

Linux Administrator

Alejandro Campos

October, 2023

Contents

1	Linux Directory Structure Explained	6
1.1	/ – The Root Directory	6
1.2	/bin – Essential User Binaries	6
1.3	/sbin – System Administration Binaries	6
1.4	/boot – Static Boot Files	6
1.5	/dev – Device Files	6
1.6	/etc – Configuration Files	6
1.7	/home – Home Folders	6
1.8	/root – Root Home Directory	7
1.9	/lib – Essential Shared Libraries	7
1.10	/lost+found – Recovered Files	7
1.11	/media – Removable Media	7
1.12	/mnt – Temporary Mount Points	7
1.13	/opt – Optional Packages	7
1.14	/tmp – Temporary Files	7
1.15	/usr – User Binaries & Read-Only Data	7
1.16	/var – Variable Data Files	8
2	Managing Linux Users and Groups	9
2.1	Introduction	9
2.2	Managing Linux Users	9
2.2.1	Type of Users in Linux	9
2.2.2	Understanding the /etc/passwd file	9
2.2.3	Understand the /etc/shadow file	10
2.2.4	Add User to Linux System	11
2.2.5	Switching User in Linux - su command	13
2.2.6	Delete User in Linux System	13
2.2.7	Manage User from Linux System	14
2.2.8	SSH Key-Based Authentication	14
2.3	Managing Linux Groups	15
2.3.1	Understanding the /etc/group file	15
2.3.2	Add a Group in Linux	15
2.3.3	Change the group ID	16
2.3.4	Rename a group	16
2.3.5	How to Assign Users to Groups in Linux	16
2.3.6	How to Delete Users from Groups in Linux	16

2.3.7	How to delete a group	16
2.4	Sudo Command	16
2.4.1	Give sudo permissions with password	16
2.4.2	Give only some actions sudo permission	18
2.4.3	How to enable sudo without entering a password	19
2.4.4	How to gain su permissions with sudo	19
2.5	Su - root user	20
2.5.1	First Approach - Enabling root account temporary	20
2.5.2	Enable root user	20
2.5.3	Disable root user	20
3	Basic Linux Commands	22
3.1	Linux System Information	22
3.2	Linux System Consumption	22
3.3	Moving between directories	23
3.4	ls -la Analyzing Results	23
3.5	chmod	24
3.6	chown	25
3.7	Mkdir (create files)	25
3.8	Mv / Cp	26
3.9	Simbolik Links	26
3.10	Alias	26
3.10.1	Alias Temporal	27
3.10.2	Alias Permanente	27
3.11	Shutdown machines or terminals	27
3.12	Others	27
3.13	Link with examples and usage of basic commands	28
4	.bashrc, .bash_profile, /etc/bashrc & path	29
4.1	.bashrc vs .bash_profile	29
4.2	PATH	29
4.3	Set your PATH	29
4.3.1	For current terminal	29
4.3.2	Permanently for interactive sessions	29
5	Curl	30
6	Proxy definition for binaries	32
7	Update System CAs (Certificates Authority)	33

8	FQDN	34
9	Grep (Global search for Regular Expressions and Print out)	35
9.1	Two variants of grep usage	35
9.2	Useful Flags	35
10	Helm	37
11	JSONPath	38
11.1	Basic Usage	38
11.2	Filters	39
11.3	Example	40
11.4	JSONPath K8s	44
12	JQ	46
13	Localhost Networking	47
13.1	Ports Exposed	47
13.2	Localhost Adresses	47
14	Others	49
15	Source	50
16	Tar Command	52
16.1	Compress	52
16.2	Extract	52
16.3	More flags	53
17	Vim	54
17.1	Vim Config	54
17.2	Hacer y deshacer	56
17.3	Borrar lineas enteras	56
17.4	Buscar Ocurrencias	56
18	WSL	58
18.1	Remove all old dependencies	58
19	Cat	59
20	SSH	60
20.1	What is SSH?	60
20.2	How to authenticate via SSH?	61
20.2.1	Default user-password authentication method	61

20.2.2	Public Key authentication method	61
20.2.3	Generating public and private keys in our host	62
20.2.4	Appending the Public Key into the authorized_keys of the Server	63
20.3	SFTP	63
21	Find	64
22	Sed (Stream Editor)	66
23	Docker Desktop	67
24	Base64 Encoding	68
25	Tmux	69
25.1	Arguments	69
25.2	Commands Inside tmux	70
26	Others	71
26.1	Ubuntu vs RH7	71
26.2	Vagrant	71
26.3	Red Hat Package Installer	71
26.3.1	RPM	71
26.3.2	YUM	72
27	Timeshift to Backup and Restore Your Linux System	72
27.1	Introduction	72
27.2	Timeshift Installation	72
27.3	Create a Snapshot	72

1 Linux Directory Structure Explained

1.1 / – The Root Directory

Everything on your Linux system is located under the `/` directory, known as the root directory. You can think of the `/` directory as being similar to the `C:\` directory on Windows. But this isn't strictly true, as Linux doesn't have drive letters. While another partition would be located at `D:\` on Windows, this other partition would appear in another folder under `/` on Linux.

1.2 /bin – Essential User Binaries

The `/bin` directory contains the essential user binaries (programs) that must be present when the system is mounted in single-user mode. Users applications such as Firefox are stored in `/usr/bin`, while important system programs and utilities such as the bash shell, python, ansible, docker are located in `/bin`. Placing these files in the `/bin` directory ensures the system will have these important utilities even if no other file systems are mounted.

1.3 /sbin – System Administration Binaries

The `/sbin` directory is similar to the `/bin` directory. It contains essential system administration binaries, which are generally intended to be run by the root user for system administration.

1.4 /boot – Static Boot Files

The `/boot` directory contains the files needed to boot the system. For example, the GRUB boot loader's files and your Linux kernels are stored here. The boot loader's configuration files aren't located here, though they're in `/etc` with the other configuration files.

1.5 /dev – Device Files

Linux exposes devices as files, and the `/dev` directory contains a number of special files that represent devices. This directory also contains pseudo-devices, which are virtual devices that don't actually correspond to hardware. For example, `/dev/random` produces random numbers. `/dev/null` is a special device that produces no output and automatically discards all input. When you pipe the output of a command to `/dev`, you discard it

1.6 /etc – Configuration Files

The `/etc` directory contains configuration files, which can generally be edited by hand in a text editor. Note that the `/etc` directory contains system-wide configuration files.

NOTE

user-specific configuration files are located in each user's home directory.

1.7 /home – Home Folders

The `/home` directory contains a home folder **for each user**. For example, if your user name is bob, you have a home folder located at `/home/bob`. This home folder contains the user's data files and user-specific configuration files. **Each user only has write access to their own home folder** and must obtain elevated permissions (become the root user) to modify other files on the system.

1.8 /root – Root Home Directory

The `/root` directory is the home directory of the root user. Instead of being located at `/home/root`, as the rest of the users, it's located at `/root`. This is distinct from `/`, which is the system root directory.

1.9 /lib – Essential Shared Libraries

The `/lib` directory contains libraries needed by the essential binaries in the `/bin` and `/sbin` folder.

NOTE

Libraries needed by the binaries in the `/usr/bin` folder are located in `/usr/lib`.

1.10 /lost+found – Recovered Files

Each Linux file system has a `lost+found` directory. If the file system crashes, a file system check will be performed at next boot. Any corrupted files found will be placed in the `lost+found` directory, so you can attempt to recover as much data as possible.

1.11 /media – Removable Media

The `/media` directory contains subdirectories where removable media devices inserted into the computer are mounted. For example, when you insert a CD into your Linux system, a directory will automatically be created inside the `/media` directory. You can access the contents of the CD inside this directory.

1.12 /mnt – Temporary Mount Points

Historically speaking, the `/mnt` directory is where system administrators mounted temporary file systems while using them. For example, if you're mounting a Windows partition to perform some file recovery operations, you might mount it at `/mnt/windows`. However, you can mount other file systems anywhere on the system.

1.13 /opt – Optional Packages

The `/opt` directory contains subdirectories for optional software packages. It's commonly used by proprietary software that doesn't obey the standard file system hierarchy. For example, a proprietary program might dump its files in `/opt/application` when you install it.

1.14 /tmp – Temporary Files

Applications store temporary files in the `/tmp` directory. These files are generally deleted whenever your system is restarted and may be deleted at any time by utilities such as `tmpwatch`.

1.15 /usr – User Binaries & Read-Only Data

The `/usr` directory contains applications and files used by users, as opposed to applications and files used by the system. For example, non-essential applications are located inside the `/usr/bin` directory instead of the `/bin` directory and non-essential system administration binaries are located in the `/usr/bin` directory instead of the `/sbin` directory.

1.16 /var – Variable Data Files

The `/var` directory is the writable counterpart to the `/usr` directory, which must be read-only in normal operation. Log files and everything else that would normally be written to `/usr` during normal operation are written to the `/var` directory. For example, you'll find log files in `/var/log`.

2 Managing Linux Users and Groups

2.1 Introduction

Linux is a multi-user system, which means that more than one person can interact with the same system at the same time. As a system administrator, you have the responsibility to manage the system's users and groups by creating and removing users and assign them to different groups .

2.2 Managing Linux Users

In a Linux system, users refer to individuals or entities that interact with the operating system by logging in and performing various tasks. User management plays a crucial role in ensuring secure access control, resource allocation, and system administration.

A user in Linux is associated with a user account, which consists of several properties defining their identity and privileges within the system. These properties are a username, UID (User ID), GID (Group ID), home directory, default shell, and password.

2.2.1 Type of Users in Linux

Linux supports two types of users: system users and regular users.

- **System users:** are created by the system during installation and are used to run system services and applications.
- **Regular users:** are created by the administrator and can access the system and its resources based on their permissions.

2.2.2 Understanding the `/etc/passwd` file

User account information is stored in the `/etc/passwd` file. This information includes the account name, home directory location, and default shell, among other values. Each field is separated by a ":" character, and not all fields must be populated, but you must delineate them.

```
username:password:UID:GID:comment:home:shell
```

- **UID:** User Identifier
 - **0:** reserved for root user
 - **1-999:** reserved by system for administrative and system users.
- **GID:** Group Identifier
 - **0:** reserved for root group
 - **1-99:** reserved by system for administrative and system groups.

NOTE

UID and GUI assignation policies are defined in the file `/etc/login.defs`

```

acamp0s@BCNLT5CG3284PRF:~$ cat /etc/login.defs | grep -i uid
# for private user groups, i. e. the uid is the same as gid, and username is
# Min/max values for automatic uid selection in useradd
UID_MIN                1000
UID_MAX                60000
#SYS_UID_MIN           100
#SYS_UID_MAX           999
# (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is
acamp0s@BCNLT5CG3284PRF:~$ cat /etc/login.defs | grep -i gid
# If you have a "write" program which is "setgid" to a special group
# In Debian /usr/bin/bsd-write or similar programs are setgid tty
# for private user groups, i. e. the uid is the same as gid, and username is
# Min/max values for automatic gid selection in groupadd
GID_MIN                1000
GID_MAX                60000
#SYS_GID_MIN           100
#SYS_GID_MAX           999
# the same as gid, and username is the same as the primary group name.

```

So you can trim the output using AWK or cut:

```
$ awk -F ":" '{ print $1}' /etc/passwd
```

```
$ cut -d ":" -f1 /etc/passwd
```

NOTE

We will discuss passwords in the next sect, but expect to see an "x" in the password field of this file.

2.2.3 Understand the /etc/shadow file

Long ago, password hashes were stored in the /etc/passwd file. This file was world-readable, allowing inquisitive users to pull password hashes for other accounts from the file and run them through password-cracking utilities. Eventually, the password hashes were moved to a file readable only by root: /etc/shadow. Today, the password field in the /etc/passwd file is marked with an x.

