

# **CONTRE-RENDU STAGE 2 : INSTALLATION D'OPENsense**

# Table des Matières

<b>Introduction :</b>	<b>3</b>
Outils Utilisé :	3
Logiciel Utilisé :	3
Site Web Utilisé :	3
Schéma Réseau :	4
<b>PARTIE 1 - Mise en place du serveur :</b>	<b>5</b>
<b>PARTIE 2 - Mise en place Hyper-V :</b>	<b>8</b>
<b>PARTIE 3 - Mise en place OPNsense :</b>	<b>11</b>
Installation via Hyper-V	11
Installation OPNsense :	15
<b>PARTIE 4 - Mise en place du Pare-Feu :</b>	<b>19</b>
<b>PARTIE 5 - Mise en place d'un Portail Captif :</b>	<b>21</b>
OPNsense :	21
Active Directory :	25
Création de l'Active Directory :	25
Création de L'Utilisateur :	29
Création de Serveur DNS :	31
Importer Portail Captif avec AD :	36
Wifi :	38
<b>Conclusion :</b>	<b>41</b>

# Introduction :

Mon tuteur de stage m'a demandé de mettre en place **un serveur pare-feu en virtuel** sur **l'hyperviseur Hyper-V** dans un serveur de **Windows Server 2012**, le but est de mettre en place un règle qui permet de se connecter uniquement sur internet. est ensuite ont va créer un **Portail Captif** qui devra passer par un **Active Directory** sur un **Windows Server 2012 Virtuelle**.

## Outils Utilisé :

- Un Ordinateur
- Clavier et Souris
- Un Serveur de la marque HP
- Un Commutateur/Switchs de la Marque Netgear
- Quatre câbles RJ45
- Une Borne wifi de la marque Ruckus

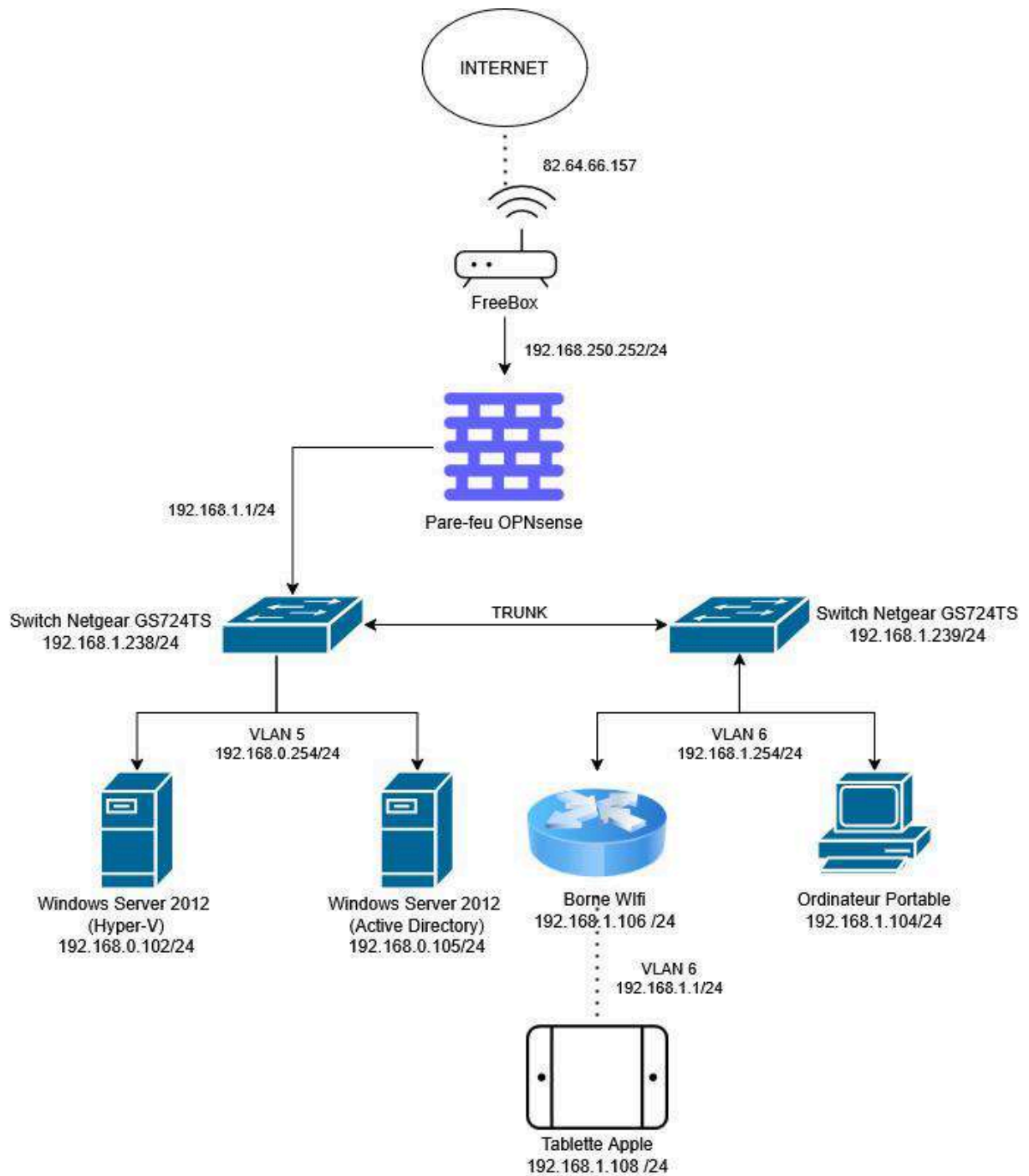
## Logiciel Utilisé :

- Hyper-V, l'hyperviseur de windows
- OPNsense, le Logiciel de pare-feu et
- L'ancienne version d'un navigateur web.

## Site Web Utilisé :

- Le Site web embarqué du serveur pare-feu
- Le Site web embarqué de la borne wifi
- Le Site web d'OPNsense

## Schéma Réseau :



Cet Image nous montre le Schéma Réseau de cette mise en place.

# PARTIE 1 - Mise en place du serveur :

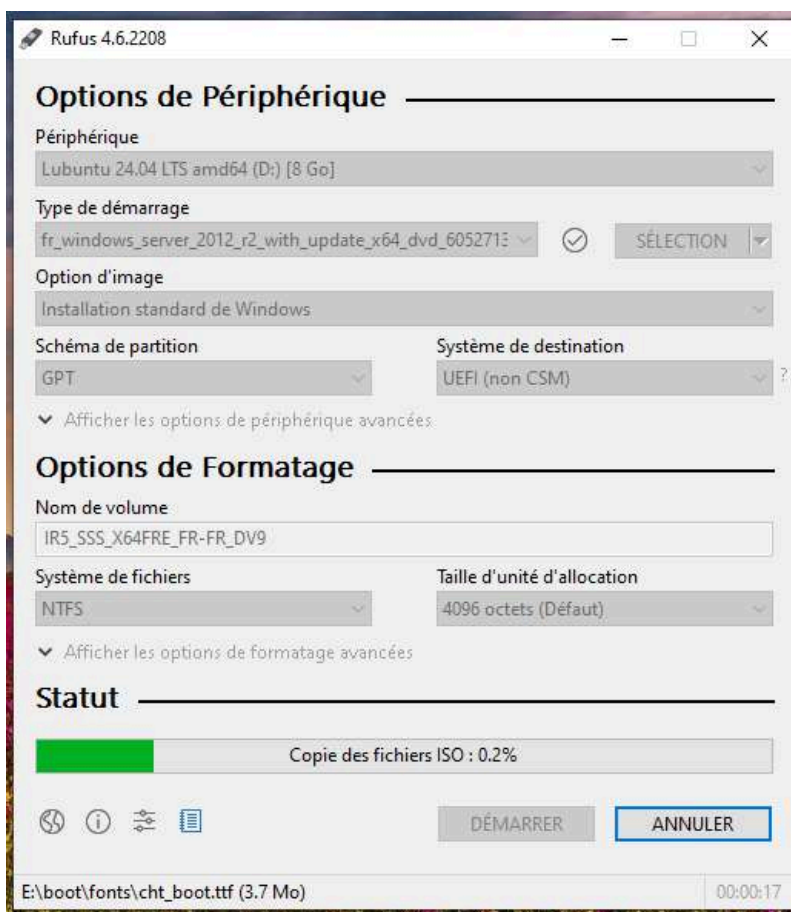
Un Serveur Informatique est un dispositif informatique qui permet d'offrir un ou plusieurs services.

Dans mon cas, j'ai dû mettre en place un serveur Windows 2012 pour un server HP, pour cela, je dois tout d'abord installer le fichier ISO du serveur.

 fr\_windows\_server\_2012\_r2\_with\_update\_x64\_dvd\_6052713 09/01/2025 12:09 Fichier d'image di... 5 318 392 Ko

Cette image nous montre le fichier ISO de Windows Server 2012.

Ensuite, je dois créer une clé bootable avec le Windows Server 2012 pour qu'on puisse l'installer dans le serveur.



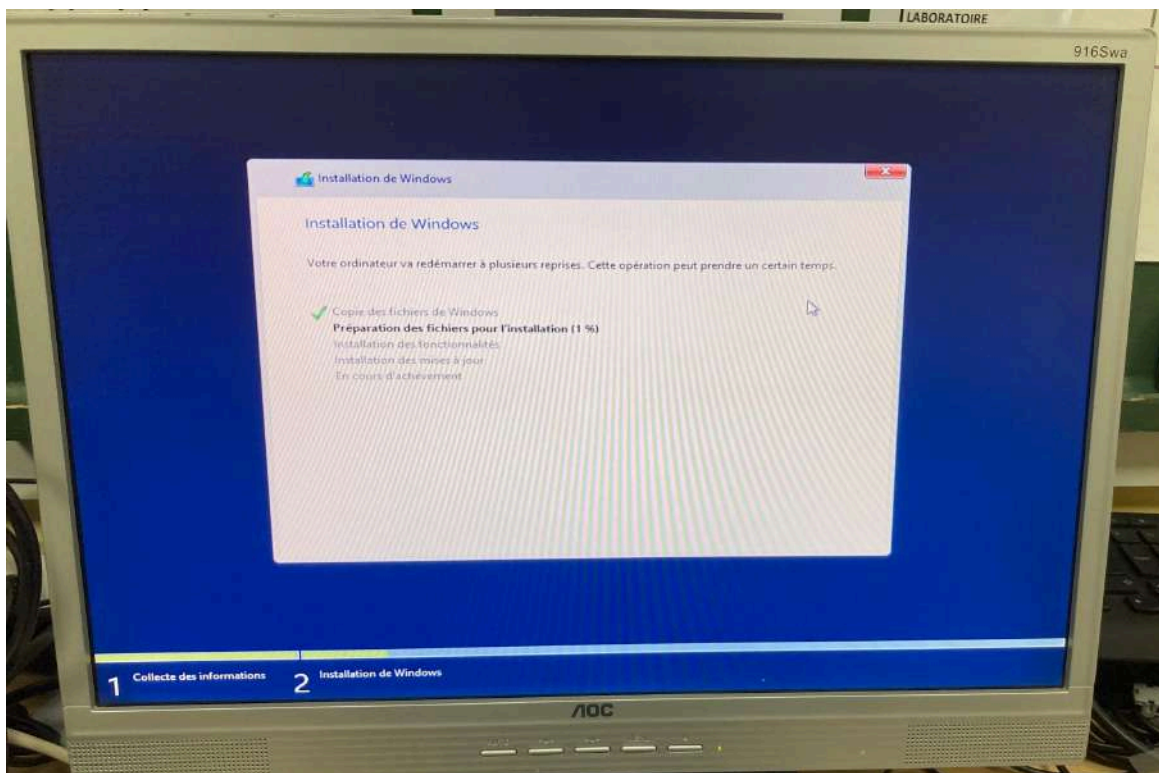
Cette image nous montre l'installation de la clé bootable.

Ensuite, une fois la clé créée, on l'enlève la clé de l'ordinateur et on le met dans le serveur.



Cette image nous montre la clé mise sur le serveur

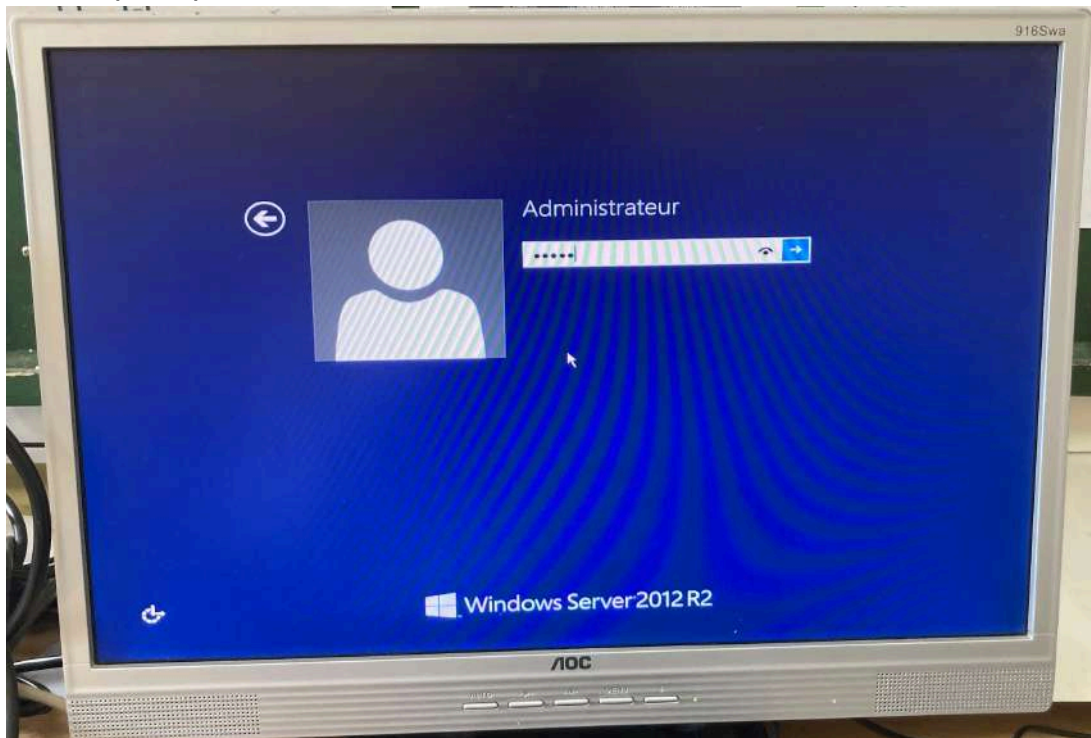
Ensuite, on attend que le serveur boot sur la clé, et enfin on commence l'installation avec un windows server 2012.



Cette image nous montre l'installation du Windows Server 2012.

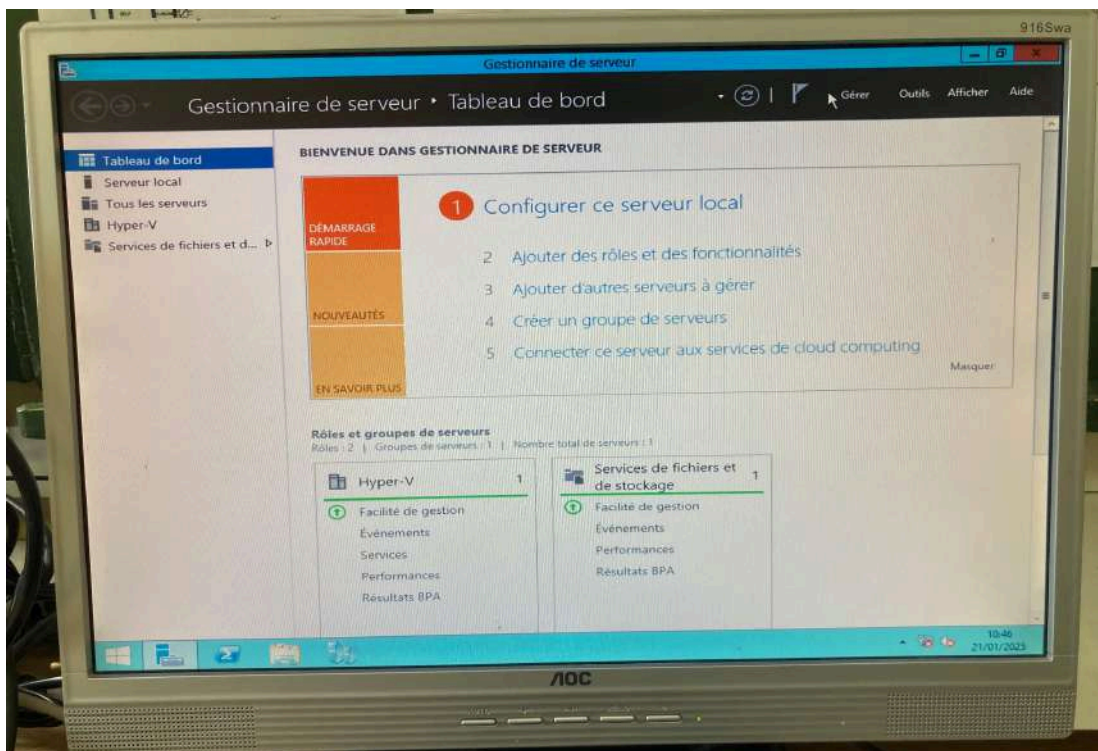
Une fois que l'installation finie, on configure cela comme dans win 10 ou 11.

il reste plus qu'à se connecter.



