Administration Linux et réseau

1 - Installer Linux

- 1.1 - Rendez vous sur le site de Linux Mint. Choisissez un environnement graphique et télécharger l'ISO correspondante. (Si vous souhaitez utiliser KDE, il vous faudra aller chercher la version 18.3)
- 1.2 - (Optionnel, mais recommandé pour plus de sécurité) Pendant que l'image télécharge, trouvez le programme `sha256sum.exe` (demander au formateur). Ouvrez une console sous Windows (Menu démarrer > taper 'cmd' pour trouver 'Invite de commande') puis lancez le programme `sha256sum.exe` sur le fichier `.iso` téléchargé précedemment. Comparez la somme de contrôle obtenue avec celle disponible sur le site de Linux Mint.
- 1.3 - Créer une nouvelle machine virtuelle en suivant les instructions :
  - de type Linux, avec comme version "Other Linux (64-bit)" ("Ubuntu (64-bit)" devrait fonctionner également) ;
  - 2048 Mo de RAM semble raisonnable ;
  - créer un disque dur virtuel, de type VDI, dynamiquement alloué, de 20 Go.
- 1.4 - Utilisez l'ISO téléchargée en tant que CD Rom virtuel que vous insérez dans la machine virtuelle. Pour ce faire : dans Configuration, Stockage, cliquer sur le CD rom (vide) puis, sur l'icone de CD rom *toute à droite*, et choisir l'ISO téléchargée.
- 1.5 - Démarrer la machine : Linux Mint est censé se lancer (utiliser le mode de compatibilité sinon)
- 1.6 - Lancer l'installation de Linux Mint
  - choisir sa langue et son clavier
  - accepter l'installation des logiciels tiers
  - lors du choix du type de partitionnement, **cliquer sur "Autre chose"**
  - créer une nouvelle table de partition, puis partitionner à l'aide du "+" l'espace de la manière suivante :
    - 300 Mo pour `/boot` en ext4
    - 14 Go pour `/` en ext4
    - 5 Go pour `/home` en ext4
    - le reste (~700 Mo) en swap
  - choisissez le fuseau horaire, puis un nom d'utilisateur, de machine, et un mot de passe.
  - lancez l'installation et prenez une pause, buvez un café, ou regardez la vidéo youtube "The UNIX operating system" et laissez Brian Kernighan vous parler de l'élégance des pipes !
- 1.7 - Redémarrez la machine et logguez-vous. Mettez-vous à l'aise et prenez vos marques dans votre nouvel environnement :
  - choisissez un nouveau fond d'écran, naviguez dans les fichiers, testez le menu démarrer, changez le thème de couleur du bureau ou du terminal (Edition > Preferences > Couleurs), personnalisez (ou pas) votre PS1 et vos alias ...
  - testez le copier-coller dans la console. Vous pouvez utiliser clic droit puis "Copier" et "Coller", ou bien Ctrl+Shift+C et Ctrl+Shift+V, ou bien sélectionner du texte et utiliser le clic du milieu de la souris.
  - tapez quelques commandes et tentez de maîtriser des raccourcis comme Ctrl+R, Ctrl+A/E, Ctrl+U/K
  - (éventuellement, testez et configurer un éditeur de texte graphique comme `xed`, `atom`, ...)
- 1.8 - Vérifiez avec `df -h`, `lsblk -f` et `mount` que le partitionnement et les points de montage correspondent à ce que vous avez fait.

