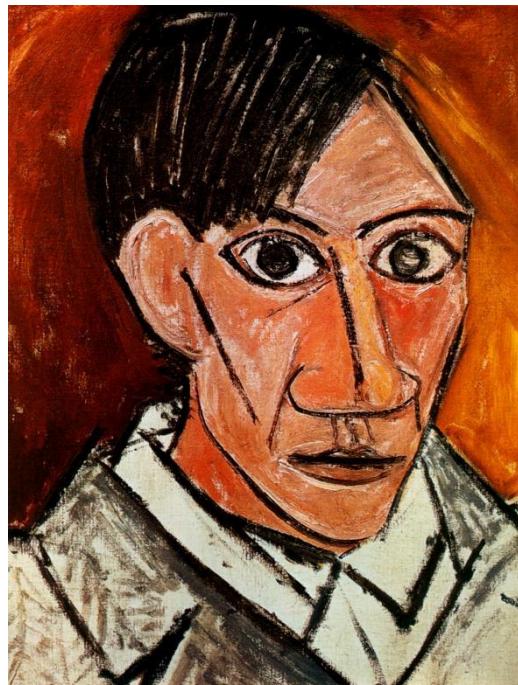


Projet d'Exposition Picasso



Auteurs: Tamara Crétard, Pierre-Louis Debuyschere,
Alan Imbault
Date: 15 janvier 2024

Tamara Crétard Pierre-Louis Debuyschere Alan Imbault	20.11.2024	
---------------------------------------------------------------	------------	-------------------------------------------------------------------------------------

Table des matières

1. Contexte.....	2
2. Gestion du projet.....	2
2.1. Plan.....	2
2.2. Issues (Problèmes).....	2
3. Solution applicative.....	3
4. Hébergement.....	3
4.1. Installer une machine virtuelle sur la ferme de serveurs.....	3
4.2. Installer SSH pour se connecter à distance.....	5
4.3. Transférer des fichiers du PC hôte au serveur web.....	7
4.4. Activer un firewall sur le serveur web.....	9
4.5. Passer le site en HTTPS avec un certificat auto-signé.....	10
4.6. Installer PHP sur le serveur.....	11
4.7. Installer MariaDB sur le serveur.....	13
4.8. Mettre en place un serveur Linux Debian dans AWS.....	13
4.9. Créer un nom de domaine DNS.....	16
4.10. Configurer Apache du serveur AWS pour utiliser le nom de domaine.....	17
4.11. Installer Certbot pour générer automatiquement un certificat SSL.....	18

Tamara Crétard
Pierre-Louis
Debuyschere
Alan Imbault

20.11.2024



1. Contexte

Expliquer le projet

2. Gestion du projet

2.1. Plan

The screenshot shows a project management interface with a dark theme. At the top, there's a header bar with a search field, a status update button, and other navigation icons. Below the header is a navigation bar with tabs for Dev, Plan (selected), Roadmap, and New view. A filter bar allows searching by keyword or field. The main area features a Kanban board with four columns: "Todo" (19 items), "In Progress" (4 items), "A faire valider" (1 item), and "Done" (0 items). Each column has a "Draft" section and a "Live" section. The "In Progress" column has one item labeled "Livrable qui présente la configuration + développement". The "A faire valider" column has one item labeled "Implémenter un serveur web sur un serveur Linux Debian 11 de la ferme de serveur". The "Done" column has no items.

2.2. Issues (Problèmes)

The screenshot shows a bug tracking system interface. At the top, it says "Fix Carousel #1" with a "FixCarousel #1" link. Below that, it says "Open" and "PLBTS opened this issue 6 minutes ago · 0 comments". A comment from PLBTS is shown, stating "Le carrousel de la page d'accueil ne s'affiche pas correctement". The bottom of the screen shows a navigation bar with links for "26", "Fix Carousel #1", "PLBTS", "Todo", "Application", and "I".

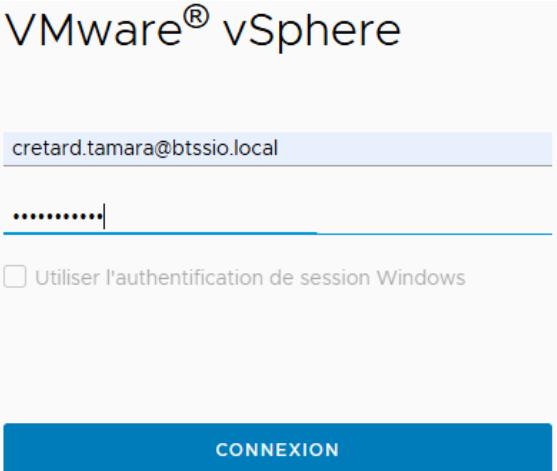
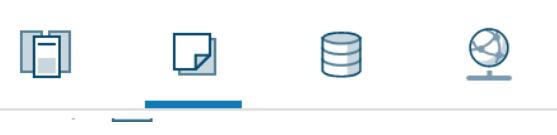
Tamara Crétard Pierre-Louis Debuyschere Alan Imbault	20.11.2024	
---------------------------------------------------------------	------------	-------------------------------------------------------------------------------------

3. Solution applicative

4. Hébergement

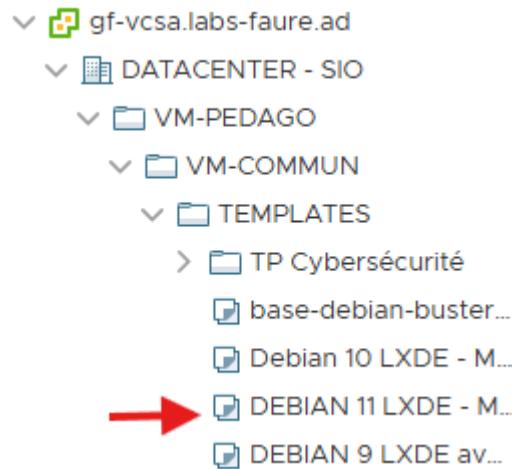
4.1. Installer une machine virtuelle sur la ferme de serveurs

