
Shell :

Job 1
Job 2
Job 3
Job 4
Job 5
Job 6
Job 7
Pour aller plus loin
Bonus

Jacques SOLKARYAN

Job 1

Consignes :

- Afficher le manuel de la commande ls
- Afficher les fichiers cachés du home de votre utilisateur
- Afficher les fichiers cachés plus les informations sur les droits sous forme de liste

Questions :

- Comment ajouter des options à une commande ?
- Quelles sont les deux syntaxes principales d'écriture des options pour une commande ?

-
- La commande man ls nous permet d'afficher le manuel de la commande ls, ls qui est une commande qui permet de lister le contenu du répertoire.
 - La commande ls -la /home nous permet d'afficher les fichiers cachés du répertoire home.
 - La commande ls -la /home nous permet d'afficher les fichiers cachés plus les informations sur les droits sous forme de liste.
-
- Pour ajouter des options à une commande il nous suffit de rajouter un "-" avant l'option en question. Les options sont souvent nommées par une seule lettre et précédées d'un tiret.
 - La première syntaxe est "-", la seconde syntaxe est le "--", le "-" permet d'ajouter une option et la deuxième permet de marquer la fin d'une option.
-

Job 2

Consignes :

- Lisez un fichier en utilisant une commande qui permet seulement de lire
- Afficher les 10 premières lignes du fichier ".bashrc"
- Afficher les 10 dernières lignes du fichier ".bashrc"
- Afficher les 20 premières lignes du fichier ".bashrc"
- Afficher les 20 dernières lignes du fichier ".bashrc"

-
- La commande cat nous permet d'afficher le contenu d'un fichier. Pour ce faire, on doit tout d'abord installer la commande cat via la commande suivante : `sudo apt install cat`. Pour finir il faut la commande cat suivi d'un répertoire puis d'un fichier ce qui nous permettra de lire un fichier dans le Shell :
`cat /home/jacques/.bashrc`
 - La commande head suivi du répertoire courant du fichier ainsi que le nom du fichier nous permet d'afficher les 10 premières lignes de notre fichier demandé, dans notre cas c'est la commande suivante :
`head /home/jacques/.bashrc`
 - La commande tail suivi du répertoire courant du fichier ainsi que le nom du fichier nous permet d'afficher les 10 dernières lignes du fichier demandé, il nous suffit de mettre la commande suivante :
`tail /home/jacques/.bashrc`
 - La commande head -n 20 nous permet d'afficher les 20 premières lignes du fichier .bashrc:
`head -n 20 /home/jacques/.bashrc`
 - La commande tail -n 20 nous permet d'afficher les 20 dernières lignes du fichier .bashrc:
`tail -n 20 /home/jacques/.bashrc`
-

Job 3

Consignes :

- Installer le paquet "cmatrix"
 - Lancer le paquet que vous venez d'installer
 - Mettre à jour son gestionnaire de paquets
 - Mettre à jour ses différents logiciels
 - Télécharger les internet : Google
 - Redémarrer votre machine
 - Éteindre votre machine
-
- Pour installer le paquet cmatrix on doit mettre la commande suivante :
`sudo apt install cmatrix`
 - Pour lancer le paquet cmatrix on doit mettre la commande suivante :
`cmatrix`
 - Pour mettre à jour le gestionnaire de paquets et les différents logiciels à jour simultanément il nous suffit de mettre la commande suivante :
`sudo apt update`
 - Pour télécharger Google Chrome il faut utiliser la commande wget dans un premier temps puis l'utiliser pour installer Chrome :
`sudo apt install wget`
`wget`
`https://dl.google.com/linux/direct/google-chrome-stable_current_amd64.deb`
 - Pour redémarrer la machine il faut mettre la commande suivante dans le shell :
`reboot`
 - Pour éteindre la machine il faut mettre la commande suivante dans le shell :
`halt`
-

Job 4

Consignes :

- Créer un groupe appelé "Plateformeurs"
- Créer un utilisateur appelé "User1"
- Créer un utilisateur appelé "User2"
- Ajouter "User2" au groupe Plateformeurs
- Copier votre "users.txt" dans un fichier "droits.txt"
- Copier votre "users.txt" dans un fichier "groupes.txt"
- Changer le propriétaire du fichier "droits.txt" pour mettre "User1"
- Changer les droits du fichier "droits.txt" pour que "User2" ai accès seulement en lecture
- Changer les droits du fichier "groupes.txt" pour que les utilisateurs puissent accéder au fichier en lecture uniquement
- Changer les droits du fichier pour que le groupe "Plateformeurs" puissent y accéder en lecture/écriture.