NOTE

To know more about the passwords, the value we can see in the /etc/passwd is a hashed value, produced by the crypt function in Linux when we set the passphrase for the user using the passwd command. The hashed passphrase follows a specific format:

```
$id$salt$hashedpassword
```

- **id:** is the hashing method used when hashing the passphrase. For example, if the hash value is produced by yescrypt, the ID will be y, and 6 if the sha512crypt method is used. For a complete list of hashing methods and their ID, we can refer to the [Official Documentation](#).
- **salt:** adding random data to the input of a hash function to guarantee a unique output, the hash, even when the inputs are the same.
- **hashedpassword:** the password encrypted

2.2.4 Add User to Linux System

2.2.4.1 Basic Addition

```
$ sudo useradd [OPTIONS] user_name
```

When invoked, `useradd` creates a new user account according to the options specified on the command line and the default values set in the `/etc/default/useradd` file.

NOTE

When executed without any option, `useradd` creates a new user account using the default settings specified in the `/etc/default/useradd` file.

WARNING

Only root or users with sudo privileges can use the `useradd` command to create new user accounts.

To check the user has been correctly created

```
$ id username
```

To be able to log in as the newly created user, you need to set the user password

```
$ sudo passwd username
```

You will be prompted to enter and confirm the password. Make sure you use a strong password.

2.2.4.2 Addition with Home Directory Creation

On most Linux distributions, when creating a new user account with `useradd`, **by default the user's home directory is not created**.

Use the `-m` (`--create-home`) option to create the user home directory as `/home/username`

```
$ sudo useradd -m username
```

The command above creates the new user's home directory and copies files from `/etc/skel` directory to the user's home directory. If you list the files in the `/home/username` directory, you will see the initialization files:

- `.bash_logout`
- `.bashrc`
- `.profile`

```
acampos@BCNLT5CG3284PRF:~$ ls -la /etc/skel/
total 20
drwxr-xr-x  2 root root 4096 May  1 23:35 .
drwxr-xr-x 73 root root 4096 Oct  5 14:51 ..
-rw-r--r--  1 root root  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 root root 3771 Jan  6  2022 .bashrc
-rw-r--r--  1 root root  807 Jan  6  2022 .profile
```

NOTE

Within the home directory, the user can write, edit and delete all files and directories.

To create another different home

```
$ sudo useradd -d /custom/home username
```

2.2.4.3 Custom Shell

```
$ sudo useradd -s /custom/shell username
```

2.2.4.4 Addition Specifying the UID

By default, when a new user is created, the system assigns the next available UID from the range of user IDs specified in the `/etc/login.defs` file.

```
acampos@BCNLT5CG3284PRF:~$ cat /etc/login.defs | grep -i uid
# for private user groups, i. e. the uid is the same as gid, and username is
# Min/max values for automatic uid selection in useradd
UID_MIN                1000
UID_MAX                60000
#SYS_UID_MIN           100
#SYS_UID_MAX           999
# (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is
```

Invoke `useradd` with the `-u` (`--uid`) option to create a user with a specific UID. For example to create a new user named `username` with UID of 1500 you would type:

```
$ sudo useradd -u 1500 username
```

WARNING

If the specified UID is already allocated to another user, you're alerted that the UID is unavailable and the operation aborts. Rerun it with a different UID number.

NOTE

An easy way to look your user UID:

```
$ id -u username
```

2.2.4.5 Addition Specifying the GID

When creating a new user, the default behavior of the `useradd` command is to create a group with the same name as the username, and same GID as UID.

The `-g` (`--gid`) option allows you to create a user with a specific initial login group. You can specify either the group name or the GID number. The group name or GID must already exist.

```
$ sudo useradd -g group username
```

WARNING

If the specified group ID is already allocated to another group, you're alerted that the GID is unavailable and the operation aborts. Rerun it with a different group ID number.

NOTE

An easy way to look your user primary group:

```
$ id -gn username
```

2.2.4.6 Addition Assigning Multiple Groups

There are two types of groups in Linux operating systems Primary group and Secondary (or supplementary) group. Each user can belong to **exactly one primary** group and **zero or more secondary groups**.

You to specify a list of supplementary groups which the user will be a member of with the `-G (--groups)` option.

```
$ sudo useradd -g primary_group -G sec_group1, sec_group2, sec_group3 username
```

NOTE

An easy way to look all your user configuration:

```
$ id username
```

2.2.4.7 Addition with more Configurations

To create users with more different configurations, you can check the [documentation](#).

2.2.5 Switching User in Linux - su command

Su allows you to change the existing user to some other user. Use the `-l username` method to define a user account if you need to execute a command as someone other than root.

2.2.6 Delete User in Linux System

Deleting a user requires deleting both the user account as well as the files that are connected with the user account. With this command you do both:

```
$ userdel -r username
```

WARNING

The above command deletes the user whose username is provided. Make sure that the user is not part of a group. If the user is part of a group then it will not be deleted directly, hence we will have to first remove him from the group and then we can delete him.

2.2.7 Manage User from Linux System

Change the home directory

```
$ usermod -d new_home_directory_path username
```

Change login name

```
$ sudo usermod -l new_login_name old_login_name
```

Change the user password

```
$ passwd
```

WARNING

It will require authentication with the old password, so you should know the old password to change it this way.

If you do not know the user password, you can use the sudo user to do it: **Change the user password**

```
$ sudo passwd username
```

NOTE

Even further, you can force Linux user to change password at their next login, check the [documentation](#)

Modify the UID of a user

```
$ usermod -u new_uid username
```

Modify the group GID of a user

```
$ usermod -g new_gid username
```

2.2.8 SSH Key-Based Authentication

Secure Shell (SSH) key-based authentication provides a more secure alternative to password-based authentication. Users generate a public-private key pair, where the public key is stored on the server and the private key is kept securely on the user's device.

With SSH key-based authentication, users like Lisa, a system administrator at CTechCo, can authenticate without entering a password. Instead, the server verifies the user's identity based on the possession of

the private key.

To configure SSH key-based authentication for Lisa, the following steps can be taken:

- Generate an SSH key pair on Lisa's machine using the `ssh-keygen` command.
- Copy the public key to the server's `/home/lisasmith/.ssh/authorized_keys` file.
- Configure the server to allow SSH key-based authentication.

2.3 Managing Linux Groups

In Linux, groups are collections of users. Creating and managing groups is one of the simplest ways to deal with multiple users simultaneously, especially when dealing with permissions. It's more efficient to group user accounts with similar access requirements than to manage permissions on a user-by-user basis.

2.3.1 Understanding the `/etc/group` file

Similar to the `/etc/passwd` file above, the `/etc/group` file contains group account information. This information can be essential for troubleshooting, security audits, and ensuring users can access the resources they need.

The fields in the `/etc/group` file are:

```
groupname:password:GID:group members
```

2.3.2 Add a Group in Linux

To create a new group:

```
$ sudo groupadd group_name
```

To view the group you just added, run the command below:

```
$ cat /etc/group | grep -i group_name
```

NOTE

When a group is created, a unique group ID gets assigned to that group. You can verify that the group appears (and see its group ID) by looking in the `/etc/group` file.

If you want to create a group with a specific group ID (GID), use the `--gid` or `-g` option:

```
$ sudo groupadd -g 1009 group_name
```

WARNING

If the specified group ID is already allocated to another group, you're alerted that the GID is unavailable and the operation aborts. Rerun it with a different group ID number.

2.3.3 Change the group ID

You can change the group ID of any group with the `groupmod` command and the `--gid` or `-g` option:

```
$ sudo groupmod -g 1011 demo1
```

2.3.4 Rename a group

You can rename a group using `groupmod` with the `--new-name` or `-n` option:

```
$ sudo groupmod -n test demo1
```

2.3.5 How to Assign Users to Groups in Linux

Once a group is created, users can be added to it in the following way:

```
$ sudo usermod -aG group_name username
```

To check the user has been successfully added:

```
$ id username
```

2.3.6 How to Delete Users from Groups in Linux

To remove a specific user from a group, you can use the `gpasswd` command to modify group information:

```
$ sudo gpasswd --delete username group_name
```

2.3.7 How to delete a group

When a group is no longer needed, you delete it by using the `groupdel` command:

```
$ sudo groupdel demo
```

2.4 Sudo Command

The `sudo` command allows you to run programs as the root user. Using `sudo` instead of login in as root is more secure because you can grant limited administrative privileges to individual users without them knowing the root password. **That's why the root user account in Ubuntu is disabled by default for security reasons, and users are encouraged to perform system administrative tasks using `sudo`.** The initial user created by the Ubuntu installer is already a member of the `sudo` group, so if you are running Ubuntu, chances are that the user you are logged in as is already granted with `sudo` privileges.

2.4.1 Give sudo permissions with password

By default, on most Linux distributions granting `sudo` access is as simple as adding the user to the `sudo` group defined in the `sudoers` file. Members of this group will be able to run any command as root. The

name of the **group** may differ from distribution to distribution.

- **sudo**: Debian, Ubuntu and derivatives groups for sudo permissions.

```
$ usermod -aG sudo username
```

- **wheel**: RedHat, CentOS and Fedora group for sudo permissions

```
$ usermod -aG wheel username
```

We can see the permission groups allowed in the `/etc/sudoers` file:

```
$ sudo cat /etc/sudoers
```

```
acamp@BCNLT5CG3284PRF:/home$ sudo tail -n 13 /etc/sudoers

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
```

So in my Linux System, any user added to the groups **sudo** or **admin** will have all sudo permissions enabled.

What would happen with a user that is not in these groups?

```
$ whoami
jimony
$ id jimony
uid=1001(jimony) gid=1002(jimony) groups=1002(jimony)
$ sudo whoami
[sudo] password for jimony:
jimony is not in the sudoers file. This incident will be reported.
$ |
```

But if we add him to the admin group... Voilà!

```
acampos@BCNLT5CG3284PRF:/home$ sudo usermod -aG admin jiminy
acampos@BCNLT5CG3284PRF:/home$ su jiminy
Password:
$ whoami
jiminy
$ id jiminy
uid=1001(jiminy) gid=1002(jiminy) groups=1002(jiminy),115(admin)
$ sudo whoami
[sudo] password for jiminy:
root
$ |
```

NOTE

The password you have to introduce to access to sudo permissions is the user password, in this case, the jiminy password.

2.4.2 Give only some actions sudo permission

To allow a specific user to run only certain programs as sudo, instead of adding the user to the sudo group, add the users to the `/etc/sudoers` file. For example, to allow the user linuxize to run only the `mkdir` command:

WARNING

Modifying `/etc/sudoers` file can be very dangerous, so do it carefully. **Se puede liar muy parda!**

Advices:

- Use **sudo visudo**, because visudo will warn you that there's a syntax error and asks to undo the changes.
- It is hardly recommended to make a copy of the file before

```
$ sudo cp /etc/sudoers sudoerscopy
```

Just if you know what you're doing, keep going:

```
$ sudo visudo
```

```
/etc/sudoers
```

```
linuxize ALL=/bin/mkdir
```

NOTE

The file you are opening with `sudo visudo` is the `/etc/sudoers` file with the Nano editor! If you are not used to Nano, you can open it with vim. But vim does not notify you if there are some syntax error in the file, nano does.

```
$ sudo vim /etc/sudoers
```

2.4.3 How to enable sudo without entering a password

Modifying the `/etc/sudoers` adding the user with the following:

WARNING

Modifying `/etc/sudoers` file can be very dangerous, so do it carefully. **Se puede liar muy parda!**

Advices:

- Use **sudo visudo**, because visudo will warn you that there's a syntax error and asks to undo the changes.
- It is hardly recommended to make a copy of the file before

```
$ sudo cp /etc/sudoers sudoerscopy
```

```
$ sudo visudo
```

```
/etc/sudoers
```

```
jiminy ALL=(ALL:ALL) NOPASSWD: ALL
```

```
$ whoami
jiminy
$ sudo tail -2 /etc/sudoers
@includedir /etc/sudoers.d
jiminy ALL=(ALL:ALL) NOPASSWD: ALL
$ sudo ls
acampos jiminy
$ |
```

Also you can modify it in the group configuration:

```
/etc/sudoers
```

```
# Members of the admin group may gain root privileges without pwd
%admin ALL=(ALL) NOPASSWD: ALL
```

2.4.4 How to gain su permissions with sudo

If you try to redirect the output of a command to a file that your user has no write permissions, you will get a "Permission denied" error.

```
$ sudo echo "test" > /root/file.txt
# Output: bash: /root/file.txt: Permission denied
```

This happens because the redirection “>” of the output is performed under the user you are logged in, not the user specified with sudo. The redirection happens before the sudo command is invoked.

