DDWS

BY Ahmed Malik Ben elkadi

1/ comment installer le serveur Apache2

Ouvrez une fenêtre de terminal et utilisez la commande suivante pour mettre à jour les paquets du système :

sudo apt-get update

Utilisez la commande suivante pour installer Apache2 à partir des dépôts du système :

sudo apt-get install apache2

Une fois l'installation terminée,on peut vérifier si Apache2 est en cours d'exécution en ouvrant un navigateur Web et en accédant à l'adresse http://localhost. Si on voit la page d'accueil d'Apache2, cela signifie que le serveur est en cours d'exécution.

Si on veut modifier la configuration d'Apache2, on peut trouver les fichiers de configuration dans le répertoire **/etc/apache2**. Vous pouvez utiliser un éditeur de texte pour modifier ces fichiers et apporter les changements souhaités.

Pour démarrer ou arrêter le serveur Apache2, vous pouvez utiliser les commandes suivantes :

sudo systemctl start apache2 # pour démarrer le serveur

sudo systemctl stop apache2 # pour arrêter le serveur

3/ Diffèrent serveur web :

Il existe de nombreux serveurs Web différents, chacun avec ses propres avantages et inconvénients. Voici quelques-uns des serveurs Web les plus couramment utilisés :

Apache HTTP Server : C'est le serveur Web le plus populaire et le plus utilisé dans le monde. Il est open source, gratuit et facile à utiliser. Il prend en charge un large éventail de technologies Web, y compris PHP, Perl et Python, et offre une flexibilité et une performance élevées.

Microsoft IIS : C'est le serveur Web inclus dans les systèmes d'exploitation Windows. Il est facile à utiliser pour les utilisateurs Windows et prend en charge un large éventail de technologies Web, y compris ASP.NET et PHP.

NGINX : C'est un serveur Web open source qui se concentre sur la performance et l'efficacité. Il est souvent utilisé en conjonction avec Apache pour gérer les requêtes statiques et dynamiques de différentes manières.

Lighttpd : C'est un serveur Web open source léger et rapide, conçu pour gérer de grandes quantités de trafic. Il est souvent utilisé pour les sites Web à fort trafic et offre une bonne flexibilité et des performances élevées.

DDWS

Node.js : C'est un serveur Web open source basé sur JavaScript qui permet de créer des applications Web en utilisant un modèle événementiel. Il offre une excellente scalabilité et une performance élevée pour les applications en temps réel.

Chaque serveur Web a ses propres avantages et inconvénients, et le choix du meilleur serveur dépendra de vos besoins spécifiques. Par exemple, si vous avez besoin d'un serveur rapide et efficace pour gérer un grand volume de trafic, NGINX ou Lighttpd pourrait être une bonne option. Si vous avez besoin d'un serveur facile à utiliser et prenant en charge un large éventail de technologies, Apache ou Microsoft IIS pourrait être un bon choix. Si vous avez besoin d'un serveur pour des applications en temps réel, Node.js pourrait être une option intéressante.

Il est important d'effectuer des recherches approfondies pour choisir le serveur Web qui convient le mieux à nos besoins, en tenant compte de facteurs tels que la performance, la flexibilité, la facilité d'utilisation et la prise en charge des technologies utilisées dans votre application.

4/ DNS :

- Pour Installer un serveur DNS sur notre serveur Linux en utilisant un des paquets disponibles, comme bind9 ou dnsmasq. On utilise la commande suivante :

  sudo apt-get install bind9

- Puis on doit Configurer le serveur DNS en modifiant le fichier de configuration principal, généralement situé dans /etc/bind/named.conf. Dans ce fichier, on peut ajouter une zone pour notre domaine local dnsproject.prepa.com, ainsi qu'une entrée pour notre serveur qui fera correspondre l'adresse IP de notre serveur au nom de domaine local. La configuration peut ressembler à ceci :

```
zone "dnsproject.prepa.com" {
    type master;
    file "/etc/bind/zones/dnsproject.prepa.com.zone";
};
```

```
server {

    // Adresse IP de notre serveur
    address 192.168.1.100;
    // Nom de domaine local de notre serveur
    hostname dnsproject.prepa.com;
};
```

  Puis on redémarre notre serveur

5/ Nom de domains :

Pour obtenir un nom de domaine public, vous devez d'abord choisir le nom de domaine que vous souhaitez utiliser. Vous pouvez vérifier si le nom de domaine est disponible en utilisant un outil en ligne comme celui proposé par l'ICANN (Internet Corporation for Assigned Names and Numbers), l'organisme chargé de la gestion des noms de domaine sur Internet.

