Guide complet pour installer Tiki Wiki sur Debian 12 - Édition 2025

Bernard Sfez - 2025-10-18 11:26

Ce guide complet montre comment configurer un serveur Debian 12 avec un panneau de contrôle d'hébergement et installer une solution web Tiki Wikisolution web Tiki Wiki)) en utilisant uniquement des logiciels open source.

Conçue pour la polyvalence, cette méthode éprouvée s'appuie sur une instance Amazon AWS Lightsail, mais peut être facilement adaptée à la plupart des plateformes d'hébergement. Suivez ce guide étape par étape pour configurer MariaDB, gérer les versions de PHP, installer Webmin|Webmin et Virtualmin, sécuriser votre serveur avec des certificats SSL et publier votre site Tiki Wiki en ligne — le tout avec des conseils d'experts et des astuces professionnelles pour simplifier le processus.

Ce tutoriel s'adresse aux administrateurs IT intermédiaires ou aux développeurs full-stack recherchant un accompagnement pour la configuration et la mise en ligne de sites web.

Dans ce tutoriel, nous allons apprendre à configurer et paramétrer :

- une instance AWS Lightsail (valable également pour une instance EC2)
- le système d'exploitation Linux, https://www.debian.org|Debian12] et https://httpd.apache.org|Apache2]
- https://mariadb.com/kb/en/innodb|MariaDB] (InnoDB)
- le panneau de contrôle d'hébergement Webmin et Virtualmin
- https://www.php.net|PHP]
- https://git-scm.com|Git] et le dépôt https://gitlab.com|Gitlab] de Tiki
- Tiki Wiki, le créateur de sites web

Avant de commencer ce tutoriel Tiki, il est recommandé d'avoir une certaine familiarité avec l'utilisation du shell et une compréhension de base des opérations sur un serveur. Cependant, ne laissez pas cela vous freiner ! Vous pouvez tout à fait vous lancer et apprendre au fur et à mesure — assurez-vous simplement de travailler dans un environnement de test sans données réelles au

début. Grâce à la possibilité de supprimer et de réinstaller les instances, et à l'offre gratuite de 3 mois sur AWS Lightsail, vous avez toute latitude pour expérimenter et peaufiner votre configuration jusqu'à ce qu'elle soit parfaite.
Compte tenu de l'évolution rapide des législations, il est essentiel de rappeler notre position : nous privilégions la souveraineté et la maîtrise des données privées, notamment via des logiciels Open Source et, lorsque c'est possible, le stockage en interne ou chez un prestataire maîtrisé. L'exemple présenté dans cet article s'appuie sur certains services AWS (Amazon), uniquement à titre illustratif. Avec de légères adaptations, vous pourrez le reproduire chez la plupart des hébergeurs, voire sur votre propre serveur « barebone ».

Si vous faites appel à un prestataire externe pour vos services d'hébergement (AWS, Google, Azure, OVH, Infomaniak, etc.), vérifiez attentivement votre contrat (conditions, annexes, clauses de droit applicable et de juridiction). La localisation physique des serveurs ne signifie pas nécessairement que le prestataire est soumis uniquement aux lois du pays d'hébergement. Ainsi, héberger en France peut réduire certains risques (résidence des données, latence, souveraineté opérationnelle), sans garantir une absence totale d'exposition à des demandes extraterritoriales.

Si vous préférez éviter la courbe d'apprentissage, gagner du temps ou confier l'installation de votre solution Open Source et de votre Tiki Wiki à un expert, faites appel directement à moi ou consultez la liste) des consultants Tiki. Avec un spécialiste Tiki pour gérer le processus, vous avez la garantie d'une installation fluide et professionnelle du début à la fin.

