

TD1 – Service Web

Emile Metral Version adaptée pour un travail sur le Cluster ESXi

L'objectif de ce TD est :

- de découvrir une nouvelle distribution Linux et ses spécificités (sécurité, gestion des packages...)
- de découvrir la notion d'adresse IP virtuel
- d'installer et configurer un service web (Apache)

Vous devrez répondre a toutes les questions et rendre un document numérique avec vos réponses. Les modalités de rendu vous seront communiquées par l'enseignant qui vous encadre.

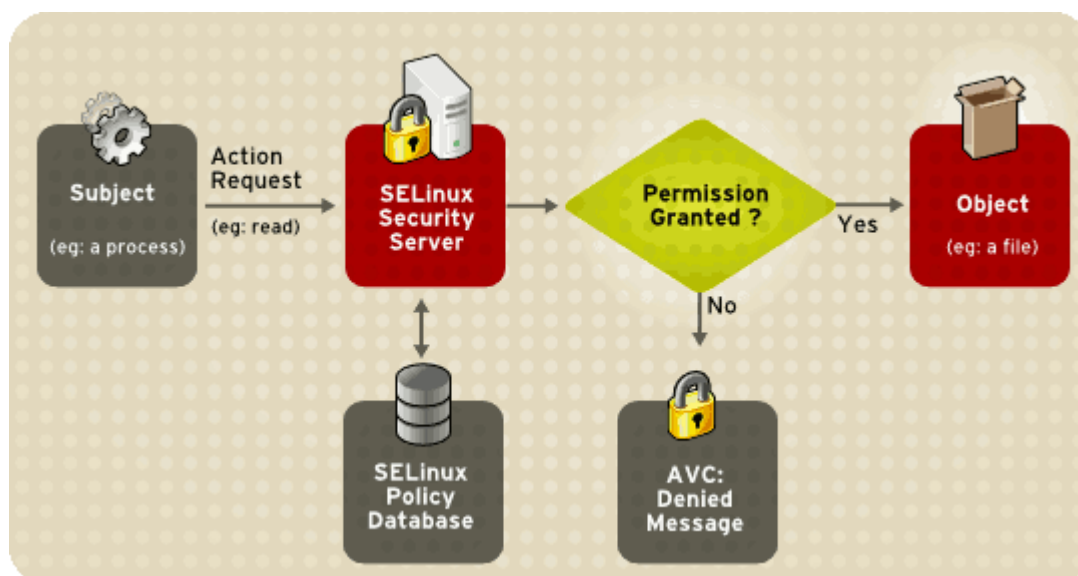
1- Les VM Centos 8 sont déployées dans la ferme. Vous trouverez un fichier vous donnant les VM ainsi que les plages d'IP qui vous sont attribuées.

- La VM est une CentOS MINIMAL (SANS Interface Graphique) avec :
 - Une seule carte réseau.
 - 2 GO de RAM
 - CPU avec 2 cores.

2-Désactivation de SELinux

- [2A] A quoi sert ce composant ?

SELinux est une architecture de sécurité qui permet de gérer les accès pour les applications, processus et fichiers système.



- [2B] Comment peut on le désactiver momentanément (Il existe au moins 2 moyens)

Moyen 1 :

Pour désactiver SELinux temporairement, dans le cadre d'un test par exemple :
`setenforce 0`

Moyen 2:

`echo 0 > /sys/fs/selinux/enforce`

- [2C] Comment peut-on le désactiver de façon permanente ?

Pour que ce changement soit permanent il faut aller modifier le champ suivant dans le fichier « `/etc/selinux/config` » :

`SELINUX=enforcing`

Le « `enforcing` » signifie que la politique de sécurité SELinux est appliquée, pour ne plus l'appliquer il faut remplacer « `enforcing` » par « `permissive` »:

`SELINUX=permissive`

- Désactivez SELinux.

3-Désactivation momentanée du pare-feu.

- [3A] Quelle commande vous permet de désactiver temporairement le firewall, le temps de procéder à la configuration de la machine ?

On le stoppe : `systemctl stop firewalld`

Puis on le désactive : `systemctl disable firewalld`

- [3B] Quelle commande vous permet d'avoir la certitude que le firewall est bien inactif ?

`systemctl status firewalld`

Results :

- `firewalld.service - firewalld - dynamic firewall daemon`
 Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
 Active: inactive (dead)
 Docs: man:firewalld(1)

Nov 15 08:53:48 localhost.localdomain systemd[1]: Starting firewalld - dynamic firewall daemon...

