

Runtrack 2

SHELL

Livio Gonzalez-Luna

Job 1 :

La syntaxe de la commande **ls** est la suivante :

- **ls [OPTION][FICHIERS]**

Lorsqu' il est utilisé sans options et sans arguments, ls affiche une liste des noms de tous les fichiers du répertoire actuel.

- **ls -l** : Affiche la liste avec un plus grand format et plus de détails
- **ls -lah** : Affiche la liste plus la taille des différents fichiers.
- **ls -1** : Affiche les fichiers en liste
- **ls -lr** : Affiche la liste des fichiers dans l'ordre inverse alphabétique.

Afficher le manuel de commande **ls** : **man ls**

Afficher la liste plus les fichiers cachés : **ls -la ; ls -all**

```
total 276
drwx----- 8 root root 4096 Oct 4 10:56 .
drwxr-xr-x 19 root root 4096 Oct 4 10:55 ..
-rw----- 1 root root 107 Oct 2 09:40 .bash_history
-rw-r--r-- 1 root root 3106 Oct 15 2021 .bashrc
-rw-r--r-- 1 root root 3160 Oct 4 10:52 .bashrc.save
drwx----- 2 root root 4096 Oct 4 10:50 .cache
lrwxrwxrwx 1 root root 13 Oct 2 09:30 Desktop -> /root/Desktop
lrwxrwxrwx 1 root root 15 Oct 2 09:30 Documents -> /root/Documents
lrwxrwxrwx 1 root root 15 Oct 2 09:30 Downloads -> /root/Downloads
drwx----- 3 root root 4096 Oct 2 14:36 .launchpadlib
drwxr-xr-x 3 root root 4096 Oct 4 10:50 .local
-rw-r--r-- 1 root root 0 Oct 2 09:33 .motd_shown
lrwxrwxrwx 1 root root 11 Oct 2 09:30 Music -> /root/Music
```

1. Ajouter des options à une commande et leur syntaxe.

Du point de vue d'Unix, une commande n'est rien d'autre qu'une liste d'arguments dont le premier représente l'exécutable. Les arguments ne sont que des chaînes de caractères.

La distinction passe par des conventions :

- o **La position** : Elle est utilisée par des commandes comme **tar**.
Exemple : la commande **tar xzvf fichier.tar.gz**
 - le premier paramètre correspond aux options de **tar** (**x**=extract, **z**=gunzip, **v**=verbose, **f**=file)

- **Le simple tiret** : Elle consiste à précéder d'un tiret une lettre représentant une option. Il est également possible avec cette convention de regrouper plusieurs options dans un seul argument.
- **Le double tiret** : la convention du double tiret permet de corriger le manque de lisibilité du simple tiret. Souvent ces deux conventions coexistent. Avec cette convention, il n'est pas possible de combiner plusieurs options en une seule

Job 2 :

La commande `cat` (concatenate) est souvent utilisée sous Linux/Unix. La commande `cat` permet d'afficher le contenu du fichier.

1. Lisez un fichier en utilisant une commande qui permet seulement de lire :
 - **`cat [FICHIER] ->`**
2. Afficher les 10 premières lignes du fichier `". bashrc"` :
 - **`head [FICHIER] -> head .bashrc`**
3. Afficher les 10 dernières lignes du fichier `". bashrc"` :
 - **`tail [FICHIER] -> tail .bashrc`**
4. Afficher les 20 premières lignes du fichier `". bashrc"` :
 - **`head -n 20 [FICHIER] -> head -n 20 .bashrc`**
5. Afficher les 20 dernières lignes du fichier `". bashrc"` :
 - **`tail -n 20 [FICHIER] -> tail -n 20 .bashrc`**

Job 3 :

La commande apt-get permet d'effectuer l'installation et la désinstallation de paquets en provenance d'un dépôt APT. Pour utiliser cette commande il faut disposer des droits d'administration.

La commande « sudo apt install [PACKET] » a 2 avantages par rapport à apt-get :

- La coloration du texte pour mieux se repérer
- Une barre d'avancement durant la décompression et la configuration des paquets.

La commande sudo apt-get install -f permet de réparer le fichier.

La commande sudo apt-get remove [PACKET] permet de désinstaller le paquet.