Dans un premier temps, il est nécessaire d'installer une machine virtuelle sur le serveur. Voici les étapes à suivre pour le réaliser:

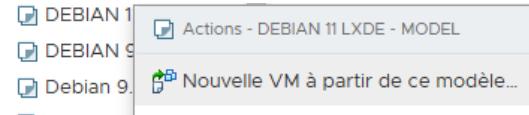
Pour accéder à la ferme de serveurs, se rendre sur https://qf-vcsa.labs-faure.ad/ et se connecter avec ses identifiants	 <p>VMware® vSphere</p> <p>cretard.tamara@btssio.local</p> <p>.....</p> <p><input type="checkbox"/> Utiliser l'authentification de session Windows</p> <p>CONNEXION</p>
Une fois connecté, aller dans le menu « VM et Modèles »	



Trouver le template DEBIAN11 LXDE dans :
 VM-PEDAGO / VM-COMMUN /
 TEMPLATES



faire click-droit, et « Nouvelle VM à partir de ce modèle »

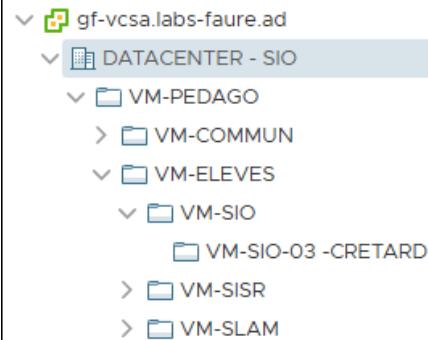


lui donner un nom et la ranger dans le répertoire situé dans VM-PEDAGO / VM-ELEVES.

Sélectionner un nom et un dossier
 Spécifiez un nom unique et un emplacement cible

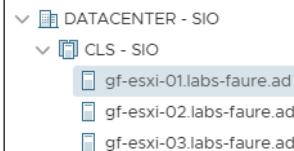
Nom de la machine virtuelle :

Sélectionnez un emplacement pour la machine virtuelle.



Pour la ressource de calcul, sélectionner au choix l'une des 3 ressources disponibles

Sélectionner une ressource de calcul
 Sélectionnez la ressource de calcul de destination pour cette opération





Pour le stockage, sélectionner DS-COMMUN

Sélectionner un stockage
 Sélectionnez le stockage pour les fichiers de configuration et de disque

Sélectionner un format de disque virtuel : Même format que la source

Stratégie de stockage VM :

Nom	Capacité	Provisionné	Libre	Type	Cluster
DS-COMMUN	931,25 Go	1,2 To	109,88 Go	VMFS 6	
DS-SISR	9,1 To	9,51 To	3,8 To	VMFS 6	

Cocher « Personnaliser le matériel de cette machine virtuelle »

- Personnaliser le système d'exploitation
 Personnaliser le matériel de cette machine virtuelle
 Mettre sous tension la machine virtuelle après la création

Comme « Network Adapter 1 », vous sélectionnez « SALLE – 209 »

Méthode virtuel Options VM AJOUTER UN PÉRIPHÉRIQUE

> CPU	1
> Mémoire	2 Go
> Hard disk 1 *	16 Go
> SCSI controller 0	Paravirtualisé VMware
> Network adapter 1 *	SALLE - 209 →
> CD/DVD drive 1	Fichier ISO banque de données
> Carte vidéo	Spécifier les paramètres personnalisés
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
> Autre	Matériel supplémentaire

Déployer la machine en cliquant sur “FINISH”

DEBIAN 11 LXDE - MODEL - Déployer depuis un modèle

✓ 1 Sélectionner un nom et...
 ✓ 2 Sélectionner une ressource...
 ✓ 3 Sélectionner un stockage
 ✓ 4 Sélectionner les options...
 ✓ 5 Personnaliser le matériel
 6 Prêt à terminer

Pour terminer Cliquez sur Terminer pour démarrer la création.

Type de provisionnement	Déployer depuis un modèle
Modèle source	DEBIAN 11 LXDE - MODEL
Nom de la machine virtuelle	projet_picaso
Dossier	VM-SIC-03 - CRÉTARD
Hôte	gf-exxi-01-lab1-faure.ad
Banque de données	DS-COMMUN
Stockage sur disque	Même format que la source
Hard disk 1 (16 Go)	DS-COMMUN (Même format que la source)

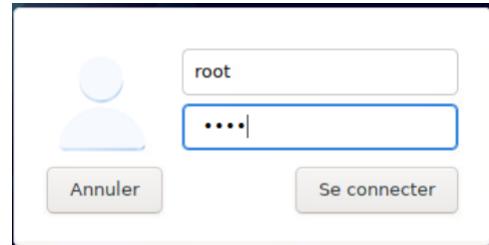
CANCEL BACK FINISH

4.2. Installer SSH pour se connecter à distance

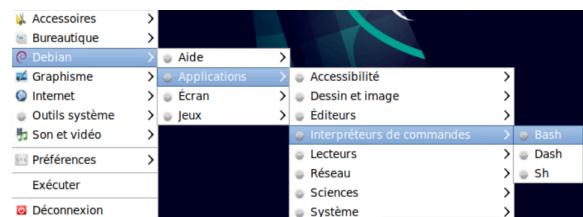
Afin de rendre possible la connexion à distance, il est nécessaire d'installer SSH sur notre machine virtuelle. Pour se faire, voici les étapes à suivre:



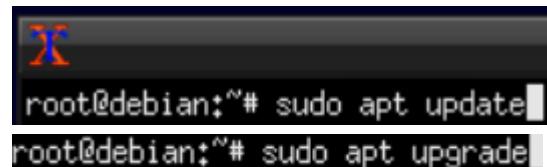
Démarrer la machine virtuelle et se connecter



Ouvrir le terminal en allant dans le menu Debian -> Applications -> Interpréteurs de commandes -> Bash.



