Formation OpenClassrooms
Administrateur Systèmes, Réseaux Et Sécurité

Soutenance Projet-04

Stéphane Perfetti

14/05/2024

BeeSafe

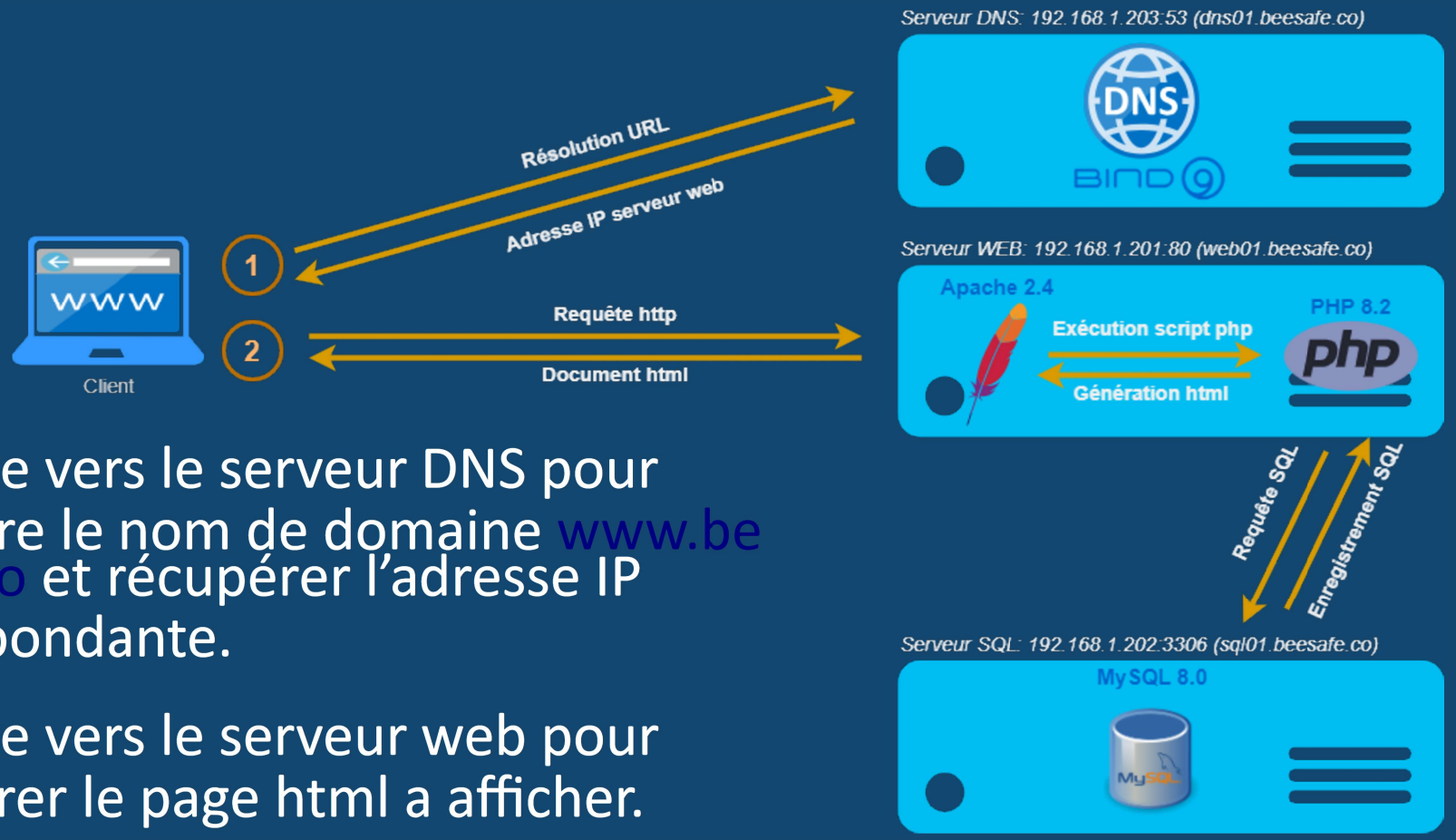
Projet 04 - Déployez une architecture n-tiers pour une PME

