JOB2

Pourquoi effectuer ces mises à jour :

-Sécurité : Les mises à jour de sécurité corrigent les vulnérabilités qui pourraient être exploitées par des attaquants. En gardant votre système à jour, vous réduisez les risques de compromission de la sécurité.

-Stabilité : Les mises à jour peuvent également corriger des bugs et des problèmes de compatibilité qui pourraient causer des instabilités dans votre système.

-Nouvelles fonctionnalités : Les mises à jour peuvent également apporter de nouvelles fonctionnalités, améliorant ainsi l'expérience utilisateur et offrant de meilleures performances.

-Compatibilité logicielle : En maintenant votre système à jour, vous assurez sa compatibilité avec les nouvelles versions des logiciels que vous utilisez.

Mettre à jour la liste des paquets	apt update	Assure que vous avez la liste la plus à jour des paquets disponibles.
Mettre à jour les paquets installés	apt upgrade	Corrige les vulnérabilités de sécurité, les bugs et améliore la stabilité du système.
Installer de nouveaux paquets	apt dist-upgrade	Offre de nouvelles fonctionnalités et assure la compatibilité avec les nouvelles versions.
Nettoyer les fichiers temporaires	apt autoclean	Libère de l'espace disque en supprimant les fichiers temporaires inutiles.
Supprimer les paquets inutilisés	apt autoremove	Nettoie le système en supprimant les paquets qui ne sont plus nécessaires.

Job3

Étapes	Commandes	Description
Installer le serveur DHCP	sudo apt update	Mettons à jour la liste des paquets disponibles.
	sudo apt install isc-dhcp-server	Installons le serveur DHCP.
Configuration	sudo nano **/etc/default/isc-dhcp-server**	Ouvrons le fichier de configuration du serveur DHCP pour spécifier les interfaces à écouter. Modifions la ligne INTERFACESv4="" pour qu'elle soit **INTERFACESv4="ens33".**
Configurer le serveur DHCP	sudo nano **/etc/dhcp/dhcpd.conf** Ajoutons les lignes suivantes à la fin du fichier : **subnet 172.16.0.0 netmask 255.255.0.0 {** **range 172.16.1.10 172.16.1.50;** **option routers 172.16.1.1;** **option subnet-mask 255.255.0.0;** **}**	Éditons le fichier de configuration du serveur DHCP pour définir les paramètres de réseau et d'attribution d'adresses. Configurons le serveur DHCP pour attribuer des adresses de classe B.
Configurer une adresse IP fixe pour la machine hôte	sudo nano **/etc/network/interfaces**	Éditons le fichier de configuration réseau pour définir une adresse IP statique pour la machine hôte.

	Ajoutons ou modifions les lignes suivantes pour définir une adresse IP statique : **iface ens33 inet static** **address 172.16.1.2** **netmask 255.255.0.0** **gateway 172.16.1.1**	Assurons que la machine hébergeant le serveur DHCP a une adresse IP fixe.
Redémarrer les services réseau et DHCP	sudo systemctl restart networking sudo systemctl restart isc-dhcp-server	Redémarrons les services réseau pour appliquer les changements de configuration.

Job4

Étapes	Commandes	Description
Assurez-vous que votre système est à jour	sudo apt update	Met à jour la liste des paquets disponibles pour téléchargement.
	sudo apt upgrade	Met à jour tous les paquets installés sur le système.
Installez proFTPd et SSH	sudo apt install proftpd ssh	Installe les serveurs FTP (proFTPd) et SSH sur le système.
Configurez proFTPd	sudo nano **/etc/proftpd/proftpd.conf**	Ouvre le fichier de configuration de proFTPd dans l'éditeur de texte nano.
	Configurer proFTPd :	
	- **ServerName** "NomDuServeurFTP"	Définit le nom du serveur FTP.
	- ServerType standalone	Définit le type de serveur.
	- DefaultServer on	Définit ce serveur comme serveur par défaut.
	- Port 21	Définit le port utilisé par le serveur FTP.

