ هنلاقي تحت /usr هنلاقي directory اسمه tmp وده عباره عن shortcut بيشاور علي /var/tmp
/usr	➢ خلينا نبدأ ب /usr انا عندي كل ال commands الموجوده عندي في اللينكس بتبقي مقسومه ل two categories ➢ اول category اسمها user commands ودي اي user سواء كان super user او regular user يقدر ي run اللي commands دي وال commands دي بتبقي stored في /usr/bin/ ➢ و تاني category اسمها System Administrator Commands اللي يقدر ي run ال commands دي هو ال super user او الادمن او ال root ودي بتبقي stored في /usr/sbin/ ➢ هنلاقي تحت /usr كمان directory اسمه Local وده بيستخدم في بعض ال Customize Software اللي انت بتعملها Install ساعات بيتعملها Install تحت /usr/local
/var	➢ ده معناها variable قالك اي files بتتغيرمع الوقت بيفضل يتكتب فيها بطريقه dynamic

Type of Files in Linux

Symbol	Meaning
-	Regular file
d	Directory
l	Link
c	Special File
s	Socket
p	Named Pipe
b	Block Device

- هنتكلم عن ال types of files in linux

- ال file عباره عن collection of data انا عندي 7 انواع من ال File Type in linux
- اول نوع ال Regular File ده بيبقي زي ال text files وال images وال binary files وال Symbol بتاعته بتبقي داش –
- تاني نوع وهو ال Directory وده زي الfolder ال Symbol بتاعه d
- تالت نوع وهو ال Link وده ال shortcut وال Symbol بتاعه l
- رابع نوع وهو ال Special File وال Symbol بتاعه c
- خامس نوع وهو ال Socket وال Symbol بتاعه s
- سادس نوع وهو ال Named Pipe وال Symbol بتاعه p
- سابع نوع وهو ال Block Device وال Symbol بتاعه b

- هنشوف من ال CLI كل نوع منهم

- لو جينا عملنا في ال CLI ال command ده ls -l علشان اجيب more details عن ال files وال Directories بتاعتي

```
[root@MohamedAtef ~]# ls -l
total 4
-rw-------. 1 root root 1380 Mar  5 19:43  anaconda-ks.cfg
drwxr-xr-x. 3 root root  128 May 28 09:42 Desktop
drwxr-xr-x. 2 root root    6 Mar  9 05:54  Documents
drwxr-xr-x. 2 root root    6 Mar  9 05:54  Downloads
```

هنلاقي في اول file عندي علي الشمال خالص اول حاجه علامه الهاش - ده كده عباره عن regular file او text file

لما تلاقيها d ف ده عباره عن directory او folder

- لو جينا دخلنا مثلا تحت /dev عن طريق cd command وبعدين اعرض محتوي ال Directory عن طريق ls -l

```
[root@MohamedAtef ~]# cd /dev/
[root@MohamedAtef dev]# ls -l
crw-r--r--. 1  root   root   10, 235  Jul  7 07:05 autofs
lrwxrwxrwx. 1 root   root    3  Jul  7 07:05 cdrom -> sr0
brw-rw----. 1 root   disk   259,   7 Jul  7 07:04 nvme0n3
```

لما تلاقي في اول ال file حرف ال c ف ده معناه special file

لما تلاقي مكتوب l ف ده عباره عن shortcut او link او من شكله هتلاقي سهم بيشاور علي location تاني

لما تلاقي مكتوب b ف ده عباره عن block device وفي المثال اللي قدامنا ال block device هو الهارد درايف ونوعه nvme

Navigation Paths

pwd command

- Displays the full path name of the current working directory for that shell.

cd command

- Change your shell's current working directory. If you do not specify any arguments to the command, it will change to your home directory.

```
[user@host ~]$ pwd
/home/user
[user@host ~]$ cd Videos
[user@host Videos]$ pwd
/home/user/Videos
[user@host Videos]$ cd /home/user/Documents
[user@host Documents]$ pwd
/home/user/Documents
[user@host Documents]$ cd
[user@host ~]$ pwd
/home/user
```

- عندي command اسمه **pwd** ده بستخدمه لو انا واقف في مكان معين وعايز اعرف ال path اللي انا واقف فيه هقوله pwd زي المثال اللي في ال slide لما قولتله pwd قالي ال path اللي انا واقف فيه هو /home/user
- لو انا عايز access directory تاني او عايز change ال directory بتاعي من ال current working directory ل path تاني بستخدم command اسمه **cd** لو انا عايز ادخل جوه ال directory اللي اسمه videos هقوله cd videos هيدخلي علي ال directory اللي اسمه videos

Change Directory

- Absolute paths and Relative paths:

```
[root@RHEL9 ~]# cd /usr/share/doc
[root@RHEL9 ~]# cd /root/Desktop
[root@RHEL9 ~]# pwd
```

```
[root@RHEL9 Desktop]# cd  or cd ~
[root@RHEL9 ~]# cd ~karim
[root@RHEL9 karim]# cd –
[root@RHEL9 karim]# cd ..
[root@RHEL9 karim]# cd ../..
```

(go to the home directory)
(go to the home directory of the user Karim)
(go to the previous directory)
(up one level)
(up two levels)

- لو انا واقف في path معين وليكن في ال Desktop وعايز ارجع تاني لل home directory هستخدم **cd** او **cd** وبعدين علامه التيلد ~ يبقي ال command اللي هيستخدم هو **cd ~**
- لو انا استخدمت – cd ده هيرجعني لل directory او الدليل السابق
- لو انا واقف مثلا تحت /var/www/html/ وعايز اطلع لل parent بتاعي او ينقلني لمستوي اعلي هستخدم **cd ..** دا كده هيرجعني ل /var/www/ ول نفذت نفس ال command تاني هيرجعني ل /var/ وهكذا
- لو انا استخدمت **cd ../..** ده هينقلني مستويين اعلي يعني لو انا واقف تحت /var/www/html/ واستخدمت **cd ../..** هينقلني ل /var/ علي طول

List Files

- The **ls** command has multiple options for displaying attributes on files. The most common and useful are **-l** (long listing format), **-a** (all files, including hidden files), and **-R** (recursive, to include the contents of all subdirectories).

```
[root@RHEL9 ~]# ls
[root@RHEL9 ~]# ls -l ~          (long list)
[root@RHEL9 ~]# ls -a            (all files and directories including hidden ones)
[root@RHEL9 ~]# ls -la
[root@RHEL9 ~]# ls -lh           (human readable)
[root@RHEL9 ~]# ls -R            (Recursive)
[root@RHEL9 ~]# ls -t            (access time)
[root@RHEL9 ~]# ls -r            (reverse order)
[root@RHEL9 ~]# dir
[root@RHEL9 ~]# dir --color
```

- عندي command اسمه ls بستخدمه لو انا عايز اعمل list لل files وال Directories بتاعت ال location اللي انا واقف فيه او بتاع اي path
- فيه مجموعه من ال options اللي ممكن نستخدمها مع ال ls command
- لو انا جيت في ال CLI وقولتله ls بس هيعمل list لل files وال directory للمكان اللي انا واقف فيه
- عندي اوبشن تاني وهو ls -l وده معناه long list بيجيب معلومات اكتر عن ال files وال directories

```
[root@MohamedAtef ~]# ls
anaconda-ks.cfg  Desktop  Downloads  media  Pictures  Templates
Documents        Music    Public     Share  Videos
```

- لو عايز اعرض كل ال files وال Directories وال hidden files هستخدم **ls -a** ف هنلاقي ال files اللي

```
[root@MohamedAtef ~]# ls -l
total 4
-rw-------. 1 root root 1380 Mar  5 19:43  anaconda-ks.cfg
drwxr-xr-x. 3 root root  128 May 28 09:42 Desktop
drwxr-xr-x. 2 root root    6 Mar  9 05:54  Documents
drwxr-xr-x. 2 root root    6 Mar  9 05:54  Downloads
```

بتبدء بي دوت **.** دي بتكون عباره عن hidden file

```
[root@MohamedAtef ~]# ls -a
.                .bash_logout    .config     Documents  .lesshst   .mozilla  .tcshrc
..               .bash_profile   .cshrc      Downloads  .local     Music     Share     Templates
anaconda-ks.cfg  .bashrc         mdas        Pictures   .ssh       Videos
.bash_history    .cache          Desktop     media      Public     .targetcli  .viminfo
```

- او ممكن استخدم **ls -la** يعني اعرضلي معلومات اكتر عن كل ال files وال Directories بالاضافه لل hidden files

```
[root@MohamedAtef ~]# ls -la
dr-xr-x---. 19 root root  4096 Jul  6 15:55 .
dr-xr-xr-x. 32 root root  4096 Jun 24 10:14 ..
-rw-------.  1 root root  1380 Mar  5 19:43 anaconda-ks.cfg
```

- لو انا استخدم **ls -lt** بستخدمه لو انا عايز اعمل list بال last modify time بتاعي يعني يعرضلي من الاحدث للاقدم يعني بيعرضلي ال files وال directory اللي اتعمله create حديثا

```
[root@MohamedAtef ~]# ls -lt
drwxr-xr-x. 2 root root     6 Jun 13 21:46 virtual
-rw-r--r--. 1  root root     0 Jun 13 13:58 file3
-rw-r--r--. 1  root root     0 Jun 13 13:58 file1
```

- لو انا عايزه اعرض احدث file عندي سكون في الاخر هستخدم ls -ltr

```
[root@MohamedAtef ~]# ls -ltr
-rw-------. 1 root root 1380 Mar  5 19:43 anaconda-ks.cfg
drwxr-xr-x. 2 root root    6 Mar  9 05:54 Videos
drwxr-xr-x. 2 root root    6 Mar  9 05:54 Templates
```

- لو انا استخدمت **ls -lR** ال R هنا معناها recursive يعني هيعرضلي كل ال file وال directory بكل اللي جوه ال directory من files و subdirectories

```
[root@MohamedAtef ~]#  ls -lR
-rw-------. 1 root root 1380 Mar  5 19:43 anaconda-ks.cfg
-rw-r--r--. 1 root root    0 Jun  6 21:33 d
drwxr-xr-x. 3 root root  128 May 28 09:42 Desktop
drwxr-xr-x. 2 root root    6 Mar  9 05:54 Documents
drwxr-xr-x. 2 root root    6 Mar  9 05:54 Downloads
```

- لو عايز اخلي ال size بتاعي وانا بعمل list يكون human radiable يعني يكون بالميجا او الجيجا وهكذا هستخدم **ls -lh**

```
root@MohamedAtef ~]# ls -lh
-rw-------. 1 root root 1.4K Mar  5 19:43 anaconda-ks.cfg
-rw-r--r--. 1 root root    0 Jun  6 21:33 d
drwxr-xr-x. 3 root root  128 May 28 09:42 Desktop
drwxr-xr-x. 2 root root    6 Mar  9 05:54 Documents
drwxr-xr-x. 2 root root    6 Mar  9 05:54 Downloads
```

- فيه عندي command شبه **ls** اسمه **dir** الفرق ان ال **ls** عنده اوبشن ال color يعني لما بتستخدم ال ls بتلاقي ال files وال directory متلونين ف تعرف من خلالهم مين ال file ومين ال directory اما ال dir معندهوش الاوبشن ده ولو عايز ال dir يلون ال files وال directories هستخدم اوبشن **--color** مع ال dir

```
[root@MohamedAtef ~]# dir
anaconda-ks.cfg  Desktop   Downloads  file3  media  Pictures  Templates  virtual
 Documents  file1    Music  Public    Share       Videos

[root@MohamedAtef ~]# dir --color
anaconda-ks.cfg  Desktop   Downloads  file3  media  Pictures  Templates  virtual
Documents  file1    Music  Public    Share       Videos
```

Creating Files And Directories

Creating Files

```
[root@RHEL9 ~]# touch file1 FILE1
[root@RHEL9 ~]# touch /root/Desktop/file
[root@RHEL9 ~]# touch {file1,file2,file3,file4}
```

(case sensitive)

If the file exist, it will reset the timestamp of the file.

- علشان اعمل create ل file هتسخدم command اسمه touch عن طريق ان انا اقوله touch وبعدين اسم لا file

```
[root@MohamedAtef Desktop]# touch file1
[root@MohamedAtef Desktop]# ls
file1
```

عملنا create ل file1 وبعدين عملنا ls علشان اعرض محتوي ال directory اللي انا فيه علشان اشوف ال file اللي عملته create

- لو انا عايز اعمل create ل اكتر من file في نفس الوقت عن طريق ان انا اقوله touch وبعدين اسم ال file الاولاني وبعدين مسافه واسم ال file التاني وبعدين مسافه واسم ال file التالت وهكذا

```
[root@MohamedAtef Desktop]# touch file1 file2 file3
[root@MohamedAtef Desktop]# ls
file1  file2  file3
```

- او ممكن مابين {} احطله اسامي ال files اللي عايز اعملها create ومبين كل file والتاني احط , comma

```
[root@MohamedAtef Desktop]# touch {file1,file2,file3}
[root@MohamedAtef Desktop]# ls
file1  file2  file3
```

Creating Files And Directories

Creating Directories

```
[root@RHEL9 ~]# mkdir dir1 dir2 dir3
[root@RHEL9 ~]# mkdir -p dir4/dir5/dir6
[root@RHEL9 ~]# mkdir 'Mahara Tech'
[root@RHEL9 ~]# mkdir " Mahara Tech "
[root@RHEL9 ~]# mkdir Mahara\ Tech
```

(If dir5 not exist it will be created)

- لو انا عايز اعمل create ل directory عن طريق ال CLI هستخدم command اسمه **mkdir**

- ف علشان اعمل create ل directory هقوله **mkdir** وبعدين اديله اسم ال directory وبعدين ادوس enter ف هيتنفذ ال command وهيعملي create لل directory

```
[root@MohamedAtef Desktop]# mkdir devops
[root@MohamedAtef Desktop]# ls
devops
```

- لو انا عايز اعمل create ل اكتر من directory

```
[root@MohamedAtef Desktop]# mkdir Dir1 Dir2
[root@MohamedAtef Desktop]# ls
Dir1  Dir2
```

- لو انا عايز اعمل create ل اكتر من directory ويكونوا جوه بعض يعني عايز اعمل create ل Dir1 وجوه Dir1 اعمل create ل Dir2 وجوه Dir2 اعمل create ل Dir3 ف انا في الحاله هستخدم اوبشن -p مع ال command بالشكل ده

```
[root@MohamedAtef Desktop]# mkdir -p Dir1/Dir2/Dir3
[root@MohamedAtef Desktop]# ls
Dir1
```

- لو انا عايز اعمل create ل directory وال file name بتاع ال directory ده فيه مسافه زي مثلا Mahara Tech ف فيه مابين الكلمتين مسافه انا لو عملت touch وكتبت Mahara Tech وبعدين ضغط enter هيعملي directory باسم Mahara و directory باسم Tech

```
[root@MohamedAtef Desktop]# mkdir Mahara Tech
[root@MohamedAtef Desktop]# ls
Mahara  Tech
```

- ف علشان اعمل create ل directory باسم Mahara Tech ومابين الكلمتين مسافه هحط اسم ال directory مابين " single quotes

```
[root@MohamedAtef Desktop]# mkdir 'Mahara Tech'
[root@MohamedAtef Desktop]# ls
 Mahara  'Mahara Tech'   Tech
```

- او ممكن استخدم ال "" double quotes

```
[root@MohamedAtef Desktop]# mkdir "Mahara Tech"
[root@MohamedAtef Desktop]# ls
'Mahara Tech'
```

- لو انا عايز اخد copy من file ل file تاني هستخدم command اسمه **cp** عن طريق ان انا بقوله cp وبعدين اسم ال file اللي عايز اخد منه copy وبعدين اسم ال file الجديد
- لو انا عايز اخد copy من ال file اللي اسمه shadow الموجود تحت /etc واحطه في المكان اللي انا فيه ف علشان احددله المكان اللي انا فيه ممكن اقوله دوت .

```
[root@MohamedAtef ~]# cp /etc/shadow .
[root@MohamedAtef ~]# ls
anaconda-ks.cfg  devops   Downloads  Music   Public  Share   Videos
Desktop   Documents  media   Pictures  shadow  Templates  virtual
```

- لو انا عايز اخد copy من ال directory بالمحتوي اللي فيه هزود اوبشن **-r** عن طريق ان انا هقوله **cp -r** وبعدين اسم الdirectory اللي هاخد منه copy وبعدين اسم ال directory الجديد

```
[root@MohamedAtef backup]# cp -r /etc/ .
[root@MohamedAtef backup]# ls
etc
```

- لو انا عايز اعمل move او rename ال move معناها cut باستخدام command اسمه **mv** ان انا هقوله mv وبعدين اسم ال file وبعدين ال new file
- علشان اعمل rename لازم اكون واقف في نفس المسار اللي فيه ال file اللي هعمله rename

```
[root@MohamedAtef ~]# mv mohamed ahmed
[root@MohamedAtef ~]# ls
ahmed        backup  devops   Downloads  Music    Public  Share    Videos
anaconda-ks.cfg  Desktop  Documents  media    Pictures  shadow  Templates  virtual
```

- لو عايز اعمل cut ل file معين ل مسار تاني هقوله mv واسم ال file اللي هعمله move وبعدين المسار اللي هنقل فيه ال file وليكن انا عايز انقل ال file اللي اسمه ahmed تحت ال Directory اللي اسمه Documents

```
[root@MohamedAtef ~]# mv ahmed Documents/
```

- لو انا عايز امسح file هقوله rm وبعدين اسم ال file وانا بعمل remove هيسالني لو انا فعلا عايز امسح ال file ف انا هقوله yes علشان يسمح

```
[root@MohamedAtef ~]# rm ahmed
```

- طب لو انا عايز امسح علي طول من غير مايسالني هستخدم اوبشن f-

```
[root@MohamedAtef ~]# rm -r ahmed
```

- لو انا عايز اعمل remove ل directory بس ال directory ده فاضي هستخدم command اسمه **rmdir** وبعدين اسم ال directory اللي هعمله remove

```
[root@MohamedAtef ~]# rmdir Dir1
```

- لو انا عندي directory وجواه ملفات وانا عايز امسح ال directory ده بالمحتوي اللي جواه هقوله **rm -r** وبعدين اسم ال directory ف لما اضغط enter هيسالني لو انا عايز امسح ال directory ولا لا

```
[root@MohamedAtef ~]# rm -r shadow
```

- لو انا مش عايزه يسالني وانا بمسح اي directory هزود اوبشن **-f**

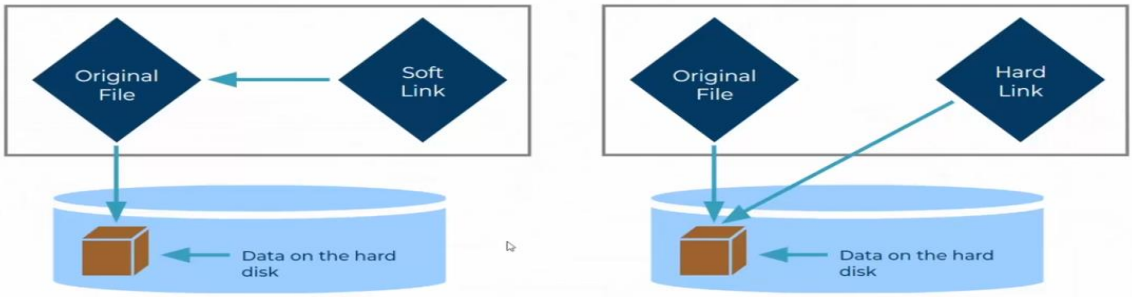
```
[root@MohamedAtef ~]# rm -rf shadow
```

- لو انا عايز امسح كل ال directories وال files بتاعت المكان اللي انا واقف فيه هقوله **rm -rf** وبعدين علامه * علامه * دي معناها في ال command انه هيمسحلك حاجه موجوده في المكان اللي انت فيه

```
[root@MohamedAtef ~]# rm -rf  *
```

Hard links and soft links

A link in Linux is a pointer to a file. Like pointers in any programming languages, links in Linux are pointers pointing to a file or a directory. Creating links is a kind of shortcuts to access a file. Links allow more than one file name to refer to the same file, elsewhere.



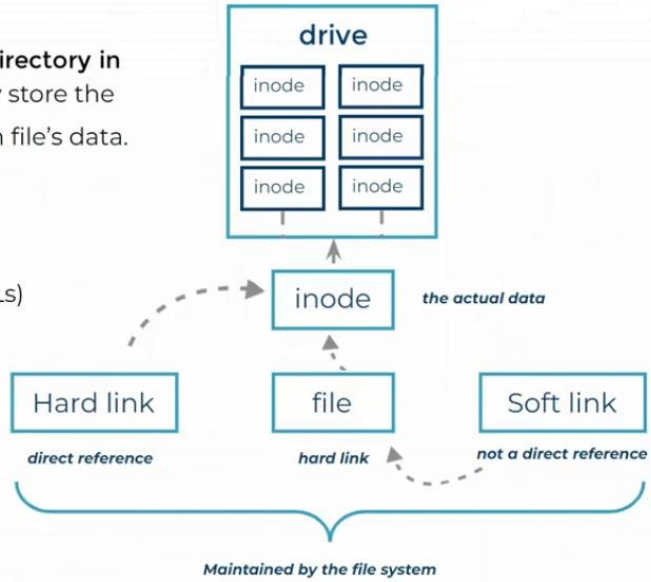
- هنتكلم عن انواع ال Link ال available عندي في اللينكس
  - مبدئيا كده ال Link عباره عن pointer بيشاور علي directory او file انا عندي نوعين من ال Link عندي نوع اسمه soft link ونوع تاني اسمه hard link
  - بالنسبه لل soft link هو عباره عن pointer او shortcut بيشاور علي ال Original File
- عندي كذا حاجه بالنسبه لل soft link او معلومه بالنسبه لل link size بتاعه هتلاقي ال size بتاعه صغير جدا مقارنتا بال size بتاع ال original file لانه مش بيشاور علي ال actual data بتاعتك الموجوده علي الهارد ديسك
- تاني معلومه لو ال original file اتمسح لاي سبب ال soft link بتاعك هتفقده
- تالت معلومه ان ال soft link ليه حاجه اسمها inode number ال inode number بتاعه مختلف عن ال inode number بتاع ال original file
  - اما بالنسبه لل hard link هتلاقيه بيشاور علي ال actual data نفسها مش بيشاور علي ال original file ف دايما هتلاقي ال hard link هو شبه بالظبط ال original file في كل حاجه لان هما الاتنين بيشاوروا علي نفس ال actual data الموجوده عندك علي الهارد درايف ف هتلاقي هما الاتنين ليهم نفس ال inode number وليهم نفس ال permissions ونفس ال size ونفس ال time stamp
- ولو انت مسحت ال original file ال hard link هيفضل شغال

Soft Link	Hard Link
Soft link is an alias to the original file similar to the shortcut feature in Windows OS.	Hard link is the exact replica of the original file it is pointing to.
It just contain the location to the original file but not the actual data.	It contains the actual content of the file.
Soft links have different Inode values pointing to the original value.	Hard links share the same Inode value pointing to the same file location.
Links can be created across filesystem.	Links cannot be created outside the filesystem.
The link becomes inaccessible when the original file is removed.	Changes in the hard linked file will reflect in the other files.
Soft links can link both to a file or a directory.	Hard links can only link to a file, not a directory.

What is inode on Linux Systems

Linux allocate an index node (inode) for every file and directory in filesystem. Inodes do not store actual data. Instead, they store the metadata where you can find the storage blocks of each file's data.

- The following metadata exists in an inode
  - File type
  - Permissions
  - Hard links count
  - Owner ID
  - Group ID
  - Size of file
  - Time stamp (access time)
  - Time stamp (modification time)
  - Soft/Hard Links
  - Access Control List (ACLs)



- خلينا نتكلم ايه هو ال inode

➢ اي file موجود عندي في اللينكس ليه حاجه اسمها inode ال inode ده عباره عن داتا بيز بيبقي stored جواها information عن ال files وال directories ماعدا حاجتين ال actual data وال file name

➢ طب ايه ال information اللي بتبقي stored جوه ال inode بيبقي stored جواه ال file type وال Permissions وال Hard links count وال Owner ID وال Group ID وال Size of file وال Time stamp وال Access Control List وال soft/hard link

Create Hard Links

- You can use the **ln** command to create a new hard link (another name) that points to an existing file.
- The following example creates a hard link named **newfile-hlink.txt** for the existing file **newfile.txt.**

```
[karim@RHEL9 ~]$ ls -li newfile.txt
163 -rw-r--r--. 1 karim karim 0 Sep 27 16:43 newfile.txt
[karim@RHEL9 ~]$
[karim@RHEL9 ~]$ ln newfile.txt newfile-hlink.txt   creates a hard link
[karim@RHEL9 ~]$
[karim@RHEL9 ~]$ ls -li newfile.txt newfile-hlink.txt
163 -rw-r--r--. 2 karim karim 0 Sep 27 16:43 newfile-hlink.txt   same inode
163 -rw-r--r--. 2 karim karim 0 Sep 27 16:43 newfile.txt
```

- علشان اعمل create ل Hard Link فيه command اسمه **ln** عن طريق ان انا هقوله ln وبعدين ال new file بتاعي اللي هو ال original file وبعدين ال link name
- ملاحظه مهمه جداااا في ال hard link ينفع اعمل hard link ل file بس مينفعش اعمل hard link ل directory
- مينفعش ان انا اعمل create ل hard link بيشاور علي file تاني في file system تاني او مكاني تاني لازم يكون في نفس المكان

- انا عندي file اسمه passwd وعايز اخد منه hard link وليكن ال hard link هسميه hard-link-passwd

```
[root@MohamedAtef Documents]# ln passwd hard-link-passwd
```

- لو عملنا ls -l هنلاحظ ان الملفين شبه بعض بالظبط مش هتعرف تفرق مابينهم هتلاقي ليهم نفس ال access time وال modification time هتلاقي الاتنين ليهم نفس ال size وليهم نفس ال ownership وليهم نفس ال permissions

```
[root@MohamedAtef Documents]# ls -l
total 8
-rw-r--r--. 2 root root 2679 Jul  7 23:58 hard-link-passwd
-rw-r--r--. 2 root root 2679 Jul  7 23:58 passwd
```

ده عدد ال hard link

ده كده ال access time وال modification time

دي ال permissions

ده ال ownership

ده ال size

- وهنلاحظ ان فيه رقم **2** اللي هو عدد ال hard link اللي اتعملها create وبتشاور علي نفس ال data اللي ال passwd بيشاور عليها
- لو جينا عملنا create ل hard link تاني ونسميه hard-link-passwd1 وبعدين نعمل list نشوف عدد ال hard link هنلاقيه بقي 3 معناه ان انا عندي 3 hard link بيشاورو علي نفس ال actual data كاني عندي نسخ من ال passwd

```
[root@MohamedAtef Documents]# ln passwd hard-link-passwd1
[root@MohamedAtef Documents]# ls -l
-rw-r--r--. 3 root root 2679 Jul  7 23:58 hard-link-passwd
-rw-r--r--. 3 root root 2679 Jul  7 23:58 hard-link-passwd1
-rw-r--r--. 3 root root 2679 Jul  7 23:58 passwd
```

- هل لو انا مسحت اي من ال hard link مش هيحصل اي حاجه عندي في باقي ال hard link
- امتي ال data بتاعتك تتمسح لو انت مسحت اخر hard link موجود عندك ساعتها ال actual data الموجوده علي الهارد درايف هتتمسح
- لو انا عايز اعرف ال inode number هستخدم ls -li

```
[root@MohamedAtef Documents]# ls -li
total 8
35437953 -rw-r--r--. 2 root root 2679 Jul  7 23:58 hard-link-passwd
35437953 -rw-r--r--. 2 root root 2679 Jul  7 23:58 passwd
```

ده كده ال inode number ولو لاحظنا هنلاقي ان الملفين ال hard link ليهم نفس ال inode number

- لو جينا نجرب اننا نعمل create ل hard link هيطلعنا error لان مينفعش اعمل hard link ل directory

```
[root@MohamedAtef Documents]# ln /etc/ hard-link2
ln: /etc/: hard link not allowed for directory
```

Creating Soft Links

- The **ln -s** command creates a soft link, which is also called a "symbolic link." A soft link is not a regular file, but a special type of file that points to an existing file or directory.
- The following example, the ln -s command is used to create a new soft link for the existing file **newfile-hlink.txt** that will be named **newfile-symlink.txt.**

```
[karim@RHEL9 ~]$ ln -s newfile-hlink.txt newfile-symlink.txt
[karim@RHEL9 ~]$
[karim@RHEL9 ~]$ ls -li newfile-hlink.txt newfile-symlink.txt
163 -rw-r--r--. 1 karim karim  0 Sep 27 16:43 newfile-hlink.txt
165 lrwxrwxrwx. 1 karim karim 17 Sep 27 17:37 newfile-symlink.txt -> newfile-hlink.txt
```

- هنشوف ازاي نعمل create ل Soft Link
- في ال soft link ينفع اعمل create ل file و directory

➢ نفس ال command اللي استخدمناه واحنا بنعمل create ل Hard Link اللي هو ln بس هنزود عليه اوبشن -s

➢ هنعمل create ل soft link للfile اللي اسمه passwd اللي استخدمناه في ال Hard Link

```
[root@MohamedAtef Documents]# ln -s passwd soft-link1
[root@MohamedAtef Documents]# ls -li
total 8
35437953 -rw-r--r--. 2 root root 2679 Jul  7 23:58 hard-link-passwd
35437953 -rw-r--r--. 2 root root 2679 Jul  7 23:58 passwd
35343358 lrwxrwxrwx. 1 root root    6 Jul  8 13:57 soft-link1 -> passwd
```

ده ال soft link هتلاقيه بيشاور علي ال file اللي اسمه passwd وهتلاقي ال size بتاعه صغيرجداا مقارنتاا بالhard link وهتلاقي ال inode number متغير وال permissions

➢ لو احنا مسحنا ال original file اللي هوال passwd هنقدر ان احنا ن access ال soft link لانه عباره عن shortcut من ال original file

```
[root@MohamedAtef Documents]# rm -f passwd
[root@MohamedAtef Documents]# ls -li
total 4
35437953 -rw-r--r--. 1 root root 2679 Jul  7 23:58 hard-link-passwd
35343358 lrwxrwxrwx. 1 root root    6 Jul  8 13:57 soft-link1 -> passwd
```

بعد اما مسحنا ال passwd اللي هو ال original file اللي واخدين منه soft link هتلاقي هنا ان شكل ال soft link اتغير بقي بالون الاحمر معناه كده ان اللينك بتاعك بقي مش موجود

Pattern Matching

PATTERN	MATCHES
*	Any string of zero or more characters.
?	Any single character.
[abc...]	Any one character in the enclosed class (between the square brackets).
[!abc...]	Any one character *not* in the enclosed class.
[^abc...]	Any one character *not* in the enclosed class.
[[:alpha:]]	Any alphabetic character.
[[:lower:]]	Any lowercase character.
[[:upper:]]	Any uppercase character.
[[:alnum:]]	Any alphabetic character or digit.
[[:punct:]]	Any printable character not a space or alphanumeric.
[[:digit:]]	Any single digit from 0 to 9.
[[:space:]]	Any single white space character. This may include tabs, newlines, carriage returns, form feeds, or spaces.

- هنتكلم عن ال Pattern Matching Features ونشوف ازاي نستخدمها علشان نقدر نrun ال commands بتاعتنا من ال CLI بطريقه efficient

- مبدئيا ال Pattern Matching او ساعات بيتقال عليها regular expression او RegEx هي طريقه انا بقدر أ match بيها باستخدام pattern معين زي اللي موجود في الجدول اللي فوق علشان اقدر أ list بيها ال files وال directories
- علشان نفهم تعال ناخد مثال انا عملت create ل مجموعه من الل files زي مواضح في المثال علشان نجرب عليها

```
[root@MohamedAtef Desktop]# ls
abc  bcd  cdf  fa  fab  fabc  file  file1  file2  file3  file4  fileab  fileb
```

- انا هنا استخدمت **ls** علشان اعمل list لكل ال files طب لو انا عايز مثلا معملش list لكل ال files الموجوده عندي غير اللي بيبدئو بحرف ال f هقوله ls هستخدم **ls f*** الاستريك * هنا معناها ان هو هيعمل search علي اي file او directory بيبدأ بحرف ال f وبينتهي بأي حاجه والحاجه دي دي ممكن تبقي zero or more characters

```
[root@MohamedAtef Desktop]# ls f*
fa  fab  fabc  file  file1  file2  file3  file4  fileab  fileb
```

- لو انا عايز اعمل List لل files اللي بتبدء بكلمه file هقوله **ls file***

```
[root@MohamedAtef Desktop]# ls file*
file  file1  file2  file3  file4  fileab  fileb
```

- طب لو انا عايز اعمل list ل اي file بيتكون من 4 حروف هستخدم ال ? Question mark هستخدمها اربع مرات ف هنلاقيه ظاهرلنا ملفين بيتكونوا من اربع حروف وهما file و fabc

```
[root@MohamedAtef Desktop]# ls ????
fabc  file
```

- طب لو انا عايز اعرض كل ال files اللي بتبدء بحرف ال f او a هتسخدم ال []

```
[root@MohamedAtef Desktop]# ls [fa]*
abc  fa  fab  fabc  file  file1  file2  file3  file4  fileab  fileb
```

- لو انا عايز اعرض كل ال files اللي مبتبدئش بحرف ال a ولا f

```
[root@MohamedAtef Desktop]# ls [!fa]*
bcd  cdf
```

- لو انا عايز اديله range يعني عايزه يعرضلي كل ال files من اول حرف a ل حرف c ف هو هييعرضلي ال files اللي بتبدء بحرف a او b او c

```
[root@MohamedAtef Desktop]# ls [a-c]*
abc  bcd  cdf
```

- لو انا عايز اقوله العكس انه ميعرضش اي files بتبدء من اول حرف ال a ل c يعني ميعرضش اي files بتبدء بحرف ال a او b او c

```
[root@MohamedAtef Desktop]# ls [^a-c]*
fa  fab  fabc  file  file1  file2  file3  file4  fileab  fileb
```

Grep command

- -i case insensitive
- -v reverse
- -r recursive
- -n number the lines
- -A3 Display 3 lines after the regular expression match.
- -B3 Display 3 lines before the regular expression match.
- -e Used for multiple search patterns

```
[karim@lab01 ~]$ grep -A3 ^cat$ /usr/share/dict/words
cat
cat.
cata-
catabaptist
[karim@lab01 ~]$ grep -B3 ^cat$ /usr/share/dict/words
Casziel
CAT
Cat
cat
[karim@lab01 ~]$
```

- ال **Grep** وظيفته انه بيعمل search ب pattern معين جوه ال file ولو لاقي اي line بي match علي ال pattern ده بي display ال line اللي فيه ال Pattern ده

- تعال مثلا نعمل grep علي كلمه Mohamed في ال file اللي اسمه passwd اللي هيعمله ال grep انه هيعمل search علي ال pattern اللي اسمه Mohamed جوه ال file اللي اسمه passwd ولو لاقا ال pattern ده هيعرضه ويلون ال pattern ده

```
[root@MohamedAtef ~]# grep mohamed /etc/passwd
mohamed:x:1004:1005::/home/mohamed:/bin/bash
```

- هنعمل grep علي كلمه bash من ال /etc/passwd هنلاحظ انه ظهرلي كل ال lines اللي فيها كلمه bash

```
[root@MohamedAtef ~]# grep bash /etc/passwd
root:x:0:0:root:/root:/bin/bash
Elbitawy:x:1000:1000:Elbitawy:/home/Elbitawy:/bin/bash
karim:x:1001:1001::/home/karim:/bin/bash
ansible:x:1002:1002::/home/ansible:/bin/bash
```

- ممكن استخدم اوبشن **-l** مع ال grep انه بدل اما يعرضلي ال lines اللي فيها ال pattern لا هو هيعرضلي ال file بمعني ان لو بعمل grep علي كلمه bash في ال /etc/passwd مش هيعرضلي ال lines زي مظهر في المثال اللي قبل ده لا هيعرضلي اسم ال file هو /etc/passwd كانه بيقولك اه موجود ال Pattern ده

```
[root@MohamedAtef ~]# grep -l bash /etc/passwd
/etc/passwd
```

- فيه اوبشن تاني ممكن استخدمه وهو **-i** بمعني case insensitive يعني بقوله اعمل search علي ال pattern سواء كان upper case او Lower case واعرضلي ال line ده
- لو انا جيت مثلا عملت grep علي كلمه ROOT وهي upper case في ال /etc/passwd مش هيعرضلي اي حاجه لان ال grep case sensitive

```
[root@MohamedAtef ~]# grep ROOT /etc/passwd
[root@MohamedAtef ~]#
```

- لو نفذت نفس ال command واستخدمت معاه اوبشن **-i** هيعرضلي كل ال Line اللي فيها upper case و lower case

```
[root@MohamedAtef ~]# grep -i ROOT /etc/passwd
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
```

- فيه اوبشن كمان وهو **-v** وده بستخدمه لو انا عايز اعرض كل ال lines ماعدا ال lines اللي فيها pattern معين

```
[root@MohamedAtef ~]# grep -v mohamed /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
```

- لو انا عايز اعمل سيرش بكلمه ذات نفسها هستخدم اوبشن **-w**

```
[root@MohamedAtef ~]# grep -w shut /etc/passwd
```

- لو انا عايز اعمل سيرش علي pattern معين وال Line اللي تلاقي فيه ال pattern ده اعرضه واعرض مثلا سطرين بعديه هستخدم اوبشن **-A** وبعدين العدد اللي انا عايز اعرضه

```
[root@MohamedAtef ~]# grep -A 2 root /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
```

- لو انا عايز اعمل العكس يعرضلي مثلا سطرين قبل ال pattern هستخدم اوبشن **-A** وبعدين عدد ال lines

```
[root@MohamedAtef ~]# grep -B 2 root /etc/passwd
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
```

- ممكن استخدم اوبشن **-r** علشان اعمل سيرش جوه ال directory بكل ال content بتاعته بال files بكل حاجه

```
[root@MohamedAtef ~]# grep -r mohamed /etc/
/etc/group:mohamed:x:1005:
/etc/gshadow:mohamed:!::
/etc/passwd:mohamed:x:1004:1005::/home/mohamed:/bin/bash
/etc/shadow:mohamed:$6$JZXFa4/ykqIK4fDK$BC2p4Cy.EWARMsQgZEKsv42I9DFQlk1cynbaHc7IBqPKymFBnt5ToY
8jHeKZ3UbvFOTXLhPRle6.uzltzxApI0:19912:0:99999:7:::
```

- ممكن اسخدم اوبشن **-lr** علشان اعرض اسامي ال files بدل اما يعرضلي ال Line اللي فيها ال pattern

```
[root@MohamedAtef ~]# grep -lr mohamed /etc/
/etc/group
/etc/gshadow
/etc/passwd
/etc/shadow
```

- لو انا عايز اعمل search ل اكتر من pattern في نفس الوقت هستخدم اوبشن **-e** مابين كلpattern

```
[root@MohamedAtef ~]# grep -e mohamed -e root /etc/passwd
root:x:0:0:root:/root:/bin/bash
operator:x:11:0:operator:/root:/sbin/nologin
mohamed:x:1004:1005::/home/mohamed:/bin/bash
```

Basic Regular Expressions

Symbol	Descriptions
.	replaces any character
^	matches start of string
$	matches end of string
*	matches up zero or more times the preceding character
\	Represent special characters
()	Groups regular expressions
?	Matches up exactly one character

- هنشوف ازاي نستخدم ال Regular Expressions مع ال Grep
- الدوت **.** بت match علي exactly one characters وبتستخدم مع ال grep command
- ال **?** Question mark بت matchعلي exactly one-character وبتستخدم مع ال ls command
- ال **^** دي بت Match علي start of string
- ال **$** dollar sign بت match علي end of string
- ال ***** معناها zero or more
- ال **** بت represent special characters
- ال **()** عباره عن Groups regular expressions