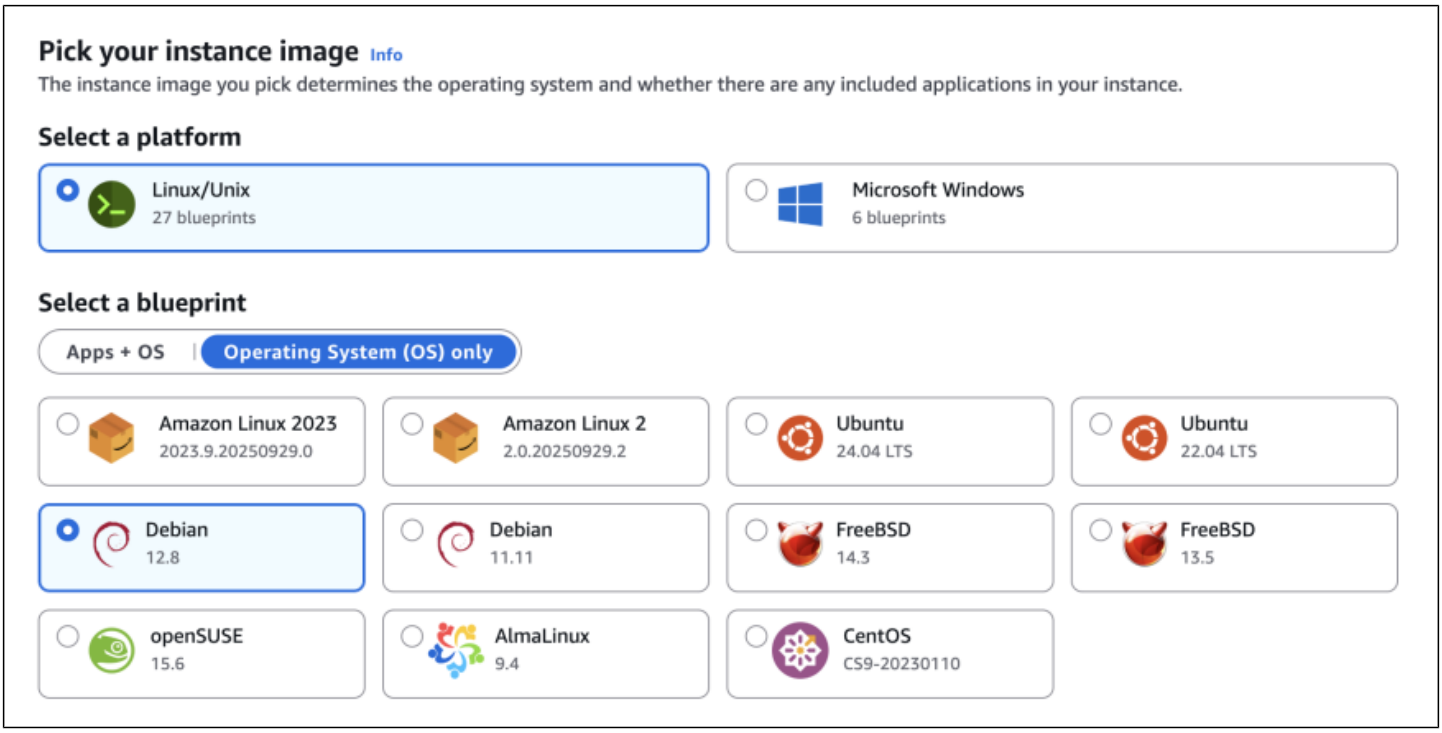
Préparation du serveur

Installer une instance Amazon Lightsail

Sélection de la région

Connectez-vous à votre console AWS (ou créez un compte) et recherchez « Lightsail » dans la barre de recherche.
Choisissez l'emplacement de votre instance en sélectionnant la région du serveur. Idéalement, optez pour la région la plus proche de vos utilisateurs cibles pour de meilleures performances.
Ensuite, sélectionnez l'image de votre instance en choisissant la plateforme.
Remarque : les instances Lightsail ne sont pas disponibles dans tous les centres de données et régions AWS.

Pour ce tutoriel, sélectionnez l'image de votre instance en cliquant sur le modèle « Linux/Unix », choisissez « OS Only », puis sélectionnez Debian 12.x.
Important : l'installation de Virtualmin requiert un système d'exploitation vierge avec uniquement les outils et bibliothèques serveur de base ; évitez donc de sélectionner autre chose qu'une installation minimale du système.



Clé SSH pour l'accès à l'instance

Dans la section clé SSH, vous serez invité à utiliser la clé SSH par défaut ou à changer la clé associée à votre compte si une clé existe déjà.

Si c'est votre première instance et que vous préférez la simplicité, choisissez la clé par défaut créée avec votre instance. Téléchargez-la dans le dossier ~/.ssh de votre ordinateur pour un accès futur.
Si vous possédez déjà une clé SSH, vous pouvez la téléverser et l'associer à cette nouvelle instance.
Pour créer une nouvelle paire de clés SSH, suivez le guide fourni par Amazon.

Sélectionner votre plan

Choisissez votre plan d'instance avec soin. Si l'option la moins chère peut suffire pour les versions de Tiki antérieures à Tiki 26, les versions à partir de Tiki 26+ nécessitent un minimum de 2 Go de RAM (et certaines pré-versions de Tiki 28 en exigent 4 Go à la date de publication de ce tutoriel).
Remarque : Lightsail ne propose pas de mise à niveau directe. Pour « upgrader » vers un plan supérieur, il faut créer une nouvelle instance et transférer un snapshot. En alternative, envisagez des solutions rapidement duplicables comme celles mises en place par Open Source Solutions, garantissant efficacité et fiabilité.

Pour éviter toute frustration ultérieure, choisissez votre plan judicieusement. En cas de doute, n'hésitez pas à contacter l'équipe Open Source Solutions pour obtenir des conseils.

Sauvegarder votre instance AWS

Donnez à votre instance un nom clair et descriptif afin de rester organisé — surtout si vous prévoyez d'en créer plusieurs pour le développement ou les tests. Ajoutez des étiquettes (tags) si nécessaire pour une meilleure classification.

Enfin, cliquez sur le bouton orange « Create Instance ». En une minute environ, votre instance sera opérationnelle. Vous pouvez y accéder immédiatement à l'aide de la console SSH intégrée en cliquant sur l'icône de terminal ( ).