Nov 15 08:53:49 localhost.localdomain systemd[1]: Started firewalld - dynamic firewall daemon.

Nov 15 08:59:23 localhost.localdomain systemd[1]: Stopping firewalld - dynamic

```
firewall daemon...
Nov 15 08:59:24 localhost.localdomain systemd[1]: Stopped firewalld - dynamic
firewall daemon.
```

4-Installation du service Apache (La configuration réseau avancé viendra par la suite)

- [4A] Quels sont les trois principaux serveurs WEB disponible sous Linux

```
Les trois principaux serveurs WEB sont :
- Apache
- Nginx
- OpenResty
```

- [4B] La commande dnf (ou anciennement yum) permet d'installer les packages.
 - Quelle commande permet de retrouver le nom du package contenant le serveur Apache ? `dnf search apache`
 - Quelle commande permet d'installer le serveur Apache ? `sudo yum install httpd`
- [4C] Démarrage du service Apache -Quelle commande permet de démarrer le service Apache ? `sudo service httpd start`
- [4D] Quelle commande vous permet d'avoir la certitude que le service Apache est fonctionnel ? `sudo service httpd status`
- [4E] Quelles informations essentielles vous sont fournies par cette commande ? Cette commande nous permet de savoir si le service est actif et si il est activé entre autres.

5-Configuration du service Apache

- [5A] Ou se trouvent les fichiers de configuration de Apache ? `/etc/httpd/`
- [5B] Quelle est la structure de ce répertoire ?

```
httpd/
|----- conf/ les fichiers de configurations principaux d'Apaches
|----- conf.d/ Les fichiers secondaires de configuration
|----- conf.modules.d Dossier contenant les fichiers de configurations des
extensions
|----- modules Dossier où se trouve les modules
A créer :
|----- sites-available : stocke les configurations de tout nos sites
|----- sites-enabled : stocke les configurations des sites actifs
```

- [5C] Ou se trouve le fichier de configuration principal ? `/etc/httpd/conf/httpd.conf`
- [5D] Que contient (du point de vue logique) le répertoire conf.d Les fichiers secondaires de configuration

- [5E] Que contient le répertoire `conf.modules.d` ? Les fichiers de configurations des extensions
- [5F] Qu'est-ce qu'un module ? Un module est utilisé pour ajouter de nouvelles fonctionnalités à Apache.
- [5G] Ou sont-ils stockés ? `/etc/httpd/modules`
- [5H] Ou sont stockés les log de Apache ? `/var/log/httpd/`

6-Exploration de la configuration de base (fichier `httpd.conf`)

- [6A] Qu'est ce que le 'DOCUMENT ROOT' ? Répertoire où le serveur va chercher les documents à servir aux requêtes
- [6B] Sur quel répertoire pointe-t-il ? `/var/www/html`
- [6C] A quoi sert la directive 'Listen' ? À définir un port et/ou une adresse sur laquelle écouter les requêtes.
- [6D] A quoi sert la déclaration 'DenyFromAll' ? Définir des règles d'accès sur un répertoire ici de base il refuse tous les accès tant qu'on a pas déclaré explicitement le contraire.
- [6E] A quoi servent les directives 'AllowOverride' et 'Require' ?

`AllowOverride` : Définit la classe de directives autorisé pour le répertoire.

`Require` : Définit un contrôle d'accès à un répertoire défini.

- [6F] A quoi sert le fichier `welcome.conf` ? Sert à définir un page d'accueil si il n'y a pas d'index dans le répertoire root par défaut
- [6G] A quoi sert la commande `apachectl` ? Permet de contrôler les fonctionnalités du service Apache httpd

7-Tests et Installations complémentaires

Un serveur Apache reste basiquement un serveur de fichiers utilisant le protocole HTTP. Il lui manque fondamentalement un certain nombre de composants permettant d'avoir le comportement d'un serveur WEB avec des pages dynamiques. Vous allez installer le moteur d'exécution PHP (php engine) permettant au serveur web d'exécuter du code php présent dans les pages web.