Cette image nous montre la page de connexion de Windows Server 2012 R2





Cette image nous montre la page de gestionnaire de serveur de Windows Server 2012 R2

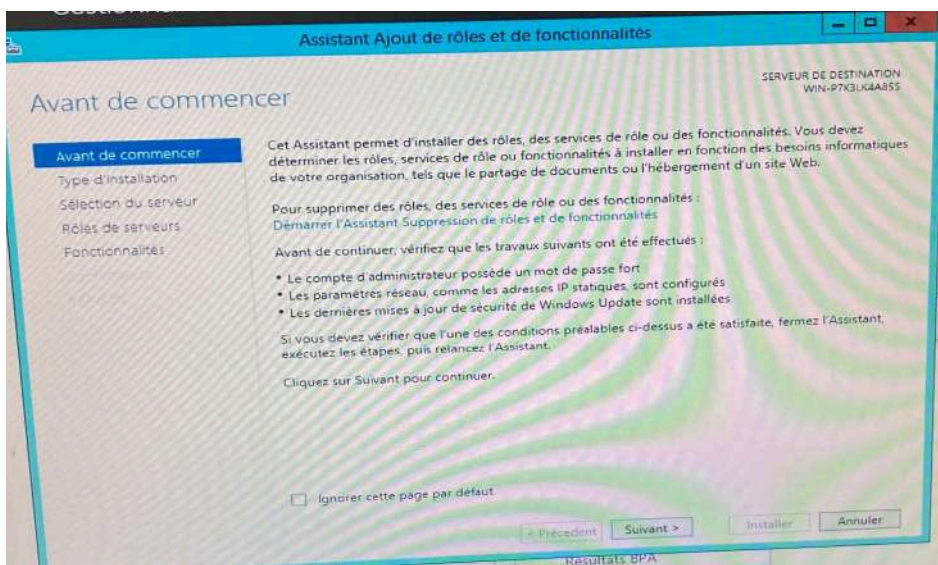
## PARTIE 2 - Mise en place Hyper-V :

Un **hyperviseur** est un logiciel de virtualisation qui permet d'émuler plusieurs systèmes d'exploitation qui fonctionnent en parallèle dans une seule machine physique.

**Hyper-V** est un hyperviseur créé et développé par Microsoft pour leur système d'exploitation Windows.

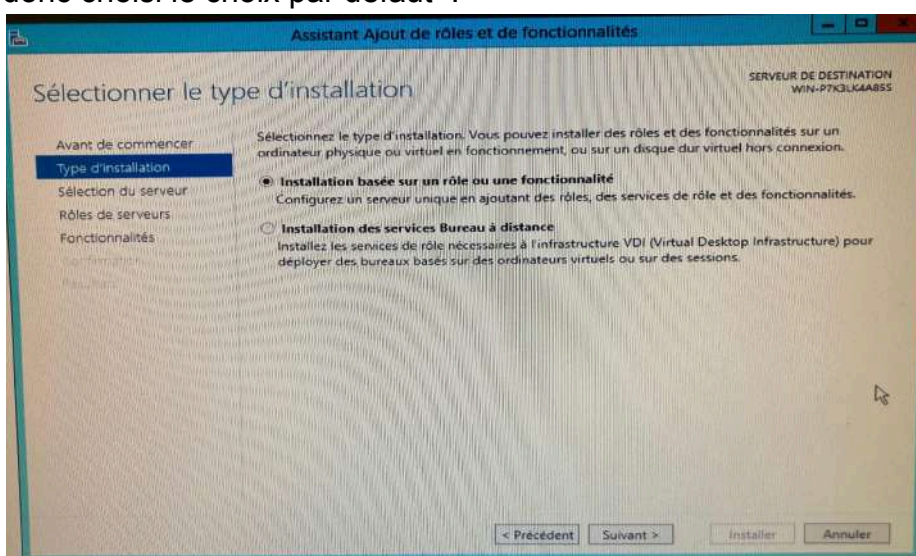
Dans notre cas, On n'a pas installé un Windows Server donc on peut installer Hyper-V directement dans le gestionnaire de serveur -> Gérer -> Ajouter des rôles et fonctionnalités





Cette Image nous montre la page d'Ajout des Rôles et de fonctionnalités

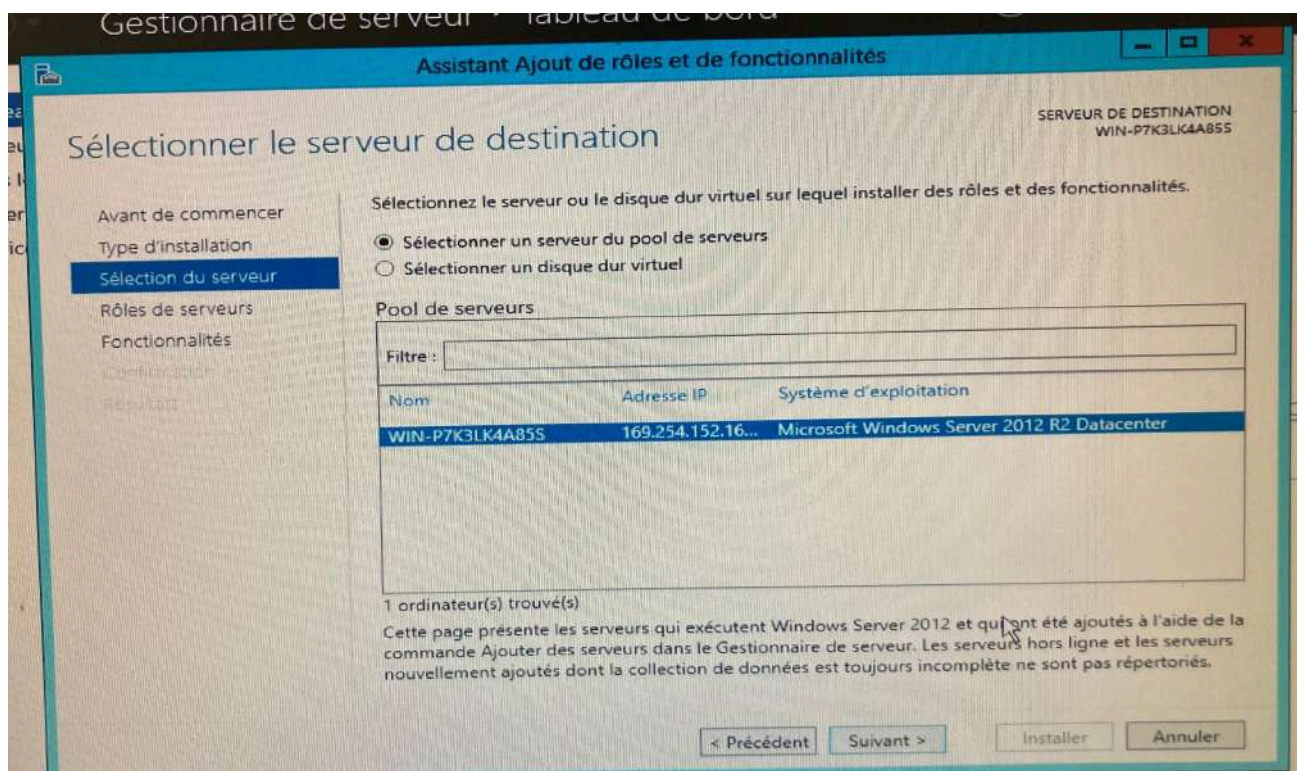
Ensuite, on choisi le type d'installation vu qu'on n'a pas prévu de gestion distanciel on vas donc choisi le choix par défaut :



Cette Image nous montre la page sélectionner le type d'installation.

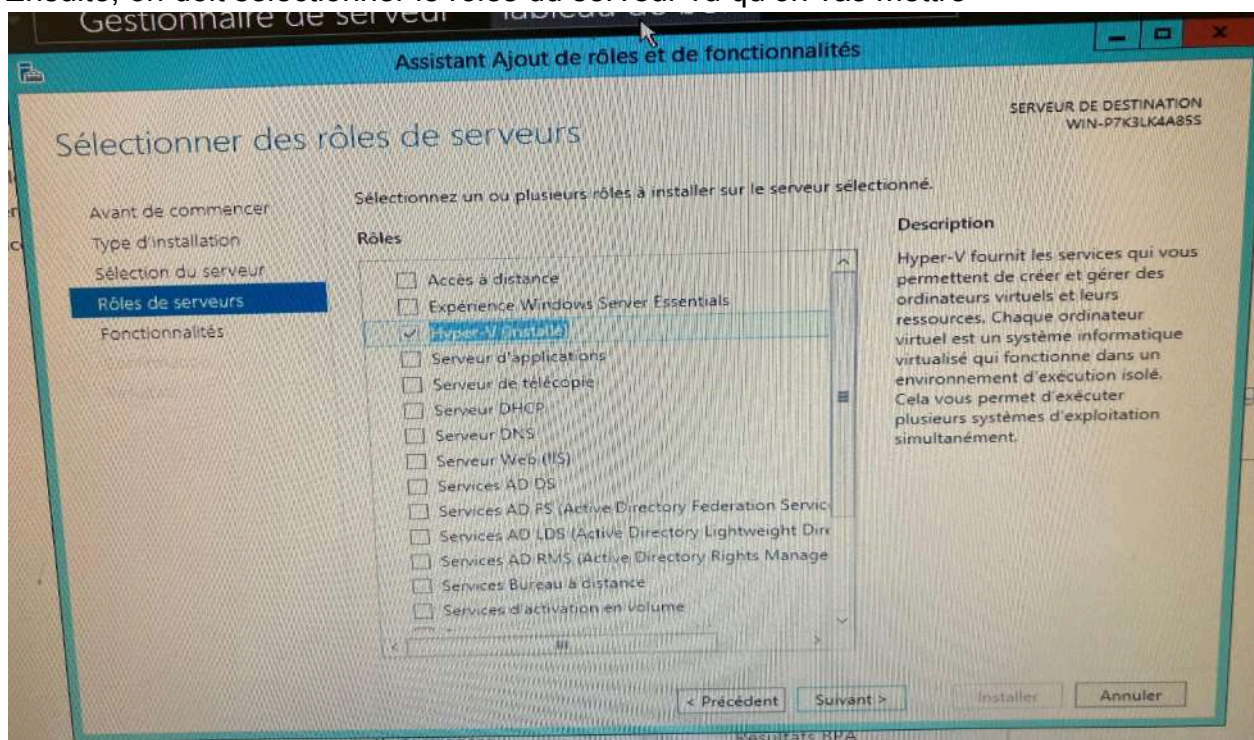
Ensuite, on doit sélectionner le type de fonction qu'on va mettre dans le serveur.





Cette Image nous montre la sélection du serveur sur Win Server 2012

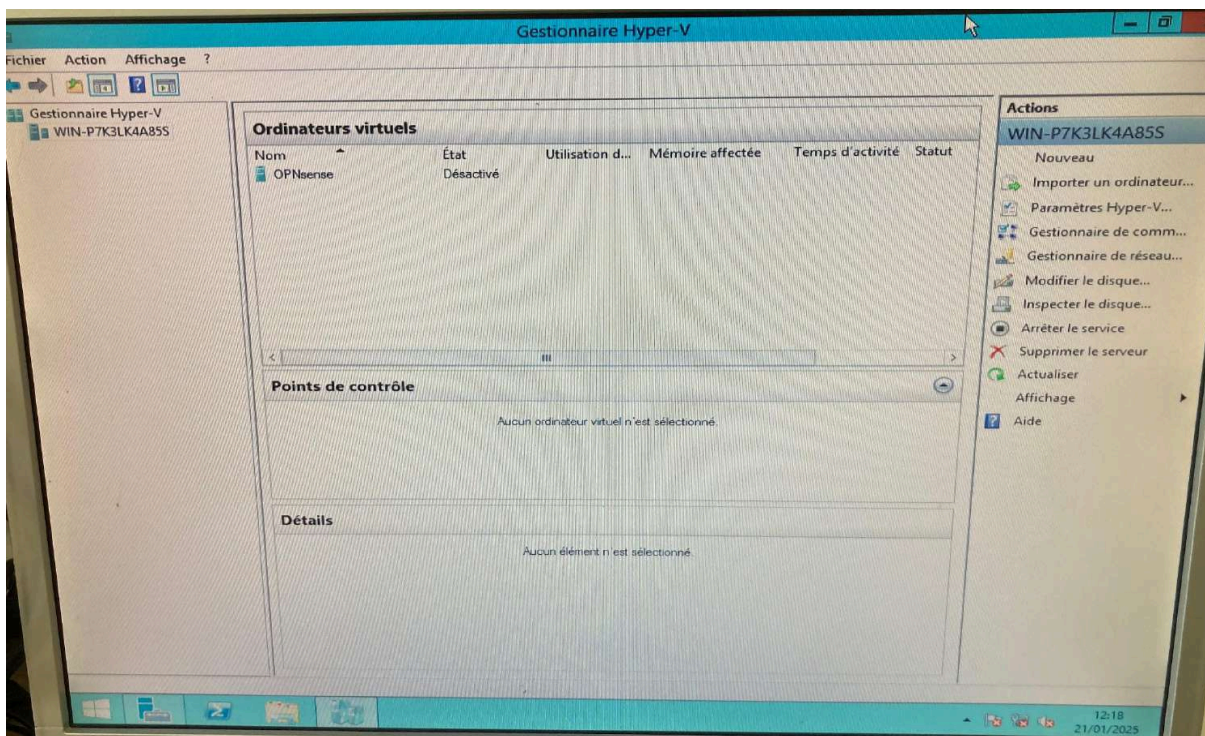
Ensuite, on doit sélectionner le rôles du serveur vu qu'on vas mettre



Cette Image nous montre la sélection du rôles du serveur sur Win Server 2012

Ensuite, on confirme notre sélection et on lance Hyper-V





Cette Image nous montre la page d'accueil du logiciel Hyper-V

## PARTIE 3 - Mise en place OPNsense :

**OPNsense** est un logiciel de pare-feu open source avec une option routage qui est basé sur le système d'exploitation FreeBSD développé par Deciso.

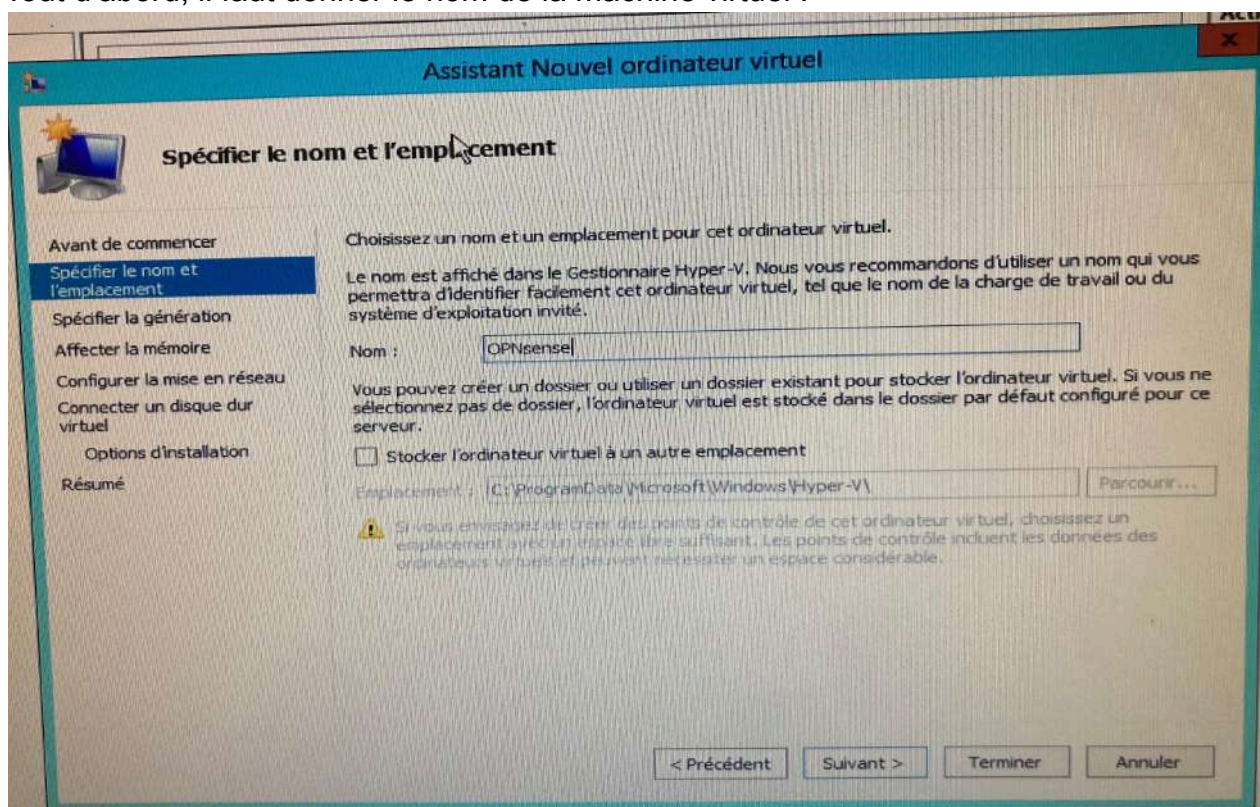
Notre but est de bloquer les sites autre que recherche sur internet (Par exemple : les téléchargement de fichier seront bloqué notre pare-feu)

Dans notre cas, on va installer OPNsense sur notre serveur grace Hyper-V, pour cela, on va tout d'abord créer la machine virtuelle, puis, on crée deux réseau différents et enfin, lancer la machine virtuelle.