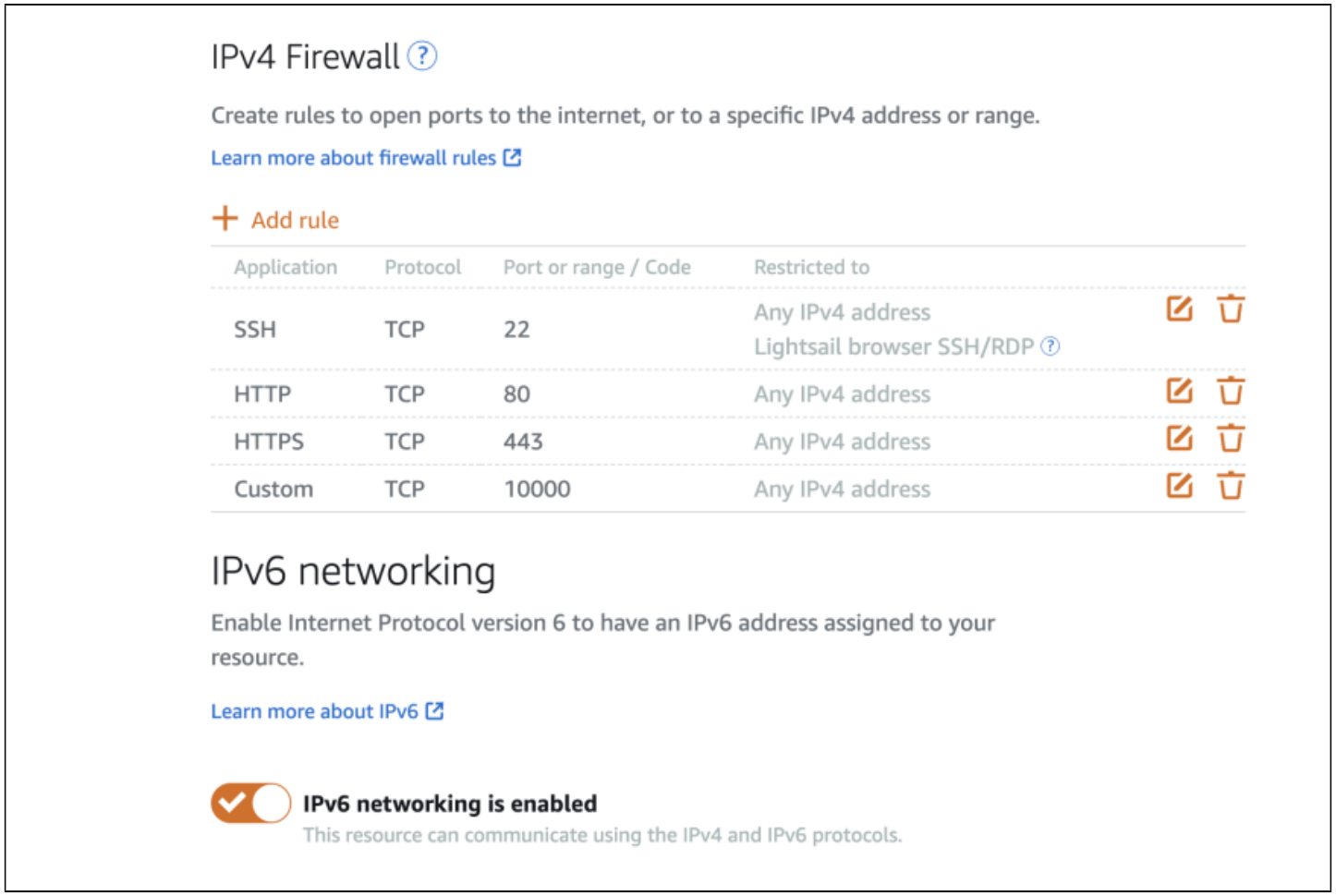
Configuration Réseau et Groupe de Sécurité Lightsail

La configuration de l'accès à votre site et au panneau de contrôle Virtualmin est essentielle pour la sécurité du serveur. Commencez par accéder au panneau de contrôle de votre instance Lightsail et sélectionnez Networking pour gérer et sécuriser vos paramètres d'accès.

Par défaut, les ports 22 (SSH) et 80 (HTTP) devraient déjà être ouverts.

1. Définir le groupe de sécurité et cliquer sur Add Rule pour ouvrir des ports supplémentaires :

- 443 pour le HTTPS (accès sécurisé au site via SSL)
- 10000 pour l'accès au panneau de contrôle Virtualmin



2. Définir des restrictions d'accès basées sur l'IP (recommandé) :

- Ouvrez les ports 80 et 443 à tout le trafic (aucune restriction IP).
- Restreignez l'accès aux ports 22 et 10000 uniquement à votre IP pour plus de sécurité. Pendant la configuration, vous pouvez utiliser l'accès SSH/RDP basé sur le navigateur Lightsail.
- Gardez le port 22 ouvert pendant la configuration mais prévoyez de le restreindre à votre IP ensuite. Pour une sécurité renforcée, envisagez de changer le port SSH par défaut une fois la configuration terminée.

Chez Open Source Solutions, nous appliquons une politique éprouvée de gestion des ports serveurs (OSS Managed Server) afin de réduire les risques d'intrusion, garantissant un contrôle strict et une sécurité accrue pour les serveurs de nos clients.

3. Configurer une IP statique :
Votre adresse IPv4 publique changera lorsque vous arrêterez et redémarrerez votre instance Lightsail. Pour éviter cela, créez et attachez une adresse IPv4 statique à votre instance depuis la section IPv4 networking. Cela garantit que votre instance conserve une adresse IP fixe.

Bien que cela soit en dehors de la portée de ce tutoriel, c'est le bon moment pour pointer votre domaine vers l'adresse IP publique statique du serveur, garantissant que votre domaine pointe correctement vers votre solution d'hébergement.

4. Appliquer et tester :
Redémarrez l'instance pour appliquer les changements. Vérifiez que votre IP statique est attachée et que les ports nécessaires sont ouverts.

Cette configuration assure une base sécurisée pour la gestion de votre site et de votre serveur sur Lightsail, protégeant les ports sensibles contre tout accès non autorisé tout en maintenant la fonctionnalité.

⚠ Activation de l'accès root

Avec votre instance AWS par défaut vient un compte "admin" membre du groupe sudoers et donc capable de passer en super-utilisateur "root" (su). N'activez la connexion « root » que si votre serveur ou votre configuration d'hébergement l'exige et nous vous le déconseillons fortement sauf éventuellement de façon temporaire.

Sudo ou Activer et utiliser la connexion root☒✓

Sudo ou Activer et utiliser la connexion root

Selon les paramètres de votre compte, vous pouvez être en mesure d'utiliser l'utilisateur root ou la commande sudo. Si vous pouvez utiliser l'utilisateur root ou sudo, c'est bon, vous pouvez passer cette étape.
Si vous souhaitez tout de même activer la connexion root… voici comment faire.

Connecté en tant qu'utilisateur par défaut "admin". (J'utilise nano mais c'est la même chose avec VI, VIM ou tout autre éditeur)

Basculer vers le super utilisateur (root)

```
sudo su
```

Modifier le fichier de configuration SSH

```
nano /etc/ssh/sshd_config
# Changez
PermitRootLogin no to PermitRootLogin yes
# Changez aussi PasswordAuthentication no pour
PasswordAuthentication yes
```

Bien sûr sauvegardez vos changements.

Vous devrez également supprimer un petit script qui empêche root d'utiliser sa clé SSH.

Modifier le fichier authorized_keys

```
nano ~/.ssh/authorized_keys
```

Le script commence par "no-port-fowarding..." ; vous devez supprimer ce script jusqu'à la clé ssh elle-même qui commence par "ssh-rsa...".
Ainsi, la clé ssh sera accessible à la connexion ssh.

