Documentation DDWS

Pour commencer nous allons installer apache2 pour pouvoir mettre en place notre serveur.

Ouvrez le terminal et entrez la commande “sudo apt install apache2”. Une fois l’installation terminée activez apache2 avec la commande “sudo systemctl enable apache2”.

Maintenant nous devons accéder à la page de lancement, pour ce faire nous aurons besoin de l’adresse ip du serveur. Pour l’obtenir nous devons entrer la commande “ip -a”. Vous verrez l’adresse ip du serveur à côté de “inet”. Entrer l’ip dans la barre de recherche de votre navigateur et la page de lancement devrait être afficher.

Il existe plusieurs serveur web nous allons en lister quelque un et voir leurs avantages et inconvénients:

Comparaison des Serveurs Web

Les serveurs web sont des éléments cruciaux de l'infrastructure Internet. Ils sont responsables de la distribution des pages web et du contenu vers les utilisateurs finaux. Il existe plusieurs serveurs web populaires, chacun ayant ses avantages et inconvénients. Voici une comparaison de quelques-uns d'entre eux :

Apache HTTP Server (Apache)

Avantages

1

Apache est polyvalent et peut être utilisé pour servir une grande variété de sites web, y compris les sites statiques et dynamiques.

Il dispose d'un vaste écosystème de modules, ce qui permet d'ajouter facilement des fonctionnalités.

Apache bénéficie d'une documentation complète et d'une communauté active, facilitant la résolution des problèmes.

Inconvénients

Apache peut être gourmand en ressources, surtout lors de la gestion de nombreuses connexions simultanées.

Nginx

Avantages

Nginx est reconnu pour ses excellentes performances, il est capable de gérer un grand nombre de connexions simultanées avec une faible utilisation de la mémoire.

La configuration de Nginx est simple et lisible.

Inconvénients

Bien que Nginx soit extensible, il peut parfois manquer de certains modules disponibles dans Apache.

Nginx est principalement un serveur web et nécessite un serveur d'application tiers pour exécuter des scripts dynamiques.

LiteSpeed

Avantages

LiteSpeed est réputé pour sa vitesse, notamment lors de la gestion de contenu dynamique.

Il propose des fonctionnalités de sécurité avancées, y compris la protection anti-DDoS.

LiteSpeed offre une interface utilisateur conviviale pour la configuration.

Inconvénients

LiteSpeed peut être coûteux par rapport à Apache et Nginx.

Bien que de plus en plus populaire, LiteSpeed n'a pas encore la même adoption qu'Apache ou nginx.

LiteSpeed, Nginx, ou Apache ?

- Si la performance est essentielle, Nginx et LiteSpeed sont d'excellents choix.

- Si la simplicité de configuration est importante, Nginx se distingue.

- Si vous avez besoin d'une grande flexibilité et d'une vaste communauté, Apache est un classique.

Le choix du serveur web dépendra des besoins spécifiques de votre projet, de vos compétences techniques et de votre budget. Il est souvent utile d'expérimenter différents serveurs web pour trouver celui qui correspond le mieux à vos exigences.

Maintenant nous allons mettre en place un DNS qui fera correspondre l'ip de notre serveur avec le nom de domaine local "dnsproject.prepa.com".

Commençons par installer Dnsmasq, c'est avec ça que nous allons mettre en place le DNS. Entrer la commande

"sudo apt-get install dnsmasq"

Maintenant que dnsmasq est installé nous allons modifier le fichier de configuration pour faire correspondre notre ip serveur a notre nom de domaine. Entrer la commande

"sudo nano /etc/dnsmasq.conf"

Aller tout en bas du fichier et ajouter

“address=/dnsproject.prepa.com/127.0.0.1”

Maintenant relancer dnsmasq avec la commande

“sudo systemctl restart dnsmasq”

Pour vous assurer que votre système utilise le DNS local, vous devrez ajouter une entrée dans le fichier `/etc/hosts` de votre système hôte. Ouvrez le fichier `/etc/hosts` avec les droits d'administration :

“sudo nano /etc/hosts”

Ajoutez la ligne suivante à la fin du fichier :

“127.0.0.1 dnsproject.prepa.com”

Enregistrez le fichier et quittez l'éditeur.

