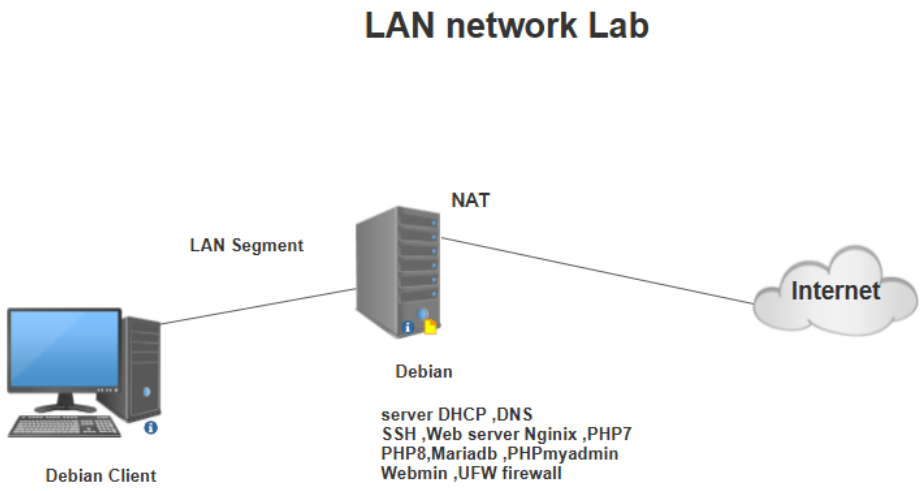
Introduction du sujet

À bord de l'USS Enterprise-D, la Fédération des Planètes Unies cherche à optimiser le développement de ses sites web stellaires en équipant ses ingénieurs de machines virtuelles (VM) via le Holodeck. L'objectif est de déployer un environnement composé de deux machines virtuelles sous Debian : une VM serveur et une VM cliente. La VM serveur sera responsable de la gestion des services réseau essentiels, tandis que la VM cliente servira à tester les sites web développés dans cet environnement.



La problématique

Il s'agit de mettre en place deux machines virtuelles avec des configurations spécifiques :

VM Serveur :

OS : Debian sans interface graphique.

Configuration : 2 Go de RAM, 2 vCPU, 32 Go de disque.

Réseau : 2 cartes réseaux (une WAN et une LAN).

Rôles : serveur DHCP, DNS, Web (Nginx), base de données (MariaDB), LDAP, et FTP (en SSL/TLS).

VM Cliente :

OS : Debian avec interface graphique.

Configuration : 2 Go de RAM, 2 vCPU, 16 Go de disque.

Réseau : connectée au LAN de la VM serveur, avec un navigateur web pour tester les sites.

La VM serveur doit assumer plusieurs rôles réseau critiques, notamment DHCP et DNS, tout en supportant des services web sécurisés.

Objectifs spécifiques :

Le serveur web doit être configuré avec Nginx en HTTPS.

PHP doit être installé en double version (7.x et 8.x), avec un site distinct pour chaque version :

www8.starfleet.lan pour PHP 8.

www7.starfleet.lan pour PHP 7.

php.starfleet.lan pour l'administration de bases de données via phpMyAdmin.

admin.starfleet.lan pour la gestion administrative de la VM.

Mise en place d’un serveur FTP sécurisé (SSL/TLS) pour gérer les transferts de fichiers vers le serveur web.

Les utilisateurs du serveur web doivent être authentifiés via un annuaire LDAP.

Aucun compte ne doit être utilisé, conformément aux règles de sécurité de Starfleet.

Mise en place d'un pare-feu restrictif, n'autorisant que les ports nécessaires aux services fonctionnels.

Les contraintes supplémentaires :

Pare-feu : Configurer un pare-feu pour autoriser uniquement les ports requis par les services (FTP, DNS, DHCP, Nginx, etc.).