- 1.9 - Au bureau, un collègue vous informe que vous aurez besoin d'une partition de type NTFS sur votre disque, pour pouvoir communiquer avec un OS de type Microsoft. Vous décidez alors d'ajuster le partitionnement de votre disque. Or, pour redimensionner une partition, celle-ci ne dois pas être en cours d'utilisation. Nous allons donc éteindre la machine et redémarrer sur le Live CD, dont les utilitaires vont nous permettre de redimensionner et créer une nouvelle partition.
  - Relancez votre machine, de nouveau avec l'ISO dans le lecteur CD virtuel
  - Depuis la live CD, lancez le programme "Gparted" depuis le "Menu Démarrer"
  - Redimensionnez la partition correspondant à `/home/` pour la réduire de 1 Go
  - Créez une nouvelle partition de type ntfs prenant le 1 Go désormais libre
  - Validez les changements, et redémarrez le système
- De retour sur votre bureau, :
  - Vérifier qu'une nouvelle partition ntfs est effectivement présente via `lsblk -f`
  - Créez un dossier `windows` dans `/media/` puis montez manuellement la nouvelle partition sur `/media/windows`. (Vérifiez le résultat avec `lsblk` et `df -h`)
- 1.10 - Rendez ce montage automatique en modifiant `/etc/fstab` et en redémarrant le système. (Vérifiez le résultat avec `lsblk` et `df -h`)

Exercices avancés

- Inspectez l'arbre des processus avec `ps -ef --forest` et identifiez le serveur graphique `Xorg`. Que se passe-t-il si vous tentez de killer ce processus ?
- De retour dans la machine virtuelle, arrangez-vous pour affichez GRUB pendant le démarrage puis appuyez sur "e" pour modifier les instructions de démarrage. À la fin de la commande "linux", ajoutez `init=/bin/bash` puis poursuivez le démarrage. Que se passe-t-il ?
- Si vous avez une clef USB, trouvez de quoi flasher l'ISO depuis Windows (par exemple, Etcher ou Unetbootin) puis tentez de démarrer votre machine physique sur la live USB (n'installez pas Linux Mint sur la machine physique !!)

2 - Le gestionnaire de paquet (et les archives)

Gestionnaire de paquet

- 1.11 Suite à l'installation de votre système, vous voulez vous assurer qu'il est à jour.
  - Lancez la commande `apt update`. Quels dépôts sont contactés pendant cette opération ?
  - À l'aide de `apt list --upgradable`, identifiez si `firefox`, `libreoffice`, `linux-firmware` et `apt` peuvent être mis à jour - et identifiez l'ancienne version et la nouvelle version.
  - Lancez la mise à jour avec `apt full-upgrade`. Pendant le déroulement de la mise à jour, identifiez les trois parties clefs du déroulement : liste des tâches et validation par l'utilisateur, téléchargement des paquets, et installation/configuration.
- 1.12 - Cherchez avec `apt search` si le programme `sl` est disponible. (Utiliser `grep` pour vous simplifiez la tâche). À quoi sert ce programme ? Quelles sont ses dépendances ? (Vous pourrez vous aider de `apt show`). Finalement, installez ce programme en prêtant attention aux autres paquets qui seront installés en même temps.
- 1.13 - Même chose pour le programme `lolcat`
- 1.14 - Même chose pour le programme `nyancat` - mais cette fois, trouvez un moyen de télécharger le `.deb` directement depuis le site de debian qui référence les paquets, puis installez ce `.deb` avec `dpkg -i`. (Pour ce faire, taper par exemple `nyancat package debian` dans un moteur de recherche. Une fois arrivé sur la bonne page, vous trouverez une section 'Download' en bas. Parmis les architectures proposées, prendre `amd64`.)