### Installation via Hyper-V

Pour installer OPNsense sur une machine virtuelle, il faut installer une nouvelle machine sur Hyper-V donc on vas sur actions -> win-(suitedumachine) -> nouveau est on suit les étapes :

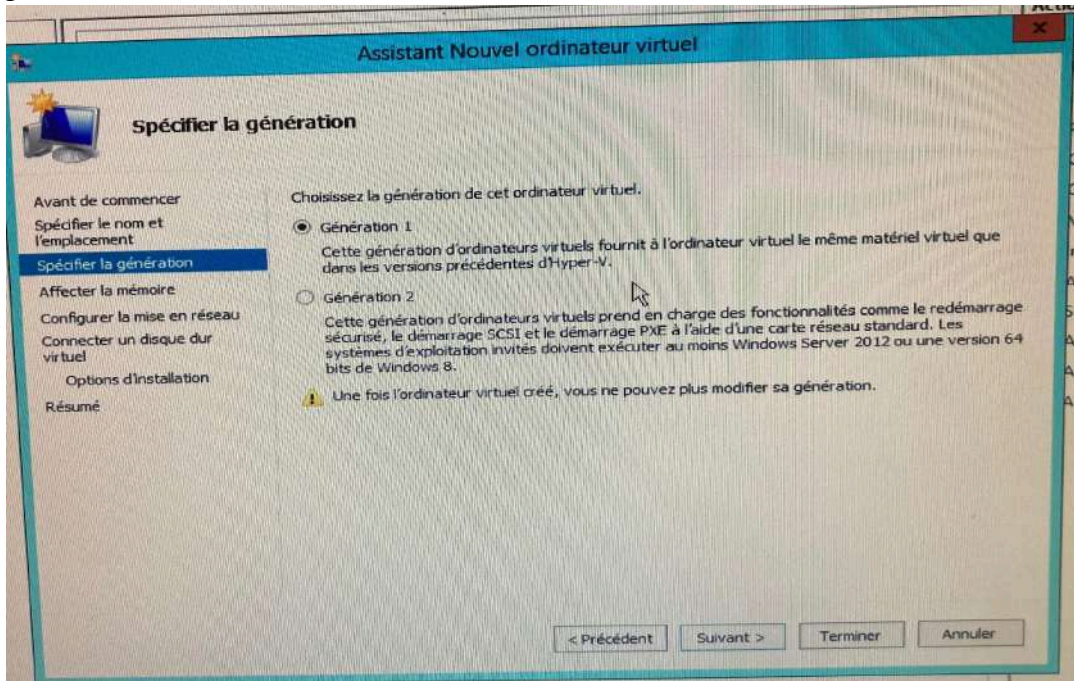
Tout d'abord, il faut donner le nom de la machine virtuel :



Cette image nous montre la page de nomination de la machine virtuel

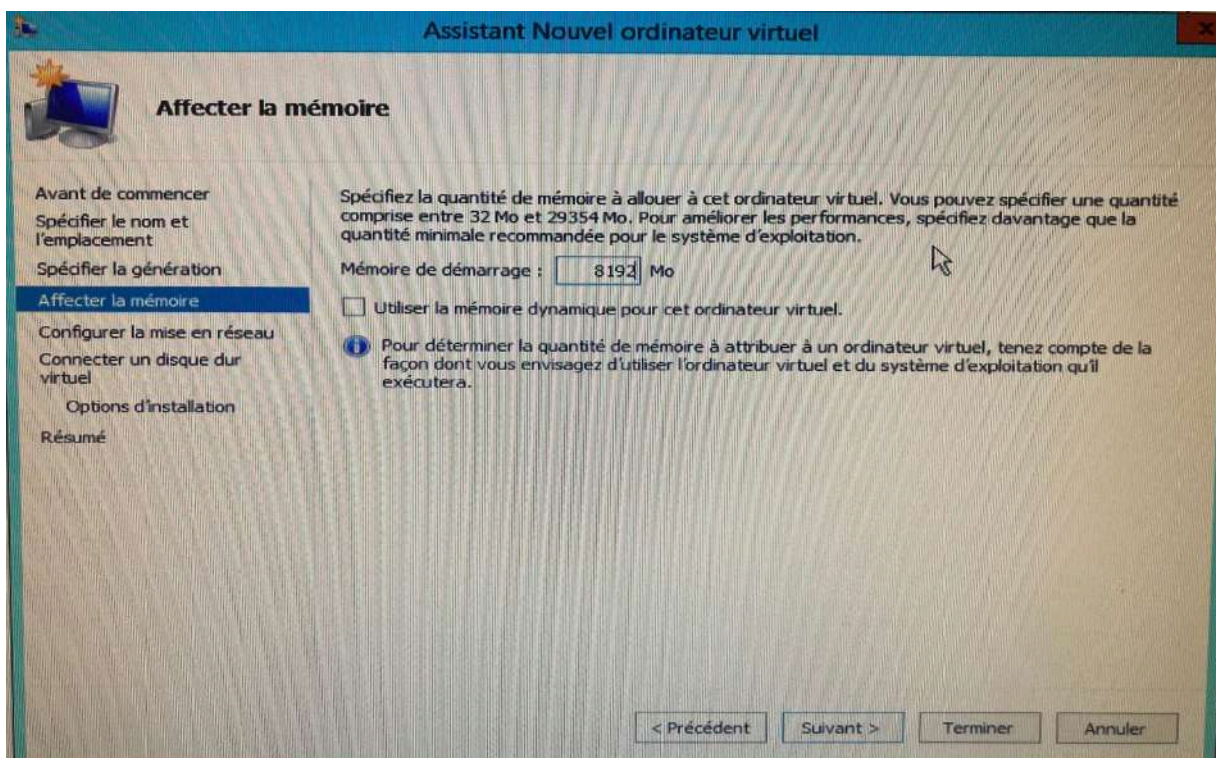


Puis, il faut donner la génération de machine virtuelle de hyper-v, en général, On prend la génération 1.



Cette image nous montre la page de choix de génération

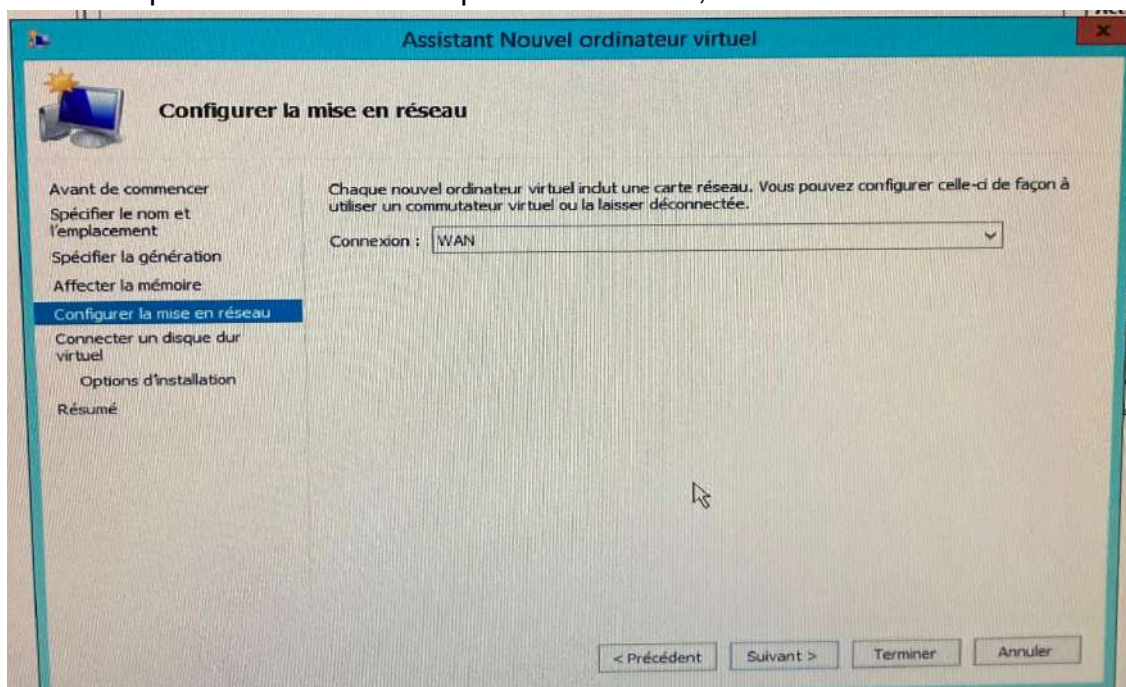
Ensuite, il faut donné de la mémoire ram de la machine virtuelle, vu que c'est un serveur, mon tuteur de stage ma dit de mettre au moins 8 go de RAM :



cette image nous montre la page de la mémoire ram.

Ensuite, on va lui donner une carte réseau

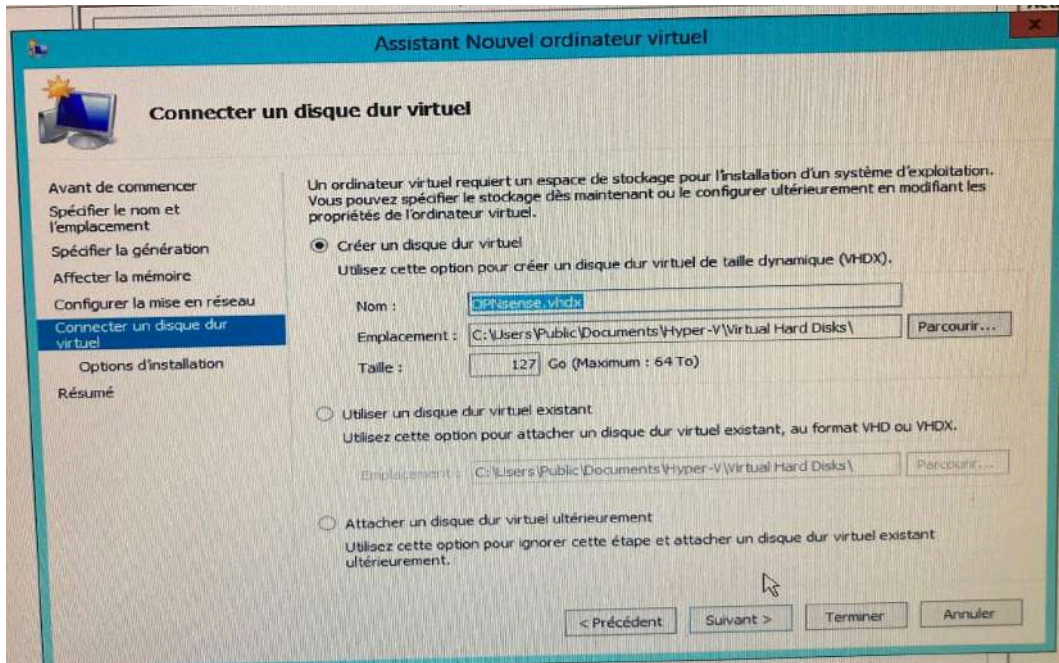
Dans notre cas, on va créer un réseau en LAN et WAN car ces deux réseaux vont servir de routeur pour notre hôte. Mais pour l'installation, on vas mettre le WAN :



Cette image nous montre la page de la carte réseaux



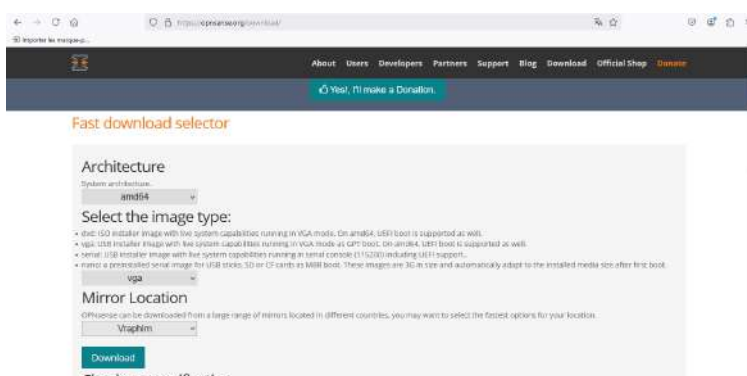
Ensuite, on va créer un disque dur virtuel pour la machine virtuelle :



Cette image nous montre la page de la création du disque dur.

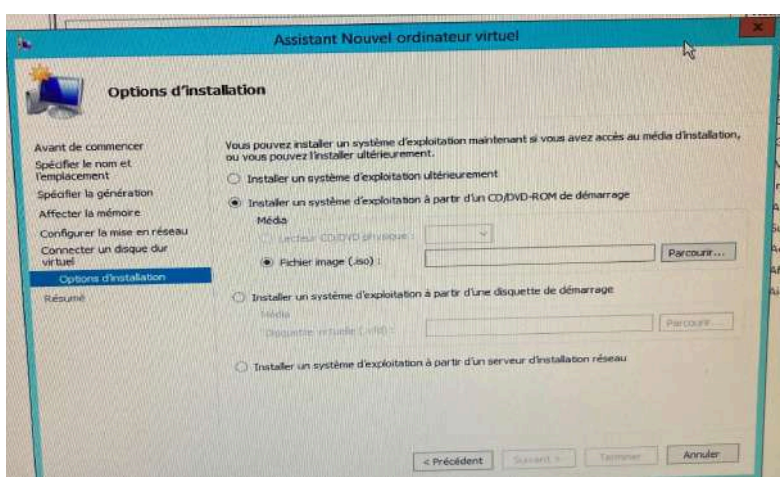
Ensuite, on va mettre le fichier.iso pour cela on va tout d'abord, l'installer le fichier .iso sur le site web, puis on va le transférer sur une clé est enfin, on va le mettre iso sur la machine virtuelle.

Le site web du OPNsense avec l'installation.



Cette Image nous montre la page installation du ISO

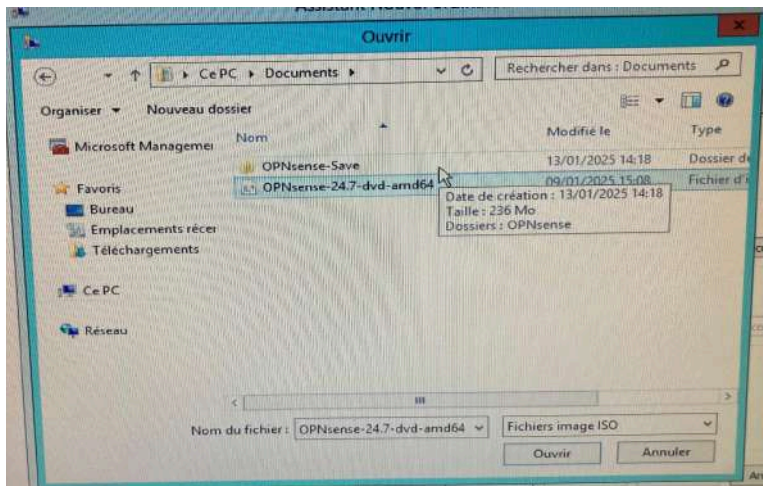
la page d'installation de hyper-v :





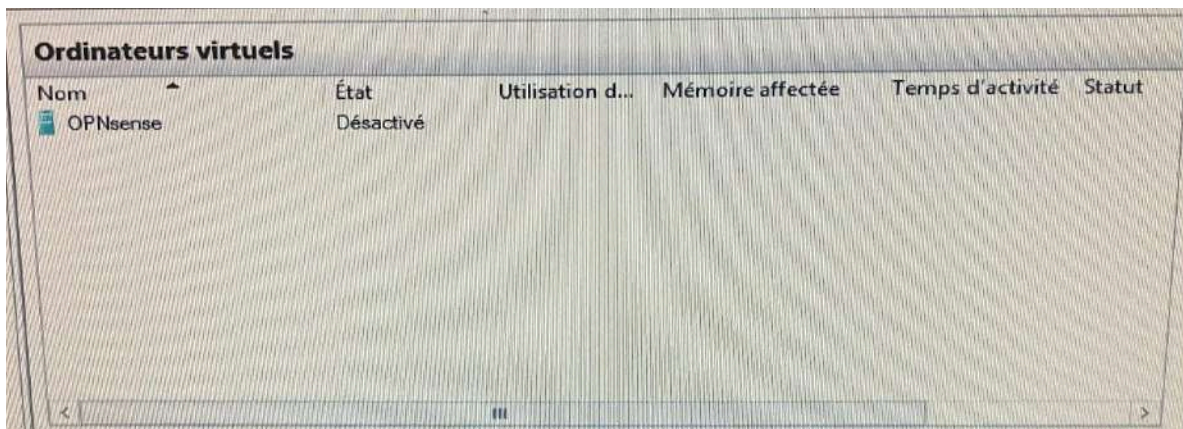
Cette image nous montre la page d'installation du iso.

