Synthèse Linux – Exercices

Sacré Christopher

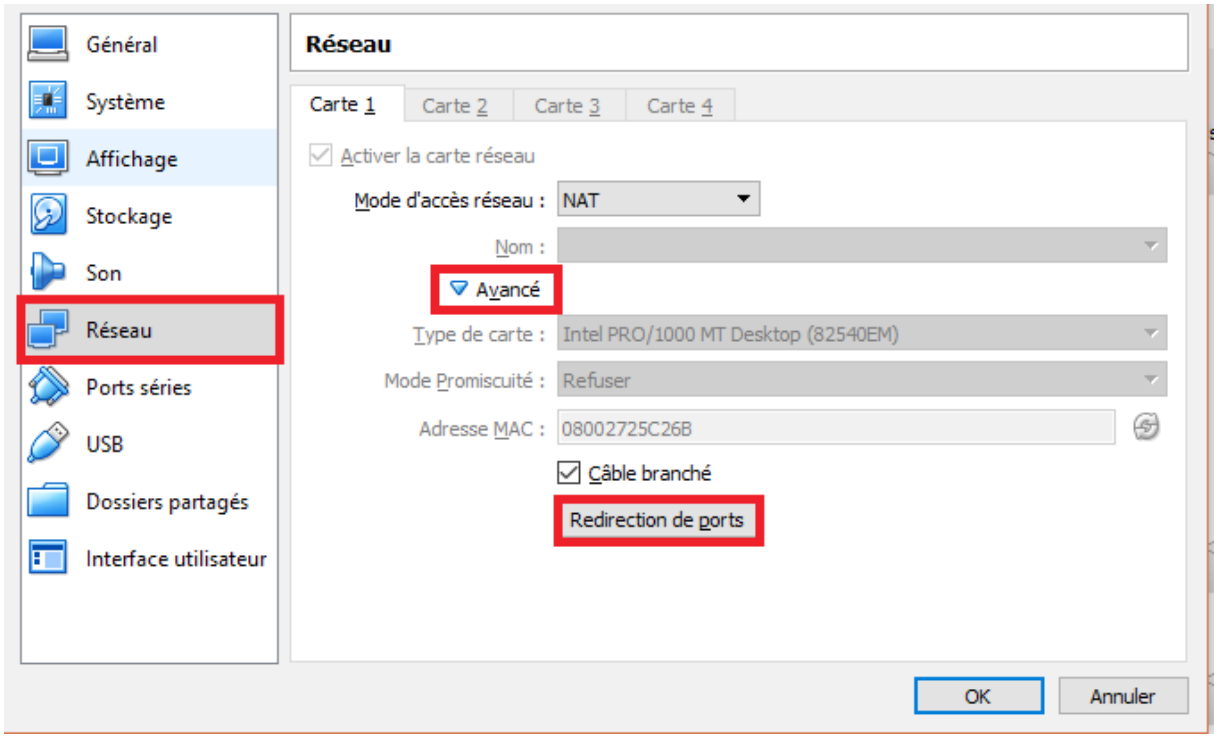
Virtual Box

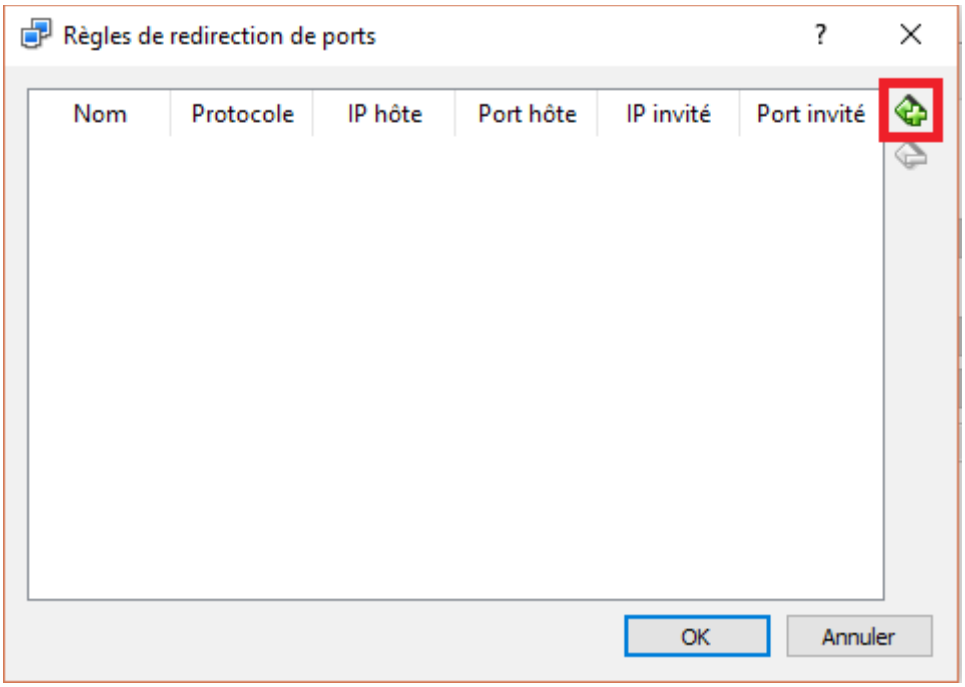
Introduction

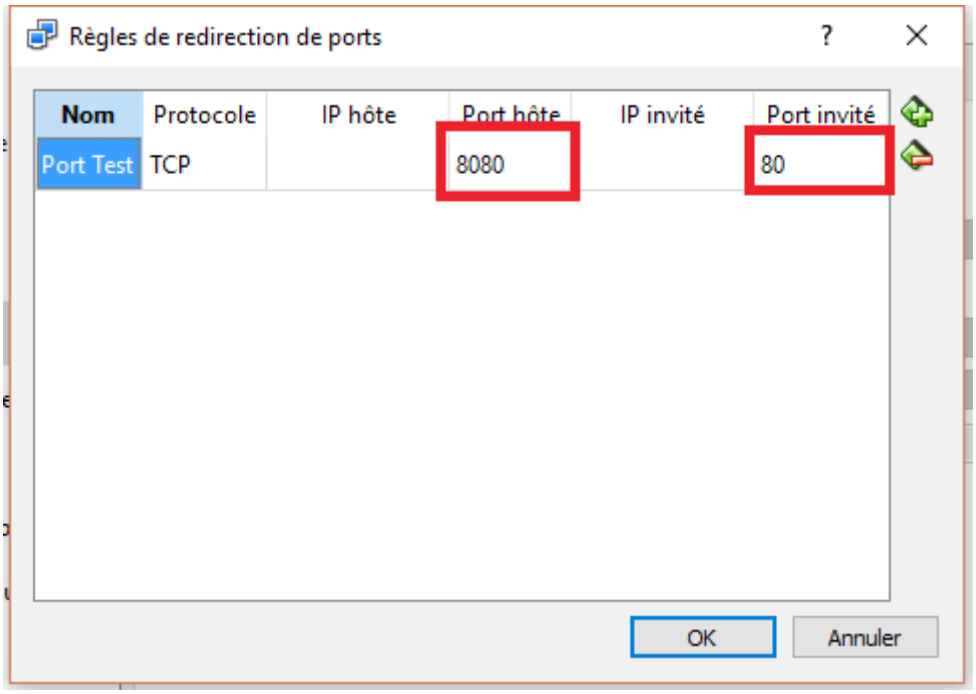
Les avantages de la virtualisation sont divers mais on notera notamment la création rapide d'un environnement de test similaire à la production et la réalisation de « snapshots » permettant de sauvegarder l'état actuel de notre machine avant toute modification.