Mettre à jour votre système avec la commande : *sudo apt update* suivi de la commande *sudo apt upgrade*



Installer le paquet openssh-server avec la commande: *sudo apt install openssh-server*

sudo apt install openssh-server

Activer et démarrer le service SSH avec les commandes suivantes:
sudo systemctl enable ssh
sudo systemctl start ssh

sudo systemctl enable ssh
sudo systemctl start ssh

Créer un utilisateur avec la commande suivante: *sudo adduser nom_utilisateur* et choisir un mot de passe

```
root@debian:~# sudo adduser tamara
Ajout de l'utilisateur « tamara » ...
Ajout du nouveau groupe « tamara » (1001) ...
Ajout du nouvel utilisateur « tamara » (1001) avec le groupe « tamara » ...
Création du répertoire personnel « /home/tamara »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe : ■
```

Ajouter le compte utilisateur au groupe sudo avec la commande suivante: *usermod -aG sudo utilisateur* et vérifier de quel groupe est l'utilisateur avec la commande *groups utilisateur*

```
root@debian:~# usermod -aG sudo tamara
root@debian:~# groups tamara
```

Se connecter à la machine virtuelle depuis le PC hôte avec la commande suivante: *ssh utilisateur@adresse_ip_debian* et entrer le mot de passe. Pour connaître l'adresse IP, faire "ifconfig" sur Debian

```
U:\>ssh tamara@192.168.209.70
tamara@192.168.209.70's password:
```

Mettre à jour la liste des paquets disponibles et les paquets déjà installés

```
tamara@debian:~$ sudo apt update && sudo apt upgrade -y
```



avec la commande `sudo apt update && sudo apt upgrade -y`

Installer le serveur Apache avec la commande `sudo apt install apache2 -y` et vérifier le statut avec `sudo systemctl status apache2`

```
tamara@debian:~$ sudo apt install apache2 -y
```

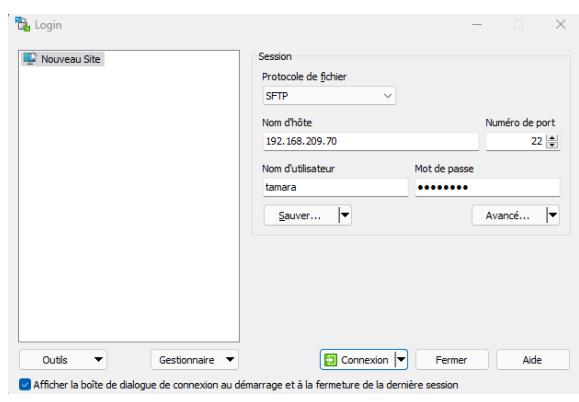
```
apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since ven 2024-11-04 15:06:49 CET; 43s ago
     Docs: https://httpd.apache.org/docs/2.4/
Main PID: 28463 (apache2)
Tasks: 88 (limit: 2397)
Memory: 39ms
CPU: 39ms
CGroup: /system.slice/apache2.service
        └─28463 /usr/sbin/apache2 -k start
          ├─28465 /usr/sbin/apache2 -k start
          ├─28466 /usr/sbin/apache2 -k start
          └─28466 /usr/sbin/apache2 -k start

dec 04 15:06:49 debian systemd[1]: Starting The Apache HTTP Server
dec 04 15:06:49 debian apachectl[28462]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, using 192.168.209.70 for ServerName
dec 04 15:06:49 debian systemd[1]: Started The Apache HTTP Server.
```

4.3. Transférer des fichiers du PC hôte au serveur web

Pour pouvoir transférer des fichiers du PC hôte au serveur web, il faut passer par un client. Dans notre cas, nous utiliserons WinSCP déjà installé. Voici les étapes à suivre pour ce transfert:

Entrer les informations concernant le serveur web et se connecter





Trouver les fichiers à transférer dans le panneau de gauche qui représente le PC hôte

C:\Users\cretard.tamara\			
Nom	Taille	Type	Date de modification
templateengine		Dossier de fichiers	21/06/2022 09:41:04
VirtualBox		Dossier de fichiers	21/11/2024 17:00:46
vscode		Dossier de fichiers	30/09/2024 14:57:07
Cisco Packet Tracer 6...		Dossier de fichiers	21/06/2022 09:41:25
Cisco Packet Tracer 8...		Dossier de fichiers	21/06/2022 09:41:25
Cisco Packet Tracer 8...		Dossier de fichiers	02/12/2024 10:08:48
Contacts		Dossier de fichiers	26/09/2024 10:12:06
Desktop		Dossier de fichiers	12/11/2024 09:05:58
Documents		Dossier de fichiers	19/11/2024 16:04:34
Downloads		Dossier de fichiers	03/12/2024 09:10:55
Favorites		Dossier de fichiers	26/09/2024 10:12:06
Links		Dossier de fichiers	26/09/2024 10:12:06
Music		Dossier de fichiers	26/09/2024 10:12:06
OneDrive		Dossier de fichiers	26/09/2024 10:13:27
Pictures		Dossier de fichiers	19/11/2024 14:34:17
Postman		Dossier de fichiers	21/06/2022 09:41:25
Saved Games		Dossier de fichiers	26/09/2024 10:12:06
Searches		Dossier de fichiers	07/10/2024 09:00:25
seo-conseils-site		Dossier de fichiers	04/12/2024 15:38:30
source		Dossier de fichiers	21/06/2022 09:41:25
Videos		Dossier de fichiers	15/10/2024 14:13:09
VirtualBox		Dossier de fichiers	14/11/2024 11:44:40
packettracer	1 KB	Fichier PACKETTR...	02/12/2024 11:08:35