Le fichier iso a sélectionné :



Cette image nous montre que le fichier ISO a été sélectionné.

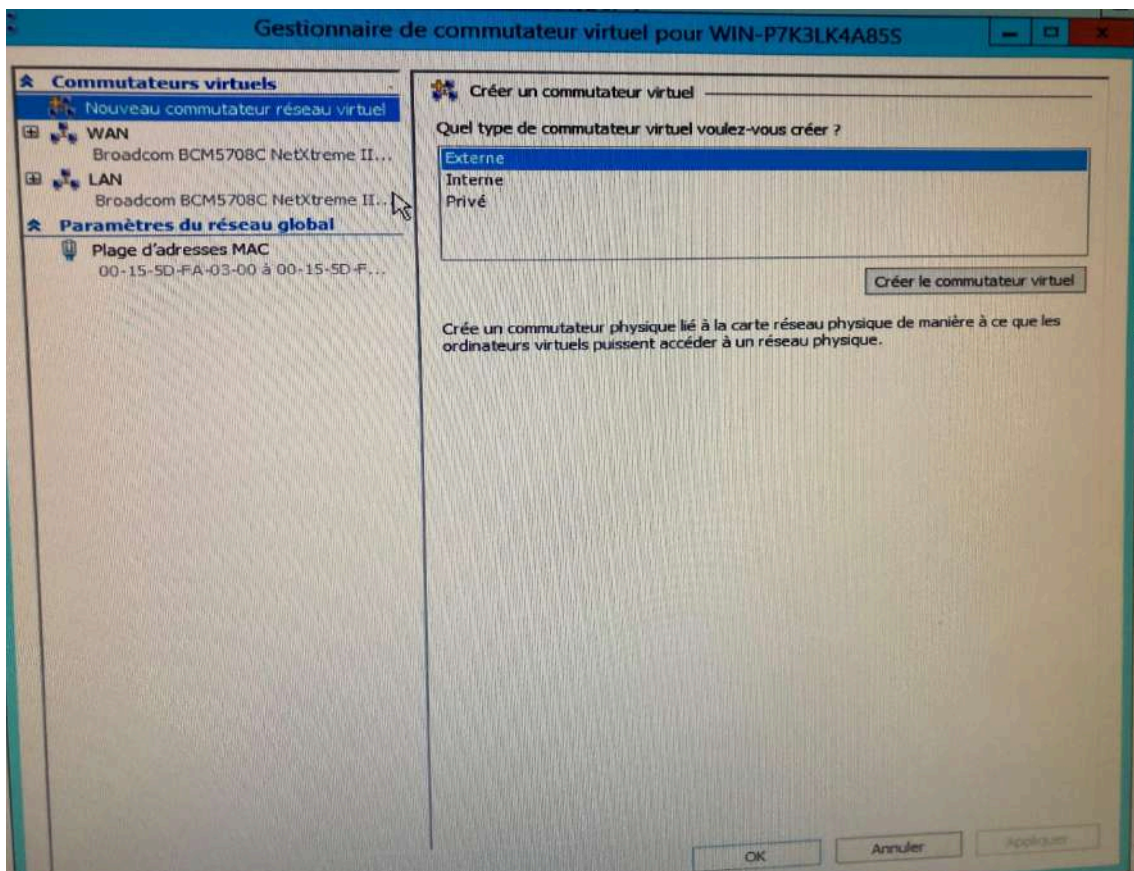
Une fois le fichier iso sélectionné il reste plus qu'à valider et lancer la machine virtuelle :



Cette image nous montre la création de la machine virtuelle.

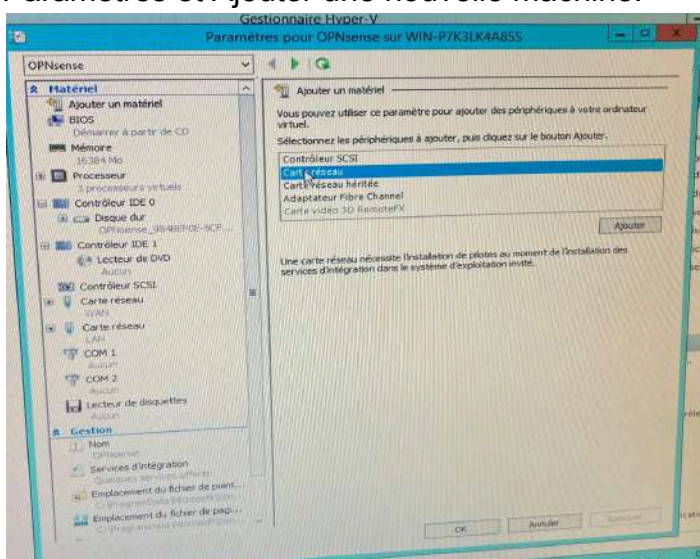
## Installation OPNsense :

Après avoir créé la machine virtuelle, il faut créer une deuxième carte réseau virtuelle internet pour qu'on puisse faire le routage sur le OPNsense donc on va sur actions -> win-(suitedumachine) -> Gestionnaire du Réseau d'Hyper V

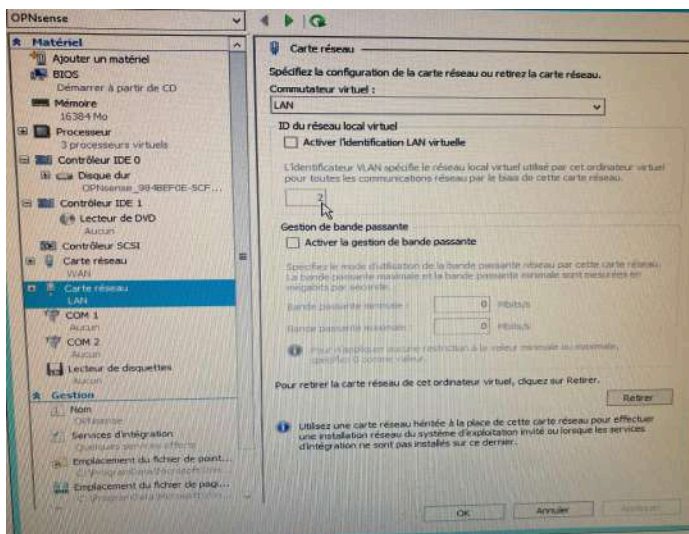


Cette image nous montre les paramètres de la carte réseau sur hyper-v  
Après, il faut le mettre dans les paramètres de la machine OPNsense en ajoutant une nouvelle carte réseau.

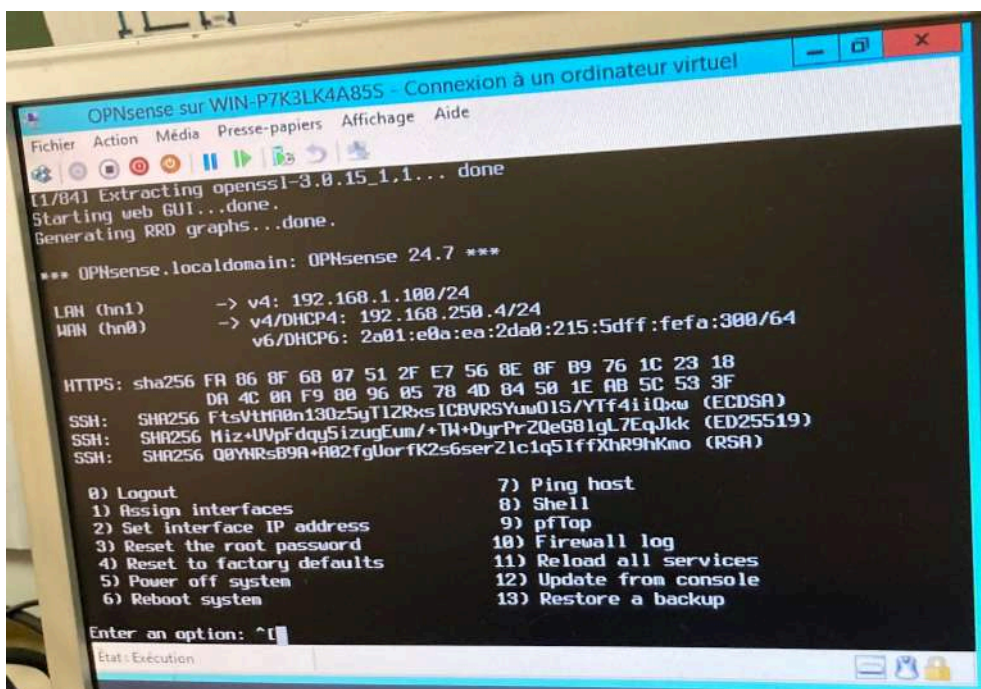
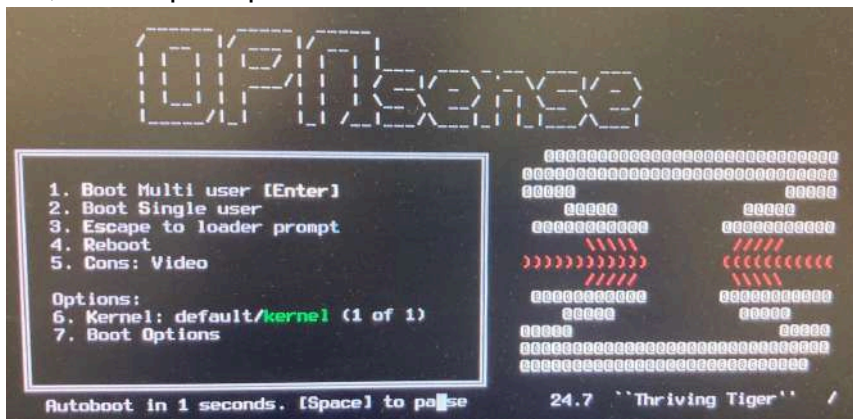
Pour cela, on ajoute la carte réseau pour cela on va sur actions -> OPNsense -> Paramètres et Ajouter une nouvelle machine.







Est, il reste plus qu'à lancer OPNsense.



Ces image nous montre l'ouverture de OPNsense

Optionnel :

au cas où, si il y a des problèmes avec les paramétrage des carte réseau, il suffit juste de le mettre manuellement.

```
2) Set interface IP address          9) pfTop
3) Reset the root password          10) Firewall log
4) Reset to factory defaults        11) Reload all services
5) Power off system                 12) Update from console
6) Reboot system                    13) Restore a backup

Enter an option: 1

Do you want to configure LAGGs now? [y/N]: n
Do you want to configure VLANs now? [y/N]: n

Valid interfaces are:

hn0          00:15:5d:fa:03:00 Hyper-V Network Interface
hn1          00:15:5d:fa:03:01 Hyper-V Network Interface

If you do not know the names of your interfaces, you may choose to use
auto-detection. In that case, disconnect all interfaces now before
hitting 'a' to initiate auto detection.

Enter the WAN interface name or 'a' for auto-detection: hn0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(or nothing if finished): hn1
```

cet image nous montre les paramètres de la carte réseaux d'OPNsense

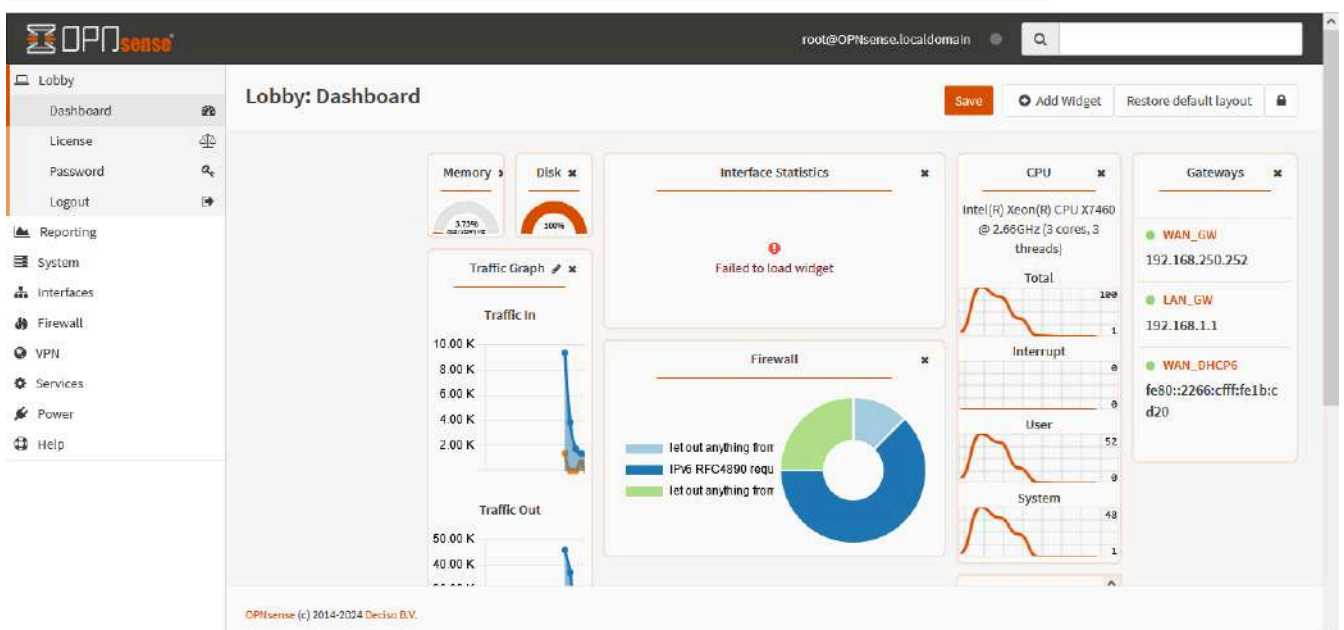
Après l'installation OPNsense, avec l'adresse IP de la carte de réseau LAN on se connecte sur le site web embarqué.

l'utilisateur : root

motdepasse : opnsense



The image shows the OPNsense login page. At the top is the OPNsense logo. Below it, there are two input fields: "Nom d'utilisateur:" (Username) and "Mot de passe:" (Password). The username field contains the text "root". The password field is masked with dots. Below the password field is an orange button labeled "Connexion" (Login).



Ces images nous montre la page d'accueil est de connexion du site web embarqué de OPNsense

## PARTIE 4 - Mise en place du Pare-Feu :

Après être connecté au site web embarqué, il faut mettre en place le pare-feu pour qu'on puisse accéder à internet pour s'informer en enlevant quelques ports informatiques pour internet.

Pour cela, on va tout d'abord garder les ports afin de se connecter sur internet, pour cela, on va dans Pare-feu -> Alias -> est on ajoute alias en type ports.

Les Ports à Garder :

- Port 443 : Le Protocole HTTPS qui rend les sites Internet possibles et sécurisés.
- Port 80 : Le Protocole HTTP qui rend les sites Internet possibles
- Port 53 : Le Protocole DNS qui permet d'accéder à internet via une adresse IP.

Edit Alias

full help

Enabled ☒

Name Servers

Type Port(s)

Categories

Content 53 80 443  
Clear All Copy Paste

Description

Cancel Save

Cette image nous montre que la page de la création de l'alias.

On crée une autre alias mais de type réseau pour notre réseau utilisé

Modifier l'alias

aide complète

Activé ☒

Nom host

Type Réseau(x)

Catégories

Contenu 192.168.1.0/24  
Tout effacer Copier Coller

Statistiques ☐

Description

Annuler Sauvegarder

Cette image nous montre que la page de la création de l'alias.

Ensuite, on va dans la page des règles pour modifier la règle d'accès à l'adresse IPv4 est ajoutée pour cela on va dans Pare-feu -> Règles(Rules en anglais) -> LAN

Tout d'abord, Mettre les protocoles de transmission TCP et UDP

The screenshot shows the 'Edit Firewall rule' configuration window. The 'Protocol' dropdown is set to 'TCP/UDP'. Other visible settings include 'Action' set to 'Pass', 'Interface' set to 'LAN', 'Direction' set to 'in', and 'TCP/IP Version' set to 'IPv4'. There is a 'full help' link in the top right corner.

Cette Image nous montre la modification du protocole de transmission

Puis, mettre modifier les sources est mettre notre alias

This screenshot shows the 'Source' and 'Destination' configuration section of the firewall rule. The 'Source' dropdown is set to 'host'. Below it, there is a 'Source' tab and an 'Avancé' (Advanced) button. The 'Destination' dropdown is set to 'any'. There is also a checkbox for 'Utilisez cette option pour inverser le sens de la correspondance' (Use this option to invert the sense of the correspondence).