Accéder à une machine virtuelle depuis notre machine

Pour ce qui est du réseau, une machine virtuelle est configurée en NAT. À cause de cette configuration, on ne peut par défaut pas accéder à la machine hôte depuis la machine virtuelle. Si l'on désire accéder à la machine virtuelle depuis le réseau pour notamment tester différents services (Serveur Web, SSH, ...), il faudra simplement configurer la redirection du port du NAT. On fera dès lors correspondre un numéro de port de la machine hôte à un numéro de port de la machine invitée. De cette manière, toutes les requêtes adressées vers le port hôte seront donc redirigées vers le port de la machine virtuelle.







Environnement de test

Il est souvent utile d'avoir recours à plusieurs machines virtuelles pouvant communiquer entre elles. Pour cela nous allons utiliser le « host only networking » (en bon français : le réseau privé d'hôte). Pour ce faire nous allons ajouter une carte réseau configurée sur ce mode réseau. Ainsi, les machines virtuelles pourront communiquer entre elles sans perturbations pour le « véritable » réseau physique connecté à la machine hôte. Malgré cela il faudra tout de même définir un réseau ainsi que des adresses IPs pour les machines virtuelles hôtes.

Outils pour l'administrateur système

Un administrateur système sera tôt ou tard confronté à des problèmes variés. Celui-ci devra donc disposer d'outils et de méthodes pour résoudre ces problèmes. Pour cela il pourra :

Consulter la documentation

De nombreuses informations peuvent être trouvées sur internet. Il faudra néanmoins faire attention et enter de récupérer une documentation se rapprochant le plus possible de notre distribution et de notre version de Linux.

Les pages du man sont également un bon moyen de récupérer des informations. Il existe notamment des pages « info » accesible via le logiciel/paquet « pinfo ».

De plus chaque paquet dispose d'une documentation spécifique qui est installée dans le /usr/share/doc/ « nomDeMonPaquet ». Si la documentation est malheureusement trop importante, le paquet peut se voir accompagné d'un « paquet-doc ».

Le plus souvent les logiciels sont installés dans /usr/share/ « nomLogiciel » tandis que les fichiers de configuration se trouve dans /etc/ « nomLogiciel ». (Attention ceci n'est surtout vrai que pour les machines Debian.

Consulter les logs

Le plupart des logiciels vont générer des logs qui seront stockés (la plupart du temps) au sein de « /var/log/nomLogicielOuNomPaquet ».

Actuellement les distributions Linux utilisent le système d'initialisation « systemd ». Celui ci permettra le démarrage de nos services/démons. Afin d'afficher journal de systemd on utilisera la commande:

journalctl -xf

Réseau

Dû au fait que de nombreux services / démons sont accesibles à distance (et tournent donc sur un port réseau), il est donc utile d'avoir un inventaire des services « réseaux » qui tournent sur notre machine. On utilisera pour cela la commande « netstat » :

netstat -taupe

En plus de cette commande, le fichier /etc/services nous permet également de voir les ports préréservés par le système.

APT – Gestion des packages

Toutes les distributions Linux dispose d'un système de gestion des packages permettant l'installation facile de logiciels et services. Ce système de gestion de packages résout en outre les problèmes de dépendances.

Fonctionnement

Tout d'abord il faut savoir que de nombreux dépôts contenants des paquets Debian (.deb) sont disponibles sur internet (Il s'agit de logiciel prêt à être installé). L'outil APT dispose d'un fichier de configuration (/etc/apt/sources.list) permettant de renseigner les dépôts à utiliser. Il suffit ensuite de mettre à jour depuis les dépôts (mise à jour du cache local) et de demander l'installation du logiciel à APT. L'outil installera automatiquement les dépendances nécessaires pour le logiciel demandé.

Backports

Dû au fait que la distribution Debian mise sur la stabilité, il n'est donc pas rare de ne pas avoir les dernières versions de certains logiciels. C'est là que le dépôt Backports va nous être utile, il contient tous les paquets actuellement en cours de test (« testing »), ces paquets seront donc plus récent mais également plus instables.