- لو انا عملت grep علي كلمه cat من ال file اللي اسمه words الموجود تحت /usr/share/dict/

```
[root@MohamedAtef ~]# grep cat /usr/share/dict/words
abacate
abboccato
abdicate
abdicated
```

ال file اللي اسمه words ده فيه تقريبا كل الكلمات الانجليزيه الموجوده عندي دا ال dictionary الموجود عندنا في اللينكس

- انا عايز أ list كل ال lines اللي بتبدء بكلمه cat او بال pattern ده هستخدم ال ^ في اول ال pattern

```
[root@MohamedAtef ~]# grep ^cat /usr/share/dict/words
cat
cat.
cata-
catabaptist
```

- لو انا عايز العكس ان انا أ list كل ال lines اللي بتنتهي بكلمه cat هستخدم $ في اخر ال pattern

```
[root@MohamedAtef ~]# grep cat$ /usr/share/dict/words
avocat
bearcat
blindcat
```

- طب لو انا عايز أ List كل ال lines اللي بتبدء بكلمه cat وبتنهي بكلمه cat ف انا هستخدم ال ^ في اول ال pattern وال $ في نهايه ال pattern

```
[root@MohamedAtef ~]# grep ^cat$ /usr/share/dict/words
cat
```

- ممكن استخدم الدوت . مع ال grep زي مثلا

```
[root@MohamedAtef ~]# grep c.t /usr/share/dict/words
abacate
abacot
abboccato
```

هنا عمل search علي اي line بي match علي ال pattern اللي انا مدهوله وهو c.t ان ال line ده يكون فيه حرف c والحرف التالت t والحرف التاني اول اللي في النص فيه اي حرف تاني

- ممكن اعمل search علي اي حاجه بتبدء ب c وبتنتهي ب t وفي النص a اوo او u

```
[root@MohamedAtef ~]# grep ^c[aou]t$ /usr/share/dict/words
cat
cot
cut
```

- ودي كده بعض الامثله الاضافيه

Grep and Regular Expressions

- used to parse out and or query files for data.

```
[karim@RHEL9 ~]$ grep cat /usr/share/dict/words
[karim@RHEL9 ~]$ grep ^cat /usr/share/dict/words
[karim@RHEL9 ~]$ grep cat$ /usr/share/dict/words
[karim@RHEL9 ~]$ grep ^cat$ /usr/share/dict/words
[karim@RHEL9 ~]$ grep c.t /usr/share/dict/words
[karim@RHEL9 ~]$ grep ^c.t$ /usr/share/dict/words
[karim@RHEL9 ~]$ grep c[aou]t /usr/share/dict/words
[karim@RHEL9 ~]$ grep ^c[aou]t$ /usr/share/dict/words
[karim@RHEL9 ~]$ grep -e cat -e tele /usr/share/dict/words
[karim@RHEL9 ~]$ grep -l ericsson /etc/passwd
[karim@RHEL9 ~]$ ps aux | grep ^root
```

Cut command

- Used for cutting out the sections from each line of files and writing the result to standard output.

```
[karim@RHEL9 ~]$ cut -f 1 -d : /etc/passwd
[karim@RHEL9 ~]$ cut -c 1-7 /etc/passwd
[karim@RHEL9 ~]$ cut -c 25- /etc/passwd
```

- بستخدم cut command لو انا عايز اعمل cut ل column معين او field معين جوه ال file

➢ لو فتحنا مثلا /etc/passwd هنلاقيه file موجود فيه معلومات عن كل ال users اللي اتعملها create عندي

```
[root@MohamedAtef ~]#  cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
```

استخدمت cut command علشان اعرض محتوي ال file ودي بعض من محتوي ال file

بيكون مابين كل filed والتاني : colon

➢ لو انا مش عايز أ display اللي content بتاعت ال file كله انا عايز بس ال column الاولاني او ال field الاولاني ف بقوله cut وبعدين احددله ال separator او ال delimiter بتاع ال file عن طريق اني اقوله d- وبعدين : colon وبعدين احددله الfiled number اللي انا هعمله list عن طريق اني اقوله f-

```
[root@MohamedAtef ~]# cut -d : -f 1 /etc/passwd
root
bin
daemon
adm
lp
```

➢ انا مثلا عايز اعرض اول خمس حروف هستخدم اوبشن c- مع ال cut واحددله عدد الحروف اللي انا عايز اعرضهم كاني بقوله اقطع اول خمس حروف من ال file اللي اسمه passwd

```
[root@MohamedAtef ~]# cut -c 1-5 /etc/passwd
root:
bin:x
daemo
adm:x
lp:x:
```

➢ لو انا عايزه مثلا يعرضلي من اول ال character رقم 5 ل اخر ال file هقوله 5 وبعدين داش-

```
[root@MohamedAtef ~]# cut -c 5- /etc/passwd
:x:0:0:root:/root:/bin/bash
x:1:1:bin:/bin:/sbin/nologin
on:x:2:2:daemon:/sbin:/sbin/nologin
x:3:4:adm:/var/adm:/sbin/nologin
:4:7:lp:/var/spool/lpd:/sbin/nologin
```

tr command

- Utility for translating or deleting characters. It supports a range of transformations including uppercase to lowercase

```
[karim@RHEL9 ~]$ echo hello world | tr a-z A-Z
[karim@RHEL9 ~]$ echo hello world | tr [a-z] [A-Z]
[karim@RHEL9 ~]$ echo hello world | tr [:lower:] [:upper:]
[karim@RHEL9 ~]$ echo "Welcome To Linux" | tr [:space:] '\t'
[karim@RHEL9 ~]$ echo "Welcome To Linux" | tr -d 'W'
[karim@RHEL9 ~]$ echo "my ID is 73535" | tr -d [:digit:]
```

- ال tr عباره عن command او utility بستخدمها لو انا عايز أ translate text او string من صوره ل اخر من upper case ل lower case او العكس او لو عندي multi spaces وانا عايز امسح ال spaces دي وهكذا

- في عندي command اسمه echo ال command ده بستخدمه لو انا عايز أ display اي string علي ال CLI
- هستخدم echo علشان اعرض جمله Hello World!

```
[root@MohamedAtef ~]# echo Hello World!
Hello World!
```

- لو انا عايز احول Hello World! من lower case ل Upper case هستخدم

```
[root@MohamedAtef ~]#  echo Hello World! | tr a-z A-Z
HELLO WORLD!
```

- لو عايز اعمل العكس احول من Upper case ل lower case هستخدم

```
[root@MohamedAtef ~]#  echo Hello World! | tr A-Z a-z
hello world!
```

- لو انا عندي مثلا space وعايزه يشيل ال space دي ويعمل مكانها tab يعني هيشيل ال space الواحده وهيحط مكانها tab وال tab هنا بتحتوي علي 8 Space

```
[root@MohamedAtef ~]#  echo Hello World! | tr [:space:] '\t'
Hello           World!
```

- لو انا عايز اعمل remove لحرف معين مثلا هستخدم اوبشن -d معناها delete

```
[root@MohamedAtef ~]# echo "Hello World" | tr -d 'l'
Heo Word
```

- لو انا عندي digit مثلا وعايزه يعمل remove لل digit دي

```
[root@MohamedAtef ~]# echo "My ID Number Is 19980704" | tr -d [:digit:]
My ID Number Is
```

Chapter 4

Getting Help in Red Hat Enterprise

Reading manual pages

- One source of documentation that is generally available on the local system are system manual pages or man pages These pages are shipped as part of the software packages for which they provide documentation, and can be accessed from the command line by using the man command.

Common Sections of the Linux Manual

SECTION	CONTENT TYPE
1	User commands *(both executable and shell programs)*
2	System calls *(kernel routines invoked from user space)*
3	Library functions *(provided by program libraries)*
4	Special files *(such as device files)*
5	File formats *(for many configuration files and structures)*
6	Games *(historical section for amusing programs)*
7	Conventions, standards, and miscellaneous *(protocols, file systems)*
8	System administration and privileged commands *(maintenance tasks)*
9	Linux kernel API *(internal kernel calls)*

- انا عندي اي command installed عندي في اللينكس هو by default بيبقي جاي معاه Manual Pages بتبقي هي ال full documentations او install فيها information عن ال command ده زي مثلا هتلاقي ال name بتاع ال command ال Syntax وDescription عنه وايه هي ال Available Options اللي ال command ده بيدعمها ولو فيه مثلا Examples ساعات بيبقي حاطط جوه ال man pages امثله عن ازاي تستخدم ال command
- ف هتلاقي دايما في الManual Pages حاططلك كل ال information اللي انت محتاجها لان ببساطه انت ك سيستم ادمن بتتعامل مع اللينكس كل يوم ف انت عندك مجموعه كبيره جدا من ال commands وكل command هتلاقي فيه options كتير جدا ف انت بيبقي صعب ان انت تبقي ملم بكل ال options بتاعت اي command او تبقي حافظ كل command بكل ال Options بتاعتها ف دايما احنا ك سيستم ادمن بنتعامل كتير مع ال man
- انا عندي الManual pages مقسومه لمجموعه من ال sections كل section فيهم بيبقي stored فيه Manual pages بتاعت حاجه معينه . احنا عادتا ك سيستم ادمن بنتعامل مع three options او four بالكتير هنتعامل مع ال section الاولاني وده بيبقي فيه ال Manual pages بتاعت ال User Commands وهنتعامل مع ال section الخامس وده بيبقي فيه ال Manual pages بتاعت اي configuration file موجوده عندك في السيستم وهنتعامل مع ال section التامن وده بيبقي فيه الSystem Administration Commands وممكن نستخدم ال section الرابع وده بيبقي فيه ال Special File

Reading manual pages getting

```
[karim@RHEL9 ~]$ man mkdir
[karim@RHEL9 ~]$ man -K passwd
[karim@RHEL9 ~]$ man 1 passwd
[karim@RHEL9 ~]$ man 5 passwd
```

- All man pages are located in **/usr/share/man**. Locate the binary, source, and manual pages located in the /usr/share/man directory by using the **whereis** command.

- كل ال manual pages الموجوده عندي بتبقي stored في السيستم تحت /usr/share/man

- انا علشان أ display ال manual pages بتاعت اي command بستخدم command اسمه man عن طريق اني اقوله man وبعدين اسم ال command

```
[root@MohamedAtef ~]# man passwd
```

- لو انا عايز احددله section معين يروح يدور فيه عن طريق اني بقوله **man** وبعدين رقم ال section اللي انا عايزه يعرضه وبعدين اسم ال file

```
[root@MohamedAtef ~]# man 5 passwd
```

- لو انا عايز اعمل search ب pattern معين هقوله man وبعدين اقوله اوبشن **-K** وبعدين احددله ال pattern اللي عايزه يعمل search عليه

```
[root@MohamedAtef ~]# man -K print
```

- فيه command احنا استخدمناه قبل كده وهو **which** وده بنستخدمه علشان نعرف بيه ال command معمول ليه stored فين

```
[root@MohamedAtef ~]# which passwd
/usr/bin/passwd
```

Reading manual pages getting

```
[karim@RHEL9 ~]$ whereis passwd
passwd: /usr/bin/passwd /etc/passwd /usr/share/man/man5/passwd.5.gz
/usr/share/man/man1/passwd.1ossl.gz /usr/share/man/man1/passwd.1.gz
```

- The --help Option
- Built in the command itself (if supported)

```
[karim@RHEL9 ~]$ who --help
```

- لو انا عايز أ Display ال manual pages معمول ليها stored فين بتاعت file او command معين فيه command اسمه **whereis**

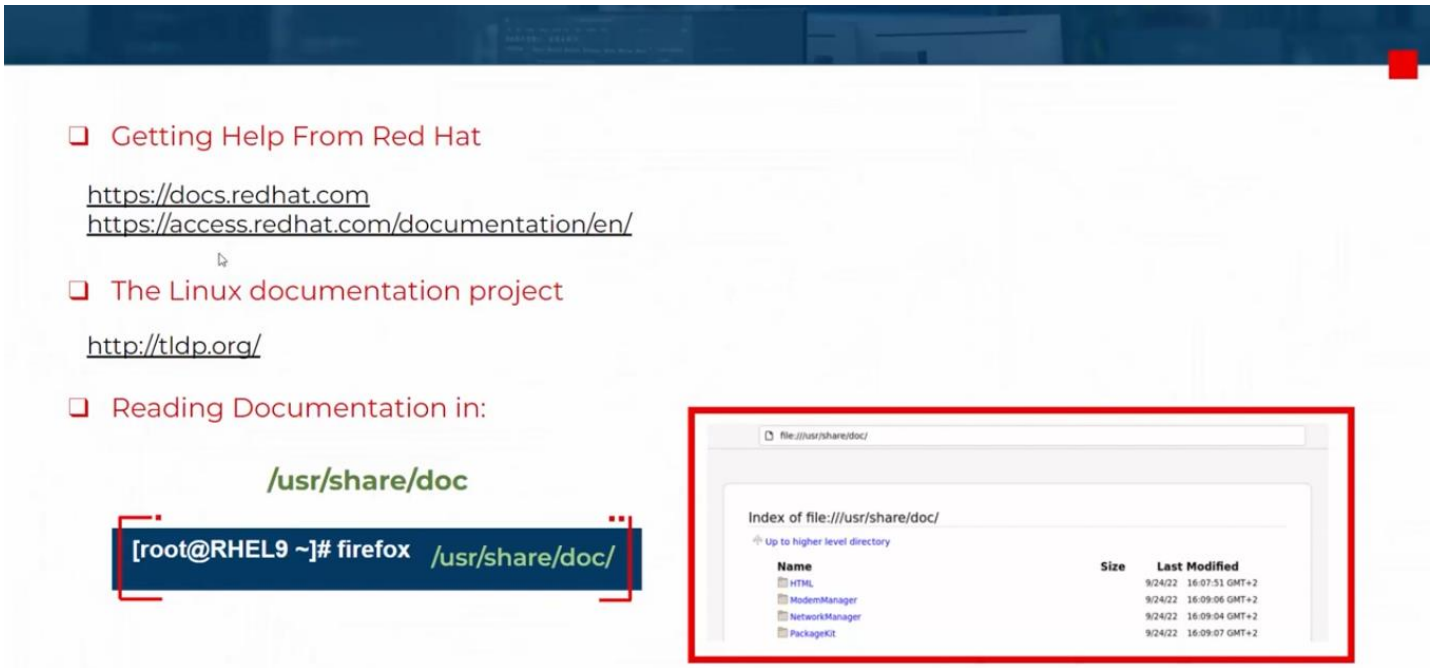
```
[root@MohamedAtef ~]#  whereis passwd
passwd: /usr/bin/passwd /etc/passwd /usr/share/man/man5/passwd.5.gz /usr/share/man/man1/passwd.1ossl.gz
/usr/share/man/man1/passwd.1.gz
```

- لو انا عايز أ List ال basic options ان انا مش عايز ال full documentation بتاعت ال man انا عايز option سريع جدا ف هسنستخدم **--help**

```
[root@MohamedAtef ~]# passwd --help
```

- لو دخلت تحت ال /usr/share/man هتلاقي كل ال Manual pages

```
[root@MohamedAtef ~]# cd /usr/share/man/
[root@MohamedAtef man]# ls
ca  de  hu  ja   man1  man2  man3p man4x man6  man7x man9  nl     pt    sk  tr   zh_TW
cs  es  id  ko   man1p man2x man3x man5  man6x man8  man9x overrides pt_BR sr  uk
da  fr  it  man0p man1x man3  man4  man5x man7  man8x mann  pl     ru    sv  zh_CN
```

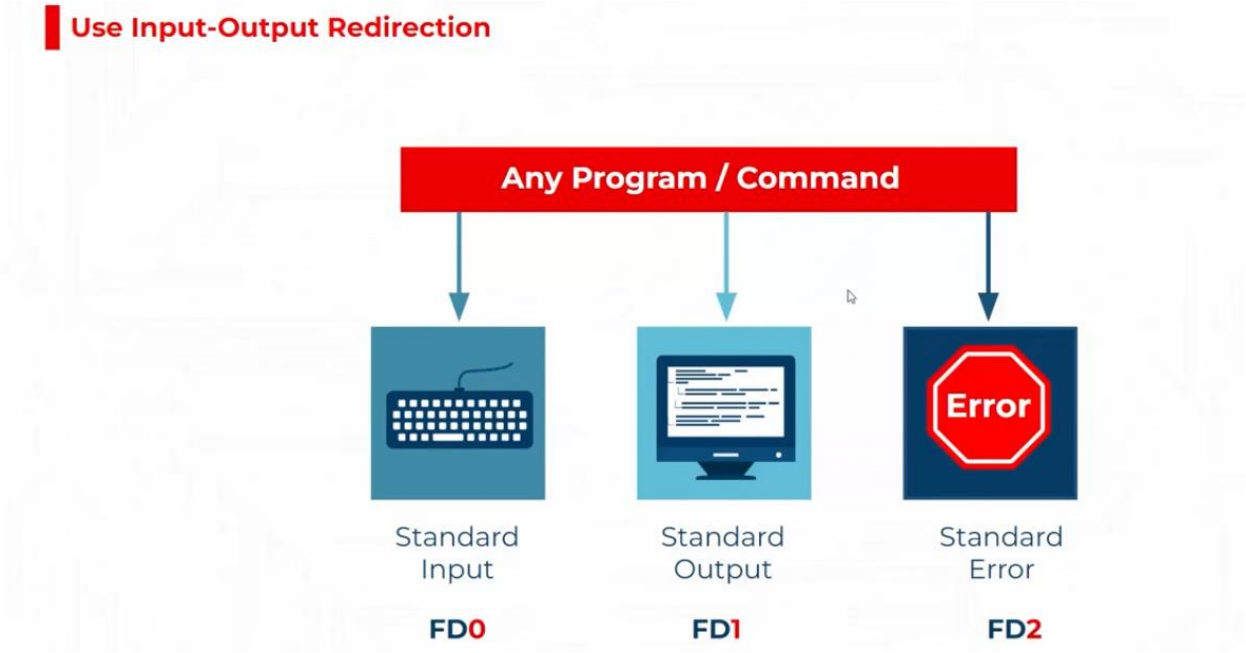


- لو انا في ال Manual pages الموجوده في ال CLI ملقتش الحاجه اللي انت عايزها في ال man ولا عن طريق اوبشن help-- ف في الحاله دي انت ممكن تلجئ ل اي online documentation هتلاقي ال documentation بتاعت ريدهات موجوده علي الويب سايت بتاعهم
- عندنا تحت /usr/share/doc فيه شويه documentations وفيها معلومات اكتر من ال man وبنفتحها عن طريق ال Firefox ممكن استخدم ال cli ان انا افتح ال Firefox وافتح ال documentations

```
[root@MohamedAtef ~]#  firefox /usr/share/doc
```

Chapter 5

Creating, Viewing, and Editing Text Files



- هنتكلم عن ال Input-Output Redirection

➢ انا عندي اي command في اللينكس هو normally بي read ال Inputs بتاعته عن طريق الكيبورد وبي Display ال output عن طريق ال Terminal window او الاسكرين بتاعتك

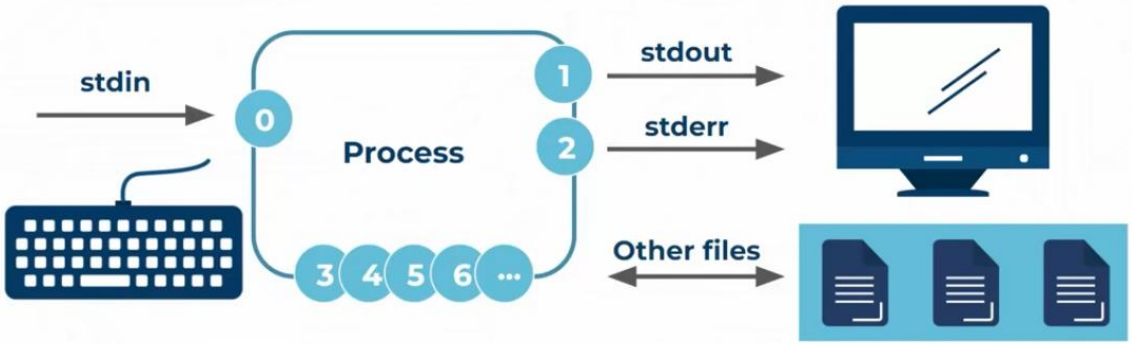
➢ انا عندي في اللينكس حاجه اسمها Standard Input وده بيكون by default ال keyboard وده في الاخر ال command هي expect ال inputs بتاعته عن طريق الكيبورد وال command ه send ال output بتاعه by default لحاجه اسمها Standard Output او ال Terminal Window للاسكرين بتاعتي

➢ وعندي حاجه اسمها Standard Error وده مثلا لو ال command بتاعك failed ل اي سبب او طلع error في الاخر ال error ده ها display علي ال Terminal Window او علي الاسكرين

➢ فيه حاجه اسمها Chanel number او file Descriptor لكل نوع من ال Standard زي مثلا ال Standard Input ليه file descriptor اسمه **FD0** وال Standard Output ليه file descriptor اسمه **FD1** وال Standard Error ليه file descriptor اسمه **FD3**

What is Redirection?

- A feature in Linux such that when executing a command, you can change the standard input/output devices.



- ال Redirection عباره عن feature في اللينكس بستخدمها علشان خاطر أredirect ال output بتاع اي command وأ save ال output ده في file معين

➢ لو انا نفذت ال command ده اللي هو **ls -l** ف طبيعي انه هيعرضلي ال output علي الاسكرين او ال Terminal زي مظاهر كده

```
[root@MohamedAtef ~]# ls -l
-rw-------. 1 root root 1380 Mar  5 19:43 anaconda-ks.cfg
drwxr-xr-x. 3 root root   17 Jul  7 21:48 backup
drwxr-xr-x. 2 root root  163 Jul  8 15:30 Desktop
drwxr-xr-x. 2 root root    6 Jul  7 14:24  devops
drwxr-xr-x. 2 root root   48 Jul  8 14:07 Documents
```

➢ طب لو انا عايز اعمل redirect لل output ده بدل اما يطلعلي علي الاسكرين هعملsave لل output ده في file معين هقوله **ls -l** وبعدين علامه الاكبر من **>** وبعدين احددله ال file

```
[root@MohamedAtef ~]# ls -l > /tmp/temp.txt
```

انا عملت redirect لل output بتاع ls -l بدل اما يعرضه علي الاسكرين لا هيعمله save في file اسمه temp.txt تحت/tmp

➢ لو جينا دلوقتي عملنا cat لل temp.txt هنلاقيه عمل save لل output في ال file

```
root@MohamedAtef ~]#  cat /tmp/temp.txt
-rw-------. 1 root root 1380 Mar  5 19:43 anaconda-ks.cfg
drwxr-xr-x. 3 root root   17 Jul  7 21:48 backup
drwxr-xr-x. 2 root root  163 Jul  8 15:30 Desktop
drwxr-xr-x. 2 root root    6 Jul  7 14:24 devops
drwxr-xr-x. 2 root root   48 Jul  8 14:07 Documents
```

➢ مثال تاني فيه عندي command اسمه date ال command ده بيعرضلي التاريخ والوقت لو انا مش عايزه يعرضلي ال output علي الاسكرين هستخدم علامه اكبر من وبعدين اسم ال file

```
[root@MohamedAtef ~]# date > date.txt
```

➢ لو عملنا cat لل date.txt هنلاقي ال output معمول ليه save في ال file

```
[root@MohamedAtef ~]# cat date.txt
Wed Jul 10 02:09:30 PM EET 2024
```

- لو انا عايز اعمل append علي file معين بمعني لو انا عندي file عليه داتا وانا عايز اعمل redirect بس ميمسحش الداتا اللي علي ال file ويبدلها بالداتا الجديده هستخدم علامه اكبر من مرتين علشان اعمل append

```
[root@MohamedAtef ~]# cal >> date.txt
[root@MohamedAtef ~]# cat date.txt
Wed Jul 10 02:09:30 PM EET 2024
     July 2024
Su Mo Tu We Th Fr Sa
   1  2  3  4  5  6
 7  8  9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30 31
```

- لو احنا عملنا run ل اي Command مش موجود هيطلعلك error

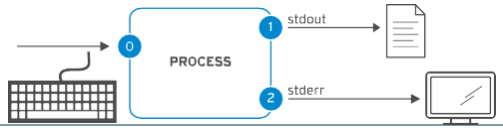
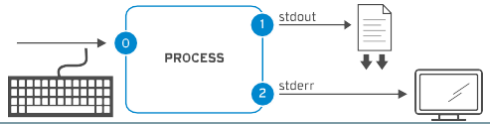
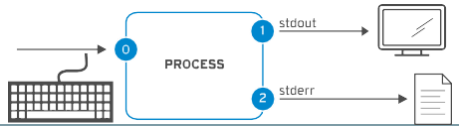
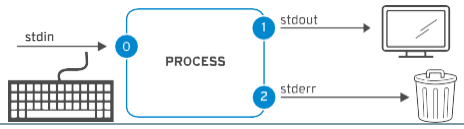
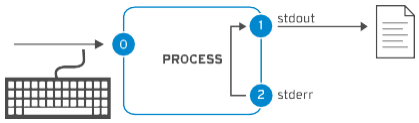
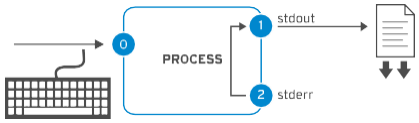
```
[root@MohamedAtef ~]# saddasd
bash: saddasd: command not found...
Failed to search for file: /media/BaseOS/ was not found
```

- لو انا اعايز عمل save لل standard error ل file معين بدل اما يظهرلي علي الاسكرين هستخدم 2> بيعمل redirect لل output في ال file اللي انا عايز احفظ ال error ده فيه

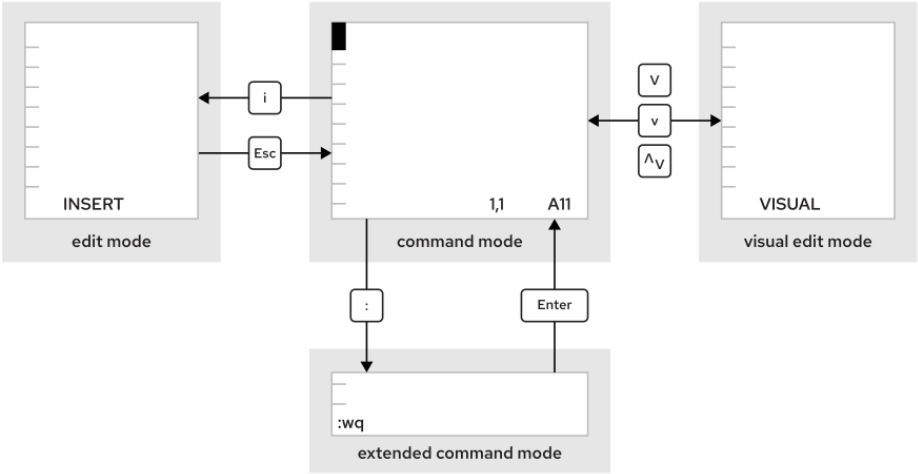
```
[root@MohamedAtef ~]# saddasd 2> error.txt
```

- ولو انا عايز اعمل append علي ال Standard error هستخدم 2>>

```
[root@MohamedAtef ~]# saddasd 2>>  error.txt
```

Usage	Explanation	Visual aid
> file	Redirect `stdout` to overwritea file.	
>> file	Redirect `stdout` to appendto a file.	
2> file	Redirect `stderr` to overwritea file.	
2> /dev/null	Discard `stderr` error messages by redirectingthem to `/dev/null`.	
> file 2>&1 ***&> file***	Redirect `stdout` and `stderr` to overwrite the same file.	
>> file 2>&1 ***&>> file***	Redirect `stdout` and `stderr` to append to the same file.	

Create and edit text files with vim



- هنشوف ازاي نستخدم ال vim في اني اعمل Create او Edit لل text files
- اول اما تفتحت اي File بال vim علشان تعمل Edit فيه بيكون موجود four modes

- اول اما تفتحت ال file بتكون في اول mode وهو ال Command Mode وده بيكون ال Default Mode وده بيسمحلي ان انا اقرء الملف او انا اخد Copy من Line او اكتر من Line او ان انا عامل cut او اني اعمل Search
- وتاني Mode اسمه Insert Mode وده بنستخدمه علشان ن Edit بيه اي Text معين وتالت Mode وهو ال Visual Mode
- ورابع Mode اسمه Extended Mode كل Mode من دول فيه شويه Commands و Features تقدر تستخدمها في اي Mode

- لو انا دلوقتي عايز اعمل switch مابين ال Mode وبعضها وليكن انا في ال Command Mode وعايز اروح ل ال Visual Mode فيه كذا طريقه ي اما استخدم V وتكون Upper Case ي اما استخدم v وتكون Lower Case ي اما استخدم Ctrl+v
- لو انا عايز ادخل علي ال Insert Mode هضغط علي i
- هتلاقي في نهايه ال File اسم ال Mode اللي انت شغال عليه
- لو انا فتحت ال File وعمل Edit فيه وعايز اعمل Save لل File لازم ادخل علي ال Extended Mode عن طريق ان انا اضغط علي : colon وبعدين اكتب wq واضغط Enter

Command Mode in Vim

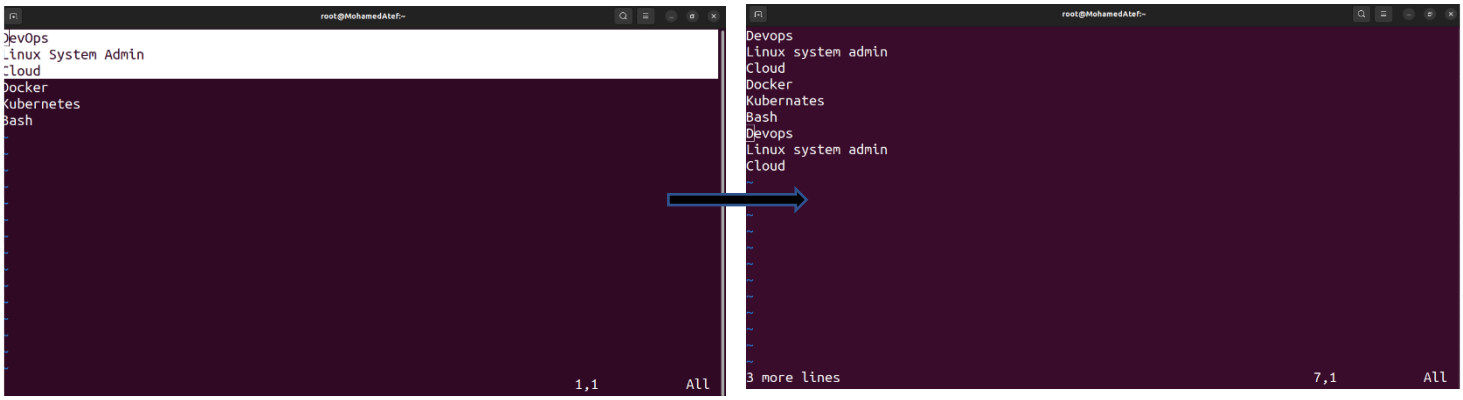
- By default, Vim starts in “command” mode.
- Command mode can be accessed from other modes by pressing Esc.

yy →	Copy a line.
3yy →	Copy three lines.
dd →	Cut a line
p →	Paste after the current cursor.
P →	Paste before the current cursor.(Upper case)
/ →	To search forward
? →	To search backward
n →	Find the next match
N →	Find the previous match

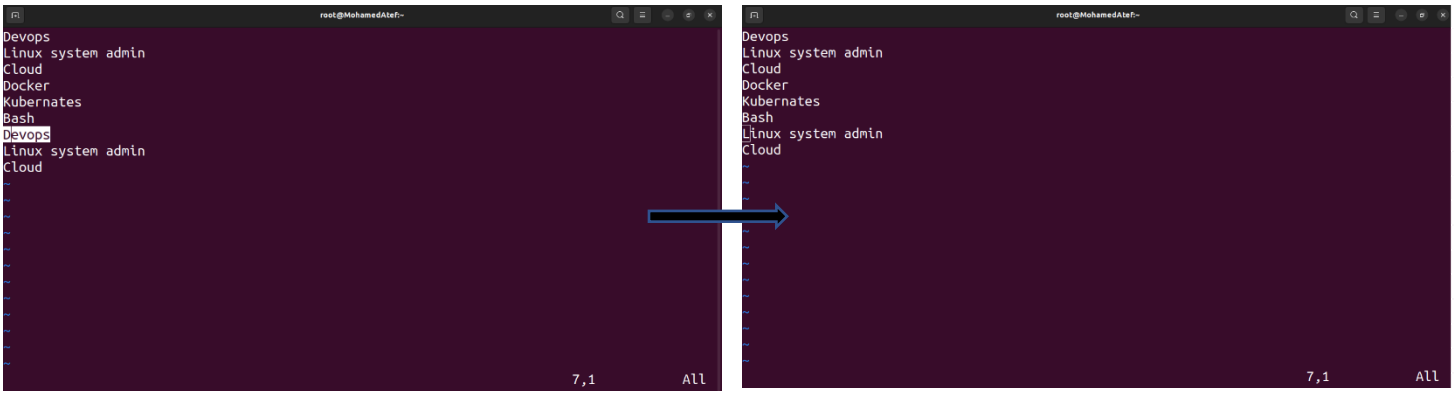
- ممكن وانا في ال Command Mode اعمل Copy او Delete او Cut او Past او Search او jump
  - ده شكل ال vim editor وموجود فيه ال Content دي

```
root@MohamedAtef:~
DevOps
Linux System Admin
Cloud
Docker
Kubernetes
Bash
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
                                                    6,4           All
```

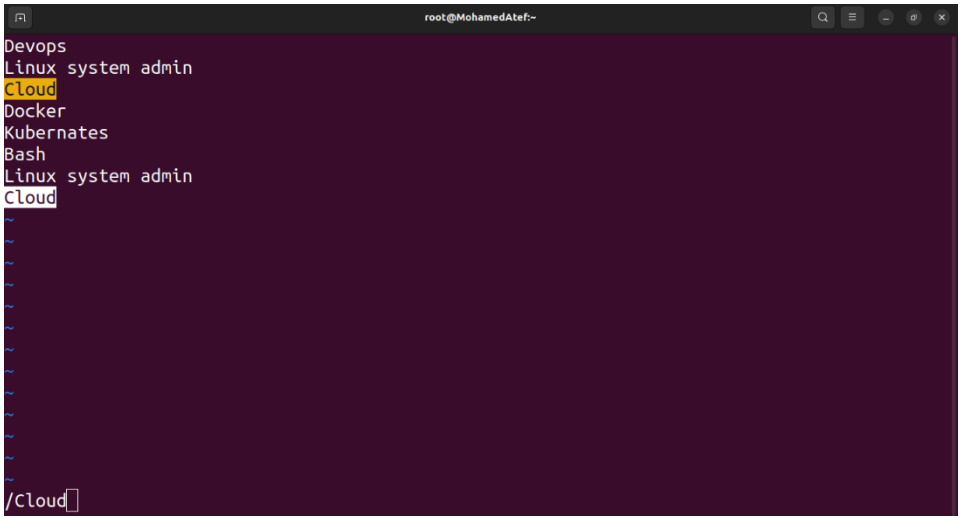
- لو انا عايز اعمل Copy ل اول Line هقوله yy ولو عايز اعمله Past فيه عندي طريقتين اول طريقه اني استخدم p وتكون lowercase وده هيعملي Copy تحت ال Line اللي انا واقف عليه وتاني طريقه اني استخدم P وتكون Upper Case وده هيعملي Copy فوق ال Line اللي انا واقف عليه
- لو انا عايز اعمل Copy ل Three Lines مع بعض هقوله رقم 3 واضغط علي yy واعملهم Past باستخدام p



- لو انا عايز اعمل Delete او Cut ل Line معين هقوله dd وليكن مثلا هعمل Delete لل Line المكتوب فيه Devops هقف علي ال Line وهضغط علي dd



- لو عايز اعمل Search علي Pattern معين وانا جوه ال File بدوس علي علامه Forward slash(\) وبعدين اكتب الكلمه اللي انا عايز اعمل Search عليها وليكن مثلا هعمل Search علي كلمه Cloud ف انا هكتب /Cloud وهو هيحددلي كل ال Lines اللي فيها الكلمه دي . ولو انت عايز تروح علي ال Next Match تاني كلمه او اتنقل مابين الكلام اللي متحدد هضغط علي n لو انا عايز ارجع ل ورا هضغط علي N وتكون Upper Case



Insert Mode in Vim

- In insert mode you can inserts characters just like a regular text editor.
- You can enter it by using an insert command from normal mode.

- **i** → insert (switches vim to insert mode)
- **a** → append (moves the cursor after the current character and enters insert mode)
- **I** → (moves the cursor to **the beginning** of the line and enters insert mode)
- **A** → (moves the cursor to **the end** of the line and enters insert mode)
- **o** → (inserts a new line **below** the current line and enters insert mode on the new line)
- **O** → (inserts a new line **above** the current one and enters insert mode on the new line)

- علشان ادخل في ال Insert Mode عندي اكتر من طريقه

- لو ضغط علي **i** هيدخلني علي ال Insert Mode بس لما اجي اكتب هكتب قبل ال Cursor
- لو ضغط علي **a** هيدخلني علي ال Insert Mode بس لما اجي اكتب هكتب بعد ال Cursor
- لو ضغط علي **A** هيدخلني علي ال Insert Mode وهينقل ال Cursor ل نهايه ال Line اللي انا واقف فيه
- لو ضغط علي **I** هيدخلني علي ال Insert Mode وهينقل ال Cursor لبدايه ال Line اللي انا واقف فيه
- لو ضغط علي **o** هيدخلني علي ال Insert Mode بس هيعملي New Line تحت ال Line اللي انا واقف فيه
- لو ضغط علي **O** هيدخلني علي ال Insert Mode بس هيعملي New Line فوق ال Line اللي انا واقف فيه

Extended Mode in Vim

- Saving files

- **:wq** → Save and quit the current file.
- **:x** → Save the current file if there are unsaved changes, then quit.
- **:w** → Save the current file and remain in editor.
- **:q** → Quit the current file (only if there are no unsaved changes).
- **:q!** → Quit the current file, ignoring any unsaved changes.
- **:10** → Jump to line number 10.

- في ال Extended Mode اقدر ان انا اعمل Save او اخرج من ال File او اعمل Jump
- لو انت في اي Mode وعايز ترجع لل Command Mode اضغط علي ال **Esc**
- لو انا عملت Edit في ال File وخلصت كل حاجه انا محتاجها وعايز احفظ اللي انا عملته واخرج هعمل save و quit هضغط علي **:wq** او **:x**
- لو انا عايز اعمل Save وافضل في ال editor بتاعي ميعملش quit يعمل save بس هتضغط علي **:w**
- لو انا عايز اخرج من غير ماعمل Save هضغط علي **:q**
- لو انا عملت اي تعديل في ال file وعايز اخرج من غير حفظ هضغط علي **:q!**

- لو انت عايز تروح ل Line معين وليكن عايز تروح لل Line رقم 10 هتقوله **:10**
- لو انت واقف عند بدايه ال Line وعايز ت jump ل نهايه ال file هتضغط علي **Shift+g** ولو انت عايز ترجع تاني ل بدايه ال File هتضغط علي g مرتين **gg** وتكون Lower Case
- علشان اعمل Search ل Pattern معين و اعمل replace لل Old Pattern ب New Pattern في نفس الوقت هستخدم **:%s/oldPattern/newPattern/g** ال s معناها Substitute وال g معناها global ان اي old pattern هتلاقيه في ا لfile اعمله replace لل new login
- لو انت جوه ال Text Editor لو انت فاتح ال File وعايز تنفذ command معين هستخدم **:!** وبعدين ال Command اللي انا عايز انفذه زي مثلا **:!date** ف هو هيخرج بره الملف ينفذلك ال command علي الاسكرين وبعدين لو عايز ترجع لل Text editor تاني هتضغط Enter
- لو انت عايز تنفذ ال Command جوه ال Text Editor هستخدم **:.!** وبعدين ال Command اللي انا عايز انفذه زي مثلا **:.!date** وهو هينفذلك ال command ده في نفس المكان اللي موجود فيه ال Cursor
- لو انا عايز انفذ ال command في line معين بمعني لو انا عايز انفذ ال Command في ال Line رقم 37 هستخدم **:37!date**
- لو انا عايز اعرف ال Available Options الموجود هستخدم **:set** وبعدين باستخدام الاسهم اقدر اشوف كل ال Options بالترتيب
- فيه اوبشن ممكن استخدمه مع set وهو number وهيكون بالطريقه دي **:set number** والاوبشن ده بيرقم ال Lines الموجوده في ال Text Editor
- لو انا عايز الغي ترقيم ال Lines هستخدم **:set nonumber** اي option عايز الغيه هسخدم **no** مع الاوبشن

Visual Mode in Vim

The visually identified text can be deleted, copied, changed, or modified with any other Vim editing command.