Certificats SSL : Générer et déployer un certificat SSL unique pour le serveur web et le serveur FTP.

les étapes de configuration du LAN segment dans VMware Workstation

Étape	Description	
1. Ouvrir VMware Workstation	Lancez VMware Workstation sur votre machine hôte.	
2. Accéder aux paramètres réseau de la machine virtuelle	Créez ou sélectionnez une machine virtuelle.	
	Clic droit sur la VM, sélectionnez "Paramètres" (ou "Settings").	
	Dans l'onglet Matériel (Hardware), cliquez sur "Adaptateur réseau" (Network Adapter).	
3. Configurer l'adaptateur réseau	Cochez la case "Personnalisé : réseau spécifique" (Custom: specific virtual network).	

	Sélectionnez "Segment de réseau" (LAN Segment) dans la liste déroulante.	
	Cliquez sur "Segment de réseau", puis "Configurer les segments de réseau" (Configure LAN Segments).	
4. Créer un nouveau LAN segment	Dans la fenêtre de configuration des segments de réseau, cliquez sur "Ajouter" (Add).	
	Donnez un nom au segment (par ex. "LAN-Segment1").	
	Cliquez sur OK pour valider.	
5. Connecter les autres machines virtuelles au LAN segment	Répétez les étapes précédentes pour chaque machine virtuelle à connecter.	
	Assurez-vous de sélectionner le même segment de réseau pour toutes les VMs.	
6. Démarrer les machines virtuelles	Démarrez toutes les machines configurées sur le même segment.	
	Elles seront connectées entre elles via un réseau isolé.	
Vérification	Testez la connectivité entre les machines avec des outils comme ping ou netstat pour vérifier la bonne connexion.	

les étapes pour attribuer une adresse IP fixe à l'interface réseau ens36 sous Debian

Étape	Description	
1. Identifier l'interface réseau	Utilisez la commande suivante pour vérifier le nom exact de l'interface réseau :	
	bash ip addr show	

2. Configurer une IP statique pour ens36	Ouvrez le fichier de configuration des interfaces réseau :	
	bash nano /etc/network/interfaces	
	Ajoutez la configuration statique pour ens36 :	
	bash auto ens36 iface ens36 inet static address 192.168.10.1 netmask 255.255.255.0 gateway 192.168.10.254	
	Explication des paramètres :	
	- auto ens36 : Active automatiquement l'interface au démarrage.	
	- iface ens36 inet static : Spécifie que l'adresse IP est en mode statique.	
	- address : L'adresse IP à attribuer.	
	- netmask : Masque de sous-réseau.	
	- gateway : La passerelle par défaut (peut être omise si le réseau est isolé).	
3. Appliquer la configuration	Redémarrez le service réseau pour appliquer les modifications :	
	bash systemctl restart networking	
	Si cela ne fonctionne pas, redémarrez le système.	
4. Vérifier l'adresse IP	Vérifiez que l'interface ens36 a bien reçu l'adresse IP statique :	
	bash ip addr show ens36	
	Vous devriez voir la configuration suivante dans la sortie :	
	sql 3: ens36: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000 inet 192.168.10.1/24 brd 192.168.10.255 scope global ens36	

les étapes d'installation et de configuration du serveur SSH avec l'adresse IP `192.168.10.1`.

Étape	Commande/Action	Description
1. Mettre à jour le système	apt update && apt upgrade	Met à jour les paquets du système avant toute installation.
2. Installer le serveur SSH	apt install openssh-server	Installe OpenSSH Server sur le serveur Debian.
3. Vérifier l'état du service SSH	systemctl status ssh	Vérifie si le service SSH est actif et en cours d'exécution.
4. Démarrer le service SSH	systemctl start ssh	Démarre le service SSH si nécessaire.
5. Activer SSH au démarrage	systemctl enable ssh	Assure que SSH se lance automatiquement au démarrage du système.
6. Configurer le serveur SSH	nano /etc/ssh/sshd_config	Modifie le fichier de configuration SSH.