Une fois que vous avez choisi un nom de domaine disponible, vous pouvez l'acheter auprès d'un registrar, qui est une entreprise autorisée à enregistrer des noms de domaine pour les utilisateurs. Vous devrez payer une redevance annuelle pour maintenir votre nom de domaine enregistré.

Les extensions de nom de domaine, également appelées "domaines de premier niveau" ou TLD (Top Level Domain), peuvent être génériques (par exemple, .com, .org, .net) ou spécifiques à un pays ou une région (par exemple, .fr pour la France, .cn pour la Chine). Certains TLD peuvent avoir des restrictions sur leur utilisation, par exemple en termes de type de contenu ou de pays d'origine des utilisateurs. Vous devriez vous renseigner sur les restrictions spécifiques liées à l'extension de nom de domaine que vous souhaitez utiliser avant de l'acheter.

6/ JOB 6 :

Pour connecter notre hôte au nom de domaine local de notre serveur Apache, On doit d'abord configurer notre serveur Apache pour qu'il écoute sur le nom de domaine local que nous avons choisi. Cela implique généralement de modifier la configuration de notre serveur Apache pour qu'il écoute sur l'adresse IP locale de notre hôte et sur le port associé au nom de domaine local (généralement le port 80 pour HTTP et le port 443 pour HTTPS).

Ensuite, nous devons configurer notre hôte pour qu'il associe le nom de domaine local à l'adresse IP locale de notre serveur Apache. Cela peut être fait en modifiant le fichier hosts de notre hôte, qui est généralement situé dans le répertoire /etc/. On ajoute une ligne au fichier hosts en associant l'adresse IP locale de notre serveur Apache au nom de domaine local que nous avons choisi.

Une fois que notre serveur Apache est configuré pour écouter sur le nom de domaine local et que notre hôte est configuré pour associer ce nom de domaine à l'adresse IP locale de notre serveur Apache, votre page Apache devrait être accessible via ce nom de domaine en utilisant un navigateur web.

7/ Allez plus loins :

Les certificats SSL sont des fichiers numériques utilisés pour sécuriser les communications sur Internet en chiffrant les données transmises entre un serveur web et un navigateur web. Ils sont généralement émis par des autorités de certification externes, comme Symantec ou DigiCert, qui sont des organismes de confiance chargés de vérifier l'identité du propriétaire du site web avant d'émettre un certificat SSL.

Un certificat SSL auto-signé, en revanche, est un certificat SSL émis par le propriétaire du site web lui-même, sans vérification de l'identité par une autorité de certification externe. Ces certificats SSL auto-signés peuvent être utiles pour les tests et les développements locaux, mais ne sont généralement pas considérés comme sécurisés pour une utilisation en production car ils ne sont pas vérifiés par une autorité de certification externe.

DDWS

La principale différence entre les certificats SSL émis par des autorités de certification externes et les certificats SSL auto-signés est donc la fiabilité et la confiance accordées à ces certificats par les utilisateurs finaux. Les certificats SSL émis par des autorités de certification externes sont généralement considérés comme plus fiables car ils ont été vérifiés par une autorité de confiance, alors que les certificats SSL auto-signés ne sont pas vérifiés et peuvent être facilement contrefaits.

Pourquoi le ssl n’est pas securisé :

Si un certificat SSL apparaît comme non sécurisé dans un navigateur web, cela signifie généralement que le certificat n'a pas été émis par une autorité de certification externe reconnue par le navigateur. Les navigateurs web ont une liste de révocateurs de certificats intégrée, qui est utilisée pour vérifier si un certificat SSL est valide et émis par une autorité de certification externe de confiance. Si le certificat n'est pas émis par une autorité de certification externe reconnue par le navigateur, il peut être considéré comme non sécurisé et un avertissement peut être affiché pour informer l'utilisateur.

Les certificats SSL auto-signés sont souvent considérés comme non sécurisés par les navigateurs web car ils ne sont pas vérifiés par une autorité de certification externe. Si vous utilisez un certificat SSL auto-signé sur votre serveur web, il est possible que votre navigateur affiche un avertissement indiquant que le certificat n'est pas sécurisé. Dans ce cas, il est recommandé de remplacer le certificat SSL auto-signé par un certificat SSL émis par une autorité de certification externe reconnue pour éviter que les utilisateurs ne reçoivent un avertissement lorsqu'ils accèdent à votre site web.