- Press **d** key to delete the text.
- Press **y** to copy the task.
- Press **p** to paste the text.
- Press **u** to undo and start again.
- Press **c** to change the highlighted text. The highlighted text will disappear, and you will be in Insert mode where you can add new text
- There are 3 keystrokes:
  - **Character mode: v** → **VISUAL** will appear at the bottom of the screen.
  - **Line mode: Shift+V** → **VISUAL LINE** will appear at the bottom of the screen.
  - **Block mode: Ctrl+V** → **VISUAL BLOCK** will appear at the bottom of the screen.

- بنستخدم ال Visual Mode في حاله لو احنا عايزين نعمل Highlight ل Text معين او ان احنا نعمل Delete او Copy او Move لل Text ده
- لو انا في ال Command Mode وعايز اروح لل Visual Mode في عندي اكتر من طريقه اول طريقه اني اضغط علي حرف ال **v** وده بيخليني ان اعمل Highlight علي ال characters اللي انا عايزها .تاني طريقه اني اضغط علي **Shift+V** وده بيدخلني علي ال Visual Line وده بيخليني اعمل Highlight علي ال Lines نفسها .وتالت طريقه اني اضغط علي **Ctrl+V** وده بيدخلي علي ال Visual Block لو انا عايز اعمل Highlight علي Block معين

Assigning Values to Variables

- Assign a value to a shell variable using the following syntax:

```
VARIABLENAME=value
```

- Variable names can contain uppercase or lowercase letters, digits, and the underscore character (_).
- For example, the following commands set shell variables:

```
[user@host ~]$ COUNT=40
[user@host ~]$ first_name=John
[user@host ~]$ file1=/tmp/abc
[user@host ~]$ _ID=RH124
```

- انا عندي نوعين من ال Variables في اللينكس عندي نوع اسمه User Defined Variables والنوع التاني اسمه Shell Variables
- بالنسبه لل User Defined Variables وده بالظبط زي اي لغه برمجه لما بتعرف Variable عن طريق ان انت تقوله اسم ال Variable وبعدين يساوي وبعدين ال Value مثلا x=10 ف هو هنا عرف Variable اسمه x وحط فيه ال Value اللي قيمتها 10

```
[root@MohamedAtef ~]# x=10
```

- لو انا عايز اعرض قيمه ال Variable علي الاسكرين بتاعتي هستخدم command اسمه **echo** وبعدين اسم ال Variable وقبل ال Variable لازم احط **$** dollar sign

```
[root@MohamedAtef ~]# echo $x
10
```

- ممكن مثلا ان انا اديله String ان انا اقوله مثلا ان ال First_Name بيكون Mohamed

```
[root@MohamedAtef ~]# First_Name=Mohamed
[root@MohamedAtef ~]# echo $First_Name
Mohamed
```

- فيه عندي Variable من ال Variable المهمه جدا وهو **$PATH** وده بيكون فيه كل ال Locations اللي انت لما تيجي ت Run اي Command من ال CLI هو هيروح يعمل Search By Default في ال Locations دي كلها علي اي Executable file بال Name اللي انت حاططهوله لو لاقاه هيعمل run لل Command ده ولو ملاقهوش هيقولك Command Not Found

```
[root@MohamedAtef ~]# echo $PATH
/root/.local/bin:/root/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin
```

Chapter 6

Managing Local Users and Groups

WHAT IS A USER?

- A user account is used to provide security boundaries between different people and programs that can run commands.
- The system distinguishes user accounts by the unique identification number assigned to them, the user ID or UID.
- There are three main types of user account: the **superuser**, **system users**, and **regular users**.

- فكره ان اللينكس عباره عن Multi user Operating System و Multi User معناها ان انت ممكن يبقي عندك اكتر من user متسجلين عندك في نفس الوقت وكل user بيعمل task معينه مطلوبه منه ففكرت ان يبقي عندك account واحد created علي السيستم بتاعك وكل ال users بتستخدم نفس الاكونت ونفس الصلاحيات علشان ت login علي السيستم ف ده ك security مش افضل حاجه بالاخص لو الاكونت ده هو ال super user ف انت ك سيستم ادمن لازم تعمل اكونت لكل user وت set ال permissions بتاعت الاكونت علي حسب ال business need بتاعت كل user محتاج انه ي login علي السيستم
- انا عندي في اللينكس اي user اتعمله created في السيستم بي assigned ليه او بيتخصص ليه حاجه اسمها User ID او UID ودي السيستم بيفرق مابين ال users وبعضها عن طريق ال UID انا عندي 3 انواع من ال user account

- عندي نوع اسمه Super User وده ال user اللي عنده full access علي السيستم بتاعك اللي هو ال root وده دايما هتلاقي ال UID بتاعه علي اي Linux OS بيكون ب zero
- وعندي نوع اسمه Regular Users وده ال user اللي انت بتستخدمه يوميا في الشغل وده بيكون ليه limited permissions علي السيستم
- ونوع اسمه System User فيه بعض ال Processes بتبقي محتاجه اللي يت create ليها system account علشان تقدر ت manage ال files بتاعتها وت secure ال files بتاعتها ف بيت create ليها user اسمه system users .

UID Ranges

- **UID 0** is always assigned to the superuser account, **root**.
- **UID 1-200** is a range of "system users" assigned statically to system processes by Red Hat.
- **UID 201-999** is a range of "system users" used by system processes that do not own files on the file system. They are typically assigned dynamically from the available pool when the software that needs them is installed.
- **UID 1000+** is the range available for assignment to regular users.
- You can use the **id** command to show information about the currently logged-in user.

```
[user01@host ~]$ id
```
uid=1000(user01) gid=1000(user01) groups=1000(user01)

```
[user01@host]$ id user02
```
uid=1002(user02) gid=1001(user02) groups=1001(user02)

- هنتكلم عن ال UID Ranges ف احنا قولنا ان كل user هيتعمله create عندي علي السيستم سواء كان Super User او Regular Users او System Users هو بيت assigned ليه User ID او UID

➢ انا عندي ال **UID** بيكون **0** دايما هتلاقيه بي assigned لل superuser account هنلاقي دايما ال root واخد **UID 0**

➢ عندك ال range من **1** لحد **999** ال range ده بي assigned لل system users يعني اي system user اتعمله create هياخد range من **1** لحد **999** وهنلاقي ال range ده مقسوم ل Two Categories

1. عندي من **1** لحد **200** دي static values محجوزه ل services معينه يعني فيه services معينه السيستم اول اما بي create ليها مثلا system user بي assigned ليها دايما static values من ال range من 1 لحد 200
2. وعندي من **201** لحد **999** ده ال dynamic range السيستم بي assign اي dynamic value من ال Range ده ل اي system account اتعمله create في السيستم

➢ اما بالنسبه لل Regular Users هتلاقي ال range بتاعهم بيبدأ من **1000** لحد **60000**

- ال configuration file الموجود فيه ال UID Range اسمه login.defs تحت /etc/

```
[root@MohamedAtef ~]# less /etc/login.defs
UID_MIN                  1000
UID_MAX                  60000
# System accounts
SYS_UID_MIN              201
SYS_UID_MAX              999
# Extra per user uids
SUB_UID_MIN              100000
SUB_UID_MAX              600100000
SUB_UID_COUNT            65536
```

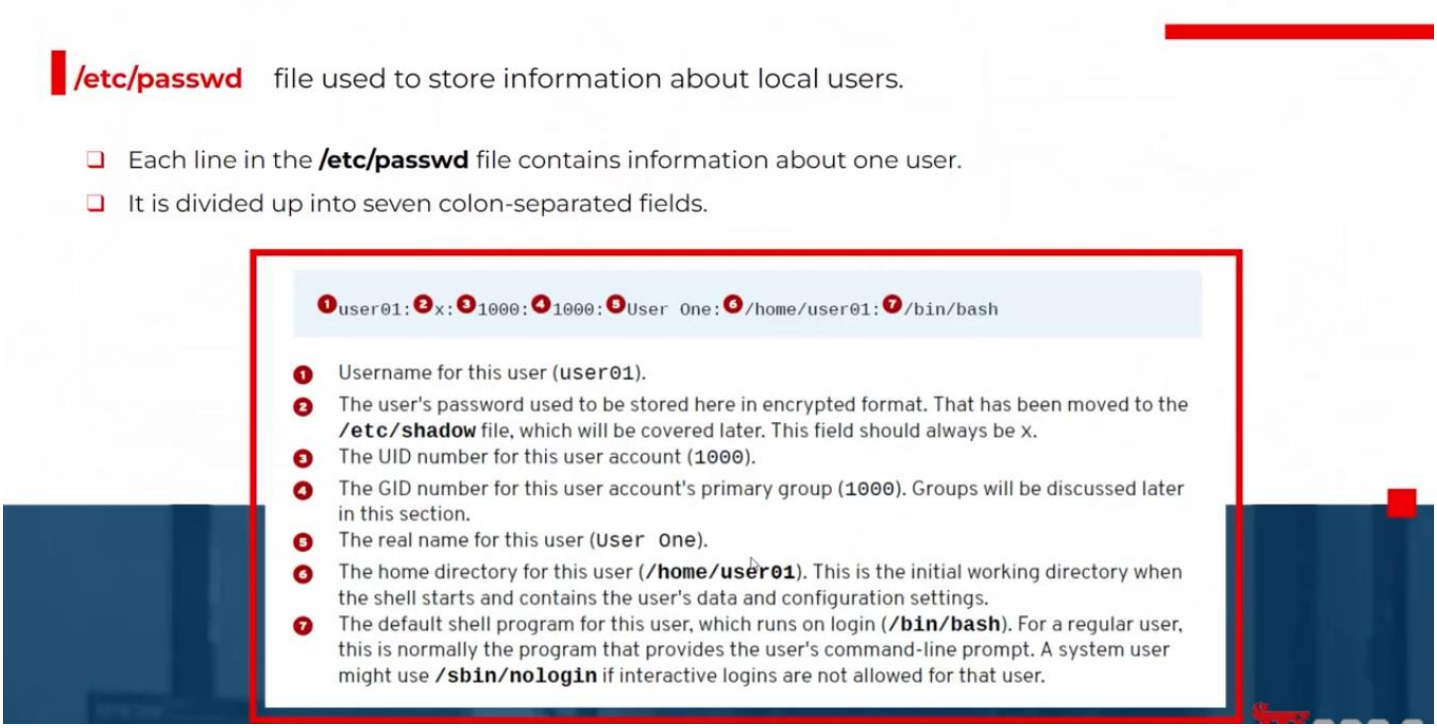
- فيه عندي command اسمه **id** بستخدمه لو انا عايز اعرف معلومات عن ال users الموجوده عندي علي السيستم

- لو انا قولتله بس id هيعرضلي معلومات عن ال user اللي انا شغال بيه وهو في الحاله دي ال root

```
[root@MohamedAtef ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

- لو عايز اعرف معلومات عن user معين هقوله id وبعدين اسم ال user انا عندي مثلا user اسمه Mohamed علي السيستم وعايز اعرف معلومات عنه ف انا لما نفذت ال command ظهرلي ال user id بتاعه وظهرلك كمان ال group id الخاص بيه وهنعرف كل ده بالتفصيل بعدين

```
[root@MohamedAtef ~]# id mohamed
uid=1004(mohamed) gid=1005(mohamed) groups=1005(mohamed)
```



- **/etc/passwd** ال file ده من ال files المهمه جدا في اللينكس ومهم جدااا انك تكون عارف ال content بتاعته عباره عن ايه
- اي local user اتعمله create عندي في السيستم سواء كان Super User او Regular Users او System Users بيبقي ليه record جوه ال **/etc/passwd** بيبقي فيه information عن ال Accounts دي
- ال file ده عباره عن سبع اعمده منفصلين عن بعض ب colon : النقطتين فوق بعض

- اول filed فيه بيكون ال user name نفسه اللي ال user بيعمل بيه login بيه علي السيستم وليكن مثلا user01
- تاني filed هتلاقيه دايما ب x كان زمان بيبقي stored في تاني filed ال encrypted password بتاعت ال users بس حاليا ال encrypted password بقي stored في file تاني اسمه **/etc/shadow**
- تالت filed وهو ال UID الخاص بال user بتاعنا وليكن مثلا 1000
- رابع filed وهو ال GID
- خامس filed ده بيبقي عباره عن comment عن ال user

- سادس filed وده بيبقي عباره عن ال home directory الخاص بال user وبيتعمل create باسم ال user تحت **/home**
- اخر filed وهو ال default shell اللي ال user لما يفتح interactive shell او ي login علي ال CLI هيبقي by default هيتفتحله ال bash هنلاقي ان ال system user ال default shell الخاص بيها هو **/sbin/nologin** لان ال system user غير مسموح ليهم انهم يفتحوا ال CLI

WHAT IS A GROUP?

- Groups can be used to grant access to files to a set of users instead of just a single user.
- Internally, the system distinguishes groups by the unique identification number assigned to them, the group ID or **GID**.
- The mapping of group names to GIDs is defined in databases of group account information.
- By default, systems use the **/etc/group** file to store information about local groups.

```
❶group01:❷x:❸10000:❹user01,user02,user03
```

1. Group name for this group (`group01`).
2. Obsolete group password field. This field should always be `x`.
3. The GID number for this group (`10000`).
4. A list of users who are members of this group as a supplementary group (`user01`, `user02`, `user03`). Primary (or default) and supplementary groups are discussed later in this section.

- فكره ال group معموله علشان لو انت عندك اكتر من user created عندك في السيستم وعايز ت grant access مثلا ل files معينه لمجموعه من ال users ف انت بدل اما ت grant ال permissions لuser user منهم علي ال files لا انت بت create group وبتخلي ال users دي كلها member في ال group ده وبمجرد انهم بقو جزء من ال group اي permissions ال group ده واخدها هياخدو نفس ال permissions علي طول لو مثلا ال group ده ليه read permissions علي files معينه كل ال users ال member من ال group ده هياخدو نفس ال read permissions علي نفس ال files
- كل Group اتعمله create عندي في السيستم بيبقي ليه Group ID او GID
- اي Group اتعمله create عندي بيقي stored information عنه في **/etc/group** هتلاقي file تحت **/etc** اسمه group ال file ده بيكون فيه four colon مابين ال colon والتاني فيه separated colon نقطتين فوق بعض :
  - اول filed عباره عن ال Group Name بتاعك
  - تاني filed عباره عن ال X
  - تالت filed هو ال GID Number
  - رابع filed بيكون فيه list of users بيكون فيه ال user ال member من ال group

Switching users

- The **su** command allows users to switch to a different user account. If you run **su** from a regular user account, you will be prompted for the password of the account to which you want to switch. When root runs **su**, you do not need to enter the user's password.

```
[user01@host ~]$ su – karim
```

- If you omit the user name, the **su** or **su** - command attempts to switch to root by default.

```
[user01@host ~]$ su -
Password:
[root@host ~]#
```

- زي ماقولنا ان ال Linux عباره عن Multi User OS ف انت ممكن يكون عندك اكتر من user عاملين تسجيل دخول في نفس الوقت او ممكن انت ك سيستم ادمن تبقي عامل login ب Regular User وده recommended ان انت دايما ك سيستم ادمن بت login ب Regular User اللي انت بتستخدمه يوميا في الشغل علشان تعمل اي task معينه ومتلجئش دايما لل superuser account الا لو فعلا انت محتاج تعمل اي admin task معينه محتاج ال superuser ف انا عندي طريقتين علشان أ gain superuser access

1- اول طريقه اني استخدم command اسمه **su** وده بنستخدمه علشان ن switch مابين ال users وبعضها لو انا مثلا فاتح ال CLI وعامل login بي user معين وعايز أ switch ل user تاني هقوله **su** وبدين داش **-** واسم ال user اللي انا عايز switch ليه

- لو انا Regular User فلما استخدم ال command **su** هيطلب مني ال password بتاعت ال user اللي انا عايز أ login بيه او switch ليه ولكن لو انا root وهعمل switch ل user مش هيطلب مني باسورد
- انا عندي user اسمه Mohamed هنعمل switch ليه

```
[root@MohamedAtef ~]# su - mohamed
[mohamed@MohamedAtef ~]$
```

هنلاقي هنا قبل اما اعمل switch ال user اللي انا عامل بيه login هو ال root
بعد اما عملنا switch بقي ال user هو mohamed

- لو عايز اعرف ال user اللي انا عامل بيه login هستخدم command اسمه **whoami**

```
[mohamed@MohamedAtef ~]$ whoami
mohamed
```

هنلاقيه هنا قايلك ان ال user اللي انت عامل ليه login هو mohamed

- لما بستخدم ال **su** وبعدين **-** ده بيوديني علي ال home directory بتاع ال user اللي عايز أ switch ليه
- لو انا استخدمت **su** وبعدين اسم ال user من غير الداش - مش هيوديني علي ال home directory الخاص بال user هيوديني علي ال current directory اللي انا كنت واقف عليه بمعني لو انا واقف تحت **/tmp** وبعدين عملت switch ل user اسمه Mohamed لما يعمل switch ال user اللي اسمه Mohamed هيكون واقف تحت /tmp

```
[root@MohamedAtef tmp]# su mohamed
[mohamed@MohamedAtef tmp]$
```

- لو انا ك user عادي عايز ا login او switch لل root هقوله **su –** او اقوله **su – root**

```
[mohamed@MohamedAtef ~]$ su - root
Password:
[root@MohamedAtef ~]#
```

هنلاقيه هنا طلب مني الباسورد بتاعت ال root علشان اقدر اعمل switch

Running commands with sudo

- In some cases, the root user's account may not have a valid password at all for security reasons.
- In this case, users cannot log in to the system as root directly with a password, and **su** cannot be used to get an interactive shell. One tool that can be used to get root access in this case is **sudo**.
- Unlike **su**, **sudo** normally requires users to enter their own password for authentication, not the password of the user account they are trying to access. That is, users who use **sudo** to run commands as root do not need to know the root password. Instead, they use their own passwords to authenticate access.
- For example, when **sudo** is configured to allow the user01 user to run the command **usermod** as root, user01 could run the following command to lock or unlock a user account:

```
[user01@host ~]$ sudo usermod -L user01
```

- تاني طريقه اسمها **sudo** بستخدمها لو انا ك سيستم ادمن مش عايز أ share ال root password مع كل ال users في الحاله دي ال users مش هينفع تستخدم ال **su** علشان ت Login باستخدام ال root ف هتستخدم ال **sudo** command عن طريق ان انا بمنح sudo privilege ل users معينه بحيث انها تكون مسموح ليها انها ت run اي superuser command

- انا دلوقتي ك user Mohamed عايز انفذ command ال command ده superuser command مينفعش اي حد ينفذ ال command غير ال root انا في الحاله دي هستخدم command ال sudo علشان يديني صلاحيات ال root

- هنجرب مثلا ننفذ command وهو **useradd** ال command ده بنستخدمه علشان نضيف user جديد وال command ده ال superuser هو اللي بينفذ ال command ده ف لو انا ك user عادي نفذت ال command ده باستخدام ال **sudo** ف اول مره بت run command sudo هتلاقيه بيقولك خلي بالك انت بتحاول ت run superuser command وهتلاقيه بيطلب منك الباسورد بتاعتك انت مش الباسورد بتاعت ال root وبعد اما تدخل الباسورد هتلاقيه بيقولك Mohamed is not the sudoers file ان ال user اللي اسمه Mohamed ملهوش اي sudoers علي انه يستخدم ال command ده ف علشان نحل المشكله دي لازم ال root هو اللي يدي ال permissions لل user انه يستخدم ال sudo

```
[mohamed@MohamedAtef ~]$ sudo useradd ahmed

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for mohamed:
mohamed is not in the sudoers file.  This incident will be reported.
```

Configuring Sudo

- The main configuration file for **sudo** is **/etc/sudoers**. To avoid problems if multiple administrators try to edit it at the same time, it should only be edited with the special **visudo** command.
- For example, the following line from the **/etc/sudoers** file enables **sudo** access for members of group wheel.

```
%wheel ALL=(ALL) ALL
```

- In this line, **%wheel** is the user or group to whom the rule applies. A % specifies that this is a group, group wheel. **The ALL=(ALL)** specifies that on any host that might have this file, wheel can run any command. The final **ALL** specifies that wheel can run those commands as any user on the system.
- To enable full **sudo** access for the user user01

```
user01 ALL=(ALL) ALL
```

- To enable full sudo access for the group group01

```
%group01 ALL=(ALL) ALL
```

- هنعرف ازاي انا ك root ازاي امنح اي user ال sudo permissions
- انا عندي file تحت /etc/ اسمه **sudoers** ال file ده انا بفتحه واكتب فيه record لل user اللي انا عايز امنحه ال sudo permissions
- لو انا مثلا عايز user اسمه user01 وعايز اديله ال sudo permissions ف انا هفتح الfile اللي اسمه **sudoers** وهكتب جواه record بالشكل ده **user01 ALL=(ALL) ALL** ال record ده معناه ان انا هخلي ال user01 زي ال root بالظبط بقي معاه full access
- ولو انا عايز امنح group معين ال sudo permissions هيبقي نفس ال record اللي استخدمناه في حاله ال user بس هنحط قبل ال record هنحط **%** زي مثلا **%group01 ALL=(ALL) ALL**
- طب ايه الفرق مابين ALL اللي في الاول واللي في النص مابين قوسين واللي ف الاخر .ALL اللي في الاول معناها on any host اللي عليه ال file و ALL الي مابين قوسين معناها any user و ALL اللي في الاخر معناها any command يعني من الاخر بقوله ال user اللي اسمه user01 بقي مسموح ليه انه ي run any commands كأنه اي user موجود عندك علي السيستم ومن اي host موجود عندك ال file ده موجود فيه

- علشان نفتح ال file اللي اسمه sudoers هنستخدم اي editor موجود عندي وليكن vim او ممكن استخدم command اسمه **visudo** ال command هيتفتحلي ال file علي طول
- لما نفتح ال file هنلاقي record موجود فيه **root ALL=(ALL) ALL** هنكتب تحت ال record ده ال record الخاص بال user اللي اللي انا عايز اديله نفس صلاحيات ال root ف انا اديت ل Mohamed نفس صلاحيات ال root

```
[root@MohamedAtef ~]# vim /etc/sudoers
## Allow root to run any commands anywhere
root        ALL=(ALL)     ALL
Mohamed     ALL=(ALL)     ALL
```

- بعد اما ضفنا ال record في ال file هنعمل save لل file وبعدين هنشوف ال command اللي احنا نفذناه قبل كده ومقبلش هنجرب نفس ال command تاني هنلاقيه قبل ومحصلش اي مشكله

```
[root@MohamedAtef ~]# sudo useradd ahmed
```

- علشان نتاكد هل ال User اللي اسمه ahmed انضاف ولا لا هنعمل cat لل file اللي اسمه passwd

```
[root@MohamedAtef ~]# cat /etc/passwd
mohamed:x:1004:1005::/home/mohamed:/bin/bash
ahmed:x:1005:1006::/home/ahmed:/bin/bash
```

هنلاقيه هنا عمل create لل user اللي اسمه ahmed

Creating Users from the Command Line

- The **useradd username** command creates a new user named username. It sets up the user's home directory and account information, and creates a private group for the user named username. At this point the account does not have a valid password set, and the user cannot log in until a password is set.
- The **useradd --help** command displays the basic options that can be used to override the defaults. In most cases, the same options can be used with the **usermod** command to modify an existing user.
- Some defaults, such as the range of valid UID numbers and default password aging rules, are read from the **/etc/login.defs** file.
- Values in this file are only used when creating new users. A change to this file does not affect existing users.

- علشان اضيف user هستخدم **useradd** وبعدين اسم ال username
- علشان اعمل modify هستخدم **usermod**
- علشان اعمل delete ل user هستخدم **userdel**

- علشان اعمل create ل user هستخدم **useradd** ف انا هعمل create ل user اسمه mahmoud

```
[root@MohamedAtef ~]# useradd mahmoud
```

- علشان نتاكد هنعمل grep ل Mahmoud في /etc/passwd هنلاقيه by default عمل create ل user اسمه Mahmoud واداله ال UID ب 1007 وال home directory بتاعته تحت /home/ اتعمل create ل folder باسم Mahmoud وده بقي ال home directory بتاعه وال default bash بتاعته /bin/bash

```
[root@MohamedAtef ~]# grep mahmoud /etc/passwd
mahmoud:x:1007:1008::/home/mahmoud:/bin/bash
```

- لو جينا عملنا tail ل اخر 3 سطور في ال passwd هنلاحظ ان انا عندي three users وكل user ليه UID الخاص بيه ف هنلاحظ ان كل اما اعمل create ل user ال UID بيزيد تدريجيا يعني اول user اللي هو ahmed هتلاقي ال UID بتاعه 1005 وال user اللي بعديه 1006 وال user اللي احنا لسه عاملينه واخد 1007

```
[root@MohamedAtef ~]# tail -n 3 /etc/passwd
ahmed:x:1005:1006::/home/ahmed:/bin/bash
ali:x:1006:1007::/home/ali:/bin/bash
mahmoud:x:1007:1008::/home/mahmoud:/bin/bash
```

- لو احنا عايزين نعرف ال basic options هستخدم help-- مع ال useradd

```
[root@MohamedAtef ~]#  useradd --help
```

```
Options:
  --badname                 do not check for bad names
 -b, --base-dir BASE_DIR    base directory for the home directory of the
                            new account
  --btrfs-subvolume-home    use BTRFS subvolume for home directory
 -c, --comment COMMENT      GECOS field of the new account
 -d, --home-dir HOME_DIR    home directory of the new account
 -D, --defaults             print or change default useradd configuration
 -e, --expiredate EXPIRE_DATE  expiration date of the new account
 -f, --inactive INACTIVE    password inactivity period of the new account
 -g, --gid GROUP            name or ID of the primary group of the new
                            account
 -G, --groups GROUPS        list of supplementary groups of the new
                            account
 -h, --help                 display this help message and exit
 -k, --skel SKEL_DIR        use this alternative skeleton directory
 -K, --key KEY=VALUE        override /etc/login.defs defaults
 -l, --no-log-init          do not add the user to the lastlog and
-m, --create-home           create the user's home directory
 -M, --no-create-home       do not create the user's home directory
 -N, --no-user-group        do not create a group with the same name as
                            the user
 -o, --non-unique           allow to create users with duplicate
                            (non-unique) UID
 -p, --password PASSWORD    encrypted password of the new account
 -r, --system               create a system account
 -R, --root CHROOT_DIR      directory to chroot into
 -P, --prefix PREFIX_DIR    prefix directory where are located the /etc/* file
 -s, --shell SHELL          login shell of the new account
 -u, --uid UID              user ID of the new account
 -U, --user-group           create a group with the same name as the user
 -Z, --selinux-user SEUSER  use a specific SEUSER for the SELinux user
mapping
```

- تعال نعمل add ل user ونستخدم بعض ال options الموجوده نقوله useradd نستخدم اوبشن **-md** علشان اعمل create ل home directory لل user اللي هعملهadd هعمل create تحت /home ل directory باسم user_01 وممكن نضيف comment عن طريق اني استخدم اوبشن **-c** وبعدين اضيف ال comment هقوله مثلا "Planning user" وممكن احددله ال default shell عن طريق اني استخدم اوبشن **-s** هستخدم مثلا /bin/sh وممكن اضيف private group اسمه karim عن طريق اني استخدم اوبشن **-g** وبعدين اضيف اسم ال private group وممكن اخليه كمان في secondary group اسمه wheel هستخدم اوبشن **-G** وممكن احدد ال UID بتاعه عن طريق اني استخدم اوبشن **-u** وبعدين ال UID وليكن مثلا 5000 وفي الاخر اديله اسم ال User بتاعي اللي هعمله create وليكن في المثال بتاعنا هنسميه **user01**

```
[root@MohamedAtef ~]# useradd -md /home/user_01 -c "Planning user" -s /bin/sh -g karim -G wheel -u 5000 user01
```

- لو عملنا grep علي ال user اللي اسمه user01 اللي عملناه في ال file اللي اسمه passwd علشان نتاكد

```
[root@MohamedAtef ~]#  grep user01 /etc/passwd
user01:x:5000:1001:Planning user:/home/user_01:/bin/sh
```

هتلاقيه هنا عملي user باسم user01 وال UID بتاعه 5000 وهتلاقي ال primary group بتاعه ال GID بتاعه 1000 وبعدين ضافلي comment عباره عن Planning user وعملي ال home directory تحت home/ باسم user_01 وال default shell بتاعته /bin/sh

- علشان اقدر أ login بال user01 واقدر اتعامل معاه لازم اعمل Set Password لل user01 عن طريق اني استخدم command اسمه **passwd** وبعدين اسم ال user

```
[root@MohamedAtef ~]# passwd user01
Changing password for user user01.
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: all authentication tokens updated successfully.
```

هيطلب منك New Password وبعد اما تضيف الباسورد هيطلب منك انك تكتب الباسورد للتاكيد وبعد كده هيعمل set للباسورد

- تعال نعمل login ل user01 وبعدين نستخدم pwd علشان اعرف ال working directory

```
[root@MohamedAtef ~]# su - user01
[user01@MohamedAtef ~]$ pwd
/home/user_01
```

لما استخدمنا ال pwd ظهرلي ال home directory اللي احنا حددناه واحنا بنعمل create لل user وهو /home/user_01

- لو جيت قولتله id

- ال group اللي اسمه wheel ده ليه record جوه ال file اللي اسمه sudores ف اي user بيكون member من الجروب ده هيكون معاه sudo privileges هيكون معاه صلاحيات ال root

```
[user01@MohamedAtef ~]$ id
uid=5000(user01) gid=1001(karim) groups=1001(karim),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

هنلاقيه هنا ال UID ب 5000 | هنلاقي ال GID ب 1000 | هنلاقي هنا ال groups اللي هو member | ده ال private group | ده ال second group

- لو عملنا delete ل user معين باستخدام ال user01 هنلاقيه عمل delete لان user01 بيكون member من ال group اللي اسمه wheel والجروب ده عنده صلاحيات ال root هنعمل delete باستخدم **userdel**

```
[user01@MohamedAtef ~]$ sudo userdel ali
```

- علشان اعمل modify ل اي user موجود عندي هستخدم command اسمه **usermod** وال options المستخدمه مع **usermod** هي نفسها ال options المستخدمه مع useradd

```
[root@MohamedAtef ~]# usermod -u 2000 -c "user01" -g wheel -s /bin/bash user01
```

- علشان اعمل delete هستخدم **userdel** وبعدين اسم ال user بس لما اعمل delete لل user ال home directory بتاع ال User اللي بعمله delete هيفضل موجود ف لو انا عايز اعمل delete ل user بال home directory بتاعه هستخدم اوبشن **-r** مع **userdel** زي مثلا **userdel -r ali**

```
[root@MohamedAtef ~]#  userdel -r ali
```

- لو انا عايز اضيف secondary group هستخدم اوبشن **-G** مع usermod والاوبشن ده بيعمل overwrite لل secondary group بمعني لو انا عندي secondary group اسمه wheel واستخدم اوبشن-G علشان اضيف secondary group تاني اسمه مثلا karim ف الاوبشن ده هيعمل overwrite هيشيل ال secondary group اللي اسمه wheel وهيضيف karim

```
[root@MohamedAtef ~]# useradd user02
[root@MohamedAtef ~]# id user02
uid=2001(user02) gid=2001(user02) groups=2001(user02)
[root@MohamedAtef ~]# usermod -G wheel user02
[root@MohamedAtef ~]# id user02
uid=2001(user02) gid=2001(user02) groups=2001(user02),10(wheel)
```

عملنا user تاني اسمه user02

بعد كده عملنا id لل user02 علشان اعرف معلومات عن ال user ده ف هنلاقي ال user ده في جروب اسمه user02 ومش منضاف ليه اي secondary group

ف احنا هنضيف secondary group اسمه wheel باستخدم اوبشن -G

عملنا id تاني وهنلاحظ انه ضاف ال secondary group اللي اسمه wheel

- لو جينا ضيفنا secondary group تاني اسمه karim باستخدام نفس ال option هنلاحظ انه عمل overwrite

```
[root@MohamedAtef ~]# id user02
uid=2001(user02) gid=2001(user02) groups=2001(user02),1001(karim)
```

هنلاقيه هنا عمل overwrite وضاف الجروب اللي اسمه karim

- لو انا عايز اعمل append ل secondary group هستخدم اوبشن-aG اوبشن a معناه append

```
[root@MohamedAtef ~]# usermod -aG wheel user02
[root@MohamedAtef ~]# id user02
uid=2001(user02) gid=2001(user02) groups=2001(user02),10(wheel),1001(karim)
```

هنلاقيه هنا عملي append ومعملش overwrite لل secondary group

- لوانا عايز اعمل Lock ل user معين بستخدم اوبشن **-L** علشان ميقدرش يستخدم الاكونت ده

```
[root@MohamedAtef ~]# usermod -L karim
```

- لو عايز اعمل Un Lock ل user معمول ليه Lock هستخدم اوبشن **-U**

```
[root@MohamedAtef ~]# usermod –U karim
```

Creating Groups from the Command Line

```
[user01@host ~]# sudo groupadd -g 10000 group01
[user01@host ~]# tail /etc/group
```

The **-g** option specifies a particular GID for the group to use.

Modifying Existing Groups from the Command Line

```
[user01@host ~]# groupmod -n group0022 group02
```

The **-n** option specifies a new name for the group

Deleting Groups from the Command Line

```
[user01@host ~]# groupdel group0022
```

- فكرة ال group انك بت create group وبتديله permissions معينه وفي الاخر بتخلي اي user يكون member من ال group ده ف انت بمجرد انك خليت ال user ده member من ال group اللي انت عملتله create واديته permissions معينه هو في الاخر هياخد نفس ال permissions بتاعت ال group
- علشان اعمل create ل group بستخدم **groupadd** وعلشان اعمل modify ل group بستخدم **groupmod** وعلشان اعمل delete ل group بستخدم **groupdel**

- ممكن استخدم help-- علشان اعرف كل ال Options اللي ممكن استخدمها مع ال groupadd

```
[root@MohamedAtef ~]# groupadd --help
Usage: groupadd [options] GROUP

Options:
  -f, --force                   exit successfully if the group already exists,
                                and cancel -g if the GID is already used
  -g, --gid GID                 use GID for the new group
  -h, --help                    display this help message and exit
  -K, --key KEY=VALUE           override /etc/login.defs defaults
  -o, --non-unique              allow to create groups with duplicate
                                (non-unique) GID
  -p, --password PASSWORD       use this encrypted password for the new group
  -r, --system                  create a system account
  -R, --root CHROOT_DIR         directory to chroot into
  -P, --prefix PREFIX_DI        directory prefix
  -U, --users USERS             list of user members of this group
```

- هنعمل create ل group عن طريق اني استخدم groupadd وبعدين هستخدم اوبشن g- علشان اضيف GID وليكن مثلا ال GID هيكون 3000 واسم الgroup مثلا group01

```
[root@MohamedAtef ~]# groupadd -g 3000 group01
```

- لو جينا عملنا grep ل group01 تحت /etc/group هنلاقيه اتعمله create

```
[root@MohamedAtef ~]# grep group01 /etc/group
group01:x:3000:
```

هنلاقيه هنا عمل create لل group01 واداله GID 3000 ومفيش اي user member من ال group ده

- هنخلي ال user اللي اسمه كريم member من ال group01

```
[root@MohamedAtef ~]# usermod -aG group01 karim
```

- هنعمل grep تاني علي group01 ف هنلاحظ دايما انه قدام group01 اتحط قدامه ال list of users اللي هما member من الgroup ده

```
[root@MohamedAtef ~]# grep group01 /etc/group
group01:x:3000:karim
```

هنلاقيه هنا ضافلي الuser اللي اسمه karim في ال group01

- لو انا عايز أ modify هستخدم **groupmod** لو انا عايز اغير ال GID هستخدم اوبشن g- وبعدين ال GID الجديد

```
[root@MohamedAtef ~]#  groupmod -g 4000 group01
[root@MohamedAtef ~]# grep group01 /etc/group
group01:x:4000:karim
```

- لو انا عايز اعمل rename لل group هستخدم اوبشن **n-**

```
[root@MohamedAtef ~]# groupmod -n group0022 group01
```

- لو انا عايز اعمل delete ل group معين هستخدم **groupdel**

```
[root@MohamedAtef ~]# groupdel group01
```

Managing user passwords

- Like **/etc/passwd**, each user has a line in the **/etc/shadow** file. A sample line from **/etc/shadow** with its nine colon-separated fields is shown below.

```
❶user03:❷$6$CSsX...output omitted...:❸17933:❹0:❺99999:❻7:❼2:❽18113:❾
```

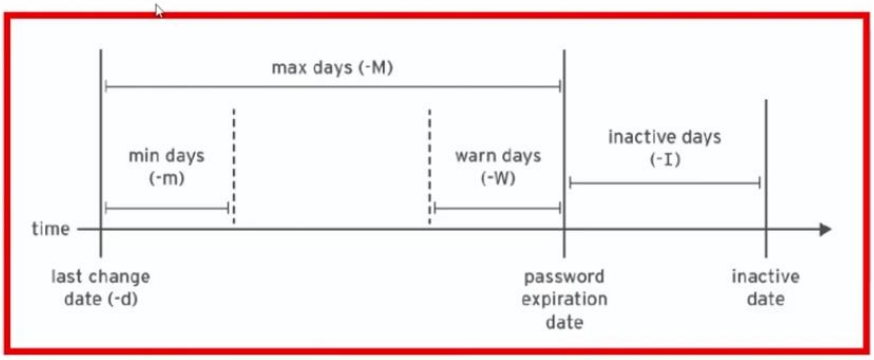
1. Username of the account this password belongs to.
2. The *encrypted password* of the user. The format of encrypted passwords is discussed later in this section.
3. The day on which the password was last changed. This is set in days since 1970-01-01, and is calculated in the UTC time zone.
4. The minimum number of days that have to elapse since the last password change before the user can change it again.
5. The maximum number of days that can pass without a password change before the password expires. An empty field means it does not expire based on time since the last change.
6. Warning period. The user will be warned about an expiring password when they login for this number of days before the deadline.
7. Inactivity period. Once the password has expired, it will still be accepted for login for this many days. After this period has elapsed, the account will be locked.
8. The day on which the password expires. This is set in days since 1970-01-01, and is calculated in the UTC time zone. An empty field means it does not expire on a particular date.
9. The last field is usually empty and is reserved for future use.

