



MINISTÈRE CHARGÉ
DE L'EMPLOI

DOSSIER PROFESSIONNEL (DP)

Nom de naissance

► Mechenane

Nom d'usage

►

Prénom

► Omar

Adresse

► 10 avenue vauquelin, 93370 Montfermeil

Titre professionnel visé

Technicien supérieure système et réseau

MODALITE D'ACCES :

- Parcours de formation
- Validation des Acquis de l'Expérience (VAE)

Présentation du dossier

Le dossier professionnel (DP) constitue un élément du système de validation du titre professionnel. **Ce titre est délivré par le Ministère chargé de l'emploi.**

Le DP appartient au candidat. Il le conserve, l'actualise durant son parcours et le présente **obligatoirement à chaque session d'examen.**

Pour rédiger le DP, le candidat peut être aidé par un formateur ou par un accompagnateur VAE.

Il est consulté par le jury au moment de la session d'examen.

Pour prendre sa décision, le jury dispose :

1. des résultats de la mise en situation professionnelle complétés, éventuellement, du questionnaire professionnel ou de l'entretien professionnel ou de l'entretien technique ou du questionnement à partir de productions.
2. du **Dossier Professionnel** (DP) dans lequel le candidat a consigné les preuves de sa pratique professionnelle
3. des résultats des évaluations passées en cours de formation lorsque le candidat évalué est issu d'un parcours de formation
4. de l'entretien final (dans le cadre de la session titre).

[Arrêté du 22 décembre 2015, relatif aux conditions de délivrance des titres professionnels du ministère chargé de l'Emploi]

Ce dossier comporte :

- ▶ pour chaque activité-type du titre visé, un à trois exemples de pratique professionnelle ;
- ▶ un tableau à renseigner si le candidat souhaite porter à la connaissance du jury la détention d'un titre, d'un diplôme, d'un certificat de qualification professionnelle (CQP) ou des attestations de formation ;
- ▶ une déclaration sur l'honneur à compléter et à signer ;
- ▶ des documents illustrant la pratique professionnelle du candidat (facultatif)
- ▶ des annexes, si nécessaire.

Pour compléter ce dossier, le candidat dispose d'un site web en accès libre sur le site.



<http://travail-emploi.gouv.fr/titres-professionnels>

Sommaire

Exemples de pratique professionnelle

Assister les utilisateurs en centre de services	p. 5
--	-------------

- ▶ Intitulé de l'exemple n° 1 Mettre en service un équipement numérique p. 5
- ▶ Intitulé de l'exemple n° 2 Gestion d'un parc informatique avec l'installation de GLPI et De Fusion Inventory p. 09
- ▶ Intitulé de l'exemple n° 3 Dépannage d'une panne réseaux p. 12

Maintenir, exploiter et sécuriser une infrastructure centralisée	p. 17
---	--------------

- ▶ Intitulé de l'exemple n° 1 Installation et configuration d'un serveur DNS sur Debian p. 17
- ▶ Intitulé de l'exemple n° 2 Création d'un environnement virtualisé sur ESXI avec migration à chaud des serveurs virtuels p. 20
- ▶ Intitulé de l'exemple n° 3 Configurer un accès à distance à un commutateur Cisco avec le protocole Secure Shell (SSH) p. 23

Maintenir, exploiter une infrastructure distribuée et contribuer à sa sécurisation	p. 30
---	--------------

- ▶ Intitulé de l'exemple n° 1 configurer un VPN-SSL client-to-site avec OpenVPN p. 30
- ▶ Intitulé de l'exemple n° 2 Installation et configuration d'un serveur de déploiement WDS avec une machine de référence dans un environnement Active Directory p. 33

Titres, diplômes, CQP, attestations de formation (<i>facultatif</i>)	p. 38
---	--------------

Déclaration sur l'honneur	p. 39
----------------------------------	--------------

Documents illustrant la pratique professionnelle (<i>facultatif</i>)	p. 40
---	--------------

Annexes (<i>Si le RC le prévoit</i>)	p. 41
---	--------------

EXEMPLES DE PRATIQUE PROFESSIONNELLE

Activité-type 1 Assister les utilisateurs en centre de services

Exemple n°1 ► Mettre en service un équipement numérique

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Lors de ma formation au sein du centre de formation Afpa, on a simulé l'installation d'un point d'accès Wifi pour une école fictif nommé école 1

Scénario :

Pour l'école 1 mettre en place la topologie LAN, configuré et sécurisé un commutateur et mettre en place un point d'accès Wifi (protocole 802.11) en mode infrastructure sécurisé en WPA2 et prise en mains et configuration du réseau des tablettes ou téléphone Androïde

1. Etape de réalisation :

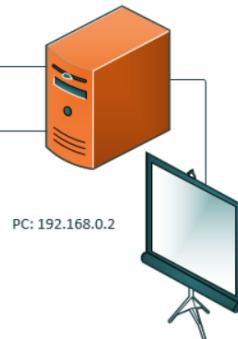
- Je fais l'inventaire du matériel et de la documentation
- Je lis la documentation du Point d'Accès Wifi et le cahier de charge
- Je fais les câblages en suivant le schéma de la topologie décrite dans la documentation

A. Topologie :

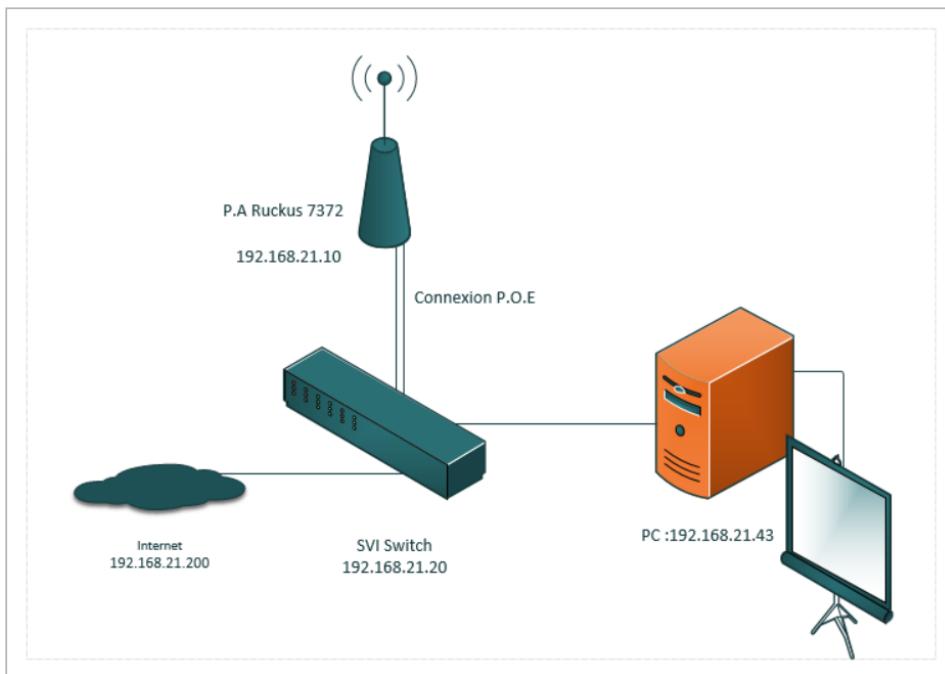
1. Topologie pour configurer le point d'accès wifi :

Connexion P.O.E
Ruckus 7372
192.168.0.1

Connexion P.O.E



2. Topologie finale :



- ✓ je branche mon pc au point d'accès wifi puis je donne une adresse IP à mon PC dans le réseau du point d'accès qui est **192.168.0.1**, donc pour mon PC : **192.168.0.2**
- ✓ je me connecte au point d'accès wifi avec le SSID et mon de passe par default et le configurer sur la fréquence 2,4 GHZ et change le SSID et mot de passe
- ✓ je donne une adresse IP dans le réseau **192.168.21.0** à mon point d'accès wifi, ici **192.168.21.10** après avoir consulté le carnet d'adresse disponible
- ✓ je clique sur l'option "Redémarrer" dans le menu de gauche pour redémarrer le point d'accès et appliquer les nouvelles configurations
- ✓ je réalise la topologie finale :
 - Je branche le câble droit entre le port FastEthernet 0/1 du switch et le PC
 - Je branche le câble croisé entre le switch et la table numérotée 50
 - Je branche le câble console entre le port console du switch et le port console du PC
 - Je branche un câble droit entre le port FastEthernet 0/2 du switch et le port P.O.E du point d'accès wifi
 - Je branche un câble droit entre le point d'accès wifi et le PC
 - Je branche le switch à l'alimentation
 - Je réinitialise le commutateur et je branche un câble console entre le PC et le commutateur
- ✓ Je remets l'adresse IP d'origine du pc, ici 192.168.21.43

- ✓ J'ouvre le logiciel PuTTY, ensuite je me mets sur port serial et le speed 9600 ou 115200
- ✓ je configure et sécurise mon commutateur
 - Je mets un Password sur le mode user et privilégié
 - Je crypte la configuration grâce au service password-encryption
 - Je sécurise les line VTY
 - Je mets une bannière motd
 - Je donne une adresse IP à son Vlan de gestion de sorte que sa soit sur le même réseau LAN 192.168.21.0, dans mon cas c'est le vlan 99, ici **192.168.21.20** après avoir consulté le carnet d'adresses disponibles

Pour connecter ma tablette Samsung à mon point d'accès Wifi, je m'assure que votre point d'accès est correctement configuré et en état de fonctionnement. Ensuite, je suis ces étapes:

- J'ouvre les paramètres de ma tablette.
- Je sélectionne "Wi-Fi" dans la liste des options.
- Je m'assure que le Wifi est activé en appuyant sur l'interrupteur en haut de l'écran, une liste de réseaux Wifi disponibles s'affiche et je sélectionne le nom de réseau Wifi ECOLE1.
- J'entre le mot de passe configurer précédemment lorsque je suis invité.
- J'appuie sur "Connecter" pour me connecter au réseau.
- Vérifier le fonctionnement en ouvrant une page web par exemple

2. Précisez les moyens utilisés :

- PC
- Commutateur POE
- Point d'accès Wifi de marque Ruckus
- Tablette de marque SAMSUNG model
- Câbles Ethernet (droit et croisé) et câbles console
- Logiciel putty

3. Avec qui avez-vous travaillé ?

En atelier du centre de Formation Afpa en collaboration avec ma Formatrice Claire Sobesky

4. Contexte

Nom de l'entreprise, organisme ou association **Centre de formation Afpa Champs-sur-Marne**

Chantier, atelier, service ► Atelier de Formation

Période d'exercice ► Le 27/09/2022

5. Informations complémentaires (facultatif)

En suivant une activité d'installation d'un point d'accès Wi-Fi, vous pouvez apprendre les compétences suivantes :

- ✓ Choix d'un matériel : j'ai appris à choisir le matériel adéquat pour mon réseau Wi-Fi, en fonction de mes besoins en termes de portée, de vitesse, de nombre d'utilisateurs, etc.
- ✓ Configuration du matériel : j'ai appris à configurer le matériel en utilisant l'interface web du routeur ou en utilisant un logiciel dédié. J'ai également appris à configurer les options de base, telles que le nom du réseau (SSID), le canal, le type de sécurité, les paramètres de déploiement
- ✓ Connexion des utilisateurs : j'ai appris à permettre aux utilisateurs de se connecter à mon réseau Wi-Fi en leur fournissant les informations de connexion appropriées, telles que le nom du réseau et la clé de sécurité.
- ✓ Gestion des utilisateurs : j'ai appris à gérer les utilisateurs qui se connectent à mon réseau Wi-Fi, en utilisant les fonctionnalités de filtrage d'adresses MAC, de contrôle de bande passante, de limites de connexion, etc.
- ✓ Résolution des problèmes : j'ai appris à dépanner les problèmes courants rencontrés lors de la mise en place d'un point d'accès Wi-Fi, tels que les erreurs de configuration, les problèmes de sécurité, les problèmes de connectivité, etc.

Ci-joint en annexe ma procédure pour l'installation

Activité-type 1 Assister les utilisateurs en centre de services

Exemple n°2 ▶ *Gestion du parc informatique avec l'installation de GLPI et de Fusion Inventory*

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :



GLPI (Gestionnaire libre de parc informatique) : est un système de gestion de parc informatique open source. Il est utilisé pour gérer les ressources informatiques d'une organisation, telles que les ordinateurs, les périphériques réseau, les logiciels, les licences, les utilisateurs, etc.

GLPI est conçu pour fournir une vue complète et à jour du parc informatique, y compris les informations sur les équipements, les licences, les garanties, les contrats de maintenance, les historiques de maintenance, etc. Il offre également des fonctionnalités de suivi des incidents, de gestion des demandes de service et de gestion des projets pour aider les entreprises à gérer les problèmes informatiques rapidement et efficacement.

GLPI est une solution flexible et personnalisable qui peut être utilisée dans de nombreux environnements, y compris les petites et moyennes entreprises, les grandes entreprises et les organismes gouvernementaux. Il est également compatible avec un large éventail de systèmes d'exploitation, de bases de données et de technologies réseau. En raison de sa grande souplesse et de ses fonctionnalités avancées, GLPI est devenu un choix populaire pour les entreprises souhaitant améliorer leur gestion de parc informatique.