- Changer le port SSH	Dans /etc/ssh/sshd_config, modifier : Port 2222	Change le port SSH (optionnel).
- Désactiver la connexion root	Dans /etc/ssh/sshd_config, ajouter/modifier : PermitRootLogin no	Désactive la connexion en tant que root pour des raisons de sécurité.
- Restreindre l'accès à certains utilisateurs	Dans /etc/ssh/sshd_config, ajouter : AllowUsers utilisateur	Limite les connexions SSH à des utilisateurs spécifiques.
7. Redémarrer le service SSH	systemctl restart ssh	Applique les modifications en redémarrant SSH.
8. Ouvrir le port SSH dans le pare-feu	Pour le port 22 : ufw allow ssh ou pour un autre port : ufw allow 2222/tcp	Ouvre le port SSH dans le pare-feu si nécessaire.
9. Installer le client SSH	apt install openssh-client	Installe le client SSH sur la machine cliente si ce n'est pas déjà fait.

10. Générer une clé SSH	ssh-keygen -t rsa -b 4096	Génère une paire de clés SSH (public/privé) sur la machine cliente.
11. Copier la clé publique sur le serveur	ssh-copy-id utilisateur@192.168.10.1	Copie la clé publique vers le serveur pour permettre l'authentification par clé.
12. Se connecter au serveur via SSH	ssh utilisateur@192.168.10.1 ou ssh utilisateur@192.168.10.1 -p 2222 (si port personnalisé)	Se connecte au serveur SSH depuis le client.
13. Configurer le fichier ~/.ssh/config (facultatif)	Créer ou modifier le fichier ~/.ssh/config et ajouter des alias pour simplifier les connexions.	Facilite la connexion à plusieurs serveurs avec des alias dans un fichier config.

les étapes pour installer et configurer un serveur DHCP pour une interface réseau spécifique (ens36) sous Linux en utilisant ISC DHCP Server,

Étape	**Description**	
1. Installation du	Mettez à jour les paquets et installez ISC DHCP Server :	

serveur DHCP	bash apt-get update apt-get install isc-dhcp-server	
2. Configurer le serveur DHCP pour une seule carte réseau (ens36)	**Configurer l'interface réseau** : Modifiez le fichier /etc/default/isc-dhcp-server pour que DHCP fonctionne uniquement sur ens36 :	
	bash nano /etc/default/isc-dhcp-server	
	Remplacez la ligne :	
	bash INTERFACESv4=""	
	Par :	
	bash INTERFACESv4="ens36"	
3. Configurer la plage d'adresses IP (subnet)	**Modifier la configuration du sous-réseau** : Éditez le fichier /etc/dhcp/dhcpd.conf pour définir la plage d'adresses IP distribuées par DHCP sur ens36 :	
	bash nano /etc/dhcp/dhcpd.conf	
	Ajoutez la configuration suivante :	

	bash
	 subnet 192.168.10.0 netmask 255.255.255.0 {
	 range 192.168.10.100 192.168.10.200;
	 option routers 192.168.10.1;
	 option subnet-mask 255.255.255.0;
	 option broadcast-address 192.168.10.255;
	 }	

	Explications :	
	- Plage d'adresses : 192.168.10.100 - 192.168.10.200	
	- Routeur : 192.168.10.1	
	- Masque de sous-réseau : 255.255.255.0	
4. Redémarrer le serveur DHCP	Après avoir modifié les fichiers de configuration, redémarrez le serveur DHCP :	
	bash systemctl restart isc-dhcp-server	
5. Vérifier le statut du serveur DHCP	Vérifiez que le serveur DHCP fonctionne et qu'il écoute bien sur ens36 :	
	bash systemctl status isc-dhcp-server	
6. Tester la configuration DHCP	**Tester sur une autre machine** : Connectez une autre machine virtuelle au même LAN segment et configurez-la pour obtenir une adresse IP via DHCP. Vérifiez qu'elle a reçu une adresse IP dans la plage définie à l'aide de la commande ifconfig ou ip addr.	
Remarques	Si ens36 est connectée à un LAN segment, toutes les autres machines virtuelles sur ce segment recevront des adresses IP via ce serveur DHCP.	
	Le serveur DHCP n'affectera que ens36, les autres interfaces réseau ne seront pas concernées.	