One solution is to invoke a new shell as root by using `sudo sh -c`:

```
$ sudo sh -c 'echo "test" > /root/file.txt'
```

Another option is to pipe the output as a regular user to the tee command , as shown below:

```
$ sudo echo "test" | sudo tee /root/file.txt'
```

2.5 Su - root user

As we comment in the previous section, Using sudo instead of login in as root is more secure because you can grant limited administrative privileges to individual users without them knowing the root password. **That's why the root user account in Ubuntu is disabled by default for security reasons, and users are encouraged to perform system administrative tasks using sudo.**

2.5.1 First Approach - Enabling root account temporary

If you only need the root account for a particular task or job, run the following command and supply the super user password to authenticate the action with sudo.

```
$ sudo -i
```

What behind the scenes this command makes is to enable the root user only in the current shell (associated Linux process), and when this shell is shot down (for example typing exit) and you come back to you user, the root will be disabled again.

2.5.2 Enable root user

```
$ sudo -i passwd root
```

You will have to enter the new password for the root user and go ahead.

```
acampos@BCNLT5CG3284PRF:~$ users
acampos root
```

2.5.3 Disable root user

```
$ sudo passwd -dl root
```

```
acampes@BCNLT5CG3284PRF:/home$ sudo cat /etc/shadow
root:!:19635:0:99999:7:::
daemon:!:19478:0:99999:7:::
bin:!:19478:0:99999:7:::
root:!:19478:0:99999:7:::
```

3 Basic Linux Commands

3.1 Linux System Information

Prints information about your machine's kernel, name, and hardware

The order is: kernel name, network node hostname, kernel release, kernel version, machine hardware name, processor type, hardware platform and os.

```
$ uname -a
```

To check Linux Distro

```
$ uname -or
```

To know more about Linux Distro

```
$ cat /etc/os-release
```

```
$ cat /etc/lsb-release
```

```
$ lsb_release -a
```

```
$ hostnamectl
```

3.2 Linux System Consumption

Displays running processes and the system's resource usage

```
$ top
```

```
$ htop
```

Displays the system's overall disk space usage

```
$ df -h
```

Displays a folder/file disk space usage

```
$ df -h folder_name
```

Checks a file or directory's storage consumption

```
$ du -h directory_name
```

NOTE

`-h` flag shows an humanize output, it specifies K, M, G, etc. If you want to have the output in Kibibyte do not use the flag.

3.3 Moving between directories

- `pwd`: nos indica donde estamos
- `cd == cd ~` : nos lleva al `$HOME` del usuario
- `cd /` : nos lleva a la raíz
- `cd .` : no hace nada
- `cd ..` : nos lleva un directorio atrás
- `ls -l` : nos muestra todo lo que contiene un directorio (no oculto)
- `ls -la` : nos muestra todo lo que contiene un directorio (oculto o no)
- `Ctrl + R` : nos busca comandos anteriores

Nota

Si después de un comando hacemos `"\"`, nos pasa a la siguiente línea para que podamos seguir con el comando

3.4 `ls -la` Analyzing Results

El primer carácter al extremo izquierdo representa el tipo de archivo, los posibles valores para esta posición son los siguientes:

- **- (Guion)**: representa un archivo común (de texto, html, mp3, jpg, etc.)
- **d**: representa un directorio
- **l**: link, es decir un enlace o acceso directo
- **b**: binario, un archivo generalmente ejecutable

Los siguientes 9 restantes, representan los permisos del archivo y deben verse en grupos de 3

- Los **tres primeros** representan los permisos para el propietario del archivo.
- Los **tres siguientes** son los permisos para el grupo del archivo.
- Los **tres últimos** son los permisos para el resto del mundo u otros.
- **r**: read
- **w**: write
- **x**: execute

Nota

The `/etc/group` is a text file which defines the groups to which users belong under Linux and UNIX operating system. Under Unix / Linux multiple users can be categorized into groups. Unix file system permissions are organized into three classes, user, group, and others. The use of groups allows additional abilities to be delegated in an organized fashion, such as access to disks, printers, and other peripherals

3.5 chmod

You may need to know how to change permissions in numeric code in Linux, so to do this you use numbers instead of “r”, “w”, or “x”. Cause Basically, you add up the numbers depending on the level of permission you want to give.

- **0:** No Permission
- **1:** Execute
- **2:** Write
- **4:** Read

Examples:

- To give read, write, and execute permissions for everyone:

```
$ chmod 777 folder/file_name
```

- To give read, write, and execute permissions for the owner user only.

```
$ chmod 700 folder/file_name
```

- To give write and execute (3) permission for the owner user, w (2) for the group, and read, write, and execute for the rest of users.

```
$ chmod 321 foldername
```

Permiso	Valor	Descripción
rw- - - - - -	600	El propietario tiene permisos de lectura y escritura
rw- -x - -x	711	El propietario lectura, escritura y ejecución, el grupo y otros solo ejecución
rw- r-x r- - x	755	El propietario lectura, escritura y ejecución, el grupo y otros pueden leer y ejecutar el archivo
rw- rw- - rw-	777	El archivo puede ser leído, escrito y ejecutado por quien sea
r- - - - - - -	400	Solo el propietario puede leer el archivo, pero ni el mismo puede modificarlo o ejecutarlo y por supuesto ni el grupo ni otros pueden hacer nada en el
rw- r- - - - -	640	El usuario propietario puede leer y escribir, el grupo puede leer el archivo y otros no pueden hacer nada

Figure 1: Permissions

3.6 chown

The **chown** command allows you to change the user and/or group ownership of a given file, directory, or symbolic link.

In Linux, all files are associated with an owner and a group and assigned with permission access rights for the file owner, the group members, and others.

```
$ chown [OPTIONS] USER[:GROUP] FILE(s)
```

USER is the user name or the user ID (UID) of the new owner. **GROUP** is the name of the new group or the group ID (GID). **FILE(s)** is the name of one or more files, directories or links.

NOTE

Numeric IDs should be prefixed with the + symbol.

For example, the following command will change the ownership of a file named `file1` to a new owner named `linuxize`:

```
$ chown linuxize file1
```

To change recursively

```
$ chown -R linuxize /var/www/
```

NOTE

If the directory contains symbolic links you should add the flag `-h`

```
$ chown -hR linuxize /var/www/
```

Using a Reference File The `--reference=ref_file` option allows you to change the user and group ownership of given files to be same as those of the specified reference file (**ref_file**).

```
$ chown --reference=REF_FILE FILE
```

WARNING

If the reference file is a symbolic link `chown` will use the user and group of the target file.

3.7 Mkdir (create files)

- `mkdir -p`: permite crear un directorio con padres e hijos (`mkdir -p first/second/third...`)
- `mkdir -m a=rwx`: permite crear un directorio cuyos ficheros vayan a tener los permisos `a`.
- `rm -rf`: borra el fichero escogido
- `rm *.txt`: borra todos los ficheros `.txt` que hay en un directorio

3.8 Mv / Cp

Para copiar / mover todo el contenido de una carpeta en otra:

```
$ cp -R path/to/source/* /path/dest/folder/
```

```
$ mv -R path/to/source/* /path/dest/folder/
```

Para copiar / mover una carpeta en otra:

```
$ cp -R path/to/source/ /path/dest/folder/
```

```
$ mv -R path/to/source/ /path/dest/folder/
```

to copy / move multiple directories on Linux

```
$ cp -R path/to/source/ /path/dest/folder/
```

```
$ mv -R path/to/source1/ /path/dest/folder2/ ... path/to/sourcen/ /path/dest/foldern/
```

NOTE

Ambos directorios deben existir

3.9 Simbolik Links

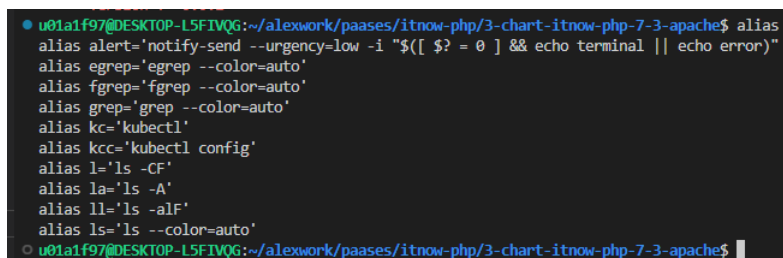
Para crearlo debemos encontrarnos en la carpeta donde queremos crearlo y hacer referencia a la carpeta que queremos apuntar desde esta con ../ o desde el /.

```
$ ln -s /Users/titocampis/Desktop/TFG/Proyecto TFG
```

3.10 Alias

Para conocer los alias que tenemos en nuestro Linux:

```
$ alias
```



```
u01a1f97@DESKTOP-L5FIVQG:~/alexwork/paases/itnow-php/3-chart-itnow-php-7-3-apache$ alias
alias alert='notify-send --urgency=low -i "${?} = 0" && echo terminal || echo error'
alias egrep='egrep --color=auto'
alias fgrep='fgrep --color=auto'
alias grep='grep --color=auto'
alias kc='kubectl'
alias kcc='kubectl config'
alias l='ls -CF'
alias la='ls -A'
alias ll='ls -alF'
alias ls='ls --color=auto'
u01a1f97@DESKTOP-L5FIVQG:~/alexwork/paases/itnow-php/3-chart-itnow-php-7-3-apache$
```

Figure 2: Los alias por defecto y configurados por mi en mi Ubuntu

3.10.1 Alias Temporal

Para generar un alias temporal:

```
$ alias nombreAlias="tu comando personalizado aquí"
```

Examples

```
$ alias docker=podman
```

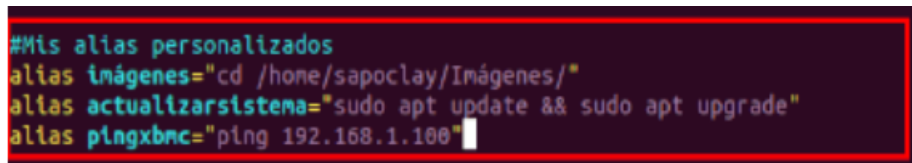
```
$ alias kcc="kubectl config"
```

3.10.2 Alias Permanente

Para mantener los alias entre sesiones, vas a tener que guardarlos en el archivo de perfil para la configuración de shell de tu usuario. Estos podrían ser:

- Bash → ~/.bashrc
- ZSH → ~/.zshrc
- Fish → ~/.config/fish/config.fish

La sintaxis que hay que utilizar en este caso, es la misma que cuando creamos uno temporal. La única diferencia viene del hecho de que esta vez lo guardaremos en un archivo.



```
#Mis alias personalizados
alias imágenes="cd /home/sapoclay/Imágenes/"
alias actualizar sistema="sudo apt update && sudo apt upgrade"
alias pingxbmc="ping 192.168.1.100"
```

Figure 3: Alias in permanent files

3.11 Shutdown machines or terminals

- Apagar la maquina que este corriendo en el momento.

```
$ sudo shutdown -r now
```

- Apagar la ventana de terminal.

```
$ exec "$SHELL"
```

3.12 Others

To create a new empty file

```
$ touch main.py
```

Checks a file's type

```
$ file main.py
```

Displays a file's first ten lines

```
$ head main.py
```

Displays a file's last ten lines

```
$ tail main.py
```

Compares two files' content and their differences

```
$ diff main.py main_old.py
```

Prints command outputs in Terminal and a file

```
$ echo "Hello" | tee output.txt
```

3.13 Link with examples and usage of basic commands

<https://www.hostinger.com/tutorials/linux-commands>

4 .bashrc, .bash_profile, /etc/bashrc & path

4.1 .bashrc vs .bash_profile

- **.bashrc [non interactive login]:** para que se apliquen los cambios debemos abrir otro terminal interactivo (no se aplican en el actual pues este fichero se ejecuta la iniciare un nuevo terminal it).
- **.bash_profile [interactive login]:** solamente se ejecuta cuando hay un proceso de login, al iniciar de nuevo la maquina, al utilizar ssh, sudo... Pero no al abrir un nuevo terminal.