Redémarrer SSHD pour valider les changements

```
systemctl restart sshd
```

Définir le mot de passe root

```
passwd root
```

Redémarrer votre instance

```
sudo reboot
```

Vous serez déconnecté, reconnectez-vous et vérifiez que tout fonctionne correctement lorsque vous vous connectez en root.

Connexion en root

```
ssh root@xx.xx.xx.xx
 (IP de votre instance)
```

Note : C'est une bonne pratique, et je le recommande vivement, de désactiver l'accès root sur les serveurs de production une fois que tout est en place. Cela peut être fait en définissant les paramètres "PermitRootLogin" et "PasswordAuthentication" sur "no" dans le fichier "/etc/ssh/sshd_config".

Connexion à votre serveur en utilisant SSH

Connexion en utilisant le SSH/RDP basé sur le navigateur AWS

Une fois votre instance en cours d'exécution, vous pouvez commencer à la gérer. Une façon simple d'accéder à votre serveur est d'utiliser le SSH/RDP basé sur le navigateur de Lightsail, qui fournit un accès SSH direct et sécurisé via un terminal AWS.

Pour la plupart des tâches de gestion, cette méthode basée sur le navigateur est suffisante. Cependant, vous devriez également pouvoir vous connecter en utilisant une application de terminal externe, et plus tard, nous utiliserons le terminal intégré de Virtualmin pour des tâches plus avancées.

Connexion en utilisant SSH depuis un terminal externe

Vous pouvez également vous connecter à votre serveur en utilisant votre application de terminal préférée (par ex. PuTTY, Terminal macOS ou autre) pour un accès shell. Cette approche nécessite l'IP publique de votre instance et votre clé SSH locale. L'utilisateur administratif par défaut défini par AWS est admin.

La commande pour se connecter (en supposant que votre clé SSH soit enregistrée comme LightsailDefaultKeyPair-us-east-1.pem) serait :

SSH en utilisant la clé par défaut enregistrée

```
ssh -i ~/.ssh/LightsailDefaultKeyPair-us-east-1.pem admin@xx.xx.xx.xx
```

Remplacez xx.xx.xx.xx par l'adresse IP publique de votre instance. Cette méthode offre une plus grande flexibilité, notamment pour la configuration avancée et l'installation de logiciels.

Si vous n'avez pas configuré la clé SSH lors de la création de l'instance, cela peut être un peu difficile si vous n'êtes pas familier avec l'administration système. Voici comment procéder :

- Remplacez LightsailDefaultKeyPair-us-east-1.pem par le nom de votre clé.
- Téléchargez la clé SSH sur votre ordinateur.
- Déplacez la clé dans votre répertoire ~/.ssh.
- Définissez les bonnes permissions de fichier :

Définir les permissions du fichier

```
sudo chmod 600 ~/.ssh/LightsailDefaultKeyPair-us-east-1.pem
```

Après cela, vous devriez pouvoir vous connecter avec la commande suivante :

SSH en utilisant la clé par défaut enregistrée

```
ssh -i ~/.ssh/LightsailDefaultKeyPair-us-east-1.pem admin@xx.xx.xx.xx
```

Pour plus de documentation, consultez le guide Amazon Lightsail SSH Using Terminal.

Vérification du nom d'hôte

Pour assurer le bon fonctionnement de Virtualmin/Webmin, il est essentiel de configurer correctement le nom d'hôte de votre serveur ainsi que le nom de domaine complet (FQDN – Fully Qualified Domain Name). Par défaut, votre serveur peut générer automatiquement un nom d'hôte, mais il est important de le vérifier et de le corriger si nécessaire.

Étape 1 : Vérifier le nom d'hôte actuel
Une fois connecté à votre serveur via SSH, utilisez la commande suivante pour vérifier le nom d'hôte actuel :

Vérifier le nom d’hôte

```
hostnamectl
```

En retour, le "Static hostname" affichera généralement l’adresse IP locale de l’instance.
Confirmez cela en exécutant la commande suivante pour n’afficher que le nom d’hôte :

Vérifier le nom d’hôte

```
hostname
```

Étape 2 : Définir le nom d’hôte selon votre FQDN
Vous devez mettre à jour le nom d’hôte pour qu’il corresponde à votre FQDN (par exemple : votredomaine.com) avant de passer à l’étape suivante (installation de Virtualmin).
Pour ce faire, éditez le fichier de configuration du nom d’hôte :

Modifier le nom d’hôte

```
sudo nano /etc/hostname
```

Remplacez l’entrée existante par votre FQDN souhaité (exemple : sousdomaine.domaine.com).

__Étape 3 : Modifier le fichier Hosts
Ensuite, vérifiez et mettez à jour le fichier /etc/hosts afin d’y inclure votre FQDN.
Il devrait ressembler à ceci :
`127.0.1.1 sousdomaine.domaine.com sousdomaine` mais par défaut, cela n’est pas configuré et vous devez mettre à jour la configuration.

Pour vérifier la configuration actuelle, exécutez :

Vérifier le fichier hosts

```
cat /etc/hosts
```

Pour modifier le fichier hosts et définir le bon FQDN, utilisez :

Modifier le fichier hosts

```
sudo nano /etc/hosts
```

Ajoutez ou mettez à jour la ligne comme indiqué ci-dessus (remplacez sousdomaine.domaine.com et sousdomaine par votre domaine et sous-domaine réels).

Étape 4 : Redémarrer le serveur
Après avoir effectué ces modifications, redémarrez votre serveur pour que les changements prennent effet :

Redémarrer le serveur

```
sudo reboot
```

Étape 5 : Vérifier les changements
Une fois le serveur redémarré, vérifiez que tout est bien configuré en exécutant :

Vérifier le nom d'hôte

```
hostname
```

Si votre FQDN s'affiche correctement, vous êtes prêt à procéder à l'installation de Virtualmin. Sinon, revérifiez vos fichiers de configuration ou consultez les options de dépannage ci-dessous.