les étapes pour tester la connectivité d'une machine virtuelle dans le réseau `ens36`

Étape	Description	
1. Vérifier l'attribution d'une adresse IP via DHCP	Configurez une machine virtuelle sur le même réseau ens36 pour obtenir une adresse IP via DHCP.	
	Exécutez la commande suivante sur la machine cliente :	
	bash dhclient -v ens36	
	Cela permet à la machine cliente de demander une adresse IP au serveur DHCP. Vérifiez qu'elle obtient une IP dans la plage configurée (ex. 192.168.10.100 - 192.168.10.200).	
2. Tester la connectivité entre les machines	Utilisez la commande ping pour tester la connectivité entre la machine avec ens36 (l'hôte DHCP) et une autre machine sur le même réseau LAN segment :	
	bash ping 192.168.10.x # Adresse IP d'une autre machine sur le réseau	
	Cela permet de vérifier si les machines peuvent se joindre sur le réseau local.	

les étapes pour configurer un serveur DNS pour le domaine `starfleet.lan` sur Debian avec Bind9,

Étape	Description	
1. Installer Bind9	Installez Bind9 et ses utilitaires :	
	bash apt update apt install bind9 bind9utils bind9-doc	
2. Configurer Bind9	**Configurer les Options Globales** :	
	Modifiez le fichier /etc/bind/named.conf.options pour définir les options globales :	
	bash nano /etc/bind/named.conf.options	
	Exemple de configuration :	

	bash
	 options {
	 directory "/var/cache/bind";
	 forwarders { 8.8.8.8; 8.8.4.4; };
	 dnssec-validation auto;
	 listen-on { 192.168.10.1; };
	 allow-query { 192.168.10.0/24; };
	 allow-recursion { 192.168.10.0/24; };
	 }	

3. Configurer la Zone DNS	**Créer le fichier de zone** :	
	Créez un fichier pour la zone starfleet.lan :	
	bash nano /etc/bind/db.starfleet.lan	
	Exemple de fichier de zone :	
	bash ; BIND data file for starfleet.lan $TTL 604800 @ IN SOA ns.starfleet.lan. admin.starfleet.lan. (1 ; Serial 604800 ; Refresh 86400 ; Retry 2419200 ; Expire 604800) ; Negative Cache TTL @ IN NS ns.starfleet.lan. @ IN A 192.168.10.1 ns IN A 192.168.10.1	
4. Inclure la Zone DNS dans la Configuration	**Modifier le fichier** :	
	Éditez /etc/bind/named.conf.local pour inclure la nouvelle zone DNS :	
	bash nano /etc/bind/named.conf.local	
	Ajoutez la configuration suivante :	

	bash
	 zone "starfleet.lan" {
	 type master;
	 file "/etc/bind/db.starfleet.lan";
	 };	

5. Redémarrer Bind9	Redémarrez le service Bind9 pour appliquer les modifications :	
	bash systemctl restart bind9	
	Activez Bind9 au démarrage :	
	bash systemctl enable bind9	
6. Vérifier la Configuration	**Vérifiez la configuration de Bind9** :	
	bash named-checkconf	
	Vérifiez les fichiers de zone :	
	bash named-checkzone starfleet.lan /etc/bind/db.starfleet.lan	

7. Tester la Résolution DNS	Testez la résolution DNS avec la commande dig :	
	bash dig @192.168.10.1 starfleet.lan	
	Ou avec nslookup depuis une machine cliente :	
	bash nslookup starfleet.lan 192.168.10.1	
8. Configurer les Clients pour Utiliser le Serveur DNS	**Pour les clients DHCP** :	
	Modifiez /etc/dhcp/dhcpd.conf pour que le serveur DHCP fournisse l'IP du serveur DNS :	
	bash option domain-name-servers 192.168.10.1;	
	Redémarrez le service DHCP :	
	bash systemctl restart isc-dhcp-server	

les étapes pour configurer le client DNS sur Debian afin d'utiliser un serveur DNS local sur l'interface `ens36` avec l'IP `192.168.10.1`