- هنتكلم عن ال Password Management زي ماقولنا اي user اتعمله create عندي في السيستم بيبقي stored معلومات عنه تحت /etc/passwd اما بالنسبه لل password information بتبقي stored في مكان تاني اسمه /etc/shadow وال root هو بس اللي ليه permission علي ال file ده
- ال file اللي اسمه shadow بيتكون من nine colon-separated field

1- اول filed فيهم بيبيقي عباره عن ال username بتاعنا
2- تاني filed هو ال encrypted password
3- تالت filed عباره عن عدد الايام من 1-1-1970 لحد ال last password change بمعني لو انا جيت غيرت الباسورد انهارده ف هيتحط عدد الايام من 1-1-1970 لحد انهارده اليوم اللي غيرت فيه الباسورد
4- رابع filed ده اسمه ال minimum days required before password change يعني ايه هي في ال slide محطوطه ب 0 دي معناها انها معمول ليها disable طب لو انا غيرتا ل 2 معناها ان انت لو غيرت الباسورد بتاعتك انهارده ف انت مش هيبقي مسموح ليك انك تغير الباسورد الا لما يعدي عليك يومين
5- خامس filed دي ال maximum number days دي عدد الايام اللي بعديها الباسورد بتاعتك هيحصلها expired هي محطوطه 99999 دي معناها ان الباسورد بتاعتك مش هيحصلها expired خالص
6- سادس filed بيتقال عليه ال warning period هنلاقيها معموله 7 ايام معناها ان قبل اما الباسورد بتاعتك يحصلها expired ب 7 ايام هيبعتلك warning ان الباسورد بتاعتك هيحصلها expired
7- سابع filed وده ال inactivity period وليكن مثلا انا عامل ان بعد 30 يوم هيحصل expired للباسورد هل السيستم هيعمل Lock للاكونت علي طول بعد ال 30 يوم لا مش هيعمل lock قالك ان ممكن يديك سماحيه يومين مثلا او كذا يوم انك ت login وتغير الباسورد
8- ثامن filed بيبقي فيه عدد الايام من 1-1-1970 لحد الباسورد expired day بمعني لو الباسورد بتاعتك حصلها expired انهارده ف عد عدد الايام من 1-1-1970 لحد انهارده اللي هو اليوم اللي حصل فيه expired للباسورد ويتحط في ال filed رقم 8
9- تاسع filed ال filed ده هتلاقيه فاضي

Configuring password aging

- The following diagram relates the relevant password aging parameters, which can be adjusted using the **chage** command to implement a password aging policy




```
[root@host ~]# chage -m 0 -M 90 -W 7 -I 14 user03
```

The preceding **chage** command uses the **-m**, **-M**, **-W**, and **-I** options to set the minimum age, maximum age, warning period, and inactivity period of the user's password, respectively.

- هنشوف ازاي ن configure ال password aging parameters احنا كل ال parameters اللي اتكلمنا عليها في /etc/shadow سواء كان ال minimum days او ال maximum days ال warning ال inactivity period كل الكلام ده كله انت تقدر ت Modify فيه او ت set parameters معينه باستخدام command اسمه **chage**
- علشان ت Modify الكلام ده هتقوله **chage** وبعدين اوبشن **-m** علشان تchange ال minimum days وبعدين احددله ال minimum days انا عاملها ب 0 معناها ان انا عاملها disable ان انا ممكن اغير الباسورد في اي وقت وبعدين لو انا عايز اغير ال maximum days هستخدم اوبشن **-M** وبعدين احددله ال maximum days انا هنا قايله ب 90 معناها ان الباسورد هيحصلها expired بعد 90 يوم بعد 3 شهور وبعدين لو انا عايز اغير ال warning period بستخدم اوبشن **-W** انا محددله 7 ايام بمعني ان قبل اما ال90 يوم يخلصوا ب 7 ايام ابدء ابعتلي warning بعد كده بحددله ال inactive days باستخدام اوبشن **-I** انا هنا مديله سماحيه 14 يوم بعد اما ال 90 يوم يخلصوا يعمل change للباسورد قبل اما يحصل lock للاكونت

```
[root@MohamedAtef ~]# chage -m 0 -M 90 -W 7 -I 14 user03
```

- نشوف مثال تاني تعال نعمل grep للuser اللي اسمه karim في /etc/shadow هنلاقي ان ال minimum ب 0 وال maximum ب 99999 وال warning معموله ب 7 وال inactivity period مش محططوطه

```
[root@MohamedAtef ~]# grep karim /etc/shadow
karim:$6$2qSY1aV94FJD1zQQ$RizHBdwPjJkhUlTsPF6mXmaDqCw9MrLB1QC10cr57pQJafvZfa7Xm2bWEixKlfyz3fR1
:19792:0:99999:7:::
```

- هنعمل modify في ال user اللي اسمه karim

```
[root@MohamedAtef ~]# chage -m 2 -M 90 -W 5 -I 7 karim
[root@MohamedAtef ~]# grep karim /etc/shadow
karim:$6$2qSY1aV94FJD1zQQ$RizHBdwhUlTsPmkF6mXmaDqCw9MKDmpci2tAKl0nBy0rLB1QC10cr57pQJafvZf3fR1
:19792:2:90:5:7::
```

Restricting access

- The **usermod** command can lock an account with the **-L** option.

```
[user01@host ~]$ sudo usermod -L user03
[user01@host ~]$ su - user03
Password: redhat
su: Authentication failure
```

- If a user leaves the company, the administrator may lock and expire an account with a single **usermod** command.

```
[root@host ~]# usermod -L -e 2021-12-14 karim
```

- The preceding **usermod** command uses the **-e** option to set the account expiry date for the given user account.
- The **-L** option locks the user's password.

- لو انت عايز ك سيستم ادمن ت restrict access ل user معين او تعمل Lock ل user معين انت ممكن تعمل Lock ل user لو انت حسيت ان ال user ده بيعمل اي حاجه مش مسموح بيها بيحاول ي run اي admin command بيحاول انه يrun ال command وهو معهوش اي sudo permissions بتبقي انت محتاج انك ت Lock الاكونت لحد اما تشوف الاكونت ده بتاع مين وبيحاول يعمل ايه
- علشان تعمل lock ل اي اكونت هتقوله **usermod -L** واسم ال user

- وليكن انا عايز اعمل lock لل user اللي اسمه user03

```
[root@MohamedAtef ~]# usermod -L user03
```

- لو انا حاولت ان انا اعمل Login بال user اللي اسمه user03 مش هيقبل

```
[mohamed@MohamedAtef ~]$ su – user03
Password:
su: Authentication failure
```

- لو انا عايز اعمل Unlock هستخد اوبشن **-U** زي ماقولنا قبل كده

```
[root@MohamedAtef ~]# usermod –U user03
```

- فيه اوبشن تاني باستخدام اوبشن **-e** ان انا ممكن اعمله Lock واحددله ان الباسورد بتاعته ت expired في وقت معين انا مثلا قايله ان ال user اللي اسمه karim اعمله lock دلوقتي واعمله expired للباسورد بتاعته بتاريخ 14-12-2021

```
[root@MohamedAtef ~]# usermod –L -e 2021-12-14 karim
```

The nologin Shell

- The **nologin** shell acts as a replacement shell for the user accounts not intended to interactively log into the system.
- It is wise from the security standpoint to disable the user account from logging into the system when the user account serves a responsibility that does not require the user to log into the system.
- For example, a mail server may require an account to store mail and a password for the user to authenticate with a mail client used to retrieve mail. That user does not need to log directly into the system.
- A common solution to this situation is to set the user's login shell to **/sbin/nologin**. If the user attempts to log in to the system directly, the **nologin** shell closes the connection.

```
[root@host ~]# usermod -s /sbin/nologin user03
[root@host ~]# su - user03
```

This account is currently not available.

- هنتكلم عن ال nologin shell احنا قولنا اننا عندنا 3 انواع من ال users عندك ال superuser وال regular users وال system users وقولنا ان ال default shell بتاعت ال superuser وال regular users بتكون /bin/bash واحنا قولنا ان اي system account مش مسموح ليهم انهم يفتحوا interactive shell ف هتلاقي دايما ان ال default shell بتاعتهم اسمها /sbin/nologin
- ف انت عندك طريقه تانيه اوبشن تاني انك تعمل Lock ل user لو انت مش عايزه يفتح interactive shell علي CLI بدل اما تستخدم **usermod -L** لا هتستخدم **usermod -s** وتقوله **/sbin/nologin** انك تخلي ال default shell بتاعته nologin فساعتها لما الuser ده يجي ي Login علي السيستم هيقولك This account is currently not available

- تعال نعمل Lock لل user اللي اسمه Karim باستخدام nologin

```
[root@MohamedAtef ~]# usermod -s /sbin/nologin karim
```

- لو عملنا grep ل karim في /etc/passwd هتلاقي ال shell بقت /sbin/nologin

```
[root@MohamedAtef ~]# grep karim /etc/passwd
karim:x:1001:1001::/home/karim:/sbin/nologin
```

- لو جينا عملنا Login ب karim هتلاقيه بيقولنا This account is currently not available

```
[root@MohamedAtef ~]# su - karim
This account is currently not available.
```

Chapter 7

Controlling Access to Files

Linux file-system permissions

- File permissions control access to files. The Linux file permissions system is simple but flexible, which makes it easy to understand and apply, yet still able to handle most normal permission cases easily.
- Files have three categories of user to which permissions apply. The file is owned by a user, normally the one who created the file. The file is also owned by a single group, usually the primary group of the user who created the file, but this can be changed.
- Different permissions can be set for the **owning user**, the **owning group**, and for all **other users** on the system that are not the user or a member of the owning group.
- Three categories of permissions apply: **read**, **write**, and **execute**.

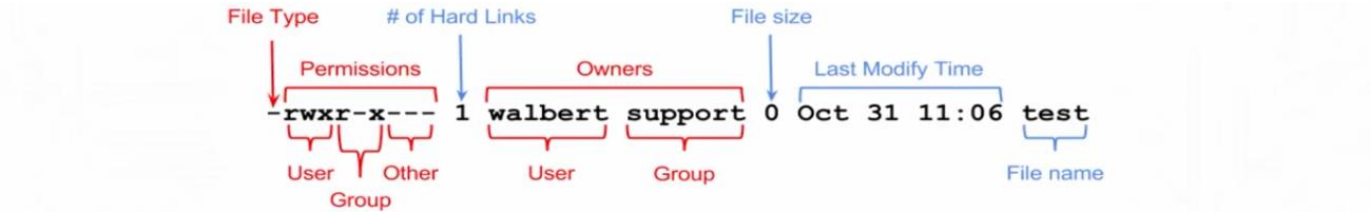
- في الشابتر ده هنتكلم عن ال Linux file-system permissions
- اللينكس عباره عن multi user operating system معني multi user ان انت ممكن يكون عندك اكتر من user موجودين عندك علي السيستم وكل user منهم بيhandle task معينه مطلوبه منه ف انت ك سيستم ادمن محتاج ان انت ت set ال permissions علي ال level ال file system بتاعك بحيث ان انت ت maintain ال security او ت provide يعني security علي Level ال files وال Directories الموجوده عندك في السيستم
- انا عندي by default اي file او directory اتعمله create في السيستم بتاعي بيكون ليه حاجه اسمها user owner ده بيكون ال user اللي م create ال file وليه حاجه اسمها group owner ده بيكون ال primary group او ال private group
- انا عندي ال Permissions بتتطبق علي ال user owner وال group owner وال others
- انا عندي Three categories لل permissions بيتعملوهم apply علي ال file او ال directory وهما read و write و execute
- هنشوف تاثير ال permissions علي ال files وال Directory

Permission	Effect on files	Effect on directories
r (read)	لو انت عندك read permissions علي file ف انت تقدر تقرا ال content بتاعت ال file ده	لو انت ليك read permissions علي directory معين ف انت تقدر ت list بس ال file name
w (write)	لو انت عندك write permissions علي file ف انت تقدر ت modify و change في ال content بتاعت ال file ده	لو انت ليك write permissions على directory معين ف انت تقدر انك ت create او ت delete اي files
x (execute)	كل ال commands الموجوده عندك في السيستم هتلاقي لو انت ليك execute permissions علي ال command نفسه تقدر ان انت ت run ال command ده او لو عند اسكريبت معين وليك execute عليه تقدر ت run الاسكريبت ده	لو انت ليك execute permissions علي directory معين ف انت تقدر تعمل cd وتدخل جوه ال directory ده وتقدر انك ت access وت modify ال files اللي جوه ال directory لو ال permissions اللي علي ال files بتسمح بده

Viewing file and directory permissions and ownership

The **-l** option of the ls command shows more detailed information about file permissions and ownership,
You can use the **-d** option to show detailed information about a directory itself, and not its contents.

- علشان نشوف ال different permissions اللي علي ال files او ال Directories وال Ownership بتاعت ال files انا عندي command اسمه **ls** بستخدم معاه اوبشن **-l** علشان اجيب more details او more information عن ال files و**-d** علشان اعرف more information عن ال directories الموجوده عندي زي مظاهر كده



- ف هنلاقي اول حاجه عندنا هي ال File Type وهو بيكون عباره عن نوع من الانواع دي
  - **-** is a regular file
  - **d** is a directory.
  - **L** is a symbolic link.
  - **c** is a character device file.
  - **b** is a block device file.
  - **p** is a named pipe file.
  - **s** is a local socket file.
- تاني حاجه وهي ال Permissions ودي بتكون عباره عن 8 bit permissions

- اول 3 bit منهم دي بتكون ال permissions اللي بتتطبق علي ال User Owner انا عندي ال file اللي اسمه test ال user owner بتاعه اسمه walbert وال group owner بتاعه اسمه support ف عندي ال permissions اللي واخدها ال user اللي اسمه walbert علي ال file اللي اسمه test هي **rwx**
- وتاني 3 bit بيكونوا ال permissions اللي بتتطبق علي ال group ف انا عندي بالنسبه للgroup هو واخد **r-x permissions** ومعني ال الداش او الماينص **-** ان ملهوش write permissions
- اخر 3 bit بيكونوا لل other يعني ايه other يعني اي حد ولا هو ينطبق عليه user owner ولا هو member من ال group اللي اسمه support اي user تاني موجود عندك في السيستم ومعني **---** ان كده ملهوش اي permissions علي ال file ده ولا ليه read ولا write ولا execute

- ال owners انا عندي اي file انا لسه عامله create ال user owner بتاعه بيكون اسم ال user اللي عامل create لل file ده ونفس الكلام لل group بيكون هو ال primary او ال private group بتاع ال user اللي لسه عامل create
- بيكون دايما اول bit بتعبر عن ال read وتاني bit بتعبر عن ال write وتالت bit بتعبر عن ال execute ولو لاقيت في ال Permissions علامه داش - ده كده معناه انه ملهوش permissions

Changing file and directory permissions

- The command used to change permissions from the command line is **chmod**
- **Symbolic method**

u, g, o, a (for user, group, other, all)
+, -, = (for add, remove, set exactly)
r, w, x (for read, write, executable)

owner – u
group – g
other – o
all – a

+ means add
– means take away

read – r
write – w
execute – x

- علشان ت change ال permissions بتاعت ال file وال Directory الموجوده عندك بنستخدم command اسمه **chmod** انا عندي طرقتين بنستخدمهم علشان نت change ال permissions اول طريقه وهي ال symbolic method والطريقه التانيه اسمه Numeric method

1- symbolic method

- لو انا عايز أ add permission او remove permission معينه لل owner هيبقي الاوبشن بتاعها هو**-u** و **-u** بيعبر عن ال owner وبالنسبه لل group هيبقي الاوبشن الخاص بيه هو **-g** وبالنسبه لل other الاوبشن الخاص بيه هو **-o** ولو انا عايز ا set permissions لكل ال users الموجودين عندي هستخدم اوبشن **-a**
- ولو انا عايز اعمل add ل permission هستخدم **+** ولو انا عايز اعمل remove ل permission بستخدم **–**
- وعندي three category لل permissions وهما read permissions ودي بنعبر عنها ب **r** وعندي write permission ودي بنعبر عنها ب **w** وعندي execute permission ودي بنعبر عنها ب **e**

- هنعمل create ل directory اسمه dir1

```
[root@MohamedAtef home]# mkdir dir1
```

- هنعمل **ls -ld** ل dir1 علشان اعرف more information عنها هنلاقي by default ان ال user owner هو ال root علشان هو اللي عامل create ل dir1 وهنلاقي الgroup owner هو ال root ف هنلاحظ بالنسبه لل default permissions اللي ال dir1 واخدها هنلاقي ال user owner واخد read و write و execute وبالنسبه لل group واخد read و execute وبالنسبه لل other واخدين read و execute بس

```
[root@MohamedAtef home]# ls -ld dir1
drwxr-xr-x. 2 root root 6 Jul 15 20:36 dir1
```

اول حاجه هنا هنلاقيها نوع ال file وهو ظاهرهنا d معناها directory

دي كده ال permissions الخاصه بال user وهي rwx ومعناه read وwrite وexecute

دي كده ال permissions الخاصه بال group وهي r-x ومعناها read وexecute

دي كده ال permissions الخاصه بال other وهي r-x ومعناها read وexecute

- لو انا عايز اغير ال permission اللي علي dir1 هستخدم **chmod** ف احنا هنعمل remove لل execute(x) من ال other(o) ف علشان اعمل remove هستخدم اوبشن - ف هقوله ال other(o) وبعدين remove(-) وبعدين ال execute(x) ف هتكون بالشكل ده o-x وفي الاخر اسم ال directory

```
[root@MohamedAtef home]#  chmod o-x dir1
```

- لو عملنا تاني ls -ld dir1 ف هنلاحظ ان ال other بقي ليه read permissions بس

```
[root@MohamedAtef home]# ls -ld dir1
drwxr-xr--. 2 root root 6 Jul 15 20:36 dir1
```

- هنعمل create لبعض ال files في ال dir1

```
[root@MohamedAtef dir1]# touch file1 file2 file3
[root@MohamedAtef dir1]# ls
file1  file2  file3
```

- احنا قولنا ان تاثير ال read permission علي ال directory ان انا مسموح ليا بس ان انا اعمل List لل files الموجوده في ال directory ف انا عندي read بس علي ال other ف كده اي user مش هيقدر غير انه يعمل list فقط علي الdir1
- ف لو عملنا ls ل dir1 باستخدام اي user تاني غير ال root وليكن mohamed هنلاحظ انه عمل list لل file name الموجوده عندي بس مطلعلي Permissions denied معناها انه بيقولك خلي بالك ان اخرك انك تشوف ال file name بس انت ملكش غيرread permissions علي ال directory ده ف مش هتعرف معلومات اكتر عن ال files غير اسمهم بس

```
[mohamed@MohamedAtef home]$ ls dir1
ls: cannot access 'dir1/file1':  Permission denied
ls: cannot access 'dir1/file2': Permission denied
ls: cannot access 'dir1/file3': Permission denied
file1  file2  file3
```

- حتي لو حاولت انك تدخل جوه ال directory هيقولك Permissions deny

```
[mohamed@MohamedAtef home]$ cd dir1/
-bash: cd: dir1/: Permission denied
```

- لو انا عايز اضيف execute permission علي dir1 هقوله o+x

```
[root@MohamedAtef home]#  chmod o+x dir1
```

- ف لو جينا عملنا ls -l علي dir1 هنلاقيه عمل List لل files اللي عندي وجايبلي more details عن ال files دي واقدر ادخل جوه ال directory ده واعمل list بس مقدرش اعمل create ل اي files او directory علشان هو واخد read وexecute ومش واخد write ف علشان اقدر اعمل create لازم اديله write permissions

```
[mohamed@MohamedAtef home]$ ls -l dir1/
total 0
-rw-r--r--. 1 root root 0 Jul 15 21:51 file1
-rw-r--r--. 1 root root 0 Jul 15 21:51 file2
-rw-r--r--. 1 root root 0 Jul 15 21:51 file3
```

- ف لو عملنا create ل اي file في dir1 زي ماقولنا هيقولك permission denied لان انت معندكش اي permissions انك ت create او ت delete اي files موجوده عندك مش مديله write permission

```
[mohamed@MohamedAtef dir1]$ touch file
touch: cannot touch 'file': Permission denied
```

- ف علشان تقدر ت create او ت delete لازم تدي لل directory ده write permission لل other

```
[root@MohamedAtef home]#  chmod o+w dir1
```

- لو عملنا ls -l علي dir1 هنلاقي انه ال Other ليه rwx

```
[root@MohamedAtef home]# ls -l
total 0
drwxr-xrwx. 2 root root 45 Jul 15 21:51 dir1
```

- ف لو جيت دلوقت عمل create ل اي file هيعمل create عادي جدا ف هنلاقي ان ال user owner وال group owner هو Mohamed علشان Mohamed هو اللي عمل create لل file4

```
[mohamed@MohamedAtef dir1]$ touch file4
[mohamed@MohamedAtef dir1]$ ls -l
total 0
-rw-r--r--. 1 root    root    0 Jul 15 21:51 file1
-rw-r--r--. 1 root    root    0 Jul 15 21:51 file2
-rw-r--r--. 1 root    root    0 Jul 15 21:51 file3
-rw-r--r--. 1 mohamed mohamed 0 Jul 15 22:43 file4
```

- انت ليك Permission علي dir1 انك تعمل create او تعمل remove ل اي files بس ملكش permissions انك ت add في ال content بتاعت ال file ف لو حاولت انك تضيف في ال file هيقولك permission denied علشان انت ملكش اي write permissions علي ال file انت ليك بس read

```
[mohamed@MohamedAtef dir1]$ echo "Hello World" > file1
-bash: file2: Permission denied
```

- ف علشان ت add في ال content بتاعت ال files لازم يكون ليك write permissions ف باستخدام ال root هندي write permission لل other

```
[root@MohamedAtef dir1]#  chmod o+w file1
```

- لو حاولنا اننا ن add في ال content تاني مش هيظهر عندنا اي مشكله وهيعمل add بكل سهوله علشان ال other ليهم write علي ال file1

```
[mohamed@MohamedAtef dir1]$ echo "Hello World" > file1
[mohamed@MohamedAtef dir1]$  cat file1
Hello World
```

- لو انت ليك write permission بس ف انت تقدر انك تmodify او ت change ال content بتاعت ال file بتاعك من بره ولكن متقدرش تدخل او تفتح ال file باستخدام ال vim editor و ت modify فيه لان انت عندكwrite بس معندكش read ف علشان تدخل علي ال file باستخدام vim لازم يكون عنك علي الاقل read علشان تقدر تشوف ال content وت modify فيه

- لو انت عايز ت change ال Permission بتاعت ال user وال group وال other مع بعض

```
[root@MohamedAtef home]# chmod u-wx,g-x,o-wx dir1
```

- او ممكن استخدم اوبشن a بمعني all وليكن مثلا هدي write لكل الناس ال other وال group وال user

```
[root@MohamedAtef home]# chmod a+w dir1
```

- لو انا عايز اعمل remove لكل ال permissions اللي موجوده عندي واعمل replace لكل اللي موجود ب execute permission علي طول بدل اما اعمل remove وبعدين اعمل add هستخدم يساوي=

```
[root@MohamedAtef home]# chmod a=x dir1
```

- لو عملنا ls -l ل dir1

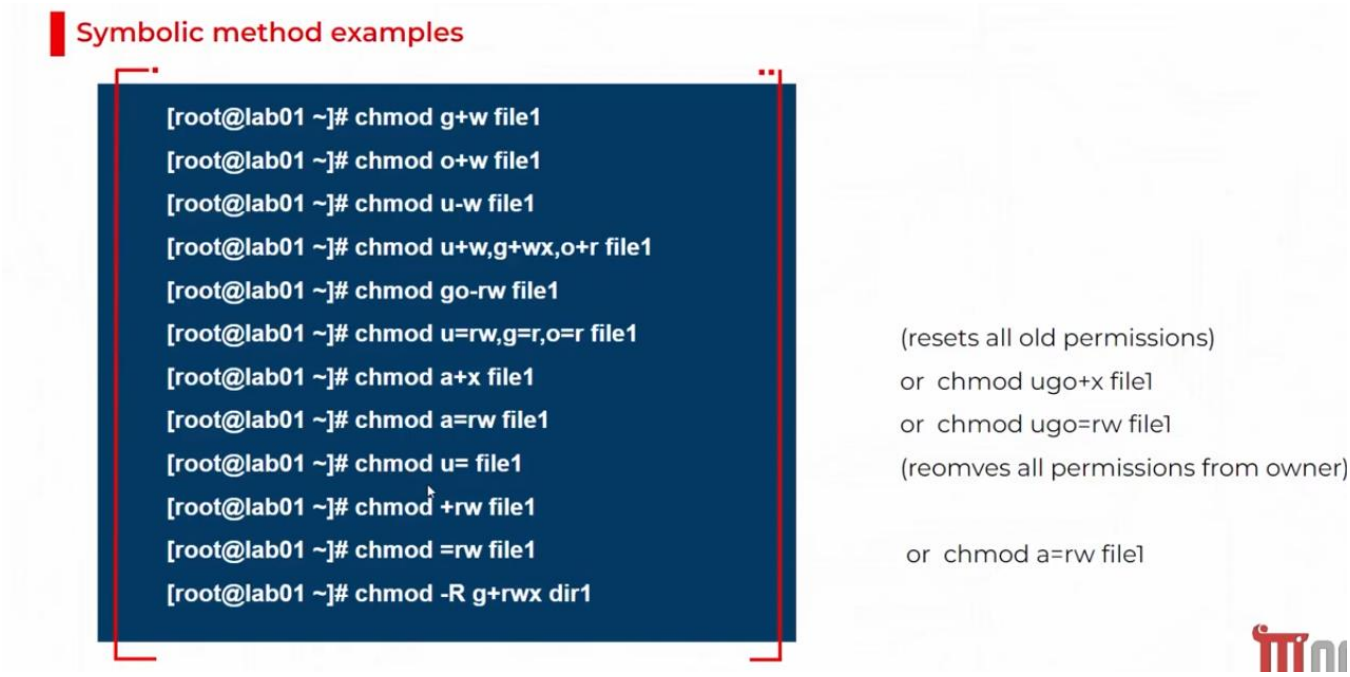
```
[root@MohamedAtef home]# ls -ld dir1
d--x--x--x. 2 root root 58 Jul 15 22:43 dir1
```

- لو انا اعمل remove لكل ال permissions هستخدم a=-

```
[root@MohamedAtef home]# chmod a=- dir1
```

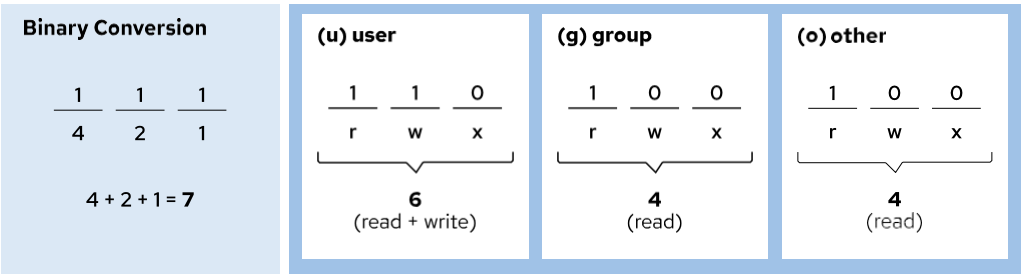
- لو انا عايز ادي permission ل directory بكل ال folders اللي تحتيه اذا كانت files او directories ف هستخدم اوبشن -R ومعناها recursive

```
[root@MohamedAtef home]# chmod -R o+rwx dir1
```



Numeric method -2

- تاني طريقه وهي الطريقه ال numeric



- في الطريقه دي بيكون عندي 3 ارقام بيعبروا عن ال Permissions زي مثلا 644 ف انا عندي اول رقم عندي بيعبر عن ال permissions بتاعت ال user owner وتاني رقم بيعبر عن ال permissions بتاعت ال group owner وتالت رقم بيعبر عن ال permissions بتاعت ال other
  - ف انا عندي ال read permissions بيعبر عنها ب رقم 4
  - وال write permissions بيعبر عنها برقم 2
  - وال execute permissions بيعبر عنها برقم 1
- ف مثلا علشان ادي permissions لل user وليكن انا عايز ادي للuser مثلا read و write ف انا بشوف ال read بيعبر عنا برقم كام وهو 4 وال write بيعبر عنها برقم كام وهو 2 وبعدين اجمع الرقمين دول هيكونوا ب 6 يبقي ال permissions اللي هياخدها ال user هي 6 ورقم 6 بيعبر عن ان ال user واخد read وwrite لان ال read + write بيساوي 6
  - ولو مثلا عايز ادي read permissions لل group يبقي اشوف ال read بيعبر عنها ب ايه بيعبرعنها برقم 4
  - لو انا عايز ادي full permissions لل user وال group وال other هيكونوا 777 ليه علشان انا عندي ال read ب 4 وال write ب 2 وال execute ب 1 مجموعهم كلهم ب 7
    - هنشوف مثال انا عندي directory اسمه dir1 وdir1 ده معلهوش اي permissions زي ماحنا شايفين

```
[root@MohamedAtef home]# ls -l
total 0
d---------. 2 root root 58 Jul 15 22:43 dir1
```

    - لو انا عايز ادي read و write ل ال user علي dir1

```
[root@MohamedAtef home]# chmod 6 dir1
```

    - لو انا عايز ادي read ل ال user هستخدم 4 وادي read و write و execute لل group هستخدم7

```
[root@MohamedAtef home]# chmod 47 dir1
```

    - لو انا عايز ادي full permissions

```
[root@MohamedAtef home]# chmod 777 dir1
```

    - لو عملنا ls -l هنلاقيهم كلهم واخدين full permissions

```
[root@MohamedAtef home]# ls -l
total 0
drwxrwxrwx. 2 root root 58 Jul 15 22:43 dir1
```

Required permissions

Command	Source directory	Source file	Target Directory
cd	x	N/A	N/A
ls	x, r	N/A	N/A
mkdir, rmdir	x, w	N/A	N/A
cat, less	x	r	N/A
cp	x	r	x, w
cp -r	x, r	r	x, w
mv	x, w	none !!!	x, w
vi	x, r	r, w	N/A
rm	x, w	none !!!	N/A

- دي كده ال minimum permissions المطلوبه علشان تقدر تعمل task معينه او ت run command معينه
- لو نفترض ان انت عندك source directory وعايز تدخل جوه ال directory ده ف علشان تقدر تعمل **cd** وتدخل جواه يبقي لازم علي الاقل يكون عندك execute permissions
- ولو عايز اعمل List لل files names اللي عندي لازم يكون عندي الاقل read and execute permissions علشان اقدر اعمل list واستخدم**ls command**
- لو انت عايز ت create وت remove اي directory باستخدام ال **mkdir** وال **rmdir** لازم يكون عندك علي الاقل علي ال execute and write permissions علي ال directory
- لو انت عايز ت display ال content بتاعت file معين باستخدام مثلا **cat** او **less** ف لازم اعمل حاجتين او حاجه انت عندك ال file ده موجود جوه directory ف انت لازم يكون عندي علي الاقل execute علي ال directory اللي جواه ال file علشان تقدر انك تدخل وت access ال file ده تاني حاجه لازم يكون عندكread علي ال file علشان تقدر ت display ال content بتاعت ال file
- لو انت عايز تعمل copy ل file باستخدام **cp** انت هتعمل **cp** من ال source directory ل target directory او ال destination ف انت علي ال source directory لازم يكون عندك علي الاقل execute permissions وعلي ال file ذات نفسه لازم يكون عليه read permissions وعلي ال target directory لازم يكون عليه write و execute
- لو انت هتعمل copy ل directory باستخدام **cp -r** هتكون نفس ال permissions في حاله ال **cp** بس هنزودread permissions في حاله ال source directory
- لو انا عايز اعمل move من directory ل directory تاني باستخدام **mv** ف انت محتاج write و execute علي كل من ال source directory وال target directory
- علشان تفتح file باستخدام **vi** وتعمل edit عليه لازم ال file اللي هتعمل عليه edit لازم يكون ليك عليه read و write ولازم يكون ليك علي ال source directory اللي فيه ال file يكون عليه read و execute

Changing file and directory user or group ownership

- Only root can change the ownership of a file.
- Root or the file's owner can change group ownership.

```
[root@lab01 ~]# chown karim file1
[root@lab01 ~]# chown karim dir1
[root@lab01 ~]# chown -R karim dir1
[root@lab01 ~]# chown :sales file1
[root@lab01 ~]# chgrp sales file1
[root@lab01 ~]# chown karim:sales file1
[root@lab01 ~]# chown -R karim:sales dir1
```

(change the group ownership)
(change the group ownership)
(change the owner and group)

- علشان نعمل change ل ownership بتاعت ال file وال directory انا عندي two command عندي command اسمه **chown** وcommand اسمه **chgrp**
  - انا عندي file اسمه file1 ال file ده ال user owner وال group owner بتاعه هو ال root

```
[root@MohamedAtef dir1]# ls -l
total 4
-rw-r--rw-. 1 root root 12 Jul 15 23:01 file1
```

  - ف لو انا عايز اغير ال user owner هتستخدم **chown** وبعدين اسمه ال user owner وبعدين اسم ال file

```
[root@MohamedAtef dir1]# chown mohamed file1
```

  - لو عملنا **ls -l** تاني هنلاقي ال user owner اتغير من root ل Mohamed

```
[root@MohamedAtef dir1]# ls -l
total 4
-rw-r--rw-. 1 mohamed root 12 Jul 15 23:01 file1
```

  - لو انا عايز اغير ال group owner هستخدم **chgrp**

```
[root@MohamedAtef dir1]# chgrp mohamed file1
[root@MohamedAtef dir1]# ls -l
total 4
-rw-r--rw-. 1 mohamed mohamed 12 Jul 15 23:01 file1
```

  - لو انا عايز اعمل change ل ال user owner وال group owner في نفس ال Line مره واحده هستخدم **chown** وبعدين احدد اول حاجه ال user owner وبعدين ال group owner واحط مابينهم : وبعدين ال file

```
[root@MohamedAtef dir1]# chown root:root file1
```

  - لو انا عايز احدد ال group owner باستخدام ال **chown**

```
[root@MohamedAtef dir1]# chown   :mohamed file1
```

  - لو انا عايز أ change ال ownership بتاعت ال directory بكل ال content اللي تحتيه هستخدم اوبشن **-R**

```
[root@MohamedAtef dir1]# chown -R  mohamed:mohamed dir1
```

Special permissions

- Special permissions provide additional access-related features over and above what the basic permission types allow. This section details the impact of special permissions, summarized in the table below.

SPECIAL PERMISSION	EFFECT ON FILES	EFFECT ON DIRECTORIES
u+s (suid)	File executes as the user that owns the file, not the user that ran the file.	No effect.
g+s (sgid)	File executes as the group that owns the file.	Files newly created in the directory have their group owner set to match the group owner of the directory.
o+t (sticky)	No effect.	Users with write access to the directory can only remove files that they own; they cannot remove or force saves to files owned by other users.

- هنتكلم عن حاجه اسمها **Special Permissions** وايه هي ال effect بتاعها علي ال files وال directories
- انا عندي 3 انواع من ال Special Permissions

1- اول نوع وهو set user id او suid بستخدمها عن طريق اوبشن u+s

- ال suid ملهاش اي تاثير علي ال Directories ليها بس تاثير علي ال file لانها بتكون applied علي ال file يعني وانت بت execute ال file ف انت هتاخد ال permissions بتاعت ال owner بتاعت ال file ذات نفسه ولو ال owner بتاع ال file هو ال root ف انت هاخد ال permission بتاعت ال root

2- تاني نوع وهو set group id او sgid بستخدمها عن طريق اوبشن g+s

- ال sgid بتكون applied علي ال files وال directories
- تاثيرها علي ال file كان انت ال group owner بتاع ال file انت هتاخد نفس ال permissions اللي group owner واخدها تحس انها شبه ال suid بس في ال suid انت بتاخد permissions ال owner نفسه بتاع ال file اما ال sgid بتاخد permission ال group owner
- تاثيرها علي ال Directory لو انت عندك مثلا directory عليه sgid وانت عملت create لأي file جوه ال directory ده في ال file اللي اتعملها create جوه ال directory هتاخد نفس ال group owner بتاع ال directory

3- تالت نوع وهو ال Sticky bit او sticky بستخدمها عن طريق اوبشن o+t

- ال sticky bit بتكون permissions applied علي ال Other
- ملهاش اي تاثير علي ال files
- وتاثيرها علي ال Directories ان كل واحد يقدر ي remove ال files بتاعته وميقدرش يمسح ال file الخاصه باي user تاني

Setting Special Permissions

- Symbolically: setuid = u+s; setgid = g+s; sticky = o+t
- Numerically (fourth preceding digit): setuid = 4; setgid = 2; sticky = 1

Examples

- Add the setgid bit on directory:

```
[user@host ~]# chmod g+s directory
```

- Set the setgid bit and add read/write/execute permissions for user and group, with no access for others, on directory:

```
[user@host ~]# chmod 2770 directory
```

- لو انا عايز اعمل setting لل Special Permissions فيه عندي طريقتين ي اما استخدم الطريقه ال Symbolically ي الطريقه ال Numerically
- لو هستخدم الطريقه ال symbolically عن طريق ان انا لو عايز اعمل add ل **setuid** هستخدم **u+s** ولو عايز اعمل add ل **setgid** هستخدم **g+s** ولو عايز اعمل add لل **sticky** هستخدم **o+t**
- ولو انا عايز اعمل remove ل **setuid** هستخدم **u-s** ولو عايز اعمل remove ل **setgid** هستخدم **g-s** ولو عايز اعمل remove ل **sticky** هستخدم **o-t**
- احنا في الطريقه ال Numerically العاديه بيكون فيه 3 ارقم بس ف علشان تعمل add هنزود علي الشمال رقم كمان ي ازود 4 او 2 او 1 ف لو **4** معناها **setuid** ولو **2** معناها **setgid** ولو **1** معناها **sticky**

Setuid

- **setuid** permission on an executable file means that commands run as the user owning the file, not as the user that ran the command.
- One example is the **passwd** command:

```
[user@host ~]$ ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 32648 Aug 10  2021 /usr/bin/passwd
```

- In a long listing, you can identify the setuid permissions by a lowercase s where you would normally expect the x (owner execute permissions) to be. If the owner does not have execute permissions, this is replaced by an uppercase **S**.