Après avoir installé des machines virtuelles avec virtuelle box sur mon pc, j'ai installé ensuite le logiciel GLPI (gestion libre de parc informatique) et l'agent Fusion Inventory pour faire l'inventaire du parc virtuel, crée des utilisateurs pour simuler des pannes, crée et résoudre des tickets d'incidents, comme suit :

- ✓ Installation de machines virtuelles sur mon pc

- ✓ Installation de **Xampp** sur Windows et activation des serveurs Apache et MySQL
- ✓ Activation de l'extension PHP fileinfo
- ✓ Placer le dossier GLPI dans le répertoire htdocs de Xampp
- ✓ Lancer l'installation de **GLPI** à partir de <http://localhost/glpi/>:
- ✓ Décompresser l'archive fussinnventory et mettre le répertoire dans le dossier plugin dans GLPI
- ✓ Activer et installer le plugin Fusioninventory dans GLPI
- ✓ Installation de l'agent **Fusioninventory** sur mon pc et sur les VM et forcer l'inventaire
- ✓ Ajouter une imprimante manuellement
- ✓ Rajouter un contrat d'assurance pour l'imprimante
- ✓ Créations d'entité, de groupe et d'utilisateurs
- ✓ Créations de tickets d'incidents
- ✓ Résolutions de tickets d'incidents et alimenter la base de donner

2. Précisez les moyens utilisés :

- PC
- Le logiciel Virtuelle box
- Plusieurs VM
- L'archive contenant le dossier GLPI (fichier glpi-0.90.1.4.tar.gz)
- Le logiciel XAMPP (fichierxampp-win32-5.6.8-0-VC11-installer.exe)
- L'agent Fusion Inventory (fichiers fusioninventory-for-glpi_0.90.1.4.tar.gz et fusioninventory-agent_windows-x64_2.3.18.exe)
- WINRAR ou 7ZIP

3. Avec qui avez-vous travaillé ?

La procédure d'installation m'a été transmise par ma formatrice claire Sobesky
 La mise en œuvre ainsi que sa description ont été faite par moi-même en centre de formation
 Afpa Champs-sur-Marne

4. Contexte

Nom de l'entreprise, organisme ou association ► ***Centre de formation Afpa Champs-sur-Marne***

Chantier, atelier, service	► Atelier Afpa
Période d'exercice	► Le 04/09/2022

5. Informations complémentaires (facultatif)

Cette activité m'a permis d'apercevoir la façon de gérer un parc informatique et ces ressources (licence, hardware comme pc et cartouches d'imprimantes, utilisateur) et la façon dont communique-les différent groupe d'utilisateur (administrateurs, techniciens, utilisateurs)

- ✓ J'ai appris à utiliser GLPI pour gérer les ressources informatiques de mon organisation, telles que les ordinateurs, les périphériques réseau, les logiciels, les licences, les utilisateurs, etc. j'ai également appris à utiliser les différents modules de GLPI, tels que la gestion des incidents, la gestion des demandes de service et la gestion des projets.
- ✓ J'ai appris à personnaliser GLPI en utilisant les différents plugins disponibles pour ajouter des fonctionnalités supplémentaires, telles que la gestion des contrats de maintenance, la gestion des garanties, la gestion des historiques de maintenance, etc.
- ✓ J'ai appris à configurer GLPI en définissant les options de base, telles que les informations de connexion à la base de données, les options de sécurité, les options d'authentification, les options de gestion des droits d'accès, etc.

En suivant cette activité, j'ai une compréhension plus approfondie de GLPI et de ses fonctionnalités. J'ai également développé mes compétences en matière de gestion de parc informatique et améliorer mes capacité à gérer les ressources informatiques de mon organisation de manière efficace et organisée.

Activité-type 1 Assister les utilisateurs en centre de services

Exemple n°3 ► Dépannage d'une panne réseaux

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

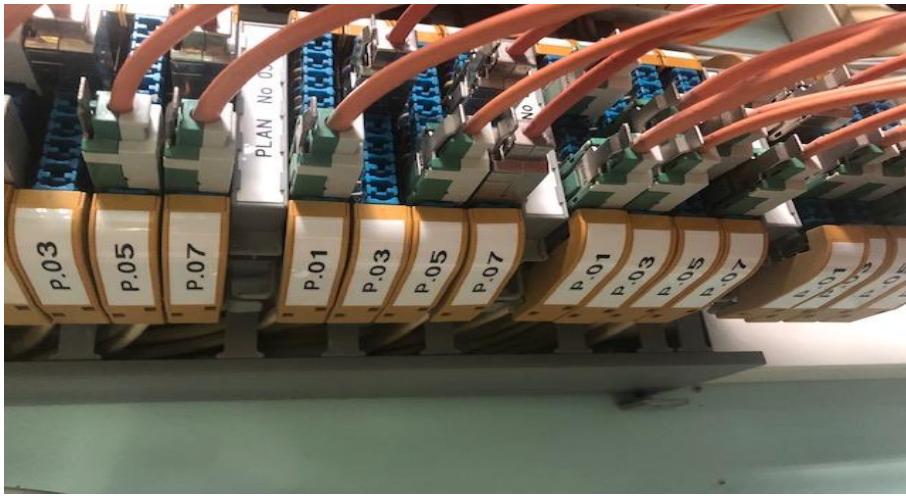
Je suis intervenu sur un ordinateur qui avait un problème de connexion réseau. Mon formateur m'avait signalé que l'ordinateur ne pouvait pas se connecter à Internet. Après avoir discuté avec l'utilisateur et analysé la configuration de l'ordinateur, j'ai commencé à effectuer des tests de diagnostic pour identifier

la cause du problème.

J'ai commencé par vérifier si le câble réseau était correctement connecté à l'ordinateur et à la baie de brassage.

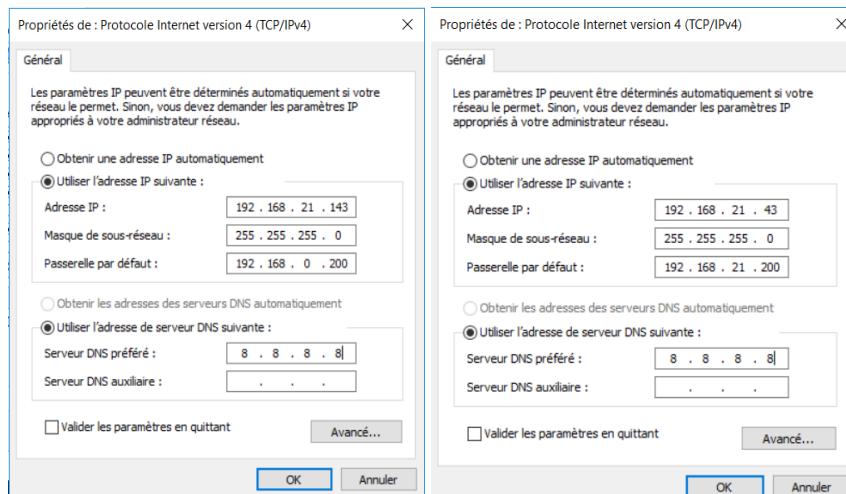
J'ai constaté que le câble était mal connecté et j'ai immédiatement corrigé le problème



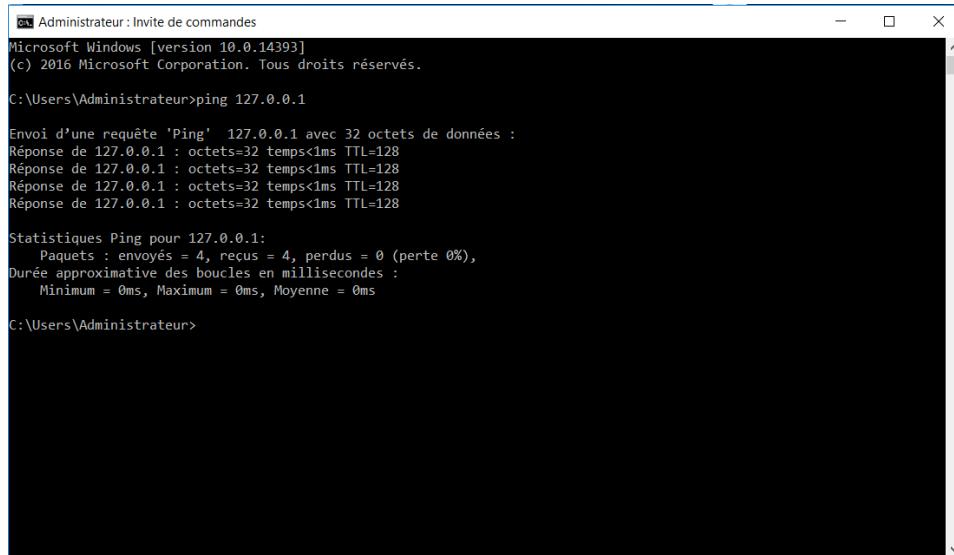


J'ai ensuite vérifié la configuration de la carte réseau de l'ordinateur.

Pour cela, j'ai utilisé la commande "ipconfig" dans l'invite de commandes pour obtenir les informations de configuration réseau de l'ordinateur. J'ai remarqué que les paramètres de la carte réseau étaient mal configurés. J'ai alors ajusté les paramètres de la carte réseau pour qu'ils correspondent à la configuration réseau de l'entreprise.



Après cela, j'ai effectué une série de tests de ping pour vérifier que la connexion réseau avait été rétablie avec succès. J'ai commencé par effectuer un ping vers l'adresse de bouclage (127.0.0.1) pour vérifier si la carte réseau de l'ordinateur était fonctionnelle. J'ai reçu des réponses de l'adresse de bouclage, ce qui indiquait que la carte réseau de l'ordinateur était opérationnelle



```
Administrator : Invite de commandes
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

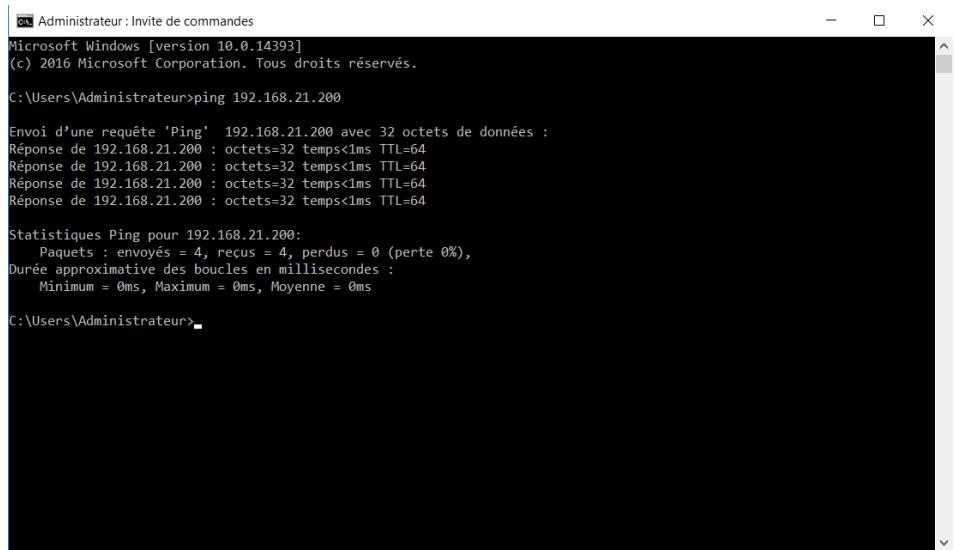
C:\Users\Administrateur>ping 127.0.0.1

Envoi d'une requête 'Ping' 127.0.0.1 avec 32 octets de données :
Réponse de 127.0.0.1 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 127.0.0.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>
```

J'ai ensuite effectué un ping vers l'adresse IP de la passerelle par défaut pour vérifier si l'ordinateur était capable de communiquer avec le routeur. J'ai reçu des réponses de la passerelle par défaut, ce qui indiquait que l'ordinateur était capable de communiquer avec le routeur.



```
Administrator : Invite de commandes
Microsoft Windows [version 10.0.14393]
(c) 2016 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping 192.168.21.200

Envoi d'une requête 'Ping' 192.168.21.200 avec 32 octets de données :
Réponse de 192.168.21.200 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.21.200:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\Administrateur>
```

J'ai également effectué un ping vers un autre appareil connecté au même réseau pour vérifier si l'ordinateur était capable de communiquer avec d'autres appareils.

J'ai reçu des réponses de l'autre appareil, ce qui indiquait que l'ordinateur était capable de communiquer avec d'autres appareils sur le réseau.

Finalement, j'ai effectué un test de ping vers un serveur distant pour vérifier si l'ordinateur était capable de se connecter à Internet. J'ai reçu des réponses du serveur distant, ce qui indiquait que l'ordinateur était capable de se connecter à Internet.

Après avoir effectué ces tests de ping, j'ai conclu que la panne réseau était due à un problème de configuration sur la carte réseau de l'ordinateur. J'ai ajusté les paramètres de la carte réseau pour résoudre le problème et j'ai répété les mêmes tests de ping pour vérifier que la connexion avait été rétablie avec succès.

En conclusion, grâce à l'ensemble de ces actions de diagnostic et de dépannage, j'ai pu résoudre le problème de connexion réseau sur l'ordinateur et vérifier que la connexion avait été rétablie avec succès.

2. Précisez les moyens utilisés :

- Environnement classe AFPA avec :
- Serveur win2016 serveur
- Bie de brassage
- Câbles Ethernet

3. Avec qui avez-vous travaillé ?

En centre de formation Afpa en coopération avec mon formateur Patrice Krzanik

4. Contexte

Nom de l'entreprise, organisme ou association ► *Centre de formation Afpa Champs-sur-Marne*

Chantier, atelier, service ► Atelier Afpa

Période d'exercice ► Du 12/01/2023 au 12/01/2023

5. Informations complémentaires (*facultatif*)

En réalisant cette activité, j'ai appris beaucoup de choses sur la résolution de problèmes de connexion réseau. J'ai pu identifier les éléments qui peuvent être à l'origine d'un problème de connexion et comment utiliser des outils de diagnostic tels que le gestionnaire de périphériques et les commandes ping pour diagnostiquer les problèmes de réseau.

J'ai également appris comment configurer les paramètres de réseau pour assurer une connectivité réseau optimale. En vérifiant les câbles, j'ai pu identifier que certains d'entre eux n'étaient pas correctement connectés, ce qui causait le problème de connexion. J'ai ensuite corrigé le problème en connectant correctement le câble.

