

Mise en place d'un Intranet pour chaque Filiale

En tant que administrateur Système, installation d'un serveur LAMP et de Wordpress

Authors

Roblot Jean-Philippe - jroblot.simplon@proton.me

Moreau Ronan - rmoreau.simplon@proton.me

Version

15/02/2024 - V1R0

Releases

Debian 11 WordPress

Powered by <https://shields.io>

Contexte

Il est nécessaire de pouvoir communiquer a tout le monde au sein de la filiale afin de partager les informations importantes de l'entreprise.

Les e-mails ne permettant pas d'avoir un historique pertinent, il a été choisit de procéder a la mise en place d'un Intranet.

Questions

- Quelles sont les étapes principales pour installer un serveur LAMP sur un système Linux ?
Pour installer un serveur LAMP (Linux, Apache, MySQL, PHP) sur un système Linux, vous pouvez suivre les étapes suivantes :
Mise à jour du système :

```
apt-get update
```

Installation d'Apache :

```
apt-get install apache2 libapache-mod-php
```

Après l'installation, le serveur Apache démarre directement. Vous devriez pouvoir accéder à sa page par défaut en utilisant l'adresse IP de votre serveur.

Installation de MySQL :

```
apt-get install mariadb-server
```

Pendant l'installation, entrer un mot de passe pour le compte d'administration de MySQL.

Installation de PHP :

```
apt-get install php
```

Installation des modules PHP

```
sudo apt install php-curl php-gd php-intl php-json php-mbstring php-xml  
php-zip php-mysql
```

Redémarrage du serveur Apache : Après l'installation d'une extension sur votre serveur LAMP, pensez à redémarrer le service Apache

```
service apache2 restart
```

- Quelles distributions Linux sont compatibles avec un serveur LAMP ? Un serveur LAMP peut être installé sur la plupart des distributions Linux.
- Quel est le rôle d'Apache dans un serveur LAMP et comment configurer un site web virtuel avec Apache ? Apache joue le rôle de serveur web dans une pile LAMP (Linux, Apache, MySQL, PHP). Il gère la communication entre le serveur et les clients.
- Comment installer et configurer MySQL pour fonctionner avec un serveur LAMP ?
- Quelles sont les bonnes pratiques pour sécuriser une base de données MySQL sur un serveur LAMP ?

```
sudo mysql_secure_installation # Sécurise l'installation de MySQL, suivre  
les instructions
```

```
sudo mysql -u root -p # se connecter à la DB
```

```
# Créer une DB et un utilisateur
```

```
CREATE DATABASE ma_base_de_donnees;
```

```
CREATE USER 'mon_utilisateur'@'localhost' IDENTIFIED BY  
'mon_mot_de_passe';
```

```
GRANT ALL PRIVILEGES ON ma_base_de_donnees.* TO
```

```
'mon_utilisateur'@'localhost';
```

```
FLUSH PRIVILEGES;
```