Cette Image nous montre la modification de la règles

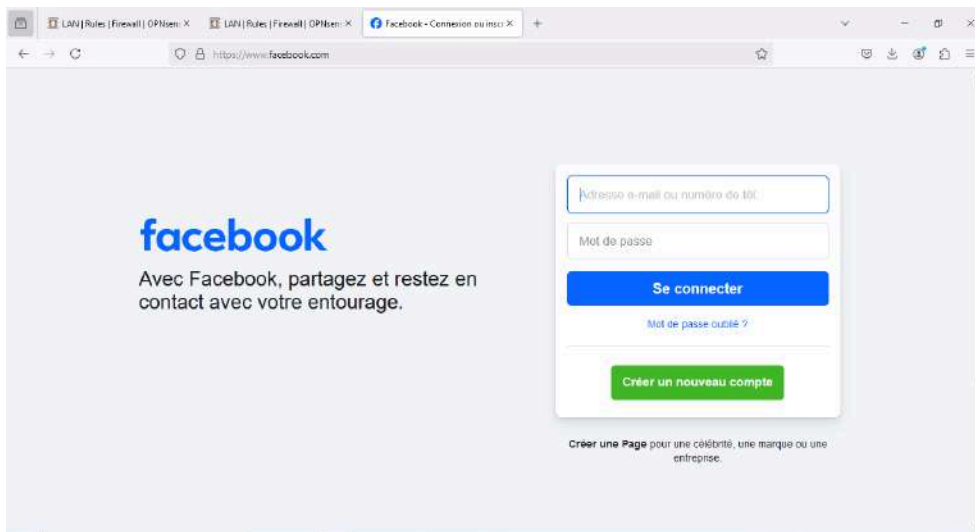
Enfin, validé la configuration.

This screenshot shows the bottom of the WinBox interface with the rule list. The rule is named 'IPv4 TCP/UDP' with source 'host' and destination 'PORTS'. The status is 'Default allow LAN to any rule'. There are icons for back, edit, copy, and delete.

Cette Image nous montre la validation de la configuration de la règles

il reste plus qu'à tester internet.





## PARTIE 5 - Mise en place d'un Portail Captif :

Un Portail captif est une technique consistant à forcer les clients HTTP d'un réseau de consultation à afficher une page authentification avant d'accéder à Internet normalement


Dans notre cas, mon tuteur de stage, ma demande de créer un Portail Captif avec une active directory virtuelle, pour qu'un client puisse se connecter via un réseau wifi avec une tablette.






### OPNsense :

Avant de le mettre en marche notre nouvelle active directory virtuelle, il faut tout d'abord paramétrer notre Portail Captif c'est pour cela, il faut créer un nouvel utilisateur.

il faut aller dans Système -> Accès -> Utilisateur est ajouté un nouvel utilisateur.

**Système: Accès: Utilisateurs**

aide complète 

Défini par	USER
 Désactivé	<input type="checkbox"/>
 Nom d'utilisateur	<input type="text" value="user"/>
 Mot de passe	<div><input type="password"/> <input type="password"/> (confirmation)</div> <div><input type="checkbox"/> Générer un mot de passe aléatoire pour empêcher l'utilisateur de se connecter à la base de données</div>
 Nom complet	<input type="text" value="Utilisateur"/>
 Courriel	<input type="text"/>

OPNsense (c) 2014-2024 Deciso B.V.

Cette image nous montre la création d'un utilisateur

**Système: Accès: Utilisateurs**

Nom d'utilisateur	Nom complet	Groupes	
 root	System Administrator	admins	
 user	Utilisateur	stage	 

 Administrateur Système    Utilisateur désactivé    Utilisateur standard

Cette image nous montre la page des utilisateurs.

Ensuite, il faut créer un groupe d'utilisateurs pour accéder à internet via le groupe. pour cela, il faut aller dans Système -> Accès -> Groupes est ajouté un nouveau groupe d'utilisateur.

**Système: Accès: Groupes**

Défini par  
 Nom du groupe:   
 Description:   
 Membre du groupe:

Non membre de

root

→

←

Membre de

user

Privileges attribués

Type:  Nom:

Cette image nous montre la création du groupe d'utilisateur

**Système: Accès: Groupes**

Nom du groupe	Nombre de membre(s)	Description	
admins	1	System Administrators	
stage	1		

Groupe superutilisateur 
 Groupe normal

Cette image nous montre la page des groupes d'utilisateur.

Maintenant, il faut créer notre portail captif. Pour cela on va dans : Service -> Portail Captif -> administration est ajouté un portail captif.

Dans le portail captif, il faut bien connecter avec une base de données en local avec le bon groupe d'utilisateur est mettre une adresse ip d'un hôte,

*nb : j'ai mis un temps de connexion à 10 minutes pour faire des tests de connexion avec le portail captif sinon il faut mettre 0 pour ne pas mettre de temps de connexion.*

Editer la zone

mode avancé

aide complète

Activé

☒

Numéro de zone

0

Interfaces

LAN

Tout effacer

Sélectionner tout

Allow inbound

WAN

Tout effacer

Sélectionner tout

Identifier en utilisant

Local Database

Tout effacer

Sélectionner tout

Envoyez toujours des demandes de comptabilité

☐

Appliquer le groupe local

stage

Annuler

Sauvegarder

Editer la zone

Délai d'inactivité (minutes)

0

Hard timeout (minutes)

10

Connexions simultanées d'utilisateurs

☒

Certificat SSL

Aucun

Nom d'hôte

Adresses autorisées

192.168.1.102/24

Tout effacer

Copie

Pâte

Texte

Modèle personnalisé

Aucun

Description

Service Portail Captif

Annuler

Sauvegarder

Ces images nous montrent les paramétrages du portail captif.

est il reste plus qu'à créer une règle pour accepter le portail captif.

image en cours,

est faire les tests :

cette image nous montre la page de d'authentification sur internet.

Cette image nous montre les logs du portail captif.

## Active Directory :

Active directory est dispositif de gestion d'utilisateur est de Groupe d'utilisateur.

Maintenant, on va créer une machine virtuelle pour un Windows Server 2012 ou dans laquelle, on va mettre en place un active directory avec des utilisateurs. pour qu'on puisse accéder avec portail captif avec c'est compte en question.

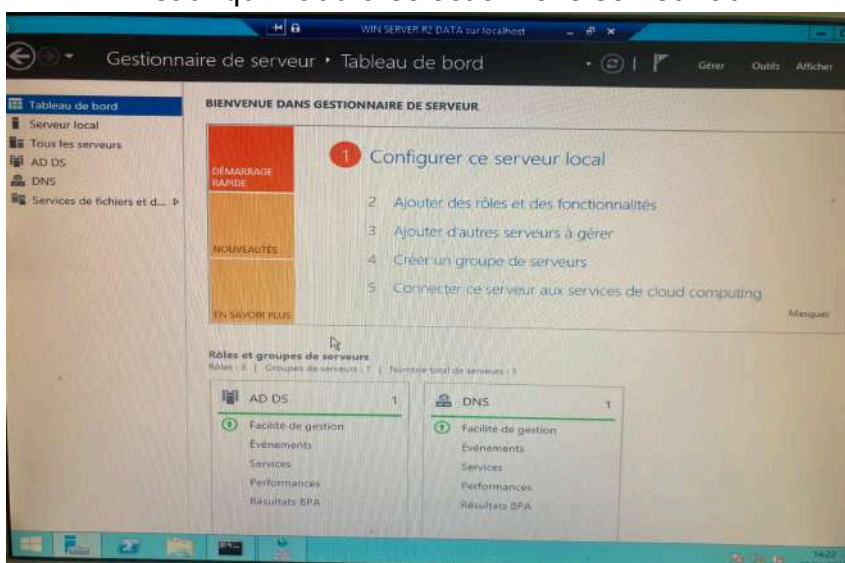
## Création de l'Active Directory :

Pour cela on vas tout d'abord, créer une machine virtuelle avec un Windows Server 2012 R2 (comme pour l'hyper-v) :



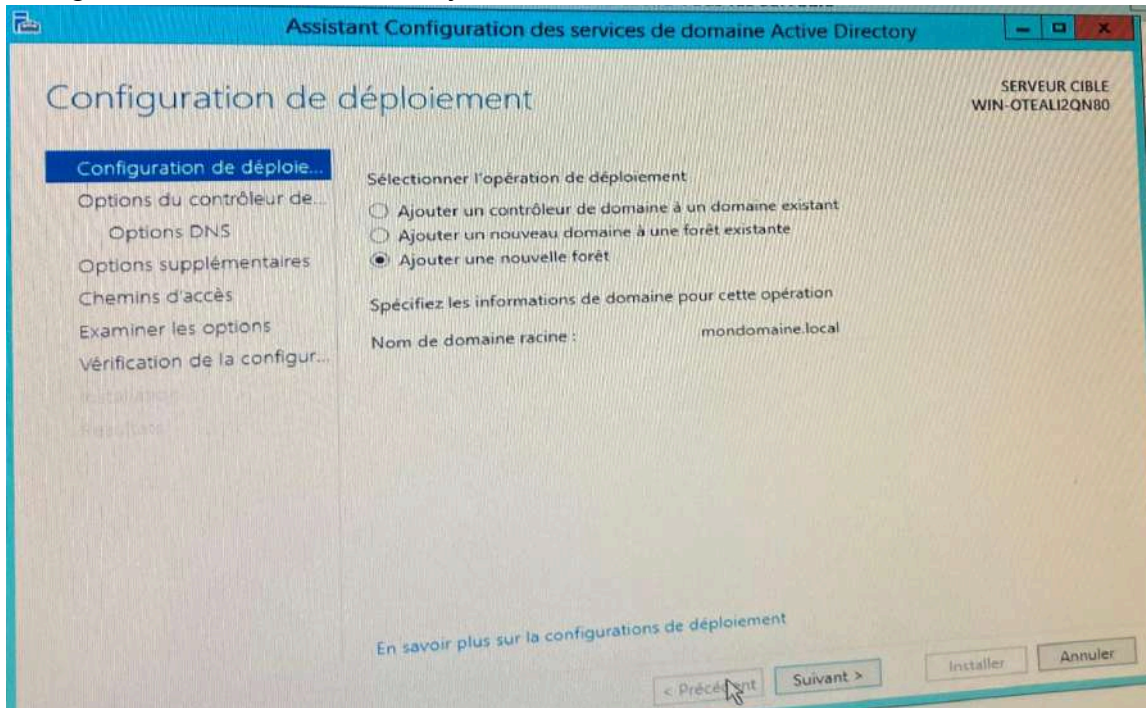
Cette image nous montre la page d'ouverture de Windows Server 2012 R2

Une fois l'installation faite, on commence par créer un nouveau serveur comme avec HYPER-V sauf qu'il faudra sélectionné le serveur ad :



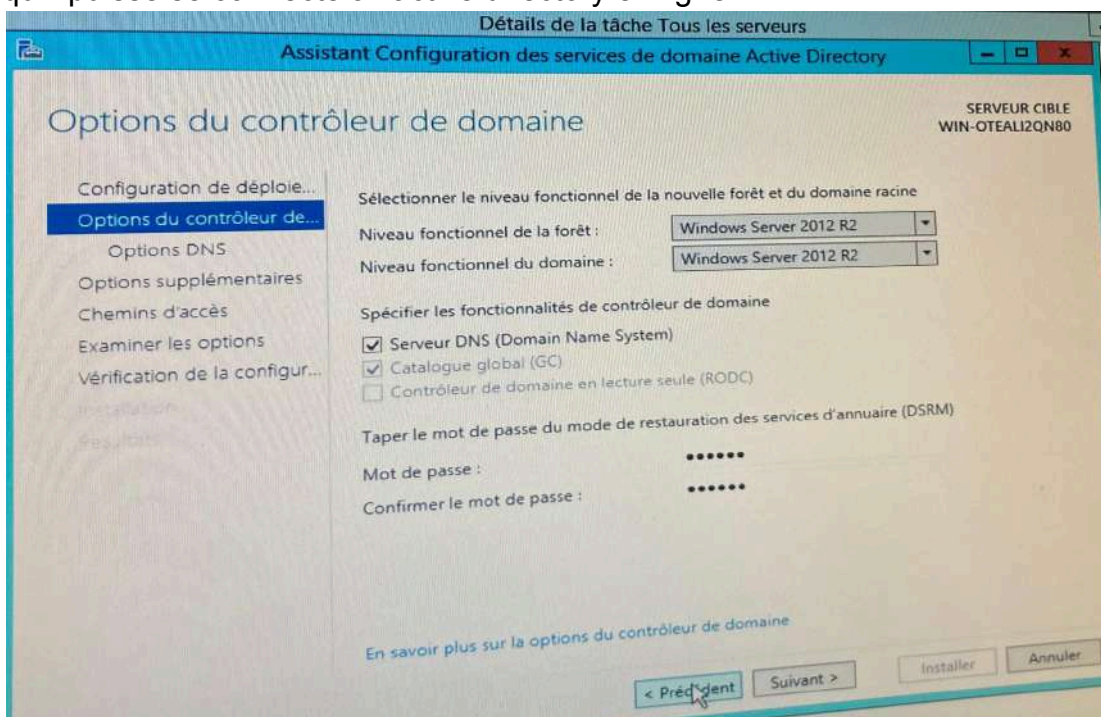


Cette image nous montre le gestionnaire de serveur avec le serveur AD et DNS  
Ensuite on va créer un utilisateur dans un fichier de l'active directory, pour cela on va dans Outils -> Utilisateur et Ordinateur Active Directory. est il vont nous rediriger sur une configuration de Active Directory



Cette image nous la configuration de déploiement de l'active directory

Ensuite, on choisit le domaine de l'active directory en général il faut lui mettre un dns pour qu'il puisse se connecté à l'active directory en ligne...

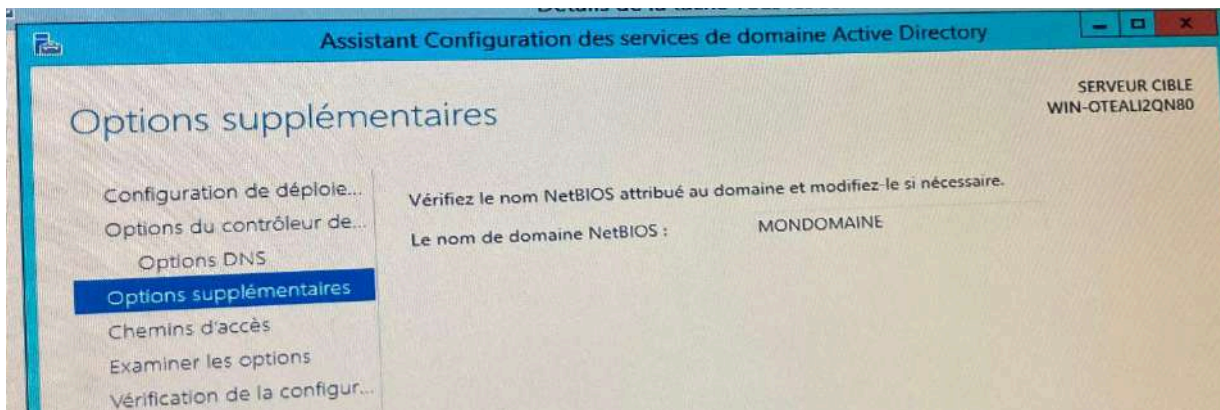




Cette image nous la configuration de déploiement de l'active directory

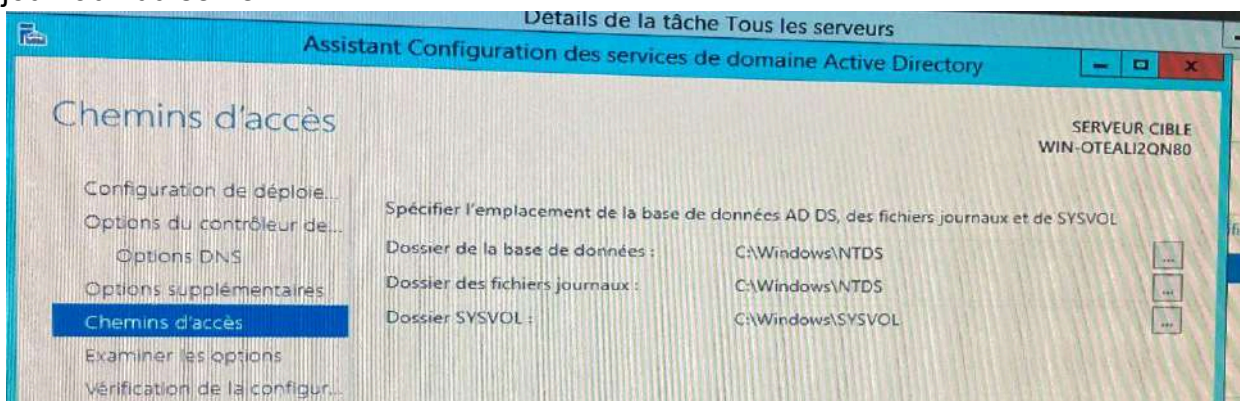
Ensuite, je dois mettre le nom du domaine du NetBIOS pour qu'on puis se connecté à ce domaine plus tard :

NetBIOS est un système de nommage et une interface logicielle qui permet d'établir des sessions entre différents ordinateurs d'un réseau.



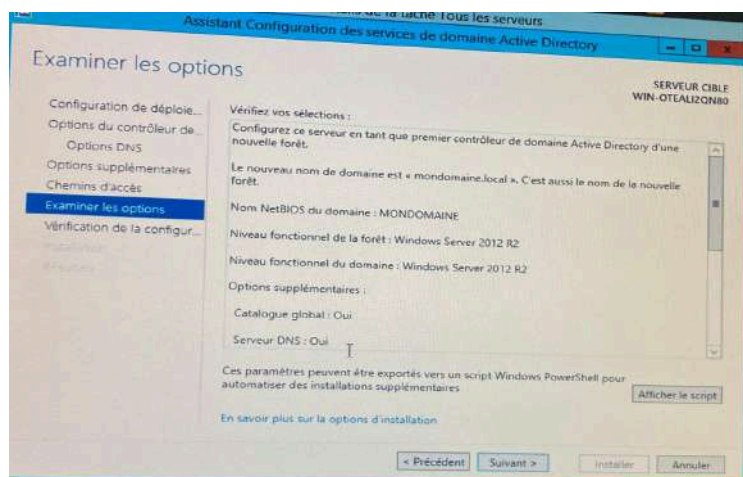
Cette image nous montre la création du nom de domaine NetBIOS

Ensuite, je dois mettre en place le chemin d'accès pour la base de données et le fichier journaux du server.