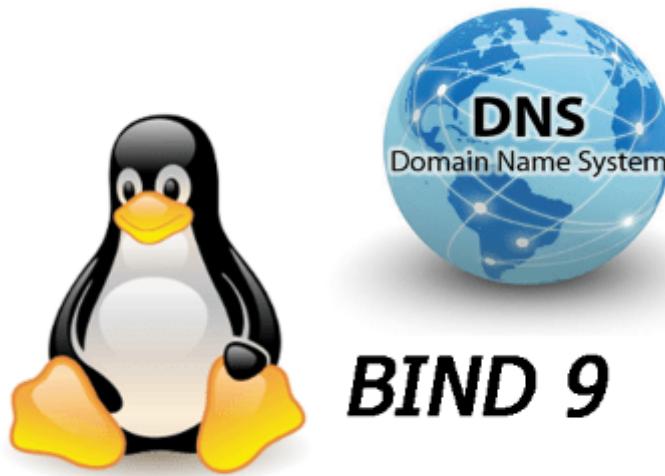
J'ai également vérifié que les paramètres de ma carte réseau étaient correctement configurés, ce qui a résolu le problème de connexion. Après avoir effectué ces actions, j'ai effectué des tests de validation en utilisant des commandes ping pour vérifier que la connexion avait été rétablie avec succès.

En résumé, cette activité m'a permis de développer mes compétences en matière de résolution de problèmes de réseau et d'apprendre comment diagnostiquer et résoudre les problèmes de connexion réseau en utilisant des outils de diagnostic standardisés.

Activité-type 2 Maintenir, exploiter et sécuriser une infrastructure centralisée

Exemple n°1 ▶ Installation et configuration d'un serveur DNS sur Debian

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :



Dans le cadre d'un TP, je dois mettre en place un serveur DNS (Domaine Name service) sur une machine Debian version 10.9 en type Master

- ✓ J'ai configuré des adresses IP statique sur mes serveurs Debian
Pour cela je me rends au fichier de configuration qui se trouve dans /etc/network/interface
 - Je choisis l'adresse IPv4 10.0.2.15/24 pour mon serveur Master
- ✓ Je vérifie ma liste des dépôts dans le fichier /etc/apt/sources.list.
- ✓ Je mets à jour mes systèmes avec un apt-get update ça va mettre à jour la base de données qui contient la liste de tous les logiciels qui sont installable sur nos systèmes
- ✓ Installer le paquet bind9 avec la commande apt-get install bind9
- ✓ Modifier le fichier /etc/hostname pour y mettre le nom FQDN du serveur DNS
- ✓ Modifier le fichier /etc/hosts pour associer l'adresse IP du serveur DNS à son nom FQDN
- ✓ Modifier le fichier /etc/resolv.conf (client DNS) pour indiquer le domaine et la zone de recherche DNS, dans mon cas le domaine est mondomaine.lan et d
- ✓ Modifier le fichier /etc/bind/named.conf.local pour déclarer les zones DNS à gérer par le serveur
- ✓ Je créer mes fichiers de base de données à partir des fichiers existant, Je créer les databases pour notre domaine mondomaine.lan : cp db.local db.mondomaine.lan (fichiers de

zone directe) et cp db.127 db.mondomaine.lan.inv (fichiers de zone indirecte) et y définir les enregistrements DNS des machines du réseau

- ✓ Redémarrer le service bind9 avec la commande service bind9 restart
- ✓ Tester la configuration avec la commande systemctl status bind9 et corriger les éventuelles erreurs
- ✓ Tester le bon fonctionnement du serveur DNS avec les commandes dig, nslookup ou ping

2. Précisez les moyens utilisés :

- Deux pc avec systèmes d'exploitation linux avec la distribution Debian 10.9
- Virtuelle box

3. Avec qui avez-vous travaillé ?

En centre de formation Afpa en coopération avec mon formateur Patrice Krzanik

4. Contexte

Nom de l'entreprise, organisme ou association ► ***Centre de formation AFPA***

Chantier, atelier, service ► Atelier Afpa

Période d'exercice ► Du 24/01/2023 Au 24/01/2023

5. Informations complémentaires (*facultatif*)

En suivant une activité d'installation d'un serveur DNS sur Linux Debian, j'ai appris les compétences suivantes :

- Installation du logiciel BIND (Berkeley Internet Name Domain) : j'ai appris à installer le logiciel BIND sur un système Linux Debian en utilisant les commandes apt.
- Configuration du fichier named.conf : j'ai appris à configurer le fichier named.conf pour définir les options de base du serveur DNS, telles que l'adresse IP du serveur, les options de journalisation, les options de sécurité, les options de contrôle d'accès, etc.
- Création de fichiers de zone : j'ai appris à créer des fichiers de zone pour définir les enregistrements de ressources (RR) pour les domaines gérés par le serveur DNS.
- Test de la configuration : j'ai appris à tester la configuration du serveur DNS en utilisant les commandes nslookup et dig pour vérifier la résolution des noms de domaine.
- Dépannage des problèmes : j'ai appris à dépanner les problèmes courants rencontrés lors de l'installation et de la configuration d'un serveur DNS, tels que les erreurs de configuration, les erreurs de zone, les erreurs de sécurité, etc.

En suivant cette activité, j'ai une compréhension approfondie des bases du serveur DNS et des techniques d'installation et de configuration sur un système Linux Debian. Cela peut m'aider à développer mes compétences en matière d'administration système et à gérer efficacement les ressources informatiques dans mon organisation.

Activité-type 2

Maintenir, exploiter et sécuriser une infrastructure centralisée

Exemple n°2 ► Création d'un environnement virtualisé sur ESXI avec migration à chaud des serveurs virtuelle

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

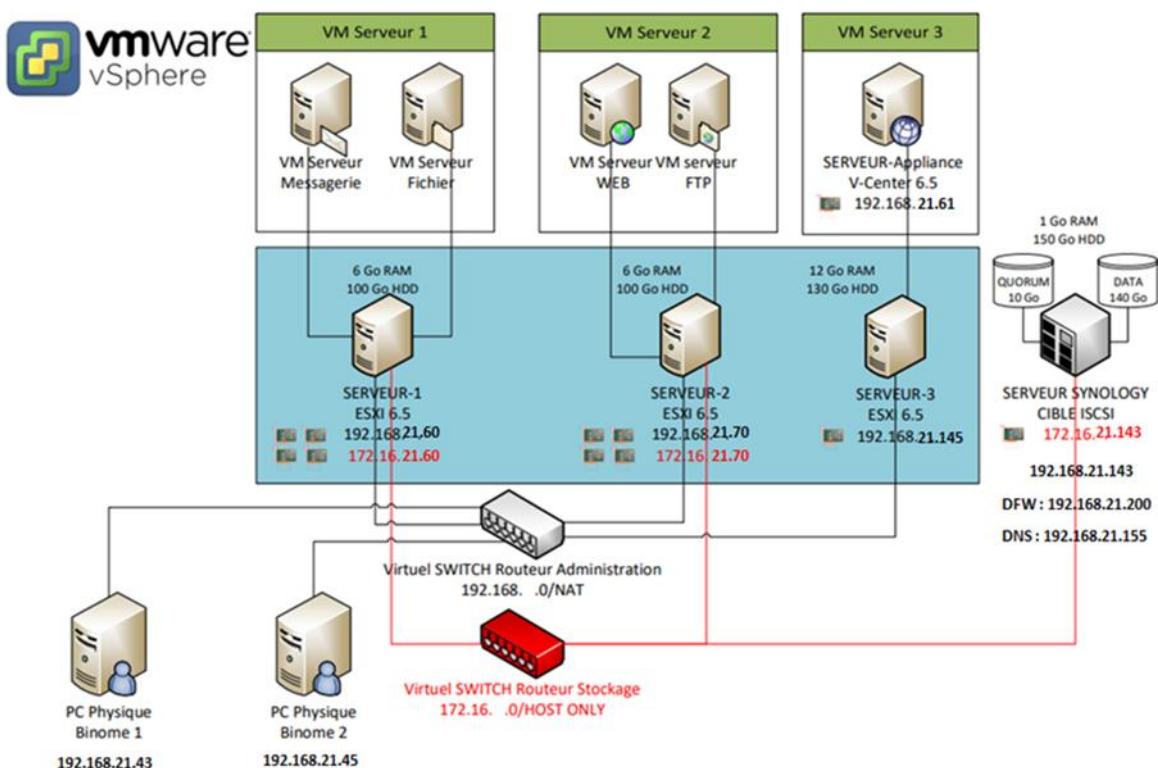
L'objectif de cette mission est de nous familiariser avec un environnement vtilisé, nous allons mettre en place

l'architecture ci-après avec un hyperviseur de type 1 (ESXI 6.5). Ce schéma se fera dans un environnement virtualité, car l'ESXI repose lui-même sur un système d'exploitation.

Pour la réalisation de ce projet, nous avons mis en place :

- Trois serveurs ESXI. Le premier serveur héberge les serveurs Messagerie et Fichier, le deuxième serveur héberge les serveurs WEB et FTP et le troisième dispose du VCenter uniquement
- Serveur Synology
- Serveur VCenter

Schéma de connexion des serveurs ESXI 6.5



Ce projet est détaillé sous forme de procédure, qui se trouve en annexe, dans laquelle nous expliquerons par étape l'ensemble des tâches effectuées.

2. Précisez les moyens utilisés :

- VMware Workstation pro 17
- Deux PC Windows
- Un Synology S.A.N
- Des images ISO ESXi 6.5.0
- Image ISO du VCenter

3. Avec qui avez-vous travaillé ?

En binôme avec Solange Sanches Pereira sous la supervision de notre formateur Luis de Oliveira en atelier de formation Afpa

4. Contexte

Nom de l'entreprise, organisme ou association ► **Centre de formation Afpa Champs-sur-Marne**

Chantier, atelier, service ► Atelier

Période d'exercice ► Du 12/12/2022 Au 15/12/2022

5. Informations complémentaires (facultatif)

En suivant une activité de création d'un environnement virtualisé sur ESXi avec migration à chaud de serveurs virtuels, vous pouvez apprendre les compétences suivantes:

- ✓ Virtualisation avec VMware ESXi : j'ai appris à utiliser le logiciel VMware ESXi pour créer et gérer des machines virtuelles. J'ai également appris à installer et à configurer ESXi sur un serveur physique.
- ✓ Création de machines virtuelles : j'ai appris à créer des machines virtuelles à l'aide de VMware VSphere, en définissant les paramètres de base tels que la configuration du processeur, de la

mémoire, du disque dur, etc.

- ✓ Migration à chaud : j'ai appris à effectuer une migration à chaud de serveurs virtuels, ce qui signifie que le serveur virtuel continue à fonctionner pendant la migration vers un autre hôte ESXi.
- ✓ Stockage de données : j'ai appris à utiliser des systèmes de stockage en réseau (SAN) pour stocker les données des machines virtuelles, ce qui permet une meilleure disponibilité et une gestion plus facile des données.
- ✓ Sauvegarde et restauration : j'ai appris à effectuer des sauvegardes des machines virtuelles et à les restaurer en cas de problèmes.

En suivant cette activité, j'ai acquis une solide compréhension de la virtualisation avec VMware ESXi et de la migration à chaud de serveurs virtuels. J'ai également développé mes compétences en matière de gestion de serveurs virtuels et améliorer mes capacité à déployer des environnements virtualisés fiables et efficaces

Activité-type 2

Maintenir, exploiter et sécuriser une infrastructure centralisée

Exemple n°3 ▶ Configuration des accès à distance sur un commutateur Cisco avec le protocole Secure Shell (SSH)

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

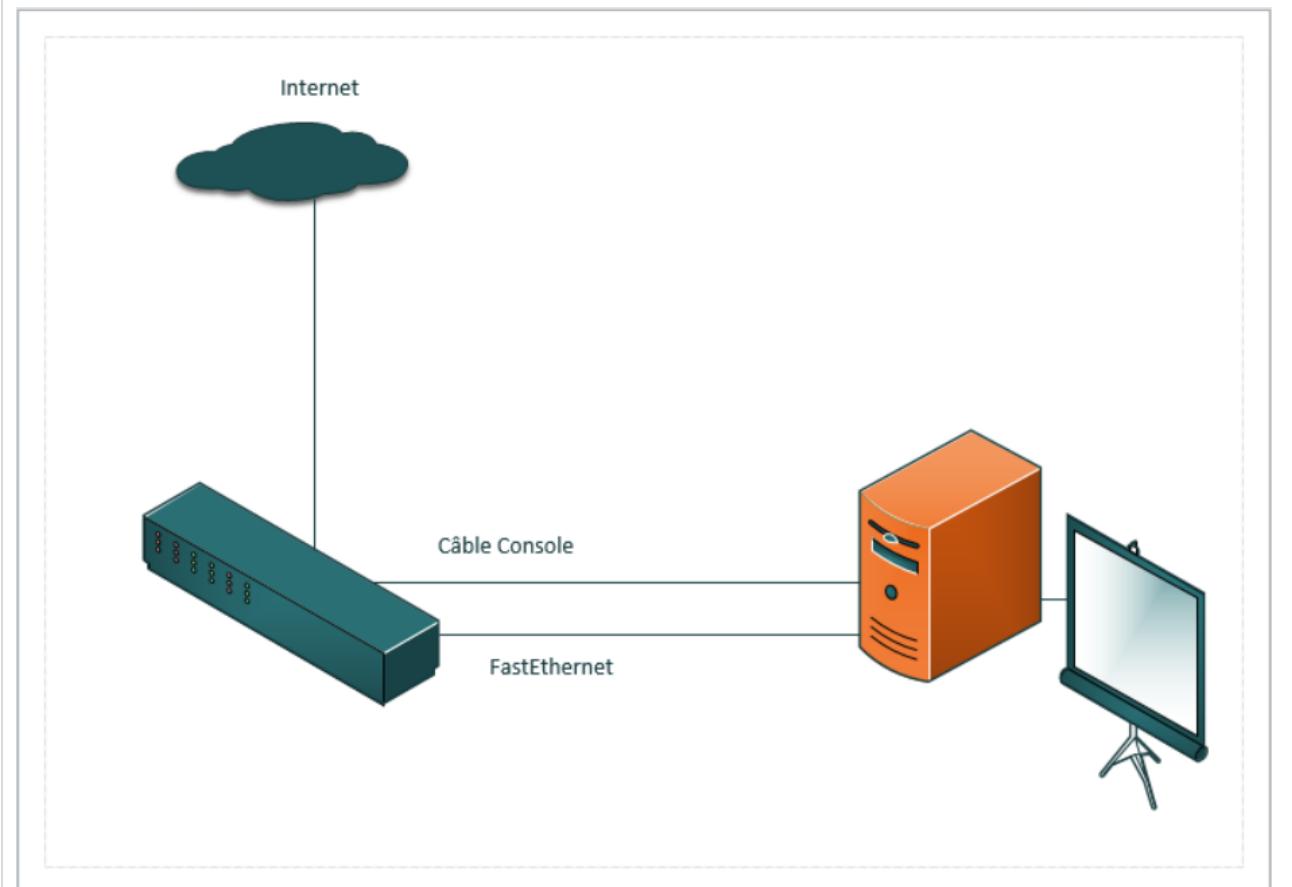
SENARIO : tout comme Telnet, Secure Shell (SSH, port 22) est un protocole qui permet de se connecter à un commutateur ou un routeur distant, mais de manière bien plus sécurisée. En effet, ce protocole chiffre les données, ce que Telnet ne fait pas.