- Scénario :
  - La société BeeSafe, startup d'assurance souhaite déployer un nouveau site web.
  - En charge de la mise en place de l'architecture 3-tiers devant héberger les services du site web.
- Plan d'action :
  - Schéma d'architecture 3-tiers
  - Installation et configuration des 3 services :
    - DNS
    - Serveur web
    - Serveur base de donnée

Domaine et Architecture n-tiers

- Domaine: beesafe.co
- Architecture 3-tiers, basée sur 3 machines virtuelles :
  - Serveur DNS (hostname: dns01) :
    - Debian 12
    - Bind9
  - Serveur web (hostname: web01) :
    - Debian 12
    - Apache2
    - PHP 8
  - Serveur sql (hostname: sql01) :
    - Debian 12
    - MySQL 8

Schéma architecture



1. Requête vers le serveur DNS pour résoudre le nom de domaine www.beesafe.co et récupérer l'adresse IP correspondante.
2. Requête vers le serveur web pour récupérer le page html a afficher.

Serveur DNS : Configuration

- Serveur :
  - FQDN: dns01.beesafe.co ; IP: 192.168.1.203
  - Installation Bind9

- Bind9 :
  - Paramétrage des options, fichier /etc/bind/named.conf.options :
    - Déclaration de forwarders pour résoudre les requêtes des zones non gérés par le DNS local.

```
root@dns01:/etc/bind# cat named.conf.options
options {
        directory "/var/cache/bind";

        forwarders {
                8.8.8.8;
        };

        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

  - Déclaration des zones DNS beesafe.co directe et inverse sous /etc/bind/named.conf.local :
    - db.beesafe.co.direct
    - db.beesafe.co.reverse

```
root@dns01:/etc/bind# cat named.conf.local
zone "beesafe.co" {
        type master;
        file "/etc/bind/db.beesafe.co.direct";
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/db.beesafe.co.reverse";
};
```

Serveur DNS : Configuration

- Bind9 :
  - Création du fichier bd.beesafe.co.direct :
    - Délégation d'autorités du domaine au serveur DNS avec un enregistrement de type SOA.
    - Définition du nom du serveur de nom pour la zone avec un enregistrement de type NS.
    - Définition des hôtes / adresse IP avec des enregistrements de type A.
    - Définition d'alias avec enregistrement de type CNAME

```
root@dns01:/home/debian# cat /etc/bind/db.beesafe.co.direct
$TTL    604800
@       IN      SOA     dns01.beesafe.co. admin.beesafe.co. (
                        202405022       ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dns01.beesafe.co.
dns01   IN      A       192.168.1.203
@       IN      A       192.168.1.201
www     IN      CNAME   @
web01   IN      CNAME   @
sql01   IN      A       192.168.1.202
```

  - Création du fichier bd.beesafe.co.reverse :
    - Délégation d'autorités du domaine au serveur DNS avec un enregistrement de type SOA.
    - Définition du nom du serveur de nom pour la zone avec un enregistrement de type NS.
    - Définition des adresse IP / hôtes avec des enregistrements de type PTR.

```
root@dns01:/home/debian# cat /etc/bind/db.beesafe.co.reverse
$TTL    604800
@       IN      SOA     ns.beesafe.co. admin.beesafe.co. (
                        202405021       ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      dns01.beesafe.co.
203     IN      PTR     dns01.beesafe.co.
201     IN      PTR     www.beesafe.co.
201     IN      PTR     web01.beeasafe.co
202     IN      PTR     sql01.beesafe.co
```

  - Validation des fichiers de configurations :
    - Commande : named-checkconf named.conf.local
    - Commande : named-checkzone beesafe.co db.beesafe.co.direct

```
debian@dns01:/etc/bind$ named-checkzone beesafe.co db.beesafe.co.direct
zone beesafe.co/IN: loaded serial 202405022
OK
```

Serveur DNS : Configuration machines clientes

- Configuration de l'adresse du serveur DNS sur chaque machines du réseau, ainsi que sur le serveur DNS lui même :
  - A partir du serveur DHCP, si existant
  - En local sur chaque machine, pour des tests, car non permanent a partir du fichier /etc/resolv.conf :