Étape	Description	
1. Modifier /etc/resolv.conf	**Ouvrir le fichier resolv.conf** :	
	bash nano /etc/resolv.conf	
	Ajouter l'adresse IP du serveur DNS :	
	Supprimez les lignes existantes si nécessaire et ajoutez :	
	bash nameserver 192.168.10.1	
	Enregistrer et fermer le fichier :	
	- Enregistrer : Ctrl + O, puis Entrée	
	- Quitter : Ctrl + X	
2. Empêcher la réinitialisation de /etc/resolv.conf	**Rendre le fichier immuable** :	
	Pour éviter que le fichier soit modifié automatiquement :	
	bash chattr +i /etc/resolv.conf	
	Remarque : Si vous souhaitez modifier à nouveau le fichier, utilisez la commande suivante pour supprimer l'attribut immuable :	
	bash chattr -i /etc/resolv.conf	
3. Redémarrer les services réseau	Pour appliquer les changements de configuration DNS, redémarrez les services réseau :	

(facultatif)	bash systemctl restart networking	
4. Vérification de la configuration DNS	**Utiliser la commande dig** :	
	Pour tester si la configuration fonctionne :	
	bash dig google.com	
	Vous devriez voir que la requête DNS passe par 192.168.10.1.	
	Utiliser nslookup :	
	bash nslookup google.com	
	La sortie devrait indiquer que le serveur DNS utilisé est 192.168.10.1.	

Voici les étapes pour installer Nginx depuis les sources, présentées en format tableau :

Étape	**Description**	

Mettre à jour les sources APT	**Mettre à jour les listes de paquets** :	
	bash apt update	
Préparer l'environnement	**Installer les paquets nécessaires** :	

	bash
	  apt update
	  apt install -y build-essential libpcre3 libpcre3-dev zlib1g zlib1g-dev libssl-dev	

Télécharger Nginx	**Télécharger la version source de Nginx** :	
	bash wget http://nginx.org/download/nginx-1.23.4.tar.gz	
	Extraire l'archive :	
	bash tar -zxvf nginx-1.23.4.tar.gz cd nginx-1.23.4	
Configurer, Compiler et Installer Nginx	**Configurer Nginx avec les modules requis** :	
	bash ./configure --with-http_ssl_module --with-pcre --with-zlib=/usr/include --with-openssl=/usr/include	
	Compiler le code source :	
	bash make	
	Installer Nginx :	
	bash make install	
	Nginx sera installé dans /usr/local/nginx.	

la configuration pour installer et configurer Nginx, PHP, MariaDB, et les services DHCP/DNS :

Étape	**Description**	
1. Configurer Nginx pour HTTPS	Générer des certificats SSL auto-signés :	

	bash
	  mkdir -p /usr/local/nginx/ssl
	  openssl req -new -x509 -days 365 -nodes -out /usr/local/nginx/ssl/nginx.crt -keyout /usr/local/nginx/ssl/nginx.key	

	Modifier la configuration Nginx :	
	bash nano /usr/local/nginx/conf/nginx.conf	
	Ajouter la configuration des serveurs.	
2. Redémarrer Nginx	Pour appliquer les modifications :	
	bash /usr/local/nginx/sbin/nginx -s reload	
3. Installer PHP 7.4 et 8.1	Ajouter le dépôt PHP :	
	``bash	
	apt install -y lsb-release apt-transport-https ca-certificates	
	wget -qO - https://packages.sury.org/php/apt.gpg	