Afin d'utiliser les backports il faudra ajouter cette ligne au fichier /etc/apt/sources.list :

deb http://ftp.debian.org/debian jessie-backports main

Une autre manière de faire sera de procéder à une installation manuelle. Mais dans un tel cas, les mises à jour ne se feront pas à l'aide d'un simple apt-get upgrade.

Utilisation

Mettre à jour depuis les dépôts

apt-get update

Installer un logiciel

apt-get install <paquet1> <paquet2> ...

Supprimer un logiciel

apt-get remove <paquet1> <paquet2> ...

Rechercher un logiciel

apt-cache search <word>

Mettre à jour le système

apt-get upgrade

Sécurité

Les mises à jour des distributions Linux sont le plus souvent assurées par l'outil APT. La première règle en terme de sécurité informatique étant de garder un

système le plus à jour possible, APT est un outil important pour se prémunir contre des attaques éventuelles.

Dû à cela, un administrateur système doit donc réaliser des mises à jour de son système régulièrement et en particulier des mises à jour de sécurité (corrections de bogues, corection de failles, ...). Debian offre donc la possibilité de distinguer ces mises à jours des autres (cela se fait au sein du fichier /etc/apt/sources.list) et il sera donc facile d'appliquer uniquement ce type de mises à jour.

Il est également possible d'automatiser cette application de mises à jours à l'aide notamment d'outils tels que Cron.

De plus il existe même un paquet pour installer automatiquement et quotidiennement les mises à jour de sécurité.

apt-get install unattended-upgrades apt-listchanges

SSH

Les systèmes Linux actuels sont le plus souvent gérés en lignes de commande (pas d'interface graphique) et à distance. Pour ce faire, on pourrait utiliser telnet mais ce protocole a le gros inconvénient de ne rien crypter. Une simple écoute réseau permettrai alors de récupérer le mot de passe root. C'est donc pour cela que SSH est venu remplacer telnet.

Fonctionnement

Le protocole SSH effectue un échange de clés de chiffrement avant d'utiliser ces dernières pour crypter toutes les communications entre le client et le serveur.

Le port 22 est le port par défaut utilisé par SSH.

SSH est un service qui est initialisé/démarré par systemd.

Installation

apt-get install ssh

Configuration

Le fichier de configuration client est : /etc/ssh/ssh_config.

Le fichier de configuration serveur est : /etc/ssh/sshd_config.

Par défaut, SSH est installé pour permettre une authentification par login et mot de passe pour tout les utilisateurs présents sur le serveur (y compris root).

Après avoir effectué une modification dans un fichier de configuration, il faut redémarrer le service pour que les modifications soient prises en compte. On utilisera pour cela :

/etc/init.d/ssh restart

OU service ssh restart

OU systemctl restart ssh

Utilisation

Le client SSH a besoin des informations suivantes : un nom de machine ou une adresse IP, un login et un mot de passe. On peut remplacer cette authentification par login/mdp par une clé. Exemple de commande :

ssh nomutilisateur@nommachineOUadresseIP

Sécurité

Il est possible de configurer le serveur SSH pour interdire l'usage du compte root pour les connexions SSH. L'option « PermitRootLogin » doit être positionnée à « No » dans le fichier de configuration du serveur SSH.

De plus, Il également possible de restreindre l'utilisation que depuis certaines machines et qu'avec certains utilisateurs.

AllowUsers utilisateurAutorisé@sousRéseauAutorisé

Copie de fichiers

Il est à noter que dès que vous avez un accès SSH, vous pouvez copier des fichiers entre votre machine hôte et invitée via SCP/SFTP. Ceci peut se faire avec le logiciel WinSCP (Windows) ou Cyberduck(Mac).