Corriger le fichier hosts et rendre les changements permanents☒✓
Vous devez également vérifier et ajouter votre hôte dans le fichier hosts si votre fournisseur ne l'a pas correctement configuré.
Cependant, si vous le modifiez directement (en éditant /etc/hosts), les changements seront annulés lors du prochain redémarrage.
Pour les rendre permanents, vous devez modifier le modèle utilisé pour recréer le fichier hosts à chaque redémarrage.

Certaines instances peuvent utiliser un fichier de configuration Cloud, d'autres un fichier hosts Debian.
Vous trouverez des informations utiles dans les premiers commentaires de `/etc/hosts`.
Si le fichier commence par : "Your system has configured 'manage_etc_hosts' as True.", cela signifie que votre serveur utilise cloud-init, et vous devez alors définir la valeur de "preserve_hostname" sur true dans /etc/cloud/cloud.cfg.

Modifier hosts.debian.tmpl

```
nano /etc/cloud/cloud.cfg
preserve_hostname: true
```

Redémarrez le serveur et vérifiez que les changements sont permanents.

Mettre à jour votre système Debian

En supposant que vous disposiez d'un accès root et des informations SSH vous permettant de vous connecter par mot de passe ou clé SSH, commençons par nous assurer que notre instance est à jour.

Nous voulons travailler avec les dernières versions des dizaines de logiciels et de bibliothèques dont votre serveur dépendra. Connectez-vous à votre serveur et mettez-le à jour avec les commandes suivantes :

Mise à jour du serveur Linux

```
sudo apt update
sudo apt upgrade
```

Créer un fichier swap (swapfile)

Depuis l'introduction du nouveau système Built dans Tiki (à partir de Tiki 27), l'installation depuis Git est plus exigeante en ressources que l'installation via le package de release (installation standard).

Avec Tiki 29, il faut généralement plus de 2 Go de RAM pour terminer l'installation correctement avec les packages NPM (obligatoire). Si votre serveur dispose de peu de mémoire vive, nous vous recommandons de créer et activer un fichier swap (swapfile) afin d'éviter les erreurs liées à un manque de mémoire (processus interrompus, échec de compilation/installation, etc.).

Il est préférable de mettre en place le swap le plus tôt possible, idéalement avant de lancer l'installation, afin que l'ensemble du déploiement (et plus largement le serveur) puisse en bénéficier.
Consultez la procédure complète (Debian/Ubuntu) que nous mettons à votre disposition.

Installer Webmin et Virtualmin

Virtualmin installera tout ce dont vous avez besoin, et il est essentiel que l'installation de Virtualmin soit effectuée en premier.
Sinon, vous serez averti que des outils ou bibliothèques ont déjà été installés, et il faudra parfois les supprimer manuellement avant de continuer.

Nous allons télécharger le script d'installation automatique de Virtualmin et l'exécuter. Il s'agit essentiellement d'un script shell qui prendra en charge le reste de l'installation une fois lancé.

Télécharger le script d'installation de Virtualmin

```
sudo wget https://software.virtualmin.com/gpl/scripts/install.sh
```

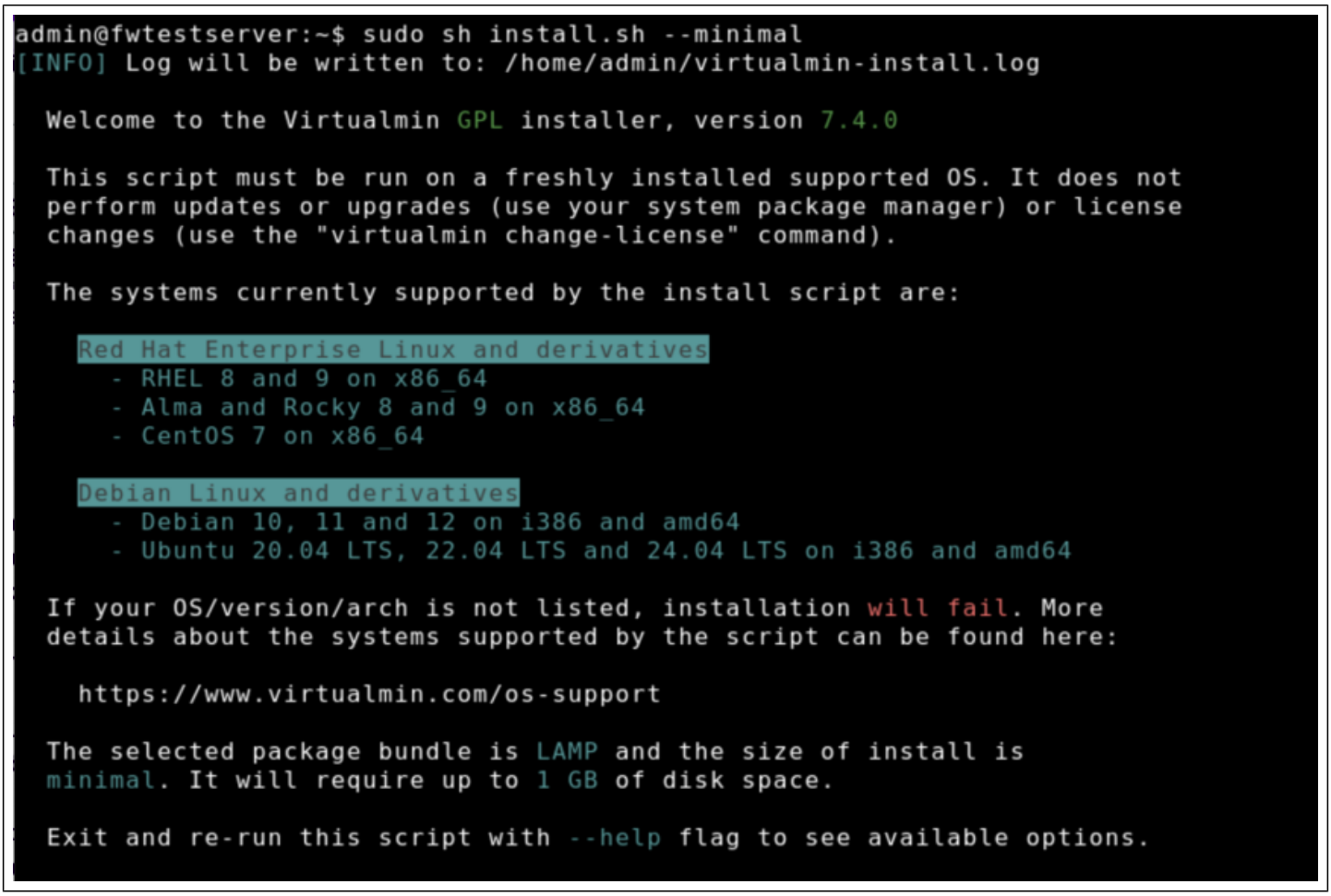
Vous pouvez effectuer une installation complète, mais aussi une installation minimale, qui économisera les ressources de votre instance. Par exemple, lorsque je n'ai pas besoin d'un serveur mail, je fais une installation minimale.