4. Installer MariaDB	Installer MariaDB :	
	bash apt install -y mariadb-server mariadb-client	
	Sécuriser l'installation :	
	bash mysql_secure_installation	
5. Configurer les Sites Web	Créer des répertoires pour chaque site :	
	bash mkdir -p /var/www/www8.starfleet.lan mkdir -p /var/www/www7.starfleet.lan mkdir -p /var/www/php.starfleet.lan mkdir -p /var/www/admin.starfleet.lan	
	Ajouter des fichiers index.php ou index.html pour tester.	
6. Configurer le Serveur DHCP/DNS	Configurer DHCP :	
	bash nano /etc/dhcp/dhcpd.conf	
	Exemple de configuration :	
	conf subnet 192.168.10.0 netmask 255.255.255.0 { range 192.168.10.100 192.168.10.200; option routers 192.168.10.1; option domain-name-servers 8.8.8.8, 8.8.4.4; option domain-name "starfleet.lan"; }	
	Configurer le serveur DNS (bind9) :	
	bash nano /etc/bind/db.starfleet.lan	
	Exemple de zone DNS :	
	conf zone "starfleet.lan" { type master; file "/etc/bind/db.starfleet.lan"; }	
7. Redémarrer les Services DHCP/DNS	Redémarrer les services :	
	bash systemctl restart isc-dhcp-server systemctl restart bind9	
8. Tester la Configuration	Accédez aux sites :	
	https://www8.starfleet.lan	
	Testez les services DNS/DHCP avec des résolutions de noms et des attributions d'IP.	

la configuration pour l'installation et la configuration de phpMyAdmin

Étape	Description	
1. Télécharger phpMyAdmin	Téléchargez phpMyAdmin manuellement :	
	bash cd /usr/share/ wget https://www.phpmyadmin.net/downloads/phpMyAdmin-latest-all-languages.tar.gz tar xzf phpMyAdmin-latest-all-languages.tar.gz mv phpMyAdmin-*-all-languages phpmyadmin rm phpMyAdmin-latest-all-languages.tar.gz	
2. Configurer phpMyAdmin	Créez le dossier temporaire et configurez les permissions :	
	bash mkdir /usr/share/phpmyadmin/tmp chown -R www-data:www-data /usr/share/phpmyadmin/tmp	
3. Créer un fichier de configuration Nginx pour phpMyAdmin	Créez un fichier dédié à phpMyAdmin :	
	bash nano /usr/local/nginx/conf/phpmyadmin.conf	
	Ajoutez la configuration suivante :	

	nginx
	 server {
	 listen 80;
	 server_name your_domain_or_ip;
	 root /usr/share/phpmyadmin;
	 index index.php index.html index.htm;
	 location / { try_files $uri $uri/ =404; }
	 location ~ \.php$ {
	 fastcgi_pass unix:/var/run/php/php7.4-fpm.sock;
	 fastcgi_index index.php;
	 fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
	 include fastcgi_params; }
	 location ~ /\.ht { deny all; }
	 }	

4. Inclure la configuration phpMyAdmin dans Nginx	Ouvrez et modifiez le fichier principal de Nginx :	
	bash nano /usr/local/nginx/conf/nginx.conf	
	Ajoutez la ligne :	
	nginx include /usr/local/nginx/conf/phpmyadmin.conf;	
5. Recharger Nginx	Rechargez Nginx pour appliquer les modifications :	
	bash /usr/local/nginx/sbin/nginx -s reload	
6. Accéder à phpMyAdmin	Ouvrez votre navigateur à l'adresse suivante :	
	http://your_domain_or_ip/phpmyadmin	
	Vous devriez voir l'interface de connexion de phpMyAdmin.	

La configuration pour la gestion des utilisateurs MySQL

Étape	Commande SQL	
1. Créer l'utilisateur	CREATE USER 'alaa'@'%' IDENTIFIED BY 'alaa';	
2. Accorder des privilèges	GRANT ALL PRIVILEGES ON *.* TO 'alaa'@'%';	
3. Appliquer les changements	FLUSH PRIVILEGES;	
4. Vérifier les utilisateurs	SELECT User, Host FROM mysql.user;	

les étapes de l'installation, de la configuration et des tests du serveur LDAP et de l'utilisateur.