Gestion des utilisateurs

Commandes basiques

adduser

Permet d'ajouter un utilisateur. De plus cette commande crée un profil pour l'utilisateur basé sur un squelette situé dans /etc/skel. Par défaut la home directory créée par adduser sera disponible par tout le monde (Cette configuration sera présente au sein de : /etc/adduser.conf), ceci pourrait ne pas correspondre à notre politique de confidentialité.

deluser

Permet de supprimer un utilisateur.

addgroup

Permet d'ajouter un groupe.

delgroup

Permet de supprimer un groupe ?

SU

Cette commande permet de changer d'utilisateur.

su admin

Sans argument, cela permet de devenir root.

su

Sudo

Cette a pour objectif de permettre à des utilisateurs d'exécuter des commandes en tant que superutilisateur. Attention, pour qu'un utilisateur puisse exécuter une commande avec « sudo », il doit faire partie du groupe sudo.

Installation

apt-get install sudo

Configuration

Par défaut, un utilisateur ajouté au groupe sudo possède les mêmes privilèges que root. On peut cependant changer ce comportement dans le fichier de configuration /etc/sudoers. On peut par exemple faire en sorte qu'un utilisateur sudo ne puisse exécuter que certaines commandes. Le fichier /etc/sudoers s'édite via la commande particulière visudo.

sudo visudo

Utilisation

Pour ajouter un utilisateur au groupe sudo : adduser toto sudo

Pour vérifier l'appartenance d'un utilisateur au groupe sudo : groups

Pour permettre à un utilisateur d'exécuter une commande privilégiée (« root »). Ajouter une ligne dans le fichier /etc/sudoers.

user_name ALL=NOPASSWD: /usr/bin/apt-get install

Passwd

Il est possible de verrouiller ou de désactiver le compte root. Verrouiller le compte root empêche simplement de pouvoir se connecter directement avec le compte root tandis que la désactivation le rend totalement inutilisable.

Pour verrouiller le compte root :

sudo passwd -l root

Pour désactiver le compte root :

sudo usermod --expiredate 1 root

On peut cependant encore utiliser le compte root via :

sudo -s

Sécurité

Sudo

Les avantages du SUDO sont les suivants :

1. Permettre à des utilisateurs d'exécuter une commande en tant que superutilisateur sans devoir le mot de passe de root.

2. Travailler en mode non privilégié et n'utiliser le mode privilégié que quand cela est nécessaire. Ceci réduit le risque de commettre des dommages pour le systèmes.

3. Contrôler et enregistrer qui fait quoi (SUDO enregistre toutes le commandes sudo effectuées dans /var/log/auth.log).

4. Renforcer la sécurité. En désactivant le compte root et en le remplaçant par un compte « sudo », un attaquant ne connaîtra pas le mot de passe mais également le nom du compte !

Politique de sécurité des mots de passe

Il est important d'avoir des mots de passe assez solides et de s'assurer qu'ils ne pourront pas être facilement «crackés ». Les systèmes Linux ont une sécurité de mot de passe par défaut pour les utilisateurs normaux. Les mot de passes doivent avoir une longueur de 6 caractères minimum. Ceci peut s'avérer assez faible comme sécurité. Cette politique de sécurité peut être améliorée notamment ceci :

1. Imposer un minimum de 8 caractères pour les mot de passes

2. N'autoriser que x essais pour le mot de passe

3. Imposer un nombre minimum de caractères différents lors du changement de mot de passe.

4. Fixer une durée de vie minimale et maximale du mot de passe (adduser)

La politique de sécurité se gère au moyen du module PAM(Pluggable Authentication Module) sous Linux.

Pour améliorer la politique de sécurité, on peut installer le paquet suivant :

apt-get install libpam-cracklib

Ensuite dans le fichier de configuration de pam → /etc/pam.d/common-password.
password requisite pam_cracklib.so retry=3 minlen=8 difok=3

1. retry →nombre de tentatives autorisées

2. minlen → nombre minimum de caractères pour le mot de passe

3. difok →nombre de caractères différents entre ancien et nouveau mot de passe

Apache

Fonctionnement

Le principe de fonctionnement d'Apache2 repose sur l'utilisation de modules. En effet, il suffit d'installer et/ou d'activer des modules suivant nos besoins. Il existe donc un module pour PHP, pour activer SSL, pour une authentification LDAP, … .