- [7A] Exécutez la commande `yum install php -y`, Quels packages sont installés ? Les packages de php 7.2 et ses modules `common`, `cli`, et `fpm` sont installés
- [7B] Le service Apache utilise désormais systématiquement le package 'php-fpm' contenant les éléments nécessaires pour l'exécution de pages web dynamiques. Que contient ce package ? Ce package contient la gestion avancée des processus, la journalisation, le redémarrage d'urgence en cas de destruction accidentelle du cache opcode, le support de l'upload accéléré, la journalisation des scripts qui s'exécutent lentement, la naissance de processus fils, les informations sur la SAPI et les fichiers de configuration basés sur `php.ini`.
- [7C] Comment prouver que le serveur Web est désormais capable d'exécuter du PHP ?

```
On créé une page avec du php dedans :  
nano /var/www/html/index.php  
avec dedans :
```

```
<?php phpinfo(); ?>
```

- [7D] Quelle version de php est installée ? **PHP Version 7.2.24**
- [7E] Comment connaître la configuration complète du serveur web (bibliothèques installées, avec leurs versions et configurations?)
- [7F] Installez les packages et donnez le rôle des packages suivants : - php-gd : Manipulation d'images - php-mysqlnd : Manipulation des données mysql - php-pdo : Interaction avec une base de données - php-mbstring : Manipulation des chaîne de caractère

```
yum -y install php-mysqlnd php-pdo php-gd php-mbstring
```

8- Configuration avancée

Vous allez procéder à une configuration avancée (mais pas forcément conventionnelle) vous permettant de toucher du doigt les principaux points clefs d'une configuration : problèmes de permissions et d'accès, configuration de serveurs virtuels par IP, configuration de serveurs virtuels par nom.

- [8A] Installez le service vsftpd, et bien sûr, vérifiez qu'il est opérationnel. Qu'avez vous fait comme commande ? **yum -y install vsftpd.x86_64 && service vsftpd status**
- [8B] Créez un compte utilisateur nommé 'web'. Le répertoire de travail de l'utilisateur 'web' contiendra les dossiers hébergeant les différents sites web gérés par l'utilisateur 'web' : -un dossier `www.campagne.sys` pour l'instance httpd virtuel qui répondra aux requêtes sur une IP (serveur virtuel par IP, cf virtualhost) -un dossier `www.montagne.sys` et `www.glacier.sys` pour l'instance httpd virtuel qui répondra aux requêtes les deux domaines (Hébergement mutualisé, cf web multi-homing) -un dossier `www.sommet.sys` pour tester la mise en place d'un serveur répondant aux requêtes https. Donnez la liste des commandes utilisées.

```
sudo useradd web --create-home --shell /bin/bash;  
mkdir -p /home/web/www.campagne.sys /home/web/www.glacier.sys  
/home/web/www.montagne.sys /home/web/www.sommet.sys  
chown web:web -R /home/web/
```

- [8C] Vérifiez que vous pouvez accéder en lecture/écriture à tous les répertoires présents dans le répertoire `/home/web` en utilisant un client ftp comme FileZilla. Donnez les permissions de `/home/web` ainsi que celles des dossiers précédemment créés

```
Vérification des droits :  
stat -c "User:%U Rights:%A Directory:%N" /home/web/  
Résultat :
```

```
User:web Rights:drwx----- Directory:'/home/web/'

stat -c "User:%U Rights:%A Directory:%N" /home/web/*
Résultats :
User:web Rights:drwxr-xr-x Directory:'/home/web/www.campagne.sys'
User:web Rights:drwxr-xr-x Directory:'/home/web/www.glacier.sys'
User:web Rights:drwxr-xr-x Directory:'/home/web/www.montagne.sys'
User:web Rights:drwxr-xr-x Directory:'/home/web/www.sommet.sys'
```

9-Configuration réseau :

Votre VM est connectée sur un réseau en 172.16.0.0/16

Pour les configurations réseau, les Linux de la famille RedHat/CentOS utilisent des fichiers de configurations situés dans /etc/sysconfig/network-scripts.

Classiquement, les fichiers portent le nom 'ifcfg-nom_carte_reseau'. La commande `ip addr` permet de voir les différents périphériques réseaux reconnus par le système au démarrage et de récupérer leurs noms.

Voici un fichier de configuration minimal permettant de configurer une carte réseau nommée 'enp1s0' avec une IPV4 statique. Vous devez l'adapter a votre configuration :

```
TYPE="Ethernet"
BOOTPROTO="static"
DEFROUTE="yes"
NAME="enp1s0"
DEVICE="enp1s0"
ONBOOT="yes"
IPADDR=192.168.0.5
NETMASK=255.255.255.0
GATEWAY='gateway déclaré pour le vmnet8'
```

- [9A] Configurer votre carte réseau avec l'IP fixe 172.16.xxx.5/24 et donnez le contenu du fichier.