-
- Pour créer un groupe on doit mettre la commande suivant :
`sudo groupadd Plateformeurs`
 - Pour créer un nouvel utilisateur appelé "User1" il nous suffit de mettre la commande suivante :
`sudo useradd User1`
 - Pour créer un nouvel utilisateur appelé "User2" il nous suffit de mettre la commande suivante :
`sudo useradd User2`
 - Pour ajouter User2 dans le groupe Plateformeurs créé auparavant on doit mettre la commande suivante :
`sudo adduser User2 Plateformeurs`
 - Pour copier votre users.txt et le renommer en droits.txt on doit mettre la commande suivante :
`cp users.txt droits.txt`

- Pour copier votre users.txt et le renommer en groupes.txt on doit mettre la commande suivante :
`cp users.txt groupes.txt`
 - Pour changer le propriétaire du fichier droits.txt on doit utiliser la commande chown (chown= change owner) :
`sudo chown User1 droits.txt`
 - La commande qui permet de mettre User2 uniquement en lecteur sur le fichier droits.txt est la suivante :
`sudo chmod o-wx User2 droits.txt`
 - La commande qui permet de mettre les utilisateurs uniquement en lecteur sur le fichier droits.txt est la suivante :
`sudo chmod ugo-wx droits.txt`
 - La commande permettant de changer les droits du fichier pour que le groupe "Plateformeurs" puissent y accéder en lecture/écriture est la suivante :
`sudo chmod g-x Plateformeurs droits.txt`
-

Job 5

Consignes :

- Ajouter un alias qui permettra de lancer la commande "ls -la" en tapant "la"
- Ajouter un alias qui permettra de lancer la commande "apt-get update" en tapant "update"
- Ajouter un alias qui permettra de lancer la commande "apt-get upgrade" en tapant "upgrade"
- Ajouter une variable d'environnement qui se nommera "USER" et qui sera égale à votre nom d'utilisateur
- Mettre à jour les modifications de votre bashrc dans votre shell actuel
- Afficher les variables d'environnement
- Ajouter à votre Path le chemin "/home/'votre utilisateur'/Bureau"

-
- L'alias qui nous permettra de lancer la commande "ls -la" en tapant "la" est la suivante :
alias la='ls -la'
 - L'alias qui nous permettra de lancer la commande "apt get update" en tapant "update" est la suivante :
alias update='apt get update'
 - L'alias qui nous permettra de lancer la commande "apt get upgrade" en tapant "upgrade" est la suivante :
alias upgrade='apt get upgrade'
 - Pour mettre une variable d'environnement qui se nommera "USER" et qui sera égale à votre nom d'utilisateur est la suivante :
USER=jacques
 - Pour mettre à jour le fichier bashrc dans votre shell actuel on doit tout d'abord se trouver dans le répertoire du fichier puis taper la commande suivante :
source .bashrc

- La commande pour afficher les variables d'environnement est la suivante :
`printenv`
 - Pour ajouter à votre Path le chemin `"/home/jacques/Bureau"` on doit mettre la commande suivante dans le terminal :
`export PATH=$PATH:/home/jacques/Bureau`
-

Job 6

Consignes :

- Vous devez télécharger l'archive suivante et la désarchiver seulement avec le terminal.
-

- La première étape consiste à télécharger l'archive "Ghost in the Shell.tar" via le lien de téléchargement du drive directement sur la documentation . Ensuite nous devons ouvrir le terminal pour effectuer une commande via tar. Pour se faire nous devons nous trouver dans le même répertoire que notre fichier pour simplifier la commande. Cette commande est la suivante :
`tar -xvf Ghost\ in\ the\ Shell.tar.gz`

Nous avons ensuite notre fichier désarchiver que nous pouvons directement ouvrir. Le fichier désarchiver se mettra directement dans le répertoire où l'on se trouve.