Installation complète de Virtualmin

```
sudo sh install.sh
```

Installation minimale de Virtualmin

```
sudo sh install.sh --minimal
```



Vous devriez maintenant voir les différents composants s'installer un par un.
Cela peut prendre un certain temps... il suffit d'attendre que le processus se termine.

L'installation devrait se terminer par le message :
"SUCCESS to configure at https://xxx-xxx-xxx-xxx:10000 (or https://yourFQDN:10000)."
Vous devriez maintenant pouvoir vous connecter à votre panneau Virtualmin en utilisant vos identifiants root si votre pare-feu est correctement configuré.
Il arrive que certains services d'hébergement n'ouvrent que certains ports par défaut, comme 80, 443 et 22. Pour Virtualmin, vous devez également ouvrir le port 10000.

Configurer votre accès root à Virtualmin

Pour pouvoir utiliser Virtualmin en tant que root sans activer la connexion root SSH, exécutez la commande webmin passwd pour définir ou modifier le mot de passe root de Webmin et activer l'authentification par mot de passe Webmin.

Définir l'utilisateur root de Webmin

```
sudo webmin passwd --user root
```

Utilisez ce mot de passe pour vous connecter à votre nouvelle instance Virtualmin :
https://xxx-xxx-xxx-xxx:10000 (ou https://yourFQDN:10000)

Configuration et options post-installation de Virtualmin

Une fois connecté à l'interface web de Virtualmin, il se peut que vous deviez autoriser l'utilisation d'un certificat SSL périmé et valider votre accès à cette page (selon votre navigateur et votre configuration système).

Suivez ensuite l'assistant de configuration post-installation de Virtualmin (Virtualmin Post-Installation Wizard).
Cet assistant est simple et vous guide étape par étape pour compléter la configuration.
Les questions peuvent varier selon votre système et la version de Virtualmin utilisée, mais dans la plupart des cas, il est sûr d'accepter les valeurs par défaut proposées.
Serveurs de base de données

- Exécuter le serveur de base de données MariaDB ?
  J'utilise MariaDB pour mes installations Tiki Wiki, donc oui.
  Vous devrez valider ou modifier le mot de passe root de MariaDB, le saisir et le conserver précieusement pour une utilisation ultérieure.
- Exécuter le serveur de base de données PostgreSQL ?
  Comme mentionné ci-dessus, la réponse sera non.

Configuration DNS
Le serveur de noms principal doit afficher le nom d'hôte défini précédemment.
Adresse e-mail système
Définissez votre adresse e-mail administrateur.

Vous pouvez vous arrêter ici et avoir suffisamment pour lancer votre premier serveur virtuel (site), ou continuer avec les paramètres optionnels de l'assistant.

Stockage des mots de passe
Nous ne voulons pas stocker les mots de passe en clair sur le serveur, donc il sera judicieux de sélectionner "Only store hashed passwords" (Ne stocker que les mots de passe encrypté).

Taille de la configuration MariaDB
Cela dépend de l'utilisation prévue de votre instance Tiki Wiki, mais sélectionner l'option "suggested" proposée par l'assistant Virtualmin convient très bien.

Répertoire des clés SSL
Sauf si vous savez exactement ce que vous faites, laissez la valeur par défaut (Per-domain).

À ce stade, le processus devrait être terminé.
Cependant, il se peut qu'un dialogue vous demande si vous souhaitez créer un serveur virtuel par défaut.
Si c'est le cas, je recommande de sélectionner "No" afin de configurer manuellement les paramètres de votre domaine.

Après avoir effectué les modifications nécessaires, je vérifie toujours la configuration pour m'assurer que tout est en ordre.
Une fois satisfait, procédez à un dernier redémarrage du serveur, puis vérifiez que tous vos paramètres sont bien conservés — vous pourrez alors créer votre premier Virtual Server, c'est-à-

dire un site web.

Créer votre premier Serveur Virtuel (votre site web)

- Définissez votre nom de domaine
- Donnez-lui une description
- Définissez le mot de passe d'administration (même si vous utilisez une clé SSH, garder un second accès est judicieux)
- Ajoutez une clé publique SSH (copiez votre clé publique)
- Définissez le nom d'utilisateur administrateur (ou conservez celui par défaut)

Dans le panneau Advanced, je ne modifie généralement que le nom de base de données par défaut.
Dans le panneau Enabled features, si vous n'utilisez pas le courriel ni les statistiques AWStats, je vous conseille de les désactiver (Mail for domain et Enable AWStats reporting).
Ne modifiez pas le reste et créez votre serveur.
Une fois créé, revenez à l'écran Virtual Server et, dans le panneau Quotas and limits, vérifiez la Server Quota.
Lors de l'installation de Tiki Wiki depuis Git, le processus de configuration peut nécessiter plus de 2 Go. Vous pouvez donc définir la limite sur illimitée pendant l'installation, puis limiter la quota une fois le système en fonctionnement.

