

Sommaire

1. Présentation du contexte :	3
2. Liste des besoins :	4
3. Cahier des charges incluant une estimation financière des investissements :	5
3.1 Introduction et Contexte du projet.....	5
3.2 Objectif du projet.....	5
3.3 Information sur les services	6
3.4 Estimation financière	7
4. Schémas des processus de l'entreprise modifiés par le projet :	8
5. Diagramme de Gantt du projet.....	9
5.1 Durée prévisionnelle du projet	9
5.2 Durée effective du projet.....	9
5.3 Diagramme des ressources montrant la répartition des taches.....	9
6. Description de la réalisation étape par étape :	10
6.1 DEJA-DUP	10
6.2 Postfix.....	11
6.3 Nextcloud	12
6.4 Active Directory.....	14
6.5 RDP	16
6.6 DHCP	17
6.7 Configuration du portail captif.....	18
6.8 TrueNas Core.....	19
7. Jeu de tests :	21
7.1 DEJA-DUP :	21
7.2 Postfix :	27
7.3 Nextcloud :	28
7.4 Active Directory :	31
7.5 Connexion RDP.....	33
7.6 Serveur DHCP	36
7.7 Portail Captif	38
7.8 TrueNas	40
8. Manuel technique :	41
8.1 Installation du logiciel de système de sauvegarde : DEJA DUP.....	41
8.2 Configuration d'un serveur de messagerie sur ubuntu : Postfix	43
8.3 Configuration d'un serveur cloud local : Nextcloud	45

8.4 Configuration d'un active directory: Windows server	48
8.5 Configuration D'une connexion à Distance : RDP	55
8.6 Configuration d'un Serveur DHCP : Pf sense.....	57
8.7 Installation pfSense et mise en place d'un portail captif.....	63
8.8 Rapport technique installation serveur fichier TrueNas Core	69
9. Manuel utilisateur :.....	76
9.1 Installation du logiciel de système de sauvegarde : DEJA DUP.....	76
9.2 Configuration d'un serveur de messagerie sur ubuntu : Postfix	78
9.3 Configuration d'un serveur cloud local : Nextcloud	80
9.4 Configuration d'un active directory: Windows server	84
9.5 Configuration D'une connexion à Distance : RDP	92
9.6 Configuration d'un Serveur DHCP : Pf sense.....	95
9.7 Rapport Détailé portail captif pfSense.....	102
9.8 Rapport technique installation serveur fichier TrueNas Core	109
10. Références bibliographiques (liste des sources documentaires)	116
11. Conclusion sur le travail réalisé ou restant à faire :.....	117

1. Présentation du contexte :

Spoon est une agence de consulting disposant d'une infrastructure informatique. Ils sont confrontés à un problème non négligeable : leur infrastructure informatique, absolument indispensable pour la réalisation de ses biens et services est totalement dépassé par rapport à ce que d'autres entreprises de même catégorie peuvent avoir. Avec l'importance primordial qu'à l'informatique au sein de notre époque il est primordial pour Spoon de moderniser leur infrastructure. C'est dans ce contexte que l'on va devoir mettre en place diverses services avec une importance différente entre chaque service. Chacun de ces services mis en place permettront à l'infrastructure de se développer considérablement et d'être au norme de nos jours.

2. Liste des besoins :

- **Serveur de messagerie** : Un serveur de messagerie local afin de permettre aux employés de communiquer entre eux en toute sécurité
- **Téléphonie IP** : Un système qui va nous permettre d'utiliser les adresses IP pour les appels téléphoniques.
- **Serveur fichier/NAS** : Un serveur de fichiers ou un NAS afin de permettre un stockage sécurisé, une sauvegarde ainsi qu'un partage de fichiers sur plusieurs appareils.
- **Sauvegardes/backup** : Un système de sauvegarde afin de restaurer les données en cas de cyberattaque ou accident non intentionnelle.
- **DHCP/DNS** : Un protocole DHCP afin de permettre de distribuer automatiquement des adresses IP aux machines de l'infrastructure SI et de garantir un accès internet.
- **RDP/SSH** : RDP ou SSH afin permettent aux employés de se connecter et de contrôler un ordinateur ou un serveur distant. RDP est généralement utilisé pour les interfaces graphiques (windows), tandis que SSH est utilisé pour les interfaces en ligne de commande (linux).
- **Portail Captif/Radius** : Un portail captif nécessitant une authentification avant d'accéder à un réseau. Il sera utilisé pour l'authentification des utilisateurs et la gestion de l'accès au réseau.
- **Active Directory** : Un système Active Directory pour permettre à l'entreprise de disposer de fonctionnalités telles que l'authentification centralisée, le contrôle d'accès et la gestion des stratégies (GPO).
- **Cloud local** : Un Cloud local afin de permettre aux employés de stocker localement des ressources plus ou moins importantes.