Job 7

Consignes :

- Créer un fichier "une_commande.txt" avec le texte suivant "Je suis votre fichier texte"
- Compter le nombre de lignes présentes dans votre fichier de source apt et les enregistrer dans un fichier nommé "nb_lignes.txt"
- Afficher le contenu du fichier source apt et l'enregistrer dans un autre fichier appelé "save_sources"
- Faites une recherche des fichiers commençant par "." tout en cherchant le mot alias qui sera utilisé depuis un fichier

-
- La commande qui nous permet de créer un fichier texte est nano pour se faire nous devons exécuter la commande suivante :
nano
Puis mettre ce que l'on veut dans notre fichier texte et suivre les étapes pour la création du fichier.
 - La commande qui nous permet de compter le nombre de lignes dans votre fichier de source apt et les enregistrer dans un fichiers nommé "nb_lignes.txt" est la suivante :
wc -l sources.list > /home/jacques/nb_lignes.txt
 - La commande nous permettant d'afficher le contenu du fichier source apt et l'enregistrer dans un autre fichier appelé "save_sources" est la suivante :
cat sources.list > /home/jacques/save_sources.txt
 - La commande nous permettant de faire une recherche des fichiers commençant par "." tout en cherchant le mot alias qui sera utilisé depuis un fichier est la suivante :
apt search '.' || apt search 'alias'
-

Pour aller plus loin :

Consignes :

- Installer la commande tree
- Lancer la commande tree en arrière-plan qui aura pour but d'afficher toute l'arborescence de votre / en enregistrant le résultat dans un fichier "tree.save"
- Lister les éléments présents dans le dossier courant est utilisé directement le résultat de votre première commande pour compter le nombre d'éléments trouvés
- Lancer une commande pour update vos paquets, si l'update réussit alors, vous devrez lancer un upgrade de vos paquets. Si l'update échoue, votre upgrade ne se lancera pas

-
- La commande permettant d'installer la commande tree est la suivante :
`sudo apt install tree`
 - La commande qui permet de lancer la commande tree en arrière plan tout en enregistrant le résultat dans un fichier "tree.save" est la suivante :
`tree / > /home/jacques/tree.save`
 - La commande qui nous permet de lister les éléments trouvés dans le dossier courant grâce au résultat de votre première commande est la suivante :
`ls -lA |wc -l`
 - La commande nous permettant d'update puis un upgrade nos paquets est la suivante :
`sudo apt get update && sudo apt get upgrade`
-

Bonus :

Consignes :

- Installer SSH
- Générer une clé SSH
- Se connecter à une VM ou l'ordinateur d'un camarade via SSH
- Configurer SSH pour empêcher le login root (root ne peut pas se connecter en SSH)
- Modifier le port de connexion de SSH (autre que 22)
- Se connecter en SSH sans avoir à renseigner de mot de passe
- Uploader un fichier avec SSH (de votre pc ou VM vers le pc ou VM d'un camarade)
- Télécharger un fichier avec SSH (de votre pc ou VM vers le pc ou VM d'un camarade)
- Limiter l'utilisation de SSH à un groupe particulier nommé "Plateforme_ssh"

Questions :

- Quel est l'intérêt d'utiliser SSH ?
- Est-ce que les clés générées par SSH par défaut sont-elles assez sécurisées ? Justifier votre réponse
- Citez d'autres protocoles de transfert ? Quelles sont les différences entre ses protocoles ?

