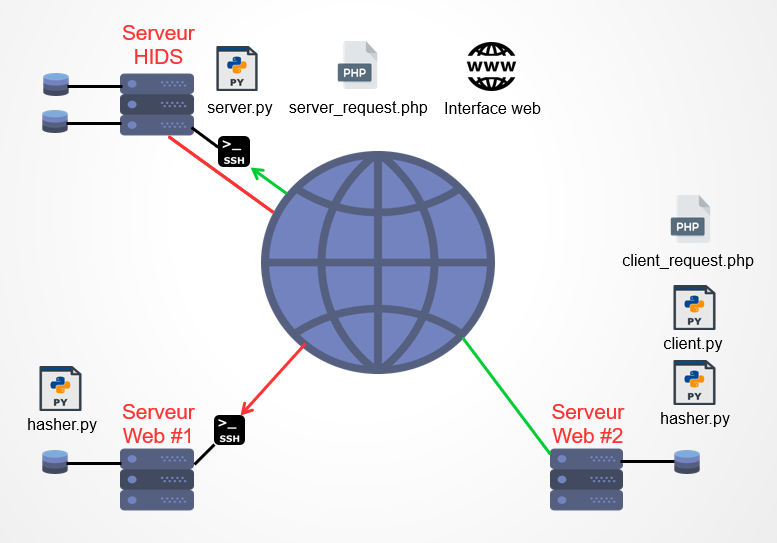
Présentation

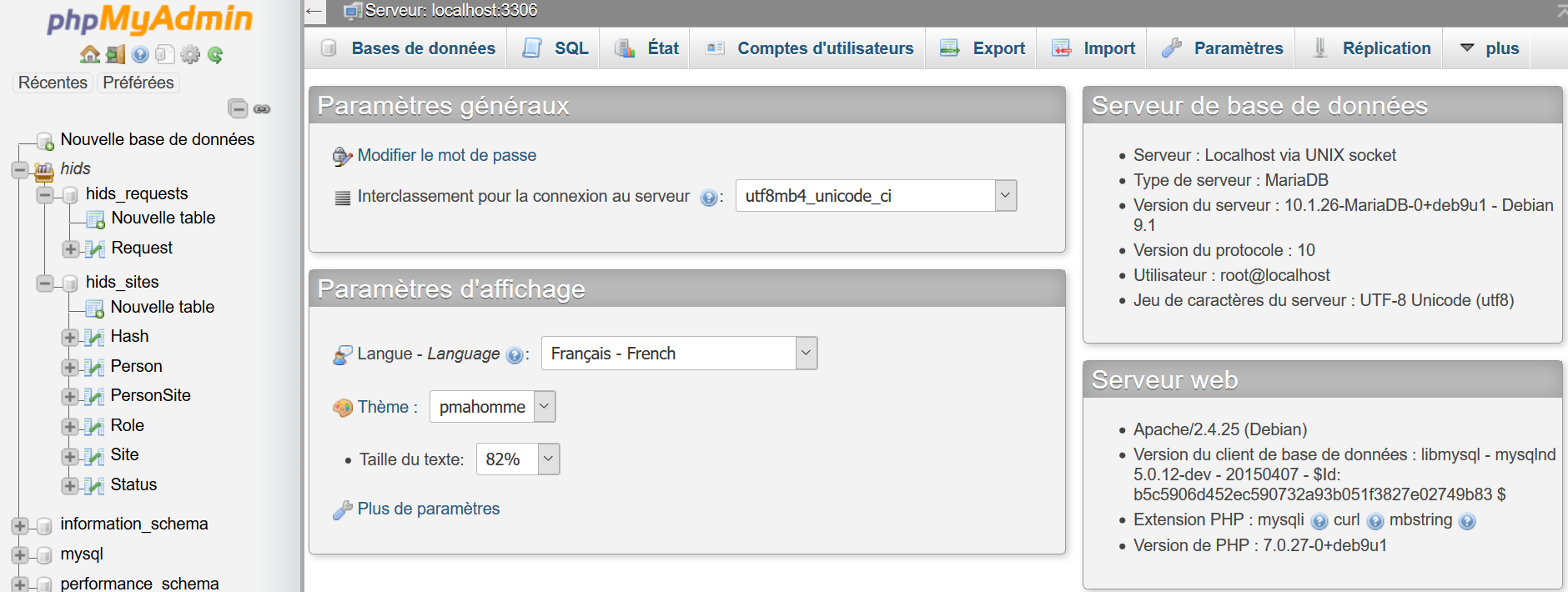
## L’infrastructure



## Serveur HIDS (SECU-HIDS)

Tous les serveurs Web sont partitionné en 1 lvm :

Le serveur HIDS est définit par ses deux bases de données.

* hids\_requests  : sert pour les requêtes entres les serveurs web et l’HIDS.
* Hids\_sites : sert pour les empreintes des sites.
* OS : Debian 9
* Serveur Web : Apache2 (HTTPS)
* Serveur SSL 

## Serveur WEB #1 (SECU-WEB1)

Le serveur SECU-WEB1 se compose d’un serveur Apache2 contenant un site Wordpress et un serveur SSH.

Défini par :

* Serveur Apache2
* Site Wordpress
* Serveur SSH : Connexion avec l’HIDS en SSH

## Serveur WEB #2 (SECU-WEB2)

Le serveur SECU-WEB2 se compose d’un serveur Apache2 contenant un site Wordpress mais ne disposant pas de Serveur SSH. La connexion entre SECU-HIDS et SECU-WEB2 s’effectuera avec le script server\_request.php

Défini par :

* Serveur Apache2
* Site Wordpress
* Connexion avec l’HIDS avec le script server\_request.php

## Scripts

### SERVER.PY

Ce script est sur SECU-HIDS, il permet de se connecter aux serveurs SECU-WEB1 et SECU-WEB2 et de copier des fichiers.

SERVER.PY se lance au démarrage du serveur et fonctionne en arrière-plan. Il consulte et analyse la base de données des requêtes et des sites. Il peut également consulter et modifier la base de données des empreintes.

Les requêtes sont envoyées via le CLIENT\_REQUEST.PHP

### SERVER\_REQUEST.PHP



### HASHER.PY

### CLIENT.PY

### CLIENT\_REQUEST.PHP