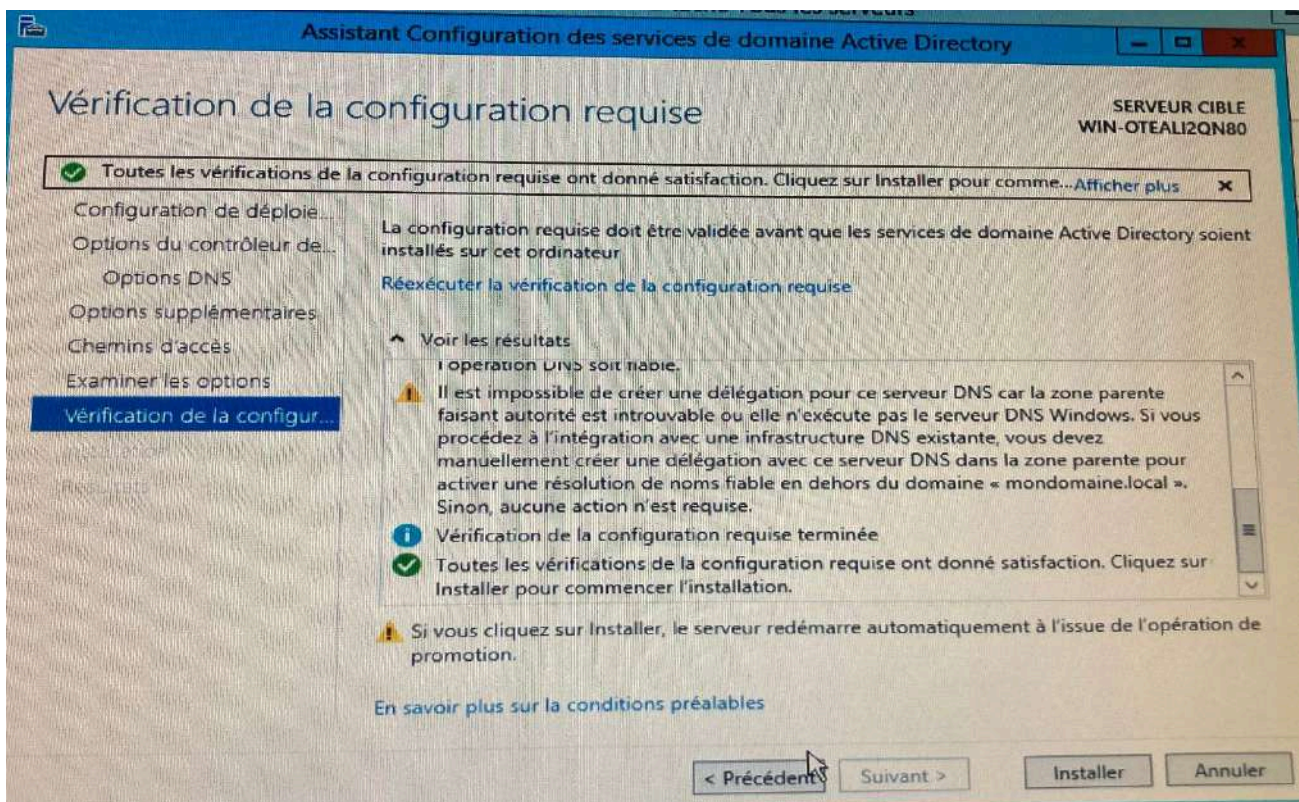


Cette image nous montre la mise en place des chemins d'accès.

Enfin, il reste plus à examiner et verifir la configuration :



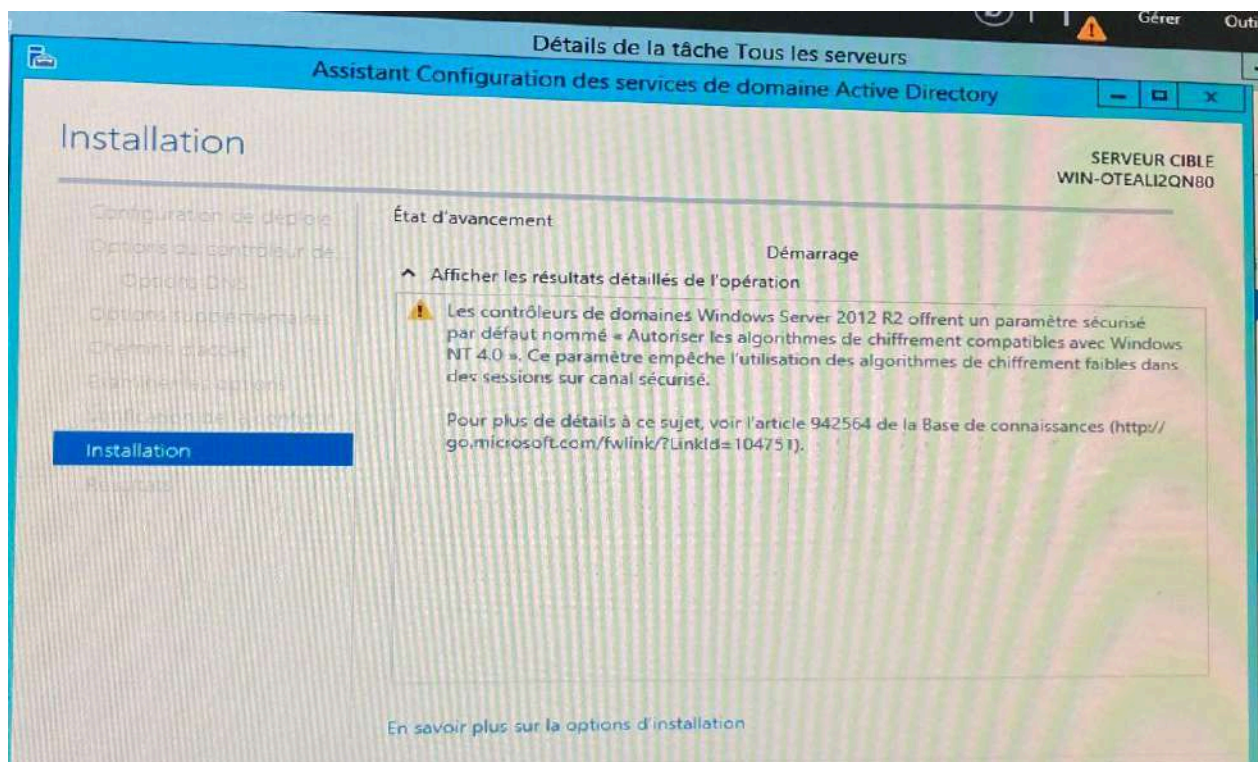
Cette image nous montre la page examination de la configuration de l'Active directory



Cette Image nous montre la vérification de Configuration de l'active directory.

Il reste plus qu'à commencer l'installation.



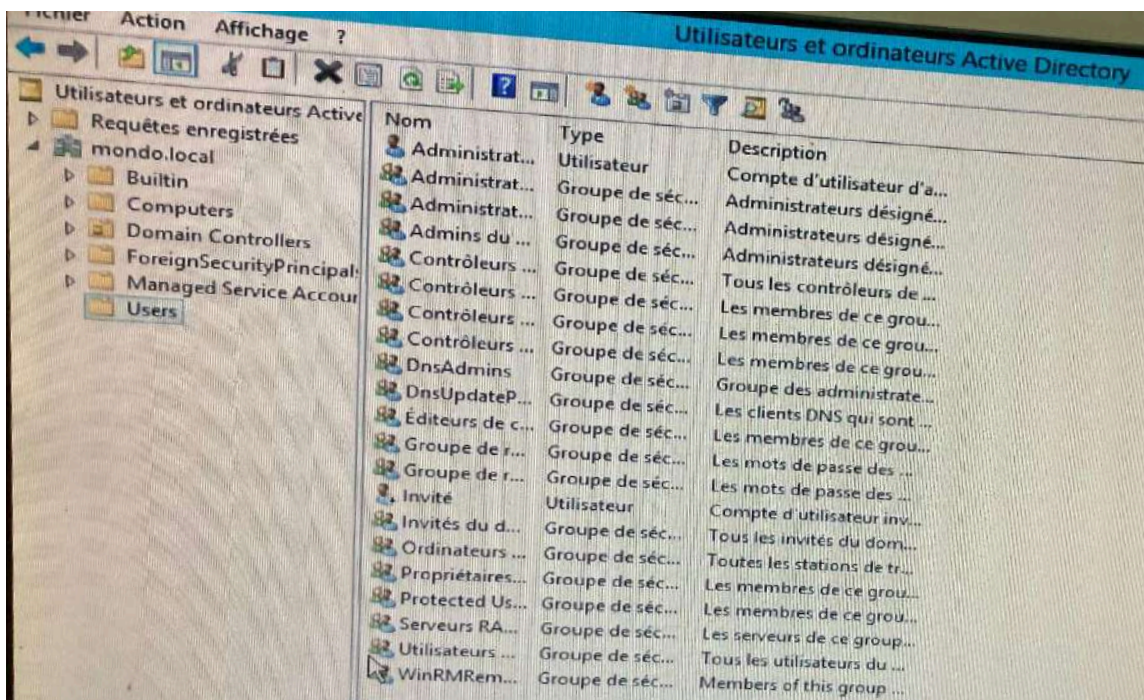


Cette image nous montre l'installation de la configuration de L'Active Directory.

### Création de L'Utilisateur :

Une fois, qu'on n'a créé le notre active directory, on va redémarrer le serveur et on va mettre en place un utilisateur pour qu'il puisse se connecter avec le portail captive plus tard.

Pour cela, on va retourner dans l'outil -> Utilisateur et ordinateur de l'active directory.



Cette image nous montre la page Utilisateur et ordinateurs de l'active directory.

Ensuite on va dans notre domaine -> Users et faire un clic droit sur la souris est créer un utilisateur est saisir les données de l'utilisateur.

**Nouvel objet - Utilisateur**

Créer dans : mondo.local/Users

Prénom :  Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :  @mondo.local

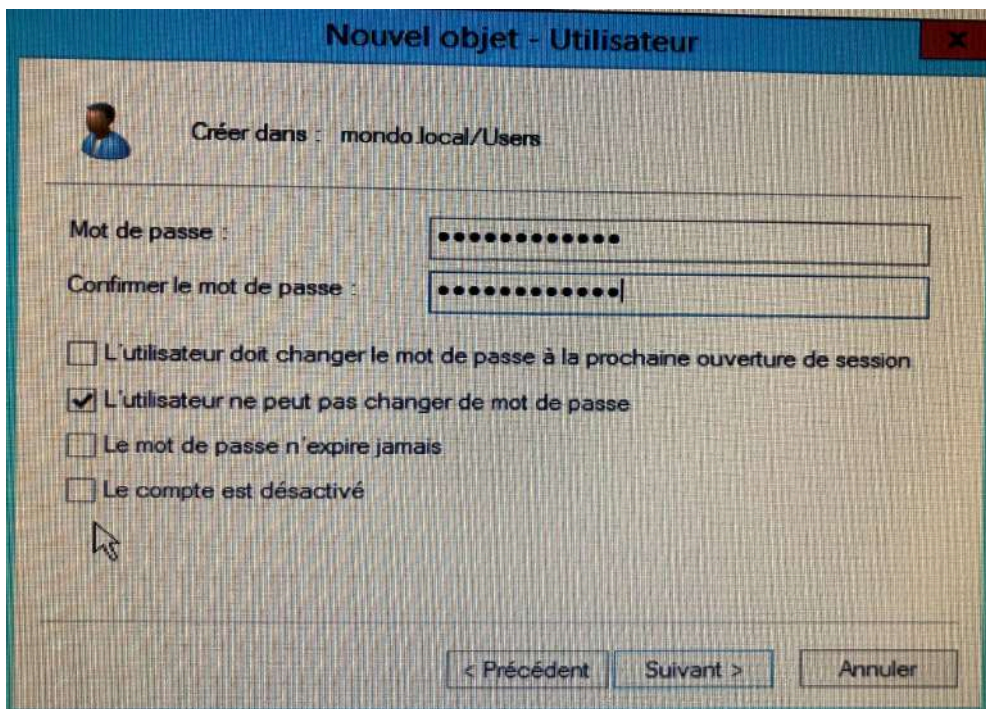
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent    Suivant >    Annuler

Cette image nous montre la page de création de l'utilisateur.

Ensuite on va saisir le mot de passe, il faut bien décocher la première case et cocher la deuxième pour ne pas avoir de problème avec le portail captif plus tard.

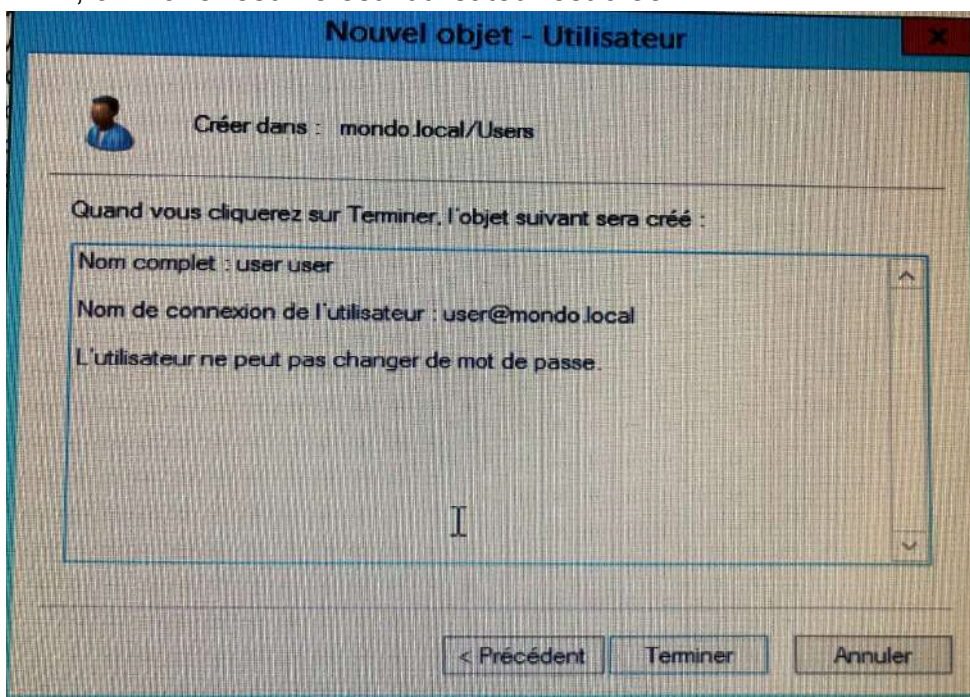




The screenshot shows a window titled "Nouvel objet - Utilisateur" with a close button (X) in the top right corner. Below the title bar, there is a user icon and the text "Créer dans : mondo.local/Users". The main area contains two password input fields: "Mot de passe :" and "Confirmer le mot de passe :", both filled with dots. Below these fields are four checkboxes with the following labels: "L'utilisateur doit changer le mot de passe à la prochaine ouverture de session", "L'utilisateur ne peut pas changer de mot de passe" (which is checked), "Le mot de passe n'expire jamais", and "Le compte est désactivé". At the bottom right, there are three buttons: "< Précédent", "Suivant >", and "Annuler".

cette image nous montre la création du mot de passe de l'utilisateur

Enfin, on n'a le resumé est l'utilisateur est créé.