- هنشوف Example علي **setuid**

- احنا عارفين ان كل ال Password Information بتاعت ال users بتكون موجوده في ال /etc/shadow لو جينا عملنا **ls -l** علي ال file اللي اسمه shadow لو بصينا هنلاقي ان مفيش اي حد ليه اي permissions علي ال file نفسه

```
[root@MohamedAtef ~]# ls -l /etc/shadow
----------. 1 root root 1940 Jul 13 14:55 /etc/shadow
```

- طب ازاي انا ك user بقدر اني اغير الباسورد بتاعتي انا اه ليا execute permission علي ال command اللي اسمه passwd بس انا لما بغير الباسورد ل باسورد جديده هو بيعمل update للباسورد الجديده في ال /etc/shadow طب ازاي هيعمل update وانا مليش اي permissions علي ال file اللي اسمه shadow ف من هنا ظهرت قصه ال special permissions

- ف لو جيت عملت **ls -l** علي /usr/bin/passwd هنلاقي مكان ال user permissions هنلاقيه مكان ال **x** فيه **s** ال **s** دي معناها ان ال command ده عليه **suid** permissions معناها ان اي regular user هيروح ي run ال command ده هياخد permissions ال owner اللي هو ال root لان ال root واخد Permissions علي /etc/shadow ف علشان كده انا ك user بقدر اني اغير الباسورد بتاعتي

```
[root@MohamedAtef ~]# ls -l /usr/bin/passwd
-rwsr-xr-x. 1 root root 32648 Aug 10  2021 /usr/bin/passwd
```

- لو انا عايز اضيف **suid** علي ال files هقوله **chmod** وبعدين **u+s**

```
[root@MohamedAtef ~]# chmod u+s /usr/bin/passwd
```

- لو انا عايز احذف ال **suid** من علي اي fileهقوله **chmod** وبعدين **u-s**

```
[root@MohamedAtef ~]# chmod u-s /usr/bin/passwd
```

Setgid

- The special permission **setgid** on a directory means that files created in the directory inherit their group ownership from the directory, rather than inheriting it from the creating user.
- An example of this is the **/run/log/journal** directory:

```
[user@host ~]$ ls -ld /run/log/journal
drwxr-sr-x+ 3 root systemd-journal 60 Sep 24 16:21 /run/log/journal
```

- احنا قولنا ان ال setgid بتتطبق علي ال files وال Directories

- انا مثلا directory تحت /run/log اسمه journal لو عملنا ls -ld علي ال directory ده هنلاقي مكان ال group owner محطوط **s** معناها ان ال directory ده متطبق عليه setgid permissions هنلاقي كمان ال group owner اسمه system-journal معناها ان انت اي file عملتله create جوه ال directory ده هياخد نفس ال group owner بتاع ال parent بتاعه

```
[root@MohamedAtef ~]# ls -ld /run/log/journal/
drwxr-sr-x+ 3 root systemd-journal 60 Jul 16 18:23 /run/log/journal/
```

Sticky bit

- The **sticky bit** for a directory sets a special restriction on deletion of files. Only the owner of the file (and root) can delete files within the directory. An example is **/tmp**:

```
[user@host ~]$ ls -ld /tmp
drwxrwxrwt. 16 root root 4096 Sep 28 03:37 /tmp
```

Default file permissions

- When you create a new file or directory, it is assigned initial permissions. There are two things that affect these initial permissions.
- The first is whether you are creating a **regular file** or a **directory**. The second is the current **umask**.
- The **umask** command without arguments will display the current value of the shell's umask:

```
[root@client ~]# umask
0022
[karim@client ~]$ umask
0002
```

- انا عندي اي new created file او directory بي assigned ليه initial permissions او بنقول عليها default permissions ف ال default permissions علي اي file او directory هي مش حاجه عشوائيه لا احنا نقدر ن control ال default permissions اللي اي new file او directory هياخدها عن طريق حاجه اسمها **umask** ف انا لو جيت عملت run ل command اسمه **umask** بدون اي value ف هو هيعرضلي ال default umask في حاله ال root او ال regular user او superuser انا في حاله ال root ال **umask** بيكون **0022** وفي حاله ال user العادي بيكون **0002** ال zero اللي علي الشمال ده ليه علاقه بال special permission ومعني ال zero هنا ان ال special permission not set

- ف لو عملنا **umask** علي ال root هنلاقي ال default mask عندي هي 0022

```
[root@MohamedAtef ~]# umask
0022
```

- لو عملنا umask علي اي user تاني هنلاقي ان ال default umask عندي هي 0002

```
[mohamed@MohamedAtef root]$ umask
0002
```

- ازاي احسب ال **umask** علي ال file

	Symbolic	Numeric octal	Numeric binary
Initial file permissions	rw-rw-rw-	0666	000 110 110 110
umask	-------w-	0002	000 000 000 010
Resulting file permissions	rw-rw-r--	0664	000 110 110 100

- انا عندي اقصي permissions ممكن ال Normal User انه ياخدها علي ال file هي 666 اللي هي rw لل user و rw لل group و rw لل others
- ف علشان احسب ال permissions اللي علي ال file عن طريق ان انا بنقص ال permissions بتاعت ال file من ال **umask** يعني 666 – 002 = 664 يبقي 664 هي دي ال default permissions اللي ال normal user هياخدها علي ال file اللي هي rw-rw-r--

- ازاي احسب ال **umask** علي ال directory

	Symbolic	Numeric octal	Numeric binary
Initial directory permissions	rwxrwxrwx	0777	000 111 111 111
umask	-------w-	0002	000 000 000 010
Resulting directory permissions	rwxrwxr-x	0775	octal 111 111 101

- عندي اقصي permissions ممكن ال Normal User انه ياخدها علي ال directory هي 777 اللي هي rwx لل user و rwx لل group و rws لل others
- نفس الكلام علشان احسب ال permissions اللي علي ال directory عن طريق ان انا بنقص ال permissions بتاعت ال directory من ال **umask** يعني 777 – 002 = 775 يبقي 775 هي دي ال default permissions اللي ال normal user هياخدها علي ال directory

Default file permissions

- The system's default umask values for Bash shell users are defined in the **/etc/profile** and **/etc/bashrc** files .
- Users can override the system defaults in the **.bash_profile** and **.bashrc** files in their home directories.

```
[karim@client ~]$ echo "umask 007" >> ~/.bashrc
```

(Log out and log in again)

- ال **umask** من ال CLI بيديك effect في ال current bash اللي انت فاتحها ف لو انت عايز تت change ال **umask** ويكون permanent في عندي في ال home directory فيه file اسمه **.bashrc** و file تاني اسمه **.bash_profile** ال Two Files دول هتلاقيهم hidden في ال home directory ف انا بحط ال umask الجديد في اي file من ال two files دول علشان يكون permanent
- **.bashrc** ده جوه مجموعه من ال commands او الاسكريبت بيتعمله run كل مره انا بفتح bash جديده
- **.bash_profile** بيتعمله run مره واحده وانا بعمل login
- ال default values بتاعت ال umask هتلاقيها موجوده في **/etc/profile** و **/etc/bashrc** ومش recommended ان انت تغيرفي ال default values الموجوده في ال files دي علشان لو احتجت ان انت ت rollback ال change اللي انت عملته في ال hidden files بتاعتك ترجع لل default values الموجوده عندك ف ال recommended ان انت تغير في ال **.bashrc** و **.bash_profile**
- فيه عندي طريقتين علشان اخلي ال umask بتاعي permanent ي اما عن طريق ان انا افتح ال **.bashrc** او **.bash_profile** بال vim editor واكتب في اي line ال umask بتاعي
- ي اما عن طريق ال CLI هكتب ال command باستخدام ال echo

```
mohamed@MohamedAtef:~$ echo "umask 007" >> ~/.bashrc
```

Chapter 8

Monitoring and Managing Linux Processes

Monitoring and Managing Linux processes

- A process is a running instance of a launched, executable program.
- Every new process is assigned a unique process ID (PID) for tracking and security.
- The PID and the parent's process ID (PPID) are elements of the new process environment.
- Any process may create a child process.

- مبدئيا ال Process عباره عن program in execution يعني اي Program معمول ليه Install عندك و not running دلوقتي هو كده مفيش اي Process running بمجرد ان انت عملت run هيكون فيه process معمول ليها run وليها Process ID(PID) وloaded في ال memory وواخده من ال CPU وال Disk زي اي برنامج عندك في الويندوز لو عامله Install
- انا عندي اي ىnew process بي assigned ليها Process ID بيبقي رقم unique علشان السيستم يقدر ي track ال process دي بي assigned ليها process ID
- PID دي انا بستخدمها علشان اتحكم في ال Process بتاعتي زي مثلا عايز اعمل Termination لل Process ف بستخدم ال PID
- كل Process عندي بيبقي ليها Parent Process يعني مثلا انا دلوقتي فاتح الباش او Terminal او ال CLI ما الباش ده عباره عن application بمجرد ان انا فتحت الباش بقي عندي running process دلوقتي للباش طب لو من جوه الباش ذات نفسها فتحت اي application تاني عملت مثلا execute ل command معين بقي عندي كده process تانيه لما عملت execute لل command طب ال process دي مين ال parent process بتاعتها هي الباش

Listing processes

- The **ps** command is used for listing current processes. It can provide detailed process information, including:
  - User identification (UID), which determines process privileges
  - Unique process identification (PID)
  - CPU and real time already expended
  - How much memory the process has allocated in various locations
  - The location of process stdout, known as the controlling terminal
  - The current process state

- علشان اعمل List لكل ال Processes ال running عندي في السيستم بستخدم command اسمه **ps** وفيه options كتير مع ال command نفسه
- لو انت قولتله **ps** بس هيعرضلك ال processes ال running عندك في ال current terminal بتاعتك و هيعرضلك مين هو ال owner بتاع ال Process دي ال UID بتاعه او اسمه وهيقولك ال PID وكمان هيعرضلك ال CPU وال memory وال State بتاعت ال process هل هي running او stopped او witting او Terminated

- لو عملت **Ps** هيقولك ال current process في ال current terminal بتاعتك . ال ps command بي list ال running processes مره واحده بس ف لما نفذت ال **ps** قالك ان ال bash دلوقتي running وال process ID (PID) بتاعتها 1870 وTTY المكان اللي هي running منه اللي هي pts/0 وال TIME

```
[root@MohamedAtef ~]# ps
  PID TTY      TIME CMD
 1870 pts/0    00:00:00 bash
 1969 pts/0    00:00:00 ps
```

- طب هو عرف منين ال Process ID (PID) بتاعت ال bash فيه عندي command اسمه **echo $$** ال **$$** ده عباره عن shell variable بيكون stored جواه ال Process ID بتاعت ال Current bash بتاعتك ف لو نفذت ال command هيعرضلكPID وهو 1870

```
[root@MohamedAtef ~]# echo $$
1870
```

- The most common set of options, **aux**, displays all processes including processes without a controlling terminal. A long listing (options **lax**) provides more technical detail. The similar UNIX syntax uses the options **-ef** to display all processes

```
[user@host ~]$ ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.1  0.1  51648  7504 ?        Ss   17:45   0:03 /usr/lib/systemd/
syst
root         2  0.0  0.0      0     0 ?        S    17:45   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S    17:45   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   17:45   0:00 [kworker/0:0H]
root         7  0.0  0.0      0     0 ?        S    17:45   0:00 [migration/0]
...output omitted...
[user@host ~]$ ps lax
F   UID   PID  PPID PRI  NI    VSZ   RSS WCHAN  STAT TTY     TIME COMMAND
4     0     1     0  20   0  51648  7504 ep_pol Ss   ?       0:03 /usr/lib/
systemd/
1     0     2     0  20   0      0     0 kthrea S    ?       0:00 [kthreadd]
1     0     3     2  20   0      0     0 smpboo S    ?       0:00 [ksoftirqd/0]
1     0     5     2   0 -20      0     0 worker S<   ?       0:00 [kworker/0:0H]
1     0     7     2 -100  -      0     0 smpboo S    ?       0:00 [migration/0]
...output omitted...
[user@host ~]$ ps -ef
UID        PID  PPID  C STIME TTY          TIME CMD
root         1     0  0 17:45 ?        00:00:03 /usr/lib/systemd/systemd --
switched-ro
root         2     0  0 17:45 ?        00:00:00 [kthreadd]
root         3     2  0 17:45 ?        00:00:00 [ksoftirqd/0]
root         5     2  0 17:45 ?        00:00:00 [kworker/0:0H]
root         7     2  0 17:45 ?        00:00:00 [migration/0]
...output omitted...
```

- فيه عندي كذا options وكل Option فيهم بي List ال Processes ويجبلي Details معينه فيه اوبشن اسمه **ps aux** واوبشن تاني اسمه **ps lax** واوبشن تاني اسمه **ps -ef** كل واحد فيهم بيعرض more details عن التاني
- اول اوبشن وهو **ps aux** وده هيعرضلك columns وكل column بيعبر عن حاجه معينه زي مثلا

- **USER** : The user who owns the process.
- **PID** : The process ID.
- **%CPU** : The percentage of CPU usage.
- **%MEM**: The percentage of memory usage.
- **VSZ** : Virtual memory size in kilobytes.
- **RSS** : Resident Set Size, the non-swapped physical memory the process is using, in kilobytes.
- **TTY** : The terminal associated with the process (if any).
- **STAT** : The process state code.
- **START** : The time the process started.
- **TIME** : The cumulative CPU time the process has used since it started.
- **COMMAND**: The command that started the process.

- ف علشان تعرض كل ال Processes اللي عندك استخدم ps aux

```
[root@MohamedAtef ~]# ps aux
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  1.4 173236 10828 ?        Ss   Jul18   0:05 /usr/lib/systemd/system
root         2  0.0  0.0      0     0 ?        S    Jul18   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        I<   Jul18   0:00 [rcu_gp]
root         4  0.0  0.0      0     0 ?        I<   Jul18   0:00 [rcu_par_gp]
```

- لما استخدم **ps aux** هيعرضلي كل ال processes ف ممكن استخدم ال pipeline | مع less علشان يعرضلي ال process page by page

```
[root@MohamedAtef ~]# ps aux  | less
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  1.4 173236 10828 ?        Ss   Jul18   0:05 /usr/lib/systemd/system
root         2  0.0  0.0      0     0 ?        S    Jul18   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        I<   Jul18   0:00 [rcu_gp]
root         4  0.0  0.0      0     0 ?        I<   Jul18   0:00 [rcu_par_gp]
```

- تاني اوبشن وهو **ps lax** وده هيعرضلك columns وكل column بيعبر عن حاجه معينه زي مثلا
  - **F**: Fags associated with the process.
  - **UID**: User ID of the process owner.
  - **PID**: Process ID.
  - **PPID**: Parent process ID.
  - **C**: CPU usage (obsolete).
  - **PRI**: Priority of the process.
  - **NI**: Nice value, which affects scheduling priority.
  - **VSZ**: Virtual memory size of the process (in kilobytes).
  - **RSS**: Resident Set Size, the non-swapped physical memory used by the process (in kilobytes).
  - **WCHAN**: If blank, the process is running; otherwise, this column indicates the address in the kernel where the process is sleeping.
  - **STAT**: Process state (e.g., R for running, S for sleeping).
  - **TTY**: Terminal associated with the process.
  - **TIME**: Total CPU time the process has used since it started.
  - **CMD**: Command that initiated the process.

```
[root@MohamedAtef ~]# ps lax
F   UID   PID  PPID PRI  NI   VSZ   RSS    WCHAN  STAT  TTY      TIME   COMMAND
4     0     1     0   20   0 173236 10828  ep_pol    Ss    ?      0:06   /usr/lib/systemd/
1     0     2     0   20   0     0     0   kthrea     S    ?      0:00   [kthreadd]
1     0     3     2    0 -20     0     0   rescue     I<   ?      0:00   [rcu_gp]
1     0     4     2    0 -20     0     0   rescue     I<   ?      0:00   [rcu_par_gp]
```

- تاني اوبشن وهو **ps -ef** وده هيعرضلك columns وكل column بيعبر عن حاجه معينه زي مثلا
  - **UID**: Indicates which user owns the process.
  - **PID**: Helps in identifying and managing specific processes.
  - **PPID**: Shows the relationship between processes.
  - **C**: Gives a rough estimate of how much CPU the process is using.
  - **STIME**: Can help determine when the process started, useful for identifying long-running processes.
  - **TTY**: Helps identify if the process is associated with a terminal.
  - **TIME**: Shows how much CPU time the process has consumed.
  - **CMD**: Provides the command line used to start the process, helpful in understanding the purpose of the process.

```
[root@MohamedAtef ~]# ps -ef
UID        PID   PPID  C STIME TTY        TIME      CMD
root        1     0     0 Jul18   ?        00:00:06  /usr/lib/systemd/systemd rhgb --switch
root        2     0     0 Jul18   ?        00:00:00  [kthreadd]
root        3     2     0 Jul18   ?        00:00:00  [rcu_gp]
root        4     2     0 Jul18   ?        00:00:00  [rcu_par_gp]
```

- The output of **ps** displays once. Use **top** for a process display that dynamically updates.
- **ps** can display in tree format using **pstree** so you can view relationships between parent and child processes.
- PID #1 is for **systemd** (the first process in the system) ---> like initd in RHEL6 :)

```
[root@lab01 ~]# pstree                    (process status tree)
OR
[root@lab01 ~]# ps fax                    (process status tree)
[root@lab01 ~]# pstree -p                 (Display PID of each process)
[root@ lab01 ~]# pstree -p karim
[root@lab01 ~]# pgrep -u user -l          (Show process name of a specific user)
```

- لو انا عايز اعمل mounter لل processes بتاعتي في ال real time بستخدم command اسمه **top**
- لو استخدمت **top** هيعرضلي كل ال processes الموجوده عندي في ال real time ال **top** ده شبه ال task manager الموجود في ال windows

```
[root@MohamedAtef ~]# top
  PID USER     PR  NI   VIRT   RES   SHR  S  %CPU %MEM     TIME+    COMMAND
 2090 root     20   0  226012  4180  3300  R  2.3   0.5    0:01.97     top
  792 root     20   0  530012  9028  4348  S  0.3   1.2    0:46.58   vmtoolsd
 1990 root     20   0       0     0     0  I  0.3   0.0    0:00.82   kworker/u256:4-ev+
```

- فيه command تاني شبه ال **ps** اسمه **pstree** ده يعمل List لكل ال running processes في السيستم بس في شكل tree

```
[root@MohamedAtef ~]# pstree
systemd─┬─ModemManager───3*[{ModemManager}]
        ├─NetworkManager───2*[{NetworkManager}]
        ├─VGAuthService
        ├─accounts-daemon───3*[{accounts-daemon}]
        ├─alsactl
        ├─at-spi-bus-laun─┬─dbus-daemon
        │                 └─3
```

- ممكن استخدم مع **pstree** اوبشن **-p** علشان يعرضلي ال PID

```
[root@MohamedAtef ~]# pstree -p
systemd(1)─┬─ModemManager(831)─┬─{ModemManager}(850)
           │                   ├─{ModemManager}(851)
           │                   └─{ModemManager}(856)
           ├─NetworkManager(989)─┬─{NetworkManager}(994)
           │                     └─{NetworkManager}(995)
           ├─VGAuthService(791)
           ├─accounts-daemon(784)─┬─{accounts-daemon}(793)
           │                      ├─{accounts-daemon}(794)
```

- لو انا عايز اعرف ال processes ال running بتاعت user معين

```
[root@MohamedAtef ~]# pstree -p mohamed
sshd(2151)───bash(2156)
systemd(2125)───(sd-pam)(2134)
```

- او ممكن استخدم command اسمه pgrep علشان اعمل list لل processes بتاعت user معين

```
[root@MohamedAtef ~]# pgrep -u mohamed -l
2248 systemd
2257 (sd-pam)
2274 sshd
2276 bash
```

Controlling jobs

- Job control is a feature of the shell which allows a single shell instance to run and manage multiple commands.
- Only one job can read input and keyboard generated signals from a particular terminal window at a time. Processes that are part of that job are **foreground** processes of that controlling terminal.
- A **background** process of that controlling terminal is a member of any other job associated with that terminal. Background processes of a terminal cannot read input or receive keyboard generated interrupts from the terminal, but may be able to write to the terminal. A job in the background may be stopped (suspended) or it may be running. If a running background job tries to read from the terminal, it will be automatically suspended.
- Each terminal is its own session, and can have a **foreground** process and any number of independent **background** processes. A job is part of exactly one session: the one belonging to its controlling terminal.

- انا عندي نوعين من ال Processes نوع اسمه foreground ونوع تاني اسمه background
- ال foreground processes دي ال Processes اللي بيتقال عليها interactive processes او Process محتاجه Input معين من ال User
- لو في اي process تانيه مش interactive process او مش محتاجه اي Inputs من ال Users ف ممكن تعملها run في ال background لان لو انت عامل run لاي Process في ال foreground ف انت ساعتها مش هتعرف ت run اي commands تانيه من ال Terminal بتاعتك

- مثلا انا عندي command اسمه sleep لو انا قولتله مثلا sleep 100 كاني بقوله اعمل sleep ل 100 ثانيه لل terminal بتاعتي ف لو انا نفذت ال command ده انا مش هعرف انفذ اي command تاني من ال CLI لازم استني ال Process دي لحد اما تخلص ف ال process دي مش interactive مش محتاجه منك اي inputs ف انا ممكن اعملها run في ال background ف هتفضل running بس في ال background علشان اقدر استخدم ال Terminal

```
[root@MohamedAtef ~]# sleep 100
```

- انا لو انا مثلا عايز انفذ ال command ده ls -lR &>/tmp/all-files.txt ال command ده عباره عن ان انا عايزيه يعمل list لكل ال files الموجوده عندي في السيستم واعملها save في ال file اللي اسمه all-files.txt تحت /tmp في ال command ده علشان يتنفذ ال process هتاخد وقت كبير جدا ال command ده يعتبر interactive command

```
[root@MohamedAtef ~]# ls -lR &>/tmp/all-files.tx
```

- لو انا عايز اعمله run في ال background هنفذ نفس ال command واحط في الاخر علامه ال and اللي هي دي & هنلاقيه عارضلي ال PID اللي هي 2362 وعارضلي كمان ال Job ID اللي هي 1

```
[root@MohamedAtef ~]# ls -lR &>/tmp/all-files.tx &
[1] 2362
```

- علشان اعرض ال jobs اللي running عندي في ال background هستخدم command اسمه jobs

```
[root@MohamedAtef ~]#  jobs
[1]+  Running                 sleep 100 &
```

- In the preceding example, the **sleep** command is now running in the foreground on the controlling terminal. The shell itself is again asleep, waiting for this child process to exit.
- To send a foreground process to the background, first press the keyboard generated suspend request (**Ctrl+Z**) in the terminal.

```
sleep 10000
^Z
[1]+  Stopped                 sleep 10000
[user@host ~]$
```

- To start the suspended process running in the background, use the **bg** command with the same job ID.

```
[user@host ~]$ bg %1
[1]+ sleep 10000 &
```

- The **ps j** command displays information relating to jobs.

- لو انا في ال background وعايز ارجع process معينه في ال foreground هقوله **fg %** وبعدين ال Job ID

```
[root@MohamedAtef ~]# fg %1
sleep 100
```

- لو انا في ال foreground وعايز ارجع ال process بتاعتي في ال background هقوله **bg %** وبعدين ال Job ID

```
[root@MohamedAtef ~]# bg %1
sleep 100
```

- لو انا في ال foreground وعايز اعمل Terminate لل job هضغط علي **CTRL+C** ولو ضغط علي CTRL+Z هيعمل stop مؤقتا لحد اما ترجعها running في ال background
- في command تاني شبه ال command اللي اسمه jobs اسمه **ps j**

```
[root@MohamedAtef ~]# ps j
```

Killing processes

```
[root@master ~]# kill -l
[root@master ~]# pidof vim
4123
[root@master ~]# kill 4123
[root@master ~]# pidof vim
7073
[root@master ~]# kill -9 7073
[root@master ~]# kill -SIGKILL 7073

[root@master ~]# pkill vim
[root@master ~]# killall vim
[user@ master ~]$pkill -U user
```

(List all signals)

(Default is SIGTERM 15)

- kill -15 --> to terminate the process cleanly
- kill -9 --> aggressive termination (used in emergency termination but not recommended !)
- kill -1 --> SIGHUB --> to reload an re-read the configurations (configuration reload without termination)

(Default is SIGTERM 15)

- لو عايز اعمل kill ل process معينه بستخدم command اسمه **kill** هو بالاخص kill command مش بستخدمه بس علشان اعمل kill ل Process بستخدمه كمان لو عايز اعمل communicate مع Process معينه عايز مثلا اعمل Send ل Signal معينه ل process و according لل signal دي ال process دي هتعمل حاجه معينه according لل signal اللي جايلها
- **Kill** فيه مجموعه من ال Signal حوالي 64 Signal لو قولتله **kill -l** هيعمل List لكل ال Available Signal اللي عندي ممكن ت send signal معينه بالرقم بتاعها او من اسمها وكل signal عندك ليها استخدام معين اللي احنا هنشوفه وهنستخدمه هنشوف ال signal رقم 1 اللي اسمها SIGHUP وال signal رقم 9 اللي اسمها SIGKILL وال signal رقم 15 اللي اسمها SIGTERM

```
[root@MohamedAtef ~]# kill -l
 1) SIGHUP       2) SIGINT       3) SIGQUIT      4) SIGILL       5) SIGTRAP
 6) SIGABRT      7) SIGBUS       8) SIGFPE       9) SIGKILL     10) SIGUSR1
11) SIGSEGV     12) SIGUSR2     13) SIGPIPE     14) SIGALRM     15) SIGTERM
16) SIGSTKFLT   17) SIGCHLD     18) SIGCONT     19) SIGSTOP     20) SIGTSTP
21) SIGTTIN     22) SIGTTOU     23) SIGURG      24) SIGXCPU     25) SIGXFSZ
26) SIGVTALRM   27) SIGPROF     28) SIGWINCH    29) SIGIO       30) SIGPWR
31) SIGSYS      34) SIGRTMIN    35) SIGRTMIN+1  36) SIGRTMIN+2  37) SIGRTMIN+3
38) SIGRTMIN+4  39) SIGRTMIN+5  40) SIGRTMIN+6  41) SIGRTMIN+7  42) SIGRTMIN+8
43) SIGRTMIN+9  44) SIGRTMIN+10 45) SIGRTMIN+11 46) SIGRTMIN+12 47) SIGRTMIN+13
48) SIGRTMIN+14 49) SIGRTMIN+15 50) SIGRTMAX-14 51) SIGRTMAX-13 52) SIGRTMAX-12
53) SIGRTMAX-11 54) SIGRTMAX-10 55) SIGRTMAX-9  56) SIGRTMAX-8  57) SIGRTMAX-7
58) SIGRTMAX-6  59) SIGRTMAX-5  60) SIGRTMAX-4  61) SIGRTMAX-3  62) SIGRTMAX-2
63) SIGRTMAX-1  64) SIGRTMAX
```

- طب ايه الفرق بين ال signal دي وبعضها

- ال signal اللي اسمها SIGTERM دي بتعمل Terminate لل Process بتاعتك ف لو انت عايز ت End ال Signal تبعت Signal 15 وده بيكون ال default
- اما ال signal اللي اسمها SIGKILL رقم 9 دي بتعمل Terminate كانك بالظبط شديت الفيشه ودي بنستخدمها في حاله ال emergency ان مثلا ال system بتاعك unstable او فيه process وخده resources كتيره من

الميموري مخليه مثلا ال server بتاعك مهنج ف انت ساعتها بتبقي عايز ت Terminate حالا ال process دي ف بتستخدم kill -9

- اما kill -1 اللي هي ال signal اللي اسمها SIGHUP رقم 1 بنستخدمها لو عايزين ن reload process معينه يعني عملت change في Service معينه وعايز تعمل reload لل configration دي بس من غير ماتعمل restart لل service او من غير ماتعمل Termination ف بنستخدم kill -1 وبعدين ال process id
- لو عايز اعرف ال process id بتاعت اي process running عندك ف بتستخدم **pidof vim**

```
[root@MohamedAtef ~]# pidof vim
2102
```

- لو انا قولتله kill وبعدين رقم ال Process ID علي طول كده هيعمل Terminate لل Process باستخدام signal رقم 15 اللي هي ال Default

```
[root@MohamedAtef ~]# kill 2102
```

- ممكن احددله ال signal بالرقم زي مثلا

```
[root@MohamedAtef ~]# kill  -9 2102
```

- او ممكن احددله ال signal بالاسم زي مثلا

```
[root@MohamedAtef ~]# kill  -SIGKILL 2102
```

- لو انا عندي اكتر من process معمول ليها running في نفس الوقت من نفس ال process يعني انا فاتح ال vim اكتر من واحد في نفس الوقت وليكن مثلا انا مشغل 3 vim لو انا عايز اعملهم kill مره واحده عندي two option ي اما اقوله **kill -9** وبعدين احطله كل ال process id او استخدم killall وبعدين اسم ال process ف علشان تعرف ال process اللي عندك هتستخدم command اسمه **pidof** وبعدين اسم ال process

```
[root@MohamedAtef ~]# pidof  vim
38334  38333 38332
```

- علشان اعمل kill لكل ال process زي ماقولنا هنستخدم **kill -9** وبعدين كل ال process id

```
[root@MohamedAtef ~]# kill  -9 38334  38333 38332
```

- ي اما اقوله **killall** وبعدين اسم ال process

```
[root@MohamedAtef ~]# killall vim
```

- لو انا عايز اعمل kill لكل ال processes بتاعت user هستخدم **pkill -U** وبعدين اسم ال User

```
[root@MohamedAtef ~]# pkill -u mohamed
```

- امتي بحتاج اني اعمل Terminate لل Processes بتاعت user معين فيه عندي اكتر من سبب
- ممكن ال user يكون بيعمل committed a security violation
- او ممكن ال User يكون عنده Process معينه مسببه ان ال system يكون unresponsive
- او ممكن ال user يكون بيعمل run ل process كتيره جدا ماثره علي ال resources بتاعت السيستم
- او لو حسيت ان ال user داخل علي حاجات هو المفروض ميدخولش عليها او ملهوش access عليها
- ف في الحاله دي ال administrator بيبيقي محتاج انه يعمل Terminate لل Processes بتاعت ال user في نفس الوقت
- ممكن اني استخدم نوع ال signal اللي هتطبقها علي ال user عن طريق

```
[root@MohamedAtef ~]# pkill  -SIGKILL -u mohamed
```

Real-time process monitoring

- The top program is a dynamic view of the system's processes.

```
[root@master ~]# top
[root@master ~]# top -n 2
[root@master ~]# top -d 2
```

Specifies the maximum number of iterations, or frames, top should produce before ending.

Number of second between each update (the delay between screen updates) !!

type 1	to show all cpu cores
type s	to change the default refresh rate which is 3 seconds
type h	for help
type k	to kill a process
type r	to renice a process
type M	to change the display to sort by the amount of memory
type P	to change the display to sort by the CPU utilization
type n	to change the number of processes shown
type w	to save current display configuration
type q	to quit

- من شويه شوفنا ازاي ن List ال process ال running عندي مره واحده بس طب لو انا عايز ا monitoring ال process بتاعتي في ال real time بستخدم command اسمه **top** شبه بالظبط ال task manager في ال windows
- ال **top** ده بيعرضلي ال process بتاعتي في ال real time وكل شويه يعمل refresh

```
top - 13:07:21 up  1:27,  1 user,  load average: 0.04, 0.02, 0.00
Tasks: 302 total,   1 running, 301 sleeping,   0 stopped,   0 zombie
%Cpu(s):  6.5 us, 41.9 sy,  0.0 ni, 45.2 id,  0.0 wa,  3.2 hi,  3.2 si,  0.0 st
MiB Mem :    746.3 total,     62.0 free,    617.6 used,    186.4 buff/cache
MiB Swap:   2048.0 total,   1834.2 free,    213.8 used.    128.7 avail Mem
   PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  2151 root      20   0  226016   4252   3368 R  25.0   0.6   0:00.14 top
    40 root      20   0       0      0      0 S   8.3   0.0   0:05.14 kswapd0
     1 root      20   0  172976  12692   7936 S   0.0   1.7   0:05.10 systemd
     2 root      20   0       0      0      0 S   0.0   0.0   0:00.02 kthreadd
     3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
     4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
     5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
```

- ف انا ممكن استخدم اوبشن **-d** مع ال top ان انا احدد انه يعمل refresh كل قد ايه هو by default بيعمل refresh كل 3 ثواني لو انا عايز مثلا ال refresh يكون كل ثانيتين هقوله **top -d 2**

```
[root@MohamedAtef ~]# top -d 2
```

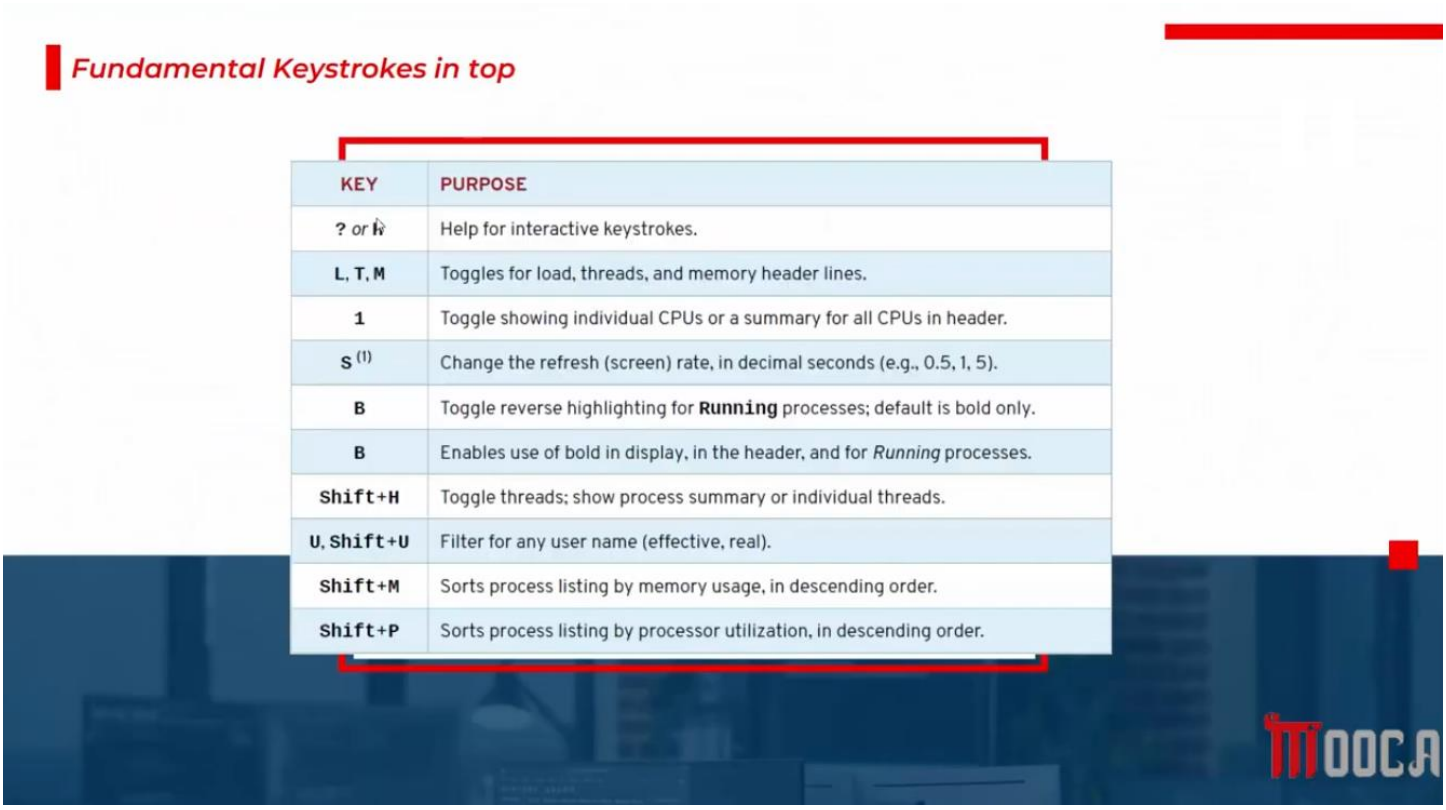
- لو انا عايز احدد ال maximum number of iterations ان بعد ال iteration دي تخلص ال top يحصله terminate هستخدم اوبشن **-n** مع ال top

```
[root@MohamedAtef ~]# top -n 2
```

- فيه options كتيره ممكن تستخدمها وانت فاتح ال top

- اول اوبشن لو انت ضغط علي رقم 1 من الكيبورد هجيبك كل ال CPU cores
- تاني اوبشن انت ممكن وانت جوه ال top تغير ال refresh rate بتاعك عن طريق انك تضغط s وهو by default بيكون 3 ثواني
- لو انت مثلا عايز تجيب ال help ف تضغط علي h
- لو انت فاتح ل top وعايز تعمل kill ل process معين هتضغط علي حرف ال k علشان ت k وبعدين تحددله ال PID
- لو انت عايز ت change ال Priority بتاعت process معينه او تعملها renice بتقوله اوبشن r
- لو ال process معمول ليها running وعايز ترتب ال process بتاعتك علي حسب ال memory utilization هضغط SHIFT+M
- لو انا عايز ارتب ال process علي حسب ال CPU utilization هضغط علي SHIFT+P
- لو انا عايز اعرض مثلا عدد محدد من ال Process يعني مثلا عايز اعرض اول 10 process هضغط علي حرف ال n وبعدين اكتب العدد اللي انا عايز اعرضه
- لو اناغيرت في ال top باستخدام اي اوبشن مالي شرحناهم وبعدين قفلت ال Terminal هو هيرجع لل default تاني ف علشان اعمل Save هضغط علي حرف ال w
- لو انا عايز اعمل quit لل top هضغط علي q

- **ودي بعض ال summary of available options جوه ال top**



Fundamental Keystrokes in top

KEY	PURPOSE
? or h	Help for interactive keystrokes.
L, T, M	Toggles for load, threads, and memory header lines.
1	Toggle showing individual CPUs or a summary for all CPUs in header.
s (1)	Change the refresh (screen) rate, in decimal seconds (e.g., 0.5, 1, 5).
B	Toggle reverse highlighting for **Running** processes; default is bold only.
B	Enables use of bold in display, in the header, and for *Running* processes.
Shift+H	Toggle threads; show process summary or individual threads.
U, Shift+U	Filter for any user name (effective, real).
Shift+M	Sorts process listing by memory usage, in descending order.
Shift+P	Sorts process listing by processor utilization, in descending order.

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.