```
nameserver 192.168.1.203
nameserver 192.168.1.254
```

  - ★ En local sur chaque machine, de façon permanente, en installant le paquet resolvconf et en précisant le DNS dans le fichier /etc/network/interfaces :

```
# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
  address 192.168.1.201
  netmask 255.255.255.0
  gateway 192.168.1.254
  broadcast 192.168.1.255
  dns-search beesafe.co
  dns-nameservers 192.168.1.203
```

- Test de résolution avec nslookup :

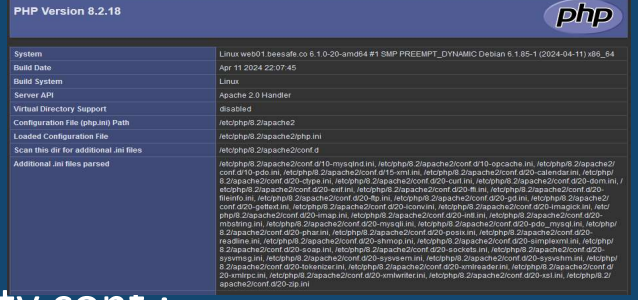
```
debian@sql01:~  $ nslookup web01.beesafe.co
Server:         192.168.1.203
Address:        192.168.1.203#53

web01.beesafe.co        canonical name = beesafe.co.
Name:   beesafe.co
Address: 192.168.1.201
```

Serveur Web : Configuration

- Serveur :
  - FQDN: web01.beesafe.co ; IP: 192.168.1.201
  - Installation :
    - apache2 et du module libapache2-mod-php
    - php8 et de divers modules (php-common, php-cli, php-mysql, …)
- Apache2 :
  - Test Apache et PHP :
    - Création d'un fichier sous /var/www/html/phpinfo.php
    - Affichage de la page web01.beesafe.co/phpinfo.php :

```
debian@web01:/var/www/html  $ cat phpinfo.php
<?php phpinfo() ?>
```



  - Modification du fichier /etc/apache2/conf-available/security.conf :
  - Désactivation du site par défaut :

```
ServerTokens Prod
ServerSignature Off
```

```
debian@web01:/var/www/html  $ sudo a2dissite 000-default.conf
Site 000-default disabled.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

Serveur Web : Configuration

- Apache2 :
  - Création du répertoire /var/www/beesafe et copie des fichiers index.php , vars.php, main.css
  - Modification du fichier /var/www/beesafe/vars.php :
    - Remplacement du nom de variable ‘db’ par ‘dbname’ pour correspondre à la commande de connexion sql du fichier index.php
    - Mise a jour des identifiants de connexion à la base de donnée beesafeDB créé par la suite.

```
debian@web01:~  $ cat /var/www/beesafe/vars.php
<?php
$servername = "sql01";
$username = "beesafe";
$password = "beesafepwd";
$dbname = "beesafeDB";
$port = 3306;
?>
```

  - Création et configuration d'un virtualhost sous /etc/apache2/sites-available/beesafe.conf basé sur 000-default.conf

```
debian@web01:~  $ cat /etc/apache2/sites-available/beesafe.conf
<VirtualHost *:80>
        ServerAdmin webmaster@beesafe.co
        DocumentRoot /var/www/beesafe
        ServerName www.beesafe.co

        <Directory "/var/www/beesafe">
                Options -Indexes
        </Directory>

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

  - Validation de configuration :

```
debian@web01:~  $ sudo apachectl -t
Syntax OK
```

  - Activation du virtualhost :

```
debian@web01:/etc/apache2/sites-available  $ sudo a2ensite beesafe.conf
Enabling site beesafe.
To activate the new configuration, you need to run:
  systemctl reload apache2
```

  - Rechargement d’apache :

```
debian@web01:~  $ sudo systemctl reload apache2.service
```

Serveur SQL : Configuration

- Serveur :
  - FQDN: sql01.beesafe.co ; IP: 192.168.1.202
  - Installation du dépôt mysql de APT, non présent par défaut sur Debian 12
  - Installation de mysql-server
  - Configuration global de MySQL avec mysql_secure_installation

- MySQL :
  - ★ Création de la base de donnée beesafeDB a partir du script beesafe_init.sql :