Étape	**Commande/Action**	
Étape 1 : Installation du serveur LDAP		
1.1 Installer slapd et ldap-utils	apt update	
	apt install slapd ldap-utils	
1.2 Reconfigurer slapd (si besoin)	dpkg-reconfigure slapd	
Configuration	- Ne pas omettre la configuration (choisir "Non")	
	- Nom de domaine : starfleet.lan	
	- Organisation : Starfleet	
	- Mot de passe administrateur LDAP	
	- Backend de base de données : MDB	
	- Ne pas autoriser les anciennes bases de données	
1.3 Vérifier l'installation	ldapsearch -x -LLL -H ldap:/// -b dc=starfleet,dc=lan	
Étape 2 : Ajouter un utilisateur LDAP "toutou yaya"		
2.1 Configurer le schéma LDAP	Créer le fichier toutouyaya.ldif avec le contenu LDAP spécifié	
Générer un mot de passe crypté	slappasswd	
2.2 Ajouter l'utilisateur LDAP	ldapadd -x -D "cn=admin,dc=starfleet,dc=lan" -W -f toutouyaya.ldif	
2.3 Vérifier l'ajout de l'utilisateur	ldapsearch -x -LLL -b "dc=starfleet,dc=lan" uid=toutouyaya	

Étape 3 : Configuration de la machine cliente pour utiliser LDAP		
3.1 Installer les paquets nécessaires	apt update	
	apt install libnss-ldap libpam-ldap ldap-utils nscd	
Pendant l'installation	Fournir l'URI LDAP, la base de recherche, la version du protocole et ne pas ajouter d'utilisateurs LDAP localement	
3.2 Configurer LDAP dans nsswitch.conf	Modifier /etc/nsswitch.conf :	
	passwd: compat ldap	
	group: compat ldap	
	shadow: compat ldap	
3.3 Configurer PAM pour LDAP	Ajouter dans /etc/pam.d/common-session :	
	session required pam_mkhomedir.so skel=/etc/skel umask=077	
3.4 Redémarrer le service NSS	systemctl restart nscd	
Étape 4 : Tester la connexion avec l'utilisateur LDAP		
Tester la connexion	ssh toutouyaya@client_machine	

la procédure pour l'installation et la configuration de vsftpd avec SSL/TLS :

Étape	**Commande/Action**	
1. Installer vsftpd	apt-get install vsftpd	
2. Configuration de vsftpd pour SSL		
2.1 Éditer le fichier de configuration	nano /etc/vsftpd.conf	
2.2 Paramètres pour activer FTPS	Ajouter/modifier les lignes suivantes :	
	ssl_enable=YES	
	rsa_cert_file=/etc/ssl/certs/starfleet.lan.crt	
	rsa_private_key_file=/etc/ssl/private/starfleet.lan.key	
2.3 Activer TLS uniquement	ssl_tlsv1=YES	
	ssl_sslv2=NO	
	ssl_sslv3=NO	

2.4 Configurer les connexions FTP sécurisées	require_ssl_reuse=NO	
	ssl_ciphers=HIGH	
2.5 Chroot du dossier web	chroot_local_user=YES	
	allow_writeable_chroot=YES	
3. Redémarrer vsftpd	systemctl restart vsftpd	
4. Chroot du dossier web pour FTP		
4.1 Limiter l'accès utilisateur	S'assurer que chroot_local_user=YES est activé dans /etc/vsftpd.conf	
4.2 Configurer les utilisateurs	S'assurer que les utilisateurs FTP ont accès uniquement à leurs répertoires personnels ou à /var/www	

les étapes pour installer et configurer FileZilla sur Debian ainsi que pour se connecter à un serveur FTPS