- ازاي ن manage ال Priority of Linux Processes

- كل process running عندي ليها Process ID (PID) بيبقي ليها Priority Level او بيتقال عليها niceness Level
- ال Operating System(OS) بيشتغل ب Technique اسمه Time-Slicing ساعات بيبقي عندك اكتر من Process waiting to by running ف ال Time-Slicing بيوزع ال Time عليهم كلهم كل Process منهم ت run شويه وتطلع وتدخل Process تانيه وهكذا اللي بي Handle القصه دي هو ال Kernel لان عنده حاجه اسمها Process Scheduler هي اللي بت manage القصه دي
- كل Process عندي ليها Priority معينه ال Levels بتاعت ال Priority دي او ال Range بتاعهم من 20- لحد 19 كل process بتاخد priority في ال Level ده .عندك حوالي 40 Level من ال Priority
- خدها قاعده ال lowest of numbers بيكون highest priority وال highest in numbers بيكون lowest priority يعني 20- لو فيه اي Process ليها 20- Priority دي كده ال highest priority ولو فيه اي Process تانيه واخده priority 19 دي كده ال Lowest Priority
- انا عندي by default بعض ال Processes بت inherit نفس ال nice level بتاع ال Parent بتاعهم اللي هو عادتا هتلاقيه ب zero
- اللي ليه Privilege انه يت change ال Priority بتاعت اي Process موجوده عندي Running هو ال Root
- ال Regular user اللي هو ال user العادي مسموح ليه بس انه ي Set ال Positive Nice Levels يعني انا ك user عادي عندي Process running دلوقتي وواخده Priority Zero اقدر اخليها 5 او او 10 لحد 19 اه عادي اهم حاجه بس انت طالما ذوت مينفعش ترجع تاني بمعني ان ال Priority كانت 5 وانا ذوتها ل 7 مثلا هل ينفع اني ارجع تاني ل 5 لا مينفعش

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
```

- علشان اعمل List لل Processes بال Priority بتاعتها احنا فيه command استخدمناه قبل كده اسمه **ps lax** هنلاقيه فيه column اسمه NI او nice هنلاقيه معظم ال Processes واخده Zero وهنلاقيه فيه processes واخده 20-

```
[root@MohamedAtef ~]# ps lax
F   UID   PID   PPID PRI  NI   VSZ    RSS    WCHAN  STAT TTY     TIME   COMMAND
4   0     1     0    20   0    173236 10828  ep_pol  Ss   ?       0:06   /usr/lib/systemd/
1   0     2     0    20   0    0      0      kthrea  S    ?       0:00   [kthreadd]
1   0     3     2    0    -20  0      0      rescue  I<   ?       0:00   [rcu_gp]
1   0     4     2    0    -20  0      0      rescue  I<   ?       0:00   [rcu_par_gp]
```

- فيه اوبشن تاني ممكن تقوله **ps axo** وبعدين تحدد ال column اللي عايز تعرضه زي مثلا

```
[root@MohamedAtef ~]# ps axo user,pid,nice,command
USER     PID  NI COMMAND
root       1   0 /usr/lib/systemd/systemd rhgb --switched-root --system
root       2   0 [kthreadd]
root       3 -20 [rcu_gp]
root       4 -20 [rcu_par_gp]
root       5 -20 [slub_flushwq]
```

- وممكن استخدم ال grep كمان لو انا عايز اعرض Process معينه

```
[root@MohamedAtef ~]# ps axo user,pid,nice,command | grep sleep
root     1981  0 sleep 1000
root     1982  0 sleep 1000
root     1983  0 sleep 1000
root     1987  0 grep --color=auto sleep
```

How to Set Linux Process Priority Using nice and renice Commands

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

```
[root@lab01 ~]# nice vim text &
[1] 9182
[root@lab01 ~]# nice -n vim text &
```

(Default is 10)

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

```
[root@lab01 ~]# renice 19 9182
[root@lab01 ~]#top
```

(19 is the new value)
(press r to renice a process)

- لو انا عايز أ change Priority معينه عندي Two Commands

1- عندي command اسمه nice ده بستخدمه لو عايز اعمل start ل Process معينه ب Predefined priority ف اقوله nice وبعدين اسم ال command نفسه اللي انا عايز اعمله execute

- لو انا قولتله nice من غير ماحددلها اي رقم هو ه assign priority رقم 10 الا لو انت قولتله nice -n وحددتله رقم معين وكتبتله بعد كده ال command نفسه فساعتها هو ه restart ال Process دي ب user defined priority بس هو by default هيكون ب 0 ال Process هت inherit نفس ال Priority بتاعت ال Parent بتاعها
- لو انا عندي running process وعايز اغير ال Priority بتاعتها ساعتها بستخدم command اسمه renice بقوله renice وبعدين ال nice value وبعدين اديله ال Process ID
- او ممكن من جوه ال top اضغط علي حرف ال r واغير ال Priority

➢ هنعمل run ل اي Process عندي وليكن هنعمل sleep كذا مره علشان نجرب

```
[root@MohamedAtef ~]# sleep 1000 &
[1] 1981
[root@MohamedAtef ~]# sleep 1000 &
[2] 1982
[root@MohamedAtef ~]# sleep 1000 &
[3] 1983
```

➢ لو عملنا grep علي ال process اللي اسمها sleep هنلاقيهم كلهم واخدين Priority Zero

```
[root@MohamedAtef ~]# ps axo user,pid,nice,command | grep sleep
root      1981   0 sleep 1000
root      1982   0 sleep 1000
root      1983   0 sleep 1000
root      1993   0 grep --color=auto sleep
```

- لو انا عايز اعمل change لل priority اللي ال PID بتاعها 1987 ف انا عايز مثلا اغير ال Priority اخليها ب 10

```
[root@MohamedAtef ~]# renice 10 1981
1981 (process ID) old priority 0, new priority 10
```

- لو عملنا grep تاني علشان نشوف ال Priority

```
[root@MohamedAtef ~]# ps axo user,pid,nice,command | grep sleep
root      1981  10 sleep 1000
root      1982   0 sleep 1000
root      1983   0 sleep 1000
root      1999   0 grep --color=auto sleep
```

- فيه عندي command اسمه pgrep بستخدمه لو انا عايز اعرف كل ال PID بتاعت Process معينه

```
[root@MohamedAtef ~]# pgrep sleep
1981
1982
1983
```

- لو انا عايز اعمل change لكل ال Process مره واحده

```
[root@MohamedAtef ~]# renice 19 $(pgrep sleep)
1981 (process ID) old priority 0, new priority 19
1982 (process ID) old priority 0, new priority 19
1983 (process ID) old priority 0, new priority 19
```

- لو انا عايز اعمل kill لكل ال Process دي هقوله killall sleep

```
[root@MohamedAtef ~]# killall sleep
[2]-  Terminated              sleep 1000
[3]+  Terminated              sleep 1000
```

- لو عايز ت start service معينه ب Predefined priority هتقوله nice ولو استخدم nice بس هيحط ال default priority اللي هو 10

```
[root@MohamedAtef ~]# nice sleep 1000 &
[3] 2033
```

- لو عملنا grep تاني علشان نشوف ال Priority

```
[root@MohamedAtef ~]# ps axo user,pid,nice,command | grep sleep
root      2033  10 sleep 1000
```

- او ممكن احددله ال Priority

```
[root@MohamedAtef ~]# nice -n -20 sleep 1000 &
[4] 2037
```

Chapter 9

Controlling Services and Daemons

Introduction to systemd

- In Red Hat Enterprise Linux, the first process that starts (PID 1) is **systemd**.
- The **systemd** daemon manages startup for Linux, including service startup and service management in general. It activates system resources, server daemons, and other processes both at boot time and on a running system.

- مبدئيا انا عندي اول Service او اول Process بتقوم عندي في ال System بتاعي وال system بتاعي بيحصله boot up المفروض بيمر كده ب Process معينه اسمها boot Process ومن ضمن ال Process ان ال Kernel بيروح ي initialize او ي Start ال First Process اللي بتبدأ عندي في ال System
- Start from red hat 7 كانت اول Process بتقوم عندي في السيستم اسمها system قبل كد كانت اسمها init
- يبقي ال system اول Services او اول Process بتقوم عندي في السيستم وبعد كده هي ال بت manage ال start up بتاعي بتروح ت activates وبت start كل ال Services علشان توصلني ل Target معين وليكن ال Target ده GUI او Graphical

Listing service units

- You use the **systemctl** command to explore the current state of the system. For example, the following command lists all currently loaded service units

```
[root@host ~]# systemctl list-units --type=service
```

(List all active services)

- By default, the **systemctl list-units --type=service** command lists only the service units with **active** activation states.

- ال command اللي احنا هنستخدمه اسمه **systemctl** بنستخدمه علشان اعمل List واشوف ال Status بتاعت اي Service او اعمل a control ال service دي سواء كان عايز اعملها start او stop او restart

- اول command هنشوف مع بعض لو انا عايز a list كل ال active service الموجوده عندي في السيستم بقوله **systemctl list-units –type=service**

```
[root@MohamedAtef ~]# systemctl list-units --type=service
  UNIT                                  LOAD   ACTIVE  SUB     DESCRIPTION
  accounts-daemon.service               loaded   active running Accounts Service
  alsa-state.service                    loaded   active running Manage Sound Card State (resto>
  atd.service                           loaded   active running Deferred execution scheduler
  auditd.service                        loaded   active running Security Auditing Service
  autofs.service                        loaded   active running Automounts filesystems on dema>
  avahi-daemon.service                  loaded   active running Avahi mDNS/DNS-SD Stack
  colord.service                        loaded   active running Manage, Install and Generate C>
  crond.service                         loaded   active running Command Scheduler
  cups.service                          loaded   active running CUPS Scheduler
```

- لو انا عايز اعمل list لكل ال service ال active وال inactive بذود اوبشن **--all**

```
[root@MohamedAtef ~]# systemctl list-units --type=service --all
  UNIT                                  LOAD      ACTIVE   SUB     DESCRIPTION       >
  accounts-daemon.service               loaded      active   running Accounts Service
  alsa-restore.service                  loaded      inactive dead    Save/Restore Sound>
  alsa-state.service                    loaded      active   running Manage Sound Card >
● apparmor.service                      not-found inactive dead    apparmor.service
  atd.service                           loaded      active   running Deferred execution>
  auditd.service                        loaded      active   running Security Auditing >
  auth-rpcgss-module.service            loaded      inactive dead    Kernel Module supp>
● auto-cpufreq.service                  not-found inactive dead    auto-cpufreq.servi>
  autofs.service                        loaded      active   running Automounts filesys>
```

- لو انا عندي اي Failed Service وعايز اعمل List ل ال Failed Service الموجوده عندي

```
[root@MohamedAtef ~]# systemctl --failed --type=service
  UNIT LOAD ACTIVE SUB DESCRIPTION
0 loaded units listed.
```

- لو انا عايز اعرف ال status بتاعت اي service هقوله systemctl status وبعدين اسم ال service

```
[root@MohamedAtef ~]#  systemctl status sshd.service
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2024-07-20 11:51:30 EET; 3h 28min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
 Main PID: 996 (sshd)
    Tasks: 1 (limit: 4393)
   Memory: 6.0M
      CPU: 465ms
   CGroup: /system.slice/sshd.service
```

Verifying the status of a services

- The **systemctl** command provides methods for verifying the specific states of a service. For example, use the following command to verify that the a service unit is currently active (running):

```
[root@host ~]# systemctl is-active sshd.service
```

active or inactive

```
[root@host ~]# systemctl is-enabled sshd.service
```

enable or disable

```
[root@host ~]# systemctl is-failed sshd.service
```

active or failed

- To list all the failed units, run the **systemctl --failed --type=service** command

- لو انا عايز اعرف service معينه هل هي active ولا inactive هستخدم

```
[root@MohamedAtef ~]#  systemctl is-active sshd.service
active
```

- لو عايز اعرف هل ال service بتكون enable ولا disable

```
[root@MohamedAtef ~]#  systemctl is-enabled sshd.service
enabled
```

- لو انا عايز اعرف هل ال service بتكون active ولا failed

```
[root@MohamedAtef ~]#  systemctl is-failed sshd.service
active
```

Controlling system services

- To start a service:

```
[root@host ~]# systemctl start sshd.service
```

- To restart a service:

```
[root@host ~]# systemctl restart sshd.service
```

- لو انا عندي Service Not Running وعايز اعملها Start بستخدم **systemctl start** وبعدين اسم ال service

```
[root@MohamedAtef ~]# systemctl start sshd.service
```

- لو انا عايز اعمل restart ل service معينه بستخدم **systemctl restart** وبعدين اسم ال service وبستخدم ال restart لو انا غير في ال configuration بتاعتها عملت اي modification في ال configuration file بتاعتها ف بحتاج اني اعمل restart لل service علشان السيستم يكون aware بال change اللي حصلت

```
[root@MohamedAtef ~]# systemctl restart sshd.service
```

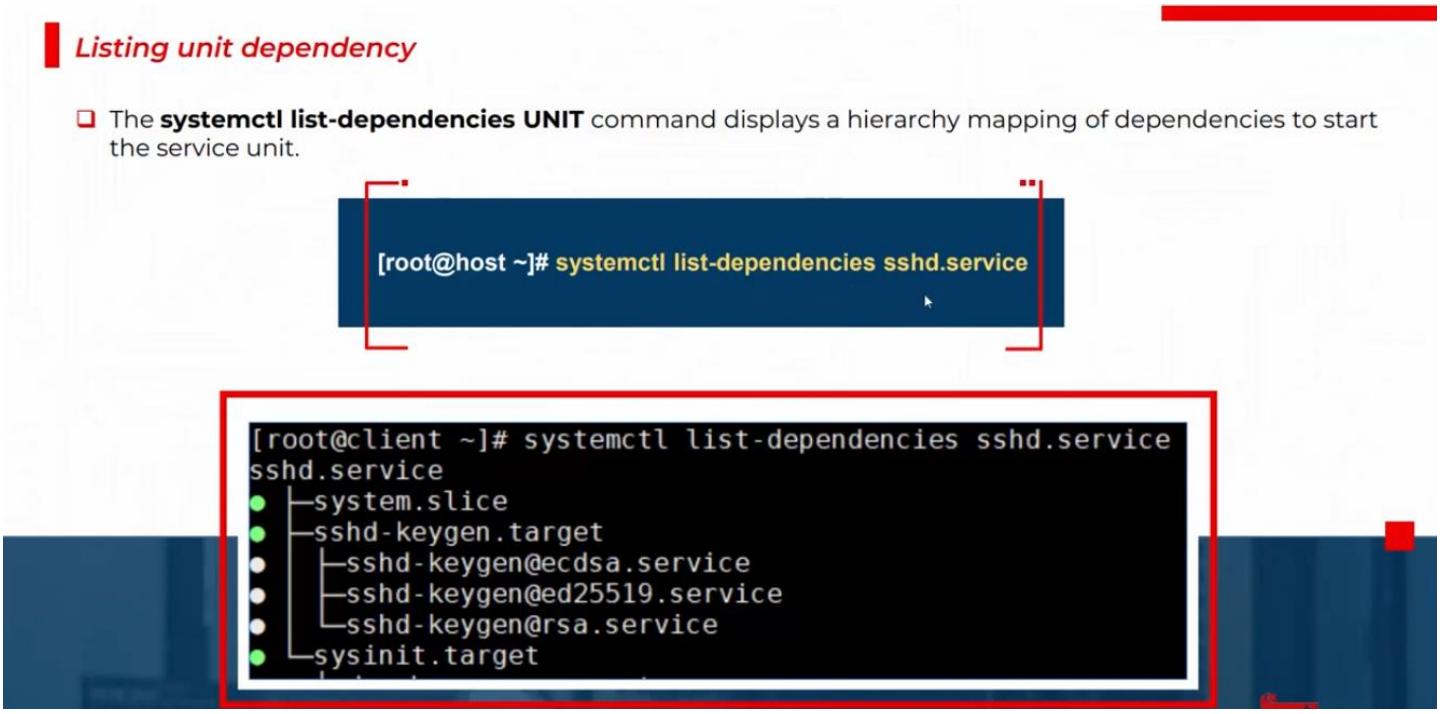
- لو انا عايز اعمل stop ل service معينه بقوله **systemctl stop** وبعدين اسم ال service

```
[root@MohamedAtef ~]# systemctl stop sshd.service
```

- لو انا عايز اعمل reload هستخدم **systemctl reload** وبعدين اسم ال service

```
[root@MohamedAtef ~]# systemctl reload sshd.service
```

- طب ايه الفرق مابين restart و reload لما بستخدم restart كاني ب stop ال service وبعدين اعملها start تاني لكن reload بتخلي ال Service تروح تقرا او ت Re-lead ال Configuration file بتاعتها



- ساعات بيبقي عندي service معتمده علي service تانيه ف بنستخدم systemctl list-dependancies علشان اشوف ال service دي بت depend علي ايه

```
[root@MohamedAtef ~]# systemctl list-dependencies sshd
sshd.service
● ├─system.slice
● ├─sshd-keygen.target
○ │ ├─sshd-keygen@ecdsa.service
○ │ ├─sshd-keygen@ed25519.service
○ │ └─sshd-keygen@rsa.service
● └─sysinit.target
● ├─dev-hugepages.mount
```

Masking and unmasking services

```
[root@host ~]# systemctl mask sendmail.service

[root@host ~]# systemctl list-unit-files --type=service | grep sendmail
sendmail.service                    masked

[root@host ~]# systemctl start sendmail.service
Failed to start sendmail.service: Unit sendmail.service is masked.

[root@host ~]# systemctl unmask sendmail
```

- امتي اعمل mask و umask ل service ولنفرض مثلا انت عندك service معمول ليها installed عندك وعايز تعمل installed ل Service تانيه ف ال vendor صاحب الابلكيشن بتاع السيرفز دي اللي انت عايز تعمله Install قالك انا ك recommendations مني ان السيرفز بتاعتي هت conflict مع السيرفز اللي Installed عندك زي مثلا عندي service اسمها sendmail السيرفز دي هت conflict مع سيرفز تانيه انت عايز تعملها install ف في الحاله دي انت بتعمل stop و disable للسيرفز طب فين المشكله لو عملت stop و disable ان ممكن يجي اي سيستم ادمن تاني وبالغلط يلاقي السيرفز دي معمول ليها stop يقوم هو عامل start للسيرفز دي فساعتها بمجرد ان السيرفز اتعملها started فساعتها ممكن ت conflict مع السيرفز التانيه وتعمل عندك service input ف في الحاله دي ك اجراء احترازي مننا بنعمل mask لل service دي
- ف علشان اعمل mask بنقوله **systemctl mask** وبعدين اسم السيرفز ف لو حاول اي حد يعمل start للسيرفز اللي معمول ليها mask هيطلعله error بالشكل ده Failed to start sendmail.service: Unit sendmail.service is masked معناها ان محدش يقدر انه يعمل start للسيرفز دي

➢ انا عندي service اسمها httpd تعال نعمل mask ليها هنلاقي لما نعمل mask هنلاقيه عمل create ل symbolic link او shortcut بيشاور علي /dev/null كان السيرفز مش موجوده

```
[root@MohamedAtef ~]# systemctl mask httpd
Created symlink /etc/systemd/system/httpd.service → /dev/null.
```

➢ لو جينا عملنا start للسيرفز دي هنلاقيه بيقولك failed ان السيرفز دي masked حاليا

```
[root@MohamedAtef ~]# systemctl start httpd
Failed to start httpd.service: Unit httpd.service is masked.
```

➢ لو انا عايز اعمل unmask قوله systemctl unmask ويعد اسم السيرفز

```
[root@MohamedAtef ~]# systemctl unmask httpd
Removed "/etc/systemd/system/httpd.service".
```

Enabling services to start or stop at boot

- To start a service at boot, use the systemctl enable command.

```
[root@root ~]# systemctl enable sshd.service
```

- To disable the service from starting automatically

```
[root@host ~]# systemctl disable sshd.service
```

- لو انا عايز اعمل enable لسيرفز معينه هستخدم systemctl enable وبعدين اسم السيرفز

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

- لو انا عايز اعمل disable هستخدم systemctl disable وبعدين اسم السيرفز

```
[root@MohamedAtef ~]# systemctl disable httpd
```

Summary of systemctl commands

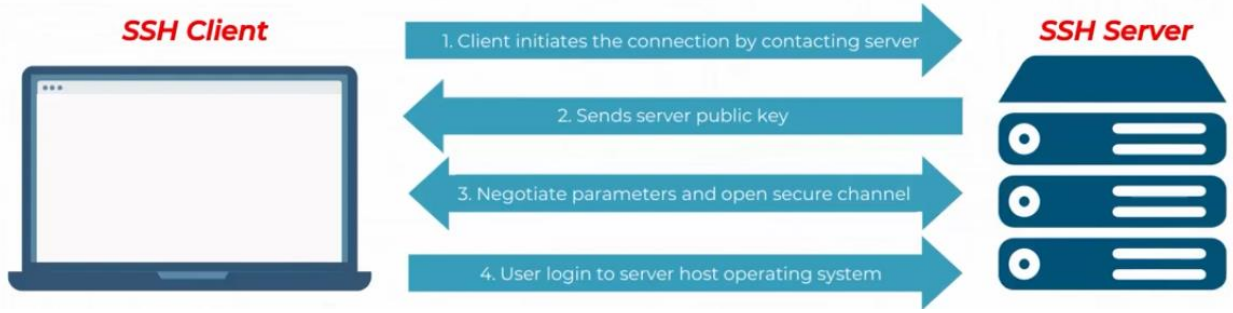
TASK	COMMAND
View detailed information about a unit state.	`systemctl status UNIT`
Stop a service on a running system.	`systemctl stop UNIT`
Start a service on a running system.	`systemctl start UNIT`
Restart a service on a running system.	`systemctl restart UNIT`
Reload the configuration file of a running service.	`systemctl reload UNIT`
Completely disable a service from being started, both manually and at boot.	`systemctl mask UNIT`
Make a masked service available.	`systemctl unmask UNIT`
Configure a service to start at boot time.	`systemctl enable UNIT`
Disable a service from starting at boot time.	`systemctl disable UNIT`
List units required and wanted by the specified unit.	`systemctl list-dependencies UNIT`

Chapter 10

Configuring and Securing SSH

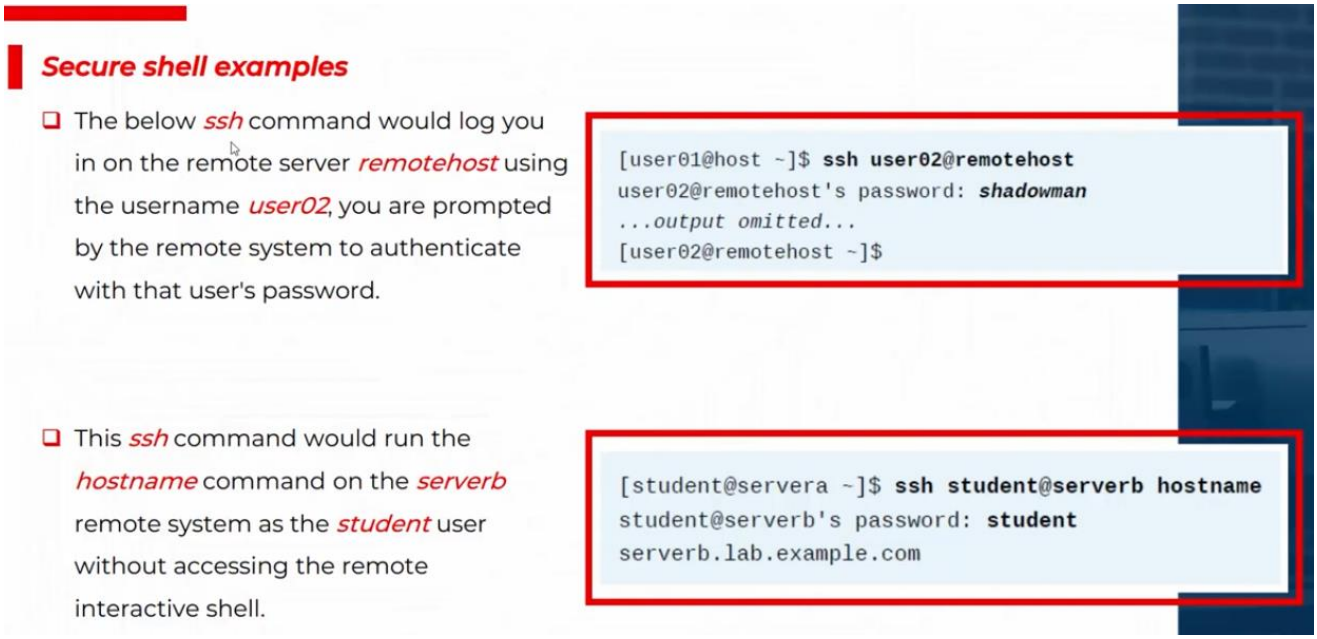
WHAT IS OPENSSH?

- OpenSSH implements the Secure Shell or SSH protocol in the Red Hat Enterprise Linux systems.
- The SSH protocol enables systems to communicate in an encrypted and secure fashion over an insecure network.
- The first time a user uses ssh to connect to a particular server, the ssh command stores the server's public key in the user's ~/.ssh/known_hosts file.



- ال **OPENSSH** او ال **SSH Protocol** او بيسمي ال **Secure shell** ده عباره عن Protocol بستخدمه علشان اعمل communicate مابين ال machines وبعضها وال communication مابين ال servers وبعضها بيكون very secure و encrypted
- علشان نفهم ازاي ال SSH بيشتغل لو انا عندي SSH Client وعندي SSH Server انا علشان اعمل login علي ال server ده remotely او عن طريق ال Network انا محتاج كذا حاجه اول حاجه محتاج ان ال SSH Service تكون معمول ليها install و Running علي ال Server ونفس الكلام علي ال Client تاني حاجه ان ال SSH تكون بت listen علي ال Port بتاعها و by default ال SSH بتستخدم Port 22 وتالت حاجه يكون ال communication اصلا مابين ال Client وال Server يكون allowed يعني من ال SSH Client اقدر من ال Source IP بتاع ال client اقدر اوصل ل Server IP بتاع ال Server
- ايه اللي بيحصل اول اما باجي اعمل Login باستخدام ال SSH اول حاجه بتحصل ان ال SSH Server بيبعتلي ال Public Key بتاعه وده by default لما بتيجي تعمل install ل SSH Server بيبقي كل server بيبقي فيه Public Key او مجموعه من ال Public Keys و Private Keys ف انا ك client اول ما initiate مع ال SSH Server ال SSH Server بي Send ال Server Public key ال Public Key بستخدمه في حاجتين اول حاجه بروح اعمل save لل Public Key في file اسمه **known_hosts** في ال Home Directory بتاع ال user اللي بيعمل SSH علي ال Server ده وده لو مش معمول ليه Create هيتعمله create by default ف انا ك client بستخدم ال Public Key في حاجتين اول حاجه علشان Authenticate ال Server ده كل مره ب SSH علي ال Server ف بيبعتلي ال Public Key بتاعه ف انا بروح اقارن ال Public key بتاعه بال Public key ال stored عندي في ال **known_hosts** file لو ال Public key لأي سبب اتغير ال SSH بي Consider ان

حصل اي attack في ال Network بتاعتك وبي break ال Connection علي طول ف انا هنا ك client بستخدم ال Public key تاني حاجه بيستخدم ال Public Key علشان خاطر ي establish ال Secure connection مع ال SSH Server ال SSH Client بي Generate حاجه اسمها Parameters key او بيتقال عليها session key وال session key بيتعملها encrypt بال Public key ال receive من ال SSH Server وبيروح باعتها تاني ل SSH Server ال encrypt session key اللي يقدر يعملها decrypt او اللي قدر يفك الشفره بتاعتها هو بس ال server اللي معاه ال Private key بتاع ال Public key ده مش اي حد يقدر يفك ال session key دي ف بمجرد ان ال SSH Server اول اما بيجيله encrypt session key بيعملها decrypt باستخدام ال private key بتاعه ويبقي كده عند ال SSH Client وال SSH Server عندهم ال session key وعملوا establish لل SSH Connections ف هيبدأ ال SSH Server وال SSH Client ان اي حد فيهم عايز يبعت للتاني بيعمل encrypted لل data عن طريق ال SSH key وال Client اول اما يستقبل الداتا يعملها decrypt بال session key



- علشان اعمل Login علي اي Server موجود عندي انا عندي Command اسمه **SSH** وده ال command اللي بستخدمه علشان اعمل connect remote علي اي Server موجود عندي
- اول حاجه هتعملها علشان ت login علي جهاز ال Server او ال Client ان انت تعرف ال IP Address الخاص بكل واحد فيهم وليكن ال IP الخاص بال Server هو 172.16.76.132 علشان تعمل login هتستخدم ssh وبعدين اسم ال user اللي هعمل connect بيه ولازم ال user ده يكون معمول ليه create انا عندي user اسمه user01 هعمل connect بيه ف هستخدم ssh user01@172.16.76.132 اول حاجه لو انت بت connect علي ال server اول مره ف ال server هيبعتلك ال Public key بتاعه او ال fingerprint بتاعتهف هيقولك Are you sure you want to continue connecting (yes/no/[fingerprint])

```
[root@MohamedAtef ~]# ssh user01@172.16.76.132
The authenticity of host '172.16.76.132 (172.16.76.132)' can't be established.
ED25519 key fingerprint is SHA256:X2fiazW2inkKFLPpNpvaSIL7J0I0fIoU+NNjsKBUmQE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

- ف لو قولتله yes هتلاقيه قايلك انه عمل Add لل public key بتاعت ال Server في ال Know hosts file
- لو عملت ls -a علي ال home directory هتلاقي hidden folder اسمه .ssh.

```
[root@MohamedAtef ~]# ls -a
.                .bash_profile  Desktop    media    Share    .viminfo
..               .bashrc        devops     .mozilla .ssh     virtual
```

- لو دخلنا جوه ال directory ده هتلاقي file اسمه known_hosts

```
[root@MohamedAtef ~]# cd .ssh/
[root@MohamedAtef .ssh]# ls
known_hosts
```

- لو عملنا cat علي ال file ده هتلاقيه جواه كل ال Public Keys بتاعت ال Server

```
[root@MohamedAtef .ssh]# cat known_hosts
172.16.76.132 ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOuiVM0I6vgWz5fK6IKxudqMX1lCHu4aatUdldE6ITA1
```

- ال Public Keys بيبقي Stored تحت /etc/ssh/ لو دخلنا في المسار ده وعملنا ls هتلاقي كل ال Public Keys

```
[root@MohamedAtef ~]# cd /etc/ssh/
[root@MohamedAtef ssh]# ls
moduli      sshd_config      ssh_host_ecdsa_key.pub   ssh_host_rsa_key
ssh_config  sshd_config.d    ssh_host_ed25519_key     ssh_host_rsa_key.pub
ssh_config.d  ssh_host_ecdsa_key  ssh_host_ed25519_key.pub
```

- لو انا مش عايز اعمل connect remotely او اعمل login علي ال Server انا بس عايز اعمل run ل command معين واعمل exit هستخدم نفس ال command عادي بس في الاخر اديله ال command اللي انا عايز اعمله run

```
[root@MohamedAtef ~]# ssh karim@172.16.76.132 hostname
```

SSH Key-Based Authentication

- You can configure an SSH server to allow you to authenticate without a password by using keybased authentication. This is based on a private-public key scheme.

Generating SSH Keys

- To create a private key and matching public key for authentication, use the *ssh-keygen* command.
- By default, your private and public keys are saved in your *~/.ssh/id_rsa* and *~/.ssh/id_rsa.pub* files, respectively.

```
[user@host ~]$ ssh-keygen
```

- Once the SSH keys have been generated, they are stored by default in the .ssh/ directory of the user's home directory.
- The permission modes must be 600 on the private key and 644 on the public key.

- فيه عندي طريقتين من ال Authentication

1- اول طريقه وهي Password Based authentication والطريقه دي اللي احنا استخدمناها قبل كده ان انت كل مره تعمل login علي ال Server بيطلب منك ال Password بتاعت ال user اللي انت بت connect بيه

2- تاني طريقه وهي SSH key-Based Authentication ان انت بدل اما تستخدم ال Password بتعمل generate لحاجه اسمها key-pair او Public key و Private key

- ف علشان أ configure ال SSH key -Based Authentication عندي كذا Step

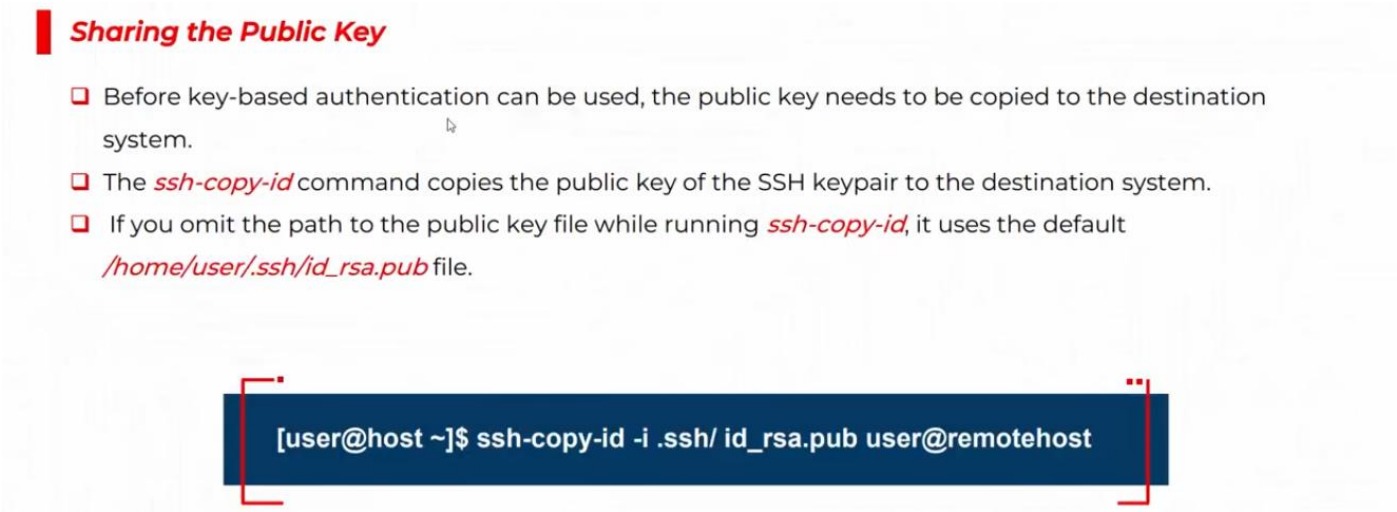
1- لازم اعملهم اول حاجه ب generate ال SSH key-pair ال Public key وال Private key علي ال Client

2- بعد كده بعمل copy لل Public key لل Server اللي انا عايز اعمل Login عليه

3- بعد كده بعمل SSH علي السيرفر ده ف ساعتها مش هيطلب مني اي Password لان هو هيعمل Authentication عن طريق ال Key بدل الباسورد

- بستخدم command اسمه ssh-keygen اعمل generate لل Public وال Private key وبيكونوا by default موجودين في ال Home Directory تحت /.ssh. وبيبقي اسمهم id_rsa بالنسبه لل Private Key وبالنسبه لل Public Key بيبقي اسمهم id_rsa.pub

- ال Private key ممنوع ان انت تعمله share مع اي حد ف لازم ت secure ال Private key بتاعك عن طريق ان انت ت restrict ال Permissions تعمل deny لاي حد ف علشان تعمل كده هتخلي ال Permission علي ال Private key بتكون 600 وبالنسبه لل Public key هيكون 644



- بعد اما انت عملت generate لل Public key وال Private key ف انت محتاج ان انت تعمل copy لل Public key بتاعك لل Server اللي انت عايز تعمل Login عليه عن طريق ان انت هتستخدم ال command ده **ssh-copy-id**

- لو جينا علي ال client ودخلنا تحت /.ssh وعملنا list هنلاحظ ان احنا عندنا ملف واحد وهو known_hosts

```
[root@Client .ssh]# ls
known_hosts
```

- لو انت قولتله ssh-keygen انت كده بتقوله ان انت عايز ت Generate Public and Private keys اول اما تضغط enter هيقولك by default ان هو هيعمل Save لل Public وال Private key بتاعك في ال Home directory لل user اللي عمل run لل **ssh-keygen** جوه /root/.ssh/ باسم id_rsa وده ال Private key بعد اما تضغط enter هيسألك يقولك Enter passphrase ان انت عايز تحط Password علي ال Private key بتاعك ولا لا لو ضغط Enter معناها ان انت مش عايز تحط باسورد بعد كده هيعمل generate

```
[root@Client .ssh]# ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa
Your public key has been saved in /root/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:gdvhfqv6+wgEteiCzdCOvc99P6++6PBEXoGoElhJpTg root@MohamedAtef
The key's randomart image is:
+---[RSA 3072]----+
| .oo. .          |
| =.. o + .       |
|E + o + + .      |
| X o o + o .     |
|o B o o S .      |
|  + . + .        |
| .  o + .        |
|  o . =.+..      |
|   o o=O*B=.     |
+----[SHA256]-----+
```

- لو عملنا ls تاني هنلاقيه عمل create ل Two file وهما id_rsa و id_rsa.pub

```
[root@Client .ssh]# ls
id_rsa  id_rsa.pub  known_hosts  known_hosts.old
```

- بعد كده هنعمل copy لل Public key بتاعك للServer باستخدام ssh-copy-id

```
[root@Client .ssh]# ssh-copy-id root@172.16.76.133
```

- بعد كده انت تقدر تعمل connect علي Server بدون اي مشكله

Customizing open SSH service configuration

- OpenSSH service is provided by a daemon called sshd. Its main configuration file is */etc/ssh/sshd_config.*

Prohibit the superuser from logging in using SSH

- It is a good practice to prohibit direct login to the root user account from remote systems. Some of the risks of allowing direct login as root include:
- The OpenSSH server uses the *PermitRootLogin* configuration setting in the */etc/ssh/sshd_config* configuration file to allow or prohibit users logging in to the system as root.
- With the *PermitRootLogin* parameter to yes, people are permitted to log in as root.
- The SSH server (sshd) must be reloaded for any changes to take effect.

```
[root@host ~]# systemctl reload sshd
```

- ازاي هنعمل customize لل open SSH Service configuration انا عندي ال main configuration file الخاص بال SSH Service موجود في /etc/ssh/sshd_config لو فتحنا ال sshd_config هنلاقي Parameters اسمه PermitRootLogin ال Parameters ده لو انت عايز تعمل deny او restrict ان مفيش اي يحد يقدر ي access ال Server بتاعك remotely باستخدام ال root ف انت بتخلي الPermitRootLogin ب No ودي حاجه recommended
- اي تغيير في ال Configuration file بتبقي محتاج ان انت تعمل reload لل Service عن طريق استخدام

```
[root@MohamedAtef ~]# systemctl reload sshd
```

Prohibiting password-based authentication for SSH

- The OpenSSH server uses the *PasswordAuthentication* parameter in the */etc/ssh/sshd_config* configuration file to control whether users can use password-based authentication to log in to the system.
- The default value of *yes* for the PasswordAuthentication causes the SSH server to allow users to use password-based authentication while logging in.
- The value of *no* for PasswordAuthentication prevents users from using password-based authentication.
- Keep in mind that whenever you change the /etc/ssh/sshd_config file, you must reload the sshd service for changes to take effect.

- فيه Parameter تاني اسمه *PasswordAuthenticaton* هل انت عايز ت enable ال Password based Authentication احنا قولنا ان فيه نوعين من ال Authentication في ال SSH فيه نوع اسمه Password based Authentication والنوع التاني key-based Authentication ال recommended وال More Secure ان انت تستخدم ال Key-Based Authentication مش ال Password Authentication . ف انت لازم تعمل Disable لل root access و Disable لل Password Authentication وطبعا متنساش في نفس الوقت لازم تبقي عامل Enable لل SSH Key او ال Key Based Authentication وعامل generate لل Public وال Private Keys علشان تقدر تعمل Login علي السيستم بتاعك

Chapter 11

Analyzing and Storing Logs

System Logging

- Processes and the operating system kernel record a log of events that happen. These logs are used to audit the system and troubleshoot problems.
- Many systems record logs of events in text files which are kept in the /var/log directory. These logs can be inspected using normal text utilities such as **less** and **tail**.
- The **systemd journald** and **rsyslog** services handle the syslog messages in Red Hat Enterprise Linux 9.

Syslog messages are handled by two service:

- **systemd-journald**: The Journal is a component of systemd that is responsible for viewing and management of log files
- **rsyslog**: The rsyslog service sorts and writes syslog messages to the log files that do persist across reboots in /var/log.