- Quelle version de PHP est recommandée pour un serveur LAMP et comment installer les extensions PHP nécessaires ?
La version 7.4, cf question 1 pour les modules
- Quels sont les outils de surveillance et de gestion disponibles pour superviser un serveur LAMP en production ?
 - ManageEngine OpManager1 : C'est un outil proactif de surveillance des serveurs qui aide les organisations à surveiller et à gérer leurs serveurs de manière transparente.
 - Site24x71 : Il offre une planification de la maintenance et des rapports personnalisables.
 - Moniteur de serveur et d'application1 : Il offre une interface Web intégrée unique et une cartographie intelligente des dépendances infra des applications.
 - Nagios3 : C'est un outil open source largement utilisé pour surveiller les performances de serveur et de réseau.
- Quelles sont les étapes pour déployer une application web sur un serveur LAMP et assurer sa disponibilité et sa stabilité ?
 - Installation du serveur LAMP.
 - Déploiement de l'application : Transférez les fichiers de votre application web sur le serveur. Assurez-vous que les fichiers sont dans le répertoire correct pour qu'Apache puisse les servir.
 - Configuration de la base de données : Créez une nouvelle base de données MySQL pour votre application.
 - Test de l'application : À ce stade, votre application devrait être accessible via un navigateur web.
 - Surveillance du serveur : Utilisez des outils de surveillance pour garder un œil sur l'utilisation du CPU, de la mémoire, de l'espace disque, etc.
 - Mise en place de sauvegardes : Configurez des sauvegardes régulières de votre base de données et de vos fichiers d'application. Cela vous permettra de récupérer rapidement en cas de perte de données.
 - Mise à jour régulière : Assurez-vous que votre serveur et votre application sont régulièrement mis à jour avec les derniers correctifs de sécurité.
 - Équilibrage de charge : Si votre application reçoit beaucoup de trafic, vous voudrez peut-être envisager de mettre en place un équilibrage de charge pour répartir le trafic entre plusieurs serveurs.
 - Plan de reprise après sinistre : Ayez un plan en place pour savoir comment vous récupérerez si quelque chose va mal. Cela pourrait inclure la bascule vers un serveur de secours, la restauration à partir de sauvegardes, etc.
- Quels sont les fichiers de configuration clés d'un serveur LAMP et où sont-ils situés sur un système Linux ?
 - Apache : *Configuration principale* : `/etc/apache2/apache2.conf`
Configuration du Virtual Host : `/etc/apache2/sites-available/000-default.conf` pour le site par défaut, et `/etc/apache2/sites-available/monsite.com.conf` pour un site spécifique.
Configuration du module : `/etc/apache2/mods-available/`
 - MySQL : *Configuration principale* : `/etc/mysql/my.cnf` ou `/etc/my.cnf`

- PHP : *Configuration principale* : `/etc/php/7.4/apache2/php.ini` pour PHP 7.4 avec Apache. Le chemin peut varier en fonction de la version de PHP et du serveur web utilisé.
- Linux : *Configuration réseau* : `/etc/network/interfaces` ou `/etc/netplan/` pour les systèmes utilisant Netplan. *Configuration du pare-feu* : `/etc/iptables/rules.v4` pour iptables, ou utilisez ufw (Uncomplicated Firewall) pour une configuration plus simple.
- Comment mettre en place un certificat SSL/TLS sur un serveur LAMP pour sécuriser les communications avec les clients ? Dans le contexte d'un site web public, il est conseillé d'acheter un nom de domaine et d'utiliser une autorité de certification reconnue comme Let's Encrypt. Dans notre contexte, nous utiliserons un certificat auto-signé.

Installation WordPress

```
cd /tmp
wget https://wordpress.org/latest.zip # Télécharge la dernière version de
WordPress
```

- Créer une DB comme vu précédemment

```
sudo apt-get update
sudo apt-get install zip # Télécharge Zip pour décompresser l'archive WP

sudo unzip latest.zip -d /var/www/html # Décompresser dans le dossier où sont
stockées les pages web par défaut de Apache

# Déplacer tout le contenu du dossier "wordpress" à la racine de notre site
cd /var/www/html
mv wordpress/* /var/www/html/
rm wordpress/ -Rf
chown -R www-data:www-data /var/www/html/ # Donne les droits à l'utilisateur
"www-data" (Apache) sur tous les fichiers du site
```

- Se connecter sur l'interface web WordPress pour finaliser l'installation et la configuration :



Vous devez saisir ci-dessous les détails de connexion à votre base de données. Si vous ne les connaissez pas, contactez votre hébergeur.

Nom de la base de données

wp_MSCYBER16_ron_jp

Le nom de la base de données avec laquelle vous souhaitez utiliser WordPress.

Identifiant

admin_wp_ron_jp

Votre identifiant MySQL.

Mot de passe

mot de passe

Afficher

Votre mot de passe de base de données.

Adresse de la base de données

localhost

Si localhost ne fonctionne pas, demandez cette information à l'hébergeur de votre site.

Préfixe des tables

wp_

Si vous souhaitez faire tourner plusieurs installations de WordPress sur une même base de données, modifiez ce réglage.