Apache2 est un service qui est initialisé/démarré par systemd. Pour redémarrer le service :

/etc/init.d/apache2 restart

OU service apache2 restart

OU systemctl restart apache2

En production, un serveur apache s'occupe de servir plusieurs sites Web et/ou sert de serveur HTTP frontal. Ces 2 points seront abordés ci-dessous.

Installation

apt-get install apache2 apache2-doc

L'installation créée un compte et un groupe www-data. Apache 2 fonctionne par défaut sur ce compte et groupe pour des raisons de sécurité et tourne sur le port 80.

Un site de base (page HTML) est placée dans /var/www ce qui permet de tester directement Apache2 après son installation : http://adresseip.

Il est à noter que si vous voulez tester apache sur un serveur ne disposant pas d'interface graphique (et donc pas de navigateur classique), vous pouvez installer lynx qui est un navigateur en mode texte (c'est moche mais cela permet de tester !).

Configuration

Modules

Apache dispose de nombreux modules. Nous n'en ferons pas l'inventaire ici. Pour activer un module il suffit d'utiliser la commande « a2enmod » (apache2 enable module).

Il existe évidemment la commande réciproque « a2dismod ».

N'oubliez pas de redémarrer le service apache2 après activation du module.

a2enmod <<module>>

Configuration PHP

Apache peut être configuré pour servir des pages PHP. Il suffit d'installer PHP ainsi que le module PHP pour apache et de redémarrer le service apache2.

apt-get install php5 php5-mysql libapache2-mod-php5

VirtualHosts

Les virtualhosts permettent de déployer plusieurs sites Web sur un même serveur (même adresse IP). La distinction se fait en général sur le nom du site, apache doit en effet savoir suivant l'url quel site il doit présenter.

L'ajout d'un vhost se fait en créant un fichier dans /etc/apache2/sites-available/ « monsite.conf » et puis d'y insérer :

<VirtualHost *:80>

ServerName monsite.be

nécéssaire pour qu'apache fasse une distinction sur le nom du site. Toute URL comportant « monsite.be » utilisera ce vhost.

ServerAdmin webmaster@localhost

Permet de préciser le responsable du site.

DocumentRoot /var/www/htdocs/monsite

Permet de préciser l'endroit où se trouve l'arborescence du site.

ErrorLog ${APACHE_LOG_DIR}/monsite_error.log

CustomLog ${APACHE_LOG_DIR}/monsite_access.log combined

Ces deux lignes vont permettre de déterminer où seront stockés les logs.

<Directory /var/www/htdocs/monsite>

Require all granted

AllowOverride All

</Directory>

</VirtualHost>

L'ajout de règles / restrictions sur le site se fera via la directive « Directory ».

n'autoriser l'accès au site que depuis localhost

require ip localhost

accès uniquement au site pour l'utilisateur admin

require user admin

pas de redéfinition possible (pas de .htaccess)

AllowOverride None

Pour activer le vhost, il suffit d'utiliser la commande « a2ensite » (apache2 enable site).

a2ensite monsite

Il existe la commande réciproque « a2dissite ».

Ne pas oublier de redémarrer le service apache2 après activation / désactivation.

Reverse Proxy

Un proxy inverse est un serveur frontal c'est-à-dire un serveur exposé sur Internet et par lequel toutes les requêtes passeront. Ce serveur ne traitera pas les requêtes mais se contentera des les rediriger vers d'autres serveurs internes à l'entreprise.

Les intérêts de ce mécanisme sont multiples. Vu qu'il n'y a qu'un seul point d'accès, la sécurité est plus facile à gérer. Cela permet également de mettre en œuvre du « load balancing » entre des serveurs internes. C'est également un moyen simple de rendre disponible un serveur interne sur le Web (pas besoin de configuration réseau).