Étape	**Commande/Action**	
1. Mettre à jour les listes de paquets	apt-get update	
2. Installer FileZilla	apt-get install filezilla	
3. Lancer FileZilla	Vous pouvez lancer FileZilla via le menu des applications ou avec la commande :	
	filezilla	
4. Configurer FileZilla pour FTPS		
4.1 Accéder au gestionnaire de sites	- Ouvrez FileZilla	
	- Cliquez sur **Fichier** dans la barre de menu	
	- Sélectionnez **Gestionnaire de sites**	
4.2 Ajouter un nouveau site	- Cliquez sur **Nouveau site**	
	- Entrez un nom pour le site dans le champ **Nom du site**	
4.3 Configurer les paramètres de connexion	- **Hôte** : Entrez l'adresse du serveur FTP (ex. 192.168.10.1)	
	- **Protocole** : Sélectionnez **FTP - File Transfer Protocol**	
	- **Chiffrement** : Sélectionnez **Utiliser explicitement FTP sur TLS** (pour une connexion sécurisée via TLS)	
	- **Type de connexion** : Sélectionnez **Normal**	
	- **Utilisateur** : Entrez votre nom d'utilisateur	
	- **Mot de passe** : Entrez votre mot de passe	
5. Se connecter au serveur	Cliquez sur **Connexion** pour vous connecter au serveur FTP.	

les étapes pour configurer UFW afin de protéger et autoriser les services nécessaires sur un serveur Debian.

Voici le processus pour configurer UFW (Uncomplicated Firewall) en tableau :		
Étape	**Description**	**Commande**
1. Identifier les ports nécessaires	Ports requis pour les services installés :	-
	- SSH (22)	
	- HTTP (80)	
	- HTTPS (443)	
	- FTP (21) + FTPS (990)	
	- DNS (53)	
	- MariaDB (3306)	
	- DHCP (67 UDP)	
	- PHPMyAdmin (HTTP/HTTPS)	
2. Installer UFW	Installer UFW sur le serveur Debian.	apt install ufw
3. Configurer UFW pour les services	Configurer UFW pour autoriser les ports nécessaires.	-
3.1 Autoriser DNS (Port 53 - TCP/UDP)	Autoriser les connexions DNS sur l'interface ens36 pour les protocoles TCP et UDP.	ufw allow in on ens36 to any port 53 proto tcp
		ufw allow in on ens36 to any port 53 proto udp
3.2 Autoriser DHCP (Port 67 - UDP)	Autoriser le serveur DHCP à écouter sur le port 67 pour la distribution des adresses IP.	ufw allow in on ens36 to any port 67 proto udp
3.3 Autoriser LDAP (Port 389 - TCP)	Autoriser les connexions LDAP sur l'interface ens36.	ufw allow in on ens36 to any port 389 proto tcp

3.4 Autoriser HTTP (Port 80 - TCP)	Autoriser l'accès HTTP sur l'interface ens36.	ufw allow in on ens36 to any port 80
3.5 Autoriser HTTPS (Port 443 - TCP)	Autoriser l'accès HTTPS sur l'interface ens36.	ufw allow in on ens36 to any port 443
3.6 Autoriser SSH (Port 22 - TCP)	Autoriser les connexions SSH sur l'interface ens36.	ufw allow in on ens36 to any port 22
3.7 Autoriser FTP (Port 21 - TCP)	Autoriser les connexions FTP sur l'interface ens36.	ufw allow in on ens36 to any port 21
3.8 Autoriser MariaDB (Port 3306 - TCP)	MariaDB est accessible localement (127.0.0.1). Pas de règle spécifique nécessaire pour l'accès distant via UFW.	-
3.9 Autoriser BIND9 RNDC (Port 953 - TCP)	Si BIND9 est utilisé, le contrôle RNDC est limité à localhost (127.0.0.1). Pas de règle nécessaire pour le réseau.	-
3.10 X11 Forwarding (Port 6010 - TCP)	Port utilisé localement pour le forwarding X11, pas besoin de règle spécifique pour le réseau.	-
4. Vérifier le statut des règles UFW	Vérifiez les règles appliquées à UFW.	ufw status verbose