Installer le certificat SSL Let's Encrypt

Remarque : Par défaut, Virtualmin tente de configurer le SSL pour tous les domaines figurant dans la liste "Domains associated with this server".
Si certains de ces domaines ne sont pas configurés correctement ou ne sont pas accessibles, la demande de certificat échouera.
Pour éviter cela, je recommande de spécifier manuellement uniquement les domaines que vous utilisez dans le champ "Domain names listed here" afin d'installer les certificats uniquement pour les domaines pertinents.

Pour installer le certificat SSL Let's Encrypt, suivez ces étapes :

- Allez dans la Virtual Server List, sélectionnez votre serveur virtuel, puis dans le menu de gauche, accédez à Manage Virtual Server > Setup SSL Certificate. Ensuite, sélectionnez Let's SSL Providers.
- Dans le champ Request certificate for, sélectionnez et saisissez les noms de domaine pour lesquels vous souhaitez un certificat SSL, en utilisant l'option Domain names listed here.
- Assurez-vous que l'option Automatically renew certificate? est réglée sur Yes, puis cliquez sur Request Certificate.

Avant de commencer, assurez-vous que votre domaine est correctement configuré chez votre registrar.

Vérification de l’état du serveur et gestion des services en cours

Dans votre tableau de bord Virtualmin, vous trouverez un panneau affichant l’état de vos serveurs et applications.
Vous pouvez y vérifier quels services sont actifs et effectuer les actions nécessaires :

- Vérifier la version de PHP : confirmez la version actuellement utilisée pour assurer la compatibilité avec vos applications.
- Courriel et applications de messagerie :
  - Gardez Postfix actif — il est essentiel pour l’envoi des e-mails tels que les notifications système ou les messages générés par les applications.
  - Désactivez Dovecot si votre serveur n’a pas besoin de traiter ou recevoir d’e-mails entrants.

Cependant, arrêter Dovecot via le tableau de bord ne stoppe le service que temporairement.
Pour le désactiver de manière permanente :
Dans le menu de gauche, accédez à Webmin > System > Bootup and Shutdown.
Recherchez les services nommés "Dovecot" dans la liste.
Sélectionnez le service, puis en bas de la page, cliquez sur Disable On Boot.
Recommandations supplémentaires

- Activer Fail2Ban : protégez votre serveur contre les attaques par force brute en activant cet outil de prévention des intrusions.
- Configurer un pare-feu : renforcez la sécurité de votre serveur en activant et configurant un pare-feu pour restreindre l’accès non autorisé.

En gérant soigneusement ces services et en appliquant ces mesures de sécurité, vous garantissez que votre serveur fonctionne efficacement et reste protégé.

Installation de plusieurs versions de PHP

Remarque : ces informations étaient exactes au moment de la rédaction de ce tutoriel et elles sont faciles à modifier pour les adapter à votre environment.

Debian 12 est livré avec PHP 8.2 par défaut, mais cette version peut ne pas correspondre à vos besoins.
Si vous avez besoin de PHP 8.1 ou d’autres versions, vous pouvez les installer et les configurer sur votre serveur.

Ajouter PHP8.1 depuis le dépôt sury

Vous pouvez configurer la version PHP par défaut utilisée sur vos nouveaux serveurs virtuels.
Vous pouvez modifier cette valeur par défaut via System Settings -> Server Templates -> Default -> PHP Options.
Pour définir la version PHP utilisée par un domaine spécifique, allez dans Virtualmin -> Server

configuration -> PHP version, puis sélectionnez la version souhaitée.

Naviguez vers System Settings > Server Templates > Default > PHP Options.

Définir la version PHP pour un domaine spécifique :
Allez dans Virtualmin, sélectionnez le domaine > Web Configuration > PHP Options.
Sur cet écran, vous pouvez choisir la version PHP pour un domaine particulier.

Installation des bibliothèques pour les versions PHP supplémentaires
Si vous devez prendre en charge plusieurs versions de PHP, installez les bibliothèques nécessaires comme suit :

Bibliothèques supplémentaires pour Tiki Wiki

N'oubliez pas que vous devez installer quelques bibliothèques supplémentaires, indispensables pour compléter l'installation.
C'est pourquoi elles ont été ajoutées ci-dessus, mais vous pouvez aussi les installer pour vos autres versions de PHP (en changeant le numéro de version).

Installer PHP8.4

```
sudo apt-get install php8.4-gd php8.4-intl php8.4-curl php8.4-zip php8.4-bcmath
```

En suivant ce processus, vous vous assurez que votre serveur dispose des versions et bibliothèques PHP nécessaires pour vos différentes applications.

Sécuriser le serveur (niveau de base)

Améliorer la sécurité d'un serveur requiert des compétences, des connaissances et une expertise qui dépassent le cadre de cet article.
Cependant, il est essentiel de mettre en place des mesures de base pour protéger votre serveur et vos données.
Nous allons ici passer en revue les étapes minimales que vous devriez suivre.
Pour une évaluation complète de la sécurité de votre installation Tiki et de votre serveur, veuillez me contacter.

Sécuriser votre base de données MySQL (MariaDB)

La dernière version de MySQL, alimentée par le moteur MariaDB, sera automatiquement installée par Virtualmin lors de la configuration.
Une fois l'installation terminée, nous allons la sécuriser afin de renforcer la défense contre les menaces potentielles et les accès non autorisés.