Le but ici est de configurer une connexion SSH à un commutateur Cisco.

Ainsi, il est possible de configurer une connexion qui passe par un réseau public sans risque d'attaque sur la machine ou sur les équipements mis en relation lors de la connexion. Il existe deux versions du protocole. La deuxième version est la plus récente et la plus sécurisée à ce jour, c'est pourquoi je vais l'utiliser pour notre connexion SSH.

Pour commencer, réalisez une connexion en console entre l'équipement Cisco et votre PC.

Topologie :



Etape1 : configurer le VLAN de gestion

Dans notre cas, sa sera le VLAN99, grâce à cette interface et son adresse IP on pourra accéder à distance avec un logiciel comme Putty ou Tera Term, pour ce faire j'allume et réinitialise l'équipement le but n'est pas de récupérer l'ancienne configuration en accédent au mode Rammon

Mais d'avoir une nouvelle configuration

Je configure l'interface VLAN99 comme suit

```
switch# configure terminal
switch (config)# interface vlan 99
switch (config-if)# ip address 192.168.246.100 255.255.255.0
switch (config-if)# no shutdown
switch (config-if)# exit
switch (config)# ip default-gateway 192.168.245.200
```

Etape2 : Vérification de la version de l'équipement Cisco pour le protocole SSH

Avant toute chose, je vérifie que la version du commutateur Cisco est bien compatible avec le protocole SSH. Pour cela, je passe en mode configuration et entrez en ligne de commande "show version". Il faut que je retrouve dans la version de l'équipement le mot "K9" comme ci-dessous.

```
switch#show version
Cisco IOS Software, C2600 Software (C2600-ADVSECURITYK9-M), Version 12.4,
RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Mon 10-Sep-2007 07:57 by prod_rel_team

ROM: System Bootstrap, Version 12.2(8r) [cmong 8r], RELEASE SOFTWARE (fc1)

switch-CISCO-RTR uptime is 5 minutes
System returned to RM in power-on
System image file is "flash:c2600-advsecurityk9-mz.124-16a.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
```

Oui c'est le cas, je peux passer à l'étape suivante.

Etape 3 : Création des noms d'hôte et de domaine, et d'un mot de passe pour le mode privilégié

La création d'un nom d'hôte et d'un nom de domaine est indispensable à la configuration d'une connexion SSH. Je dois donc être en mode configuration et réaliser les commandes suivantes :

```
hostname <nom_hôte>
ip domain-name <nom_domaine>
```

Ici, nous avons choisi de donner pour nom d'hôte switch-omar et pour nom de domaine omar.local.

```
switch#conf t
Enter configuration commands, one per line; End with CNTL/Z
switch(config)#hostname switch-omar
switch-omar(config)#ip domain-name omar.local
switch-omar(config)#exit
switch-omar#
*Mar1 02:59:36.308: %SYS-5-CONFIG_I: Configured from console by console
```

Pour créer un mot de passe pour le mode privilégié, je passe en mode configuration et entrer la commande :

```
switch-omar(conf-if)# enable password afpachamps
```

Etape 4 : Génération de la paire de clés asymétriques RSA

RSA est une méthode de chiffrement dite asymétrique. Elle est composée de deux clés, une privée et une publique, chiffrées sur 768 bits minimum pour le SSH v2, et permet d'assurer une sécurité optimale. Pour générer cette paire de clés, il suffit d'entrer la commande :

```
crypto key generate rsa
```

Il est également demandé d'entrer la taille souhaitée de la clé en bits. Il est préférable de choisir une taille supérieure à 768 bits pour assurer une plus grande sécurité. Nous avons ici choisi des clés de 1024 bits.

```
switch-omar>enable
Password:
switch-omar#conf t
Enter configuration commands, one per line; End with CNTL/Z
switch-omar(config)#crypto key generate rsa
The name for the keys will be: omar.omar-ssh.local
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take a
few minutes.
```

```
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable. . . [OK]

*Mar1 00:57:25.621: %SSH-5-ENABLED: SSH 1.99 has been enabled
switch-omar(config) #
```

Etape 5: Activation du protocole SSH sur le commutateur Cisco

Pour activer le protocole SSH, il suffit d'entrer la commande “*ip ssh version 2*”. Il faut ensuite entrer en mode configuration de ligne VTY dans le but de :

- ✓ N'accepter que les connexions SSH au routeur ou au Switch, au moyen de la commande “*transport input ssh*” ;
- ✓ Ne permettre que des connexions SSH vers d'autres équipements, au moyen de la commande “*transport output ssh*” ;
- ✓ Enregistrer le compte utilisateur existant comme compte permettant de mettre en place la connexion en entrant “*login local*”.

```
switch-omar(config)#ip ssh version 2
switch-omar(config)#line vty 0 4
switch-omar(config-line)#transport input ssh
switch-omar(config-line)#transport output ssh
switch-omar(config-line)#login local
switch-omar(config-line)#exit
switch-omar(config)#
switch-omar(config)#username omar password afpachamps
```

Je vérifie que la configuration a bien été prise en compte par l'équipement, entrez “*show run*”.

```
switch-omar #sh run
Building configuration. . .

Current configuration 1272 bytes
!
Revision 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname switch-omar
!
boot-start-marker
boot-end-marker
```

```
!
--More--█
!
line con 0
line aux 0
line vty 0 4
password 7 08354942071C110713181F13253920
login local
transport input ssh
transport output ssh
!
--More--
```

J'oublie pas d'entrer

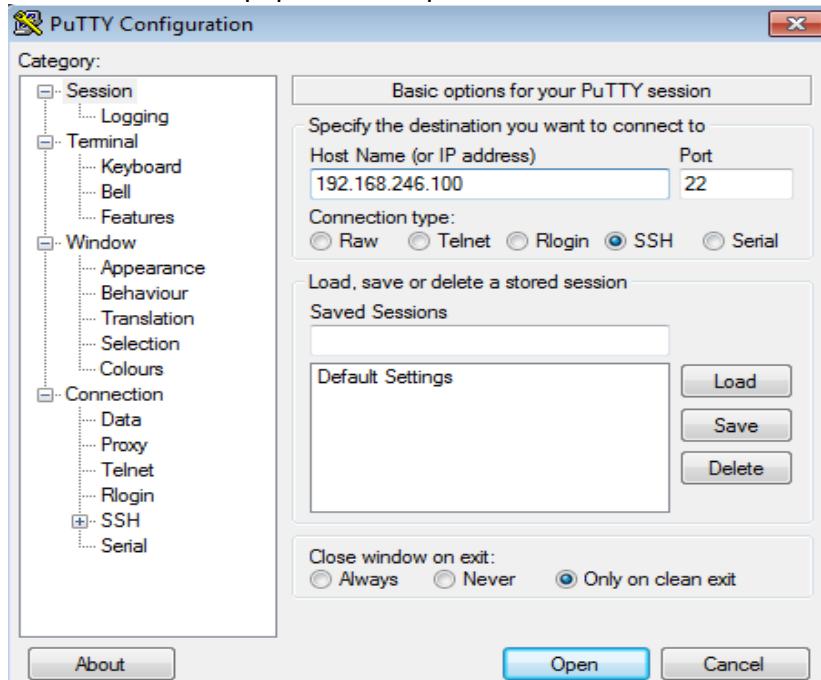
```
copy running-config startup-config
```

puis j'appuie deux fois sur Entrée pour conserver la configuration après une mise hors tension du commutateur Cisco.

Etape 6: Test de connexion SSH avec PuTTY

Je déconnecte la connexion console et je me connecte au commutateur avec un câble Ethernet. Windows ne possède pas de client SSH natif. Il faut donc en télécharger un. Il est possible d'utiliser PuTTY, logiciel téléchargeable gratuitement.

Pour le mettre en mode SSH, il vous suffit de cliquer sur "SSH" et d'entrer le nom d'hôte ou l'adresse IP de l'équipement auquel vous voulez vous connecter.



Je cliquant sur "Open", j'accède à la console du périphérique. J'entre le Username et password

créés précédemment. Je suis maintenant connecté en SSH. Pour passer en mode privilégié, il ne reste qu'à entrer le "enable password" déjà configuré.

```
login as: omar
switch@192.168.246.100's password:

switch-omar >en
Password:
switch-omar #
```

2. Précisez les moyens utilisés :

Les moyens utilisés :

- Commutateur Cisco
- Ordinateur avec systèmes d'exploitation Windows
- Logiciel d'accès à distance Putty
- Câble console

3. Avec qui avez-vous travaillé ?

En centre Afpa, supervisé par ma formatrice Claire Sobesky et en m'aident des supports cours Cisco

4. Contexte

Nom de l'entreprise, organisme ou association ► **Centre de formation Afpa Champs-sur-Marne**

Chantier, atelier, service ► Atelier Afpa

Période d'exercice ► Du 10/11/2022 au 10/11/2022

5. Informations complémentaires (facultatif)

Cette activité m'a permis de comprendre les méthodes de configuration à distance et la façon de les crypter la configuration localement et en ligne (à distance)

- ✓ Lors de cette activité de configuration des accès à distance sur un commutateur Cisco avec le protocole Secure Shell (SSH), j'ai appris les concepts suivants :
- ✓ Configuration de base de SSH sur un commutateur Cisco: j'ai appris comment configurer et activer SSH sur un commutateur Cisco pour permettre aux administrateurs réseau de se connecter à distance en toute sécurité.
- ✓ Création d'un nom d'hôte et d'une adresse IP: j'ai appris à assigner un nom d'hôte et une adresse IP statique à un commutateur pour qu'il puisse être trouvé sur le réseau.
- ✓ Configuration des utilisateurs locaux: j'ai appris à créer et à gérer des comptes d'utilisateurs locaux sur un commutateur Cisco pour permettre aux administrateurs réseau de se connecter à distance.
- ✓ Sécurité SSH: j'ai appris comment sécuriser les connexions SSH en utilisant des mécanismes tels que la vérification des clés publiques et la protection par mot de passe.
- ✓ Vérification de la configuration: j'ai appris à vérifier la configuration SSH et les connexions à distance pour s'assurer que tout fonctionne correctement.

En résumé, l'objectif de cette activité est de m'apprendre à configurer et à gérer les accès à distance sécurisés à un commutateur Cisco en utilisant le protocole SSH.

Activité-type 3

Maintenir, exploiter une infrastructure distribuée et contribuer à sa sécurisation

Exemple n°1 ▶ configurer un VPN-SSL client-to-site avec OpenVPN"

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

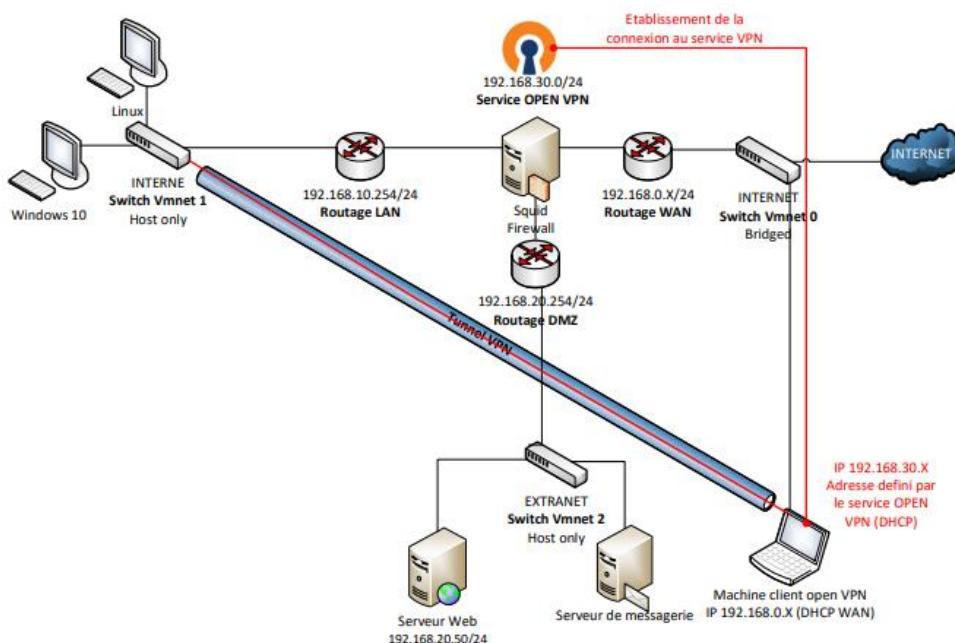
OpenVPN est une application gratuite et open source qui implémente les techniques de réseau privé virtuel (VPN) pour créer des connexions sécurisées de point à point ou de site à site dans des configurations en routées ou en pont et des installations d'accès à distance.

Il utilise un protocole de sécurité personnalisé qui utilise SSL / TLS pour l'échange de clés.