La commande sudo apt install [PACKET]

1. Installer le paquet « cmatrix » :

- **Sudo apt install cmatrix**

2. Lancer le paquet :

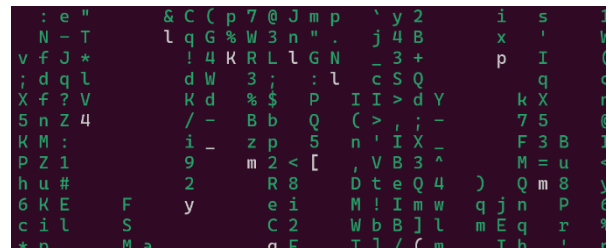
- **Cmatrix**

3. Mettre à jour son gestionnaire de paquets :

- **Sudo apt update**

4. Mettre à jour ses différents logiciels

- **Sudo apt upgrade**



1 . Télécharger Google :

2 .Checker si wget est installé :

- **Wget - -version**

1. Si aucune version apparait on installe wget :

- **sudo apt install wget**

2. Télécharger le paquet :

- Wget https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb

3. Installer le paquet :

sudo dpkg -i google-chrome-stable_current_amd64.deb

4. S'il y a des erreurs lors de l'installation

Sudo apt-get install -f

5. Saisir google-chrome dans le terminal ou dans les applications

Job 4 :

1. Afficher les utilisateurs
 - **cat /etc/passwd**
2. Afficher les utilisateurs
 - **cat /etc/group**
3. Ajouter un groupe :
 - **sudo groupadd [NAME]**
4. Ajouter user1 et user 2 :
 - **sudo useradd user1**
 - **sudo useradd user2**
5. Ajouter user2 au groupe plateformers :
 - **sudo adduser [GROUPNAME][USER]**
 - **sudo adduser plateformers user2**
6. Copier un fichier et le renommer
 - **cp [FICHIER.txt] [FICHIER_save.txt]**
7. Changer de propriétaire d'un fichier
 - **sudo chown [USER][FICHIER.txt]**
8. Changer les droits d'un utilisateur pour fichier en lecture seule :
 - **sudo chmod u=r [FICHIER.txt] ; chmod u-rx [FICHIER.txt]**
9. Changer les droits d'un fichier en lecture seule :
 - **sudo chmod u-wx [FICHIER.txt]**
10. Changer les droits d'un fichier pour que le groupe puisse y accéder en lecture/écriture
 - **sudo chmod ugo-wx [FICHIER.txt]**

Job 5 :

1. Ajouter un alias qui permettra de lancer la commande **ls -la** en tapant **la** :
 - **alias nom_alias='command'**
 - **alias la='ls -la'**
2. Ajouter un alias qui permettra de lancer la commande "apt-get update" en tapant "update" :
 - **alias update='sudo apt update'**
3. Ajouter un alias qui permettra de lancer la commande "apt-get upgrade" en tapant "upgrade"
 - **alias upgrade='sudo apt upgrade'**
4. Ajouter une variable d'environnement qui se nommera "USER" et qui sera égale à votre nom d'utilisateur
 - **USER=livio**
5. Mettre à jour les modifications de votre bashrc dans votre shell actuel
 - **Sudo apt update**
6. Afficher les variables d'environnement
 - **printenv**
7. Ajouter à votre Path le chemin "/home/votre utilisateur'/Bureau"
 - Ouvrir le dossier . **bashrc**
 - Ajouter à la fin du texte :
 - **PATH=\$PATH /home/livio/groups.txt**

```
108 # enable programmable completion features (you don't need to enable
109 # this, if it's already enabled in /etc/bash.bashrc and /etc/profile
110 # sources /etc/bash.bashrc).
111 if ! shopt -oq posix; then
112     if [ -f /usr/share/bash-completion/bash_completion ]; then
113         . /usr/share/bash-completion/bash_completion
114     elif [ -f /etc/bash_completion ]; then
115         . /etc/bash_completion
116     fi
117 fi
118
119 PATH=$PATH /home/livio/groups.txt
```

sh ▾ Tab Width: 8 ▾ Ln 119, Col 34 ▾ INS

Job 6 :

1. Premièrement Télécharger le fichier .tar sur la console
2. Ensuite Exécuter la commande :
- **tar xvf 'Ghost in the Shell'**
3. Cela décompresse le fichier en format PDF

Job 7 :

1. Création du fichier « une_commande.txt »
- sois du terminal : **mkdir [FICHIER.txt], sois d' un traitement de texte inclus comme 'nano' :**
- **nano [FICHIER_A_CREER.txt]**
2. Afficher le fichier « sources.list » :
- **gedit /etc/apt/sources.list**
3. Effectuez une recherche des fichiers commençants par "." tout en cherchant le mot 'alias'
 - La commande « grep »
 - alias qui sera utilisé depuis un fichier
 - **grep -rnw '.' -e 'alias'**

Aller plus loin :

1. Installation de tree :
 - **Sudo apt install tree**
 2. Sauver le fichier , compter les mots, mise a jour et upgrade en une seule ligne de commande :
 - **sudo tree > /home/livio/tree.save && ls | wc -w & sudo apt update && sudo apt upgrade**
-
- La Commande **wc** (Word count) :
 - wc -l** : numbers of line
 - wc -w** : numbers of words
 - wc -c** : numbers of bytes
 - wc -m** : count of charachters
 - wc -L** : count of the length of the longest line in a file

Bonus :

Le SSH (Secure Shell) désigne à la fois un protocole de communication et un programme informatique. Il permet la connexion d'une machine distante (serveur) via une liaison sécurisée dans le but de transférer des fichiers ou des commandes en toute sécurité.

