PAUL-ANDRE LE MOUEL
BTS SIO
OPTION SISR

NET SECURE 360

SERVICE DE SECURITÉ

DEBIAN 11

2024 - 2025

Table des matières

INTRODUCTION

La société FAC, établie il y a trois mois, est confrontée à des défis majeurs en matière de sécurité des systèmes d'information et des données des employés.

Afin de résoudre ces problèmes et de garantir la sécurité du personnel, il a été décidé d'implémenter une solution de sécurité appelée NetSecure360.

Les technologies utilisées pour la réalisation de ce projet reposent sur une machine virtuelle sous Debian 11 intégrant :

- Un serveur DNS
- Une base de données MySQL/MariaDB
- Un serveur FTP (VSFTPD)
- Un serveur web (Apache)
- Un serveur SSH (OpenSSH)

L'architecture comprend également :

- Un serveur d’authentification OpenLDAP
- Un pare-feu UFW
- Un VLAN
- Un serveur de supervision Zabbix
- Une solution de sauvegarde basée sur Rsync
- Un VPN (openVPN)

CONCEPTION DU PROJET

ARCHITECTURE DU PROJET

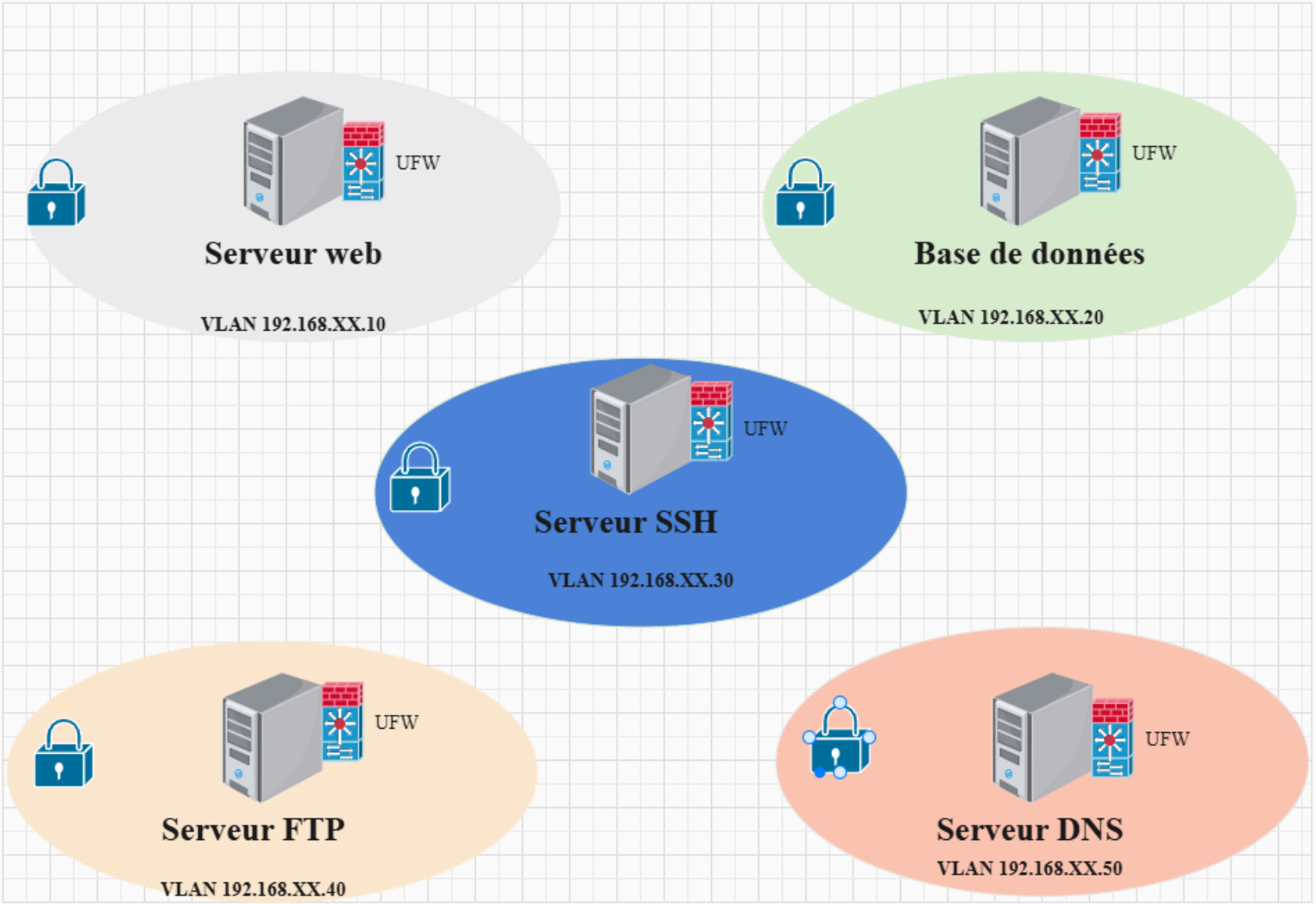


DIAGRAMME DE FLUX DE DONNÉS

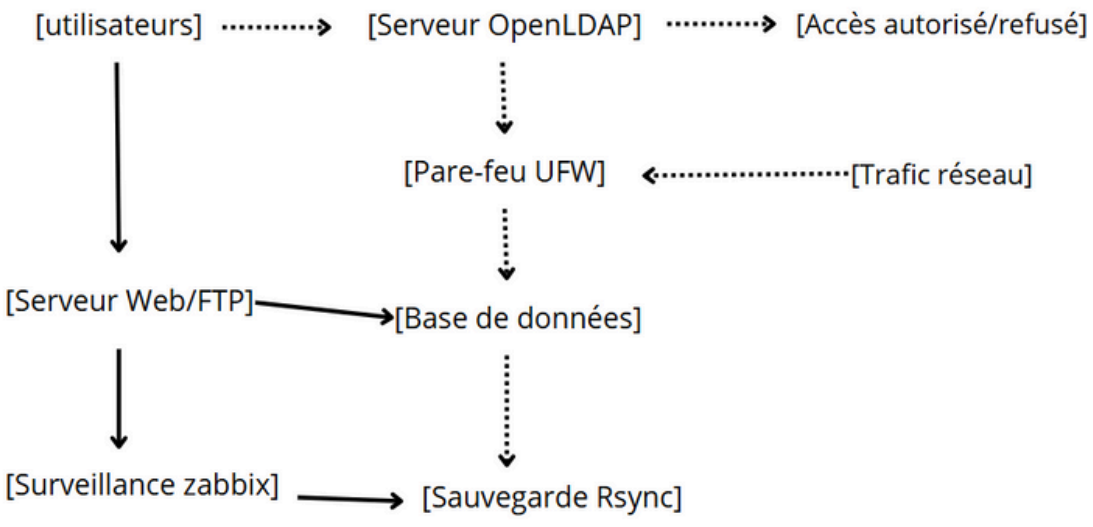
1. Authentification et gestion des accès - Entrée : Identifiants des utilisateurs - Traitement : Vérification via OpenLDAP

2. Gestion des connexions réseau et filtrage - Entrée : Trafic réseau - Traitement : Analyse et filtrage par UFW (pare-feu) et VLAN - Sortie : Accès sécurisé aux services internes

3. Hébergement et stockage de données - Entrée : Requêtes d'accès aux bases de données, au serveur web, au serveur FTP - Traitement : Gestion des données via MySQL/MariaDB, Apache, VSFTPD - Sortie : Données affichées ou stockées

4. Supervision et journalisation des activités - Entrée : Logs des serveurs et équipements - Traitement : Surveillance avec Zabbix - Sortie : Alertes et rapports

5. Sauvegarde et restauration des données - Entrée : Données des serveurs et bases de données - Traitement : Sauvegarde via Rsync - Sortie : Données stockées/restaurées en cas de besoin



Description des services simulés

- Serveur d’authentification OpenLDAP : Gère l’authentification centralisée des utilisateurs et des ressources réseau en stockant les informations d'identification dans un annuaire sécurisé.

- Pare-feu UFW : Simplifie la gestion des règles de filtrage réseau sous Linux, en contrôlant les connexions entrantes et sortantes pour renforcer la sécurité.

- VLAN : Segmente un réseau physique en plusieurs réseaux logiques isolés, améliorant ainsi la sécurité et la gestion du trafic.

- Serveur de supervision Zabbix : Surveille en temps réel l’état des serveurs, des équipements réseau et des services, en générant des alertes en cas d’anomalie.

- Solution de sauvegarde basée sur Rsync : Permet de synchroniser et sauvegarder efficacement des fichiers entre plusieurs machines, garantissant la protection des données.

- VPN (OpenVPN) : Crée un tunnel sécurisé pour chiffrer les communications entre des utilisateurs distants et le réseau de l’entreprise, assurant confidentialité et sécurité.

Installation & Configuration

Partie 1 : Services

Installation Dnsmasq:

Mise à jour et installation de Dnsmasq

palm@debian1 : ~$ sudo apt update && sudo apt install dnsmasq -y

Configuration de Dnsmasq

palm@debian1 : ~$ ~sudo nano /etc/dnsmasq.conf

Ajoute ou modifie ces lignes pour définir un DNS

interface=ens18.26
listen-adress=192.168.26.10
bind-interfaces
server=8.8.8.8
server1.1.1.1
cache-size=1000
domain=monreseau.local
dhcp-host=AA:BB:CC:DD:EE:FF,192.168.26.50,client1

Redémarre le service

palm@debian1 : ~$ sudo systemctl restart dnsmasq

Installation MariaDB:

palm@debian1 : ~$ sudo apt install Mariadb-server -y

Démarrage du service

palm@debian1 : ~$ sudo systemctl start mariadb

Vérifiez son statut

palm@debian1 : ~$ sudo systemctl status mariadb

Sécuriser l'installation

palm@debian1 : ~$ sudo mysql_secure_installation

Il te demandera de :

- Définir un mot de passe root
- Supprimer les utilisateurs anonymes → Tape Y.
- Interdire l'accès root distant → Tape Y.
- Supprimer la base de test → Tape Y.
- Recharger les privilèges → Tape Y.

Accède à MariaDb

palm@debian1 : ~$ sudo mysql -u root -p

A présent créer ta base de données

CREATE DATABASE nomdetabase;

CREATE USER 'NOM'@'localhost' IDENTIFIED BY 'MDP';

GRANT ALL PRIVILEGES ON nomdetabase. TO 'NOM'@'localhost';*

FLUSH PRIVILEGES;

EXIT;

Installation serveur FTP

palm@debian1 : ~$ sudo apt install vsftpd -y

Démarrage du serveur

palm@debian1 : ~$ sudo systemctl start vsftpd

Configuration VSFTPD

palm@debian1 : ~$ sudo nano /etc/vsftpd.conf

Modifie les lignes suivantes

local_enable=YES
write_enable=YES
chroot_local_user=YES
anonymous_enable=NO
pasv_enable=YES
pasv_min_port=40000
pasv_max_port=50000
allow_writeable_chroot=YES

Sauvegarde (ctrl + X > Y)

Créer un utilisateur FTP

palm@debian1 : ~$ sudo adduser ftpuser

Définir le répertoire FTP de l'utilisateur

palm@debian1 : ~$ sudo mkdir -p /home/ftpuser/ftp
sudo chmod 750 /home/ftpuser/ftp
sudo chown ftpuser: /home/ftpuser/ftp