OpenVPN peut traverser les traducteurs d'adresses de réseau (NAT) et les pare-feu, ce qui en fait un outil idéal pour une utilisation dans les réseaux larges et complexes.

OpenVPN est souvent utilisé pour étendre les intranets dans des emplacements distants et pour connecter en toute sécurité les employés en télétravail à leur réseau siège social. Il est également fréquemment utilisé par les particuliers pour protéger leur trafic Internet.

Schéma explicatif :



Je veux mettre en place un VPN nomade avec OpenVPN sur PfSense pour permettre à mes utilisateurs distants d'accéder au réseau local de mon entreprise de manière sécurisée.

- ✓ Je crée une autorité de certification interne sur pfSense pour générer les certificats nécessaires à l'authentification des clients et du serveur VPN
- ✓ Je configure le serveur OpenVPN sur PfSense en choisissant le mode client-to-site et en spécifiant les paramètres de sécurité, le réseau du tunnel VPN et les routes à pousser aux clients
- ✓ Je crée les utilisateurs locaux sur pfSense qui auront accès au VPN et je leur attribue un certificat
- ✓ J'installe le plugin OpenVPN Client Export Utility sur PfSense pour exporter facilement les fichiers de configuration des clients VPN
- ✓ Je configure les règles du firewall sur PfSense pour autoriser le trafic entrant et sortant du VPN
- ✓ Je teste le bon fonctionnement du VPN en me connectant depuis un poste client avec le logiciel OpenVPN et en vérifiant que j'ai accès aux ressources du réseau local

2. Précisez les moyens utilisés :

- Firewall Pfsense
- Pc portable avec systèmes d'exploitation Windows 10
- Procédure fournis par notre Formateur
- Machine virtuelle sur un Lan (Windows 2010)

3. Avec qui avez-vous travaillé ?

En centre de formation Afpa en coopération avec mon formateur Luis de Oliveira

4. Contexte

Nom de l'entreprise, organisme ou association ► **Centre de formation Afpa Champs-sur-Marne**

Chantier, atelier, service ► Atelier Afpa

Période d'exercice ► Du 19/12/2022 au 19/12/2022

5. Informations complémentaires (facultatif)

En installant un serveur OpenVPN et un client, j'ai appris les compétences suivantes :

1. Configuration de serveurs : j'ai appris comment configurer et gérer un serveur VPN en utilisant OpenVPN, y compris la gestion des paramètres de sécurité, la gestion des utilisateurs, etc.
2. Réseau et sécurité : j'ai appris les concepts de base de la sécurité du réseau, tels que l'encryptions de données, le masquage d'adresses IP, etc.
3. Système d'exploitation : utiliser l'interface de ligne de commande et à effectuer des tâches de base dans le système d'exploitation sur lequel vous installez OpenVPN.
4. Dépannage : diagnostiquer et à résoudre les problèmes liés à la configuration d'OpenVPN, tels que les problèmes de connexion, les problèmes de sécurité, etc.
5. Ces compétences peuvent être utiles pour les professionnels de l'informatique, les administrateurs réseau et les développeurs souhaitant apprendre à configurer et gérer des réseaux privés virtuels.

Activité-type 3

Maintenir, exploiter une infrastructure distribuée et contribuer à sa sécurisation

Exemple n°2 ▶ Installation et configuration d'un serveur de déploiement WDS avec une machine de référence dans un environnement Active Directory

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

L'installation et la configuration d'un serveur de déploiement WDS (Windows Déploiement Services) est une compétence clé pour les administrateurs système qui souhaitent déployer rapidement et efficacement des images de système d'exploitation Windows sur plusieurs machines. Cette activité consiste à installer le rôle de serveur WDS, à créer une image de référence et à tester le déploiement en utilisant une machine virtuelle, tout en étant intégré à un environnement Active Directory.

Voici brièvement les étapes :

1. Installation et configuration du rôle de serveur WDS :
 - J'ai ouvert le Gestionnaire de serveur sur notre serveur Windows Server.
 - J'ai cliqué sur "Ajouter des rôles et des fonctionnalités" et j'ai suivi les étapes de l'Assistant d'installation pour ajouter le rôle de serveur WDS.
 - J'ai configuré les options de déploiement en créant un répertoire de déploiement et en spécifiant les images d'installation à déployer.
2. Création d'une image de référence en utilisant le sysprep pour généraliser l'image :
 - J'ai installé Windows sur une machine de référence en utilisant une clé de produit valide.
 - J'ai personnalisé les paramètres de l'ordinateur en fonction de nos besoins.
 - J'ai exécuté le sysprep pour généraliser l'image et la préparer pour le déploiement. J'ai choisi les options appropriées pour le mode de généralisation, l'arrêt de l'ordinateur et le stockage de l'image dans le répertoire de déploiement créé précédemment.
3. Configuration du serveur DHCP pour fournir les informations de configuration réseau nécessaires pour le déploiement PXE :
 - J'ai ouvert le Gestionnaire de serveur DHCP sur notre serveur Windows Server.
 - J'ai ajouté un nouveau port étendu pour les clients PXE en utilisant les paramètres appropriés pour l'adresse IP et les options de configuration réseau.
 - Dans mon cas le serveur DHCP et le serveur WDS sont installés sur la même machine Je n'ai pas besoin de configurer l'option 60 pour spécifier que le client PXE est un ordinateur x86 ni de configurer l'option 66 pour spécifier l'adresse IP du serveur WDS, aussi je n'ai pas eu besoin de configurer l'option 67 pour spécifier le nom du fichier de démarrage à utiliser pour le déploiement PXE.
4. Test du déploiement en utilisant une machine virtuelle :
 - J'ai créé une machine virtuelle et j'ai configuré le BIOS pour qu'il amorce à partir du réseau.
 - J'ai démarré la machine virtuelle et j'ai vérifié qu'elle avait obtenu une adresse IP à partir du serveur DHCP et qu'elle avait téléchargé le fichier de démarrage à partir du serveur WDS.

- J'ai sélectionné l'image d'installation que j'avais créée précédemment et j'ai commencé le processus de déploiement.

En suivant ces étapes, j'ai réussi à installer et configurer un serveur de déploiement WDS fonctionnel dans notre environnement Active Directory, prêt à être utilisé pour déployer des images de système d'exploitation Windows sur nos machines clientes.

2. Précisez les moyens utilisés :

Voici une liste des moyens utilisés pour réaliser l'installation et la configuration du serveur de déploiement WDS sur VMware :

Matériel :

- Un ordinateur hôte avec le logiciel VMware installé
- Une machine virtuelle configurée avec les ressources nécessaires pour héberger le système d'exploitation Windows Server, telle que la mémoire RAM, l'espace de stockage, etc.
- Une machine de référence pour créer l'image à déployer
- Une machine virtuelle pour tester le processus de déploiement

Logiciel :

- Windows Server, version appropriée pour votre environnement, installé dans la machine virtuelle
- Le rôle de serveur WDS ajouté à Windows Server
- Le sysprep pour généraliser l'image de référence
- Un logiciel de virtualisation tel que VMware Workstation pour créer la machine virtuelle de test
- Le Gestionnaire de serveur pour ajouter les rôles et les fonctionnalités nécessaires
- Le Gestionnaire de serveur DHCP pour configurer les options de réseau nécessaires pour le déploiement PXE

3. Avec qui avez-vous travaillé ?

En atelier du centre de Formation Afpa en collaboration avec ma Formatrice Claire Sobesky

4. Contexte

Nom de l'entreprise, organisme ou association ► **Centre de formation Afpa Champs-sur-Marne**

Chantier, atelier, service ► Atelier Afpa

Période d'exercice ► Du 16/03/2023 au 16/03/2023

5. Informations complémentaires (facultatif)

Au cours de cette activité, j'ai appris comment installer et configurer un serveur de déploiement WDS dans un environnement Active Directory, en utilisant une machine de référence pour créer une image de système d'exploitation Windows personnalisée.

J'ai également compris comment configurer le service DHCP pour activer le déploiement PXE, ainsi que les différentes options de configuration requises pour que le processus de déploiement fonctionne correctement.

De plus, j'ai découvert l'importance de généraliser l'image de référence à l'aide de l'outil Sysprep, pour éviter les problèmes de duplication SID lors du déploiement sur plusieurs machines.

Enfin, j'ai appris comment tester le processus de déploiement en utilisant une machine virtuelle, afin de m'assurer que le déploiement se déroule correctement avant de le déployer sur les machines clientes.

Dans l'ensemble, cette activité m'a permis de comprendre les étapes nécessaires pour installer et configurer un serveur de déploiement WDS et d'acquérir des compétences pratiques dans ce domaine.

Activité-type 3

Maintenir, exploiter une infrastructure distribuée et contribuer à sa sécurisation

Exemple n°3 ▶ Cliquez ici pour entrer l'intitulé de l'exemple

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

2. Précisez les moyens utilisés :

Cliquez ici pour taper du texte.

3. Avec qui avez-vous travaillé ?

Cliquez ici pour taper du texte.

4. Contexte

Nom de l'entreprise, organisme ou association ► Cliquez ici pour taper du texte.

Chantier, atelier, service ► Cliquez ici pour taper du texte.

Période d'exercice ► **Du** Cliquez ici **au** Cliquez ici

5. Informations complémentaires (*facultatif*)

Titres, diplômes, CQP, attestations de formation

(facultatif)

Intitulé	Autorité ou organisme	Date
Baccalauréat Science de la nature et de la vie	Algérie	2001
DEUG1	Denis Diderot Paris7	2003
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.

Déclaration sur l'honneur

Je soussigné(e) [prénom et nom] *MECHENANE OMAR*,
déclare sur l'honneur que les renseignements fournis dans ce dossier sont exacts et que je
suis l'auteur(e) des réalisations jointes.

Fait à *Montfermeil*..... le *12/02/2023*.
pour faire valoir ce que de droit.

Signature :

Documents illustrant la pratique professionnelle

(facultatif)

Intitulé

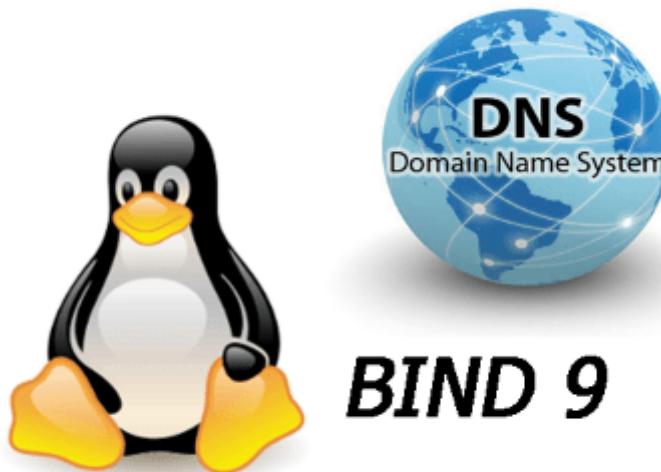
Procédure WIFI

Procédure virtualisation ESXI

ANNEXES

Activité-type 2 Maintenir, exploiter et sécuriser une infrastructure centralisée

Exemple n°1 ► Installation et configuration d'un serveur DNS sur Debian



Dans le cadre d'un TP, je dois mettre en place un serveur DNS (Domain Name service) sur une machine Debian version 10.9 en type Master et un serveur DNS secondaire de type Slave pour assurer la continuité

Du service en cas de sinistre

C quoi un serveur DNS ? :

Un serveur DNS (Domain Name System) est un système de noms de domaine qui permet de traduire les noms d'hôtes en adresses IP et inversement. Lorsque vous tapez une URL dans votre navigateur, votre ordinateur envoie une requête au serveur DNS pour obtenir l'adresse IP correspondante. Le serveur DNS répond à cette requête en fournissant l'adresse IP, ce qui permet au navigateur de charger la page web correspondante.

Les serveurs DNS sont importants pour l'internet car ils permettent aux utilisateurs de se connecter facilement aux sites web en utilisant des noms de domaine mémorisables au lieu d'adresses IP complexes. Les entreprises et les fournisseurs d'accès à Internet gèrent souvent leurs propres serveurs DNS pour assurer la rapidité et la fiabilité de la résolution des noms de domaine pour leurs clients.

Configuration du serveur DNS :

Etape 1 : sur mes deux serveurs je configure des adresses IP statique à mes serveurs Debian
Pour cela je me rends au fichier de configuration qui se trouve dans /etc/network/interface
Je choisis l'adresse IPv4 10.0.2.15/24 pour mon serveur Master

Etape 2 : je vérifie ma liste des dépôts dans le fichier /etc/apt/sources.list.