Sécuriser MariaDB

```
sudo mysql_secure_installation
```

Vous devriez pouvoir répondre à la plupart des questions sans trop réfléchir — voici mes réponses (des explications détaillées se trouvent facilement sur le Web) :

- Enter current password for root (enter for none) => entrez le mot de passe root défini lors de l'installation de Virtualmin, sinon laissez vide.
- Set root password? [Y/n] y – *Comme il s'agit d'une première installation.*
- Switch to unix_socket authentication [Y/n] Y
- Change the root password? [Y/n] n
- Remove anonymous users? [Y/n] y
- Disallow root login remotely? [Y/n] y
- Remove test database and access to it? [Y/n] y
- Reload privilege tables now? [Y/n] y

C'est terminé. Vérifions que MariaDB fonctionne :

Vérifier l'état de MariaDB

```
sudo systemctl status mariadb
```

Quelques erreurs peuvent apparaître puisque nous n'avons pas utilisé le mot de passe root pour cette commande. Cependant, MariaDB devrait indiquer qu'il est "Active", confirmant que le service fonctionne correctement.

Installer, activer et configurer Fail2Ban

Accédez à Webmin > Unused Modules.
Par défaut, vous devriez y trouver le module "Fail2Ban Intrusion Detector".
Installez le module et les paquets nécessaires, puis activez-le pour qu'il se lance automatiquement au démarrage du serveur.

⚠ Fichier jail local manquant

Sous Debian 12, un problème existe au moment de la rédaction de cet article qui a été corrigé depuis.

Fichier manquant dans fail2ban

Dans certains cas, l'installation via le module Virtualmin échoue, et il est nécessaire de l'effectuer directement depuis le terminal :

Installer Fail2Ban depuis le terminal

```
sudo apt install fail2ban
```

Vérifiez ensuite l'état du module dans le panneau Networking :

Après avoir activé le module, accédez à Webmin > Networking > Fail2Ban Intrusion Detector.

Le module peut encore apparaître comme étant arrêté.

Double vérification de l'état via le terminal :
Pour vous assurer que Fail2Ban fonctionne, exécutez la commande suivante :

Vérifier l'état de Fail2Ban

```
sudo systemctl status fail2ban
```

Si Fail2Ban est en cours d'exécution, vous verrez un message indiquant son état "active".
Sinon, démarrez le service manuellement avec :

Démarrer et vérifier Fail2Ban

```
sudo systemctl start fail2ban
sudo systemctl status fail2ban
```

Activez Fail2Ban au démarrage automatique :
Cela garantit que Fail2Ban se lancera automatiquement après chaque redémarrage du serveur.

En suivant ces étapes, Fail2Ban sera correctement installé et opérationnel.

Pour une configuration complète de Fail2Ban et une protection avancée adaptée à vos besoins, Open Source Solutions propose des services de maintenance serveur de niveau entreprise offrant une couche supplémentaire de sécurité pour votre serveur.

Installation de Tiki depuis le dépôt officiel Tiki (anonyme)

Naviguer vers votre répertoire HTML
Commencez par accéder au répertoire html.
Si vous n'êtes pas sûr de son emplacement, vérifiez-le dans le Virtual Server Summary de Virtualmin.

Cloner le dépôt Tiki

Visitez le site officiel de Tiki pour obtenir des instructions détaillées, ou consultez le guide d'installation complet.
Pour une configuration rapide, utilisez la commande suivante pour cloner la branche Tiki souhaitée (dans cet exemple, 29.x) sans l'historique du dépôt :

Télécharger Tiki depuis le dépôt git

```
git clone --depth=1 --branch=29.x https://gitlab.com/tikiwiki/tiki.git .
```

Configuration de SSH pour la connexion à GitLab

Pour utiliser la clé SSH associée à votre compte GitLab, vous devez créer un fichier config dans

votre répertoire ~/.ssh.
Voici la procédure :

Accédez au répertoire .ssh de votre dossier personnel (ex. : /home/domain/.ssh).
S'il n'existe pas, créez-le :

Créer et définir les permissions du répertoire .ssh

```
mkdir -p ~/.ssh
chmod 700 ~/.ssh
```

Créer et configurer le fichier SSH Config
Dans le répertoire .ssh, créez un fichier config et ajoutez-y le contenu suivant :

Créer le fichier config et y copier le contenu

```
# GitLab.com
Host gitlab.com
PreferredAuthentications publickey
IdentityFile ~/.ssh/id_rsa
```

Remplacez id_rsa par le nom du fichier correspondant à votre clé SSH privée.

Définir les permissions du fichier
Assurez-vous que le fichier config possède les bons droits et le bon propriétaire :

Définir les permissions du fichier config

```
chmod 600 ~/.ssh/config
chown your_user:your_user ~/.ssh/config
```

Tester la connexion SSH à GitLab pour confirmer que votre clé SSH est bien utilisée :

Tester la connexion SSH à GitLab

```
ssh -T -vvv git@gitlab.com
```

Vous devriez voir un message de réussite confirmant la connexion.
Une fois la clé SSH et la configuration en place, vous pouvez procéder au clonage de votre dépôt dans le répertoire html.

Installation de Tiki via SSH

Accédez à votre répertoire html (souvent public_html).
Si vous ne connaissez pas son emplacement sur votre nouveau serveur Virtualmin, vérifiez-le dans le Virtual Server Summary.

Télécharger Tiki depuis votre dépôt git

```
git clone --branch=target_branch --depth=1 git@gitlab.com:youruser/your_repo .
```

Il est ensuite nécessaire d'exécuter le script setup.sh de Tiki pour installer les dépendances et corriger les permissions des fichiers et répertoires.

À partir de la version 27, Tiki utilise une méthode différente pour finaliser l'installation

À partir de Tiki 27, Tiki utilise le système Tiki 27 plus Build System.
Cela inclut l'intégration d'outils tels que Composer pour les dépendances PHP et Node.js pour les dépendances JavaScript et CSS.
Veuillez consulter mon article How
to upgrade to Tiki Wiki 27 pour plus d'informations.

Tiki setup.sh pour les versions antérieures à Tiki27

À partir de là, suivez le processus d'installation Tiki habituel (setup.sh (voir les notes supplémentaires ci-dessus), création de la base de données) et vous aurez un Tiki prêt à être installé !