- 1.15 - Parfois, il est nécessaire d'ajouter un nouveau dépôt pour installer un programme (parce qu'il n'est pas disponible, ou bien parce qu'il n'est pas entièrement à jour dans la distribution utilisée). Ici, nous prendrons l'exemple de `mongodb` (un logiciel pour gérer des bases NoSQL) dont la version 4.4 n'est disponible que via un dépôt précis maintenu par les auteurs de mongodb.
  - Regarder avec `apt search` et `apt show` (et `grep` !) si le paquet `mongodb` est disponible et quelle est la version installable.
  - Ajouter un nouveau fichier (par exemple `mongodb.list`) dans `/etc/apt/sources.list.d` avec une unique ligne : `echo "deb [ arch=amd64 ] https://repo.mongodb.org/apt/ubuntu focal/mongodb-org/4.4 multiverse`
  - Faire `apt update`. Que se passe-t-il ? Quels serveurs votre machine a-t-elle essayer de contacter ? Pourquoi cela produit-il une erreur ?
  - Ajoutez la clef d'authentification des paquets avec `wget -qO - https://www.mongodb.org/static/pgp/server-4.4.asc | sudo apt-key add -`.
  - Refaire `apt update`. Est-ce que ça fonctionne ?
  - Regarder avec `apt search` et `apt show` (et `grep` !) si le paquet `mongodb-org` est disponible et quelle est la version installable.
  - Installer le paquet. Depuis où a-t-il été téléchargé ?
  - Désinstallez ce paquet (en purgeant les données / fichiers) et supprimez le `mongodb.list` puis refaites un `apt update` pour remettre à plat la liste des paquets disponibles.
- 1.16 - Regardez le contenu de `/var/cache/apt/archives`. À quoi ces fichiers correspondent-ils ? Trouvez deux méthodes pour nettoyer ces fichiers, l'une "brutale" avec `rm`, et l'autre "propre" avec `apt`.
- 1.17 - Identifiez l'utilité de la commande `apt moo`

Gestion des archives

- 1.20 - Créez une archive (non-compressée !) de votre répertoire personnel avec `tar`.
- 1.21 - En utilisant `gzip`, produisez une version compressée de l'archive de la question précédente
- 1.22 - Recommencez mais en produisant une version compressée directement
- 1.23 - En fouillant dans les options de `tar`, trouvez un moyen de lister le contenu de l'archive
- 1.24 - Créez un dossier `test_extract` dans `/tmp/`, déplacez l'archive dans ce dossier puis décompressez-là dedans.
- 1.25 - (Avancé) En reprenant le `.deb` du programme `nyancat` de la question 1.14, utilisez `ar` et `tar` pour décompresser le `.deb` jusqu'à trouver le fichier de controle debian, ainsi que l'executable contenu dans le paquet.
- 1.26 - (Avancé) Trouvez un ou des fichiers `.gz` dans `/var/log` (ou ailleurs ?) et cherchez comment combiner `cat` et `gzip` pour lire le contenu de ce fichier sans créer de nouveau fichier.

Exercices avancés

- Utilisez `aptitude why` pour trouver la raison pour laquelle le paquet `libxcomposite1` est installé
- Utilisez `apt-rdepends` pour afficher la liste des dépendances de `libreoffice`.
- Investiguez les options de `apt-rdepends` et du programme `dot` pour générer un rendu en PNG du graphe de dépendance de `firefox`.
- Trouvez où télécharger le `.deb` du paquet `nyancat` depuis `ftp.debian.org`
- (Très avancé) Renseignez-vous sur `equivs` et créez un package virtuel `lolstuff` qui dépend de `sl`, `lolcat` et `nyancat`