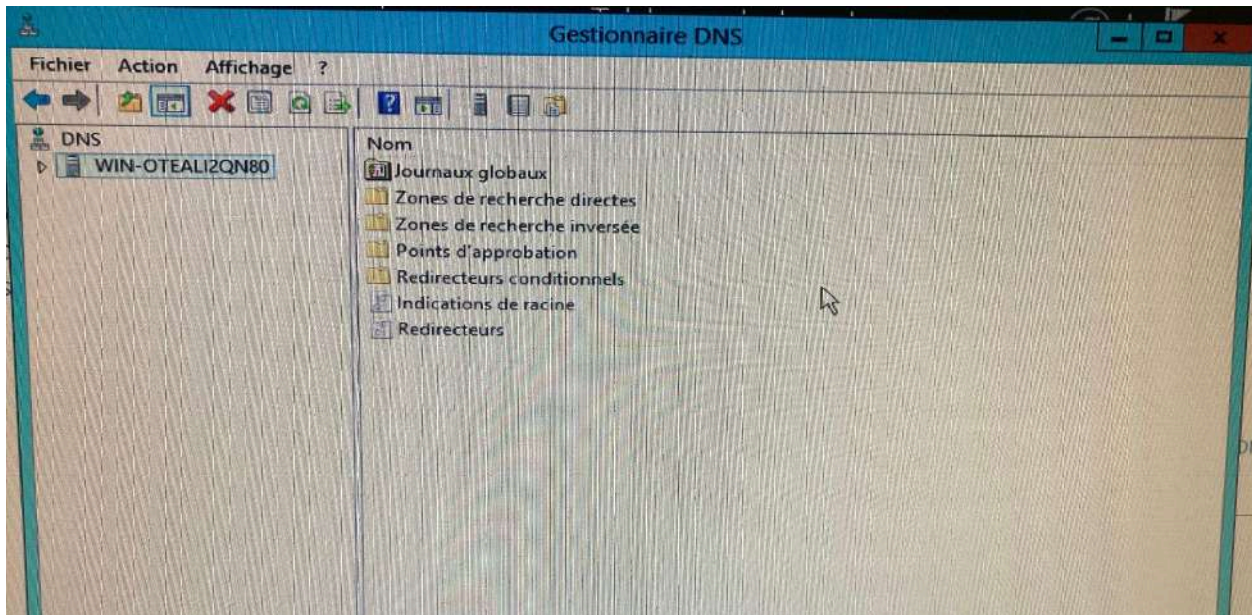
The screenshot shows the same window "Nouvel objet - Utilisateur" but at a different stage. The text "Créer dans : mondo.local/Users" remains. Below it, a message states: "Quand vous cliquerez sur Terminer, l'objet suivant sera créé :". A large text box contains the following summary information: "Nom complet : user user", "Nom de connexion de l'utilisateur : user@mondo.local", and "L'utilisateur ne peut pas changer de mot de passe.". At the bottom right, the buttons are now "< Précédent", "Terminer", and "Annuler".

Cette image nous montre le resumé de la création de l'utilisateur.



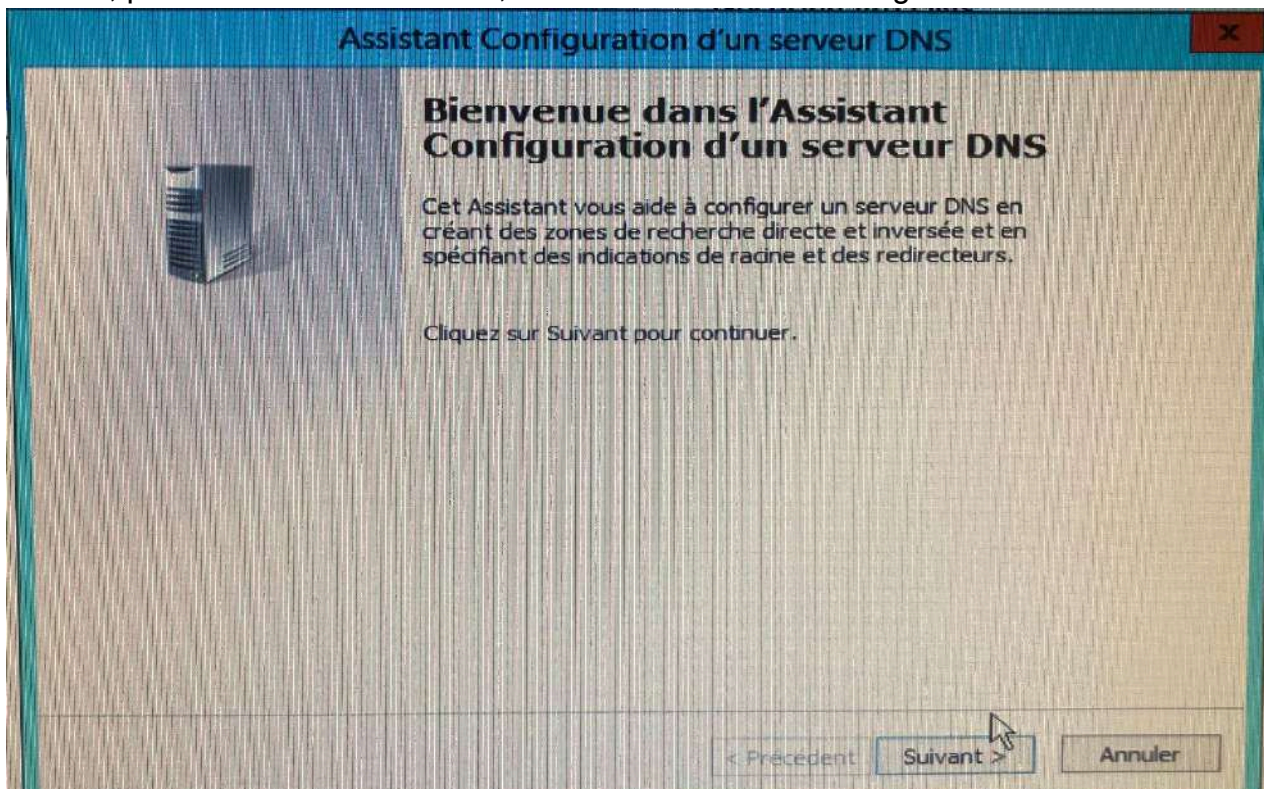
## Création de Serveur DNS :

Maintenant, on va créer le serveur DNS, afin qu'on puisse connecter les notre Active Directory avec notre Pare-feu, pour cela, on retourne dans les Gestionnaire de Serveur -> Outils -> DNS.



Cette image nous montre la page du DNS

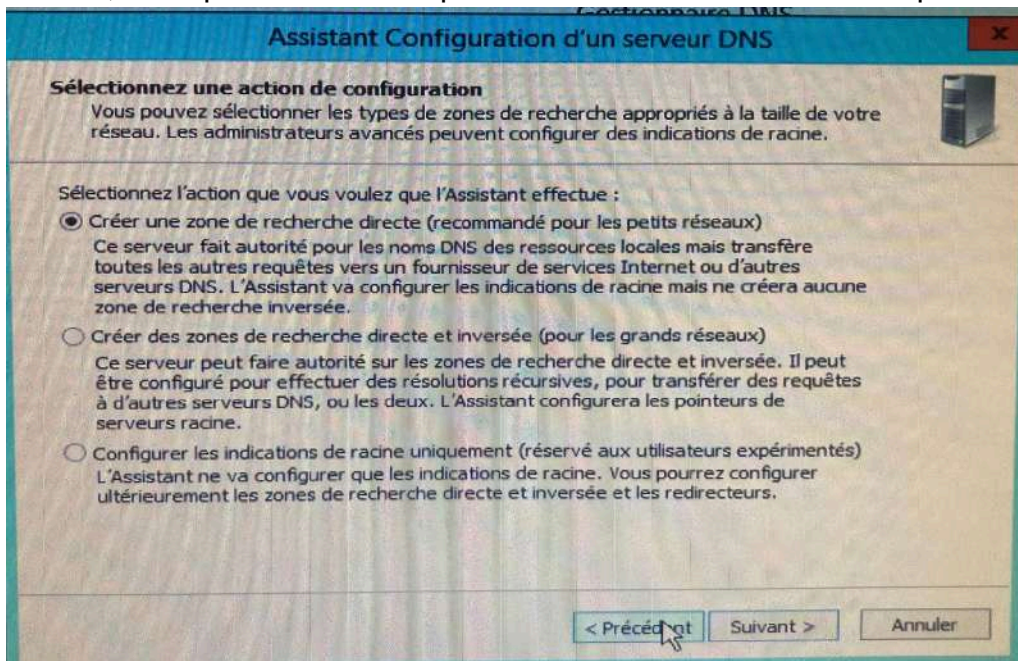
Ensuite, pour créer le serveur DNS, on va dans Action -> Configurer un serveur DNS.



Cette Image nous montre la page de la création d'un serveur dns.

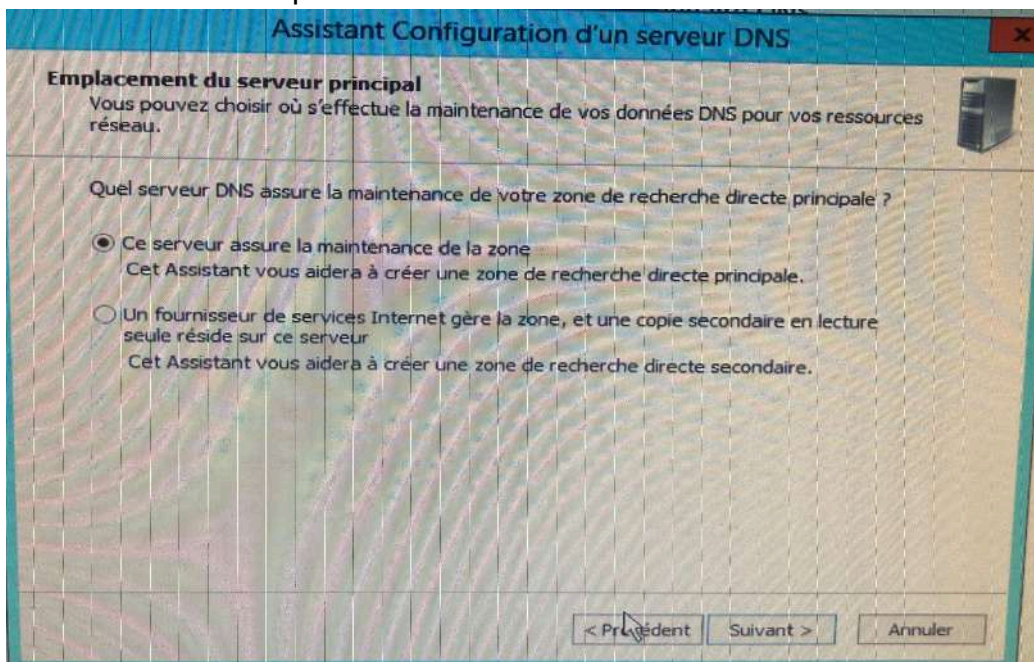


Maintenant, on va configurer le serveur DNS, tout d'abord, on va configurer les actions du serveur, on va prendre le choix par défaut car c'est recommandé pour des petites réseaux.



Cette image nous montre la sélection d'action de configuration choisie.

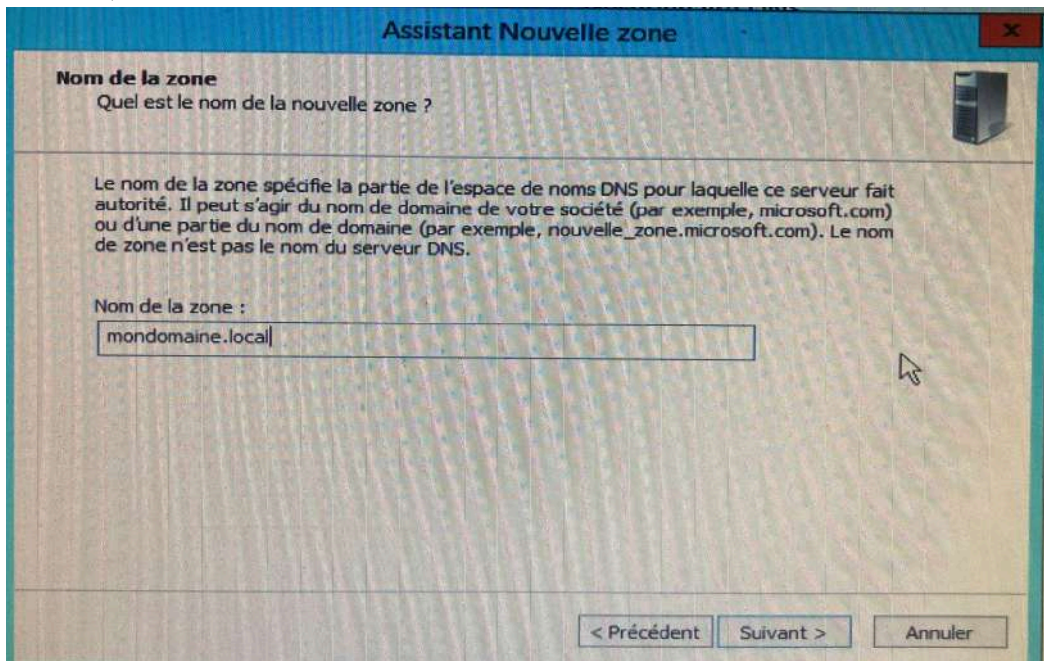
Ensuite, on va configurer le serveur DNS comme hôte de notre connexion internet pour cela on va le laisser par défaut.



Cette image nous montre la sélection choisie

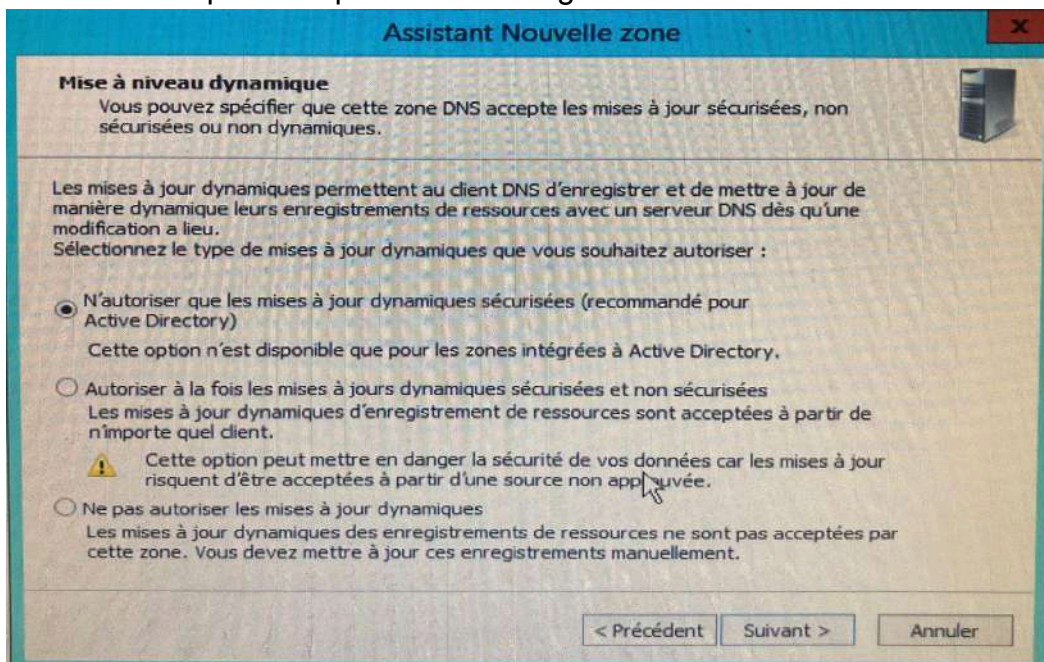


Ensuite, on va mettre le nom du domaine du serveur DNS.



Cette image nous montre le nom de mon serveur dns

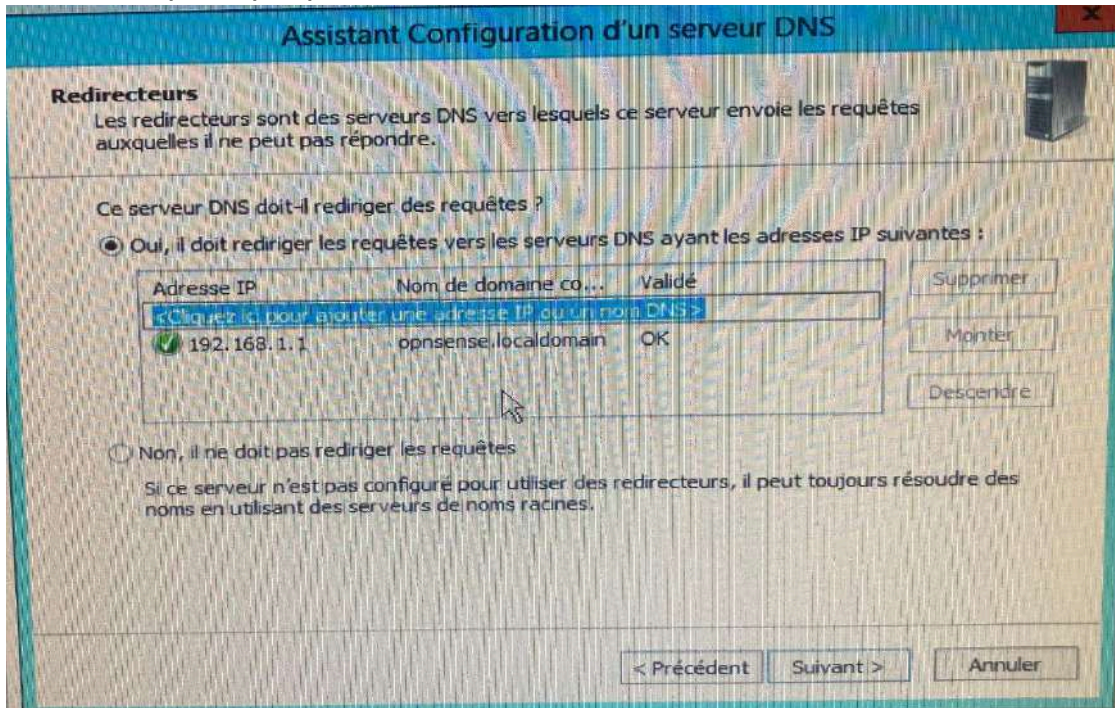
Ensuite, on va pas autorisé les mise à jour système, car il est pas recommandé pour notre AD est il n'est pas utile pour notre configuration



Cette image nous montre la sélection choisie



Ensuite, on va mettre adresse ip qui va envoyer des requêtes, dans notre cas on va mettre le Pare-feu pour qu'il puisse se connecter directement dans notre AD.