Pour mettre en place un reverse proxy, il faut activer le module apache « proxy_http » et « proxy ».

a2enmod proxy proxy_http

Ensuite dans le fichier VirtualHost :

```
<VirtualHost *:80

        ServerName siteReverseProxy

        ServerAdmin webmaster@localhost

        ProxyPass / http://www.example.com/

        ProxyPassReverse / http://www.example.com/

        ErrorLog ${APACHE_LOG_DIR}/siteReverse_error.log

        CustomLog ${APACHE_LOG_DIR}/siteReverse_access.log combined

</VirtualHost>
```

Sécurité

Un serveur Web doit être sécurisé en particulier les échanges entre le client et le serveur doivent être cryptés. Ceci se fait aisément grâce au paquet openssl. Le port par défaut pour les communications https est le 443.

Installation

apt-get install openssl

a2enmod ssl

systemctl restart apache2

Création d’un certificat auto-signé

La commande openssl permet de créer un certificat ainsi qu’un clé associée à ce certificat.

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

Ici la clé et le certificat seront déposés dans le répertoire /etc/apache2/ssl créé au préalable.

Le VirtualHost sera modifié de la sorte :

```
<VirtualHost *:443>
        ServerName monsite.be
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/htdocs/monsite
        ErrorLog ${APACHE_LOG_DIR}/monsite_error.log
        CustomLog ${APACHE_LOG_DIR}/monsite_access.log combined
        SSLEngine on
        SSLCertificateFile /etc/apache2/server.crt
        SSLCertificateKeyFile /etc/apache2/server.key
        <Directory /var/www/htdocs/monsite>
                Require all granted
                AllowOverride All
        </Directory>
</VirtualHost>
```

Let’s Encrypt

Let’s encrypt est une autorité de certification libre, gratuite et automatisée. Ceci permet d’obtenir un certificat valide pour son site Web sans trop d’effort. Cependant, la machine servant le site Web doit être « publiquement » accessible ainsi que le nom du domaine. Cela veut dire qu’en test ce procédé n’est pas applicable.

https://letsencrypt.org/

MySQL

MySQL

Il faudra donner un mot de passe sûr au compte root de MySQL.

apt-get install mysql-server mysql-client

Injecter un fichier SQL :

mysql -u utilisateur -p base_exportee < base_exportee.sql

PhpMyAdmin

Installation

apt-get install phpmyadmin

Pour tester l'installation : http://adresseip/phpmyadmin

Planification de tâches

Un administrateur système a régulièrement besoin d'outils pour exécuter des tâches récurrentes (mises à jour quotidiennes, backups quotidiens, ...). Pour faciliter ceci différents outils exite sous linux :

Cron

Cron est un démon capable d'exécuter des tâches planifiées et récurrentes. Chaque utilisateur possède une «crontab » c'est-à-dire une table reprenant les commandes que l'utilisateur souhaite exécuter et à quel moment.

Utilisation

Pour éditer sa propre crontab :

crontab -e

Le format de la crontab est le suivant :

#Format

#min heure jourDuMois mois jourSemaine commande

* peut être utilisé à la place d'une valeur pour indiquer qu'il s'agit de toutes les valeurs.

Des raccourcis fréquemment utilisés existent pour les 5 premières colonnes :

1. @yearly
2. @monthly
3. @weekly
4. @daily

5. @hourly

6.@reboot

La sortie standard et d’erreur de la commande utilisée dans la crontab peut être redirigée et envoyée vers un fichier de log.

@reboot apt-get update >> /var/log/update.log

Il est à noter que si la machine n’est pas allumée au moment où la tâche a été planifiée, celle-ci ne sera jamais exécutée.

AT

La commande at permet l’exécution d’une commande à un moment ultérieur. Celle-ci sera exécutée dès que l’horloge atteindra l’heure donnée. Si la machine n’est pas en ligne à ce moment , la commande sera réalisée dès que celle-ci sera en ligne.

at 10:00 2017-12-31 apt-get update