3 - Notions de réseau

IP locale, globale, pings

- 3.1 - Récupérez votre IP globale depuis Windows et depuis votre machine virtuelle, via `whatsmyip.com` ou `ip.yunohost.org`. Comparez avec votre voisin. Comparez avec votre smartphone.
- 3.2 - Dans votre VM, identifiez les interfaces réseaux, leur nom, leur adresse MAC, et leur adresse IP locale à l'aide de `ip a`. (Eventuellement, comparez avec votre ancienne machine virtuelle). Tapez également `ip route` et identifiez l'adresse IP de passerelle / gateway utilisée (cela correspond à la route "default")
- 3.3 - Ouvrir une invite de commande *Windows* (Menu Démarrer, puis taper 'cmd'), utilisez `ipconfig` pour identifiez votre adresse IP locale et l'adresse IP de la passerelle.
- 3.4 - Dessinez sur papier un schéma de votre compréhension de l'agencement et des relations entre ces différentes entités (internet, le routeur du centre de formation, votre machine Windows, vos VMs)
- 3.5 - Faites plusieurs tests de "ping" entre toutes ces différentes machines :
  - Testez de pinguer l'hôte Windows depuis une VM, et vice-versa
  - Testez de pinger la gateway des VM depuis les VM ... et depuis Windows
  - Testez de pinger la gateway de l'hôte Windows depuis Windows ... et depuis les VM
- 3.6 - Essayez de pinguer les machines de vos voisins / camarades. Demandez-leur leur IP : êtes-vous capable de pinguer leur machine Windows ? Leur machines virtuelles ? Tentez de lister les IPs présentent sur le réseau local en tapant `arp -a` dans une invite de commande sur l'hôte Windows.
- 3.7 - Dans la configuration de votre machine virtuelle, passez l'interface réseau en mode 'Bridge' (ou 'Pont') plutôt que NAT. Désactivez ensuite la connexion filaire pour forcer la VM à se reconnecter au réseau. Quelle est la nouvelle adresse IP ? Refaites quelques-un des tests précédents. Tentez de scanner les IP du réseau avec `sudo arp-scan --localnet`. Êtes-vous capable de pinguer les machines de vos voisins ?
- 3.8 - Arrivez-vous à pinger `89.234.141.68` ? Utilisez `whois` pour identifier l'entité propriétaire de cette IP.
- 3.9 - (Avancé) Tentez des `traceroute` vers l'IP d'un voisin, vers wikipedia.org, google.com, yunohost.org et yoloswag.team.

TCP, ports et protocoles

- 3.10 - Utilisez `lsof -i` pour lister les connexions actives. Arrivez-vous à identifier à quoi elle correspondent ? (Si la commande ne retourne rien d'intéressant, ouvrir une page Wikipedia dans Firefox et relancer la commande)
- 3.11 - Testez avec `nc -zv <adresse> <port>` si certains ports sont ouverts pour la machine 89.234.141.68. Par exemple, tester les ports 22, 53, 80, 443 et 6667.
- 3.12 - Dans une console, lancez `telnet yoloswag.team 80` puis dans le sous-shell ainsi ouvert, tapez "`GET / HTTP/1.0`". Que voyez-vous apparaître ? Qu'avez-vous fait ?
- 3.13 - (Avancé) Installez le paquet `wireshark`. Lancez cet outil en root et lancer une analyse de traffic. Vous voyez ensuite défiler les différent paquet. Ajouter un filtre pour montrer seulement le protocole HTTP. Pendant que l'analyse tourne, connectez-vous à un site en HTTP (pas HTTPS !) comme `yoloswag.team`, et regardez les paquets trouvés par `wireshark`. Êtes-vous capable de trouver le code source de la page en analysant ces paquets ?

DNS et /etc/hosts

- 3.14 - À l'aide de `host`, récupérez l'IP des machines `wikipedia.fr`, `lemonde.fr`, `yunohost.org`, `arn-fai.net` et `dismorphia.info`. Testez aussi avec `dig +short <machine>`
- 3.15 - Dans votre fichier `/etc/hosts`, ajoutez une ligne `127.0.0.1 google.fr`. Quel effet cela produit-il ? Et si vous ajoutez `92.92.115.142` à la place ?
- 3.16 - (Avancé) Analysez où sont envoyées les requêtes DNS (port 53) avec Wireshark. En déduire quel est le résolveur DNS utilisée par le système. Remplacez le contenu du `/etc/resolv.conf` par `nameserver 89.234.141.68` et refaites des requêtes DNS. Confirmez avec `wireshark` que ces requêtes sont bien envoyées vers le nouveau résolveur.