```
/* beesafeDB_init.sql :
Script sql, création et configuration de la base de donnée pour www.beesafe.co.
*/
CREATE DATABASE beesafeDB;
CREATE USER 'beesafe'@'web01' IDENTIFIED BY 'beesafepwd';
GRANT SELECT ON beesafeDB.* to 'beesafe'@'web01';
FLUSH PRIVILEGES;
USE beesafeDB;
-- Creation tables et enregistrements a partir des fichiers sources fournits
Source schema.sql;
Source data.sql;
```

Serveur SQL : Configuration

- Mysql :
  - beesafeDB vérification de la structure :

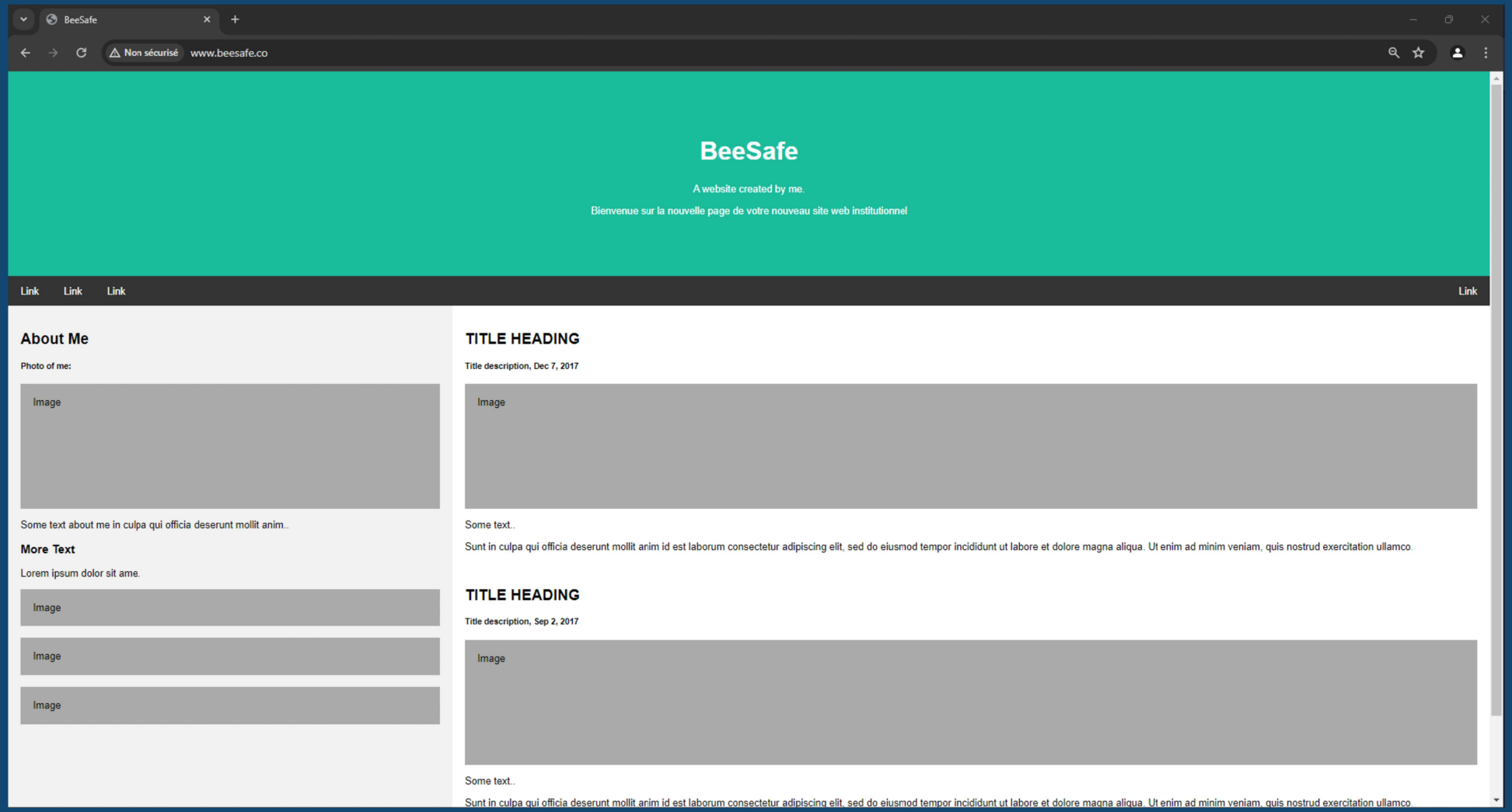
```
mysql> use beesafeDB;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show grants for 'beesafe'@'web01';
+---------------------------------------------------+
| Grants for beesafe@web01                          |
+---------------------------------------------------+
| GRANT USAGE ON *.* TO `beesafe`@`web01`           |
| GRANT SELECT ON `beesafeDB`.* TO `beesafe`@`web01` |
+---------------------------------------------------+
2 rows in set (0,00 sec)