Envoyer



Bienvenue

Bienvenue dans la très célèbre installation en 5 minutes de WordPress ! Vous n'avez qu'à remplir les informations demandées ci-dessous et vous serez prêt à utiliser la plus extensible et puissante plateforme de publication de contenu au monde.

Informations nécessaires

Veuillez renseigner les informations suivantes. Ne vous inquiétez pas, vous pourrez les modifier plus tard.

Titre du site

Les Marins d'Armor

Identifiant

Jean-Philippe

Les identifiants ne peuvent utiliser que des caractères alphanumériques, des espaces,

des tirets bas ("_"), des traits d'union ("-"), des points et le symbole @.

Mot de passe

oSjFe8kXZY*NQI5CG5

Masquer

Strong

Important : Vous aurez besoin de ce mot de passe pour vous connecter. Pensez à le stocker dans un lieu sûr.

Votre e-mail

Vérifiez bien cette adresse e-mail avant de continuer.

Visibilité par les moteurs de recherche

☐ Demander aux moteurs de recherche de ne pas indexer ce site

Certains moteurs de recherche peuvent décider de l'indexer malgré tout.

Installer WordPress

WordPress Les Marins d'Armor 0 Créer Bonjour, Jean-Philippe

Options de l'écran Aide

Tableau de bord

X Ignorer

Bienvenue sur WordPress !

[En savoir plus sur la version 6.4.3](#)

Créez des contenus riches avec les blocs et les compositions

Les compositions de blocs sont des mises en page de blocs pré-configurées. Utilisez-les pour vous en inspirer ou pour créer des nouvelles page en un clin d'œil.

[Créer une nouvelle page](#)

Personnalisez l'ensemble de votre site avec les thèmes basés sur des blocs

Bâissez l'ensemble de votre site, de l'en-tête au pied de page, en utilisant simplement des blocs et des compositions.

[Ouvrir l'éditeur de site](#)

Modifiez l'apparence de votre site avec les styles globaux

Ajustez votre site, ou donnez-lui une apparence totalement nouvelle ! Laissez libre cours à votre imagination... que diriez vous d'une nouvelle palette de couleurs ou de nouvelles polices d'écriture ?

[Modifier les styles](#)

- Pour des raison de sécurité, passer le fichier de config en lecture seule et seulement pour Apache

```
chmod 400 /var/www/html/wp-config.php
```

- Nous pouvons alors personnaliser notre site web



Toujours plus de Rhum pour contrer la houle

Les Marins d'Armor sont une entreprise de recherche sur les bienfaits
du Rhum pour marcher droit sur un pont quand la houle est forte.

[À propos](#)



Une passion pour la création d'ivrognes

Notre gamme complète de services professionnels s'adresse à une clientèle
diversifiée, allant des propriétaires de navires aux alcooliques notoires.



Rénovation et restauration



Support continu



Accès à l'application



Conseil



Gestion de projet



Architectural Solutions

Regardez, lisez, écoutez

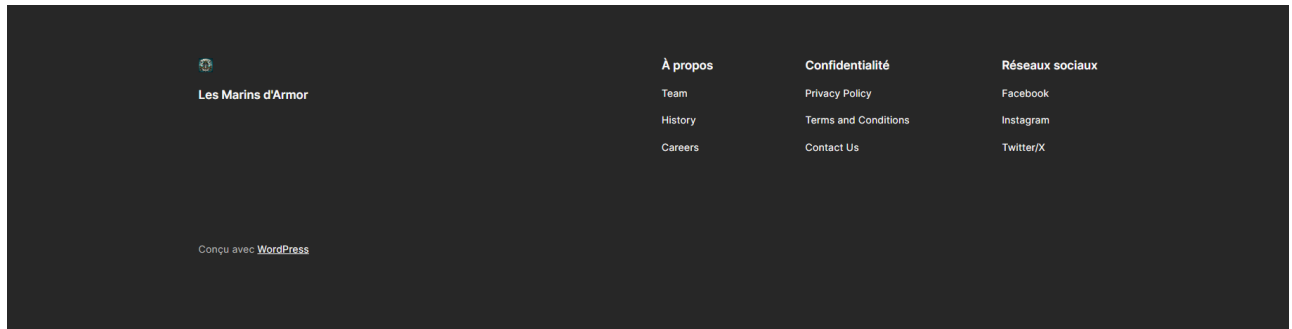
Bonjour tout le monde !