3. Cahier des charges incluant une estimation financière des investissements :

3.1 Introduction et Contexte du projet

Spoon est une petite entreprise dotée d'une infrastructure informatique dépassé. Dans notre contexte actuel l'informatique est un secteur clé, c'est donc dans cette démarche qu'il va leur falloir une mise au pont technologique afin de pouvoir assurer les biens et/ou services qu'ils proposent.

3.2 Objectif du projet

L'objectif de ce projet sera donc de mettre en place divers services afin d'améliorer l'infrastructure informatique de SPOON et de leur permettre de mieux répondre aux besoins de leur entreprise En modernisant leur infrastructure, SPOON pourra améliorer son efficacité améliorer la qualité de ses services et renforcer sa productivité.

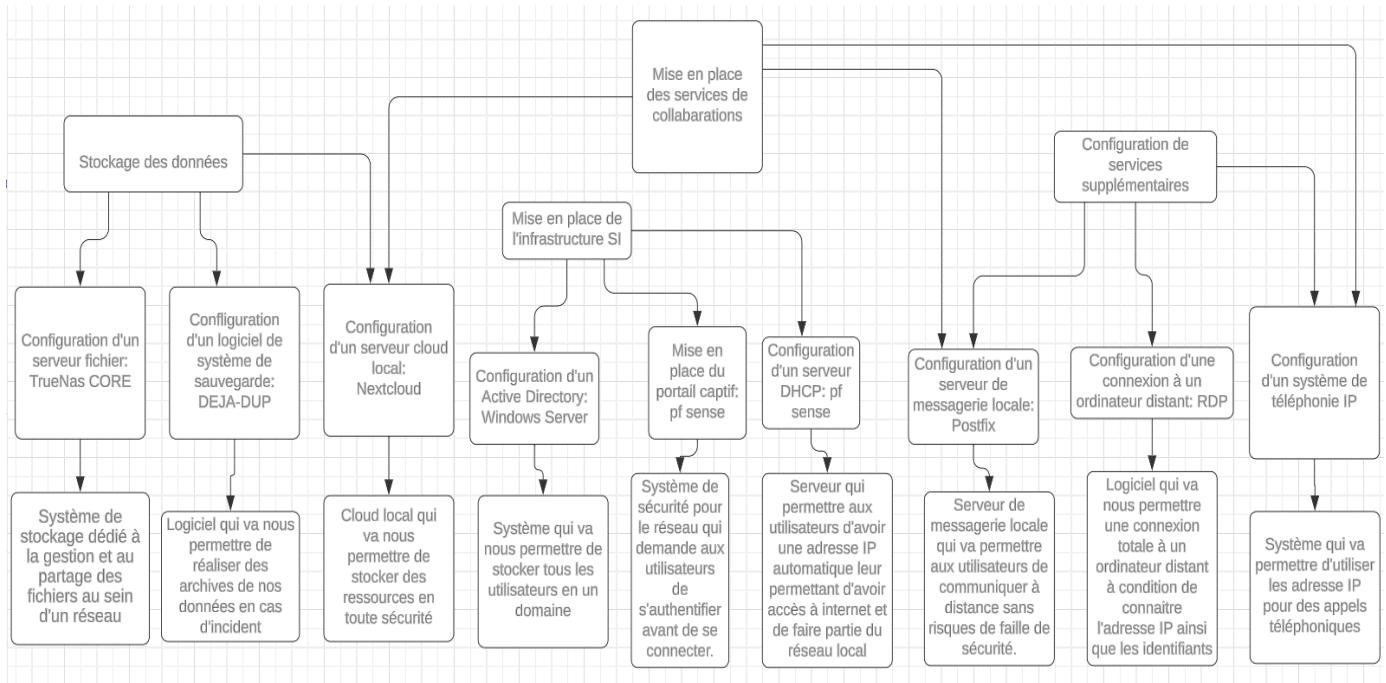
3.3 Information sur les services

Liste des services	Logiciel/ Solution utilisé	Description
Serveur de messagerie	Postfix	Serveur de messagerie locale qui va permettre aux utilisateurs de communiquer à distance sans risques de faille de sécurité.
Téléphonie IP	Service non mis en place	Système qui va permettre d'utiliser les adresse IP pour des appels téléphoniques
Serveur fichier/NAS	TrueNas	Système de stockage dédié à la gestion et au partage des fichiers au sein d'un réseau
Sauvegardes/backup	DEJA-DUP	Logiciel qui va nous permettre de réaliser des archives de nos données en cas d'incident