- انا عندي اي Event او اي Activity بتحصل عندي في السيستم بتاعي بتتكتب في مجموعه من ال Log file بتبقي By Default موجوده تحت /var/log ودي بتساعدني في ال Troubleshooting او لو عندي issues معينه وعايز اعرف ال root cause فقد ان انا اعمل Check لل Log Files الموجوده تحت /var/log علاشنا شوف المشكله دي بسبب ايه واقدر ان انا اعمل View لل Log file عن طريق اي Text Utilities زي less و tail command
- انا عندي Two Services المسئولين عن ال handle بتاع ال syslog messages في Red Hat 9
  1- اول Servers اسمها **system-journald** ودي المسئوله انها بت capture ال syslog messages وال Kernel Logs وال Boot messages وبتعمل Store في folder اسمه tmp تحت /run/data/journal ولو عملت reboot لل System بتاعك ال Logs دي بتتمسح
  2- وتاني service اسمها **rsyslog** ودي مسئوله انها ت read ال syslog messages ال received by journald service وتروح تكتبه في مجموعه من ال Log Files تحت /var/log/

➢ لو دخلنا تحت /run/log/ هنلاقي Folder اسمه Journal ف لو عملنا ls -ld علي ال Folder ده هنلاقيه ال Owner بتاعه هو ال systemd-journal وهتلاقي عليه SetGID ان اي File او Directory هيتعمله Create جوه ال Directory ده /run/data/journal هياخد نفس ال Permissions بتاعت ال Group Ownership بتاعت ال Parent بتاعه

```
[root@MohamedAtef ~]# ls -ld /run/log/journal/
drwxr-sr-x+ 3 root systemd-journal 60 Aug  2 17:23 /run/log/journal/
```

- لو دخلنا جوه ال Folder ده وعملنا ls -l هنلاقي فيه Directory اسمه af86da5aff3e4562b219715b46f478c3 وال Group owner بتاعه بيكون system-journal نفس ال group owner بتاع ال Parent

```
[root@MohamedAtef journal]# ls  -l
total 0
drwxr-s---+ 2 root systemd-journal 100 Aug  2 17:24 af86da5aff3e4562b219715b46f478c3
```

- لو دخلنا جوه ال Directory ده هنلاحظ ان احنا عندنا هنلاقي عندنا Files ال Files دي بيبقي Stored جواهم ال Journal Logs بتاعتي وزي ماقولنا ان ال Journal logs بتاعتي بتبقي tmp مش Permanent ان لو عملت reboot لل System كل ال Logs دي هتتمسح

```
[root@MohamedAtef journal]# cd af86da5aff3e4562b219715b46f478c3/
[root@MohamedAtef af86da5aff3e4562b219715b46f478c3]# ls -l
total 3128
-rw-r-----+ 1 root systemd-journal  666736 Aug  2 17:23 system@4fdb5f825dda4d8fb160ac1fbf69fa3c-0000000000000001-00061eb4ea94ea8d.journal
-rw-r-----+ 1 root systemd-journal  599432 Aug  2 17:24 system@4fdb5f825dda4d8fb160ac1fbf69fa3c-0000000000000513-00061eb4ea9cf8d7.journal
-rw-r-----+ 1 root systemd-journal 1957888 Aug  2 17:55 system.journal
```

- ولو دخلنا جوه /var/log هنلاقي موجود فيه مجموعه من ال Log files المختلفه كل Log file منهم بيبقي Stored جواه Logs معينه

```
[root@MohamedAtef ~]# cd /var/log/
[root@MohamedAtef log]# ls
boot.log-20240720  dnf.log          maillog            sa                 swtpm          vmware-vmsvc-root.log
boot.log-20240721  dnf.log.1        maillog-20240707   samba              tallylog       vmware-vmtoolsd-root.log
boot.log-20240728  dnf.rpm.log      maillog-20240714   secure             tuned          vmware-vmusr-root.log
boot.log-20240802  firewalld        maillog-20240721   secure-20240707    vmware-network.1.log  wtmp
btmp                                gdm                maillog-20240728   secure-20240714  vmware-network.2.log
btmp-20240802                       hawkey.log         messages           secure-20240721  vmware-network.3.log
```

- ومن اشهر ال Log File اللي هنتعامل معاها

Log file	Type of stored messages
/var/log/messages	من اشهر ال Log file الموجوده تحت /var/log/ هو ال messages وده معظم ال Syslog Messages او معظم ال events بتبقي Stored في ال message ده . بأستثناء لو فيه عندك اي event او Logs بتكون related لل Authentication او ال email processing او ال scheduled job execution لان كل ال Logs دي بتبقي Stored في Files تانيه
/var/log/secure	اي Messages بتكون related لل Authentication او ال Security ان user عمل Login مثلا علي السيستم ف هتلاقي event اتكتب في ال log file ده وال file ده ال root بس هو اللي ليه Permission عليه
/var/log/maillog	لو فيه عندك اي Syslog messages related لل mail Server هتلاقيها موجوده فيه ال maillog
/var/log/cron	لو فيه اي message related لل scheduled او ال Cron Tab
/var/log/boot.log	بيكون فيه ال Logs بتاعت السيستم بتاعك وهو بي Start Up السيستم وهو بي Start Up بيمر بحاجه اسمها ال Boot Process ف كل ال Logs دي بتكون موجوده في ال Boot.log

Overview of Syslog Priorities

- انا عندي فيه مجموعه من ال Priorities ان اي Event عندي بيكون ليه Priority او ليه severity وال Table ده بيوضحلك كل ال Severity او ال Standard eight syslog priority الموجوده عندي وبتبدء من تحت ل فوق وكل اما تطلع لفوق ال Severity بتاعت ال Event بتزيد معاه

Code	Priority	severity
0	emerg	System is unusable
1	alert	Action must be taken immediately
2	crit	Critical condition
3	err	Non-critical error condition
4	warning	Warning condition
5	notice	Normal but significant event
6	info	Informational event
7	debug	Debugging-level message

- ال service **rsyslog** دي المسئوله ان هي ت sort وتروح تكتب ال Log file في مجموعه من ال File تحت **/var/log** هل بكتب ال Logs دي بطريقه عشوائيه لا هي عندها configuration file اسمه **rsyslog.conf** وبيكون موجود تحت **/etc/** وده بيكون موجود فيه مجموعه من ال rules مكتوبه ب Syntax معين

```
#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                  /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none            /var/log/messages
# The authpriv file has restricted access.
authpriv.*                               /var/log/secure
# Log all the mail messages in one place.
mail.*                                  -/var/log/maillo
# Log cron stuff
cron.*                                  /var/log/cron
# Everybody gets emergency messages
*.emerg                                  :omusrmsg:*
# Save news errors of level crit and higher in a special file.
uucp,news.crit                           /var/log/spooler
# Save boot messages also to boot.log
local7.*                                /var/log/boot.log
```

- عندنا Service او Tool اسمها **logrotate** ودي وظيفتها ان هي ت audit علي ال Log files بتاعتك وتعملها rotate علشان تحافظ علي ال مساحه ال Disk ميتملاش ودي بتشتغل ب criteria معينه علي حسب ال Configuration file وال rules بتاعتها .زي مثلا عندي logfile معين عنده criteria انه بعد وقت معين روح اعمل rotate لل logfile ده و rotate يعني هيعمل rename للlogfile هيخليه مثلا Logfile.01 ويعمل create ل file تاني يكون فاضي وبعد شويه يعمل rotate لل logfile اللي اسمه Logfile.0 ويعمله rename ل Logfile.1 وال logfile يعمله rename ويخليه Logfile.0 ويعمل create ل واحد جديد تبدء تكتب عليه ويفضل يكرر الكلام ده Based علي ال Configurations
- ال Main Configuration file الخاص بال **logrotate** بيكون اسمه **logrotate.conf** وبيكون موجود تحت **/ete/logrotate.conf**

➢ لو بصينا علي ال Main Configuration file بتاع ال logrotate هنلاقيه فيه كذا Parameters

```
[root@MohamedAtef ~]# less /etc/logrotate.conf

# see "man logrotate" for details

# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# packages drop log rotation information into this directory
include /etc/logrotate.d

# system-specific logs may be also be configured here.
```

هنلاقي فيه Parameter اسمه weekly ده هيعمل كل اسبوع rotate لل file هيعمل rename لل Log file وهيعمل واحد جديد فاضي

هنلاقي فيه Parameter تاني اسمه rotate 4 يعني هنا هيعمل keep ل كام file في ال History عندك

هنلاقي فيه Parameter تاني اسمه create وده معناه ان انت عايز تعمل ل create new empty log files ان بعد اما يعمل rotate لل Old file هيعمل create ل واحد تاني فاضي بنفس الاسم

هنلاقي فيه Parameter تاني اسمه dateext وده ال File اللي انت عايز تعمله renaming بيضيف ليه suffix معين لل file

هنلاقي فيه Parameter تاني اسمه compress وبيكون معمول ليه هاش لو انت عايز تعمل compress لل Log File بتعمله uncomment وتعمل restart لل Log rotate service

- لو عملنا ls -ltr messages* هنلاقيه عمل create ل file اسمه messages وال file ده بيتكتب فيه وعمل rotate ل Four Files وبيعملهم rename لنفس الاسم وبعدين داش – وبعدين التاريخ اللي عمل فيه rotate

```
[root@MohamedAtef log]# ls -ltr messages*
-rw-------. 1 root root  1961101 Jul  7 07:05   messages-20240707
-rw-------. 1 root root  3419715 Jul 14 00:00 messages-20240714
-rw-------. 1 root root  3140423 Jul 21 14:11  messages-20240721
-rw-------. 1 root root  232448 Jul 28 18:06 messages-20240728
-rw-------. 1 root root  371786 Aug  2 23:41  messages
```

Monitoring Logs

- علشان ن Monitoring ال Logs فيه عندي Command اسمه **tail -f** ال Command ده بستخدمه لو انا عايز اعمل view لل Log file بشكل Dynamic وبعدين احددله ال Path الخاص بال Log file

```
[root@MohamedAtef log]# tail -f /var/log/secure
```

Reviewing System Journal Entries

- هنشوف ازاي هنستخدم ال **Journalctl** علشان خاطر ت View وت Manage ال Journal Logs او ال Journal Entries
- لو انت قولتله **journalctl -n** ده كده بيعرضلك اخر 10 سطور من ال Log

```
[root@MohamedAtef ~]# journalctl -n
Aug 03 13:02:24 MohamedAtef systemd[1891]: Finished Create User's Volatile Files and Directories.
Aug 03 13:02:24 MohamedAtef systemd[1891]: Reached target Basic System.
Aug 03 13:02:24 MohamedAtef systemd[1]: Started User Manager for UID 0.
Aug 03 13:02:24 MohamedAtef systemd[1891]: Reached target Main User Target.
Aug 03 13:02:24 MohamedAtef sshd[1884]: pam_unix(sshd:session): session opened for user root(uid=0) by (uid=0)
Aug 03 13:02:24 MohamedAtef systemd[1891]: Startup finished in 791ms.
Aug 03 13:02:24 MohamedAtef systemd[1]: Started Session 2 of User root.
Aug 03 13:02:24 MohamedAtef systemd[1]: Starting Hostname Service...
Aug 03 13:02:24 MohamedAtef systemd[1]: Started Hostname Service.
Aug 03 13:02:54 MohamedAtef systemd[1]: systemd-hostnamed.service: Deactivated successfully.
```

- ممكن احددله عدد ال Logs اللي هو يعرضها عن طريق اني استخدم نفس ال Command وبعدين اضيف العدد اللي انا عايز اعرض

```
[root@MohamedAtef ~]# journalctl -n 5
Aug 03 13:30:27 MohamedAtef systemd[1]: Failed to start dnf makecache.
Aug 03 13:30:27 MohamedAtef systemd[1]: dnf-makecache.service: Consumed 1.439s CPU time.
Aug 03 13:36:06 MohamedAtef kernel: vmxnet3 0000:03:00.0 ens160: NIC Link is Down
Aug 03 13:36:11 MohamedAtef kernel: vmxnet3 0000:03:00.0 ens160: NIC Link is Up 10000 Mbps
Aug 03 13:36:11 MohamedAtef NetworkManager[983]: <info>  [1722684971.6570] device (ens160): carrier: link conne>
```

- فيه Command تاني اسمه **journalctl -f** ال Command ده هيعرضلك اخر 10 logs وهيفضل مستمر معاك لو فيه اي logs حصلت هيعرضهالك علي طول قدامك ف نفس الوقت
- فيه كمان اوبشن **-p** ان انت تحدد ال Priority ان انت مثلا عايز ت List ال Logs بس اللي ال Priority بتاعتها بتكون err ولازم ال Priority تتاكد ان انت كاتبها صح بنفس ال Syntax الموجود في ال Table

```
[root@MohamedAtef ~]# journalctl -p err
Aug 03 12:42:24 MohamedAtef stratis-clevis-setup-generator[570]: stratis.rootfs.pool_uuid kernel command line p>
Aug 03 12:42:24 MohamedAtef stratis-setup-generator[571]: stratis.rootfs.pool_uuid kernel command line paramete>
Aug 03 12:42:31 MohamedAtef kernel: piix4_smbus 0000:00:07.3: SMBus Host Controller not enabled!
Aug 03 12:42:37 MohamedAtef alsactl[818]: alsa-lib main.c:1559:(snd_use_case_mgr_open) error: failed to import >
Aug 03 12:42:59 MohamedAtef setroubleshoot[839]: SELinux is preventing /usr/bin/lsmd from getattr access on the>
Aug 03 13:30:27 MohamedAtef systemd[1]: Failed to start dnf makecache.
```

- لو انا عايز اعرض ال Boot Logs بتاعتي هستخدم اوبشن -b

```
[root@MohamedAtef ~]# journalctl -b
Aug 03 12:42:16 server.iti.com kernel: Linux version 5.14.0-284.11.1.el9_2.x86_64 (mockbuild@x86-vm-09.build.en>
Aug 03 12:42:16 server.iti.com kernel: The list of certified hardware and cloud instances for Red Hat Enterpris>
Aug 03 12:42:16 server.iti.com kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-284.11.1.el9_2.x86_>
Aug 03 12:42:16 server.iti.com kernel: Disabled fast string operations
Aug 03 12:42:16 server.iti.com kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Aug 03 12:42:16 server.iti.com kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Aug 03 12:42:16 server.iti.com kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Aug 03 12:42:16 server.iti.com kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Aug 03 12:42:16 server.iti.com kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using '>
Aug 03 12:42:16 server.iti.com kernel: signal: max sigframe size: 1776
Aug 03 12:42:16 server.iti.com kernel: BIOS-provided physical RAM map:
```

- لو انا عايز اعرض ال Logs اللي حصلت امس

```
[root@MohamedAtef ~]# journalctl --since yesterday
Aug 03 12:42:16 server.iti.com kernel: Linux version 5.14.0-284.11.1.el9_2.x86_64 (mockbuild@x86-vm-09.build.en>
Aug 03 12:42:16 server.iti.com kernel: The list of certified hardware and cloud instances for Red Hat Enterpris>
Aug 03 12:42:16 server.iti.com kernel: Command line: BOOT_IMAGE=(hd0,msdos1)/vmlinuz-5.14.0-284.11.1.el9_2.x86_>
Aug 03 12:42:16 server.iti.com kernel: Disabled fast string operations
Aug 03 12:42:16 server.iti.com kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
```

- ممكن كمان احددله ال Logs بتاعت ال Service ممكن مثلا اقوله اعرضلي ال Logs بتاعت ال Service اللي ال Process ID بتاعتها ب 1 اللي هي ال Systemd Process هستخدم _PID= واكتبله ال PID

```
[root@MohamedAtef ~]# journalctl _PID=1
Aug 03 12:42:17 server.iti.com systemd[1]: Starting Create Volatile Files and Directories...
Aug 03 12:42:17 server.iti.com systemd[1]: Finished Create Volatile Files and Directories.
Aug 03 12:42:17 server.iti.com systemd[1]: Finished dracut cmdline hook.
Aug 03 12:42:17 server.iti.com systemd[1]: Starting dracut pre-udev hook...
Aug 03 12:42:17 server.iti.com systemd[1]: Finished dracut pre-udev hook.
```

- لو انا عايز اعرض ال Logs الخاصه ب User معين هستخدم _UID= وبعدين ال User ID الخاص بيه

```
[root@MohamedAtef ~]# journalctl _UID=0
Aug 03 12:42:17 server.iti.com systemd-journald[253]: Data hash table of /run/log/journal/af86da5aff3e4562b2197>
Aug 03 12:42:17 server.iti.com systemd-journald[253]: /run/log/journal/af86da5aff3e4562b219715b46f478c3/system.>
Aug 03 12:42:17 server.iti.com systemd-journald[253]: Journal started
Aug 03 12:42:17 server.iti.com systemd-journald[253]: Runtime Journal (/run/log/journal/af86da5aff3e4562b219715>
Aug 03 12:42:16 server.iti.com systemd-sysusers[255]: Creating group 'nobody' with GID 65534.
Aug 03 12:42:16 server.iti.com systemd-sysusers[255]: Creating group 'users' with GID 100.
```

➢ لو عايز اعرض ال Logs بتاعت System Unit معينه او Service معينه بستخدم _SYSTEMD_UNIT=

```
[root@MohamedAtef ~]# journalctl _SYSTEMD_UNIT=NetworkManager
-- No entries --
```

- احنا قولنا ان ال journal بتبقي Stored تحت /run/log/ ومبتكونش Permanent ان انت اول اما تعمل reboot لل machine كل ال Logs هتتمسح ف علشان نخلي ال Logs دي موجوده وتكون Permanent محتاجين نعمل كذا Step

1- اول Step هنعمل Create ل Directory بنفس الاسم اللي هو journal تحت /var/log/

```
[root@MohamedAtef ~]# mkdir /var/log/journal
```

2- تاني Step هنخلي ال Owner بتاع ال Directory اللي عملنا ليه create يكون system-journal

```
[root@MohamedAtef ~]# chown -R root:systemd-journal /var/log/journal
```

3- تالت Step هنظبط ال Permissions ان احنا هنخلي علي ال Directory يكون عليه Set group id permissions ان اي file او Directoryهيتعمله create في ال journal directory هيبقي ال Group ownership بتاعه نفس الاسم ده systemd-journal

```
[root@MohamedAtef ~]#  chmod g+s /var/log/journal/
```

4- رابع Step هنفتح ال Configuration file بتاع ال Journal بيكون موجود تحت /etc/systemd/ باسم journal.conf بيكون موجود فيه Parameters اسمه #storage=auto هنعملها uncomment ونخليه storage=persistent

```
[root@MohamedAtef ~]# vim /etc/systemd/journald.conf
[Journal]
Storage=persistent
#Compress=yes
#Seal=yes
#SplitMode=uid
```

5- اخر Step هنعمل restart للService اللي اسمها journald

```
[root@MohamedAtef ~]# systemctl restart systemd-journald
```

Maintaining Accurate Time

- هنشوف ازاي ن Configure ال Time Zone بتاعتنا ولو عايز اغير ال Time بتاعي هستخدم command اسمه **timedatectl**

➢ لو نفذنا ال command ده بس **timedatectl** هنلاقيه جايبلك ال Time Zone بتاعتك وهي Africa/Cairo وال Local time بتاعك

```
[root@MohamedAtef ~]# timedatectl
               Local time: Sat 2024-08-03 15:41:26 EET
           Universal time: Sat 2024-08-03 13:41:26 UTC
                 RTC time: Sat 2024-08-03 13:41:25
                Time zone: Africa/Cairo (EET, +0200)
System clock synchronized: no
              NTP service: inactive
          RTC in local TZ: no
```

➢ لو انا عايز اعمل List لكل ال Available Zones الموجوده عندي هستخدم **timedatectl list-timezones**

```
[root@MohamedAtef ~]# timedatectl list-timezones
Africa/Abidjan
Africa/Accra
Africa/Addis_Ababa
Africa/Algiers
Africa/Asmara
Africa/Asmera
Africa/Bamako
```

➢ لو انا عايز اغير ال zone بتاعتي هستخدم

```
[root@MohamedAtef ~]# timedatectl set-timezone America/Aruba
```

➢ لو انا عايز اختار ال time zone بتاعتي بطريقه Interactive هتسخدم command اسمه **tzselect**

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

➢ لو انا عايز اعمل Set لل Time بتاعي هستخدم

```
[root@MohamedAtef ~]# timedatectl set-time 9:00:00
```

Chapter 12

Managing Networking

Gathering network interface information

- Identifying Network Interfaces

The **ip link** command will list all network interfaces available on your system

```
[user@host ~]$ ip link show
```

- Displaying IP Addresses

```
[user@host ~]$ ip addr show ens160
```

- Displaying Performance Statistics

```
[user@host ~]$ ip -s link show ens160
```

- لو انا عايز اعرف كل ال Interfaces المتاحه عندي هستخدم **ip link show** وكان قبل كده كنا بنستخدم command اسمه **ifconfig** ف لو نفذنا ال command ده هتلاقيه بيقولك انك عندك interface اسمه ens160 وجايبلك تفاصيل عنه

```
[root@MohamedAtef ~]# ifconfig
ens160: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.76.132  netmask 255.255.255.0  broadcast 172.16.76.255
        inet6 fe80::20c:29ff:fe2f:5b7f  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:2f:5b:7f  txqueuelen 1000  (Ethernet)
        RX packets 2950  bytes 286355 (279.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1389  bytes 168654 (164.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
```

- لو انا عايز اجيب نفس ال Information اللي ظهرت لما استخدمنا ifconfig هسستخدمip link show

```
[root@MohamedAtef ~]# ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:2f:5b:7f brd ff:ff:ff:ff:ff:ff
    altname enp3s0
```

- لو عايز اجيب statistics عن Interfaces بتاعتي هزود اوبشن **-s** ف هتلاقي مثلا في ال ens160 هتلاقي ال packets ال received اللي هي RX ودي ال Incoming Traffic اللي جايه علي ال Interface ده ens160 علي ال Server وعندي Packets كمان لل Transmitted وهي TX ف كل مره بتعمل run لنفس ال command ده ip -s link show هتلاقي ال status بتاعتك بتزيد

```
[root@MohamedAtef ~]# ip -s link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    RX:  bytes packets errors dropped  missed   mcast
         9355     103      0       0       0       0
    TX:  bytes packets errors dropped carrier collsns
         9355     103      0       0       0       0
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode DEFAULT group default qlen 1000
    link/ether 00:0c:29:2f:5b:7f brd ff:ff:ff:ff:ff:ff
    RX:  bytes packets errors dropped  missed   mcast
       309899    3189      0       0       0     491
    TX:  bytes packets errors dropped carrier collsns
       179929    1477      0       0       0       0
    altname enp3s0
```

- لو اجيب معلومات اكتر عن ال Ip Address هستخدم **ip addresss show** او ممكن **ip add show** ك اختصار وده هيطلعلك نفس المعلومات اللي كان بيطلعها ifconfig

```
[root@MohamedAtef ~]# ip add show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2f:5b:7f brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 172.16.76.132/24 brd 172.16.76.255 scope global dynamic noprefixroute ens160
       valid_lft 1181sec preferred_lft 1181sec
    inet6 fe80::20c:29ff:fe2f:5b7f/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- لو انت عندك اي Connectivity issues ان مثلا ال server مابينه ومابين ال Server التاني فيه مشكله ف اول حاجه احنا بنعملها بنعمل Ping علي ال Server

```
[root@MohamedAtef ~]# ping 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=1 ttl=128 time=1.40 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=128 time=1.20 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=128 time=1.16 ms
64 bytes from 192.168.1.4: icmp_seq=4 ttl=128 time=1.06 ms
```

- لو انت عايز تعمل Ping ب عدد معين ان هو يعملك ping كام مره هستخدم اوبشن **-c**

```
[root@MohamedAtef ~]# ping -c 3 192.168.1.4
PING 192.168.1.4 (192.168.1.4) 56(84) bytes of data.
64 bytes from 192.168.1.4: icmp_seq=1 ttl=128 time=0.542 ms
64 bytes from 192.168.1.4: icmp_seq=2 ttl=128 time=0.280 ms
64 bytes from 192.168.1.4: icmp_seq=3 ttl=128 time=0.282 ms
--- 192.168.1.4 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
```

- لو انا عايز اعمل Display لل routing table هستخدم **ip route**

```
[root@MohamedAtef ~]# ip route
default via 172.16.76.2 dev ens160 proto dhcp src 172.16.76.132 metric 100
172.16.76.0/24 dev ens160 proto kernel scope link src 172.16.76.132 metric 100
```

- او ممكن استخدم Command تاني علشان اعرض ال routing table هستخدم **netstat -nr**

```
[root@MohamedAtef ~]# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt  Iface
0.0.0.0         172.16.76.2     0.0.0.0         UG        0 0          0  ens160
172.16.76.0     0.0.0.0         255.255.255.0   U         0 0          0  ens160
```

- لو انا عايز اعمل check مابين Two Hosts هستخدم command اسمه **tracepath** او **traceroute** بمعني ان ممكن يكون عندي مشكله وانا مش عارف ايه السبب مابين two hosts او الراوتر

```
[root@MohamedAtef ~]# tracepath access.redhat.com
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway                          0.258ms
 1:  _gateway                          0.207ms
```

Troubleshooting ports and services

- TCP services use **sockets** as end points for communication and are made up of an **IP address**, **protocol**, and **port number**.
- Services typically listen on standard ports while clients use a random available port. Well-known names for standard ports are listed in the **/etc/services** file.
- The **ss** command is used to display socket statistics. The ss command is meant to replace the older tool **netstat**, part of the net-tools package, which may be more familiar to some system administrators but which is not always installed

```
[user@host ~]$ ss -ta
```

OPTION	DESCRIPTION
-n	Show numbers instead of names for interfaces and ports.
-t	Show TCP sockets.
-u	Show UDP sockets.
-l	Show only listening sockets.
-a	Show all (listening and established) sockets.
-p	Show the process using the sockets.

- لو انا عايز اعمل Troubleshooting ل Ports او Services معينه فيه عندي حاجه اسمها sockets يعني ايه sockets انا علشان اعمل communicate علي اي Destination او علي اي Server معين لازم اروح اعمل communicate مع ال Server باستخدام ال Sockets وبيتكون من 3 حاجات اول حاجه IP ال Server نفسه وتاني حاجه ال Port Number وتالت حاجه ال Protocol التلاته دول اسهم sockets
- كل Service عندي بيبقي ليها Default Port زي مثلا ال SSH Server ودي بيكون ليها Default port 22 ف وانا بعمل communicate مع ال server ف انا بكلمه بال SSH ف لازم اكلم IP ال Server واكلمه بال Port 22 وال Protocol هل هو TCP او UDP

- هنلاقي معظم ال Standard Ports موجوده في /etc/services

```
[root@MohamedAtef ~]# less /etc/services
tcpmux          1/tcp                   # TCP port service multiplexer
tcpmux          1/udp                   # TCP port service multiplexer
rje             5/tcp                   # Remote Job Entry
rje             5/udp                   # Remote Job Entry
echo            7/tcp
echo            7/udp
discard         9/tcp           sink null
discard         9/udp           sink null
systat          11/tcp          users
systat          11/udp          users
daytime         13/tcp 2:
```

➢ لو عايز اجيب More Details عن ال Sockets بستخدم Command اسمه ss وقبل كده كنا بنستخدم command اسمه netstat

```
[root@MohamedAtef ~]# ss
Netid State   Recv-Q  Send-Q          Local Address:Port          Peer Address:Port   Process
u_dgr ESTAB   0       0          /run/systemd/notify 13767                  * 0
u_dgr ESTAB   0       0     /run/systemd/journal/dev-log 13780              * 0
u_dgr ESTAB   0       0     /run/systemd/journal/socket 13782               * 0
u_str ESTAB   0       0          @/tmp/dbus-xplvFHNLwa 35264                * 35263
u_str ESTAB   0       0                                  * 31156             * 31157
u_str ESTAB   0       0                                  * 29340             * 29341
u_str ESTAB   0       0                                  * 36238             * 36239
u_str ESTAB   0       0                                  * 33460             * 33461
u_dgr ESTAB   0       0                                  * 29172             * 13782
u_str ESTAB   0       0                                  * 28541             * 28542
```

➢ وممكن استخدم معاه الاوبشن دي لو انا عايز اعمل show لل TCP sockets او ال UDP وهكذا

Option	Description
`-n`	Show numbers instead of names for interfaces and ports.
`-t`	Show TCP sockets.
`-u`	Show UDP sockets.
`-l`	Show only listening sockets.
`-a`	Show all (listening and established) sockets.
`-p`	Show the process that uses the sockets.
`-A inet`	Display active connections (but not listening sockets) for the inet address family. That is, ignore local UNIX domain sockets. For the ss command, both IPv4 and IPv6 connections are displayed. For the netstat command, only IPv4 connections are displayed. (The netstat -A inet6 command displays IPv6 connections, and the netstat -46 command displays IPv4 and IPv6 at the same time.)

Configure network from the command line

- **RHEL8**
  - The **nmcli** utility is used to create and edit connection files from the command line and save configuration files in the **/etc/sysconfig/network-scripts** directory

```
[root@RHEL9 ~]# ls /etc/sysconfig/network-scripts
ifcfg-ens160
```

- لو انا عايز اعمل Configure لل Network بتاعتي هستخدم Utility او Tool اسمها **nmcli** وده ال Command اللي بستخدمه علشان اعمل configure لل Network عن طريق ال CLI
- في RHEL8 كان By Default اي Connections جديد بتعمله Create دا كان بي create ليه Text File تحت **/etc/sysconfig/network-scripts** وبيكون اسمه **Ifcfg-** واسم ال Connection بتاعك وال Text file بيكون موجود فيه كل ال Configurations اللي انت حاططها لل Interface زي ال IP Address وال Gateway وال Subnet mask وال DNS وال Interface name وهكذا

Configure network from the command line

- **RHEL9** (Say goodbye to ifcfg-files, and hello to keyfiles)
  - The **nmcli** command can be used to modify the network configuration. Network configuration will be written to files in the **/etc/NetworkManager/system-connections/** directory
  - The old network-scripts package has been removed (it was deprecated in the RHEL 8) which means you'll not find anything in the **/etc/sysconfig/network-scripts** directory

```
[root@RHEL9 ~]# ls /etc/sysconfig/network-scripts
[root@RHEL9 ~]# ls /etc/NetworkManager/system-connections/
ens160.nmconnection
```

- بدايه من RHEL9 اي connection بيتعمله Create هيكون موجوده تحت /etc/NetworkManager/system-connections/ وبيتعمله Create في هيئه key file format
  - لو دخلنا جوه ال Path ده وعملنا ls هنلاقي فيه Text File باسم ens160.nmconnection

```
[root@MohamedAtef ~]# cd /etc/NetworkManager/system-connections/
[root@MohamedAtef system-connections]# ls
ens160.nmconnection
```

- لو عملنا cat علي ال file ده هنلاقي ال Configuration بتاعت ال Connection ده ف هتلاقيه جايبلك ال id وال uuid وال type وهكذا

```
[root@MohamedAtef system-connections]# cat ens160.nmconnection
[connection]
id=ens160
uuid=1a242504-8d3f-39e7-a113-3673c6e983b0
type=ethernet
autoconnect-priority=-999
interface-name=ens160
[ethernet]
[ipv4]
method=auto
[ipv6]
addr-gen-mode=eui64
method=auto
[proxy]
```

- لو انا عايز اشوف ال Status بتاعت ال Network Devices ال Network interface ذات نفسه هستخدم **nmcli device status** ف هتلاقيه قايلك ان عندك Device اسمه ens160 ونوعه ethernet ومعمول يه connected

```
[root@MohamedAtef ~]# nmcli device status
DEVICE  TYPE       STATE              CONNECTION
ens160  ethernet   connected          ens160
lo      loopback   connected (externally)  lo
```

- لو انا عايز اجيب ال Status بتاعت ال Connections هستخدم nmcli connection show

```
oot@MohamedAtef ~]# nmcli connection show
NAME    UUID                                  TYPE      DEVICE
ens160  1a242504-8d3f-39e7-a113-3673c6e983b0  ethernet  ens160
lo      efbb9fb9-316e-4417-85e7-f84600a1d1c9  loopback  lo
```

Adding a network connection

- The **nmcli con add** command is used to add new network connections.

The next example creates an **static-ens224** connection for the **ens224** device with a static IPv4 address, using the IPv4 address and network prefix **192.168.0.5/24** and default gateway **192.168.0.254**, but still **auto connects** at startup and saves its configuration into the same file.

```
[root@host ~]#nmcli connection add con-name static-ens224 type
ethernet ifname ens224 ipv4.addresses 192.168.1.55/24 gw4 192.168.1.1
connection.autoconnect yes ipv4.method manual
```

- علشان اعمل Add ل New Connections هستخدم **nmcli con add**
- في المثال اللي فوق هو عايزك تعمل add ل connection وهيكون اسمه static-ens224 واديله static ip وهيكون ال IP Address الخاص بيه هو192.168.1.55/24 وال Gateway هيكون 192.168.0.254 وقايلك كمان auto connects وفي الاخر لازم تحددله ال method بتاعتك انك هتشتغل automatic ولا Manual
- انت هنا مبتحفظش كل اعتمادك علي ال Tab وتشوف ال Option اللي انت عايز تستخدمه يعني لو ضغط علي tab مرتين بعد nmcli connection add هيجبلك حوالي 107 اوبشن ممكن تستخدمهم زي مثلا

```
[root@MohamedAtef ~]# nmcli connection add
Display all 107 possibilities? (y or n)
autoconnect                      ipv4.addresses                    ipv6.dhcp-send-hostname
con-name                         ipv4.auto-route-ext-gw            ipv6.dhcp-timeout
connection.auth-retries          ipv4.dad-timeout                  ipv6.dns
connection.autoconnect           ipv4.dhcp-client-id               ipv6.dns-options
connection.autoconnect-priority  ipv4.dhcp-fqdn                    ipv6.dns-priority
connection.autoconnect-retries   ipv4.dhcp-hostname                ipv6.dns-search
connection.autoconnect-slaves    ipv4.dhcp-hostname-flags          ipv6.gateway
connection.dns-over-tls          ipv4.dhcp-iaid                    ipv6.ignore-auto-dns
connection.gateway-ping-timeout  ipv4.dhcp-reject-servers          ipv6.ignore-auto-routes
connection.id                    ipv4.dhcp-send-hostname           ipv6.ip6-privacy
connection.interface-name        ipv4.dhcp-timeout                 ipv6.may-fail
connection.lldp                  ipv4.dhcp-vendor-class-identifier ipv6.method
connection.llmnr                 ipv4.dns                          ipv6.mtu
```

- في المثال اللي فوق هو عايزك تعمل add ل connection جديد ف هنستخدم **nmcli connection add**
- بعد كده مطلوب منك ان ال connection ده يكون اسمه static-ens224 ف هنستخدم اوبشن **con-name** وبعدين اسم ال Connection ف هيكون con-name static-ens224
- بعد كده نوع ال connection ده هيكون ethernet ف هنستخدم اوبشن **type** وبعدين نوع ال connection ف هيكون type ethernet
- بعد كده قايلك ان هو عايز ال Interface name هيكون ens224 ف هنستخدم اوبشن **ifname** وبعدين اسم ال interface ف هيكون ifname ens224
- بعد كده مطلوب منك انك تحط ال IP Address وهو 192.168.1.55/24 ف هنستخدم **ipv4.addresses**
- بعد كده ال Gateway هيكون 192.168.1.1 ف هنستخدم اوبشن **ipv4.gateway** او استخدم الاختصار **gw4**

- وقايلك انك تخلي ال connection ده تخليه auto connect ف هتسخدم اوبشن **autoconnect yes** ومعناه ن انت لما تشغل الجهاز بتاعك هو هيقوم ال Interface ده علي طول
- بعد كده لازم تحددله ال method اللي انت شغال بيها اذا كانت auto او manual او disable احنا شغالين manual ف هنستخدم اوبشن **ipv4.method manual**

```
[root@MohamedAtef ~]# nmcli connection add con-name static-ens224 type ethernet ifname ens224
ipv4.addresses 192.168.1.55/24 gw4 192.168.1.1 connection.autoconnect yes ipv4.method manual
Connection 'static-ens224' (c0975592-0777-4b2d-bc9a-1d98768b2217) successfully added.
```

- لو دخلنا تحت /etc/NetworkManager/system-connections/ وعملنا ls هنلاقي ان عمل create ل Text File بال Connection الجديد static-ens224.nmconnection

```
[root@MohamedAtef ~]# cd /etc/NetworkManager/system-connections/
[root@MohamedAtef system-connections]# ls
ens160.nmconnection  static-ens224.nmconnection
```

- ولو عملنا **nmcli connection show** علشان نشوف ال Interafces اللي عندي

```
root@MohamedAtef ~]# nmcli connection show
NAME          UUID                                  TYPE      DEVICE
ens160        1a242504-8d3f-39e7-a113-3673c6e983b0  ethernet  ens160
lo            e32b44ef-bc28-4e73-8bc3-06e6cb113191  loopback  lo
static-ens224 c0975592-0777-4b2d-bc9a-1d98768b2217  ethernet  ens224
```

Modifying network connection setting

- The **nmcli con mod name** command is used to change the settings for a connection.

To set the IPv4 address to **192.0.2.2/24** and default gateway to **192.0.2.254** for the connection **static-ens3**:

```
[root@host ~]# nmcli con mod static-ens3 ipv4.addresses "192.0.2.2/24 192.0.2.254"
```

- علشان اعمل modify هستخدم **nmcli con mod** وبعديه علي طول اسم ال Connection بتاعك اللي هتعمل عليه modify
- وليكن مثلا هتعمل modify ان انت هتغير ال IP Address وهتخليه 192.0.2.2/24 وال Gateway هتغيره ل 192.0.2.254 ف علشان تعمل كده هتستخدم **nmcli con mod** وبعدين اسم ال connection وهو static-ens3 وبعدين علشان اعدل ال IP Address هستخدم **ipv4.addresses** واكتب ال IP الجديد 192.0.2.2/24 وبد كده علشان اعدل في ال **Gateway** هستخدم **ipv4.gateway** وبعدين ال IP الجديد 192.0.2.254
- ممكن اكتب ال IP Address وال Gateway في خطوه واحده عن طريق اكتب **ipv4.addresses** وبعدين بين ال double quotes "" هكتب ال IP Address وبعدين ال Gateway

Deleting a network connection

- The **nmcli con del name** command deletes the connection named name from the system, disconnecting it from the device and removing the file **/etc/sysconfig/network-scripts/ifcfg-name** in case of **RHEL8** and removing the file **/etc/NetworkManager/system-connections/name.nmconnection** in case of **RHEL9.**

```
[root@host ~]# nmcli con del static-ens3
```

- لو انا عايز اعمل Delete ل اي Connection او Interface هستخدم ال command ده **nmcli con del** وبعدين اسم ال Connection
- لو انت Red Hat 8 هيعمل remove لل file من تحت

  /etc/sysconfig/network-scripts/ifcfg-name
- ولو انت Red Hat 9 هيعمل remove لل file من تحت

  /etc/NetworkManger/system-connections/name.nmconnection

Who can modify network settings

- The root user can make any necessary network configuration changes with **nmcli**.
- Regular users that log in using ssh do not have access to change network permissions without becoming root.
- You can use the **nmcli gen permissions** command to see what your current permissions are.

```
[root@client ~]# nmcli gen permissions
PERMISSION                                                VALUE
org.freedesktop.NetworkManager.checkpoint-rollback        yes
org.freedesktop.NetworkManager.enable-disable-connectivity-check  yes
```

- ال command ده **nmcli gen permissions** بنستخدمه لو انا عايز اعرف ال User بتاعي عنده Permission انه يغير في ال Network ولا لا
- ال Root بس هو اللي ليه ال Permissions انه يغير في ال Network Configurations ف لما تستخدم ال Command ده مع ال Root هتلاقي كل حاجه عندك ب yes
- اما لو Regular User هتلاقي معندهوش Permissions هتلاقي ال VALUE ب No

Editing network configuration files

- By default, changes made with **nmcli con mod** name are automatically saved to:
  - /etc/sysconfig/network-scripts/ifcfg-name (**RHEL8**)
  - /etc/NetworkManager/system-connections/name.nmconnection (**RHEL9**)
- The files can also be manually edited with a text editor. After doing so, run **nmcli con reload** so that NetworkManager reads the configuration changes.
- It is also possible to configure the network by directly editing the connection configuration files. Connection configuration files control the software interfaces for individual network devices. These files are usually named **/etc/sysconfig/network-scripts/ifcfg-name** or **/etc/NetworkManager/system-connections/name.nmconnection** .

- فيه طريقه كمان ان انا اعمل Edit في ال Network Configurationبدون استخدام ال nmcli
- عن طريق ان انا هعدل في ال Configuration file ذات نفسه لو انا شغال علي Red Hat8 هعدل في ال file اللي هيكون تحت المسار ده /etc/sysconfig/network-scripts/ifcfg-name وبيكون بنفس اسم ال connection او ال Interface . ولو انا شغال علي ال Red Hat 9 هعدل في ال file اللي هيكون تحت المسار ده /etc/NetworkManger/system-connections/name.nmconnection وبيكون بنفس اسم ال connection او ال Interface
- هتلاقي ال File بالشكل ده ف اقدر اعدل فيه زي منا عايز

```
[connection]
id=static-ens224
uuid=c0975592-0777-4b2d-bc9a-1d98768b2217
type=ethernet

[ethernet]

[ipv4]
address1=192.168.1.5/24,192.168.1.1
method=manual

[ipv6]
addr-gen-mode=default
method=auto
[proxy]
```

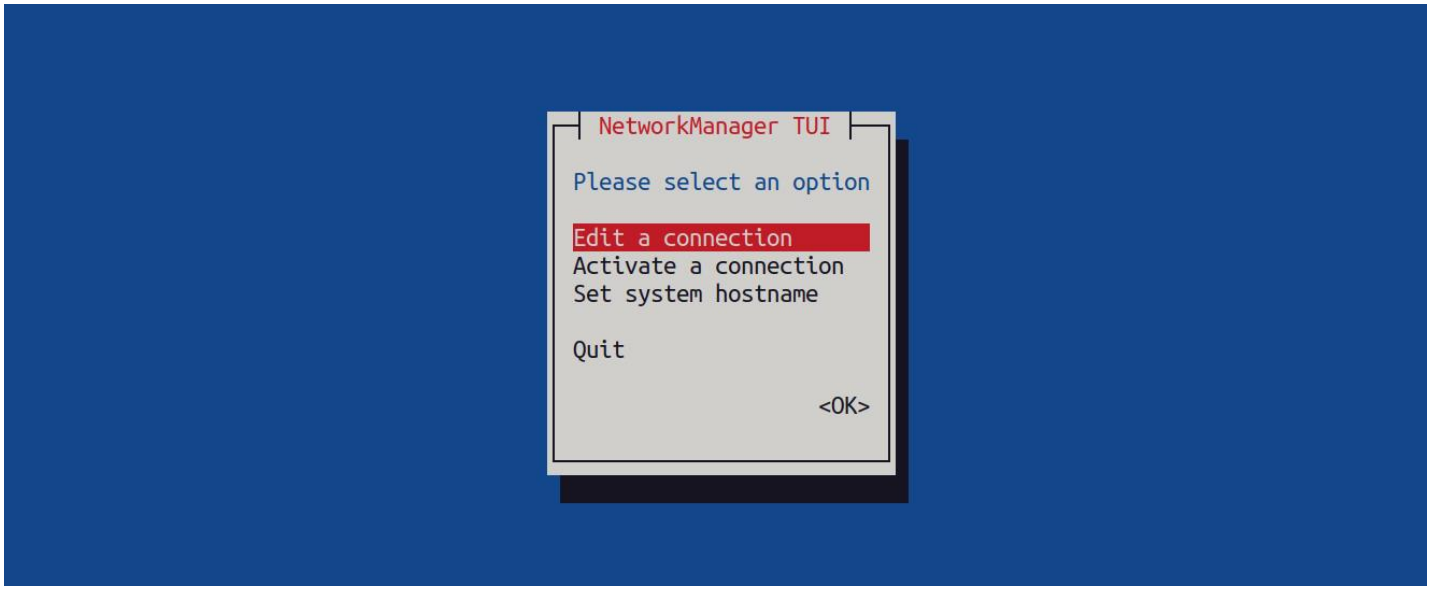
- وطالما غيرت في ال Configuration File ده ف لازم تعمل reload لل connection علشان يحس بالتغييرعن طريق انك هتستخدم **nmcli connection reload**

```
[root@MohamedAtef ~]# nmcli connection reload
```

- لو عملت reload ومحصلش اي تغيير ف عندك اوبشن تاني انك تعمل disconnect باستخدام اوبشن down لل connection بتاعك وبعدين تعمل connect تاني باستخدام اوبشن up

```
[root@MohamedAtef ~]# nmcli connection down static-ens224
[root@MohamedAtef ~]# nmcli connection up static-ens224
```

- فيه طريقه تالته لو انا عايز اعمل add ل connection جديد فيه tool عندي اسمها **nmtui** ال tool دي text User Interface ف لما تفتح معاك هيقولك انت عايز تعمل Edit a connection ولا Activate a connection ولا Set system hostname واللي انت عايزه هتختاره وهيدخلك علي قائمه تانيه علي حسب انت عايز ايه
- وليكن مثلا اخترت Edit a connection هيظهرلك قائمه موجود فيها ال Connections الموجوده وبيقولك انت عايز تعمل edit ولا Add ولا Delete



- دي كده Summary عن ال Commands اللي استخدمناها مع ال nmcli

Summary of commands

- The following table is a list of key **nmcli** commands discussed in this section.

COMMAND	PURPOSE
`nmcli dev status`	Show the NetworkManager status of all network interfaces.
`nmcli con show`	List all connections.
`nmcli con show` *name*	List the current settings for the connection *name*.
`nmcli con add con-name` *name*	Add a new connection named *name*.
`nmcli con mod` *name*	Modify the connection *name*.
`nmcli con reload`	Reload the configuration files (useful after they have been edited by hand).
`nmcli con up` *name*	Activate the connection *name*.
`nmcli dev dis` *dev*	Deactivate and disconnect the current connection on the network interface *dev*.
`nmcli con del` *name*	Delete the connection *name* and its configuration file.

Configuring host names and name resolution

- The **hostname** command displays or temporarily modifies the system's fully qualified host name.