The screenshot shows two terminal windows side-by-side. Both windows have a title bar 'Activités Terminal' and a date/time '3 févr. 09:00'. The top window shows a script being run to create a menu script. The bottom window shows the root user editing the '/etc/apt/sources.list' file to add several repository entries for 'bullseye' and 'security' releases from 'deb cdrom' and 'deb http://security.debian.org' URLs. The bottom window also shows a status bar at the bottom with keyboard shortcuts for various functions like aide, recherche, et copier/coller.

```
Activités Terminal 3 févr. 09:00
Ouvrir Enregistrer
omar@debian11a:~/script
1 # [ ] omar@debian11a:~/script$ sh scriptmenu
2 [ ] omar@debian11a:~/script$ sh scriptmenu
3 [ ] omar@debian11a:~/script$ sh scriptmenu
4 [ ] omar@debian11a:~/script$ sh scriptmenu
5 [ ] omar@debian11a:~/script$ sh scriptmenu
6 [ ] omar@debian11a:~/script$ sh scriptmenu
7 [ ] omar@debian11a:~/script$ sh scriptmenu
8 [ ] omar@debian11a:~/script$ sh scriptmenu
9 [ ] omar@debian11a:~/script$ sh scriptmenu
10 [ ] omar@debian11a:~/script$ sh scriptmenu
11 [ ] omar@debian11a:~/script$ sh scriptmenu
12 [ ] omar@debian11a:~/script$ sh scriptmenu
13 [ ] omar@debian11a:~/script$ sh scriptmenu
14 [ ] omar@debian11a:~/script$ sh scriptmenu
15 [ ] omar@debian11a:~/script$ sh scriptmenu
16 [ ] omar@debian11a:~/script$ sh scriptmenu
17 [ ] omar@debian11a:~/script$ sh scriptmenu
18 [ ] omar@debian11a:~/script$ sh scriptmenu
19 [ ] omar@debian11a:~/script$ sh scriptmenu
20 [ ] omar@debian11a:~/script$ sh scriptmenu
21 [ ] omar@debian11a:~/script$ sh scriptmenu
22 [ ] omar@debian11a:~/script$ sh scriptmenu
23 [ ] omar@debian11a:~/script$ sh scriptmenu
24 [ ] omar@debian11a:~/script$ sh scriptmenu
25 [ ] omar@debian11a:~/script$ sh scriptmenu
26 [ ] omar@debian11a:~/script$ sh scriptmenu
27 [ ] omar@debian11a:~/script$ sh scriptmenu

Activités Terminal 3 févr. 09:01
Ouvrir Enregistrer
omar@debian11a:~/script
1 # [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
2 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
3 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
4 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
5 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
6 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
7 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
8 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
9 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
10 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
11 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
12 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
13 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
14 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
15 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
16 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
17 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
18 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
19 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
20 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
21 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
22 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
23 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
24 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
25 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
26 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
27 [ ] omar@debian11a:~/script$ nano /etc/apt/sources.list
```

puis je mets à jour mes systèmes avec un apt-get update ça va mettre à jour la base de données qui contient la liste de tous les logiciels qui sont installables sur nos systèmes

```
root@debian11a:/home/omar/script# apt-get update
Atteint :1 http://security.debian.org/debian-security bullseye-security InRelease
Atteint :2 http://deb.debian.org/debian bullseye InRelease
Lecture des listes de paquets... Fait
root@debian11a:/home/omar/script#
```

Etape 3 : Installer Bind9

BIND 9 est une implémentation open source du protocole DNS (Domain Name System). C'est l'un des serveurs DNS les plus couramment utilisés sur internet et dans les entreprises pour gérer les résolutions de noms de domaine.

BIND 9 offre une grande flexibilité et une grande fiabilité pour gérer les zones DNS, y compris la gestion des noms de domaine, des enregistrements de ressources (RR), des sous-domaines et des enregistrements de noms de serveur. Il peut être utilisé pour configurer des serveurs DNS primaires, secondaires ou en cache, selon les besoins de la configuration réseau.

En plus de ces fonctionnalités de base, BIND 9 inclut également des fonctionnalités avancées telles que la prise en charge de DNSSEC (Domain Name System Security Extensions), la journalisation des activités, la gestion des erreurs et des alertes, et la gestion des accès et des autorisations. En raison de sa robustesse et de sa fiabilité, BIND 9 est largement utilisé pour gérer les serveurs DNS dans les entreprises et les organisations de toutes tailles.

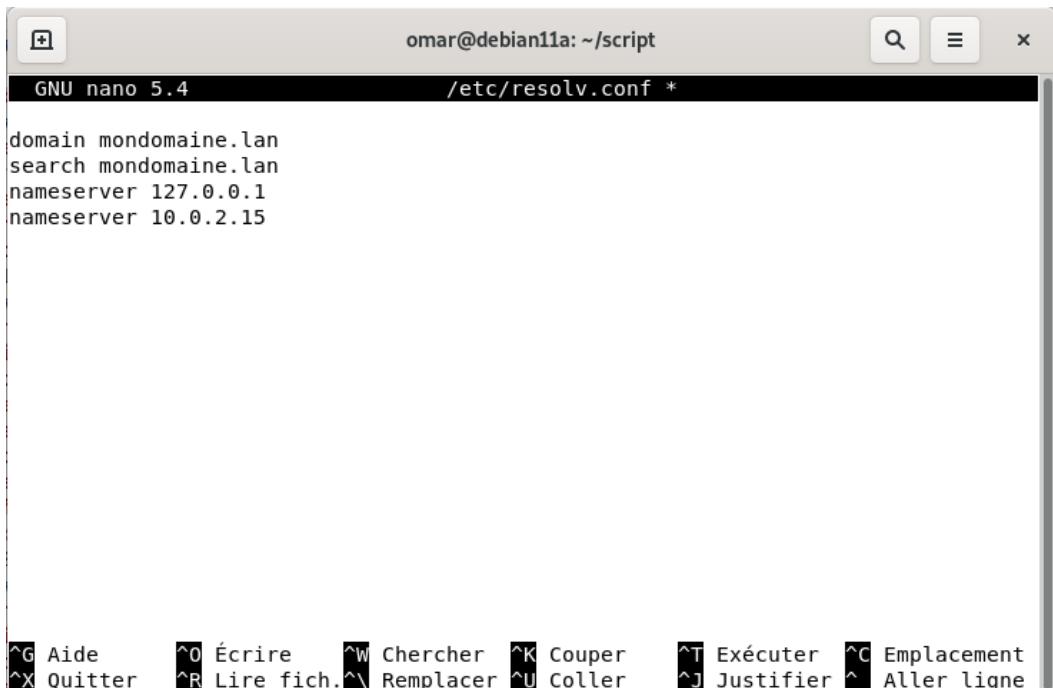
J'exécute la commande apt-get install bind9 et je suis la progression du téléchargement du paquet Bind9

```
root@debian11a:/home/omar/script# apt-get install bind9
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
  linux-image-5.10.0-10-amd64
Veuillez utiliser « apt autoremove » pour le supprimer.
Les paquets supplémentaires suivants seront installés :
  bind9-utils python3-ply
Paquets suggérés :
  bind-doc resolvconf ufw python-ply-doc
Les NOUVEAUX paquets suivants seront installés :
  bind9 bind9-utils python3-ply
0 mis à jour, 3 nouvellement installés, 0 à enlever et 1 non mis à jour.
Il est nécessaire de prendre 997 ko dans les archives.
Après cette opération, 2 351 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [0/n]
Réception de :1 http://security.debian.org/debian-security bullseye-security/main amd64 bind9-utils amd64 1:9.16.37-1~deb11u1 [435 kB]
Réception de :2 http://deb.debian.org/debian bullseye/main amd64 python3-ply all
```

Etape 4 : je modifie le fichier résolveur

```
root@debian11a:/home/omar/script# nano /etc/resolv.conf
```

pour cela je me rends dans le fichier /etc/resolv.conf et je procède aux modifications et spécifier que le search c'est **mondomaine.lan** et le domaine sera **mondomaine.lan** et que la machine 10.0.2.15 est mon serveur DNS



```
GNU nano 5.4          omar@debian11a: ~/script          /etc/resolv.conf *
```

```
domain mandomaine.lan
search mandomaine.lan
nameserver 127.0.0.1
nameserver 10.0.2.15
```

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich. ^Y Remplacer ^U Coller ^J Justifier ^ Aller ligne

Je me rends dans /etc/bind et je fais ls -l pour voir les fichiers existant

```
root@debian11a:/home/omar/script# cd /etc/bind
root@debian11a:/etc/bind# ls -l
total 48
-rw-r--r-- 1 root root 1991 25 janv. 16:22 bind.keys
-rw-r--r-- 1 root root 237 25 janv. 16:22 db.0
-rw-r--r-- 1 root root 271 25 janv. 16:22 db.127
-rw-r--r-- 1 root root 237 25 janv. 16:22 db.255
-rw-r--r-- 1 root root 353 25 janv. 16:22 db.empty
-rw-r--r-- 1 root root 270 25 janv. 16:22 db.local
-rw-r--r-- 1 root bind 463 25 janv. 16:22 named.conf
-rw-r--r-- 1 root bind 498 25 janv. 16:22 named.conf.default-zones
-rw-r--r-- 1 root bind 165 25 janv. 16:22 named.conf.local
-rw-r--r-- 1 root bind 846 25 janv. 16:22 named.conf.options
-rw-r----- 1 bind bind 100 3 févr. 09:09 rndc.key
-rw-r--r-- 1 root root 1317 25 janv. 16:22 zones.rfc1918
root@debian11a:/etc/bind#
```

Je créer mes fichiers de base se donner à partir des fichiers existant

Je créer les data bases pour notre domaine mandomaine.lan : cp db.local db.mandomaine.lan cp db.127 db.mandomaine.lan.inv

```
root@debian11a:/etc/bind# cp db.local db.mandomaine.lan
root@debian11a:/etc/bind# cp db.127 db.mandomaine.lan.inv
root@debian11a:/etc/bind#
```

Pour information : "db.local" est un fichier de configuration de zone qui peut être utilisé pour définir les enregistrements de ressources (RR) pour le nom de domaine local. Par exemple, vous pouvez utiliser ce fichier pour définir des noms d'hôte et des adresses IP pour les ordinateurs de votre réseau local.



"**db.127**" est un fichier de configuration de zone qui peut être utilisé pour définir les enregistrements de ressources pour la plage d'adresses IP de bouclage local "127.0.0.0/8". Cette plage d'adresses est réservée pour l'utilisation sur les ordinateurs individuels et ne doit pas être utilisée sur un réseau étendu. Les ordinateurs utilisent souvent ces adresses pour les applications telles que "localhost" pour se référer à eux-mêmes.

Ces fichiers sont des fichiers de configuration optionnels pour le serveur DNS BIND, et leur utilisation dépend des besoins spécifiques de la configuration DNS. Il est important de bien comprendre les fichiers de configuration de zone pour pouvoir configurer correctement le serveur DNS BIND

*Etape 5 : je configure le fichier **named.conf.local***

Le fichier **named.conf** est un fichier de configuration principal pour le serveur DNS BIND. Il définit les options de base pour le fonctionnement du serveur DNS, telles que l'adresse IP du serveur, les options de journalisation, les options de sécurité, les options de contrôle d'accès, etc.

Le fichier named.conf définit également les zones DNS gérées par le serveur et les options associées à chaque zone. Cela inclut la définition des zones primaires et secondaires, des enregistrements de ressources (RR), des enregistrements de noms de serveur, des sous-domaines, etc.

Le fichier named.conf est un fichier de configuration crucial pour le serveur DNS BIND, car il détermine comment le serveur se comportera et gérera les requêtes DNS. Il est donc important de bien comprendre les options et les syntaxes du fichier named.conf pour pouvoir configurer correctement le serveur DNS BIND.

```
GNU nano 5.4          named.conf.local *
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
zone "mondomaine.lan" {
    type master;
    file "/etc/bind/db.mondomaine.lan";
};
zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.mondomaine.lan.inv";
};

^G Aide      ^O Écrire      ^W Chercher      ^K Couper      ^T Exécuter      ^C Emplacement
^X Quitter   ^R Lire fich.  ^M Remplacer   ^U Coller       ^J Justifier   ^_ Aller ligne
```

Ainsi on crée notre zone DNS mondomaine.lan, en spécifiant que le serveur en est le « maître », et que la liste des éléments à résoudre se trouve dans le fichier /etc/bind/db.mondomaine.lan. De

la même manière on crée notre zone reverse DNS (c'est-à-dire capable de faire la translation d'une adresse IP vers un nom) qui couvre les IPs appartenant au réseau 10.0.2.15 /24 et dont la liste des éléments à résoudre se trouve dans le fichier /etc/bind/db.mondomaine.lan.inv .

Etape 6 : je configure le fichier db.mondomaine.lan comme ceci

```
GNU nano 5.4          db.mondomaine.lan *
```

```
; BIND data file for mondomaine.lan
;
$TTL    604800
@       IN      SOA     ns.mondomaine.lan. root.mondomaine.lan. (
                        2           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
@       IN      NS      localhost.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
@       IN      NS      ns.mondomaine.lan.
ns      IN      A       10.0.2.15
```

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich.^V Remplacer ^U Coller ^J Justifier ^L Aller ligne

*Etape6 : je configure le fichier db.mondomaine.lan.inv
Comme ceci :*

```
GNU nano 5.4          db.mondomaine.lan.inv *
```

```
; BIND reverse data file for mondomaine.lan
;
$TTL    604800
@       IN      SOA     ns.mondomaine.lan. root.mondomaine.lan. (
                        1           ; Serial
                        604800      ; Refresh
                        86400       ; Retry
                        2419200     ; Expire
                        604800 )    ; Negative Cache TTL
;
@       IN      NS      ns.mondomaine.lan.
15      IN      PTR     ns.mondomaine.lan.
```

^G Aide ^O Écrire ^W Chercher ^K Couper ^T Exécuter ^C Emplacement
^X Quitter ^R Lire fich.^V Remplacer ^U Coller ^J Justifier ^L Aller ligne

Etape 7 : redémarrer le service bind9 et faire les vérifications

Je tape la commande pour redémarrer le service bind9

```
root@debian11a:/etc/bind# systemctl restart bind9
Puis je vérifie le fonctionnement de mon serveur DNS
root@debian11a:/etc/bind# systemctl status bind9
● named.service - BIND Domain Name Server
  Loaded: loaded (/lib/systemd/system/named.service; enabled; vendor preset:>)
  Active: active (running) since Fri 2023-02-03 10:28:40 CET; 11s ago
    Docs: man:named(8)
  Main PID: 21932 (named)
    Tasks: 4 (limit: 4660)
   Memory: 14.5M
      CPU: 61ms
     CGroup: /system.slice/named.service
             └─21932 /usr/sbin/named -f -u bind

févr. 03 10:28:40 debian11a named[21932]: zone 127.in-addr.arpa/IN: loaded seri>
févr. 03 10:28:40 debian11a named[21932]: network unreachable resolving './DNSK>
févr. 03 10:28:40 debian11a named[21932]: network unreachable resolving './NS/I>
févr. 03 10:28:40 debian11a named[21932]: zone 255.in-addr.arpa/IN: loaded seri>
févr. 03 10:28:40 debian11a named[21932]: zone mondomaine.lan/IN: sending notif>
févr. 03 10:28:40 debian11a named[21932]: zone localhost/IN: loaded serial 2
févr. 03 10:28:40 debian11a named[21932]: all zones loaded
févr. 03 10:28:40 debian11a named[21932]: running
févr. 03 10:28:40 debian11a named[21932]: managed-keys-zone: Key 20326 for zone>
févr. 03 10:28:40 debian11a named[21932]: resolver priming query complete
lines 1-21/21 (END)
```