Redémarrer le service

palm@debian1 : ~$ sudo systemctl restart vsftpd

Installation serveur web

palm@ldap: ~$ sudo apt install apache2 -y

Démarrage du service

palm@ldap: ~$ sudo systemctl start apache2

Si le service a bien démarré verifie qu'il fonctionne

http://localhost ou http://192.168.xx.xx

Configurer un l'hote virtuel

palm@ldap: ~$ sudo mkdir -p /var/www/monsite

Définir les permissions

palm@ldap: ~$ sudo chown -R $USER:$USER /var/www

sudo chmod -R 755 /var/www/monsite

Créer un nouveau fichier de configuration

palm@ldap: ~$ sudo nano /etc/apache2/sites-available/monsite.conf

Ajoute ce contenu

```
  GNU nano 5.4
<VirtualHost *:81>
    ServerAdmin webmaster@monsite.com
    DocumentRoot /var/www/monsite
    ServerName monsite.com
    ServerAlias www.monsite2.com

    <Directory /var/www/monsite>
        Options Indexes FollowSymLinks
        AllowOverride All
        Require all granted
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Active le site et redémarre Apache

palm@ldap: ~$ sudo a2ensite monsite

sudo systemctl reload apache2

Installation serveur SSH et les prérequis

palm@ldap:~$ sudo apt update && sudo apt install -y python3 python3-pip git

Cloner le dépôt et installer les dépendances

git clone https://github/johnnykv/heralding.git

cd heralding

pip3 install -r requirements.txt

Modifie le fichier config.json selon tes besoins

Désactive OpenSSH sur le port 22 avant de lancer Heralding pour éviter les conflits

Lancer Heralding

palm@ldap:~$ python3 heralding.py

Lancer en tant que fichier

/etc/systemd/system/heralding.service

```
  GNU nano 5.4
[Unit]
Description=Heralding Honeypot
After=network.target

[Service]
ExecStart=/usr/bin/python3 /chemin/vers/heralding/heralding.py
WorkingDirectory=/chemin/vers/heralding
Restart=always
User=nobody
Group=nogroup