```
[root@host ~]# hostname
host@example.com
```

- A static host name may be specified in the **/etc/hostname** file. The **hostnamectl** command is used to modify this file and may be used to view the status of the system's fully qualified host name.

```
[root@host ~]# hostnamectl set-hostname host@example.com
[root@host ~]# hostnamectl status
```

- لو انا عايز اعرف ال Hostname الخاص بال Server بتاعي او الجهاز بتاعي هستخدم hostname

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

- لو انا عايز اعرف ال Status بتاعت ال Hostname هستخدم hostnamectl status

```
[root@MohamedAtef ~]# hostnamectl status
 Static hostname: MohamedAtef
       Icon name: computer-vm
         Chassis: vm
      Machine ID: af86da5aff3e4562b219715b46f478c3
         Boot ID: a9213168a3644e7bb6b580140e331592
  Virtualization: vmware
Operating System: Red Hat Enterprise Linux 9.2 (Plow)
     CPE OS Name: cpe:/o:redhat:enterprise_linux:9::baseos
          Kernel: Linux 5.14.0-284.11.1.el9_2.x86_64
    Architecture: x86-64
 Hardware Vendor: VMware, Inc.
  Hardware Model: VMware Virtual Platform
Firmware Version: 6.00
```

- لو انا عايز اغير ال hostname هستخدم hostname set-hostname وبعد كده اسم ال hostname الجديد

```
[root@MohamedAtef ~]# hostnamectl set-hostname server.iti.com
```

- ال hostname بيكون Stored تحت /etc/hostname

```
[root@MohamedAtef ~]# cd /etc/hostname
```

Configuring name resolution

- The DNS resolver is used to convert host names to IP addresses or the reverse. It determines where to look based on the configuration of the **/etc/nsswitch.conf** file. By default, the contents of the **/etc/hosts** file are checked first

```
[root@host ~]# cat /etc/hosts
```

- If an entry is not found in the **/etc/hosts** file, by default the stub resolver tries to look up the hostname by using a DNS nameserver. The **/etc/resolv.conf** file controls how this query is performed:

```
[root@host ~]# cat /etc/resolv.conf
```

- ال DNS Servers نفسها بنستخدمها علشان ن resolve ال IP Address ل Domain او ال Domain ل IP Address. يعني انت مثلا لو عايز تدخل علي Web Site معين ف بتحط في ال Browser ال URL او ال Domain Name بتاعه بس انت في الاخر علشان ال Network بتاعتك شغاله بس ب IP Addresses ف انت هتبقي محتاج Services معينه ال Service دي هي المسئوله انها ت resolve ال Domain Name ل IP Address علشان تقدرت Access ال Destination ده
- احنا عندنا تحت /etc/ فيه file اسمه hosts ده بيتقال عليه ال Local DNS File بتاعك اللي اول حاجه ال DNS resolver بيروح يبص عليها هو ال Domain Name بتاعك موجود ليه record في /etc/hosts/ ولا لا لو موجود record هيعمل resolve وهيجبلك ال Ip Address اللي قدام ال Domain
- ولو ملاقهوش هيروح يسال ال DNS وال DNS بيبقي ال IP Address موجود في file اسمه resolv.conf تحت /etc/ ال File ده بتحط فيه ال DNS اللي انت في الاخر هتروح تساله عن ال IP Address بتاع ال Domain Name

Configuring name resolution

- NetworkManager updates the **/etc/resolv.conf** file using DNS settings in the connection configuration files. Use the nmcli to modify the connections.

```
[root@host ~]# nmcli con mod ens160 ipv4.dns 8.8.8.8
[root@host ~]# nmcli con down ens160
[root@host ~]# nmcli con up ens160
[root@host ~]# cat /etc/sysconfig/network-scripts/ifcfg-ens160          → RHEL8
[root@host ~]# cat /etc/NetworkManager/system-connections/ens160.nmconnection  → RHEL9
```

- ممكن كمان تعمل modify لل DNS عن طريق ان انت هتستخدم nmcli con mod وبعد اسم ال connection بتاعك وبعدين تستخدم اوبشن ipv4.dns وتضيف ال dns اللي انت عايزه

Chapter 13

Archiving and Transferring Files

Managing Compressed TAR Archives

- انا ك سيستم ادمن مهم جدا ان انا اخد backups من ال Files وال Directories المهمه عندي في السيستم زي مثلا /etc وده بيكون Stored جواه ال Main Configuration Files الموجوده عندي في ال System ف لو فيه اي file بالخطأ اتمسح وال file ده مهم جدا ف ممكن يحصل عندك اي مشكله في السيستم ف مهم جدا انك تاخد كل شويه backups من /etc وت Transferring ال backup ده علي remote system او remote server علشان لو فيه اي file اتسمح بالخطأ تقدر ترجع ال file ده
- ف علشان تقدر تعمل compress لل files بتستخدم command اسمه **Tar**

Options of the tar Command

- فيه عندنا Options بنستخدمهم مع ال **Tar**
- فيه عندي اوبشن **-c** او **--create** وده بستخدمه لو انا عايز اعمل Create ل New Archive
- وعندي اوبشن تاني **-x** او **--extract** وده بستخدمه لو انا عندي Archive وعايز اعمله extract
- وعندي اوبشن تاني **-t** او **--list** ده لو انا عايز اعمل List لل Content بتاعت ال Archive بتاعي من غير ماعمله extract
- فيه عندي اوبشن **-v** او **--verbose** - ده بس بيعرضلي ال Files اللي حصلها Archived او extracted
- واوبشن **-f** او **--file=** ده بستخدمه لو انا بعمل Archive ل file وعايزه باسم معين
- واوبشن **-p** او **--preserve-permissions** بستخدمه لو انا عايز احافظ علي ال Files بتاعتي من ال umask ان يحافظ علي ال Permissions بتاعتها

Archiving files and directories

- علشان اعمل Archive وليكن مثلا ل /etc هستخدم tar وهستخدم 3 options مع بعض اول اوبشن وهو c علشان اعمل create وتاني اوبشن v وده علشان يعرضلي ال files اللي حصلها Archive واوبشن f علشان ادي لل Archive ده اسم جديد ف هستخدمهم مع بعض بالشكل ده -cvf وبعد كده اديله اسم ال Archive الجديد وليكن انا هسميه etc_backup_20240804 انت سميه اي اسم عادي بس اهم حاجه امتداد ال file ده يكون tar. وبعد كده تديله اسم ال file او ال Directory اللي انت عايز تعمله Archive وفي حالتنا هو /etc

```
[root@MohamedAtef Desktop]# tar -cvf etc_backup_20240804.tar /etc
```

- لو احنا عملنا ls -l هنلاقيه عمل create ل Archive

```
[root@MohamedAtef Desktop]# ls -l
total 26872
-rw-r--r--. 1 root root 27514880 Aug  4 23:56 etc_backup_20240804.tar
```

- لو انا عايز اعرف ال Size بتاع ال file هستخدم command اسمه **du -s**

```
[root@MohamedAtef Desktop]# du -s /etc/
29560        /etc/
```

- لو انت عايز ال Size بتاعك بال ميجا هتستخدم **du -sh /etc** ف هو جايبلك اهو ان ال size بتاع ال etc/ بيكون 29 ميجا

```
[root@MohamedAtef Desktop]# du -sh /etc/
29M /etc/
```

- لو احنا استخدمنا نفس ال command علي ال Archive اللي احنا اخدناه ونشوف ال Size بتاعه هنلاقي ال size بتاعه بقي 27 ميجا هو هنا معملهوش compress علشان حجمه صغر لا هو هنا رتبهم بطريقه معينه ف ال size صغر شويه

```
[root@MohamedAtef Desktop]# du -sh etc_backup_20240804.tar
27M etc_backup_20240804.tar
```

- لو انا عايز اعمل List لل contained بتاعت ال Tar Archive هستخدم اوبشن **-tf**

```
[root@MohamedAtef Desktop]#  tar -tf etc_backup_20240804.tar
etc/
etc/mtab
etc/fstab
etc/crypttab
etc/dnf/
etc/dnf/modules.d/
etc/dnf/aliases.d/
```

- لو انا عايز اعمل Extract هستخدم اوبشن **-xf** وبعدين اديله اسم ال Tar Archive

```
[root@MohamedAtef Desktop]#  tar -xf etc_backup_20240804.tar
```

- لو عملنا **ls** هنلاقيه عمل extract لل Archive

```
[root@MohamedAtef Desktop]# ls
etc  etc_backup_20240804.tar
```

Creating a Compressed Archive

- لو انا عايز اعمل Compressed لل Archive ان انا عايز اضغط ال Archive . فيه عندي اكتر ممكن طريقه اني اعمل Compressed. وممكن عن طريق ال Tar تقدر تعمل Compress و Archive في نفس الوقت

1- اول طريقه وهي عن طريق ال **gzip** ف اني استخدم اوبشن **-z** او **--gzip** وبيكون امتداد ال Archive بيكون **.tar.gz**

- ف هعمل compress وArchive لل Directory اللي اسمه etc عن طريق اني استخدم

```
[root@MohamedAtef Desktop]# tar -czf etc_backup.tar.gz etc
```

- لو شوفنا مساحه ال archive هنلاقيه اتعمله Compress وال Size بتاعه 6.4 ميجا

```
[root@MohamedAtef Desktop]# du -sh *
29M etc
27M etc_backup_20240804.tar
6.4Metc_backup.tar.gz
```

- لو انت عايز تعمل Extract لل Compressed Archive File هتغير بس بدل ال c هتحط x

```
[root@MohamedAtef Desktop]# tar -xzf etc_backup.tar.gz
```

2- وتاني طريقه عن طريق ال **bzip2** عن طريق اني استخدم اوبشن **-j** او **--bzip2** وبيكو ن امتداد ال Archive بيكون **.tar.bz2**

```
[root@MohamedAtef Desktop]# tar -cjf etc_backup.tar.bz2 etc
```

- لو شوفنا مساحه ال archive هنلاقيه اتعمله Compress وال Size بتاعه 5.5 ميجا

```
[root@MohamedAtef Desktop]# du -sh *
29M etc
27M etc_backup_20240804.tar
5.5Metc_backup.tar.bz2
6.4Metc_backup.tar.gz
```

- لو انت عايز تعمل Extract لل Compressed Archive File هتغير بس بدل ال c هتحط x

```
[root@MohamedAtef Desktop]# tar -xjf etc_backup.tar.bz2
```

3- وتالت طريقه عن طريق ال **xz** عن طريق اني استخدم اوبشن J- او **--xz** وبيكو ن امتداد ال Archive بيكون **.tar.xz**

- لو شوفنا مساحه ال archive هنلاقيه اتعمله Compress وال Size بتاعه 4.5 ميجا

```
[root@MohamedAtef Desktop]# du -sh *
29M etc
27M etc_backup_20240804.tar
5.5Metc_backup.tar.bz2
6.4Metc_backup.tar.gz
4.5Metc_backup.tar.xz
```

- لو انت عايز تعمل Extract لل Compressed Archive File هتغير بس بدل ال c هتحط x

```
[root@MohamedAtef Desktop]# tar -xJf etc_backup.tar.xz
```

Compress and extract files using gzip, bzip2, and xz

- Additionally, ***gzip, bzip2, and xz*** can be used independently to compress single files.

```
[root@lab01 ~]# gzip etc.tar
[root@lab01 ~]# bzip2 abc.tar
[root@lab01 ~]# xz myarchive.tar
```

- The corresponding commands to decompress are ***gunzip, bunzip2, and unxz***.

```
[root@lab01 ~]# gunzip etc.tar.gz
[root@lab01 ~]# bunzip2 abc.tar.bz2
[root@lab01 ~]# unxz myarchive.tar.xz
```

Transferring files using secure copy

- The Secure Copy command, ***scp***, which is part of the OpenSSH suite, copies files from a remote system to the local system or from the local system to a remote system.
- The following example demonstrates how to copy the local ***/etc/yum.conf*** and ***/etc/hosts*** files on host, to the remote user's home directory on the remote host remote system:

```
[user@host ~]$ scp /etc/yum.conf /etc/hosts remoteuser@remotehost:/home/remoteuser
```

- ازاي نت Transfer ال Files مابين ال Servers وبعضها خلال ال Network بتاعتك انا عندي Two Options او Two Commands

1- اول Command وهو اني استخدم **scp** وده اختصار ل Secure Copy Command وده بيكون Part من ال OpenSSH Protocol ف لو انا عايز اعمل Secure Copies لل file من ال remote system لل Local System او من ال Local System لل remote system فبستخدم ال Command بالطريقه دي بقوله **scp** وبعدين ال File اللي هعمله Transfer او مجموعه ال Files اللي هعملها Transfer وبعد كده بحط ال credential بتاعت ال Username وال IP بتاع ال Remote Server وبعدين ال Location اللي انا عايز اعمل Transfer لل Files فيها

- وليكن مثلا انا عايز اخد copy من ال Local System لل Remote System مثلا لو عندي Archive اسمه etc.tar وعايز اعمله Transfer لل Server لل User اللي اسمه root ف علشان اعمل كده هستخدم scp وبعدين ال Archive اللي هعمله transfer وهو etc.tar وبعد كده ال user اللي انت عايز تعمل ليه ال Transfer علي ال Server وهو ال root وبعد كده @ وبعدين اكتب IP ال Server وهو 192.168.220.129 وبعدين colon : وبعدين ال Path اللي هنقل فيه ال Archive وهنا انا عايزه يكون في /root/

```
[root@MohamedAtef Desktop]# scp etc.tar root@192.168.220.129:/root
```

- لو انا عايز اعمل العكس ان انا اخد حاجه من عند ال remote Server ل عندي علي ال Local Server عن طريق ان انت هتقوله ال scp وبعدين هتحددله ال Source بتاعك من حيث ال user وال IP وبعدين احددله ال File موجود فين وبعدين احددله ال Path اللي هنقل ال File ده عليه

```
[root@MohamedAtef Desktop]# scp  root@192.168.220.129:/root/data.txt /Desktop/
```

- لو انا هعمل transfer ل Directory هزود اوبشن -r

```
[root@MohamedAtef Desktop]# scp -r etc root@192.168.220.129:/root
```

Transferring files using the secure file transfer program

- To interactively upload or download files from a SSH server, use the Secure File Transfer Program, ***sftp.*** A session with the ***sftp*** command uses the secure authentication mechanism and encrypted data transfer to and from the SSH server.

```
[user@host ~]$ sftp remoteuser@remotehost
remoteuser@remotehost's password: password
Connected to remotehost.
sftp>
```

2- تاني طريقه اني استخدم **sftp** بس ال **sftp** بيفتحلك interactive session مع ال remote server ف تقدر من خلالها ان انت ت Download او ت Upload ال Files من والي ال Server بتاعك عن طريق ان انت هتقوله **sftp** وال remote user name وبعدين @ وبعدين ال remote host

- وليكن مثلا هعمل Transfer ل file علي ال Server اللي IP بتاعه هو 192.168.1.1

```
[root@MohamedAtef Desktop]# sftp root@192.168.1.1
sftp> ls
```

- هو كده فاتح Interactive Session ف اي Command انا بنفذه كده هيتنفذ علي ال remote server لو انا عايز انفذ ال Command عندي انا علي ال Local هستخدم l قبل اي Command

```
[root@MohamedAtef Desktop]# sftp root@192.168.1.1
sftp> lls
```

- لو انا عايز اعمل transfer باستخدام ال sftp هستخدم **put** وبعدين اسم ال file كده بيعمل Upload علي ال Server

```
[root@MohamedAtef Desktop]# sftp root@192.168.1.1
sftp> put test_file
```

- لو انا عايز اعمل Download ل file معين عندي هستخدم بدل **put** هستخدم **get**

```
[root@MohamedAtef Desktop]# sftp root@192.168.1.1
sftp> get test_file
```

Chapter 14

Installing and Updating Software Packages

Explaining and investigating RPM software packages

- RPM package files names consist of four elements (plus the .rpm suffix): ***name-versionrelease.architecture***

coreutils - 8.30 - 4.el8 . x86_64 .rpm

Name Version Release Arch

- ***NAME*** is one or more words describing the contents (***coreutils***).
- ***VERSION*** is the version number of the original software (***8.30***).
- ***RELEASE*** is the release number of the package based on that version, and is set by the packager, who might not be the original software developer (***4.el8***).
- ***ARCH*** is the processor architecture the package was compiled to run on. ***noarch*** indicates that this package's contents are not architecture-specific (as opposed to ***x86_64*** for 64-bit, ***aarch64*** for 64-bit ARM, and so on).

```
[root@server ~]# uname –a  and cat /etc/redhat-release
```

- انا عندي اي Software او Program في اللينكس بنقول عليها Packages او RPM Packages لو احنا عايزين نعمل download ل اي Software Packages من علي النت هنقدر نطلع من اسمها ب 4 معلومات
  - اول معلومه وهي ال Name ودي بتتكون من كلمه او كلمتين او اكتر بتصف ال content بتاعت ال Package
  - تاني معلومه وهي ال Version بتاعت ال RPM Package
  - تالت معلومه وهي ال Release بتاعت ال Package
  - رابع معلومه وهي ال Architecture Type CPU وعندي كذاا نوع ممكن يكون x86_64 او aarch64
  - اخر حاجه لازم ال Extension يكون rpm
- لو انت عايز تعرف اصدار ال Operating System بتاعك ايه فيهfile اسمه redhat-release تحت /etc/ لو عملت cat علي ال file ده هيعرضلك ال Version الخاص بال Operating System بتاعك

```
[root@MohamedAtef ~]# cat /etc/redhat-release
Red Hat Enterprise Linux release 9.2 (Plow)
```

- لو انت عايز تعرف ال CPU Architecture بتاعك ايه هتستخدم command اسمه uname -a

```
[root@MohamedAtef ~]# uname -a
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 x86_64 GNU/Linux
```

- لو انت عايز تعمل Download ل Package معينه من علي الانترنت ومعاك رابط ال Package دي ممكن تستخدم command اسمه wget وبعدين ال Url

```
[root@MohamedAtef ~]# wget https://rpmfind.net/linux/fedora/ Packages/s/sysstat-12.7.6-2.fc41.aarch64.rpm
```

Explaining RPM software packages

- The *rpm* utility is a low-level tool that can get information about the contents of package files and installed packages.
- ***rpm -qa:*** List all installed packages
- ***rpm -qf FILENAME:*** Find out what package provides FILENAME
- ***rpm -q yum:*** List what version of the package is currently installed
- ***rpm -qi yum:*** Get detailed information about the package
- ***rpm -ql yum:*** List the files installed by the package
- ***rpm -qc yum:*** List just the configuration files installed by the package
- ***rpm -qd yum:*** List just the documentation files installed by the package
- ***rpm -q --scripts openssh-server:*** List shell scripts that run before or after the package is installed or removed
- ***rpm -q --changelog:*** list change information for the package

- علشان اعمل Install او remove ل اي Package عندي من ال CLI عندي Two Tools وهما ال rpm وال yum
- اول Tool وهي ال rpm ده بستخدمه لو انا عايز اعمل List ل اي Package معمول ليها Install عندي او اعمل Install ل اي Package او اعمل remove

➢ لو انا عايز اعمل List لكل ال Packages ال Install عندي هستخدم **rpm -qa**

```
[root@MohamedAtef ~]# rpm -qa
libgcc-11.3.1-4.3.el9.x86_64
fonts-filesystem-2.0.5-7.el9.1.noarch
linux-firmware-whence-20230310-133.el9_2.noarch
crypto-policies-20221215-1.git9a18988.el9.noarch
hwdata-0.348-9.7.el9.noarch
xkeyboard-config-2.33-2.el9.noarch
tzdata-2022g-2.el9.noarch
liberation-fonts-common-2.1.3-4.el9.noarch
hyperv-daemons-license-0-0.41.20190303git.el9.noarch
```

➢ لو انا عايز اعمل Search علي Package معينه هستخدم **rpm -qa** وبعدين اسم ال Package وليكن مثلا yum

```
[root@MohamedAtef ~]# rpm -qa yum
yum-4.14.0-5.el9_2.noarch
```

➢ لو انا عايز معلومات اكتر عن Package معينه هستخدم **rpm -qi** وبعدين اسم ال Package

```
[root@MohamedAtef ~]# rpm -qi yum
Name        : yum
Version     : 4.14.0
Release     : 5.el9_2
Architecture: noarch
Install Date: Tue 05 Mar 2024 07:28:45 PM EET
Group       : Unspecified
Size        : 77898
License     : GPLv2+
Signature   : RSA/SHA256, Thu 16 Mar 2023 01:37:19 PM EET, Key ID 199e2f91fd431d51
Source RPM  : dnf-4.14.0-5.el9_2.src.rpm
Build Date  : Wed 15 Mar 2023 03:50:32 PM EET
```

- لو انا عايز اعمل List لكل ال Files الموجوده في ال Package هستخدم **rpm -ql** وبعدين اسم ال Packages

```
[root@MohamedAtef ~]# rpm -ql yum
/etc/dnf/protected.d/yum.conf
/etc/yum.conf
/etc/yum/pluginconf.d
/etc/yum/protected.d
/etc/yum/vars
/usr/bin/yum
/usr/share/man/man1/yum-aliases.1.gz
/usr/share/man/man5/yum.conf.5.gz
/usr/share/man/man8/yum-shell.8.gz
/usr/share/man/man8/yum.8.gz
```

- لو انا عايز اعمل List لل Configuration File بس هستخدم **rpm -qc** وبعدين اسم ال Packages

```
[root@MohamedAtef ~]# rpm -qc yum
/etc/dnf/protected.d/yum.conf
```

- لو انا عايز اعمل List لل Documentation بس هستخدم **rpm -qd**

```
[root@MohamedAtef ~]# rpm -qd yum
/usr/share/man/man1/yum-aliases.1.gz
/usr/share/man/man5/yum.conf.5.gz
/usr/share/man/man8/yum-shell.8.gz
/usr/share/man/man8/yum.8.gz
```

- لو انا ايز اعرف معلومات عن ال Change اللي حصلت ل اي packages هستخدم **rpm -q --changelog** وبعدين اسم ال Package

```
[root@MohamedAtef ~]# rpm -q --changelog yum
* Wed Mar 15 2023 Marek Blaha <mblaha@redhat.com> - 4.14.0-5
- Update translations

* Thu Jan 05 2023 Nicola Sella <nsella@redhat.com> - 4.14.0-4
- Ignore processing variable files with unsupported encoding (RhBug:2148871)

* Wed Dec 07 2022 Nicola Sella <nsella@redhat.com> - 4.14.0-3
- Move system-upgrade plugin to core (RhBug:2131288)
- offline-upgrade: add support for security filters (RhBug:1939975,2139326)
- Fix plugins unit tests + unload plugins upon their deletion

* Mon Oct 31 2022 Nicola Sella <nsella@redhat.com> - 4.14.0-2
- Pass whole URL in relativeUrl to PackageTarget for RPM URL download
```

Installing RPM packages

- The *rpm* command can also be used to install an RPM package that you have downloaded to your local directory.
- ***i*** → install package(s)
- ***v*** → Verbosity provide more detailed output
- ***h*** → Installation progress ####

```
[root@host ~]# rpm -ivh wonderwidgets-1.0-4.x86_64.rpm
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
Updating / installing...
   1:wonderwidgets-1.0-4              ################################# [100%]
[root@host ~]#
```

- علشان اعمل Install باستخدام ال rpm هستخدم **rpm -ivh** ال **i** معناها ان انت هتعمل install وال **v** معناها verbose علشان يعرضلك ال Output علي الشاشه اما ال **h** ده معنها #hash علشان وهو بيعمل Install يبجهولك علي هيئه ###hash
- لو انا عايز اعمل remove او uninstall ل Package معينه هستخدم **rpm -ev** وبعدين اسم ال Package
  - لو انا عايز اعمل uninstall مثلا لل Package الخاصه بال FireFox

```
[root@MohamedAtef ~]# rpm -ev firefox
Preparing packages...
firefox-102.9.0-3.el9_1.x86_64
```

  - لو انا عايز اعملها Install تاني هستخدم **rpm -ivh** واسم ال Packages

```
[root@MohamedAtef Packages]# rpm -ivh firefox-102.9.0-3.el9_1.x86_64.rpm
warning: firefox-102.9.0-3.el9_1.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID fd431d51: NOKEY
Verifying...                          ################################# [100%]
Preparing...                          ################################# [100%]
        package firefox-102.9.0-3.el9_1.x86_64 is already installed
```

Installing and updating software packages with YUM

- The low-level *rpm* command can be used to install packages, but it is not designed to work with package repositories or resolve dependencies from multiple sources automatically.
- *Yum* is designed to be a better system for managing RPM-based software installation and updates. The ***yum*** command allows you to install, update, remove, and get information about software packages and their dependencies.

Finding Software with Yum

- ***yum help*** displays usage information.
- ***yum list*** displays installed and available packages

```
[user@host ~]$ yum list 'http*'
```

- ***yum search KEYWORD*** lists packages by keywords found in the name and summary fields only.

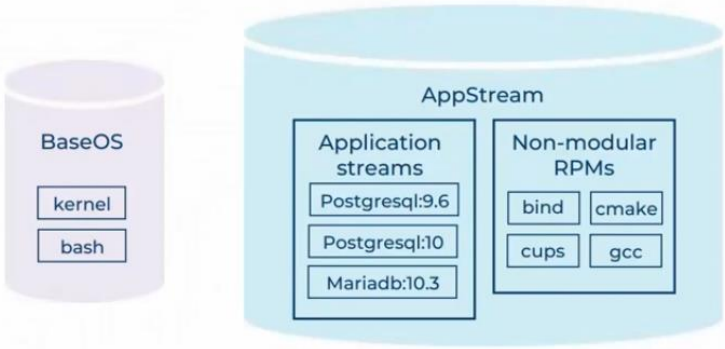
```
[user@host ~]$ yum search all 'web server'
```

- ال Yum او ال Dnf هما الاتنين واحد نفس ال Options ونفس ال Commands ال Yum ده جه يحل المشاكل اللي كانت في ال rpm
- ال Yum بيشتغل ب Concept ال Repository ان كل مره يعمل Install هيدور في ال Repository عن ال Package اللي انت عايزها ويعملها Install ولو فيه اي Package معتمد علي Packages تانيه هيعملها Install

Introduction to application stream

Two main repositories:

- The ***BaseOS*** repository mainly concerns the operating system.
- The ***AppStream*** repository contains application modules and non-modular RPMs.



IMPORTANT

- Both ***BaseOS*** and ***AppStream*** are a necessary part of a Red Hat Enterprise Linux 9 system.

- ايه هو ال Repository هو عباره عن Location او مكان سواء كان Local عندك او موجود علي Server تاني او موجود online بيكون موجود فيه كل ال Software Packages بتاعتك
- بدايه من Red Hat 8 بقي عندك Two Repository اول واحد اسمه BaseOS وده بيكون موجود فيه كل ال Packages اوال Software ودي بتكون operating system related لل Kernel او ال Bash والتاني AppStream وده بيكون فيه معظم ال Packages وبيكون عدد ال Packages اللي فيه اكبر من ال BaseOS

- علشان تقدر ت Configure ال Repository هتدخل جوه /etc/yum.repos.d/ وتعمل Create ل Two Files واحد يكون فيه ال Configuration بتاعت ال BaseOS Repository والتاني يكون فيه ال AppStream Repository او ممكن تعمل Create ل File واحد ويكون موجود فيه ال configuration الخاصه بال BaseOS وال AppStream احنا هنشتغل بال Local Repository ان احنا هن configure ال Yum انه يعمل Search في ال ISO Image ودي بيكون نازل معاها معظم ال Software Packages بتاعت Red Hat

```
[root@MohamedAtef ~]# cd /etc/yum.repos.d/
[root@MohamedAtef yum.repos.d]#
```

- علشان تقدر ت Access ال ISO Image لازم تعملها Mount وليكن هتعملها Mount تحت /media عن طريق ان انت هتستخدم mount -o loop /dev/sr0 /media

```
[root@MohamedAtef ~]# mount -o loop /dev/sr0 /media
```

- لو عملنا df -h علشان نتاكد هل عمله Mount ولا هتلاقيه عمله Mount تحت /media

```
[root@MohamedAtef ~]# df -h
Filesystem          Size  Used  Avail  Use%  Mounted on
devtmpfs            4.0M  0     4.0M   0%    /dev
tmpfs               374M  0     374M   0%    /dev/shm
tmpfs               150M  1.5M  148M   1%    /run
/dev/nvme0n1p2      20G   6.7G  14G    34%   /
/dev/nvme0n1p1      507M  249M  259M   49%   /boot
/dev/nvme0n1p3      20G   175M  20G    1%    /home
tmpfs               1.0M  0     1.0M   0%    /run/stratisd/ns_mounts
tmpfs               75M   100K  75M    1%    /run/user/0
/dev/sr0            9.0G  9.0G  0      100%  /run/media/root/RHEL-9-2-0-BaseOS-x86_641
/dev/loop0          9.0G  9.0G  0      100%  /media
```

- لو دخلنا علي /media وعملنا ls هتلاقي folder اسمه AppStream و Folder اسمه BaseOS

```
[root@MohamedAtef ~]# cd /media/
[root@MohamedAtef media]# ls
AppStream   EFI   extra_files.json   images   media.repo   RPM-GPG-KEY-redhat-release
BaseOS      EULA  GPL               isolinux RPM-GPG-KEY-redhat-beta
```

- لو عملنا List لل AppStream هتلاقي فيه Two Folder واحد اسمه Packages وده بيكون موجود فيه كل ال Packages بتاعتك والتاني اسمه repodata

```
[root@MohamedAtef media]# ls AppStream/
Packages  repodata
```

- ف احنا عملنا mount لل ISO Image بتاعتي ف هنعمل دلوقتي Create ل Two Files لل configuration بتاعت ال AppStream وال BaseOS ال Two Files دول هنعملهم Create في /etc/yum.repos.d/ ويكون امتداد ال files دي repo. مش شرط تسميهم AppStream او BaseOS اي اسم انت عايزه عاجي بس الامتداد يكون repo.

```
[root@MohamedAtef ~]# cd /etc/yum.repos.d/
[root@MohamedAtef yum.repos.d]# touch AppStream.repo BaseOS.repo
```

- بعد اما احنا عملنا Create لل Files هنعمل edit فيها ف هنستخدم ال Vim هنعمل edit في ال AppStream.repo ونفتح ال file ده بال vim ونكتب الاتي

```
[AppStream]
name = "RHEL9 Local AppStream Repo"
baseurl = file:///run/media/AppStream/
enable = 1
gpgcheck = 0
```

- هنعمل نفس الموضوع في ال File التاني ال BaseOS هنفتح ال File باستخدام ال vim و هنكتب

```
[BaseOS]
name = "RHEL9 Local BaseOS Repo"
baseurl = file://media/BaseOS/
enable = 1
gpgcheck = 0
```

- بعد كده هننفذ ال command ده **yum repolist** علشان نتاكد ان ال System شايف ال repo اللي احنا عملناه

```
[root@MohamedAtef ~]# yum repolist
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.
repo id                    repo name
AppStream                  RHEL9 Local AppStream Repo
BaseOS                     RHEL9 Local BaseOS Repo
```

- لو انت عايز تتاكد هل ال Repository دي Enable ولا Disable هتزود اوبشن **--all**

```
[root@MohamedAtef ~]# yum repolist --all
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.
repo id                    repo name                    status
AppStream                  RHEL9 Local AppStream Repo   enabled
BaseOS                     RHEL9 Local BaseOS Repo      enabled
```

- فيه warning بيظهرلك بيقولك Unable to read consumer identity وده مش related لل yum هو بيظهرلك علشان يقولك ان ال system not registered انه يستخدم ال subscription – manager فيه طريقه ان انا اعمل بيها Disable علشان ال warning ده ميظهرليش . بيكون فيه file تحت/etc/yum/pluginconf.d/ بيكون اسمه subscription-manager.conf هنفتح ال file ده و هنلاقي كلمه enable معموله ب 1 هنخليها ب zero

```
[root@MohamedAtef ~]# vim /etc/yum/pluginconf.d/subscription-manager.conf
 [main]
enabled=0
```

- لو عملنا تاني **yum repolist** هتلاقيه مجبلكش ال Warning اللي كان بيظهر

```
[root@MohamedAtef ~]# yum repolist
repo id                    repo name
AppStream                  RHEL9 Local AppStream Repo
BaseOS                     RHEL9 Local BaseOS Repo
```

- لو انا عايز اعرف معلومات اكتر عن ال yum وال Basic Options اللي ممكن استخدمها هستخدم اوبشن **help**

```
root@MohamedAtef ~]# yum help
usage: yum [options] COMMAND
List of Main Commands:
alias            List or create command aliases
autoremove       remove all unneeded packages that were originally installed as dependencies
check            check for problems in the packagedb
check-update     check for available package upgrades
clean            remove cached data
deplist          [deprecated, use repoquery --deplist] List package's dependencies and what packages provide them
```

- لو انا عايز اعمل List لكل ال installed وال Available Packages هستخدم اوبشن **list**

```
[root@MohamedAtef ~]# yum list
Last metadata expiration check: 0:09:00 ago on Mon 05 Aug 2024 06:02:19 PM EET.
Installed Packages
ModemManager.x86_64                    1.20.2-1.el9          @anaconda
ModemManager-glib.x86_64               1.20.2-1.el9          @anaconda
NetworkManager.x86_64                  1:1.42.2-1.el9        @anaconda
NetworkManager-adsl.x86_64             1:1.42.2-1.el9        @anaconda
NetworkManager-bluetooth.x86_64        1:1.42.2-1.el9        @anaconda
NetworkManager-config-server.noarch    1:1.42.2-1.el9        @anaconda
```

- لو انا عايز اعرف Information عن Package معينه هستخدم اوبشن **info**

```
[root@MohamedAtef ~]#  yum info firefox
Last metadata expiration check: 0:12:42 ago on Mon 05 Aug 2024 06:02:19 PM EET.
Installed Packages
Name        : firefox
Version     : 102.9.0
Release     : 3.el9_1
Architecture : x86_64
Size        : 276 M
Source      : firefox-102.9.0-3.el9_1.src.rpm
```

- لو انا عايز اعمل Search علي Package معينه هستخدم اوبشن **search**

```
[root@MohamedAtef ~]# yum search firefox
Last metadata expiration check: 0:32:35 ago on Mon 05 Aug 2024 06:02:19 PM EET.
========================================= Name & Summary Matched: firefox =========================================
firefox.x86_64 : Mozilla Firefox Web browser
firefox-x11.x86_64 : Firefox X11 launcher.
```

- لو انا عايز اعمل Install ل Package معينه هستخدم yum install وبعدين اسم ال Package

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

- لو انت عندك Folder معين موجود عندك وعايز تعرف ال Path ده تبع انهي Package او مين هي ال Package المسئوله عن ال Path ده هستخدم اوبشن provides وبعدين ال Path

```
[root@MohamedAtef ~]# yum provides /var/www/html
httpd-filesystem-2.4.53-11.el9_2.4.noarch : The basic directory layout for the Apache HTTP Server
Repo        : AppStream
Matched from:
Filename    : /var/www/html
```

- لو انا عايز اعمل Upgrade او Update ل Package معينه هستخدم yum update او yum upgrade

```
[root@MohamedAtef ~]# yum update firefox
[root@MohamedAtef ~]# yum upgrade firefox
```

- لو انا عايز اعمل remove هستخدم yum remove وبعدين اسم ال Package

```
[root@MohamedAtef ~]# yum remove httpd
```

- لو انا عايز اجيب ال history بتاع ال Install وال remove transactions هستخدم اوبشن history

```
[root@MohamedAtef ~]# yum history
ID    | Command line                                                    | Date and time     | Action(s)    | Altered
-------------------------------------------------------------------------------------------------------------------------
   18 |                                                                 | 2024-08-05 13:45  | Install      |   1 <
   17 | group install Virtualization Host                               | 2024-07-03 00:11  | Install      |   6 >
   16 | install firewall-config-1.2.1-1.el9.noarch                      | 2024-07-01 21:27  | Install      |   2
   15 | install setroubleshoot.x86_64                                   | 2024-06-14 17:12  | Install      |   9
   14 | install httpd                                                   | 2024-06-13 12:39  | Install      |  11
   13 | install tuned-profiles-oracle.noarch                            | 2024-06-08 19:41  | Install      |   1
   12 |                                                                 | 2024-06-01 13:22  | Install      |   4
   11 | install -y bind-chroot.x86_64                                   | 2024-06-01 11:23  | Install      |   6
   10 | install -y unbound                                              | 2024-06-01 10:22  | Install      |   1
    9 | install cockpit-machines virt-install virt-manager virt-v       | 2024-05-30 11:06  | Install      |   4
    8 | group install Virtualization Host                               | 2024-05-30 10:39  | Install      |  25
    7 | -y install libvirt virt-manager                                 | 2024-05-29 20:35  | Install      |  79 EE
```

BY: Mohamed Atef Elbitawy

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