4.2 PATH

PATH is an environmental variable in Linux that **tells the shell which directories to search for executable files** (i.e., ready-to-run programs) in response to commands issued by a user.

When you type a command into the command prompt in Linux, all you're doing is telling it to run a program. Even simple commands, like `ls`, `mkdir`, `rm`, and others are just small programs that usually live inside a directory on your computer called `/usr/bin`. Other places to search for executables: `/usr/local/bin`, `/usr/local/sbin`, and `/usr/sbin`.

When you type a command into your Linux shell, it doesn't look in every directory to see if there's a program by that name. It only looks to the ones you specified in the `$PATH` environment var.

Sometimes, you may wish to install programs into other locations on your computer, but be able to execute them easily without specifying their exact location. You can do this easily by adding a directory to your `$PATH`.

View your PATH

```
$ echo $PATH
```

4.3 Set your PATH

4.3.1 For current terminal

```
$ export PATH=$PATH:/place/to/the/binary/file
```

4.3.2 Permanently for interactive sessions

But what happens if you restart your computer or create a new terminal instance? Your addition to the path is gone! This is by design. The variable `$PATH` is set by your shell every time it launches. The exact way to do this depends on which shell you're running.

Add the following line to `~/.bash_profile`, `~/.bashrc`, or `/.profile`

```
$ export PATH=$PATH:/place/with/the/file
```

Nota

Be very careful editing these files, so one error in the configuration of these files can make some binaries crash (example: `mkdir`, `ls`, etc.)

5 Curl

curl is a tool for transferring data from or to a server. It supports these protocols: DICT, FILE, FTP, FTPS, GOPHER, GOPHERS, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, MQTT, POP3, POP3S, RTMP, RTMPS, RTSP, ... TELNET or TFTP. The command is designed to work without user interaction.

Without using proxy

```
$ curl --noproxy '*'
```

Using proxy

```
$ curl -x proxy_url conn_url
```

Nota

Cuidado con las single quotes ('), pues latex no procesa bien el simbolo, y cuando lo introduces en una terminal rebienta.

With specific timeout in seconds

```
$ curl --connect-timeout 5
```

Not show content, only info

```
$ curl -I
```

Force the protocol

```
$ -0,      --http1.0      Use HTTP 1.0
           --http1.1      Use HTTP 1.1
           --http2        Use HTTP 2
           --http2-prior-knowledge Use HTTP 2 without HTTP/1.1 Upgrade
           --http3        Use HTTP v3
```

Target different port than 443 or 8080

```
$ curl domain:port
```

Verbose

```
$ curl -v
```

HTTPS Protocol

```
$ curl https://hostname
```

Allow insecure connections, skip certificate validation

```
$ curl -k hostname
```

Authentication

```
$ curl -u user_name:pwd hostname
```

Pass Headers

```
$ curl -H "Content-Type:application/json" hostname
```

GET HTTP Requests

```
$ curl -XGET -H hostname
```

PUT HTTP Requests

```
$ curl -XPUT hostname
```

POST HTTP Requests

```
$ curl -XPOST hostname
```

POST HTTP Requests

```
$ curl -XDELETE hostname
```

6 Proxy definition for binaries

Configurando el proxy en las variables de entorno de sistema con una nomenclatura concreta, hará que muchos binarios del sistema los utilicen para establecer sus conexiones. Como por ejemplo: docker, curl, nslookup...

Incluir las siguientes variables en el fichero `/etc/bash.bashrc`:

```
# Configure Default Proxy
export http_proxy=http://yourproxyserver.com
export https_proxy=http://yourproxyserver.com
export HTTP_PROXY=http://yourproxyserver.com
export HTTPS_PROXY=http://yourproxyserver.com
export NO_PROXY=localhost
export no_proxy=localhost
```


7 Update System CAs (Certificates Authority)

Las CA's de sistema nos ayudaran a autenticar nuestro host en conexiones seguras por https. Para descargar CA's en Linux:

```
# Download CA certificates & store them in local directory /tmp/ca-sources.tar.gz
$ curl -k https://url_to_CAs.tar.gz -o /tmp/ca-sources.tar.gz
# Untar them into /usr/local/share/ca-certificates
$ sudo tar xzvf /tmp/ca-sources.tar.gz -C /usr/local/share/ca-certificates
# Update System Certificates
$ sudo update-ca-certificates
```

Nota

Cuando lanzamos el comando `sudo update-ca-certificates`, este nos actualiza e instala las CA's a nivel de sistema. Si bien es cierto que busca en `/usr/local/share/ca-certificates`, por mucho que de ahí los borremos no los borrará del sistema, pues el sistema los coge de otro directorio.

Nota

WSL utiliza tanto recursos de Linux como de Windows, dependiendo que programa se ejecute, tomará las configuraciones de Windows, Linux o ambas. Por tanto, es imprescindible tener también los certificados bien instalados, configurados y actualizados en nuestro sistema Windows.

8 FQDN

El término Fully Qualified Domain Name (FQDN) se refiere a la dirección completa y única necesaria para tener presencia en Internet. Está compuesta por el nombre de host y el de dominio y se utiliza para localizar hosts específicos en Internet y acceder a ellos mediante la resolución de nombres. Este nombre de dominio único que contiene toda la información necesaria para poder acceder a una máquina a través de una red pública, como puede ser internet. A través de un FQDN un equipo es capaz de conectarse con cualquier otro.

La estructura del FQDN viene determinada por el sistema de nombres de dominio (DNS) y está conformada por etiquetas. Cada etiqueta se corresponde con el nombre de un nivel en el espacio de nombres de dominio y está separada de la siguiente por un punto. Ha de constar de entre 1 y 63 caracteres, que pueden ser números, letras y guiones (aunque realmente los guiones no se pueden usar al comenzar una etiqueta) y el total de caracteres del FQDN no debe exceder los 255.

El Fully Qualified Domain Name consta como mínimo de tres etiquetas: el dominio de nivel superior, el nombre de dominio y el nombre de host. Se lee al revés.

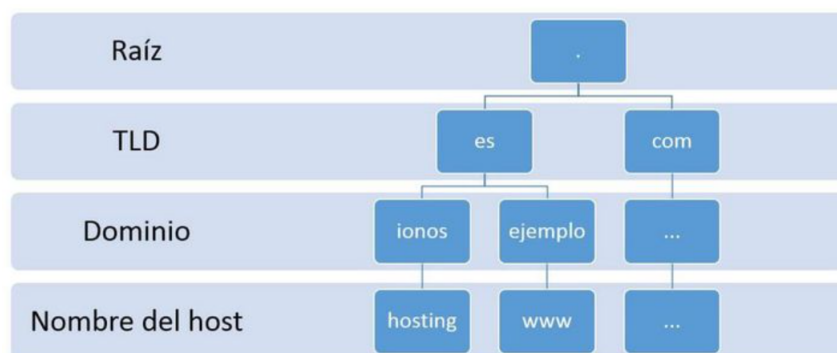


Figure 4: Representación esquemática de la estructura del Fully Qualified Domain Name

Ejemplo de un FQDN

[Nombre de host].[Dominio].[TLD].[Raíz]

hosting.ionos.es

1. La etiqueta del dominio raíz tras el punto permanece vacía
2. El **dominio de primer nivel**: en nuestro ejemplo es ".es", dominio de nivel superior geográfico, también conocido por las siglas ccTLD (country code-top level domain). Frente a ellos se encuentran los TLD genéricos como .com o .org, también designados gTLD (generic top-level domain).
3. El **dominio de segundo nivel**, también conocido como nombre de dominio. En el ejemplo se corresponde con "ionos".
4. El **dominio de tercer nivel**, en el extremo izquierdo, tenemos el nombre del host, en nuestro ejemplo "hosting".

Los FQDN se suelen utilizar en cualquier interacción en Internet, ya que son más fáciles de recordar que las direcciones IP. Otro ejemplo `www.wordpress.com`

Para más información consultad: [FQDN](#) / [FQDN 2](#)

9 Grep (Global search for Regular Expressions and Print out)

Nota

grep, egrep, fgrep, rgrep - print lines that match patterns. In addition, the variant programs egrep, fgrep and rgrep are the same as grep -E, grep -F, and grep -r, respectively. These variants are deprecated, but are provided for backward compatibility.

9.1 Two variants of grep usage

1. Use grep to search text in a file / files

```
$ grep "texto-buscado" <archivo/archivos>
```

2. Use grep to search text in the Terminal STDOUT

```
$ COMMAND [args...] | grep "texto-buscado"
```

El resultado de esto son las ocurrencias del patrón (por la línea en la que se encuentra) en los archivos / stdout. Si no existe una coincidencia, no se imprimirá ninguna salida en la terminal.

Nota

Las son necesarias para convertir a String. Si lo que le introducimos ya lo es no harían falta. Ejemplo:

- `grep alias file.txt`: No necesitamos comillas
- `grep "alias pepito" file.txt`: Si necesitamos comillas

9.2 Useful Flags

liNe Number

```
$ grep -n ...
```

Count, el numero de líneas de coincidencia

```
$ grep -c ...
```

IgnoreCase, indiferencia mayusculas-minusculas

```
$ grep -i ...
```

Before Context or Aftercontext

```
$ grep "text" file -A NUMBER_A -B NUMBER_B
```

Con este comando imprimimos las NUMBER_B líneas antes (before-context) y las NUMBER_A líneas después de la coincidencia (after-context).

Recursive Search

```
$ grep -R
```

Por defecto, `grep` no puede buscar directorios. Si tú intentas hacerlo, obtendrás un error ("Es un directorio"). Con la opción `-R`, la búsqueda de archivos entre directorios y subdirectorios se vuelve posible.

Introduce "-"

```
$ grep -e "-loquesea" file
```

```
$ grep -- "-loquesea" file
```

10 Helm

Compilar

Estando en el directorio que contiene el fichero Chart.yaml:

```
$ helm lint .
```

Prueba de despliegue Resources en Cluster with file

```
$ helm install -f ./values_ssp.yaml . --debug \  
--name-template standalone-11 --dry-run > output.yaml
```

Prueba de despliegue Resources en Cluster with file

```
$ helm install -f ./values_ssp.yaml . --debug \  
--name-template standalone-11
```

11 JSONPath

JSONPath is a query language for JSON, similar to XPath for XML. AlertSite API endpoint monitors let you use JSONPath in assertions to specify the JSON fields that need to be verified.

Nota

Cuidado en este apartado con las single quotes (' '). Pues latex no procesa bien el simbolo, y cuando lo introduces en una terminal rebienta.

11.1 Basic Usage

A JSONPath expression specifies a path to an element (or a set of elements) in a JSON structure.

Dot Notation

```
$.store.book[0].title
```

Bracket Notation

```
$['store']['book'][0]['title']
```

Mix

```
['store'].book[0].title
```

Nota

Note that dots are only used before property names not in brackets.

Nota 2

The leading "\$" represents the root object or array and can be omitted. For example, *\$.foo.bar* and *foo.bar* are the same, and so are *\$\$[0].status* and *[0].status*.

Nota 3

Using Bracket Notation be care to put **single quotes**, because double quotes are not accepted:

```
['name']
```

Nota 4

JSONPath expressions, including property names and values, are case-sensitive.

Syntax Elements

- `$`: The root object or array.
- `.property` = `['property']`: Selects the specified property in a parent object.
- `[n]`: Selects the n-th element from an array. Indexes are 0-based.