Dans le panneau de droite, naviguer vers l'emplacement où Apache héberge les fichiers web: /var/www/html

/var/www/html/				
Nom	Taille	Date de modification	Droits	Proprié...
..	04/12/2024 15:06:46	11 KB	rw-r--r--	root root
index.html	04/12/2024 15:06:46			

Glisser-déposer les fichiers ou dossiers du panneau de gauche (PC) vers le panneau de droite (serveur)

Un message code d'erreur 3 Permission Denied peut s'afficher. L'erreur est due au fait que l'utilisateur ne possède pas les permissions du répertoire dans lequel les fichiers vont être transférés. Pour la régler, voici les étapes à suivre:

Se connecter à la machine virtuelle depuis le terminal du PC hôte	ssh tamara@192.168.209.70 tamara@192.168.209.70's password:
Vérifier qui est le propriétaire du répertoire avec ls -ld /var/www/html . On observe que le propriétaire est <i>root</i> et non <i>tamara</i>	tamara@debian:~\$ ls -ld /var/www/html drwxr-xr-x 2 root root 4096 4 déc. 15:06 /var/www/html
Pour attribuer les permissions à l'utilisateur souhaité, entrer la commande suivante: sudo chown -R utilisateur:utilisateur /var/www/html	tamara@debian:~\$ sudo chown -R tamara:tamara /var/www/html
On peut denouveau vérifier qui est le propriétaire du répertoire avec ls -ld /var/www/html . Le propriétaire est maintenant <i>tamara</i>	tamara@debian:~\$ ls -ld /var/www/html drwxr-xr-x 2 tamara tamara 4096 4 déc. 15:06 /var/www/html

Tamara Crétard Pierre-Louis Debuyschere Alan Imbault	20.11.2024	
---------------------------------------------------------------	------------	-------------------------------------------------------------------------------------

Il est maintenant possible de “glisser-déposer” les fichiers ou dossiers du panneau de gauche (PC) vers le panneau de droite (serveur):

/var/www/html/					
Nom	Taille	Date de modification	Droits	Proprié...	
..		04/12/2024 15:06:46	rwxr-xr-x	root	
seo-conseils-site		04/12/2024 16:20:18	rwxr-xr-x	tamara	
index.html	11 KB	04/12/2024 15:06:46	rw-r--r--	tamara	

4.4. Activer un firewall sur le serveur web

Pour sécuriser le serveur web, il faut installer un Firewall. Nous installerons un Firewall UFW qui permettra de bloquer des requêtes qui n'ont pas été autorisées. Pour ce faire, voici les étapes à suivre:

Se connecter à la machine virtuelle depuis le terminal du PC hôte	<pre>ssh tamara@192.168.209.70 tamara@192.168.209.70's password:</pre>
Mettre à jour le système avec la commande <code>sudo apt update && sudo apt upgrade -y</code>	<pre>tamara@debian:~\$ sudo apt update && sudo apt upgrade -y</pre>
Installer UFW avec la commande <code>sudo apt install ufw</code>	<pre>tamara@debian:~\$ sudo apt install ufw</pre>
Ajouter les règles suivantes: <code>sudo ufw allow ssh</code> , <code>sudo ufw allow https</code> , <code>sudo ufw allow 22</code>	<pre>tamara@debian:~\$ sudo ufw allow ssh Rules updated Rules updated (v6) tamara@debian:~\$ sudo ufw allow 22 Rules updated Rules updated (v6) tamara@debian:~\$ sudo ufw allow https Rules updated Rules updated (v6)</pre>
Activer UFW avec la commande suivante: <code>sudo ufw enable</code>	<pre>tamara@debian:~\$ sudo ufw enable Command may disrupt existing ssh connections. Proceed with operation (y n)? y Firewall is active and enabled on system startup</pre>



Vérifier que tout fonctionne correctement avec *sudo ufw status verbose*

```
tamara@debian:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         --          --
22/tcp                     ALLOW IN   Anywhere
22                         ALLOW IN   Anywhere
443                        ALLOW IN   Anywhere
22/tcp (v6)                 ALLOW IN   Anywhere (v6)
22 (v6)                    ALLOW IN   Anywhere (v6)
443 (v6)                   ALLOW IN   Anywhere (v6)
```

4.5. Passer le site en HTTPS avec un certificat auto-signé

Il est nécessaire de sécuriser les échanges entre le serveur et le client ainsi que d'authentifier le site web. Pour ce faire, il faut passer le site en HTTPS avec un certificat auto-signé. Voici les étapes à suivre:

Se connecter à la machine virtuelle depuis le terminal du PC hôte	ssh tamara@192.168.209.70 tamara@192.168.209.70's password:
Créer un répertoire pour stocker les certificats avec <i>sudo mkdir /etc/ssl/self-signed</i>	tamara@debian:~\$ sudo mkdir /etc/ssl/self-signed [sudo] Mot de passe de tamara :
Générer une clé privée avec <i>sudo openssl genrsa -out /etc/ssl/self-signed/selfsigned.key 2048</i>	tamara@debian:~\$ sudo openssl genrsa -out /etc/ssl/self-signed/selfsigned.key 2048 Generating RSA private key, 2048 bit long modulus (2 primes)+++++ e is 65537 (0x100001)
Créer une demande de certificat (CSR) et un certificat auto-signé avec la commande <i>sudo openssl req -x509 -new -nodes -key /etc/ssl/self-signed/selfsigned.key -sha256 -days 365 -out /etc/ssl/self-signed/selfsigned.crt</i>	tamara@debian:~\$ sudo openssl req -x509 -new -nodes -key /etc/ssl/self-signed/selfsigned.key \ -sha256 -days 365 -out /etc/ssl/self-signed/selfsigned.crt [sudo] Mot de passe de tamara : You are about to be asked to enter information that will be incorporated into your certificate request: What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. ----- Country Name (2 letter code) [AU]:FR State or Province Name (F.e. name) [Some-State]:Auvergne-Rhône-Alpes Locality Name (e.g. city) []:Moulins Organization Name (e.g. company) [Internet Widgits Pty Ltd]:SIOI Organization Unit Name (e.g. section) []:SIOI Common Name (e.g. server FQDN or YOUR name) []:192.168.209.70 Email Address []:tamara.cretard@lycee-faure.fr
Activer le module SSL avec <i>sudo a2enmod ssl</i> et redémarrer Apache avec la commande <i>sudo systemctl restart apache2</i>	tamara@debian:~\$ sudo a2enmod ssl Enabling module mod_ssl. Module mod_ssl already enabled Considering dependency mime for ssl: Module mime already enabled Considering dependency socache_shmcb for ssl: Enabling module socache_shmcb. Module socache_shmcb already enabled Enabling module ssl. Module ssl already enabled See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates. To activate the new configuration, you need to run: systemctl restart apache2
Lister les fichiers avec <i>ls -l /etc/apache2/sites-available/</i> s'il n'y a pas notre site, créer le fichier de configuration avec <i>sudo nano /etc/apache2/sites-available/seo-conseils-site.conf</i>	tamara@debian:~\$ ls -l /etc/apache2/sites-available/ total 12 -rw-r--r-- 1 root root 1496 4 déc. 17:28 000-default.conf -rw-r--r-- 1 root root 6338 4 oct. 17:21 default-ssl.conf tamara@debian:~\$ sudo nano /etc/apache2/sites-available/seo-conseils-site.conf



Modifier le contenu du fichier:

```
sudo nano
/etc/apache2/sites-available/seo-conseils-site.conf
```

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName tamaral.sio.local
    DocumentRoot /var/www/html/seo-conseils-site
    DirectoryIndex seo-conseils.html

    <Directory /var/www/html/seo-conseils-site>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName tamaral.sio.local
    DocumentRoot /var/www/html/seo-conseils-site
    DirectoryIndex seo-conseils.html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    <Directory /var/www/seo-conseils-site>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    SSLEngine on
    SSLCertificateFile /etc/ssl/self-signed/selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/self-signed/selfsigned.key
</VirtualHost>
```

Activer le site avec sudo a2ensite
seo-conseils-site.conf et redémarrer
 Apache avec
sudo systemctl reload apache2

```
tamara@debian:~$ sudo a2ensite seo-conseils-site.conf
Enabling site seo-conseils-site.
To activate the new configuration, you need to run:
    systemctl reload apache2
tamara@debian:~$ sudo systemctl reload apache2
```

4.6. Installer PHP sur le serveur

Mettre à jour le système avec *sudo apt update && sudo apt upgrade -y*

```
tamara@debian:~$ sudo apt update && sudo apt upgrade -y
```

Installer PHP et les extensions avec: *sudo apt install php libapache2-mod-php php-mysql -y*

php : le langage PHP
libapache2-mod-php : permet à Apache d'interpréter les fichiers PHP
php-mysql : extension pour que PHP interagisse avec MariaDB