! [Conf_réseau](img/conf_reseau.png)

- [9B] A quoi sert la commande `nmcli` Elle permet de contrôler le service network manager
- [9C] A quoi sert le service NetworkManager Le service NetworkManager permet de gérer plus facilement les connections réseaux
- [9D] A quoi sert le fichier /etc/resolv.conf ? le fichier de configuration de la bibliothèque resolver permettant de déterminer, entre autre, quel serveur DNS utiliser pour résoudre un nom de domaine.
- [9E] Que devez-vous faire comme tests pour vérifier la connectivité de votre VM ? `ping 1.1.1.1`
- [9F] Votre machine peut-elle joindre `www.free.fr` ? Quelle commande avez vous utilisée pour le vérifier ? `ping free.fr` et elle le peut
- [9G] Votre VM peut-elle être jointe par l'un de vos collègues ? Si non, pourquoi ? Quels tests avez vous effectués ? Oui elle peut être jointe. `ping 192.168.100.6` fonctionne .

10-IP Virtuelles

Vous allez rajouter 3 IP virtuelles a votre VM. Classiquement, pour rajouter une IP virtuelle, il faut créer un fichier de configuration par IP virtuelle, dont le nom est de la forme, par exemple, ifcfg-ens33:0 pour la première IP virtuelle portée par la carte réseau ens33 ou ifcfg-ens33:1 pour la seconde IP virtuelle portée par la même carte réseau ens33, et ainsi de suite. Voici un exemple de configuration pour une IP virtuelle : (/etc/sysconfig/network-scripts/ifcfg-ens33:0)

```
TYPE="Ethernet"
BOOTPROTO="static"
DEFROUTE="yes"
NAME="ens33:0"
DEVICE="ens33:0"
ONBOOT="yes"
IPADDR=192.168.80.6
NETMASK=255.255.255.0
```

- [10A] Ajouter trois adresses IP virtuelles :
 - 172.16.xxx.6/16 permettant de contacter le site web www.campagne.sys



```
GNU nano 2.9.8 ifcfg-ens192:0
TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="yes"
IPADDR=192.168.100.6
NETMASK=255.255.255.0
GATEWAY=192.168.100.254
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens192:0"
UUID="7c924435-cfe0-4880-b2ac-120e7d8fe350"
DEVICE="ens192:0"
ONBOOT="yes"
```

- 172.16.xxx.10/16 permettant de joindre www.montagne.sys et www.glacier.sys

```
GNU nano 2.9.8 ifcfg-ens192:1

TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="yes"
IPADDR=192.168.100.7
NETMASK=255.255.255.0
GATEWAY=192.168.100.254
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens192:1"
UUID="7c924435-cfe0-4880-b2ac-120e7d8fe350"
DEVICE="ens192:1"
ONBOOT="yes"
```

- 172.16.xxx.15/16 permettant de joindre www.sommet.sys

```
GNU nano 2.9.8 ifcfg-ens192:2

TYPE="Ethernet"
PROXY_METHOD="none"
BROWSER_ONLY="no"
BOOTPROTO="static"
DEFROUTE="yes"
IPADDR=192.168.100.8
NETMASK=255.255.255.0
GATEWAY=192.168.100.254
IPV4_FAILURE_FATAL="no"
IPV6INIT="yes"
IPV6_AUTOCONF="yes"
IPV6_DEFROUTE="yes"
IPV6_FAILURE_FATAL="no"
IPV6_ADDR_GEN_MODE="stable-privacy"
NAME="ens192:2"
UUID="7c924435-cfe0-4880-b2ac-120e7d8fe350"
DEVICE="ens192:2"
ONBOOT="yes"
```

Donnez le contenu des 3 fichiers de configuration.

- [10B] Comment prouver que votre configuration est fonctionnelle ?

```
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:89:10:cb brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.6/24 brd 192.168.100.255 scope global noprefixroute ens192
        valid_lft forever preferred_lft forever
    inet 192.168.100.7/24 brd 192.168.100.255 scope global secondary noprefixroute ens192:0
        valid_lft forever preferred_lft forever
    inet 192.168.100.8/24 brd 192.168.100.255 scope global secondary noprefixroute ens192:1
        valid_lft forever preferred_lft forever
    inet 192.168.100.9/24 brd 192.168.100.255 scope global secondary noprefixroute ens192:2
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fe89:10cb/64 scope link
        valid_lft forever preferred_lft forever
```

11- Configuration du premier serveur virtuel : serveur virtuel par IP Ce premier serveur virtuel par IP nous permettra de joindre le site web hébergé à l'URL <http://172.16.xxx.6>. Vous êtes invité à lire la page <https://httpd.apache.org/docs/2.4/fr/vhosts/examples.html>