J'ai bien la mention active (running)

j'essaye la commande nslookup de mondomaine.lan et inversement avec l'adresse IP comme dernière vérification

```
root@debian11a:/etc/bind# nslookup mondomaine.lan
Server:          127.0.0.1
Address:         127.0.0.1#53

Name:  mondomaine.lan
Address: 127.0.0.1
Name:  mondomaine.lan
Address: ::1

root@debian11a:/etc/bind# nslookup 10.0.2.15
15.2.0.10.in-addr.arpa  name = ns.mondomaine.lan.

root@debian11a:/etc/bind#
```

J'ai bien le résultat escompté dans les deux cas

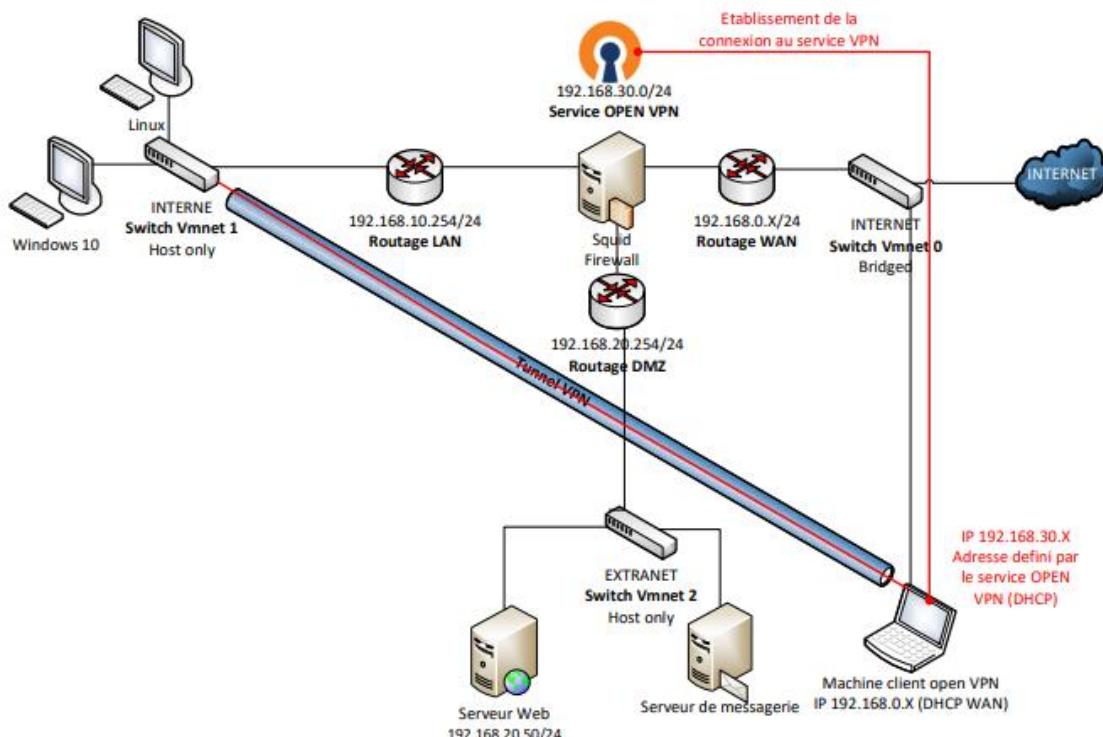
OpenVPN est une application gratuite et open source qui implémente les techniques de réseau privé virtuel (VPN) pour créer des connexions sécurisées de point à point ou de site à site dans des configurations en routées ou en pont et des installations d'accès à distance.

Il utilise un protocole de sécurité personnalisé qui utilise SSL / TLS pour l'échange de clés.

OpenVPN peut traverser les traducteurs d'adresses de réseau (NAT) et les pare-feu, ce qui en fait un outil idéal pour une utilisation dans les réseaux larges et complexes.

OpenVPN est souvent utilisé pour étendre les intranets dans des emplacements distants et pour connecter en toute sécurité les employés en télétravail à leur réseau siège social. Il est également fréquemment utilisé par les particuliers pour protéger leur trafic Internet.

Schéma explicatif :



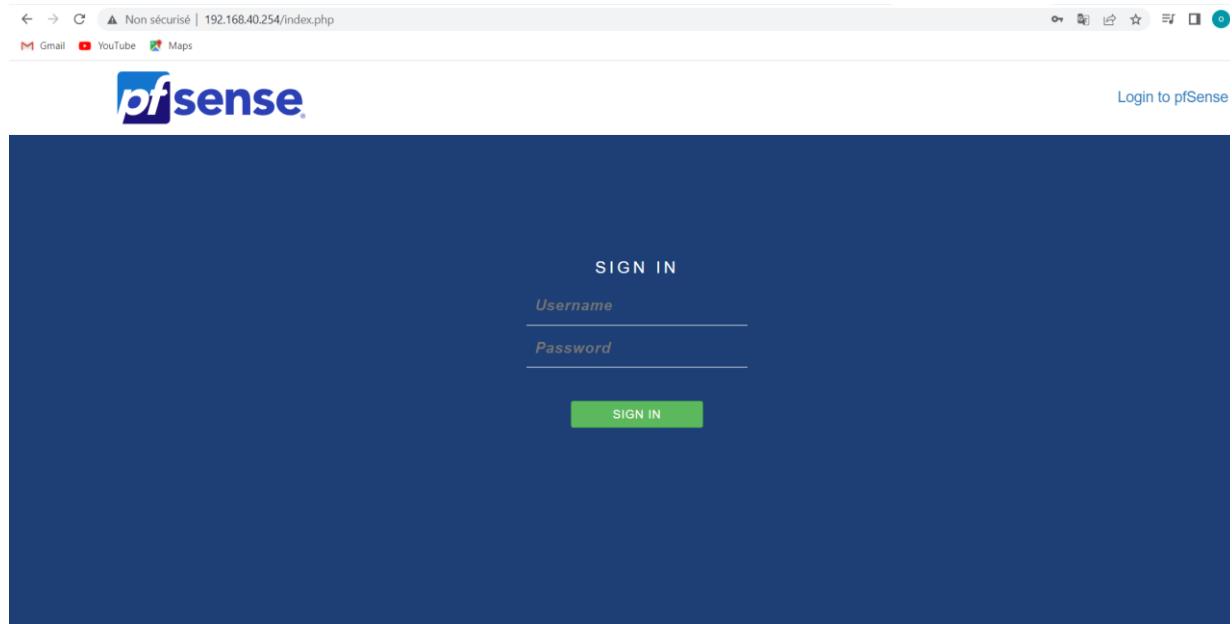
Pour rappel, ce type de VPN sert à établir un lien direct entre le PC et le réseau de l'entreprise, grâce à un tunnel chiffré et sécurisé.

Ma configuration s'effectuera sur mon firewall PFSENSE et pour cela j'ai suivi l'étape suivante :

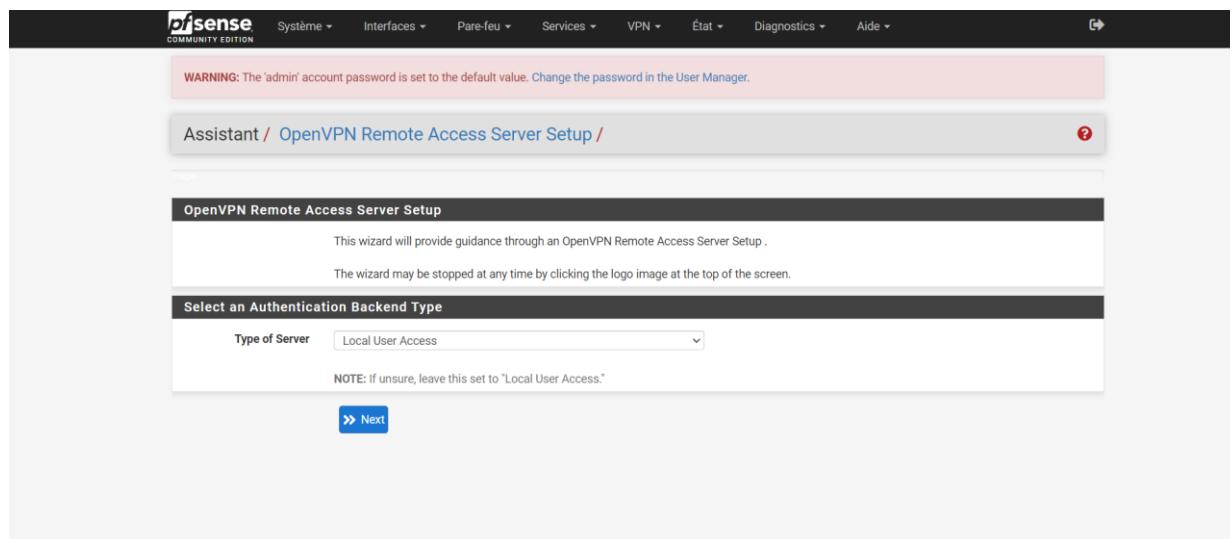
2. Configurer le serveur OpenVPN

J'accéder à l'interface Pfsense grâce à son URL 192.168.40.254 le Username par défaut est admin

et le mot de passe par default est Pfsense



Je sélectionne VPN puis OpenVPN et Assistants



B. Créer l'autorité de certification :

Ici c'est la création de l'autorité de certificat dans lequel on renseigne le Nom descriptif CA-VPN Le code pays FR l'état ou province Ile-de-France, la ville Champs-sur-Marne et l'organisation Formation bien entendu ces infos seront différentes et pas obligatoire. Cliquer ensuite sur Add New CA

Certificate Authority Selection

OpenVPN Remote Access Server Setup Wizard

Create a New Certificate Authority (CA) Certificate

Nom descriptif	CA-champs	A name for administrative reference, to identify this certificate. This is the same as common-name field for other Certificates.
Longueur de la clé	2048 bit	Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Durée de vie	3650	Lifetime in days. This is commonly set to 3650 (Approximately 10 years.)
Code du pays	FR	Two-letter ISO country code (e.g. US, AU, CA)
État ou province	Ile-de-france	Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
Ville	Champs-sur-Marne	City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organisation	Formation	Organization name, often the Company or Group name.

>> Add new CA

C. Créer le certificat Server :

Nous devons créer un certificat de type "Server" en nous basant sur notre nouvelle autorité de certification. Toujours dans "**Certificate Manager**", cette fois-ci dans l'onglet "**Certificates**", cliquez sur le bouton "**Add/Sign**".

Server Certificate Selection

OpenVPN Remote Access Server Setup Wizard

Create a New Server Certificate

Nom descriptif	serveur-champs	A name for administrative reference, to identify this certificate. This is also known as the certificate's "Common Name."
Longueur de la clé	2048 bit	Size of the key which will be generated. The larger the key, the more security it offers, but larger keys take considerably more time to generate, and take slightly longer to validate leading to a slight slowdown in setting up new sessions (not always noticeable). As of 2016, 2048 bit is the minimum and most common selection and 4096 is the maximum in common use. For more information see keylength.com
Durée de vie	398	Lifetime in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.
Code du pays	FR	Two-letter ISO country code (e.g. US, AU, CA)
État ou province	Ile-de-france	Full State or Province name, not abbreviated (e.g. Kentucky, Indiana, Ontario).
Ville	Champs-sur-Marne	City or other Locality name (e.g. Louisville, Indianapolis, Toronto).
Organisation	Formation	Organization name, often the Company or Group name.

>> Create new Certificate

Nous voici arrivé au paramétrage du réseau

Server Setup

OpenVPN Remote Access Server Setup Wizard

General OpenVPN Server Information

Interface	WAN	The interface where OpenVPN will listen for incoming connections (typically WAN.)
Protocole	UDP on IPv4 only	Protocol to use for OpenVPN connections. If unsure, leave this set to UDP.
Local Port	1194	Local port upon which OpenVPN will listen for connections. The default port is 1194. This can be left at its default unless a different port needs to be used.
Description	vpn-champs	A name for this OpenVPN instance, for administrative reference. It can be set however desired, but is often used to distinguish the purpose of the service (e.g. "Remote Technical Staff"). It is also used by OpenVPN Client Export to identify this VPN on clients.

Et je configure les paramètres cryptographiques on laisse tout par default l'authentification TLS et la régénération de clef partagé.

Ensuite je configure les paramètres du tunnel dans le local Network 192.168.10.0/24 ici je donne l'adresse

192.168.30.0/24

Paramètres du tunnel

Réseau Tunnel IPv4	192.168.30.0/24	This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.
Tunnel réseau IPv6		This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.
Rediriger la passerelle IPv4	<input type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel.	
Rediriger la passerelle IPv6	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.	
Réseau(x) local/locaux IPv4	192.168.10.0/24	IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Réseau(x) local/locaux IPv6		IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.
Connexions simultanées	10	Spécifier le nombre maximum de clients autorisés à se connecter en même temps à ce serveur.
Allow Compression	Refuse any non-stub compression (Most secure)	Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the

Je renseigne le DNS 192.168.10.254 et le DNS de Google 8.8.8.8 je clic sue Next et j'arrive sur Firewall Rule Configuration

Je coche Firewall Rule et Openvpn Rule et je clic à nouveau sur Next et Finish pour terminer la configuration.

Etape 10 de 11

Firewall Rule Configuration

OpenVPN Remote Access Server Setup Wizard

Firewall Rule Configuration

Firewall rules control what network traffic is permitted. Rules must be added to allow traffic to the OpenVPN server's IP and port, as well as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the wizard.

Traffic from clients to server

Firewall Rule Add a rule to permit connections to this OpenVPN server process from clients anywhere on the Internet.