Vous pouvez maintenant tester la résolution DNS en utilisant la commande

“ ping dnsproject.prepa.com”

Comme vous pouvez le voir le ping fonctionne ce qui veut dire que vous pourrez accéder a la page Apache avec le nom de domaine.

Bien sûr, voici une documentation pour configurer un pare-feu en utilisant UFW (Uncomplicated Firewall) sur votre serveur principal de manière à ce que votre hôte puisse accéder à la page Apache par défaut, mais ne puisse plus pinguer votre serveur.

Nous allons maintenant mettre en place un pare-feu en utilisant ufw sur notre serveur pour faire en sorte que la page Apache soit accessible par défaut mais qu’il ne puisse plus être ping par l’hôte.

Commençons par installer ufw avec la commande:

“sudo apt-get install ufw”

Pour autoriser l'accès à la page Apache par défaut (port 80), nous allons utiliser la commande:

“sudo ufw allow 80/tcp”

Pour empêcher le serveur d'être pingé, nous allons bloquer les paquets ICMP. Pour faire ça nous allons entrer la commande

“sudo ufw deny proto icmp”

Maintenant nous allons activer UFW pour appliquer les règles que nous avons configurées :

“sudo ufw enable”

Maintenant vous pourrez accéder à la page Apache par défaut depuis l’hôte mais vous ne pourrez plus le ping.

Pour mettre en place un dossier partagé sur votre serveur Linux de manière à ce qu'il soit accessible par les autres machines virtuelles sur le réseau et visible dans un gestionnaire de fichiers en interface graphique, vous pouvez utiliser le protocole Samba. Voici comment procéder :

1. **Installer Samba** :

Assurez-vous que le service Samba est installé sur votre serveur Linux. Vous pouvez l'installer avec la commande suivante :

```

sudo apt update

sudo apt install samba

```

Ouvrez le fichier de configuration de Samba avec la commande:

“ sudo nano /etc/samba/smb.conf”

Et ajouter cette section dans le fichier:

“ [PartageCommun]

comment = Dossier partagé pour les membres du réseau

path = /chemin/vers/votre/dossier

browseable = yes

writeable = yes

guest ok = yes

create mask = 0777

directory mask = 0777”

Enregistrez les modifications et quittez.

Vous devez créer un utilisateur Samba qui aura accès au dossier partagé. Utilisez la commande suivante pour ajouter

un utilisateur Samba :

“sudo smbpasswd -a nom_utilisateur”

Redémarrez le service Samba pour appliquer les modifications de configuration :

“sudo systemctl restart smbd”

Maintenant allez dans le gestionnaire de tâche et entrez “smb://IP_DU_SERVEUR” dans la barres d’adresse.

Vous devriez maintenant avoir accès au dossier partagé.

Maintenant nous allons faire l’installation d’un certificat pour notre serveur web à l’aide d’open SSL.

Commencez par installer Open ssl avec la commande:

“sudo apt install openssl”

Maintenant passons à la l’installation de notre certificat SSL.

Utilisez la commande OpenSSL pour générer une clé privée et une demande de certificat :

“openssl req -newkey rsa:2048 -nodes -keyout nom_de_la_cle.key -out nom_de_la_demande.csr”

“nom_de_la_cle.key” C'est le nom du fichier de clé privée que vous souhaitez créer.

“nom_de_la_demande.csr” : C'est le nom du fichier de demande de certificat que vous souhaitez créer.

Pour auto-signer le certificat, utilisez la commande suivante :

“openssl x509 -req -in nom_de_la_demande.csr -signkey nom_de_la_cle.key -out nom_du_certificat.crt”

“nom_du_certificat.crt”: Le nom du fichier de certificat auto-signé que vous souhaitez créer.

Assurez-vous que le module SSL est activé :

“sudo a2enmod ssl”

Redémarrez Apache pour appliquer les modifications de configuration :

“sudo systemctl restart apache2”

Vous devez sûrement vous demander quelle est la différence entre un certificat auto signé et un fourni par un organisme extérieur ?

C’est simple les certificats SSL d'organismes extérieurs sont émis par des autorités de certification reconnues, tandis que les certificats auto-signés sont créés par nous même .

Le certificat apparaît comme non sécurisé pourquoi ?

Les certificats auto-signés apparaissent comme non sécurisés dans les navigateurs car ils ne sont pas vérifiés par une autorité de certification tiers.