- `[index1,index2,...]`: Selects array elements with the specified indexes. Returns a list.
- `..property`: Recursive descent: Searches for the specified property name recursively and returns an array of all values with this property name. Always returns a list, even if just one property is found.
- `*`: Wildcard selects all elements in an object or an array, regardless of their names or indexes. For example, `address.***` means all properties of the address object, and `book[*]` means all items of the book array.
- `[:n]`: Selects the first n elements of the array. Returns a list.
- `[-n]`: Selects the last n elements of the array. Returns a list.

11.2 Filters

We can use some expression to filter the output of the JSON in function of parameters introduced in the syntax.

Syntax Elements

- `[?(expression)]`: Filter expression. Selects all elements in an object or array that match the specified filter. Returns a list.
- `@`: Used in filter expressions to refer to the current node being processed.

11.3 Example

JSON Example

```
{
  "store": {
    "book": [
      {
        "category": "reference",
        "author": "Nigel Rees",
        "title": "Sayings of the Century",
        "price": 8.95
      },
      {
        "category": "fiction",
        "author": "Herman Melville",
        "title": "Moby Dick",
        "isbn": "0-553-21311-3",
        "price": 8.99
      },
      {
        "category": "fiction",
        "author": "J.R.R. Tolkien",
        "title": "The Lord of the Rings",
        "isbn": "0-395-19395-8",
        "price": 22.99
      }
    ],
    "bicycle": {
      "color": "red",
      "price": 19.95
    }
  },
  "expensive": 10
}
```

Expressions

Nota

In all these examples, the leading \$. is optional and can be omitted.

```
$.store.* = ['store'][*]
```

- **Meaning:** All direct properties of store (not recursive).
- **Result:**

```
[
  "book": [
    {
      "category": "reference",
      "author": "Nigel Rees",
      "title": "Sayings of the Century",
      ...
    }
  ]
]
```



```

        },
        { ...
      }
    ],
    "bicycle": {
      "color": "red",
      ...
    }
  }
]

```

```
$.store.bicycle.color = ['store']['bicycle']['color']
```

- **Meaning:** The color of the bicycle in the store.
- **Result:** red

```
$.store..price = \$...price = ..['price']
```

- **Meaning:** The prices of all items in the store.
- **Result:** [8.95, 8.99, 22.99, 19.95]

```
$.store.book[*] = \$...book[*] = ..['book'][*]
```

- **Meaning:** All books in the store.
- **Result:**

```

[
  {
    "category": "reference",
    "author": "Nigel Rees",
    "title": "Sayings of the Century",
    "price": 8.95
  },
  {
    "category": "fiction",
    "author": "J.R.R. Tolkien"
    ...
  }
]

```

```
$...book[*].title = ..['book'][*]['title']
```

- **Meaning:** The title of all books in the store.
- **Result:**

```

[
  Sayings of the Century,
  Moby Dick,
  The Lord of the Rings
]

```

```
$.book[0]
```

- **Meaning:** The first book.
- **Result:**

```
[
  {
    "category": "reference",
    "author": "Nigel Rees",
    "title": "Sayings of the Century",
    "price": 8.95
  }
]
```

```
$.book[0].title
```

- **Meaning:** The title of the first book.
- **Result:** Sayings of the Century

```
$.book[0,1].title
```

- **Meaning:** The titles of the first two books.
- **Result:** [Sayings of the Century, Moby Dick]

```
$.book[-1:].title
```

- **Meaning:** The title of the last book.
- **Result:** The Lord of the Rings

```
$.book[?(@.author=='J.R.R. Tolkien')].title
```

- **Meaning:** The titles of all books by J.R.R. Tolkien (exact match, case-sensitive).
- **Result:** It is a list because -n always returns a list. [The Lord of the rings]

```
$.book[?(@.isbn)]
```

- **Meaning:** All books that have the isbn property.
- **Result:** [Moby Dick, The Lord of the Rings]

```
$.book[?!@.isbn]
```

- **Meaning:** All books without the isbn property.
- **Result:** [Sayings of the Century]

```
$..book[?(@.price < 10)].title
```

- **Meaning:** All books cheaper than 10 titles.
- **Result:** [Sayings of the Century, Moby Dick]

```
$..book[?(@.price > \$.expensive)]
```

- **Meaning:** All expensive books.
- **Result:**

```
$ [
  {
    "category": "fiction",
    "author": "J.R.R. Tolkien",
    "title": "The Lord of the Rings",
    "isbn": "0-395-19395-8",
    "price": 22.99
  }
]
```

```
$..book[?(@.category == 'fiction' ||
@.category == 'reference')].title
```

- **Meaning:** All fiction and reference books titles.
- **Result:** [Sayings of the Century, Moby Dick, The Lord of The Rings]

```
$..book[?(@.category != 'fiction')]
```

- **Meaning:** All not fiction books.
- **Result:**

```
[
  {
    "category": "reference",
    "author": "Nigel Rees",
    "title": "Sayings of the Century",
    "price": 8.95
  }
]
```

For more information about JSONPath, check the following [page](#)

11.4 JSONPath K8s

JSONPath template is composed of JSONPath expressions enclosed by curly braces . Kubectl uses JSONPath expressions to filter on specific fields in the JSON object and format the output. In addition to the original JSONPath template syntax, the following functions and syntax are valid:

- `range, end`: iterate list. `{range .items[*]}{.metadata.name}`
- `{"\n"}, {"\t"}`: to write salto de linea or tab. `{..metadata.name}{"\t"}{..matadata.image}`

Example 1

Get all **containers** / **initContainers** running and their images used inside a **Pod** or declared in pod.spec of **Deployment/Statefulset** . It is exactly the same changing little things. At least, it is showed in column view separated by tab.

```
$ kc get RESOURCE_TYPE RESOURCE_NAME \
-o jsonpath='{range ..containers[*]}{.name}{"\t"}{.image}{"\n"}' \
|sort|column -t
```

1. To choose between **Pod** or **Deploy/Sateful**: modify `RESOURCE_TYPE` & `RESOURCE_NAME`
2. To choose between **containers** or **initContainers**: modify the range.
 - containers: `{range ..containers[*]}`
 - initContainers: `{range ..initContainers[*]}`

```
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ kc get po slb03a-s3javastandaloner-tst-88cd46994-kg8gq \
> -o jsonpath='{range ..containers[*]}{.name}{"\t"}{.image}{"\n"}' \
> |sort|column -t
cloudapphealth      docker-registry.cloud.caixabank.com/catalog/paas/java-runtime-health-standalone-1-8:1.0.0
java-standalone-1-8  docker-registry.cloud.caixabank.com/containers/slb03a/s3javastandaloner:latest
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$
```

Figure 5: Get all containers parsing a Pod JSON

```
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ kc get deploy slb03a-s3javastandaloner-tst \
> -o jsonpath='{range ..initContainers[*]}{.name}{"\t"}{.image}{"\n"}' |sort|column -t
init-cacerts  docker-registry.cloud.caixabank.com/catalog/docker-init-setup:2.3.0
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$
```

Figure 6: Get all initContainers parsing a Deployment JSON

Example 2

Get all ports exposed by a Pod, Deployment or Statefulset.

```
$ kc get RESOURCE_TYPE RESOURCE_NAME \
-o jsonpath='{range ..containers[*]}{.name}{"\t"}{.ports}{"\n"}' \
|sort|column -t
```

```
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ kc get po slb03a-s3javastandaloner-tst-88cd46994-kg8gq \
> -o jsonpath='{range ..containers[*]}{.name}{"\t"}{.ports}{"\n"}' \
> |sort|column -t
cloudapphealth      [{"containerPort":8180,"name":"health","protocol":"TCP"}]
java-standalone-1-8 [{"containerPort":8080,"name":"http","protocol":"TCP"}, {"containerPort":8090,"name":"metrics","protocol":"TCP"}]
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$
```

Figure 7: Get all ports exposed in a Pod parsing a Pod JSON

```

u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ kc get deploy slb03a-s3javastandaloner-tst \
> -o jsonpath='{range ..containers[*]}.{.name}{"\t"}{.ports}{"\n"}}' \
> |sort|column -t
cloudapphealth [{"containerPort":8180,"name":"health","protocol":"TCP"}]
java-standalone-1-8 [{"containerPort":8080,"name":"http","protocol":"TCP"},{"containerPort":8090,"name":"metrics","protocol":"TCP"}]
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$

```

Figure 8: Get all ports exposed in a Pod parsing a Deployment JSON

Example 3

Get all Volume Mounts of container called CONTAINER_NAME inside a Pod, Deployment or Statefulset.

```

$ kc get RESOURCE_NAME -o jsonpath=\
'{range ..containers[?(@.name == "CONTAINER_NAME")]\
.volumeMounts[*]}.{.name}{"\t"}{.mountPath}{"\n"}}' \
|sort|column -t

```

```

u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ kc get deploy slb03a-s3javastandaloner-tst \
> -o jsonpath='{range ..containers[?(@.name == "java-standalone-1-8")].volumeMounts[*]}.{.name}{"\t"}{.mountPath}{"\n"}}' \
> |sort|column -t
.
.init-cacerts /opt/ca-certs
.pvc-mounted-heapdump-cxb-slb03a-s3javastandaloner-tst /storage
.volume-from-configmap-testproperty /tmp/properties/testproperty
.volume-from-configmap-tsttest /tmp/properties/tsttest
.volume-from-secret-certbueno /tmp/secretos/certbueno
.volume-from-secret-certmalo /tmp/secretos/certmalo
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$

```

Figure 9: Get all volumeMounts in a container parsing a Deployment JSON

12 JQ

To parse into a beautiful json format:

```
$ cat file.json | jq '.'
```

13 Localhost Networking

13.1 Ports Exposed

Para saber que puertos tiene escuchando nuestro localhost:

1. Using `lsof`

```
$ sudo lsof -i -P -n
```

```
$ sudo lsof -i -P -n | grep -i listen
```

2. Using `netstat`

```
$ netstat -putona | grep numero-de-puerto
```

- **p:** muestra las conexiones para el protocolo especificado que puede ser TCP o UDP
- **u:** lista todos los puertos UDP
- **t:** lista todos los puertos TCP
- **o:** muestra los timers
- **n:** muestra el numero de puerto
- **a:** visualiza todas las conexiones activas del sistema

NOTE

`netstat` command shows the system's network information, like routing and sockets.

13.2 Localhost Adresses

De puertas para adentro

1. **Ipv4:**

- localhost
- 127.0.0.1

2. **Ipv6**

- 0:0:0:0:0:0:1
- ::1

De puertas para fuera

- **ifconfig:** displays the system's network interfaces and their configurations. In this case our localhost direction to outside is 172.21.220.125/20 (172.21.220.125 with mask 255.255.240.0)

```
$ ifconfig
```

```

titocampis@DESKTOP-FMGU3N7:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.21.220.125 netmask 255.255.240.0 broadcast 172.21.223.255
    inet6 fe80::215:5dff:feab:2d48 prefixlen 64 scopeid 0x20<link>
    ether 00:15:5d:ab:2d:48 txqueuelen 1000 (Ethernet)
    RX packets 63 bytes 8021 (8.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7 bytes 586 (586.0 B)
    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>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Figure 10: ifconfig

- `ip -br addr list eth0`

```

titocampis@DESKTOP-FMGU3N7:~$ ip -br addr
lo                UNKNOWN      127.0.0.1/8 ::1/128
bond0             DOWN
dummy0            DOWN
tunl0@NONE        DOWN
sit0@NONE         DOWN
eth0              UP              172.21.220.125/20 fe80::215:5dff:feab:2d48/64
titocampis@DESKTOP-FMGU3N7:~$

```

Figure 11: ip -br

Nota

Netmask

24 (number of 1's):

255.255.255.0

11111111 11111111 11111111 00000000

20 (number of 1's):

255.255.240.0

11111111 11111111 11110000

14 Others

Netcat

```
$ nc -zv hostname port
```

Telnet

```
$ telnet hostname port
```

15 Source

```
$ source filename [arguments]
```

Cuando se ejecuta desde una shell un comando o un script, se crea un subprocesso (proceso hijo) de la shell que ejecuta el comando o el script (proceso padre).

Si el script que ejecuta el proceso hijo crea o modifica alguna variable de entorno, esos cambios o variables desaparecen cuando finaliza el comando o script.

Si deseamos que dichos cambios permanezcan, podemos utilizar el comando de Bash `source`. Este comando hace que el proceso o comando se ejecute sin crear ningún proceso hijo, de forma que los cambios efectuados en las variables de entorno y demás, se mantengan al finalizar el archivo.

More information: [Source in Bash](#)

Example:

```
script.sh

#!/bin/bash

export RHT_OCP4_DEV_USER="nwmwsv"
export RHT_OCP4_DEV_PASSWORD="1ecc25feca97466e81c5"
export RHT_OCP4_MASTER_API="https://api.eu410.prod.nextcle.com:6443"
export Console_Web_Application=\
"https://console-openshift-console.apps.eu410.prod.nextcle.com"
export Cluster_Id="5650752a-edc7-4546-a1ff-8900d7e8e35b"
```

1. Si lo ejecutamos con `./`

- En primer lugar hay que darle permisos

```
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ ll d280lab.sh
-rw-r--r-- 1 u01a1f97 u01a1f97 319 Dec  5 08:20 d280lab.sh
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ ./d280lab.sh
bash: ./d280lab.sh: Permission denied
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ chmod 744 d280lab.sh
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ ./d280lab.sh
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$
```

- En segundo lugar, como bien preveíamos, no se guardan los cambios en la terminal, pues se ejecuta un subprocesso por detrás el cual nunca mergea cambios a nivel de sistema en el proceso padre.