4 - Notions de cryptographie

- 4.0 - Installer `gpg` si le programme n'est pas déjà présent
- 4.1 - Générer une clef GPG avec `gpg --full-generate-key`. Lors de la création, on peut garder toutes les options par défaut. Pour le nom et email, vous pouvez utilisez de "fausses" informations comme `votreprenom@formationlinux`.
- 4.2 - Récupérer la clef GPG du formateur puis l'importer avec `gpg --import <chemin_vers_la_clef>`. S'assurer que la clef a bien été importée avec `gpg --list-keys`.
- 4.3 - Écrire un court message pour le formateur dans un fichier (par exemple, 'Je fais du chiffrement !') puis chiffrer ce fichier avec

```
gpg --recipient leformateur@example.com --encrypt --armor <fichier>
```

Affichez ensuite le contenu de `<fichier>.asc` : il s'agit du message chiffré à destination du formateur !

- 4.4 - Affichez votre clef publique avec

```
gpg --armor --export votreprenom@formationlinux
```

Il vous faudra la fournir au formateur pour qu'il puisse vous répondre en chiffré !

- 4.5 - Envoyez depuis `yopmail.com`, un mail au formateur contenant le message chiffré **et votre clef publique**.
- 4.6 - Attendre une réponse, et tenter de la déchiffrer avec `gpg --decrypt`.

5 - Se connecter et gérer un serveur avec SSH

- 5.1 - Pingez votre serveur, connectez-vous dessus en root (si possible en vérifiant la fingerprint du serveur) et **changer le mot de passe** ! (Choisir un mot de passe un minimum robuste : il sera mis à l'épreuve !!!). Dans une autre console, constater qu'il y a maintenant une entrée correspondant à votre serveur dans `~/.ssh/known_hosts`.
- 5.2 - **Sur votre serveur**, familiarisez-vous avec le système :
  - de quelle distribution s'agit-il ? (`lsb_release -a` ou regarder `/etc/os-release`)
  - quelle est la configuration en terme de CPU, de RAM, et d'espace disque ? (`cat /proc/cpuinfo`, `free -h` et `df -h`)
  - quelle est son adresse IP locale et globale ?
- 5.3 - **Sur votre serveur** : donnez un nom à votre machine avec `hostnamectl set-hostname <un_nom>`. (Attention, ce nom est purement cosmétique et interne à la machine. Il ne s'agit

pas d'un vrai nom de domaine résolvable et accessible par n'importe qui sur internet, comme celui qui sera configuré à la question 10.8)

- 5.4 - **Sur votre serveur** : créez un utilisateur destiné à être utilisé plutôt que de se connecter en root.
  - Créez-lui un répertoire personnel et donnez-lui les permissions dessus.
  - Définissez-lui un mot de passe.
  - Ajoutez-le au groupe `ssh`.
  - Assurez-vous qu'il a le droit d'utiliser `sudo`.
- 5.5 - **Depuis votre machine de bureau (VM Mint)** : connectez-vous en ssh sur votre serveur avec le nouvel utilisateur. Personnalisez (ou pas) le PS1, les alias, et votre .bashrc en général. Créez quelques fichiers de test pour confirmer que vous avez le droit d'écrire dans votre home.
- 5.6 - **Depuis votre machine de bureau (VM Mint)** : ajoutons maintenant une vrai clef SSH :
  - générez une clef SSH pour votre utilisateur avec `ssh-keygen -t rsa -b 4096 -C "un_commentaire"` ;
  - identifiez le fichier correspondant à la clef publique créé (generalement `~/.ssh/un_nom.pub`) ;
  - utilisez `ssh-copy-id -i clef_publique user@machine` pour copiez et activer la clef sur votre serveur ;
  - (notez que sur le serveur, il y a maintenant une ligne dans `~/.ssh/authorized_keys`)
  - tentez de vous connecter à votre utilisateur en utilisant désormais la clef (`ssh -i clef_privee user@machine`)
- 5.7 - **Depuis votre machine de bureau (VM Mint)**, configurez `~/.ssh/config` avec ce modèle de fichier. Vous devriez ensuite être en mesure de pouvoir vous connecter à votre machine simplement en tapant `ssh nom_de_votre_machine`

```
Host nom_de_votre_machine
    User votre_utilisateur
    Hostname ip_de_votre_machine
    IdentityFile chemin_vers_clef_privee
```