Traffic from clients through VPN

OpenVPN rule Add a rule to allow all traffic from connected clients to pass inside the VPN tunnel.

>> Next

Voici la configuration du serveur terminé

VPN / OpenVPN / Serveurs

Serveurs Clients Ré-écritures spécifiques au client Assistants

Serveurs OpenVPN

Interface	Protocole / Port	Réseau tunnel	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.3.0/24	Mode: Remote Access (SSL/TLS + User Auth) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	vpn-champs	  

+ Ajouter

3. Créer les utilisateurs locaux

Je vais dans systèmes et gestion d'usagers et je clic sur Ajouter

Système / Gestionnaire d'usagers / Utilisateurs

Utilisateurs Groupes Paramètres Serveurs d'authentification

Utilisateurs				
Nom d'utilisateur	Nom complet	État	Groupes	Actions
<input type="checkbox"/> admin	System Administrator	✓	admins	

Ajouter Supprimer

Je renseigne le nom et le mot de passe, la date d'expiration et je crée le certificat client

Propriétés utilisateur

Défini par	USER
Désactivé	<input type="checkbox"/> Cet utilisateur ne peut pas s'authentifier
Nom d'utilisateur	omar
Mot de passe	****
Nom complet	MECHENANE Nom complet de l'utilisateur, à des fins administratives uniquement
Date d'expiration	
Laissez vide si le compte ne doit pas expirer, sinon entrez la date d'expiration sous la forme MM/JJ/AAAA.	
Paramètres personnalisés	<input type="checkbox"/> Utilisez les options GUI individuelles personnalisées et la disposition du tableau de bord pour cet utilisateur.
Appartenance à un groupe	<div style="display: flex; align-items: center;"> <div style="flex: 1;"> <input type="checkbox"/> admins Pas un membre de </div> <div style="flex: 1;"> <input type="checkbox"/> Membre de </div> </div>
<div style="display: flex; justify-content: space-around;"> Déplacer vers la liste "Membre de" Déplacer vers la liste "Non membre de" </div> <p>Maintenez la touche CTRL (PC)/COMMAND (Mac) enfoncée pour sélectionner plusieurs éléments.</p>	
Certificat	<input checked="" type="checkbox"/> Cliquez pour créer un certificat client

Je donne un nom descriptif et je choisis l'autorité de certification et j'enregistre

Créer un certificat pour l'utilisateur

Nom descriptif	ca-omar-vpn
Autorité de certification	CA-champs
Key type	RSA
2048	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Algorithm de hachage	sha256
The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid	
Durée de vie	3650

Clés

Clés SSH autorisées	Entrez les clés SSH autorisées pour cet utilisateur
Clé pré-partagée IPsec	

Enregistrer

Voici le résultat que Final

Système / Gestionnaire d'usagers / Utilisateurs				
Utilisateurs Groupes Paramètres Serveurs d'authentification				
Utilisateurs				
Nom d'utilisateur	Nom complet	État	Groupes	Actions
<input type="checkbox"/> admin	System Administrator	✓	admins	
<input type="checkbox"/> omar	MECHENANE	✓		

Ajouter **Supprimer**

4. Exporter la configuration OpenVPN

Il faut maintenant récupérer le client qui contient le certificat ainsi que toute la configuration pour qu'il puisse se connecter. Pour l'installation du client, il existe un paquet d'export du certificat qui intègre le logiciel client. Il va falloir installer ce paquet L'installation se fait depuis Système puis Gestionnaire de paquets

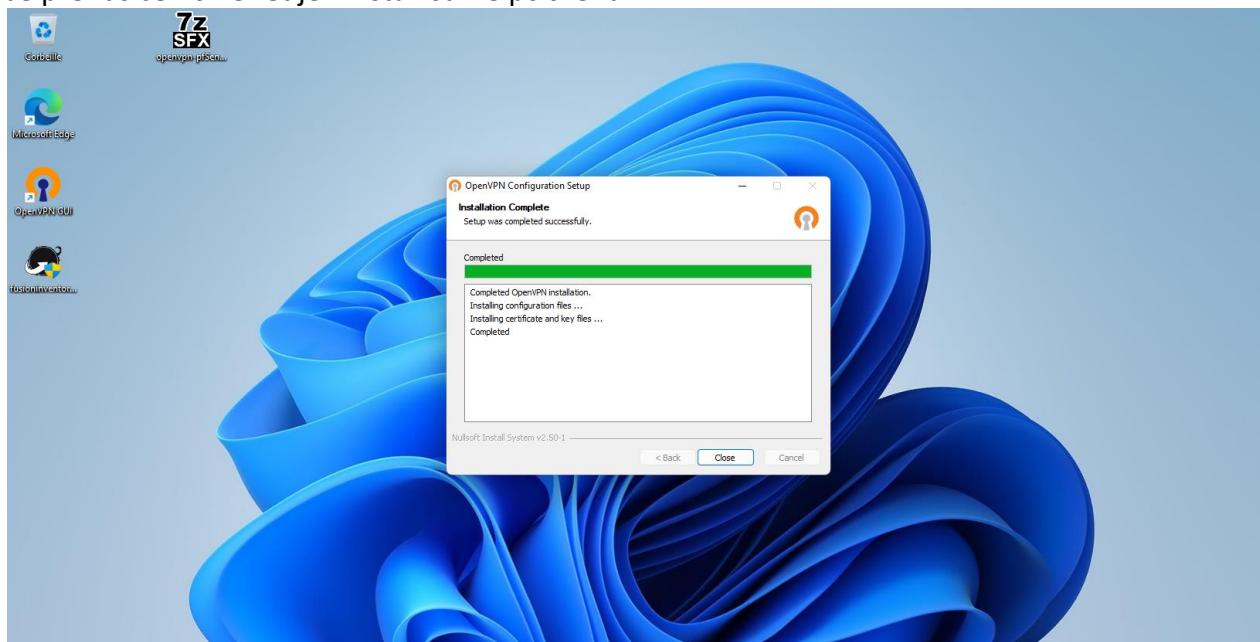
Ensuite il suffit de sélectionner Paquet disponibles puis dans Terme de recherche taper openvpn et rechercher et enfin Install du paquet openvpn-client-export

Il faut maintenant récupérer le client pour le transférer sur la machine qui sera client VPN. Pour cela allez dans VPN puis OPENVPN et cliquer sur Client Export (c'est ce qu'il à été installé

précédemment)

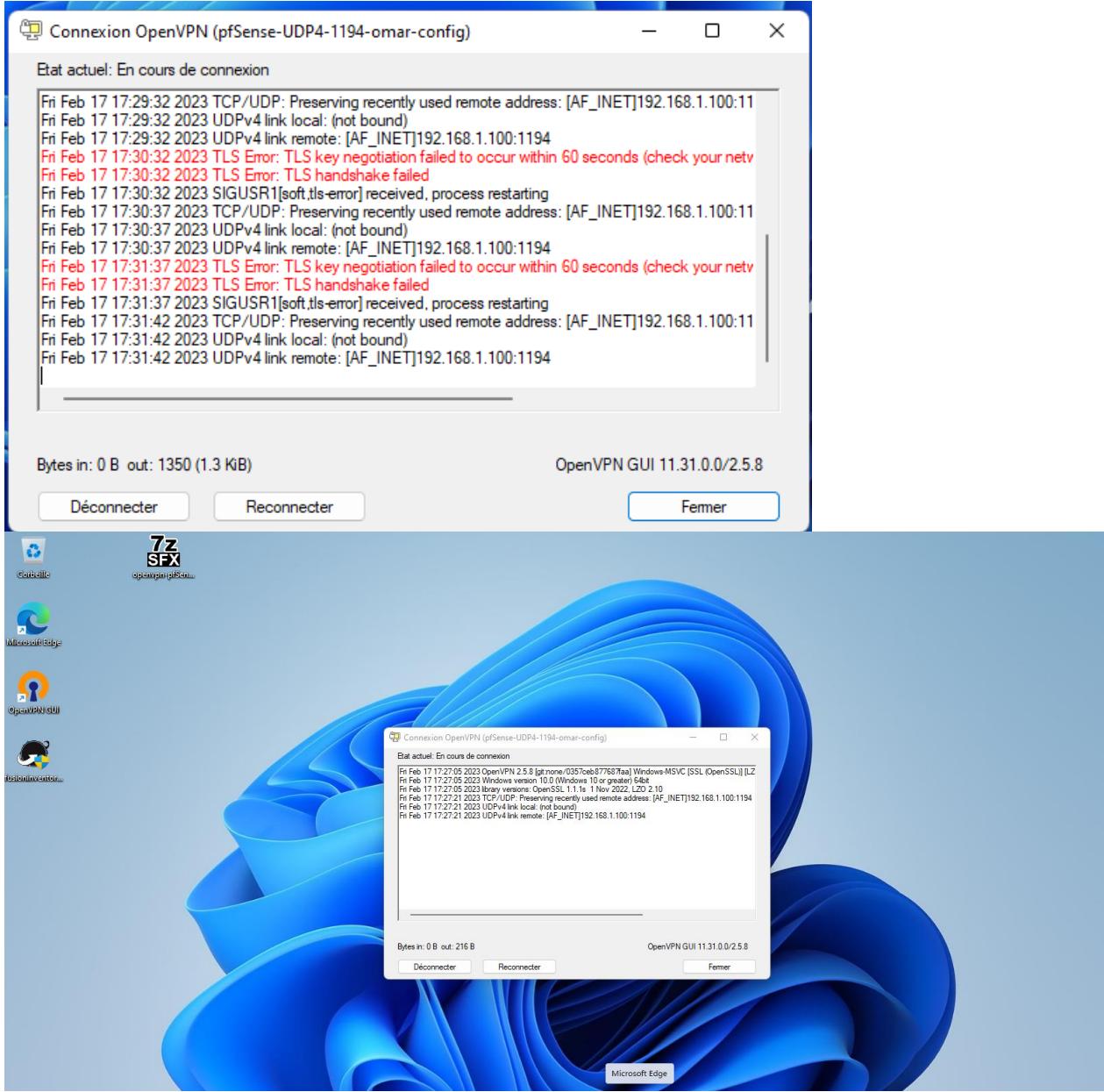
Clients OpenVPN		
Utilisateur	Nom du certificat	Export
omar	ca-omar-vpn	<ul style="list-style-type: none">- Inline Configurations:  Most Clients  Android  OpenVPN Connect (iOS/Android)- Bundled Configurations:  Archive  Config File Only- Current Windows Installers (2.5.8-lx04):  64-bit  32-bit- Legacy Windows Installers (2.4.12-lx01):  10/2016/2019  7/8/8.1/2012r2- Viscosity (Mac OS X and Windows):  Viscosity Bundle  Viscosity Inline Config

Je choisis selon la configuration du pc client, dans mon cas c'est Windows 64-bit
Une fois que le client a été téléchargé il est placé dans le répertoire des téléchargements.
Je prends ce fichier et je l'Install sur le pc client



5. Tester l'accès distant depuis un poste client

Je saisie le nom utilisateur et le mot de passe puis je vérifie que je n'ai pas des erreurs, dans le cas d'erreur Il faut simplement dans la configuration du pare feu puis Règles et mettre des règles Dans mon cas j'ai des erreurs donc je vais mettre en place des règles et retester plus tard



6. Créer les règles de firewall pour OpenVPN

a) Autoriser le flux OpenVPN :

On s'aperçoit que la règle dans le WAN bloque les réseaux privés, ce qui est normal car une connexion client en VPN ne vient pas de ces réseaux mais de réseau Public. Comme ici on fait du Lab. ça bloque. Il suffit de dé-valider cette règle pour que tout rentre dans l'ordre Pour cela cliquer sur l'engrenage pour modifier les règles

Flottant(e) WAN LAN OpenVPN

Règles (Faire glisser pour changer l'ordre)

Etat	Protocole	Source	Port	Destination	Port	Filtre	Passerelle d'attente	Ordonnancement	Description	Actions
<input checked="" type="checkbox"/> 0 / 0 B	*	Réseaux RFC 1918	*	*	*	*	*	*	Bloquer les réseaux privés	
<input checked="" type="checkbox"/> 0 / 0 B	*	Réservee Non assignées par l'IANA	*	*	*	*	*	*	Bloquer les réseaux invalides	
<input checked="" type="checkbox"/> 0 / 0 B	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	aucun		Assistant vpn-champs OpenVPN	

Ajouter Ajouter Supprimer Enregistrer Séparateur

Réseaux réservés

Bloquer les réseaux privés et les adresses de loopback
 Bloque le trafic depuis des adresses IP qui sont réservées pour les réseaux privés (RFC 1918: 10/8, 172.16/12, 192.168/16), les adresses locales uniques (RFC 4193: fc00::/7) et les adresses de boucle locale (127/8). Cette option doit généralement être activée, sauf si l'interface réseau est également dans un réseau privé.

Bloquer les réseaux invalides
 Blocks traffic from reserved IP addresses (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and so should not appear as the source address in any packets received.
 This option should only be used on external interfaces (WANs), it is not necessary on local interfaces and it can potentially block required local traffic.
 Note: The update frequency can be changed under System > Advanced, Firewall & NAT settings.

Enregistrer

b) Résultat final :

cette fois-ci si l'on retourne sur la machine cliente, la connexion est bien réalisée



Depuis la commande IPCONFIG /ALL la machine client à bien reçu une IP correspondante au réseau VPN 192.168.3.0/24

7. Resultat final :

Je ping mon Lan résultat positive

```
invite de commandes
```

```
Adresse physique . . . . . : 3C-55-76-6A-5B-8C
DHCP activé. . . . . : Oui
Configuration automatique activée. . . : Oui

C:\Users\omar>ping 192.168.10.51

Envoi d'une requête 'Ping' 192.168.10.51 avec 32 octets de données :
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.10.51:
 Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),

C:\Users\omar>ping 192.168.10.254

Envoi d'une requête 'Ping' 192.168.10.254 avec 32 octets de données :
Réponse de 192.168.10.254 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.10.254:
 Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
 Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\omar>
```