[Install]
WantedBy=multi-user.target
```

Active le service

palm@ldap:~$ sudo systemctl daemon-reload

sudo systemctl enable heralding

sudo systemctl start heralding

Installation NetSecure360

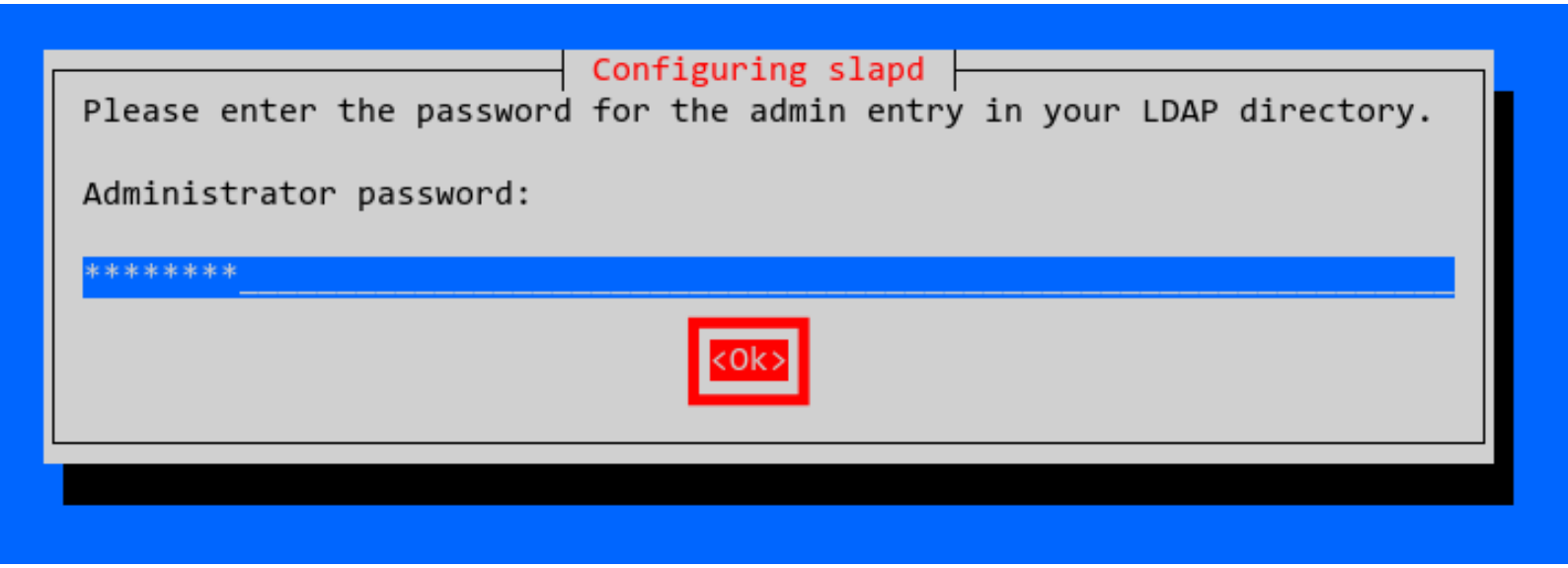
Installation serveur d’authentification LDAP

Commencer l’installation

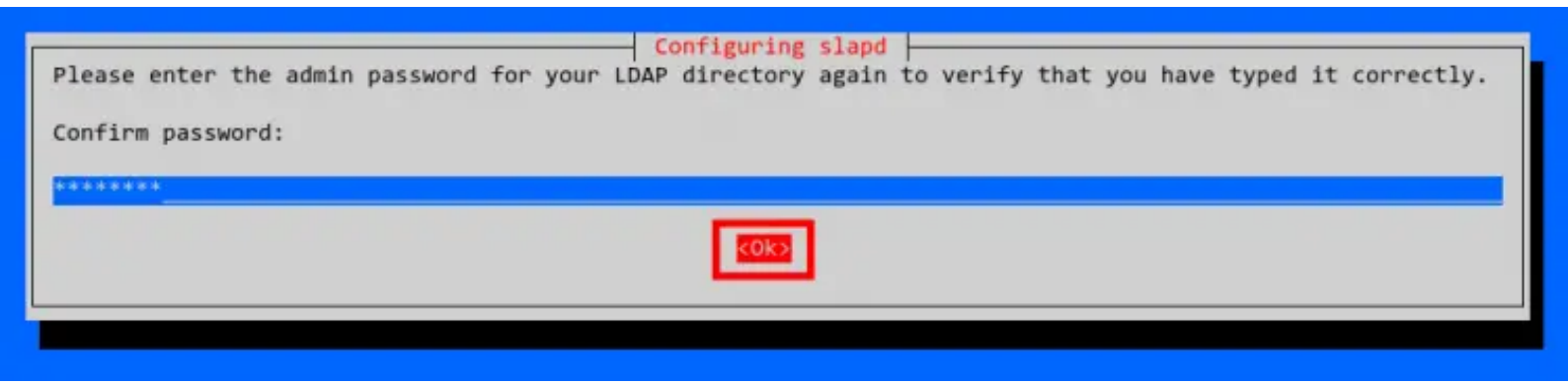
palm@ldap:~$ sudo apt install slapd ldap-utils

Confirmez l’installation

Il vous sera maintenant demandé de configurer le mot de passe de l’utilisateur administrateur OpenLDAP



Répétez votre mot de passe et sélectionnez « OK », puis appuyez à nouveau sur « ENTER ». Et l’installation d’OpenLDAP est terminée.



Configurons le serveur

Mais avant cela, configurons le FQDN (Fully Qualified Domain Name) du serveur à l'aide de la commande suivante.