Fév 14, 2024 — par Jean-Philippe dans Non classé

Rejoignez plus de 900 abonnés/abonnées

Restez au courant de tout ce que vous devez savoir.

[S'inscrire](#)



Paramétrage de l'intranet pour le domaine

- Configurer votre serveur Web afin d'avoir un vhost répondant pour votre domaine, tout en conservant la page par défaut accessible.

```
GNU nano 6.2 /etc/apache2/sites-available/lma-breizh.local.conf
<VirtualHost *:80>
    ServerAdmin admin_wp_ron_jp@localhost
    ServerName lma-breizh.local
    ServerAlias www.lma-breizh.local
    DocumentRoot /var/www/html/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

```
sysadmin@linuxroxx:~$ sudo a2ensite lma-breizh.local.conf
Enabling site lma-breizh.local.
To activate the new configuration, you need to run:
    systemctl reload apache2
sysadmin@linuxroxx:~$ systemctl reload apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units ====
Authentication is required to reload 'apache2.service'.
Authenticating as: SysAdmin (sysadmin)
Password:
==== AUTHENTICATION COMPLETE ====
```

```
PS C:\Users\Utilisateur> ping lma-breizh.local
# Copyright (c) 1993-2009 Microsoft Corp.
Envoi d'une requête 'ping' sur lma-breizh.local [192.168.1.40] avec 32 octets de données :
Réponse de 192.168.1.40 : octets=32 temps<1ms TTL=64
Réponse de 192.168.1.40 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.40 : octets=32 temps=2 ms TTL=64
Réponse de 192.168.1.40 : octets=32 temps=1 ms TTL=64
Statistiques Ping pour 192.168.1.40:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes:
    Minimum = 0ms; Maximum = 2ms; Moyenne = 1ms
PS C:\Users\Utilisateur>
```

- Afin de résoudre vers le domaine de test, il est nécessaire de modifier le fichier "hosts" pour lui associer l'IP du serveur.

Sur windows :

📁 > Ce PC > Windows (C:) > Windows > System32 > drivers > etc

elements	Nom	Modifié le	Type	Taille
its	hosts	07/12/2019 10:12	Fichier	1 Ko
	hosts.ics	14/02/2024 09:03	Calendar	1 Ko
	lmhosts.sam	07/12/2019 10:12	Fichier SAM	4 Ko
	networks	07/12/2019 10:12	Fichier	1 Ko
n	protocol	07/12/2019 10:12	Fichier	2 Ko
	services	07/12/2019 10:12	Fichier	18 Ko

*hosts - Bloc-notes

Fichier Edition Format Affichage Aide

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
#
192.168.1.40 lma-breizh.local
```

Sécuriser les flux

Mettre en place un certificat ssl auto-signé pour votre domaine.

```
# Activer SSL
a2enmod ssl
systemctl restart apache2

# Création du certificat et suivre les indications du prompt
openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt

# Configurer Apache pour utiliser SSL et redirection HTTP vers HTTPS
nano /etc/apache2/sites-available/lma-breizh.local.conf
```

```
# Nano
<VirtualHost *:443>
  ServerName your_domain_or_ip
  DocumentRoot /var/www/your_domain_or_ip

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
  SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
</VirtualHost>

<VirtualHost *:80>
  ServerName your_domain_or_ip
  Redirect / https://your_domain_or_ip/
</VirtualHost>
# /Nano

systemctl reload apache2
```

Si vous envisagez d'utiliser SSL pour un site web public, vous devriez envisager d'acheter un nom de domaine et d'utiliser une autorité de certification largement reconnue telle que Let's Encrypt.