```
tamara@debian:~$ sudo apt install php libapache2-mod-php php-mysql -y
```

Tamara Crétard Pierre-Louis Debuyschere Alan Imbault	20.11.2024	
---------------------------------------------------------------	------------	-------------------------------------------------------------------------------------

Vérifier l'installation avec <code>php -v</code>	<pre>tamara@debian:~\$ php -v PHP 7.4.33 (cli) (built: Dec 7 2024 22:44:42) (NTS) Copyright (c) The PHP Group Zend Engine v3.4.0, Copyright (c) Zend Technologies with Zend OPcache v7.4.33, Copyright (c), by Zend Technologies</pre>
Vérifier que le module est bien installé avec <code>dpkg -l grep libapache2-mod-php</code>	<pre>tamara@debian:~\$ dpkg -l grep libapache2-mod-php ii libapache2-mod-php 7.4.33-1+deb11u7 all server-side, HTML-embedded scr ii libapache2-mod-php7.4 7.4.33-1+deb11u7 amd64 server-side, HTML-embedded scr</pre>
Vérifier les modules disponibles: <code>ls /usr/lib/apache2/modules grep php</code>	<pre>tamara@debian:~\$ ls /usr/lib/apache2/modules grep php libphp7.4.so</pre>
Activer le module voulu avec <code>sudo a2enmod php7.4</code> et redémarrer Apache <code>sudo systemctl restart apache2</code>	<pre>tamara@debian:~\$ sudo a2enmod php7.4 Considering dependency mpm_prefork for php7.4: Considering conflict mpm_event for mpm_prefork: Considering conflict mpm_worker for mpm_prefork: Module mpm_prefork already enabled Considering conflict php5 for php7.4: Module php7.4 already enabled</pre>
Modifier le fichier de configuration Apache en ajoutant un <code>DirectoryIndex index.php</code> et redémarrer denouveau Apache	<pre><VirtualHost *:80> ServerAdmin webmaster@localhost ServerName tamaral.sio.local DocumentRoot /var/www/html/seo-conseils-site DirectoryIndex seo-conseils.html index.php <Directory /var/www/html/seo-conseils-site> Options Indexes FollowSymLinks AllowOverride All Require all granted </Directory> ErrorLog \${APACHE_LOG_DIR}/error.log CustomLog \${APACHE_LOG_DIR}/access.log combined </VirtualHost> <VirtualHost *:443> ServerAdmin webmaster@localhost ServerName tamaral.sio.local DocumentRoot /var/www/html/seo-conseils-site DirectoryIndex seo-conseils.html index.php ErrorLog \${APACHE_LOG_DIR}/error.log CustomLog \${APACHE_LOG_DIR}/access.log combined <Directory /var/www/seo-conseils-site> Options Indexes FollowSymLinks AllowOverride All Require all granted </Directory> SSLEngine on SSLCertificateFile /etc/ssl/self-signed/selfsigned.crt SSLCertificateKeyFile /etc/ssl/self-signed/selfsigned.key </VirtualHost></pre>
Tester PHP en créant un fichier de test dans le répertoire par défaut d'Apache: <code>sudo nano /var/www/html/seo-conseils-site/index.php</code> et en ajoutant: <code><?php echo "PHP fonctionne !"; ?></code>	<pre>sudo nano /var/www/html/info.php <?php echo "PHP fonctionne !"; ?></pre> 

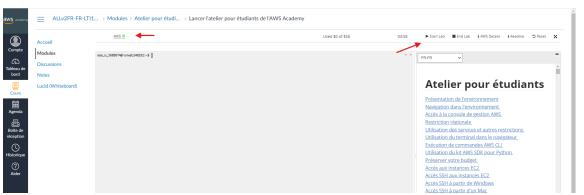
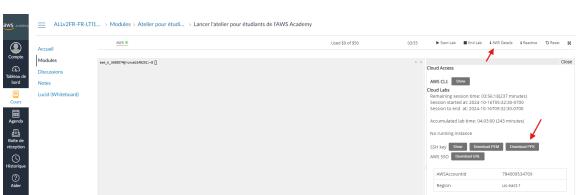


devrait y avoir une page d'informations PHP

4.7. Installer MariaDB sur le serveur