palm@ldap:~$ sudo hostnamectl set-histname ldap.mydomain.local

palm@ldap:~$ sudo nano /etc/host

Ajoutez cette configuration et assurez-vous de remplacer l'adresse IP par la votre et le nom du serveur par le votre

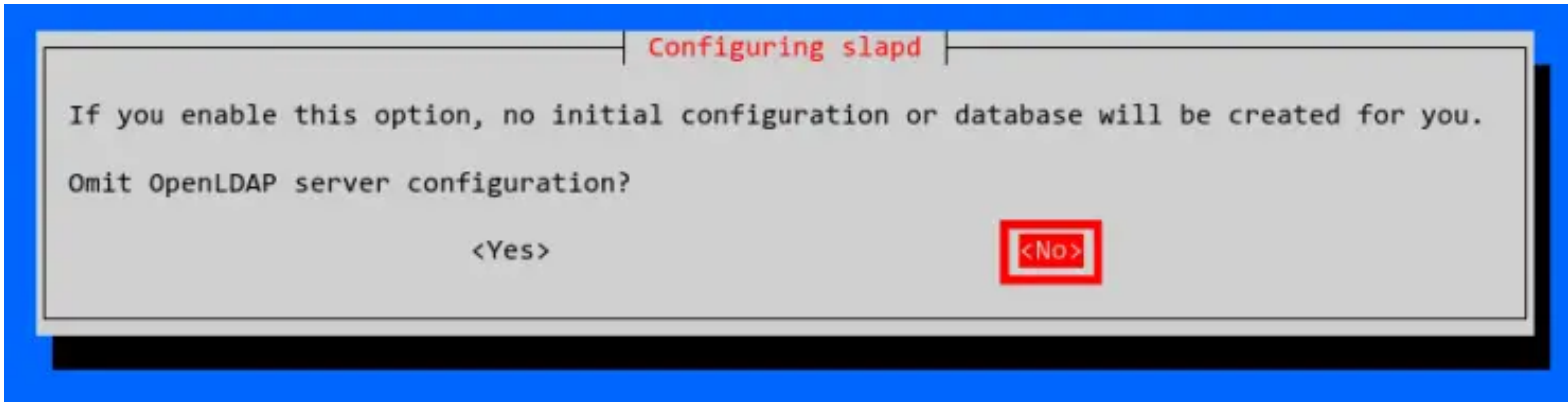
palm@ldap:~$ 192.168.26.50 ldap-mydomain.local ldap

Enregistrez et fermez (ctrl + X > Y + ENTRER)

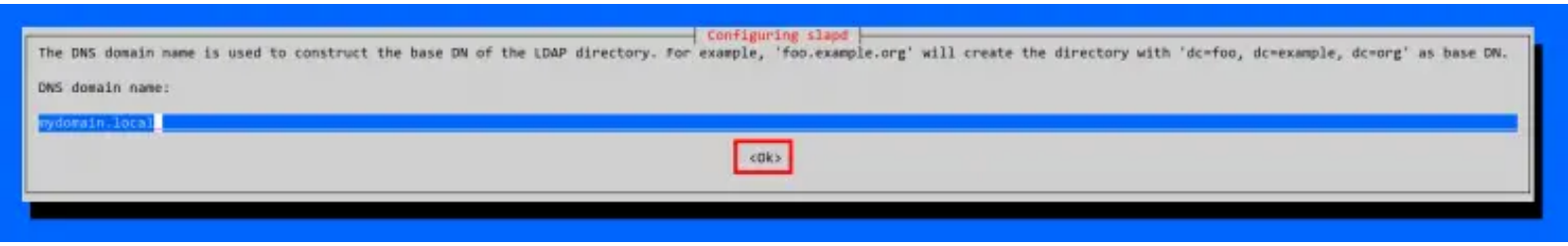
Déconnectez-vous maintenant de votre session SSH actuelle et reconnectez-vous à votre serveur.

palm@ldap:~$ sudo dpkg-reconfigure slapd

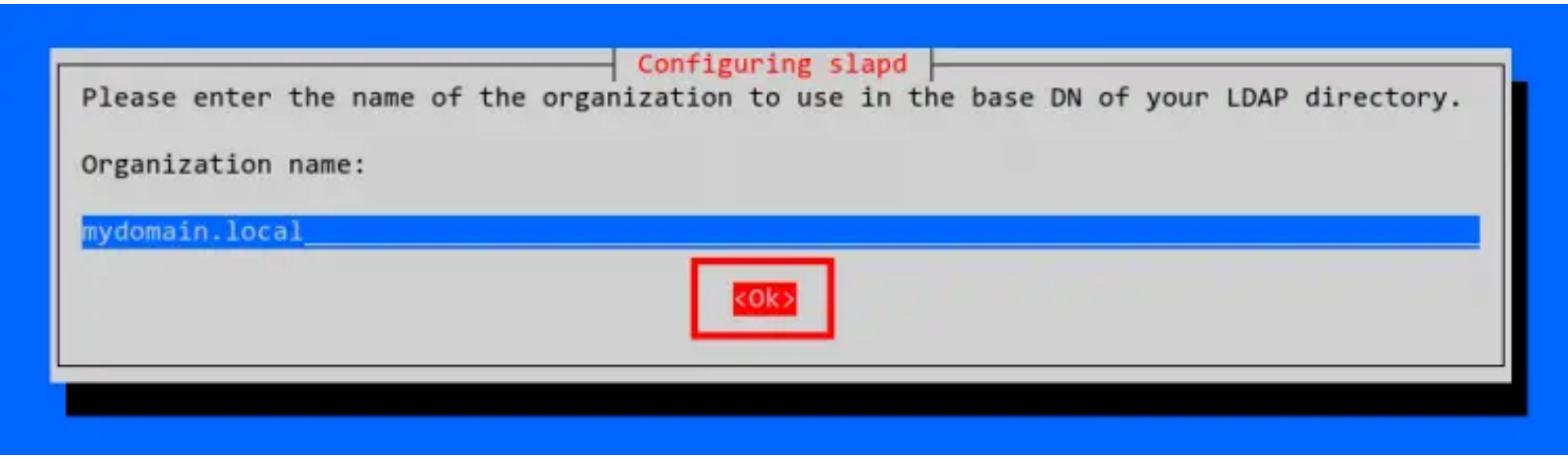
Entrez cette commande pour reconfigurer le package OpenLDAP 'slapd'



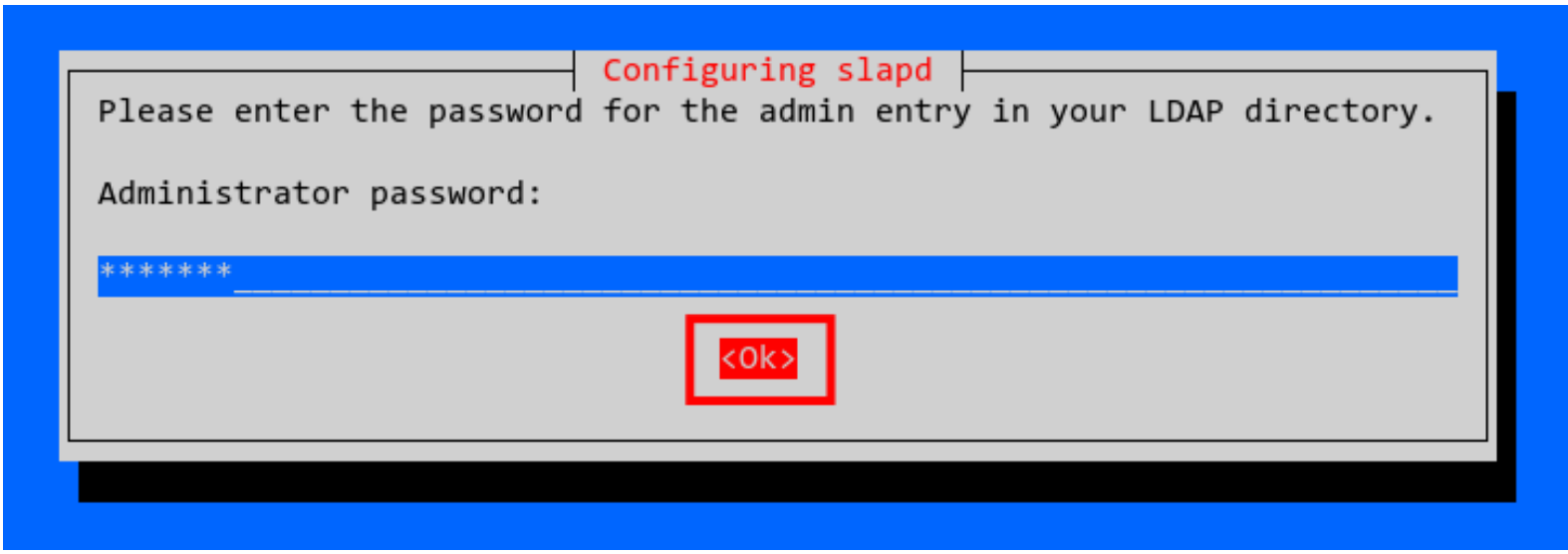
Entrez maintenant le nom de domaine DNS local de votre serveur OpenLDAP et sélectionnez OK.