- [11A] Créez le premier serveur web virtuel. La racine (DocumentRoot) de ce serveur web sera bien sûr le répertoire `www.campagne.sys`. Donnez le nom et le contenu du fichier de configuration.

```
/etc/httpd/sites-available/www.campagne.sys.conf :  
  
<VirtualHost 192.168.100.7:80>  
    ServerName www.campagne.sys  
    ServerAlias 192.168.100.7  
  
    DocumentRoot /home/web/www.campagne.sys/  
    <Directory "/home/web/www.campagne.sys/">  
        Options +Indexes +FollowSymLinks  
        AllowOverride none  
        Allow from all  
        Require all granted  
    </Directory>  
  
</VirtualHost>  
  
Puis :  
ln -s /etc/httpd/sites-available/www.campagne.sys.conf /etc/httpd/sites-enabled/
```

- [11B] Prouvez que votre serveur virtuel est à l'écoute et joignable depuis une machine présente sur le réseau `vmnet8`. Quelle est votre démarche ?

En ajoutant comme entrée sur une autre machine linux dans le fichier `/etc/hosts` :

```
192.168.100.7 www.campagne.sys
```

Puis se rendre sur un navigateur et taper `www.campagne.sys` on doit tomber sur le message présent dans le fichier `/home/web/www.campagne.sys/index.html`

- [11C] Testez votre configuration en utilisant votre navigateur (depuis votre Windows ou depuis une autre VM). Pouvez-vous prouver que c'est bien le serveur virtuel que vous venez de configurer qui a répondu ? Comment ?

Car il affiche bien le message du fichier se trouvant
`/home/web/www.campagne.sys/index.html`

- [11D] Votre serveur vous a retourné un message « access denied » ? C'est probablement normal, pourtant vous avez prouvé qu'il était à l'écoute :
- A quoi sert la directive « Allow » dans le fichier de configuration.
- Quelles sont les permissions sur le répertoire `/home/web` et `/home/web/www.campagne.sys` ?
- Proposez une solution « propre » pour résoudre le problème.

La directive Allow permet de definir quelle hote peuvent acceder a certaines zones du serveur.

Pour regler le probleme du Access Denied il faut :

- Changer le proprietaire du dossier /home/web/www.campagne.sys : `chown -R apache:apache /home/web/www.campagne.sys/`
- Changer les droits sur le dossier /home/web : `chmod 755 /home/web`
- Autoriser tous les hotes a utiliser les ressources de ce repertoire a travers la directive directory et allow du vhost :

```
<Directory "/home/web/www.campagne.sys/">
    Options +Indexes +FollowSymLinks
    AllowOverride none
    Allow from all
    Require all granted
</Directory>
```

- [11E] Déployez l'application web phpsysinfo (<http://phpsysinfo.github.io/phpsysinfo/>) dans le répertoire `www.campagne.sys` et fournissez une copie d'écran de la page d'accueil de cette application.

The screenshot shows the phpsysinfo application interface. It has a blue header with the 'phpSysInfo' logo and a navigation bar. The main content area is divided into two columns. The left column, titled 'System Vital', contains a table with system metrics. The right column, titled 'Hardware Information', contains a table with hardware details. At the bottom, there is a 'Memory Usage' section with a table showing memory usage statistics.

System Vital	
Canonical Hostname	localhost
Listening IP	192.168.100.7
Kernel Version	4.18.0-80.11.2.el8_0.x86_64 (SMP) x86_64
Distro Name	CentOS Linux release 8.0.1905 (Core)
OS Type	Linux
Uptime	5 hours 49 minutes
Last boot	Mon, 15 Nov 2021 14:01:05 GMT
Current Users	1
Load Averages	0.14 0.04 0.01
System Language	English United States (en_US)
Code Page	UTF-8
Processes	229 (4 running, 136 sleeping, 89 other)

Hardware Information	
Machine	VMware, Inc. VMware7,1/440BX Desktop Reference Platform, BIOS VMW71.00V.13989454.B64.1906190538 06/19/2019
CPU	Number of processors: 4
	Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
	Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
	Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
	Intel(R) Xeon(R) Silver 4110 CPU @ 2.10GHz
PCI	Number of devices: 43
SCSI	Number of devices: 2

Memory Usage				
Type	Usage	Free	Used	Size
Physical Memory		3.19 GiB	671.48 MiB	3.85 GiB

- [11E] Testez l'URL `http://172.16.xxx.5` Avez vous obtenu une réponse ? Si Oui pourquoi ?