DHCP/DNS	pf-sense	Serveur qui permettre aux utilisateurs d'avoir une adresse IP automatique leur permettant d'avoir accès à internet et de faire partie du réseau local
RDP/SSH	RDP	Logiciel qui va nous permettre une connexion totale à un ordinateur distant à condition de connaître l'adresse IP ainsi que les identifiants
Portail Captif/Radius	pf-sense	Système de stockage dédié à la gestion et au partage des fichiers au sein d'un réseau
Active Directory	Windows Server	Système qui va nous permettre de stocker tous les utilisateurs en un domaine
Cloud local	Nextcloud	Cloud local qui va nous permettre de stocker des ressources en toute sécurité

3.4 Estimation financière

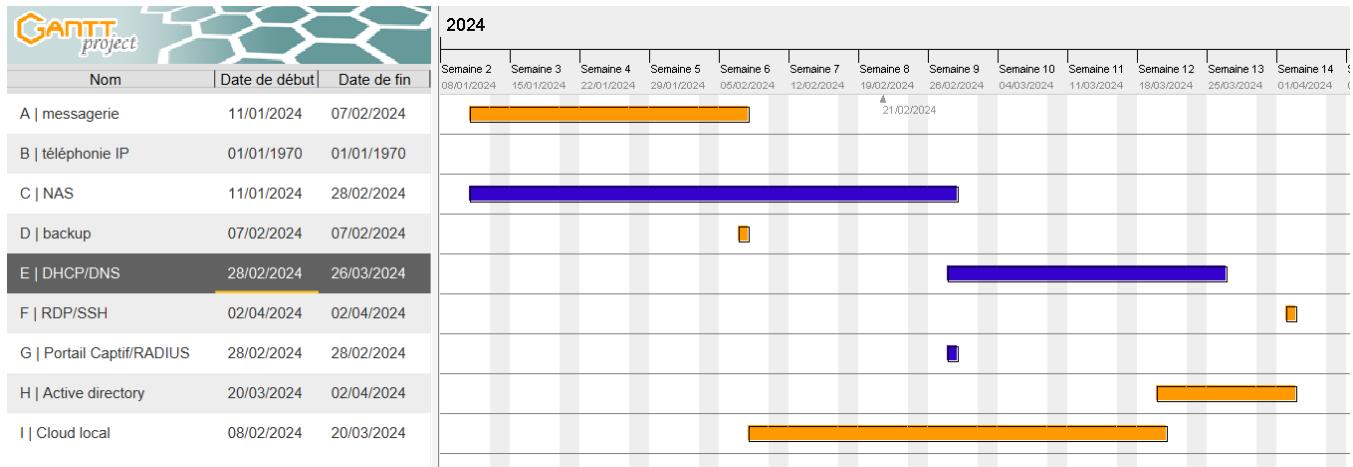
Service	Matériel requis	Prix
Service de messagerie	ISO Ubuntu	0€
Téléphonie IP	ISO AsteriskNow	0€
Serveur fichier/NAS	ISO TrueNas	0€
Sauvegardes/backup	ISO ubuntu	0€
DHCP/DNS	Iso Pfsense Machine dédié au serveur dhcp	Peut varier entre 500€ et 830€
RDP/SSH	OS Windows 10 Machine windows sur lequel on va se connecter à distance	Peut varier selon le besoin de l'utilisateur qui va se connecter En bas de gamme entre 180€ et 300€ En milieu de gamme nous aurons entre 500€ et 830€ Pour du haut de gamme on aura entre 900€ et 1200€
Portail Captif/Radius	ISO pf-sense Machine dédié au portail captif	Comme pour le serveur DHCP peut varier entre 500€ et 830€ puisque la différence de spécification requise est moindre
Active Directory	ISO windows server Machine dédié à l'active directory	Peut varier entre 850€ et 1300€
Cloud local	ISO ubuntu	0€