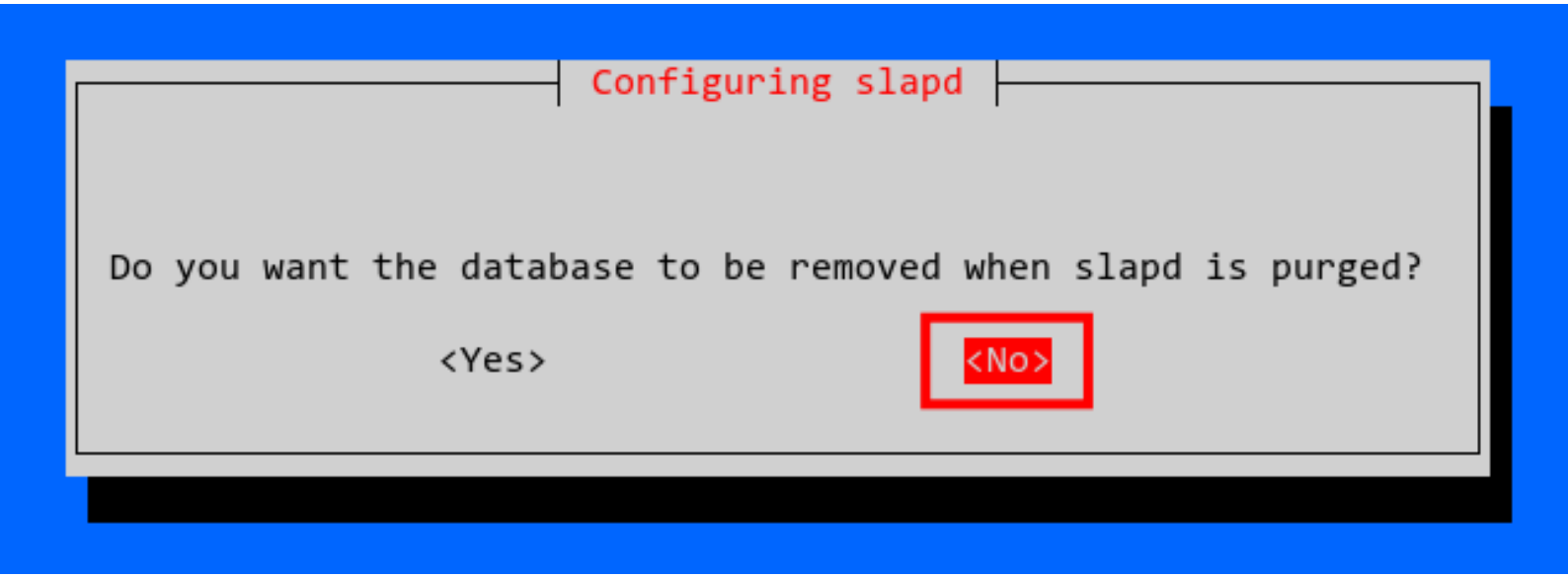
Entrez le nom de l'organisation et sélectionnez OK. Si vous le souhaitez, vous pouvez le laisser par défaut avec le même nom que le nom de domaine.



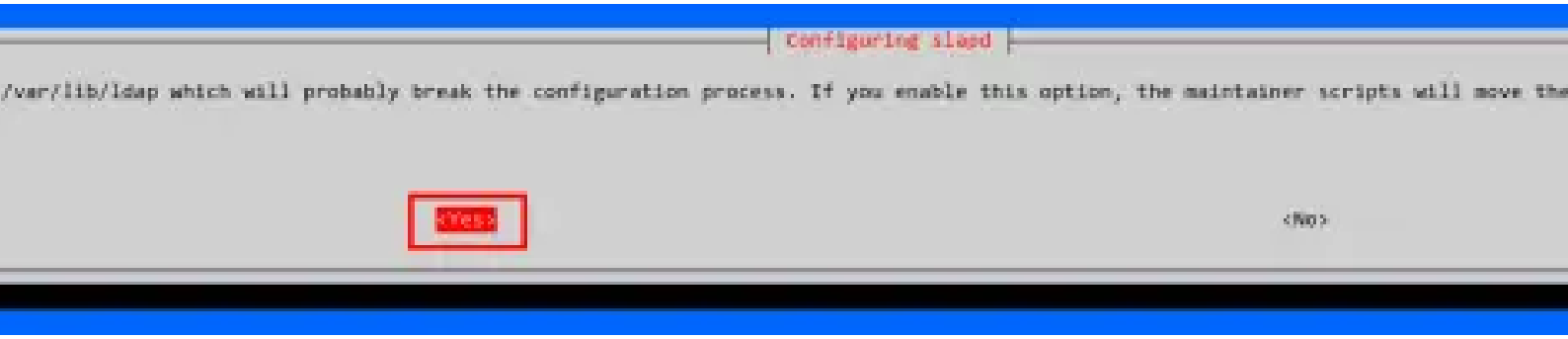
Entrez maintenant le mot de passe administrateur OpenLDAP et sélectionnez OK pour continuer.



Sélectionnez NON lorsqu'on vous demande de supprimer l'ancienne base de données slapd.



Sélectionnez maintenant Oui pour déplacer l'ancienne base de données slapd.



La configuration des packages OpenLDAP est maintenant terminée.

Enfin, redémarrez le service 'slapd' pour appliquer les nouvelles modifications. Vérifiez ensuite le service 'slapd'.

palm@ldap:~$ sudo systemctl restart slapd
palm@ldap:~$ sudo systemctl status slapd