J'ai obtenu une reponse qui se trouve etre le vhost par default que j'ai en mis en place au debut du TP afin de verifier que mon serveur fonctionne.

12- Serveur virtuel par nom

Les pages <https://httpd.apache.org/docs/2.4/fr/vhosts/examples.html> et <https://httpd.apache.org/docs/2.4/fr/vhosts/name-based.html> contiennent les informations nécessaires à la configuration des serveurs virtuels par nom.

- [12A] Créer les deux serveurs webs virtuels répondant pour le domaine `www.montagne.sys` et `www.glacier.sys` sur l'IP `172.16.xxx.10` et donnez le contenu du/des fichier-s de configuration.

```
/etc/httpd/sites-available/www.montagne.sys.conf :

<VirtualHost 192.168.100.8:80>
    ServerName www.montagne.sys

    DocumentRoot /home/web/www.montagne.sys/
    <Directory "/home/web/www.montagne.sys/">
        Options +Indexes +FollowSymLinks
        AllowOverride none
        Allow from all
        Require all granted
    </Directory>

</VirtualHost>

Puis :
ln -s /etc/httpd/sites-available/www.montagne.sys.conf /etc/httpd/sites-enabled/

-----

/etc/httpd/sites-available/www.glacier.sys.conf :

<VirtualHost 192.168.100.8:80>
    ServerName www.glacier.sys

    DocumentRoot /home/web/www.glacier.sys/
    <Directory "/home/web/www.glacier.sys/">
        Options +Indexes +FollowSymLinks
        AllowOverride none
        Allow from all
        Require all granted
    </Directory>

</VirtualHost>

Puis :
ln -s /etc/httpd/sites-available/www.glacier.sys.conf /etc/httpd/sites-enabled/
```

- [12B] Avez vous vu la note concernant la configuration des DNS ? Donnez-en un résumé

Il faut ajouter une entrée dans les serveurs DNS pour pouvoir résoudre les nouveaux noms de domaines mais nous pouvons aussi les rentrer dans fichiers

/etc/hosts qui nous permettra d'y accéder avec leurs noms de domaine mais ça ne sera valable que pour les machines sur lesquelles nous l'auront fait.

- [12C] Mettez en place une solution permettant de garantir que le serveur virtuel hébergeant `www.montagne.sys` est bien le bon à répondre et procédez aux tests. Justifiez votre démarche.

En créant un fichier index.html avec un message personnalisé comme "Bienvenue sur le site montagne de Emile METRAL" je pourrais vérifier que c'est bien le bon serveur à répondre.

- [12D] Testez l'URL `http://172.16.xxx.5` . Quel serveur virtuel a répondu ? Est-ce le comportement attendu ? Justifiez votre réponse.

Le serveur virtuelle par défaut pointant vers les ressources present dans /var/www/html a répondu. C'est bien normal car je ne l'ai pas désactivé pour le moment.

- [12E] Avez vous vu la note intitulée « Le serveur principal disparaît » ? Quelle information essentiel contient-elle ?

Il faut créer un serveur virtuel par défaut qui comporterait une directive `ServerName` avec le nom du serveur principal. Car toute requête qui ne correspond pas à un `VirtualHost` est traitée avec la configuration du serveur principal.

13- Serveur virtuel, HTTPS et SSL

Vous avez remarqué que les serveurs virtuels ne répondent pas sur le port 443. Vous allez mettre en place un serveur web avec chiffrement fort SSL/TLS. La page [https://httpd.apache.org/docs/2.4/fr/sslssl howto.html](https://httpd.apache.org/docs/2.4/fr/sslssl%20howto.html) devrait vous aider.

- [13A] Avez vous vérifié que le module nécessaire à l'utilisation du HTTPS était installé et chargé ? Quel est le nom du module ? qu'avez vous fait pour vérifier qu'il était chargé en mémoire par Apache ?

Il faut le module mod_ssl.

```
Pour vérifier si il est installé : rpm -qa | grep mod_ssl || echo "mod_ssl pas
installé"
```

Si il ne l'est pas : `dnf install mod_ssl`

On peut maintenant vérifier qu'il est dans les modules d'Apache avec : `ls /etc/httpd/modules/ | grep mod_ssl.so`

- [13B] La commande « `openssl req -x509 -nodes -newkey rsa:1024 -keyout serveur.cle -out certificat.pem` » permet de générer les fichiers nécessaires pour l'utilisation de l'https.

