Installer et configurer Ubuntu

Ubuntu est un système d'exploitation open-source basé sur le noyau Linux, largement utilisé pour les serveurs, les ordinateurs personnels et les machines virtuelles. Dans cet article, nous allons examiner comment installer et configurer Ubuntu dans une machine virtuelle, configurer les groupes et comptes utilisateurs, gérer les paquets, analyser le réseau et filtrer le trafic avec un pare-feu, surveiller l'activité du système, créer un tunnel sécurisé avec SSH et utiliser un client FTP.

Télécharger Ubuntu

Tout d'abord, vous devez télécharger l'ISO d'Ubuntu sur le site officiel. Il est recommandé de télécharger la dernière version stable. Ensuite, vous devez créer une nouvelle machine virtuelle dans votre logiciel de virtualisation. Lorsque vous créez une nouvelle machine virtuelle, vous devez sélectionner Ubuntu comme système d'exploitation invité et spécifier l'ISO que vous avez téléchargé comme source d'installation.

Configurer les paramètres de la machine virtuelle

Une fois que vous avez créé la machine virtuelle, vous devez configurer les paramètres de la machine virtuelle tels que la quantité de RAM, la taille du disque dur et le nombre de processeurs. Il est recommandé de donner à la machine virtuelle au moins 2 Go de RAM, 20 Go de disque dur et un processeur avec au moins deux cœurs.

Installer Ubuntu

Une fois que vous avez configuré les paramètres de la machine virtuelle, vous pouvez maintenant démarrer la machine virtuelle à partir de l'ISO que vous avez téléchargé. Lorsque vous démarrez la machine virtuelle, vous serez invité à installer Ubuntu. Suivez simplement les instructions à l'écran pour installer Ubuntu. Il est recommandé d'installer Ubuntu avec le bureau complet.

Configurer les groupes et comptes utilisateurs

Créer un nouveau groupe

Vous pouvez créer un nouveau groupe en utilisant la commande suivante :

sudo groupadd [nom_du_groupe]

Par exemple, pour créer un groupe appelé "devs", vous pouvez utiliser la commande suivante :

sudo groupadd devs

Ajouter un utilisateur à un groupe existant

Vous pouvez ajouter un utilisateur existant à un groupe existant en utilisant la commande suivante :

sudo usermod -a -G [nom_du_groupe] [nom_de_l_utilisateur]

Par exemple, pour ajouter un utilisateur appelé "john" au groupe "devs", vous pouvez utiliser la commande suivante :

sudo usermod -a -G devs john

Gérer les paquets

Ubuntu utilise le gestionnaire de paquets APT (Advanced Packaging Tool) pour installer, mettre à jour et supprimer les paquets. Voici quelques commandes utiles pour gérer les paquets :

Mettre à jour la liste des paquets disponibles :

sudo apt-get update

Mettre à jour les paquets installés :

sudo apt-get upgrade

Installer un nouveau paquet :

sudo apt-get install [nom_du_paquet]

Supprimer un paquet :

sudo apt-get remove [nom_du_paquet]

Analyser le réseau et filtrer le trafic avec un pare-feu

Dans Ubuntu, vous pouvez utiliser le pare-feu intégré, appelé ufw (Uncomplicated Firewall), pour filtrer le trafic réseau entrant et sortant et sécuriser votre système. Voici comment l'utiliser :

Vérifier que le pare-feu est activé :

sudo ufw status

Si le pare-feu est désactivé, vous pouvez l'activer en utilisant la commande suivante :

sudo ufw enable

Pour autoriser le trafic sur un port spécifique, utilisez la commande suivante :

sudo ufw allow [port]/[protocole]

Par exemple, pour autoriser le trafic sur le port 80 (HTTP) en utilisant le protocole TCP, vous pouvez utiliser la commande suivante :

sudo ufw allow 80/tcp

Pour bloquer le trafic sur un port spécifique, utilisez la commande suivante :

sudo ufw deny [port]/[protocole]

Par exemple, pour bloquer le trafic sur le port 22 (SSH) en utilisant le protocole TCP, vous pouvez utiliser la commande suivante :

sudo ufw deny 22/tcp

Pour autoriser le trafic provenant d'une adresse IP spécifique, utilisez la commande suivante :

sudo ufw allow from [adresse_IP]

Pour bloquer le trafic provenant d'une adresse IP spécifique, utilisez la commande suivante :

sudo ufw deny from [adresse_IP]

Pour supprimer une règle spécifique, utilisez la commande suivante :

sudo ufw delete [règle]

Par exemple, pour supprimer la règle qui autorise le trafic sur le port 80, utilisez la commande suivante :

sudo ufw delete allow 80/tcp

Pour bloquer tout le trafic entrant sauf celui qui est explicitement autorisé, utilisez la commande suivante :

sudo ufw default deny incoming

Pour autoriser tout le trafic sortant, utilisez la commande suivante :

sudo ufw default allow outgoing

Pour vérifier les règles du pare-feu, utilisez la commande suivante :

sudo ufw status

Surveiller l'activité du système

Il existe plusieurs outils que vous pouvez utiliser pour surveiller l'activité du système dans Ubuntu. Voici quelques-uns d'entre eux :

Top : Affiche les processus en cours d'exécution et leur utilisation de CPU.

sudo top

Htop : Une alternative plus avancée à la commande top.

sudo apt-get install htop sudo htop

Sysstat : Une suite d'utilitaires qui permet de surveiller les performances du système et d'enregistrer des statistiques sur une période de temps.

sudo apt-get install sysstat sar

Créer un tunnel sécurisé avec SSH

SSH (Secure Shell) est un protocole de communication sécurisé qui permet de se connecter à un serveur distant de manière sécurisée. Vous pouvez utiliser SSH pour créer un tunnel sécurisé qui permet de transférer des données entre deux machines de manière chiffrée. Voici comment créer un tunnel SSH :

Ouvrez un terminal sur la machine locale et entrez la commande suivante :

ssh -L [port_local]:[adresse_IP_distante]:[port_distante] [nom_utilisateur]@[adresse_IP_distante]

Par exemple, pour créer un tunnel qui relie le port local 8080 à l'adresse IP distante 192.168.0.100 sur le port 80, vous pouvez utiliser la commande suivante :

ssh -L 8080:192.168.0.100:80 user@192.168.0.100

Une fois que le tunnel SSH est créé, vous pouvez utiliser votre navigateur web local pour accéder à l'adresse IP distante en utilisant le port local que vous avez spécifié dans la commande précédente. Par exemple, vous pouvez accéder à http://localhost:8080 dans votre navigateur web pour accéder au serveur web distant.

Utiliser un client FTP

Il existe plusieurs clients FTP disponibles pour Ubuntu, tels que FileZilla et gFTP. Voici comment installer et utiliser FileZilla :

Installer FileZilla :

sudo apt-get update sudo apt-get install filezilla

Ouvrir FileZilla :

filezilla

Se connecter au serveur FTP distant en entrant l'adresse IP, le nom d'utilisateur et le mot de passe dans les champs appropriés.

Une fois connecté, vous pouvez utiliser FileZilla pour télécharger et téléverser des fichiers entre la machine locale et le serveur FTP distant en utilisant une interface graphique conviviale.