```
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ ./d280lab.sh
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ echo $RHT_OCP4_DEV_USER
u01a1f97@DESKTOP-L5FIVQG:~/alexwork$
```

2. Si lo ejecutamos con `bash/sh`

- En este caso, no son necesarios permisos, pues se pasa como argumento del ejecutable `bash`.
- En segundo lugar, como bien preveíamos, sucede lo mismo que con `./`, no se guardan los cambios en el terminal (proceso padre).

```

• u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ ll d280lab.sh
-rw-r--r-- 1 u01a1f97 u01a1f97 319 Dec  5 08:20 d280lab.sh
• u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ bash d280lab.sh
• u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ echo $RHT_OCP4_DEV_USER

○ u01a1f97@DESKTOP-L5FIVQG:~/alexwork$

```

3. Si lo ejecutamos con source

- En este caso, no son necesarios permisos, pues se pasa como argumento del ejecutable source.
- En segundo lugar, como bien prevíamos, los cambios se transmiten al proceso padre! Y por tanto se guardan en nuestro terminal.

```

• u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ ll d280lab.sh
-rw-r--r-- 1 u01a1f97 u01a1f97 319 Dec  5 08:20 d280lab.sh
• u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ source d280lab.sh
• u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ echo $RHT_OCP4_DEV_USER
nwmwsv
• u01a1f97@DESKTOP-L5FIVQG:~/alexwork$ echo $RHT_OCP4_DEV_PASSWORD
1ecc25feca97466e81c5
○ u01a1f97@DESKTOP-L5FIVQG:~/alexwork$

```

16 Tar Command

The tar command on Linux is often used to create .tar.gz or .tgz archive files, or extract them into local directories.

16.1 Compress

Basics

Use the following command to compress an entire directory or a single file on Linux. It'll also compress every other directory inside a directory you specify—in other words, it works recursively.

```
$ tar -czvf name-of-archive.tar.gz /path/to/directory-or-file
```

Compress multiple files/directories in a unique archive

```
$ tar -czf FILENAME.tar.gz path/to/dir1 path/to/file1 path/to/dir2 ...
```

Exclude files or directories

```
$ tar -czf FILENAME.tar.gz path/to/dir1 \  
--exclude=/path/to/dir1/excludeddir \  
path/to/dir2 --exclude=/path/to/dir1/*.mp4
```

16.2 Extract

Basics

Once you have an archive, you can extract it with the tar command. The following command will extract the contents of archive.tar.gz to the current directory.

```
$ tar -xzvf archive.tar.gz
```

Choose the extract directory

You may want to extract the contents of the archive to a specific directory. You can do so by appending the -C switch to the end of the command:

```
$ tar -xzvf archive.tar.gz -C /path/to/directory/to/extract
```

More information in: [How-To Geek tar](#)

Here's what those switches actually mean:

- **-c:** create an archive
- **-z:** compress into gzip
- **-v:** verbose [removable]
- **-f:** allows you to specify the FILENAME **filename** of archive

Nota

-f switch must be the last one, because is the flag which specifies the name of the file indicated after.

16.3 More flags

- **-x:** Extract the archive
- **-t:** displays or lists files in archived file
- **-u:** archives and adds to an existing archive file
- **-A:** concatenates the archive files
- **-j:** filter archive tar file using tbzip
- **-W:** verify a archive file
- **-r:** update or add file or directory in already existed .tar file

17 Vim

17.1 Vim Config

```
$ sudo vim ~/.vimrc
```

```

" Disable compatibility with vi which can cause unexpected issues.
set nocompatible

" Enable type file detection. Vim will be able to try to detect the type of file in use.
filetype on

" Enable plugins and load plugin for the detected file type.
filetype plugin on

" Load an indent file for the detected file type.
filetype indent on

" Set authomatic indentation
" set autoindent

" Turn syntax highlightin
syntax on

" Add numbers to each line on the left-hand side.
set number

" Highlight cursor line underneath the cursor horizontally.
set cursorline

" Highlight cursor line underneath the cursor vertically.
set cursorcolumn

" Set shift width to 4 spaces.
set shiftwidth=4

" Set tab width to 4 columns.
set tabstop=4

" Use space characters instead of tabs.
set expandtab

" Colorful (),[],{}
set showmatch

" While searching though a file incrementally highlight matching characters as you type.
set incsearch

" Ignore capital letters during search.
set ignorecase

" Use highlighting when doing a search.
set hlsearch

" Enable auto completion menu after pressing TAB.
set wildmenu

" Make wildmenu behave like similar to Bash completion.
set wildmode=list:longest

" Enable black theme
" set background=dark

" Tab helper
" set smarttab

```

If you want to persist this configuration when using `sudo vim` you will need to do something a little bit tricky:

- Create an alias in your `~/.bashrc` file:

```
alias svim='sudo -E vim'
```

- Use always

```
$ svim <file>
```

17.2 Hacer y deshacer

undo: para deshacer acciones

```
vim editor - Command Mode  
:u
```

redo: para volver a hacer acciones

```
vim editor - Normal Mode  
Ctrl + r
```

```
vim editor - Normal Mode  
:r
```

17.3 Borrar líneas enteras

```
{vim editor - Normal Mode}  
dd + intro
```

17.4 Buscar Ocurrencias

Para buscar

```
{vim editor - Normal Mode}  
/<palabra>
```

Para ir a cualquier ocurrencia: Intro

Para pasar entre ocurrencias: n

Si queremos hacerlo insensible a minúsculas y mayúsculas: antes de buscar, ejecutar lo siguiente.


```
{vim editor - Normal Mode}  
:set ignorecase
```

18 WSL

18.1 Remove all old dependencies

1. Remove all Ubuntu packages in Windows - **Add or remove programs**
2. Remove all WSL packages in Windows - **Add or remove programs**
3. Go to Powershell / Cmder
4. Remove the current distros:

```
$ wsl --unregister
```

5. Install WSL:

```
$ wsl --install
```

6. Install WSL:

```
$ wsl --install
```

7. Check WSL available distros, if there is anyone, remove it using `wsl --unregister <DISTRO>`

```
$ wsl -l
```

8. Install the desired distro

```
$ wsl --install -d <DISTRO_NAME>
```

19 Cat

Cat nos va a permitir ver el contenido de ficheros sin abrirlos, crear ficheros si no existen o redireccionar salidas del terminal.

- Basic usage: mostrar el contenido de un fichero

```
$ cat test
```

- Mostrar contenido de test y test2

```
$ cat test1 test2
```

- Nos añade el contenido de test2 en el fichero test1, si habia contenido sobrescribe, si no había nada, crea el nuevo fichero

```
$ cat test1 > test2
```

- Para que nos añada el contenido de test2 en el final del fichero test1, sin sobrescribir lo que había

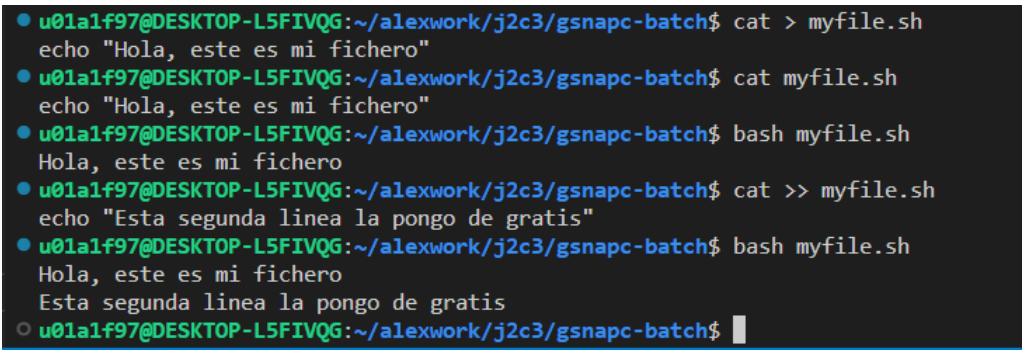
```
$ cat test1 >> test2
```

- Show line number

```
$ cat -n file
```

- Para escribir en un fichero el conenido que queramos (ACABAR CON CTRL+D)

```
$ cat > filename
```



```
u01a1f97@DESKTOP-L5FIVQG:~/alexwork/j2c3/gsnapc-batch$ cat > myfile.sh
echo "Hola, este es mi fichero"
u01a1f97@DESKTOP-L5FIVQG:~/alexwork/j2c3/gsnapc-batch$ cat myfile.sh
echo "Hola, este es mi fichero"
u01a1f97@DESKTOP-L5FIVQG:~/alexwork/j2c3/gsnapc-batch$ bash myfile.sh
Hola, este es mi fichero
u01a1f97@DESKTOP-L5FIVQG:~/alexwork/j2c3/gsnapc-batch$ cat >> myfile.sh
echo "Esta segunda linea la pongo de gratis"
u01a1f97@DESKTOP-L5FIVQG:~/alexwork/j2c3/gsnapc-batch$ bash myfile.sh
Hola, este es mi fichero
Esta segunda linea la pongo de gratis
u01a1f97@DESKTOP-L5FIVQG:~/alexwork/j2c3/gsnapc-batch$
```

Figure 12: amazing cat

20 SSH

20.1 What is SSH?

SSH, also known as Secure Shell or Secure Socket Shell, is a network protocol that gives users, particularly system administrators, a secure way to access a computer over an unsecured network. Secure Shell provides strong password authentication and public key authentication, as well as encrypted data communications between two computers connecting over an open network, such as the internet.

In addition to providing strong encryption, SSH is widely used by network administrators to manage systems and applications remotely, enabling them to log in to another computer over a network, execute commands and move files from one computer to another.

The most basic use of SSH is to connect to a remote host for a terminal session. The form of that command is the following:

- IP:

```
$ ssh user_name@host_IP
```

- Hostname:

```
$ ssh user_name@SSHserve.example.com
```

The SSH key command instructs your system that you want to open an encrypted Secure Shell Connection. `user_name` represents the account you want to access. For example, you may want to access the `root` user or `acampos` user.

NOTE

To connect via ssh using a user, it is needed to have this user created in the host machine.

- **host machine:** refers to the remote server you are trying to access.
- **client machine:** refers to the server you are using to access the host.

For the first time negotiating a connection between the local host and the server, the user will be prompted with the remote host's public key fingerprint and prompted to connect.