Installer MariaDB avec <code>sudo apt install mariadb-server -y</code>	<code>sudo apt install mariadb-server -y</code>
Vérifier que MariaDB est actif avec <code>sudo systemctl status mariadb</code>	<pre>[root@el7 ~]# sudo systemctl status mariadb mariadb.service - MariaDB 10.5.26 database server Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled) Active: active (running) since Wed 2024-12-11 14:28:32 CET; 35min ago Docs: man:/usr/share/man/man8/mariadb.8.gz https://mariadb.org/db/en/library/systemd/ Main PID: 11703 (mariadbd) Tasks: 9 (limit: 15239) Memory: 75.2M CPU: 539ms CGroup: /system.slice/mariadb.service └─11703 /usr/sbin/mariadbd Dec 11 14:28:32 el7 mariadbd[11703]: Version: '10.5.26-MariaDB-1:10.5.26+maria~Debian10~' Dec 11 14:28:32 el7 mariadbd[11703]: socket: '/run/mysqld/mysqld.sock' port: 3306 Dec 11 14:28:32 el7 mariadbd[11703]: Started MariaDB 10.5.26 database server. Dec 11 14:28:33 el7 [mysqld]: Upgrading MySQL tables if necessary. Dec 11 14:28:33 el7 [mysqld]: Looking for 'mariadb' as /usr/bin/mariadb Dec 11 14:28:33 el7 [mysqld]: Looking for 'mariadb-check' as /usr/bin/mariadb-check Dec 11 14:28:33 el7 [mysqld]: This installation of MariaDB is already upgraded to 10.5.26-Mari Dec 11 14:28:33 el7 [mysqld]: There is no need to run mysql_upgrade again for 10.5.26-MariaDB. Dec 11 14:28:33 el7 [mysqld]: If you still want to run mysql_upgrade Dec 11 14:28:33 el7 [mysqld]: Checking for incorrect root access Dec 11 14:28:33 el7 [mysqld]: Triggering myisam-recover for all MyISAM tables and aria-recove Lines 1-29/29 (END)</pre>

4.8. Mettre en place un serveur Linux Debian dans AWS

Aller sur le site awsacademy, dans “cours” puis “lancer l’atelier pour étudiants de l’AWS Academy”. Cliquer sur le bouton “Start Lab” et attendre que le bouton AWS devienne vert.	
Aller dans “AWS Details” et télécharger le fichier PPK	
Aller dans la console AWS, puis rechercher le service AWS et cliquer dessus	



Dans la fenêtre qui s'ouvre, cliquer sur "lancer une instance".

Donner un nom à l'instance et sélectionner Debian.

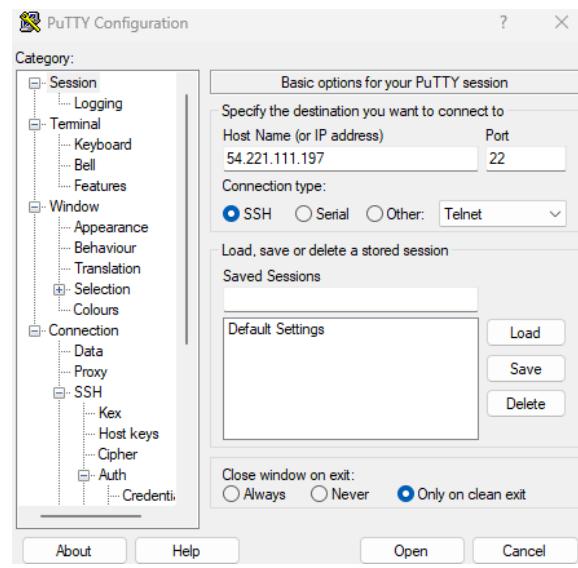
Sélectionnez le nom de la paire de clés "vokey". Cliquez ensuite sur "lancer l'instance".

Une fois le lancement de l'instance réussi, cliquez sur "Afficher toutes les instances" puis, cliquez sur l'ID de votre instance.

Notez l'adresse IP publique de votre machine ainsi que son nom DNS public.



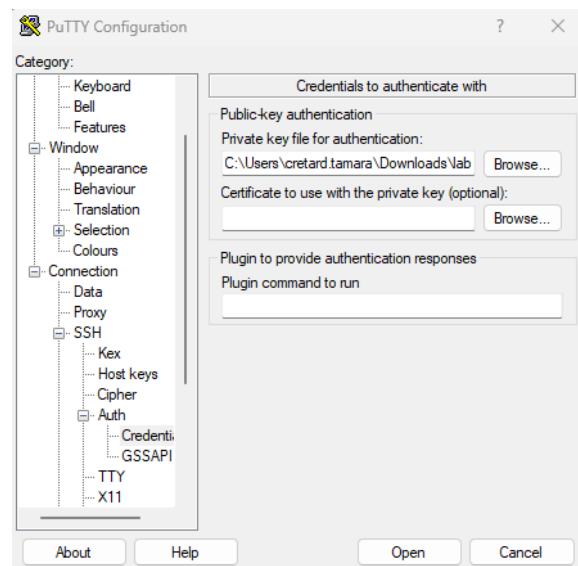
Sur le PC, lancer l'application Putty.
 Dans la zone « Host Name (or IP address),
 entrer l'adresse IP publique



Dans le volet **Catégorie**, développer **Connexion**, développer **SSH**, puis développer **Auth** et choisir **Credentials**. Suivre les instructions suivantes :

1. Choisir **Parcourir**.
2. Sélectionner le fichier .ppk que téléchargé précédemment

Cliquer sur Open pour se connecter à la machine Debian



Dans la fenêtre qui s'ouvre cliquer sur "accept" et entrer admin

Mettre à jour le système avec `sudo apt update && sudo apt upgrade -y`