```
● slapd.service - LSB: OpenLDAP standalone server (Lightweight Directory Access Protocol)
     Loaded: loaded (/etc/init.d/slapd; generated)
    Drop-In: /usr/lib/systemd/system/slapd.service.d
             └─slapd-remain-after-exit.conf
     Active: active (running) since Wed 2022-03-02 12:56:18 UTC; 9s ago
       Docs: man:systemd-sysv-generator(8)
    Process: 3723 ExecStart=/etc/init.d/slapd start (code=exited, status=0/SUCCESS)
      Tasks: 3 (limit: 2340)
     Memory: 3.0M
        CPU: 30ms
```

Installation Pare-feu (UFW)

palm@ldap:~$ sudo apt install ufw -y

Configuration UFW

Autoriser le SSH

palm@ldap:~$ sudo ufw allow OpenSSH

Définir des règles générales, Bloquer tout le trafic entrant par défaut

palm@ldap:~$ sudo ufw default deny incoming

Autoriser tout le trafic sortant :

palm@ldap:~$ sudo ufw default allow outgoing

N’oublie pas d’ouvrir les ports nécessaires

exemple : Serveur WEB

palm@ldap:~$ sudo ufw 80/tcp
sudo ufw allow 443/tcp

Activer UFW

palm@ldap:~$ sudo ufw enable

Vérifie si UFW est actif et quelles règles sont en place :

palm@ldap:~$ sudo ufw status verbose

Félicitation l’installation est terminé

Installer PHP et ses modules

palm@ldap:~$ sudo apt install php php-mbstring php-gd php-xml php-bcmath php-ldap php-mysql php-zip -y

Installer le serveur Zabbix

wget https://repo.zabbix.com/zabbix/6.0/debian/pool/main/z/zabbix-release/zabbix-release_6.0-4+debian$(lsb_release -rs)_all.deb

palm@ldap:~$suod dpkg -i zabbix-release_6.0'4 +debian$

palm@ldap:~$ sudo apt update

Installe Zabbix Server, l'Agent et le frontend Web

sudo apt install zabbix-server-mysql zabbix-frontend-php zabbix-apache-conf zabbix-agent -y

Configurer la base de données pour Zabbix

palm@ldap:~$ sudo mysql -uroot -p