4. Schémas des processus de l'entreprise modifiés par le projet :



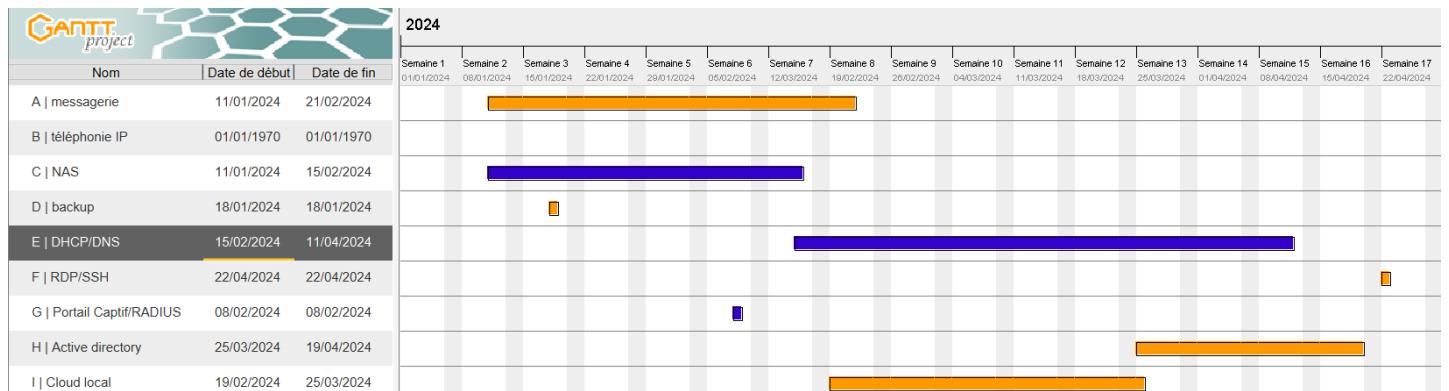
5. Diagramme de Gantt du projet

5.1 Durée prévisionnelle du projet

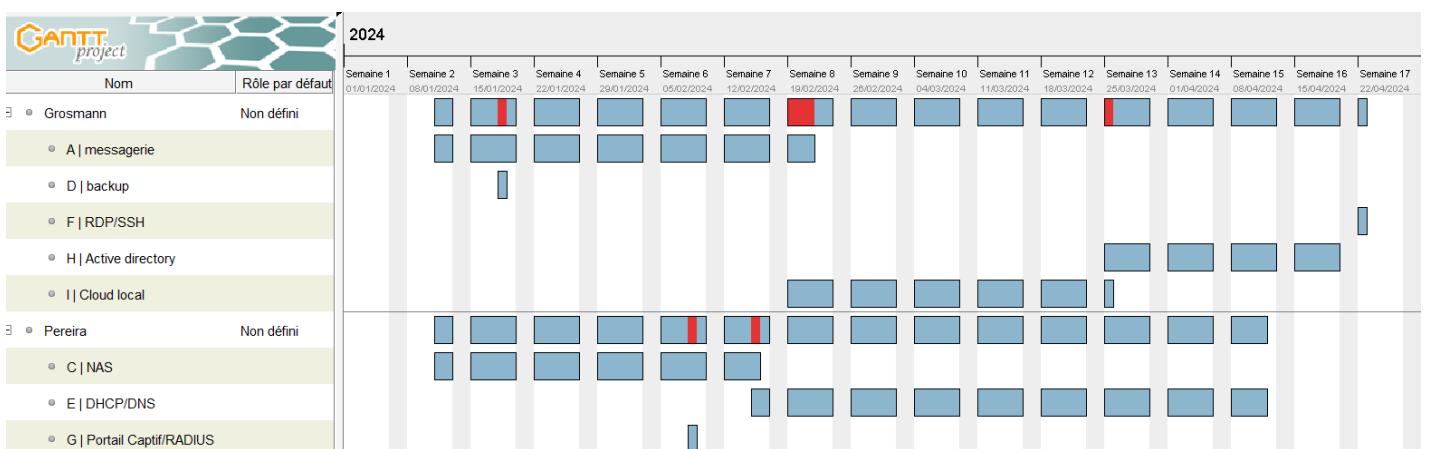


La date de début et de fin de téléphonie IP a été mis au 1^{er} janvier 1970 puisque nous avons pas pu la traiter.

5.2 Durée effective du projet



5.3 Diagramme des ressources montrant la répartition des tâches



6. Description de la réalisation étape par étape :

6.1 DEJA-DUP

ETAPE 1 : Récupération des paquets et installation de DEJA-DUP

1. Pour la configuration du logiciel de système de sauvegarde on commence par mettre à jour la liste des paquets avec « sudo apt update »
2. Ensuite on va pouvoir installer DEJA-DUP avec la commande « sudo apt install déjà-dup ».

ETAPE 2 : Choix du moyen de stockage de l'archive

Maintenant que DEJA-DUP est installé on va pouvoir choisir un moyen de stocker notre archive (one drive, google drive, localement sur le disque)

ETAPE 3 : Configuration de L'archive

Une fois qu'on s'est connecté dans le cas ou on a choisi google drive ou one drive on aura le choix d'entrer un mot de passe de chiffrement pour sécuriser l'archive et qui sera demandé pour sauvegarder et restaurer.