```
The authenticity of host 'sample.ssh.com' cannot be established.  
DSA key fingerprint is 01:23:45:67:89:ab:cd:ef:ff:fe:dc:ba:98:76:54:32:10.  
Are you sure you want to continue connecting (yes/no)?
```

Answering yes to the prompt will cause the session to continue, and the host key is stored in the local system's `known_hosts` file. This is a hidden file, stored by default in a hidden directory, called `/.ssh/known_hosts`, in the user's home directory. Once the host key has been stored in the `known_hosts` file, the client system can connect directly to that server again without need for any approvals; the host key authenticates the connection.

```
acampes@BNC1T5CG3284PRF:~/work/opticlimb$ cat ~/.ssh/known_hosts
[1]/9rmhwbZ4qA7yc+oET4qSiqBY=|WcLPZsOha/xbtLEyWd3oX5o94U= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIEFFvzDJXiUu2iuu8j4cEVQbOH9cXSX54YwvJ4IaPE0I
[1]BzdKxkC0QRMEfud4w/rvtdQgW4=|ygyfyp0pkHAscl5bNv7kAHfxL08U= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOIx2nnszRk5QDJSVCVA+agB7Vx6HRKZOLwRITweV3eUc
[1]rQeGrSv4REETw69a7Y010zOX/NQ=|4sjM12fVfJYuzcUJkplEbU0GA8= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIL6CIKDNQwT0yGH16KLUL6em6EeLbEblOMxSWrLkmT
[1]8KcWmKTBD0d4FTR+A0WXPxtK3A=|IDLy4NnsUJ4chEQUEmv/NZ86jd0= ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDUaRNe39+gxSvGiqEN5otQYteHsxwkaexBYqHYDRkm1xT488c8Se9pWVD
J/zokG9vU0Iz597RA1MR1KHRR4gn8EupjQR3+4627Fa1Nv+V8hj576SJKHuTI3VD0drZ0kv2RoFLh27idPHVbw73G67eVsC3+Zhqo9VMGfK8bpUCsmYct5NI7o8VC3UPYLL6NmXQ2PcdhLDAI6Esqjay6L
G+2PD5jFvO+2U2e0+5UJ4ol.c077x5h0ub6yt0MvdmY2IaRY0Cgq/IdCxqLj5B2Hm2JImJfdeuiclym6PjH1Wx9JnPhLanaIUQ3/2+/zid8W5wiKyC+8F4+/G69c7AJVDJ0b7PeKwGE7KETabbwGz
T1fLX4eP8B8UG5VpE3uSteyz088D0tPqKwKsH2pJ483fHn/esd4x/0mMuhJtKzNnsQPvZ0S3j28j1881g27w7cvGjVa7Sru8uLT69pJgnjKjZGBXWmJF2i/5QKrrbZIIIsAc=
[1]B21lU0/qmD5TVLZV9HgE5Sa4Bne=|C0iYx4AXDHMF0uFMBST5Mg8B8es= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlZdHAyNTYAAABBBP/mJNKG+vIPYxRFZA/1WW
no3MVvAeyasneNyxhR3+tkpNhmGEyEu0KsJBDGTmQj80xMbHhFvPipjbeDpPFW=
[1]qEPd08lgCj14tW2UtoB0T8HRXZ0=|WEecMAGcXcUILLH90szjcv7B/cng= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlZdHAyNTYAAABBBLJXQm24i4gw0LfMNHJjtYA
iyyM3dsN0cqfRymYc3r2LE2HoThierLJf0unoCVbL0qU7eukvHMD/euVjZ1q/A8=
[1]Qn5XbJfL8m+B+BB68K3FYl-fHgF0=|9Xtv+hhmS6xNuSG0spzdV3flzz= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPcsqduLjZEFQMTcN/tlug/ePhi+PvEnDNf6mZcStde
[1]LxxrXehRUjYopfgzrNPv/4ZF8Fq0=|2dgVAaRBD0lly+AgGGR+1yFouhA= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKGDU4gg4CXHYzBjn5R3R3pvpwph9ykv27j03wf/QQJsm
[1]soAYHGzrrkoPjFTHth/jmUMAtLpc=|2A+I7E8UtKpotZMqfMAv4IcTpII= ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIIIsLePk3hZW8YPLHkn7H0HVaxKD+0wn6S86mD0V2nZF
[1]S9ACITDcVQCRw7jJ/+2/cVWFqE=|ks/xJmQ7UVi9JuIQmzSBZsUL580= ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlZdHAyNTYAAABBBOK+WvgdSx6WIM/vpoLFGTh
d4KVsuXxaQ8k9KraYfxP8StkUEzPGFmpT8VgclLqEkcjxwb+tt7etXJ2VnQt/d3k=
```

Present in all data centers, SSH ships by default with every Unix, Linux and Mac server. SSH connections have been used to secure many different types of communications between a local machine and a remote host, including secure remote access to resources, remote execution of commands, delivery of software patches, and updates and other administrative or management tasks, manage routers, server hardware, virtualization platforms, operating systems (OSes), and inside systems management and file transfer applications.

Secure Shell is used to connect to servers, make changes, perform uploads and exit, either using tools or directly through the terminal. SSH keys can be employed to automate access to servers and often are used in scripts, backup systems and configuration management tools.

NOTE

SSH operates on **TCP port 22** by default (though SSH port can be changed if needed). The host (server) listens on port 22 (or any other SSH assigned port) for incoming connections. It organizes the secure connection by authenticating the client and opening the correct shell environment if the verification is successful.

It is hardly recommended to change the port in which the host machine listen, because to let port 22 is more easily to enter the machine without authorization.

20.2 How to authenticate via SSH?

20.2.1 Default user-password authentication method

By default SSH protocol doesn't use public key cryptography for authenticating hosts and users. It still uses the **Linux user-password authentication method**, so you only have to pass the **username** of the Linux user via the `ssh` command and introduce the **password** of this user:

```
$ ssh -P=custom_port linux_username@hostname_or_ip
```

NOTE

If you run the command without specifying user, `ssh` will take your Linux current **username**.

20.2.2 Public key authentication method

Generally, the SSH service is configured to use public key cryptography for authenticating hosts and users. SSH introduced public key authentication as a more secure alternative to the older **.rhosts** authentication. It improved security by avoiding the need to have password stored in files, and eliminated the possibility of a compromised server stealing the user's password.

However, SSH keys are authentication credentials just like passwords. Thus, they must be managed somewhat analogously to user names and passwords. They should have a proper termination process so

that keys are removed when no longer needed.

20.2.3 Generating public and private keys in our host

For that reason, we should generate SSH public and private key on our client and authorize them into the host.

Depending on the technology of the host you want to connect, you need to create the keys:

- **rsa**: an old algorithm based on the difficulty of factoring large numbers. A key size of at least 2048 bits is recommended for RSA; 4096 bits is better. All SSH clients support this algorithm.

```
$ ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

- **ed25519**: this is a new algorithm added in OpenSSH. Support for it in clients is not yet universal.

```
$ ssh-keygen -t ed25519 -C "your_email@example.com"
```

WARNING

For SSH to recognize the SSH keys they should be stored in:

```
~/.ssh/
```

```
acampos@BCNLT5CG3284PRF:~/work/opticlimb$ ls -la ~/.ssh/
total 24
drwxr-xr-x  2 acampos acampos 4096 Oct  4 14:02 .
drwxr-x--- 11 acampos acampos 4096 Oct  4 11:49 ..
-rw-----  1 acampos acampos 3369 Oct  4 10:51 id_rsa
-rw-r--r--  1 acampos acampos  733 Oct  4 10:51 id_rsa.pub
-rw-----  1 acampos acampos 2798 Oct  4 13:49 known_hosts
-rw-----  1 acampos acampos 2576 Oct  4 13:49 known_hosts.old
```

Also, **rsa keys** should have the **permissions** you see in the image above, if not, it will not be valid to authenticate in any server. If you have generated the keys, they are generated with the correct permissions, but if you have copied, it can be wrong.

NOTE

By default, when you establish ssh connection, it uses the following private keys names:

- ~/.ssh/id_ecdsa
- ~/.ssh/id_ecdsa_sk
- ~/.ssh/id_ed25519
- ~/.ssh/id_ed25519_sk
- ~/.ssh/id_xmss
- ~/.ssh/id_xmss_sk
- ~/.ssh/id_dsa
- ~/.ssh/id_rsa

For more information, check the documentation of [how to do if for github servers](#).

20.2.4 Appending the Public Key into the `authorized_keys` of the Server

To use public key authentication, the public key must be **installed in the `authorized_keys`** file of the server. This can be conveniently done using the `ssh-copy-id` tool. Like this:

```
$ ssh-copy-id -i ~/.ssh/my_ssh_key.pub user_name@hostname
```

WARNING

With the command above, we will append the host **pubkey** in the `authorized_keys` file of the server.

Once the public key has been configured on the server, the server will allow any connecting user that has the private key to log in. During the login process, the client proves possession of the private key by digitally signing the key exchange.

NOTE

For git you should do it different, just adding your public ssh key in the GUI, accessing to your profile settings. You can follow the [Official Documentation](#)

20.3 SFTP

FTP, or “File Transfer Protocol” was a popular unencrypted method of transferring files between two remote systems.

SFTP, which stands for SSH File Transfer Protocol, or Secure File Transfer Protocol, is a separate protocol packaged with SSH that works in a similar way but over a secure connection. The advantage is the ability to leverage a secure connection to transfer files and traverse the filesystem on both the local and remote system.

In almost all cases, SFTP is preferable to FTP because of its underlying security features and ability to piggy-back on an SSH connection. FTP is an insecure protocol that should only be used in limited cases or on networks you trust.

```
$ sftp -oPort=custom_port user_name@host_ip_or_hostname
```

21 Find

- Buscar ficheros desde la raíz con el nombre "linux"

```
$ find / -name "linux"
```

- Buscar ficheros desde la raíz con el nombre "linux" y listarlos

```
$ find / -name "linux" -ls
```

- Buscar dentro del directorio /etc/config/ del sistema de todos los ficheros y directorios con el nombre "linux" sin importar mayúsculas y minúsculas

```
$ find /etc/config/ -type d -name "linux"
```

- Buscar desde el directorio donde nos encontramos los ficheros cuyo nombre contienen la cadena "Thr"

```
$ find . -name "*Thr*"
```

```
[default@iks03-iksphpitnowr-pre-59f9b86968-hlj2k ~]$ find /var/template/ -name "*envvar*" -ls
 8  4 -rw-r--r--  1 100      1000      423 Jan  4 14:46 /var/template/batch-db3-envvar
 7  4 -rw-r--r--  1 100      1000      423 Jan  4 14:46 /var/template/mysql-db3-envvar
 6  4 -rw-r--r--  1 100      1000      348 Jan  4 14:46 /var/template/postgresql-envvar
 5  4 -rw-r--r--  1 100      1000      600 Jan  4 14:46 /var/template/oracle-envvar
 4  4 -rw-r--r--  1 100      1000      179 Jan  4 14:46 /var/template/mysql-envvar
 3  4 -rw-r--r--  1 100      1000      179 Jan  4 14:46 /var/template/db2-envvar
[default@iks03-iksphpitnowr-pre-59f9b86968-hlj2k ~]$
```

Figure 13: use of find

```
[default@iks03-iksphpitnowr-pre-59f9b86968-hlj2k usr]$ find / -name entrypoint.sh -ls
find: '/proc/tty/driver': Permission denied
find: '/run/cryptsetup': Permission denied
find: '/root': Permission denied
find: '/etc/pki/CA/private': Permission denied
find: '/opt/rh/httpd24/root/root': Permission denied
find: '/opt/rh/httpd24/root/var/lib/dav': Permission denied
find: '/opt/rh/httpd24/root/var/lib/httpd': Permission denied
find: '/opt/rh/httpd24/root/var/cache/httpd': Permission denied
find: '/opt/rh/rh-php73/root/root': Permission denied
find: '/opt/rh/rh-php73/register.content/var/opt/rh/rh-php73/lib/php/session': Permission denied
find: '/opt/rh/rh-php73/register.content/var/opt/rh/rh-php73/lib/php/wsdldcache': Permission denied
find: '/opt/rh/devtoolset-6/root/root': Permission denied
find: '/var/lib/machines': Permission denied
find: '/var/cache/ldconfig': Permission denied
6038346  4 -rwxr-xr-x  1 default  group-default    420 Jun 29  2022 /usr/local/bin/entrypoint.sh
2757922  4 -rwxr-xr-x  1 root      root              314 Jun 29  2022 /usr/local/entrypoint.sh
[default@iks03-iksphpitnowr-pre-59f9b86968-hlj2k usr]$
```

Figure 14: another use of find

NOTE

Las comillas en estos casos son opcionales, pues como siempre, tan solo sirven para marcar string

22 Sed (Stream Editor)

It is a very essential tool for text processing, specifically it is common used for text replacement. Con Sed podemos editar archivos, incluso sin abrirlos, de manera individual o masiva. Dicho sea, que esta forma, es mucho más rápida para encontrar y reemplazar algo en un archivo de manera manual.