-
- La commande qui nous permet d'installer ssh est la suivante :
`sudo apt install ssh`
 - La commande nous permettant de générer une clé ssh est la suivante :
`ssh-keygen`
 - Pour empêcher le login root on doit aller directement dans le fichier `sshd_config` changer le paramètre "PermitRootLogin yes" on supprime le yes et on met un "no" à la place de celui-ci. Pour se

connecter à l'ordinateur ou à la VM d'un camarade il faut entrer la commande suivante :

```
ssh username@server
```

```
nano /etc/ssh/sshd_config
```

- Pour changer le port de connexion ssh on doit aller dans le même dossier que pour empêcher le login de root et modifier paramètre "Port 22" changer le "22" par un autre port.

```
nano /etc/ssh/sshd_config
```

- Pour se connecter en SSH sans avoir à renseigner le mot de passe il faut rentrer la commande suivante, mais on doit également changer le paramètre "PasswordAuthentication yes" on met "no" :

```
ssh-copy-id remote_username@server_ip_address
```

```
nano /etc/ssh/sshd_config
```

On sera ensuite invité à saisir le mot de passe et le mot de passe et on aura donc retiré le mot de passe pour les connexions en ssh.

- Pour Upload/Download on doit saisir les commandes suivantes :

```
scp 'fichier à uploader' <ip>@<ipadress> : 'path'
```

```
scp <ip>@<ipadress> : 'path' 'path'
```

- Pour limiter l'utilisation à un groupe il faut rentrer les commandes suivantes :

```
groupadd Plateforme_ssh
```

```
sudo chown :Plateforme_ssh /bin/ssh
```

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

```
usermod -gG Plateforme_ssh 'utilisateur'
```

-
- Le principal avantage de SSH est l'utilisation de cryptage pour assurer un transfert d'informations sécurisé entre le client et le serveur. SSH permet aux utilisateurs d'exécuter des commandes shell sur un ordinateur distant comme s'ils se trouvaient devant la machine physique.
 - Les clés générées de ssh par défaut sont sécurisées car elles sont en 2048 bits mais on peut changer ce paramètre pour générer une nouvelle clé en 4096 bits par exemple :

```
ssh-keygen -b 4096
```

- **FTP** : Le protocole de transfert de fichiers FTP, est une méthode de transfert populaire qui existe depuis des décennies. FTP échange des données en utilisant deux canaux distincts : le canal de commande pour authentifier l'utilisateur et le canal de données pour transférer les fichiers.

FTPS : Abréviation de FTP, FTPS est un protocole de transfert de fichiers sécurisé qui vous permet de transférer des fichiers en toute sécurité par SSL/TLS (Secure Sockets Layer/ Transport Layer Security). Les transferts FTPS peuvent être authentifiés par des méthodes de prise en charge, comme les certificats de clients, les certificats de serveurs et les mots de passe.

SFTP : SFTP signifie FTP part SSH (Secure Shell). Il s'agit d'un protocole FTP sécurisé représentant une excellente alternative aux outils FTP non sécurisés ou aux scripts manuels. SFTP permet d'échanger des données via une connexion SSH qui offre un niveau de protection élevé pour les partages de fichiers entre systèmes, cloud, collaborateurs, etc.

TFTP : Comme FTPS et SFTP, TFTP est basé sur le protocole FTP. TFTP (Trivial File Transfer Protocol) est un protocole de transfert simple qui permet d'envoyer et recevoir des fichiers. TFTP est utilisé lorsque l'on connaît la fiabilité du fichier et qu'aucune sécurité n'est requise lors de l'envoi ou de la réception du fichier car l'authentification ainsi que le chiffrement des données ne sont pas possibles. Toute personne connaissant le chemin d'accès peut télécharger les fichiers. Ce n'est donc pas la solution de transfert la plus sécurisée.

SCP : SCP, ou Secure Copy Protocol, est un ancien protocole réseau qui prend en charge les transferts de fichiers entre les hôtes d'un réseau. Il est quelque peu similaire à FTP, toutefois SCP prend en charge les fonctions de chiffrement et d'authentification.

La différence entre ses protocoles c'est que certains d'entre eux sont sécurisés et d'autres non. Ils ont également chacun leur particularité.