```
[sudo] Mot de passe de palm :
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 30
Server version: 10.5.28-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Dans MariaDB, exécute ces commandes

```
MariaDB [(none)]> CREATE DATABASE zabbix CHARACTER SET utf8mb4 COLLATE utf8mb4_bin;
Query OK, 1 row affected (0,315 sec)

MariaDB [(none)]> CREATE USER 'zabbix'@'localhost' IDENTIFIED BY 'MonMotDePasse';
Query OK, 0 rows affected (0,312 sec)

MariaDB [(none)]> GRANT ALL PRIVILEGES ON zabbix.* TO 'zabbix'@'localhost';
Query OK, 0 rows affected (0,028 sec)

MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,025 sec)

MariaDB [(none)]> EXIT;
Bye
palm@ldap:~$
```

Importer le schéma de base de données

palm@ldap:~$ zcat /usr/share/doc/zabbix-server-mysql/create.sql.gz | mysql -uzabbix -p zabbix*

Configurer Zabbix Server

palm@ldap:~$ sudo nano /etc/zabbix/zabbix_server.conf

Modifie ces lignes :

DBHost=localhost

DBName=zabbix

DBUser=zabbix

DBPassword=MonMotsDePasse

Sauvegarde et ferme (CTRL+X, Y, Entrée).

Démarrer les services Zabbix

palm@ldap:~$ sudo systemctl restart zabbix-server zabbix-agent apache2

Configurer le frontend Zabbix

Accède à http://<TON IP>/zabbix depuis un navigateur

Installation Rsync

palm@ldap:~$ sudo apt install rsync -y

Synchroniser un fichier local vers un autre répertoire local

palm@ldap:~$ rsync -av /cheminfichier /cheminfichier

ynchroniser un fichier ou un répertoire vers une machine istante

cheminfichier user@serveur :/cheminrepertoire

Synchroniser depuis une machine distante vers une machin locale

palm@ldap:~$ rsync -av user@serveur :/chemin fichier /chemin repertoire

Exécution en tâche de fond

palm@ldap:~$ nohup rsync -av /source /destination

Planifier des sauvegardes avec cron

Ouvrir le crontab pour l'édition

palm@ldap:~$ crontab -e

Ajouter une ligne pour exécuter la commande à une heure régulière (par exemple tous les jours à 3h du matin)

*palm@ldap:~$ 0 3 * * * rsync -av /source /destination*

Cela exécutera la commande rsync tous les jours à 3h du matin.

Félicitation l’installation est terminé

Installation OpenVPN

palm@ldap:~$ curl -o https://raw.github.com/angristan/openvpn-install/master/openvpn-install-install.sh

palm@ldap:~$ chmod +x openvpn-install.sh

Ensuite, exécutez le script

palm@ldap:~$ /openvpn-install.sh

Lors de la première exécution, vous serez invité à répondre à quelques questions pour configurer votre serveur VPN. Une fois OpenVPN installé, vous pouvez réexécuter le script pour :

Cela vous permet d'ajouter de nouveaux utilisateurs ou de révoquer des utilisateurs existants.

Configurer OpenVPN

palm@ldap:~$ zcat /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz | sudo tee /etc/openvpn/server.conf > /dev/null

Copiez les fichiers nécessaires dans le répertoire OpenVPN

palm@ldap:~$ cp /root/openvpn-ca/pki/{ca.crt,dh.pm,ta.key} /etc/openvpn

palm@ldap:~$ cp /root/openvpn-ca/pki/issued/server.cr /etc/openvpn

palm@ldap:~$ cp /root/openvpn-ca/pki/private/server.key /etc/openvpn

Modifiez /etc/openvpn/server.conf pour qu'il corresponde à ce qui suit

ca ca.crt
cart server.crt
key server.key
dh dh.pem
;tls-auth ta.key 0
tsl-crypt ta.key

Activer le transfert IP

palm@ldap:~$ sudo nano /etc/sysctl.conf

décommentez cette ligne : net.ipv4.ip_forward=1

Appliquez les changements :

palm@ldap:~$ sudo sysctl -p

Démarrer et activer OpenVPN

palm@ldap:~$ sudo systemctl start openvpn@server
sudo systemctl enable openvpn@server

Se connecter au serveur OpenVPN

palm@ldap:~$ ./easyrsa gen-req client1 nopass
$ ./easyrsa sign-req client1 client1
$ cp pki/private/client1.key /etc/openvpn/client/
$ cp pki/issued/client1.crt /etc/openvpn/client/
$ cp pki/{ca.crt,ta.key} /etc/openvpn/client/