- A quoi sert l'option « -x509 » : Il permet de générer un certificat auto-signé
- A quoi sert le paramètre « rsa:1024 » de l'option « -newkey » ? Ce paramètre est-il pertinent à l'heure actuelle ? newkey permet de dire de générer un nouveau certificat et rsa:1024 permet de définir l'algorithme de chiffrement donc le RSA et la taille de la clé. La taille de 1024 bits semble faible car il est recommandé aujourd'hui une taille de 2048bit pour l'algorithme RSA. -Quels sont les fichiers générés ? Que contiennent-ils ? Il y a été généré la clé privée et le certificat auto-signé
- [13C] Mettez en place le serveur virtuel www.sommet.sys Il devra répondre sur les ports 80 et 443, et donnez le contenu du fichier de configuration.

changement de la taille de cle en 2048 bits pour que cela marche puis :
/etc/httpd/sites-available/www.sommet.sys.conf

```
## Redirect HTTP Traffic to HTTPS
<VirtualHost 192.168.100.9:80>
    ServerName www.sommet.sys

    <IfModule mod_rewrite.c>
        RewriteEngine On
        RewriteCond %{HTTPS} !=on
        RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,QSA,R=permanent]
    </IfModule>

</VirtualHost>
```

/etc/httpd/sites-available/www.sommet.sys-ssl.conf

```
<IfModule mod_ssl.c>
<VirtualHost 192.168.100.9:443>
    ServerName www.sommet.sys
    # On active le chiffrement (HTTPS)
    SSLEngine On
    SSLCertificateFile /etc/ssl/certs/serveurkey/certificat.pem
    SSLCertificateKeyFile /etc/ssl/certs/serveurkey/serveur.cle

    <Directory "/home/web/www.sommet.sys/">
        Options +Indexes +FollowSymLinks
        AllowOverride none
        Allow from all
        Require all granted
    </Directory>

</VirtualHost>
</IfModule>
```

- [13D] Quel message avez-vous obtenu lors de vos tests avec votre navigateur ? Pourquoi avez vous obtenu ce message ?

Le navigateur nous demande si on est sûr de vouloir rentrer sur ce site car il n'est pas sécurisé. Cela vient du certificat auto signé car il n'est pas validé par un organisme de certification reconnu.

- [13E] Connaissez vous le site Let's Encrypt (<https://letsencrypt.org/fr/>). Quel est son rôle ? Comment peut-il vous aidez pour le problème précédent ?

Let's Encrypt fourni des certificats validé car c'est une autorite de certification. Il nous permettrai de ne plus avoir le message lorsqu'on se rend sur notre site.

14-Restriktion de l'accès utilisateur

Dans certains cas, il sera nécessaire de restreindre les accès a certains répertoires, ou alors d'autoriser des opérations particulières comme la réécriture d'URL (souvent nécessaire pour l'utilisation d'un framework PHP) Le fragment de configuration suivant permet de restreindre l'accès au répertoire « demo » :

```
<Directory demo >
  AuthName "You need an account !"
  Require valid-user
  ... autres parametres...
</Directory>
```

- [14A] Quels sont les modes d'authentification possibles?`
 - Authentification basic
 - Authentification par fournisseur`
- [14B] Qu'est ce qu'un fournisseur d'accès dans ce contexte? **Un serveur externe dediée à l'authentification avec un protocole comme le ldap**
- [14C] Pour le site www.campagne.sys, créer un répertoire « secure » et vérifier que vous pouvez bien accéder au contenu de ce répertoire. Quels tests avez-vous effectués ?

```
mkdir /home/web/www.campagne.sys/secure
```

Verification des droits :

```
stat -c "User:%U Rights:%A Directory:%N" /home/web/www.campagne.sys/secure
```

Creation d'un index.html dans le repertoire secure avec un message personnalise.

- [14D] Changer la configuration de ce serveur virtuel pour restreindre l'accès au répertoire « secure ». Vous utiliserez une authentification « basic » avec un « provider file». Donnez le contenu du fichier de configuration.

```
<VirtualHost 192.168.100.7:80>
  ServerName www.campagne.sys
  ServerAlias 192.168.100.7

  DocumentRoot /home/web/www.campagne.sys/
  <Directory "/home/web/www.campagne.sys/">
    Options +Indexes +FollowSymLinks
    AllowOverride none
    Allow from all
    Require all granted
  </Directory>
  <Directory "/home/web/www.campagne.sys/secure/">
    Options +Indexes +FollowSymLinks
    AuthType Basic
    AuthName "Acces restreint aux utilisateurs authentifies"
    AuthBasicProvider file
    AuthUserFile "/etc/httpd/passwords"
    Require valid-user
  </Directory>

</VirtualHost>
```

- [14E] Créez un utilisateur « Apache » avec les identifiants « leon/123+aze » et vérifiez qu'il a bien accès au répertoire « secure » . La commande htpasswd vous sera nécessaire. Quels tests avez-vous effectués ? Quelles commandes avez-vous utilisées ?

```
sudo htpasswd -c /etc/httpd/passwords leon
```

En me rendant sur www.campagne.sys/secure/ et en rentrant les login.