Cette image nous montre la sélection choisie

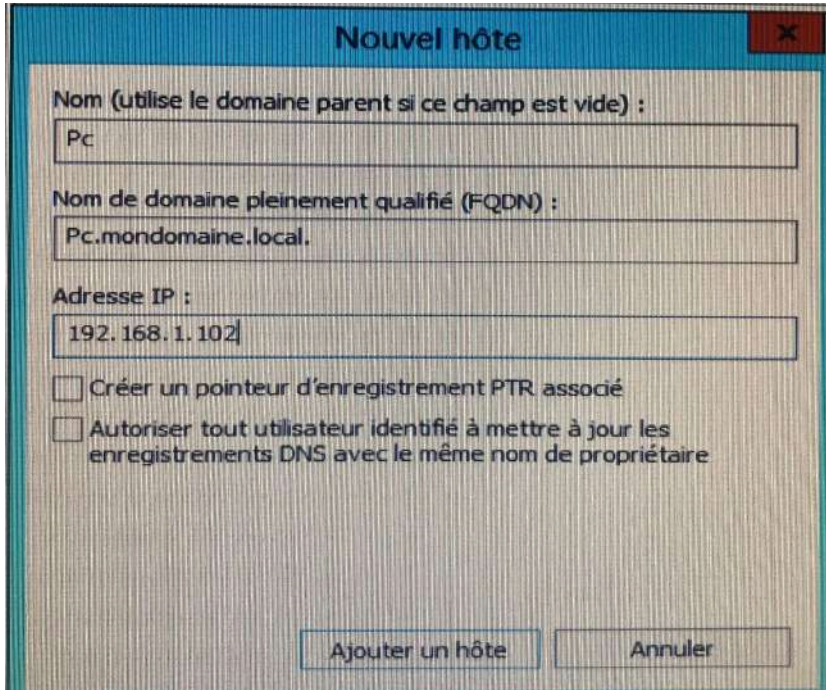
Enfin, il reste plus qu'à valider.



Cette image nous montre la fin de la configuration du DNS.

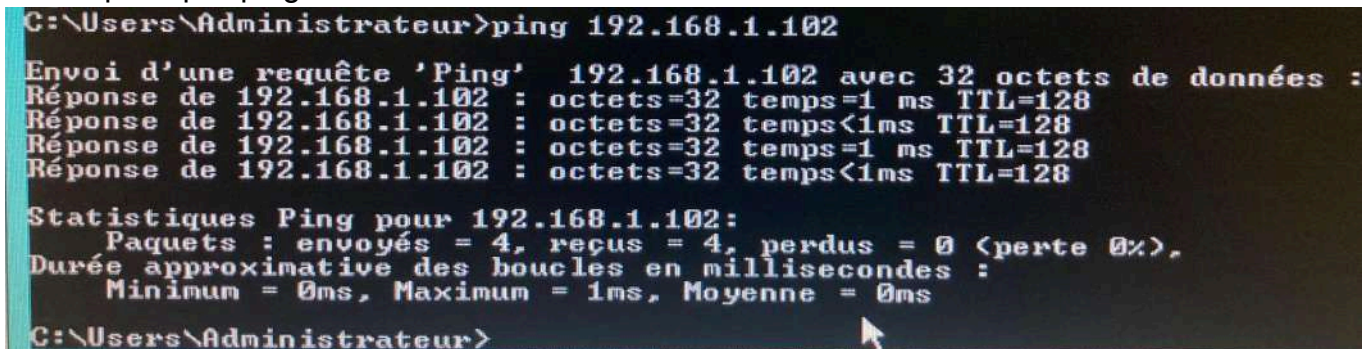


Ensuite, il reste plus qu'à créer un hôte de connexion avec notre ordinateur pour cela on va dans Action -> Nouvel Hôte.



Cette image nous montre la création de l'hôte dans notre serveur.

il reste plus qu'à ping l'ordinateur.



Cette image nous montre qu'on ping l'ordinateur.

## Importer Portail Captif avec AD :

Une fois que la création du serveur fini, il faut paramétrer l'OPNsense afin que notre Portail captif se connecte avec les utilisateurs de L'Active Directory.

Pour cela, il faut tout d'abord créer le serveur sur l'OPNsense. pour cela on va dans système -> accès -> serveurs est créé est ajouté notre serveur.

### Système: Accès: Serveurs

[aide complète](#)

Nom descriptif	AD_LDAP
Type	LDAP
Nom d'hôte ou adresse IP	<input type="text" value="192.168.1.105"/> <small>NOTE: Quand SSL est utilisé, le nom d'hôte DOIT correspondre au Nom Commun (CN) du certificat SSL du serveur LDAP.</small>
Numéro de port	<input type="text" value="389"/>
Transport	<input type="text" value="TCP - Standard"/> <small>Lorsque vous choisissez StartTLS ou SSL, veuillez configurer les autorités de certification privées requises dans Système -&gt; Confiance</small>
Version du protocole	<input type="text" value="3"/>
Identités de liaison	<div>DN de l'utilisateur : <input type="text" value="CN=Administrateur,CN=Users,DC=mondomaine,DC=local"/></div> <div>Mot de passe : <input type="password" value="*****"/></div> <div><small>Laisser vide pour permettre l'utilisation de liaisons anonymes afin de résoudre les noms uniques</small></div>
Étendue de la recherche	<input type="text" value="Un Niveau"/>
DN de Base	<input type="text" value="CN=Users,DC=mondomaine,DC=local"/>
Conteneurs d'authentification	<div><input type="text" value="CN=Users,DC=mondomaine,DC=local"/> <input type="button" value="Sélectionner"/></div> <div><small>Liste de noms distinctifs séparés par des points-virgules contenant des composants DC=.</small></div> <div><small>Exemple: OU=Freelancers,O=Company,DC=example,DC=com;CN=Users,OU=Staff,O=Company,DC=example,DC=com</small></div>
Requête Étendue	<div><input type="text"/></div> <div><small>Exemple: &amp;(objectClass=inetOrgPerson)(mail=*@example.com)</small></div>
Attribut de nom d'utilisateur	<input type="text" value="sAMAccountName"/>

**Synchroniser les groupes** ☐

Synchroniser les groupes spécifiés par l'attribut memberOf ou class après la connexion, cette option nécessite d'activer la lecture des propriétés. Les groupes seront extraits de la première section CN= et ne seront pris en compte que s'ils existent déjà dans OPNsense. Les membres des groupes seront conservés dans OPNsense. Utilisez l'outil de test du serveur pour vérifier si memberOf est renvoyé par votre serveur LDAP avant d'activer l'option.

**Contraint groups** ☐

Constraint allowed groups to those selected in the container section. This may offer additional security in cases where users are able to inject memberOf attributes in different trees.

**Groupes limites**

Limiter les groupes qui peuvent être utilisés par cet authentificateur, laisser vide pour prendre en compte tous les groupes locaux dans OPNsense. Lorsque des groupes sont sélectionnés, vous pouvez attribuer manuellement à l'utilisateur des groupes non assignés.

**Création automatique d'utilisateurs** ☐

À utiliser en combinaison avec la synchronisation des groupes, pour permettre à l'authentificateur de créer de nouveaux utilisateurs locaux après une connexion réussie avec les appartenances aux groupes renvoyées pour l'utilisateur.

**Correspondance insensible à la casse** ☒

Autoriser la saisie de caractères mixte lors de la collecte des paramètres utilisateur locaux.

**Sauvegarder**

Ces Images nous montre l'ajouter de notre serveur active directory dans l'OPNsense



**Système: Accès: Serveurs**

Nom du serveur	Type	Nom d'hôte	
AD_LDAP	LDAP	192.168.1.105	 
Base de données locale	Base de données locale	OPNsense	

Cette Image nous montre l'ajout du serveur Active directory



Ensuite, il reste plus qu'à modifier notre portail captif pour qu'il passe dans l'Active directory que dans la base de données local.

**Interfaces**

 Tout effacer  Sélectionner tout



Sélectionner la ou les interface(s) à activer pour le portail captif.

**Allow inbound**

 Tout effacer  Sélectionner tout

Select interfaces from which to allow inbound (stateful) traffic. This can be convenient if the zone in question contains machines/servers which should be accessible from other networks attached to this firewall.

**Identifier en utilisant**

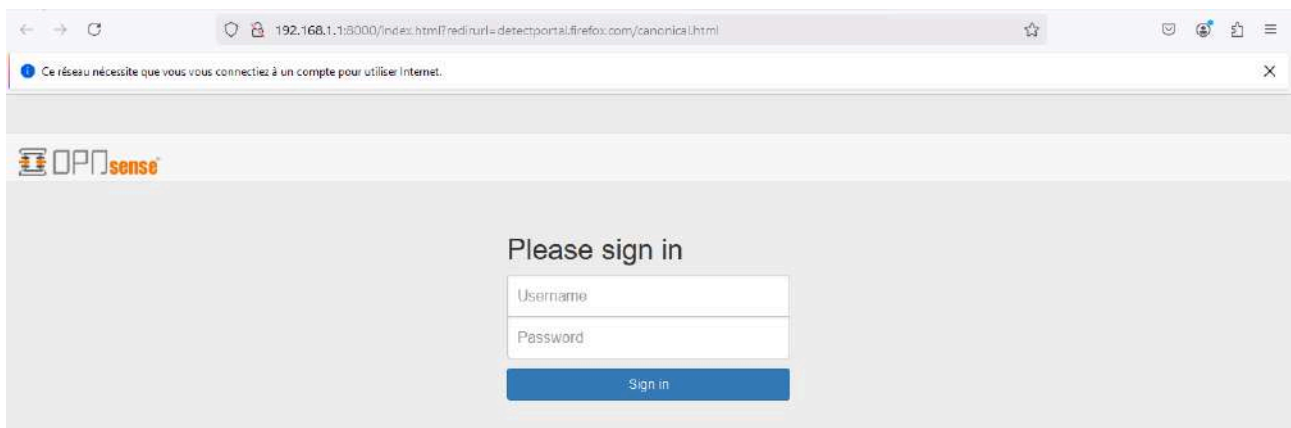
 Tout effacer  Sélectionner tout

Sélectionner la méthode d'authentification, laisser vide quand aucune authentification n'est exigée.

Cette Image nous montre la modification du portail captif

Enfin, il reste plus qu'à tester avec le nom de l'utilisateur.



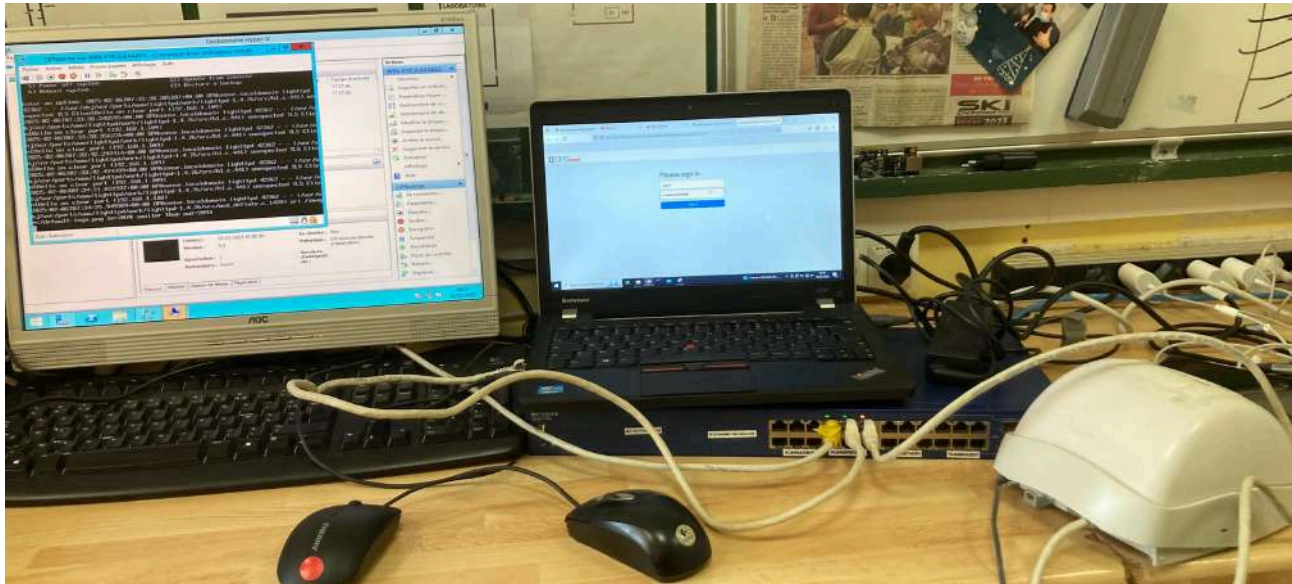


Cette image nous montre la page de connexion de mon réseau.

## Wifi :

Pour que notre portail captif utilise sa propre fonction, on va installer une borne wifi de la marque Ruckus, afin de tester le portail captif avec un réseau sans fil.

Pour cela, on va connecter la borne wifi dans l'un des vlan d'un des switch que j'ai configuré dans un compte-rendu précédent avec l'ordinateur et le serveur.



Cette image nous montre l'ajout de la borne wifi dans le réseau.

Ensuite, on va se connecter dans un navigateur web ancien pour qu'il puisse se connecter dans le site web embarqué de la borne wifi.



The image shows the Ruckus Wireless Admin login page. At the top is the Ruckus logo, which features a stylized dog head and the text 'Ruckus WIRELESS'. Below the logo is the title 'Ruckus Wireless Admin' in blue. There are two input fields: 'Username:' with the value 'super' and 'Password:' with a masked password of eight dots. Below these fields is an orange 'Login' button.

Cette image nous montre la page de connexion du site web embarqué.

**Ruckus 2942 Multimedia Hotzone Wireless AP**

**Status**

- Device
- Internet
- Local Subnets
- Wireless

**Configuration**

- Device
- Internet
- Local Subnets
- Wireless
- Ethernet Ports
- Hotspot

**Maintenance**

- Upgrade
- Reboot / Reset
- Support Info

**Administration**

- Management
- Diagnostics
- Log

**Status :: Device**

Device Name: RuckusAP

Device Location:

GPS Coordinates:

MAC Address: 00:22:7F:04:84:40

Serial Number: 320801003764

Software Version: 9.3.4.0.21

Uptime: 27 mins 19 secs

Current Time (GMT): Fri Oct 1 11:42:06 2021

LAN Port Status <a href="#">Refresh</a>					
Port	Interface	802.1X	Logical Link	Physical Link	Label
0	eth0	None	Up	Up 100Mbps full	10/100PoE
1	eth1	None	Down	Down	10/100

Cette image nous montre la page d'accueil du site web embarqué.

Ensuite, il faut configurer notre connexion Wi-Fi, pour cela on va dans configuration -> wireless est configuré la connexion sans fil.

**Configuration :: Wireless :: Common**

Common OPNwifi OPNwifi Wireless 3 Wireless 4 Wireless 5

Wireless Mode: Auto-select

Channel: SmartSelect

Country Code: No country set

Advanced Settings: Edit Common Settings

External Antenna: ☐ Disabled ☐ Enabled

AeroScout RFID

AeroScout RFID tag detection: ☐ Disabled ☐ Enabled

Update Settings Restore previous settings

Cette image nous montre la configuration sans fil de notre wifi.

Ensuite on va configurer la connexion internet de notre wifi, pour qu'il prenne un rôle de portail captif, on va mettre notre connexion en sécurité la plus bas avec le protocole wep.

**Configuration**

Device  
Internet  
Local Subnets  
**Wireless**  
Ethernet Ports  
Hotspot

**Maintenance**  
Upgrade  
Reboot / Reset  
Support Info

**Administration**  
Management  
Diagnostics  
Log

Wireless Network: OPNwifi

Wireless Availability? ☒ Enabled ☐ Disabled

Broadcast SSID? ☒ Enabled ☐ Disabled

SSID: OPNwifi

Threshold Settings: Edit Settings

Rate Limiting: Edit Settings

Access Control: Edit Settings

Packet Forward: Bridge to WAN

Hotspot Service: None

Access VLAN: 1

Insert DHCP option 82? ☒ Enabled ☐ Disabled

Encryption Method: Disabled

Update Settings Restore previous settings

Cette image nous montre la configuration de notre wi-fi.

Enfin, il reste plus qu'à tester avec une tablette Apple



Ces images nous montrent la connexion wifi avec le portail captif via une tablette Apple.

## Conclusion :

En outre, j'ai créé un serveur pare-feu explorant plusieurs aspects clés d'OPNsense, notamment la configuration du pare-feu, la mise en place d'un portail captif, ainsi que l'authentification avec un Active Directory.

L'OPNsense sécuriser et gérer un réseau, mais aussi l'importance d'une configuration précise pour garantir un fonctionnement optimal. Avec une bonne maîtrise des protocoles d'authentification, du routage et des règles de filtrage, OPNsense devient un atout essentiel pour une infrastructure réseau robuste et sécurisée.