- 5.8 - Définissons maintenant un vrai nom de domaine "public" pour votre serveur, de sorte qu'il soit contactable facilement par n'importe quel être humain connecté à Internet :
  - aller sur `netlib.re` et se connecter avec les identifiants fourni par le formateur ;
  - créer un *nouveau* nom de domaine (en `.netlib.re` ou `.codelib.re`). (Ignorez les nom déjà créé, ce sont ceux de vos camarades !) ;
  - une fois créé, cliquer sur le bouton 'Details' puis (en bas) ajouter un nouvel enregistrement de type 'A' avec comme nom '@' et comme valeur l'IP globale(!) de votre serveur ;
  - de retour dans une console, tentez de résoudre et pinger le nom de domaine à l'aide de `host` et `ping` ;
  - modifiez votre `~/.ssh/config` pour remplacer l'ip de la machine par son domaine, puis tentez de vous reconnecter en SSH.
- 5.9 - Depuis votre machine de bureau (Mint), récupérez sur internet quelques images de chat ou de poney et mettez-les dans un dossier. Utilisez `scp` pour envoyer ce dossier sur le serveur.

Exercices avancés

- Installez MobaXterm sous Windows et essayez de vous connecter à votre serveur avec cet outil.

- Utilisez `sshfs` pour monter le home de votre utilisateur dans un dossier de votre répertoire personnel.
- Utilisez `ssh -D` pour créer un tunnel avec votre serveur, et configurez Firefox pour utiliser ce tunnel pour se connecter à Internet. Confirmez que les changements fonctionnent en vérifiant quelle semble être votre IP globale depuis Firefox.

6 - Services et sécurité basique d'un serveur

- 6.1 - Sur votre serveur, identifiez le processus `sshd` dans la liste des processus, et vérifiez le status du service "sshd".
- 6.2 - Interdisons à root de se logguer en ssh en utilisant un mot de passe. Pour ce faire, :
  - ouvrir le fichier `/etc/ssh/sshd_config` et changer la valeur de `PermitRootLogin` de `yes` à `prohibit-password`. (Attention à ne pas faire d'erreur de syntaxe !). Dans un contexte réel, nous aurions directement mis ce paramètre à `no`, mais le formateur a besoin de pouvoir encore se connecter en root via un clef - nous desactivons donc ici juste le login par mot de passe !
  - recharger ensuite le service `ssh` à l'aide de `systemctl reload sshd`
  - refaire un `systemctl status sshd` pour confirmer que le service a bien été rechargé
  - connaissant le mot de passe, tentez depuis un autre terminal d'ouvrir une nouvelle connexion ssh en root. Y arrivez-vous ? Est-ce normal ?
- 6.3 - Étudiez le fichier de log `/var/log/auth.log`, et notamment les lignes concernant `sshd`.
  - à quoi correspondent ces lignes ?
  - à l'aide de `whois`, renseignez-vous sur quelques-une des IP liée à des tentatives de connections échouées - et en particulier celles avec des IP ne correspondant pas au centre de formation.
- 6.4 - Installons un service qui bloquera ces tentatives répétées de brute-forcer le mot de passe. Fail2ban est un tel service qui analyse en permanence certains fichier de log pour déclencher automatiquement des actions (e.g. bannir une ip pour un certain temps)
  - installez le programme / service `fail2ban` ;
  - vérifiez qu'il existe désormais un service `fail2ban` actif ;
  - étudiez le fichier `/etc/fail2ban/jail.conf` et en particulier à quoi correspondent les réglages `bantime`, `findtime` et `maxretry` ;
  - étudiez le contenu de `/var/log/fail2ban.log` ;
  - modifiez les paramètres de `bantime`, `findtime` et `maxretry`. Par exemple, diminuez `maxretry` à 3 et augmentez `findtime` à 1800 ;
  - rechargez le service avec `systemctl reload fail2ban`
  - demandez à un camarade d'essayer de se connecter (en vain, et sans connaitre le mot de passe) à votre serveur **depuis son serveur à lui/elle** (*pas depuis le centre de formation !*). Observer avec lui/elle ce qui se produit dans sa console et dans le fichier de log `/var/log/fail2ban.log`
- 6.5 - Finalement, installons un firewall nommé `ufw` pour contrôler explicitement quels ports sont ouverts
  - installer `ufw` ;
  - vérifier que le firewall est pour le moment inactif avec `ufw status` ;
  - par défaut, autorisons toutes les connections sortantes mais interdisons toutes connection entrante. Pour cela, utiliser `ufw default deny incoming` et `ufw default allow outgoing` ;
  - autorisons le cas particulier de ssh, en terme de connection entrante : `ufw allow ssh` (ou plus explicitement si vous le souhaitez : `ufw allow 22/tcp` !) ;
  - activer le firewall avec `ufw enable` et vérifier le status avec `ufw status verbose`.
- 6.6 - Est-ce une bonne idée de stopper le service `sshd` ?