- [14F] Quelle démarche vous a permis de vérifier que le compte « leon » avec le mot de passe « 123+aze » a bien accès au répertoire « secure » ?

En me rendant sur www.campagne.sys/secure/ et en rentrant les login.

15-Fichier .htaccess

Ce fichier permet de redéfinir certains paramètres de configuration du serveur ou certains accès a des répertoires sans avoir touché les fichiers de configuration du serveur Apache, donc sans avoir à être « root ». La seule contrainte est que le fichier de configuration (du serveur virtuel) autorise une modification de ces paramètres (directive AllowOverride) pour le répertoire ou l'arborescence contenant le fichier .htaccess

- [15A] Qu'est ce qu'une réécriture d'URL ? Quel module est nécessaire pour faire une réécriture d'URL ?
- [15B] Qu'est ce qu'un Framework ? Une plateforme de developpement qui fournit les foundations pour construire de nouveaux programmes
- [15C] A quoi sert la directive AllowOverride ? Permet de gerer les possible reecriture de directive dans un dossier par un .htaccess
- [15D] Quels sont les 6 paramètres pris en compte par la directive AllowOverride ? AuthConfig - FileInfo - Indexes - Limit - Nonfatal - Options
- [15E] Lequel des paramètres permet d'autoriser l'usage d'une réécriture d'URL a partir d'un fichier .htaccess ? FileInfo
- [15F] Créez un répertoire « private » avec un fichier .htaccess. Donnez le contenu du fichier .htaccess

```
mkdir /home/web/www.campagne.sys/private  
  
touch /home/web/www.campagne.sys/private/.htaccess
```

- [15G] Dans le fichier .htaccess précédent, mettez en place les directives nécessaires pour autoriser uniquement l'utilisateur « Apache gaston/123+aze » a accéder au répertoire. Quelle est votre démarche ? Quelles commandes avez vous utilisées ?

```
sudo htpasswd -c /etc/httpd/passwords gaston  
  
nano /home/web/www.campagne.sys/private/.htaccess  
  
AuthUserFile /etc/httpd/passwords  
AuthName "Authorization Private"  
AuthType Basic  
  
#Allow only one user with specified username  
require user gaston  
  
nano /etc/httpd/sites-available/www.campagne.sys.conf  
  
<VirtualHost 192.168.100.7:80>  
    ServerName www.campagne.sys  
    ServerAlias 192.168.100.7  
  
    DocumentRoot /home/web/www.campagne.sys/  
    <Directory "/home/web/www.campagne.sys/">  
        Options +Indexes +FollowSymLinks  
        AllowOverride none  
        Allow from all  
        Require all granted  
    </Directory>  
    <Directory "/home/web/www.campagne.sys/secure/">  
        Options +Indexes +FollowSymLinks  
        AuthType Basic  
        AuthName "Acces restreint aux utilisateurs authentifies"
```



```
        AuthBasicProvider file
        AuthUserFile "/etc/httpd/passwords"
        Require valid-user
    </Directory>
    <Directory "/home/web/www.campagne.sys/private/">
        Options +Indexes +FollowSymLinks
        AllowOverride AuthConfig
    </Directory>

</VirtualHost>
```

16-Personnalisation de pages d'erreurs

Il est extrêmement désagréable et peu rassurant pour un utilisateur de rencontrer une erreur d'exécution (Erreur PDO, erreur 404, erreur 500 ...)

Sur un serveur de production il est préférable de mettre en place une gestion des erreurs, qui affichera un message personnalisé.

- [16A] Utilisez la directive « ErrorDocument » pour afficher une jolie page d'erreur 404. Cette URL devrait vous inspirer : <https://www.leptidigital.fr/webmarketing/pages-erreur-404-8896/> . Quels fichiers avez-vous modifiés ? Donnez les modifications.

```
echo "ErrorDocument 404 https://geekflare.com/errorpage" >>
/etc/httpd/conf/httpd.conf
```