	- PassivePorts 49152 65534	Définit les ports passifs utilisés pour les connexions de données.
	- **MaxInstances 1**	Limite le nombre maximal d'instances de serveur.
	- DefaultRoot ~	Définit le répertoire racine par défaut pour les utilisateurs.
	- RequireValidShell off	Autorise l'accès FTP aux utilisateurs sans shell valide.
	- <Global>	Ouverture de la section globale des directives de configuration.
	DenyAll	Refuse toutes les commandes FTP par défaut.
	- </Global>	Fermeture de la section globale des directives de configuration.
	- <Limit LOGIN>	Ouverture de la section de limitation pour les connexions.
	AllowUser laplateforme	Autorise uniquement l'utilisateur "laplateforme" à se connecter.
	- </Limit>	Fermeture de la section de limitation pour les connexions.
Créez l'utilisateur "laplateforme" et définissez le mot de passe	**sudo useradd -m laplateforme**	Crée un nouvel utilisateur nommé "laplateforme" avec un répertoire personnel dans /home.
	sudo passwd laplateforme	Définit un mot de passe pour l'utilisateur "laplateforme".
Redémarrez proFTPd pour appliquer les modifications	**sudo systemctl restart proftpd**	Redémarre le service proFTPd pour appliquer les modifications de configuration.
Configurez SSH pour SFTP	**sudo nano /etc/ssh/sshd_config**	Ouvre le fichier de configuration SSH dans l'éditeur de texte nano.
	- **Subsystem sftp internal-sftp**	Définit le sous-système SFTP utilisant l'implémentation interne.

Redémarrez le service SSH pour appliquer les modifications	**sudo systemctl restart sshd**	Redémarre le service SSH pour appliquer les modifications de configuration.

Job5

Étape	Description	Commandes/Codes
1. Installation du Serveur DNS	- On installe un serveur DNS tel que BIND sur notre première machine.	**sudo apt-get install bind9**
2. Configuration du Servheur DNS	- On ajoute une zone pour notre domaine dans le fichier named.conf.local.	**sudo nano /etc/bind/named.conf.local**
		zone "ftp.com" { **type master;** **file "/etc/bind/db.ftp.com";** **};**
	- On crée un nouveau fichier de zone nommé db.ftp.com dans /etc/bind/ et on spécifie les enregistrements DNS appropriés.	**sudo nano /etc/bind/db.ftp.com**

	$TTL 604800 **@ IN SOA dns.ftp.com. admin.ftp.com. (** **2024033001 ; Serial** **604800 ; Refresh** **86400 ; Retry** **2419200 ; Expire** **604800) ; Negative Cache TTL** **;** **@ IN NS dns.ftp.com.** **dns IN A 172.16.1.10**	
3. Redémarrage du Service DNS	- On redémarre le service BIND pour appliquer les changements de configuration.	**sudo systemctl restart bind9**

*sur la machine du client,dans le fichier /etc/resolv.conf on ajoute l'adresse IP du serveur DNS auquel le système d'exploitation doit faire appel pour résoudre les noms de domaine.

nameserver 172.16.0.2

JOB6

Test de la connexion SFTP :

On teste la connexion SFTP en utilisant les identifiants fournis. On utilise la commande SFTP dans notre terminal pour cela.

Par exemple :

sftp laplateforme@dns.ftp.com

JOB7

1. Modifier le fichier de configuration SSH :

sudo nano /etc/ssh/sshd_config

- Ajoutons les lignes suivantes à la fin du fichier :

Match User laplateforme

PasswordAuthentication yes

2. Changer le port :

Port 6500

3. Éviter les connexions anonymes :

PermitEmptyPasswords no

PermitRootLogin no

4. Enregistrons les modifications et redémarrons le service SSH :

sudo systemctl restart sshd