mysql> show tables;
+--------------------+
| Tables_in_beesafeDB |
+--------------------+
| pages              |
+--------------------+
1 row in set (0,00 sec)

mysql> describe pages;
+---------+--------------+------+-----+---------+----------------+
| Field   | Type         | Null | Key | Default | Extra          |
+---------+--------------+------+-----+---------+----------------+
| id      | int unsigned | NO   | PRI | NULL    | auto_increment |
| title   | varchar(30)  | YES  | MUL | NULL    |                |
| content | text         | YES  |     | NULL    |                |
+---------+--------------+------+-----+---------+----------------+
3 rows in set (0,00 sec)
```

Test connexion a www.beesafe.co :

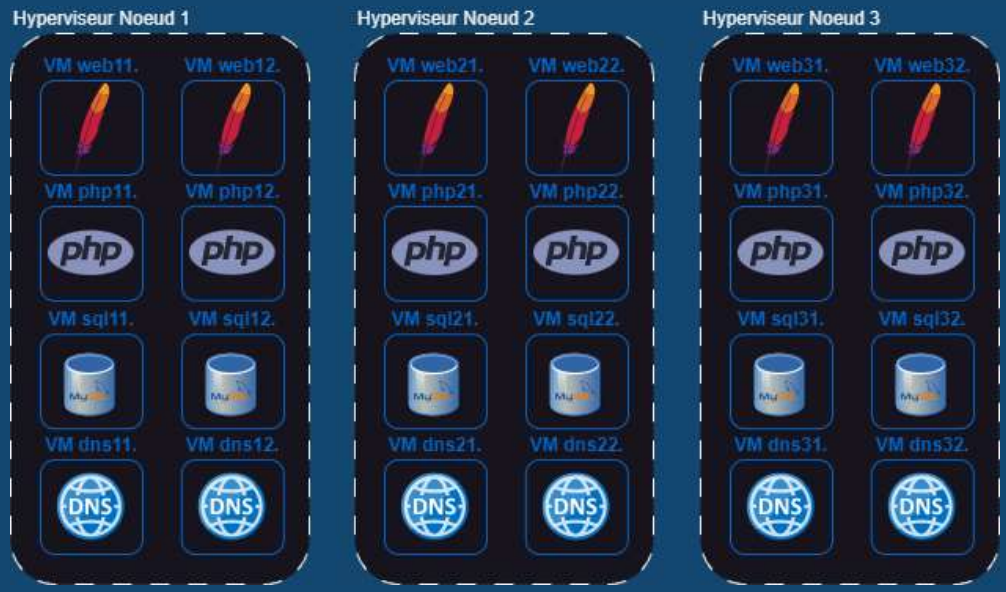


Voies d’améliorations :

- Machine virtuelle dédié a PHP avec PHP-FPM, pour la performance.

- Redondance des machines virtuelles Apache2, PHP, Mysql, DNS (serveur maître et esclave) pour la maintenance.

- Ajouter des serveurs hyperviseur de type 1, avec trois nœud pour une architecture haute disponibilité.



Questions / Réponses