7 - Installer et configurer un serveur web

- 7.1 - Installer `nginx` puis vérifier que le service tourne bien avec `systemctl status nginx`. On pourra aussi utiliser `ps -ef --forest` pour constater qu'un processus nginx tourne bien, ainsi que `netstat -tulpn` pour constater qu'il écoute bien sur le port 80.
- 7.2 - Tester d'accéder à votre serveur depuis un navigateur web. Que se passe-t-il ? En déduire qu'il faut taper `ufw allow 80/tcp` - puis retenter l'opération. Comparez la page alors obtenue au fichier se trouvant dans `/var/www/html/`.
- 7.3 - Nous voudrions maintenant servir notre propre contenu web plutôt que l'exemple de nginx. Créer un dossier `mywebsite` dans `/var/www/` et à l'intérier, créer un fichier `index.html` qui contient par exemple :

```
<html>
Hello world !
</html>
```

Ensuite, modifier le fichier `/etc/nginx/sites-enabled/default` : trouvez l'instruction à modifier pour servir le dossier `/var/www/mywebsite/` plutôt que `/var/www/html/`. Vérifiez ensuite que vos changements ne causent pas de problèmes grâce à `nginx -t`, puis si tout est ok, recharger le service avec `systemctl reload nginx`. Arrivez-vous maintenant à accéder à votre page web ?

- 7.4 - Modifier votre page web pour inclure une image (se renseigner sur la balise HTML `<img>`). Par exemple, des images de chatons peuvent être trouvées sur `https://placekitten.com/` et téléchargée sur le serveur à l'aide de la commande `wget`.
- 7.5 - Rendez-vous dans `/var/log/nginx/` et lancer une surveillance du log `access.log` à l'aide de `tail -f access.log`. Depuis votre navigateur, rechargez plusieurs fois la page de votre site et étudiez les lignes qui apparaissent dans votre console.
- 7.6 - Continuez de personnaliser votre page web. Par exemple, rajoutez un lien vers une autre page web se situant dans un sous-dossier de `mywebsite`.
- 7.7 - Que se passe-t-il si vous arrêter nginx avec `systemctl stop nginx` ?

8. Déploiement d'une application PHP/Mysql : Nextcloud

Dans cette partie, on se propose de déployer une application basée sur PHP / Mysql, ce qui est un exemple classique d'application "dynamique" (c.f. architecture LAMP).

Une telle installation implique typiquement les étapes suivantes :

- téléchargement de l'application et extraction dans le bon dossier
- installation de dépendances
- création de la base de donnée
- configuration du serveur web
- configuration de l'application
- test et finalisation de l'installation

Les instructions suivantes ne viennent pas de `/dev/urandom` : elles ont été récupérées depuis le site officiel de Nextcloud (et aussi du script d'installation de l'app YunoHost !).