Créez un fichier de configuration client dans le répertoire /root/openvpn-ca

palm@ldap:~$ cp pki/issued/client 1.crt /etc/openvpn/client/

Modifiez le fichier à l'aide de nano et configurez les variables :

user nobody
group nogroup
;ca ca.crt
;cert client.crt
;key client.key
;tls-auth ta.key 1
key-direction 1

Créez un script pour compiler la configuration de base avec les fichiers de certificat, clé et chiffrement nécessaires :

root@ldap:~# nano config gen.sh

Incluez le contenu suivant :

```
#!/bin/bash# Premier argument : identifiant du client
KEY_DIR=/etc/openvpn/client
OUTPUT_DIR=/root
BASE_CONFIG=/root/openvpn-ca/client.conf
cat${BASE_CONFIG} \
    <(echo -e '<ca>') \
    ${KEY_DIR}/ca.crt \
    <(echo -e '</ca>\n<cert>') \
    ${KEY_DIR}/${1}.crt \
    <(echo -e '</cert>\n<key>') \
    ${KEY_DIR}/${1}.key \
    <(echo -e '</key>\n<tls-crypt>') \
    ${KEY_DIR}/ta.key \
    <(echo -e '</tls-crypt>') \
    > ${OUTPUT_DIR}/${1}.ovpn
```

Rendez le script exécutable :

root@ldap:~$ chmod 700 /root/openvpn-ca/config_gen.sh
$ ./config_gen.sh client1

Félicitation l'installation est terminé

Sécurité et précautions

Risques associés :

1. Accès non autorisé : Risque de compromission des données.
- Mesure : OpenLDAP pour une gestion centralisée des accès, et UFW pour filtrer les connexions.

2. Attaques DoS : Risque de rendre les services indisponibles.
- Mesure : VLAN pour isoler le trafic et Zabbix pour la supervision et les alertes.

3. Perte de données : Risque de corruption ou de fuite de données sensibles.
- Mesure : Rsync pour les sauvegardes régulières et VPN pour des connexions sécurisées.

4. Accès réseau non sécurisé : Risque d'interception des communications.
- Mesure : VPN (OpenVPN) pour chiffrer les connexions à distance.

5. Mauvaise configuration du réseau : Risque d’exploitation de vulnérabilités internes.
- Mesure : UFW et VLAN pour sécuriser les flux réseau et segmenter l’accès.

Sécurité et précautions

Mesures de sécurité mises en place :

1. Dans le cadre de l'authentification et de la gestion des accès, nous utilisons OpenLDAP pour l'authentification centralisée et UFW pour filtrer l'accès aux services.

2. En ce qui concerne la sécurisation du réseau, nous avons recours au VLAN afin de segmenter le réseau et à OpenVPN pour garantir la sécurité des connexions à distance.

Nous assurons la surveillance et la gestion des incidents en utilisant Zabbix pour surveiller l'état des serveurs et détecter toute activité suspecte.

Pour ce qui est de la protection des données, nous utilisons Rsync pour réaliser des sauvegardes régulières et sécurisées des données.

Enfin, nous assurons un contrôle des services en restreignant l'accès aux services essentiels uniquement grâce à l'utilisation de UFW et VLAN.

Capture et Analyse des Attaques

UFW :

Notre firewall UFW analyse le trafic entrant et sortant du réseau, en enregistrant des informations de logs pour chaque paquet de données.

Les logs incluent l'adresse IP source et destination, le type de trafic (par exemple, HTTP, SSH), les actions prises (bloqué, autorisé) et des détails sur les tentatives d'intrusion ou d'accès non autorisés.

Ces logs sont essentiels pour détecter les activités suspectes et comprendre les tentatives d'attaque.

Capture et Analyse des Attaques

Zabbix :

Zabbix offre une fonctionnalité de collecte de logs permettant de surveiller des fichiers logs spécifiques sur les serveurs et équipements supervisés.

Les fichiers logs sont configurés dans Zabbix, qui les vérifie régulièrement à la recherche d'événements ou d'erreurs prédéfinis.
En cas de détection d'un motif d'alerte configuré, Zabbix envoie une notification immédiate à l'utilisateur.

Cette fonctionnalité permet une centralisation des logs importants pour une meilleure visibilité de l'infrastructure et une réactivité face aux problèmes potentiels.

En résumé, le firewall capture les logs du trafic réseau, tandis que Zabbix surveille les logs système et d'application pour renforcer la sécurité et la performance.

Résultats et Analyse

Impact de l'intégration d'une solution de sécurité

- Protection accrue des données : Réduction des risques de cyberattaques, fuites de données et intrusions.
- Amélioration de la continuité d'activité : Moins de risques d'interruptions liées aux cyberattaques.
- Optimisation de la gestion des accès : Sécurisation des identités et limitation des accès aux ressources sensibles.
- Augmentation de la confiance : Clients et partenaires ont davantage confiance dans l’entreprise.

Retour sur les résultats

- Diminution des incidents de sécurité : Moins de tentatives réussies d’hameçonnage, de ransomwares ou d’intrusions.
- Amélioration de la réactivité : Détection et réponse plus rapide aux menaces grâce aux systèmes de surveillance et d’alerte.
- Formation et sensibilisation du personnel : Meilleure compréhension des risques par les employés, réduisant les erreurs humaines.

Conclusion

Cette initiative a constitué une expérience très bénéfique, aussi bien pour l'amélioration des performances de l'entreprise que pour mon développement personnel.

La sécurisation des systèmes représente actuellement un enjeu majeur, et en tant que spécialiste passionné de la cybersécurité, j'ai pris un réel plaisir à piloter efficacement ce projet.

NET SECURE 360