1. Installer SSH (Secure Shell)
 - **sudo apt install ssh**
 - **systemctl enable ssh**
 - **systemctl start ssh**
2. Générer une clé SSH
 - **ssh-keygen -t rsa**
 - **ssh [USERNAME]@[IPADDRESS] [-p [NUM_PORT]]**
 - Deux clefs se génèrent : Une clé privée et une clé publique
3. Se connecter à une VM ou l'ordinateur d'un camarade via SSH pour empêcher le login root

4. Configurer SSH pour empêcher le login root :

- **sudo nano /etc/ssh/ssh_config v**

- Dans la ligne PermitRootLogin yes, remplacez le mot Yes par le mot No et sauvegarder le fichier. Ensuite redémarrer le programme.

- **systemctl restart ssh**

5. Modifier le port de connexion de SSH (autre que 22)

- **Sudo nano /etc/ssh/sshd_config**

- Mettre le port désiré sur le document nano

6. Ensuite se connecter en SSH sans avoir à renseigner de mot de passe

Uploader un fichier avec SSH :

- **Sudo nano /etc/ssh/sshd_config**

- Commenter

- **PasswordAuthentication yes PasswordAuthentication no**

7. Télécharger un fichier avec SSH (de votre pc ou VM vers le pc ou VM d'un camarade)

- **scp 'fichier à uploader' [ip]@[ipadress] : 'path'**

- **scp [ip@[ipadress]] : / 'pathtofile' 'path'**

- Limiter l'utilisation de SSH à un groupe particulier nommé "Plateforme_ssh" :

- **groupadd Plateforme_ssh**

- **sudo chown :Plateforme_ssh /bin/ssh**

- **sudo chmod o-rwx /bin/ssh**

- **usermod -gG Plateforme_ssh 'utilisateur'**

Questions Bonus :

1. Quel est l'intérêt d'utiliser SSH ?

SSH, ou Secure Shell, est un protocole d'administration à distance qui permet aux utilisateurs de contrôler et de modifier leurs serveurs distants sur Internet.

2. Est-ce que les clés générées par SSH par défaut sont-elles assez sécurisées ?

En paramétrant l'authentification sur un serveur SFTP, deux possibilités s'offrent à nous :

- a. Le sécuriser avec un mot de passe : Authentifier un serveur SFTP avec un mot de passe est relativement simple. L'administrateur crée un identifiant et un mot de passe pour un utilisateur. Une fois le paramétrage effectué, lorsque l'utilisateur se connecte, le serveur vérifie si la combinaison identifiant et mot de passe est correcte en acceptant ou refusant la demande.
- b. Le sécuriser avec une clé ssh : S'authentifier sur un serveur SFTP avec une clé SSH demande un peu plus de travail de paramétrage. Une paire de clés SSH est composée d'une clé privée et d'une clé publique. La paire de clés est générée automatiquement par l'ordinateur et peut atteindre 4096 bits, ce qui est beaucoup plus long qu'un mot de passe classique.

3. Les différents protocoles de transfert et leurs différences :

SMB / CIFS (Common Internet File Service)

Parfois appelé service de fichiers SMB, Samba ou Windows, le protocole CIFS est principalement utilisé par les ordinateurs Microsoft Windows, Linux et parfois par les ordinateurs MacOS. Ce service est activé par défaut.

AFP (Protocole de fichiers Apple)

AFP est utilisé par MacOS.

NFS (Network File Service)

4. vNFS est utilisé par les ordinateurs Linux et Unix. Si les utilisateurs d'un système Linux ou Unix doivent pouvoir accéder à votre NAS, il faut activer ce service.

FTP (File Transfert Protocol) et FTPS (FTP avec chiffrement SSL)

FTP est largement utilisé par les sites publics de chargement et de téléchargement. Après avoir effectué le réglage du serveur FTP. On peut également utiliser un client FTPS pour établir une connexion et des transferts de données sécurisés et chiffrés.

WebDAV

5. WebDAV est l'abréviation de Web Distributed Authoring and Versioning. WebDAV est une méthode de connexion HTTP qui permet de glisser-déposer des fichiers pour les transférer, de la même manière que via l'interface standard de Windows ou d'un MacOS.

SFTP

6. SFTP (SSH File Transfer Protocol) est un protocole de transfert de fichiers basé sur le service SSH.

Rsync

7. Rsync est un protocole réseau qui permet de synchroniser des fichiers et des répertoires d'un endroit à un autre.