- 8.1 - Télécharger l'archive de la dernière version de Nextcloud (c.f. lien fourni sur Dismorphia). Décompresser l'archive à l'aide de `tar` et mettre son contenu dans `/var/www/nextcloud`.

- 8.2 - Installer les dépendances de Nextcloud (c.f. liste fournie sur Dismorphia). Vérifier qu'il y a bien un service `php7.0-fpm` et `mysql` (ou `mariadb`) qui tourne désormais sur le serveur - à la fois via `systemctl` et `ps`.

- 8.3 - Créez un utilisateur `nextcloud` et une base de donnée portant le même nom. Pour ceci, il faut ouvrir une console mysql et utiliser les incantations correspondantes (éventuellement, remplacez `password` par un vrai mot de passe) (aussi : n'oubliez pas les `;` !)

```
$ mysql -u root
MariaDB [(none)]> CREATE USER 'nextcloud'@'localhost'
                  IDENTIFIED BY 'password';
MariaDB [(none)]> CREATE DATABASE IF NOT EXISTS nextcloud;
MariaDB [(none)]> GRANT ALL PRIVILEGES ON nextcloud.*
                  TO 'nextcloud'@'localhost'
                  IDENTIFIED BY 'password';
MariaDB [(none)]> FLUSH privileges;
MariaDB [(none)]> quit
```

- 8.4 - Configurons maintenant Nextcloud pour utiliser la base de donnée qui vient d'être créée. Pour cela, rendez-vous dans `/var/www/nextcloud`. Assurez-vous qu'il existe un fichier `occ` dans ce dossier. Lancez ensuite la commande suivante (êtes-vous capable de comprendre le rôle de ses différents morceaux ?). Il vous faudra peut-être remplacer `password` par le mot de passe précédemment choisi.

```
$ php occ maintenance:install \
     --database      "mysql"     --database-name "nextcloud" \
     --database-user "nextcloud" --database-pass "password" \
     --admin-user    "admin"     --admin-pass    "password"
```

- 8.5 - Il nous faut aussi définir le domaine derrière lequel Nextcloud est hébergé : éditez le fichier `config/config.php` de Nextcloud, et rajoutez votre nom de domaine dans les "trusted domains". Ajoutez également le paramètre `overwriteprotocol` avec la valeur `http`. (Pour ces deux manipulations, il vous faudra essayer de deviner la syntaxe à partir du contenu déjà présent dans le fichier ;))

- 8.6 - Configurons maintenant Nginx pour servir l'application Nextcloud. Pour cela, récupérer et étudiez le modèle de configuration (fourni sur Dismorphia). Il vous faudra ajouter ce modèle à votre configuration nginx, et remplacer `__WEB_PATH__` et `__UNIX_FOLDER__` par des valeurs appropriée. (Ne remplacez pas toutes les occurrences à la main, utilisez un outil approprié !). Notez l'existence d'une ligne mentionnant `/var/run/php/php7.0-fpm.sock`. À votre avis, à quoi sert ce fichier et cette ligne ?

- 8.7 - Testez que la configuration nginx semble valide avec `nginx -t`, rechargez la configuration nginx et tentez d'accéder à votre application via un navigateur web. Si elle ne fonctionne pas correctement (c'est probable !), investiguez les logs d'erreur de nginx. Comparez les messages aux permissions de `/var/www/nextcloud`, et à l'utilisateur avec lequel tournent les processus `php-fpm`. Comment faut-il modifier les permissions pour que l'application fonctionne correctement ?

- 8.8 - Une fois le problème résolu, tester que l'application fonctionne correctement et découvrir Nextcloud (téléversez des fichiers, créez des dossier, etc...). (Il est même possible d'installer une application Nextcloud sur votre smartphone pour synchroniser les fichiers !)