```
admin@ip-172-31-22-107:~$ sudo apt update && sudo apt upgrade -y
```

Installer Apache avec `sudo apt install apache2 -y`

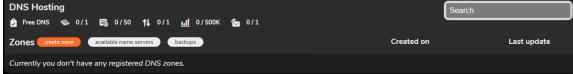
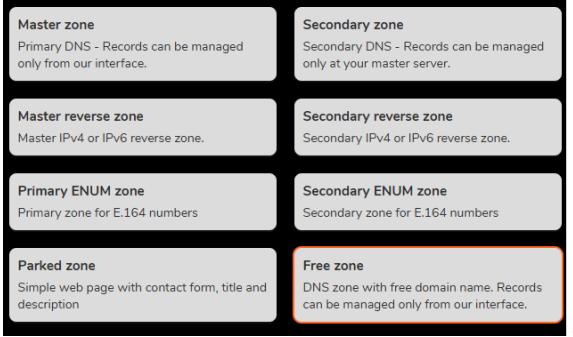
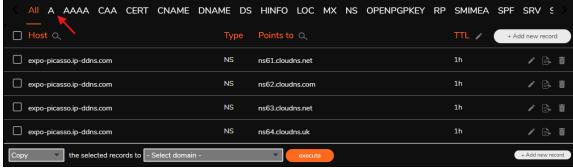
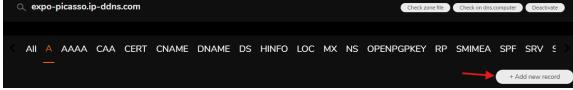
```
admin@ip-172-31-22-107:~$ sudo apt install apache2 -y
```

Utilisez la commande `systemctl` pour configurer le serveur Web Apache afin qu'il soit lancé à chaque démarrage système.

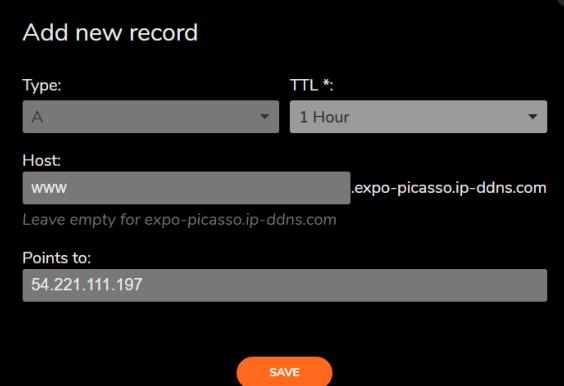
`sudo systemctl enable apache2`

Tamara Crétard Pierre-Louis Debuyschere Alan Imbault	20.11.2024	
---------------------------------------------------------------	------------	-------------------------------------------------------------------------------------

4.9. Créer un nom de domaine DNS

Aller sur https://www.cloudns.net/ , sélectionner “Sign-up for free” et créer un compte	
Cliquer sur “Create Zone” dans DNS Hosting	
Sélectionner “Free Zone”	
Entrer le nom de domaine	
Aller dans A → L'enregistrement "A" associe un nom d'hôte à une adresse IP	
Cliquer sur “Add new record”	

Tamara Crétard Pierre-Louis Debuyschere Alan Imbault	20.11.2024	
---------------------------------------------------------------	------------	-------------------------------------------------------------------------------------

Entrer le Host ainsi que l'adresse IP du serveur	
--------------------------------------------------	------------------------------------------------------------------------------------

4.10. Configurer Apache du serveur AWS pour utiliser le nom de domaine

Créer le fichier de configuration avec <i>sudo nano /etc/apache2/sites-available/expo-picasso.conf</i>	<pre>admin@ip-172-31-22-107:~\$ sudo nano /etc/apache2/sites-available/expo-picasso.conf</pre>
Modifier le fichier pour ajouter le nom de serveur et la page index	<pre><VirtualHost *:80> ServerAdmin webmaster@localhost ServerName www.expo-picasso.ip-ddns.com DocumentRoot /var/www/html/expo-picasso DirectoryIndex expo-picasso.html <Directory /var/www/html/expo-picasso> Options Indexes FollowSymLinks AllowOverride All Require all granted </Directory> ErrorLog \${APACHE_LOG_DIR}/error.log CustomLog \${APACHE_LOG_DIR}/access.log combined </VirtualHost> <VirtualHost *:443> ServerAdmin webmaster@localhost ServerName www.expo-picasso.ip-ddns.com DocumentRoot /var/www/html/expo-picasso DirectoryIndex expo-picasso.html ErrorLog \${APACHE_LOG_DIR}/error.log CustomLog \${APACHE_LOG_DIR}/access.log combined <Directory /var/www/expo-picasso> Options Indexes FollowSymLinks AllowOverride All Require all granted </Directory> </VirtualHost></pre>
Activer le site avec <i>sudo a2ensite expo-picasso.conf</i> et redémarrer Apache	<pre>admin@ip-172-31-22-107:~\$ sudo a2ensite expo-picasso.conf</pre>

Tamara Crétard Pierre-Louis Debuyschere Alan Imbault	20.11.2024	
---------------------------------------------------------------	------------	-------------------------------------------------------------------------------------

avec
sudo systemctl reload apache2

4.11. Installer Certbot pour générer automatiquement un certificat SSL

Installer Snapd (Certbot est généralement installé via Snapd): <i>sudo apt install snapd</i>	<pre>admin@ip-172-31-22-107:~\$ sudo apt install snapd</pre>
Activer Snapd avec <i>sudo systemctl enable --now snapd.socket</i>	<pre>admin@ip-172-31-22-107:~\$ sudo systemctl enable --now snapd.socket</pre>
Installer Certbot via Snapd avec: <i>sudo snap install --classic certbot</i>	<pre>admin@ip-172-31-22-107:~\$ sudo snap install --classic certbot</pre>
Faire en sorte que la commande certbot peut être utilisée: <i>sudo ln -s /snap/bin/certbot /usr/bin/certbot</i>	<pre>admin@ip-172-31-22-107:~\$ sudo ln -s /snap/bin/certbot /usr/bin/certbot</pre>
Créer un fichier conf: <i>sudo nano /etc/apache2/sites-enabled/expo-picasso.conf</i>	<pre>admin@ip-172-31-22-107:~\$ sudo nano /etc/apache2/sites-enabled/expo-picasso.conf</pre>
Obtenir un certificat automatiquement avec certbot: <i>sudo certbot --apache</i>	<pre>admin@ip-172-31-22-107:~\$ sudo certbot --apache Saving debug log to /var/log/letsencrypt/letsencrypt.log Which names would you like to activate HTTPS for? * (automatically selecting either all domains, or all domains in a VirtualHost/server block) : www.expo-picasso.ip-ddns.com : expo-picasso.ip-ddns.com Select the appropriate numbers separated by commas and/or spaces, or leave input blank to select all options shown (inner '0' to cancel): 1 Press Enter to select all options shown (inner '0' to cancel): 1 Press Enter to select all options shown (inner '0' to cancel): 1 You have an existing certificate that has exactly the same domains or certificate name you requested and isn't close to expiry. (soft) /etc/letsencrypt/renewal/www.expo-picasso.ip-ddns.com.conf) What would you like to do? * Attempt to reinstall this existing certificate * Honor a replace the certificate (may be subject to CA rate limits) * Renew the certificate Select the appropriate number [1-2] then [enter] (press 'l' to cancel): 2 Renewing existing certificate /etc/letsencrypt/renewal/www.expo-picasso.ip-ddns.com.conf Successfully received certificate. certificate is saved at /etc/letsencrypt/live/www.expo-picasso.ip-ddns.com/fullchain.pem key is saved at: /etc/letsencrypt/live/www.expo-picasso.ip-ddns.com/privkey.pem This certificate expires on 2018-01-18. These files will be automatically renewed when the certificate renames. certbot has set up a scheduled task to automatically renew this certificate in the background. Deploying certificate Successfully deployed certificate for www.expo-picasso.ip-ddns.com to /etc/apache2/sites-enabled/seo-conseils-site.conf Your existing certificate has been successfully renewed, and the new certificate has been installed. If you like Certbot, please consider supporting our work by: * Donating to ISRG / Let's Encrypt: https://letsencrypt.org/donate * Donating to EFF: https://eff.org/donate-is</pre>



Modifier le fichier conf: *sudo nano /etc/apache2/sites-enabled/expo-picasso.conf*

```
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName www.expo-picasso.ip-ddns.com
    DocumentRoot /var/www/html/seo-conseils-site
    DirectoryIndex seo-conseils.html

    <Directory /var/www/html/seo-conseils-site>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>

<VirtualHost *:443>
    ServerAdmin webmaster@localhost
    ServerName www.expo-picasso.ip-ddns.com
    DocumentRoot /var/www/html/seo-conseils-site
    DirectoryIndex seo-conseils.html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    SSLEngine on
    SSLCertificateFile /etc/letsencrypt/live/www.expo-picasso.ip-ddns.com/fullchain.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/www.expo-picasso.ip-ddns.com/privkey.pem

    <Directory /var/www/html/seo-conseils-site>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>
</VirtualHost>
```

Redémarrer Apache: *sudo systemctl restart apache2*

```
admin@ip-172-31-22-107:~$ sudo systemctl restart apache2
```