Print the content of "fichero.txt" replacing the first occurrence of the string "Microsoft Windows" by "GNU Linux" in the file "fichero.txt"

```
$ sed 's/Microsoft Windows/GNU Linux/' fichero.txt
```

Save the changes in the file:

```
$ sed -i 's/Microsoft Windows/GNU Linux/' fichero.txt
```

Replace all the occurrences of the string "Microsoft Windows" by "GNU Linux" in the file "fichero.txt" and save.

```
$ sed -i 's/Microsoft Windows/GNU Linux/g' fichero.txt
```

Replace just the 3rd occurrence of "Microsoft Windows" by "GNU Linux" in the text and save

```
$ sed 's/Microsoft Windows/GNU Linux/3g' fichero.txt
```

Replace the string "Microsoft Windows" just in line 1:

```
$ sed '1 s/Microsoft Windows/GNU Linux/' fichero.txt
```

NOTE

By default sed is **case SENSITIVE** but to change it by case insensitive, you can add I at the end of the REGEX:

```
$ sed -i 's/Microsoft Windows/GNU Linux/gI' fichero.txt
```

WARNING

Sed will replace all the string matches, without differentiating if it is completed or partial, for example:

```
acampos@BCNLT5CG3284PRF:~$ echo "Alex and Alexandra go to Pedraforca" | sed 's/Alex/Helena/g'  
Helena and Helenaandra go to Pedraforca
```

To replace the exact match you should use spaces, in **REGEX** space=\s:

```
$ sed 's/Alex\s/Claudia /g'
```

For more information: [Uso del Comando Sed](#)

23 Docker Desktop

- Docker desktop corre en nuestro Ubuntu desde Windows. Por tanto, si queremos que el Docker de nuestro Ubuntu tenga los certificados necesarios para conectarse a los recursos de nuestra empresa, debemos tener los certificados descargados, actualizados e instalados en nuestro sistema Windows nativo.
- Desde un terminal rellenamos el contenido del fichero de configuración de docker `~/.docker/config.json`:

```
~/.docker/config.json

{
  "auths": {
    "docker-registry.cloud.yourcompany.com": {}
  },
  "credsStore": "desktop.exe",
  "proxies": {
    "default": {
      "httpProxy": "http://urltoproxy",
      "httpsProxy": "http://urltoproxy/"
    }
  }
}
```

- En Docker Engine modificar el fichero que ahí introducimos por el siguiente:

```
{
  "builder": {
    "gc": {
      "defaultKeepStorage": "20GB",
      "enabled": true
    }
  },
  "experimental": false,
  "features": {
    "buildkit": false
  },
  "insecure-registries": [
    "docker-registry.cloud.yourcompany.com"
  ]
}
```

- Ejecutar el comando para logearnos contra el registry que hayamos escogido:

```
$ docker login -u USER -p PASSWORD docker-registry.cloud.yourcompany.com
```

- Probar el acceso al registry:

```
$ docker pull docker-registry.cloud.yourcompany.com/catalog/paas/j
```

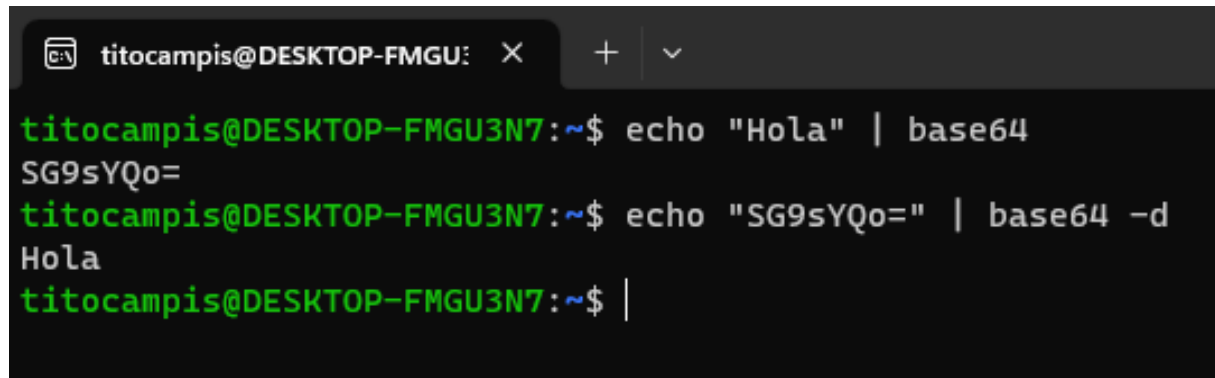
24 Base64 Encoding

Code

```
$ echo -n $PASSWORD_CLEAR | base64
```

Decode

```
$ echo -n $PASSWORD_CODED | base64 -d
```



```
titocampis@DESKTOP-FMGU: X + v
titocampis@DESKTOP-FMGU3N7:~$ echo "Hola" | base64
SG9sYQo=
titocampis@DESKTOP-FMGU3N7:~$ echo "SG9sYQo=" | base64 -d
Hola
titocampis@DESKTOP-FMGU3N7:~$ |
```

25 Tmux

Tmux, short for "Terminal Multiplexer," is a powerful command-line tool that enhances the capabilities of your terminal sessions. It allows you to organize multiple terminal windows or sessions within a single terminal window, effectively turning your terminal into a multi-pane workspace.

With Tmux, you can create multiple independent terminal sessions within a single window. This means you can work on different tasks or projects simultaneously without cluttering your desktop with multiple terminal windows.

As well tmux enable separate the execution from terminal, so if you lose the connection, what you launched continues executing.

25.1 Arguments

Configuration File

The configuration file is passed through arguments:

```
$ tmux -f /path/to/file
```

What we can do is generate a file in `/tmp/custom-tmux.conf` as follows: The configuration file is passed through arguments:

```
/tmp/custom-tmux.conf

set -g history-limit 10000
setw -g mode-keys vi

# MAJOR ops
set-option -g prefix C-a
unbind C-b
bind-key C-a last-window

# Set status bar
set -g status-left-length 30
set -g status-bg black
set -g status-fg white
set -g status-left "[fg=green]#H"
set -g status-right "[fg=yellow]#(uptime | awk -F\: '{print $5}')"
setw -g monitor-activity on
set -g visual-activity on
```

In tmux, when we want to go to **command mode**, by default we need to use **Ctrl+b**. But we are going to configure it as **screen**, with **Ctrl+a**, it is configured in the config file.

-2

tells Tmux to start in 256-color mode. Tmux supports both 256-color and 16-color modes for terminal color support. The **-2** option enables the 256-color mode.

```
$ tmux -f /path/to/file -2
```

-L [socket_name]

Sets the name of the socket used by the tmux server. The socket is a communication endpoint that allows

different processes to communicate with each other, in this case, allowing the tmux client (the terminal you're using) to communicate with the tmux server (the process managing your terminal sessions).

```
$ tmux -f /path/to/file -2 -L test-tmux
```

attach

Attach to tmux session X, it is used when you want to join an already created tmux session:

```
$ tmux -f /path/to/file -2 -L attach
```

25.2 Commands Inside tmux

General

Command	What it does?
CTRL-a c	New tmux "tab"/session
CTRL-a n	Next "tab"
CTRL-a p	Prev "tab"
CTRL-a #N	Next "tab"
exit	exit current tab
CTRL-d	exit current tab
CTRL-a ,	change current tab name
CTRL-a d	de-attach tmux
CTRL-a &	Destroy current tab

Sppliting

Command	What it does?
CTRL-a "	New tmux "tab"/session
CTRL-a %	Next "tab"
CTRL-a <arrow-keys>	Prev "tab"
CTRL-a CTRL-<arrow-keys>	Next "tab"
exit	exit current tab
CTRL-a x	exit current tab
CTRL-a CTRL-o	change current tab name
CTRL-a q	de-attach tmux
CTRL-a META-o	de-attach tmux
CTRL-a space &	Destroy current tab

26 Others

26.1 Ubuntu vs RH7

Ubuntu es una distribución de Linux que se basa en un kernel Debian, lo que significa que no funciona exactamente igual que otras distribuciones con otros kernel. RH7 al igual que Centos (Open Source) trabajan con un kernel diferente y por tanto los comandos son diferentes. Por ejemplo el gestor de paquetes de Debian es apt-get y el de RH7 es yum.

26.2 Vagrant

Vagrant is a tool for building and managing virtual machine environments in a single workflow.

- **vagrant global-status:** nos muestra el estado de todas las maquinas vagrant que tenemos corriendo. Ojo! **This data is cached and may not be completely up-to-date (use "vagrant global-status -prune" to prune invalid entries).**
- **vagrant global-status -prune:** same as before, but up-to-date.
- **vagrant status vagrant_id or vagrant_name:** shows the status of the vagrant with "vagrant_id" or "vagrant_name" (vagrant_name == cloudlabxxx)
- **vagrant up vagrant_name:** initialize a new vagrant with the id "vagrant_id", it can take a lot of time (15 minutes).
- **vagrant halt vagrant_id or vagrant_name:** stops the vagrant
- **vagrant destroy -f vagrant_id or vagrant_name:** destroy the vagrant with the id "vagrant_id", you lose all your configurations, but not your data into /vagrant.
- **ps -ef | grep cloudlabxxx:** show the processes running in vagrant.
- **kill -9 process_id:** kill the process with "process_id"

26.3 Red Hat Package Installer

26.3.1 RPM

RPM (Red Hat Package Manager) is a free open and **powerful package management system**. The name refers to file format **.rpm** and the package manager program itself. An RPM package can contain an arbitrary set of files. Most RPM files are “binary RPMs” (or BRPMs) containing the compiled version of some software. There are also “source RPMs” (or SRPMs) containing the source code used to build a binary package.

It is capable of:

- **Building computer software from source** into easily distributable packages.
- **Installing, updating and uninstalling** packaged software.
- **Querying detailed information** about the packaged software, whether installed or not.
- **Verifying integrity** of packaged software and resulting software installation.

26.3.2 YUM

27 Timeshift to Backup and Restore Your Linux System

27.1 Introduction

Linux is susceptible to system failures caused by incorrect commands or system operations. So if you use Linux on your main computer, you may frequently encounter problems. Fortunately, there are system restoration tools that create snapshots of your files and settings, which you can restore on your system to put it back to its previous functioning point in case any of your operations renders it unusable.

Timeshift works by creating a snapshot of your system using either `rsync` or `btrfs` mode, depending on your Linux distro. To do this, what Timeshift essentially does is create a restore point for your system at a time when everything's running smoothly. This backup includes all the system files and settings—and no user files or documents. That way, when you accidentally mess up something on your system while configuring or customizing it, you can restore it back to this restore point and revert all your changes.

27.2 Timeshift Installation

The first step is install timeshift, depending on your system you will use different commands. For Ubuntu:

```
$ sudo apt install timeshift
```

27.3 Create a Snapshot

```
$ sudo timeshift --create --comments "A new backup" --tags D
```