6.2 Postfix

ETAPE 1 : Récupération des paquets et installation de Postfix

1. Comme pour la configuration précédente on commence par mettre à jour la liste des paquets avec « sudo apt update ».
2. Après avoir effectué cette commande on installera postfix avec « sudo apt install postfix ».

ETAPE 2 : Configuration de Postfix

1. On arrivera sur deux menu qui nous intéresse, le premier va nous permettre de configurer postfix. On sélectionne « local uniquement » car on souhaite configurer un serveur de messagerie locale.
2. Concernant le deuxième menu on aura la possibilité d'entrer un nom de domaine pour la messagerie. Après avoir entrer un nom de domaine on peut finaliser la configuration.

ETAPE 3 : Vérification et finalisation de la configuration

1. Il faudra s'assurer que le fichier de configuration comporte aucune erreur, pour cela on va l'ouvrir avec la commande « sudo nano /etc/postfix/main.cf ».
2. Si tout est bon ou que vous avez corrigé les erreurs vous pouvez fermer le fichier en sauvegardant les changements puis redémarrer postfix avec la commande « sudo systemctl restart postfix »
3. Pour pouvoir recevoir des messages il va falloir installer le paquet « mailutils » avec la commande « sudo apt install mailutils »

6.3 Nextcloud

ETAPE 1 : Récupération des paquets et installation du serveur MySQL

1. Premièrement on va effectuer la commande « sudo apt update » comme pour Postfix et DEJA-DUP afin de mettre à jour la liste des paquets.
2. On va ensuite installer un serveur MySQL avec la commande « sudo apt install MySQL-server ».

ETAPE 2 : Création et configuration de la base de données

1. Maintenant que nous avons un serveur mysql installé on utilise la commande « sudo mysql » pour lancer le serveur.
2. Nous pouvons à présent créer une base de données avec la commande « CREATE DATABASE nextcloud »
3. Ensuite après avoir créé une base de données on créer un utilisateur avec « CREATE USER 'netxcloud'@'localhost' IDENTIFIED BY 'password' ; »
4. On lui donnera ensuite tous les droits avec « GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost' » et on recharge les droits avec « FLUSH PRIVILEGES ».

ETAPE 3 : Installation d'Apache

Après la configuration de la base de données on va pouvoir installer apache2 avec la commande « sudo apt install apache2 ».

ETAPE 4 : Installation de Nextcloud

1. Maintenant on va pouvoir installer nextcloud grâce à la commande « wget <https://download.nextcloud.com/server/releases/nextcloud-?.zip> » en remplaçant « ? » par la syntaxe correspond à la version de votre choix.
2. On va ensuite extraire l'archive dans le répertoire /var/www avec la commande « sudo unzip nextcloud- ?.zip -d/var/www »

ETAPE 5 : Configuration de Nextcloud

1. On va ensuite donner les droits à Nextcloud sur ce répertoire avec « sudo chown -R www-data :www-data /var/www/nextcloud ».
2. Après cela on va s'assurer que le fichier de configuration « nextcloud.conf » soit correctement configuré grâce à la commande « sudo nano /etc/apache2/sites-available/nextcloud.conf ». S'il ne comporte aucune erreur on peut quitter et sauvegarder si on a effectué des changements.
3. On activera ensuite le fichier de configuration avec la commande : « sudo a2ensite nextcloud.conf » puis redémarrer le serveur apache2 « sudo systemctl restart apache2 ».
4. Il va ensuite falloir installer php-curl avec la commande « sudo apt install php-curl ». Il va falloir redémarrer encore une fois le serveur apache avec la commande précédemment indiqué.
5. Pour accéder à nextcloud il va falloir ouvrir un navigateur internet et entrer votre adresse ip suivi de « /nextcloud ». Il vous suffira juste de vous connecter l'utilisateur de la base de données et vous aurez désormais accès à Nextcloud.

6.4 Active Directory

ETAPE 1 : Installation du rôle de contrôleur de domaine

1. Premièrement, on va ouvrir le gestionnaire de serveur puis sélectionner « Gérer » puis « Ajouter des rôles et des fonctionnalités ».
2. On laisse les choix par défaut puis pour l'installation, il faudra sélectionner « AD DS » et « DNS ».
3. Après cela, il faudra sélectionner le drapeau en haut de la fenêtre pour promouvoir ce serveur en domaine de contrôle.
4. On arrive sur une nouvelle fenêtre, on sélectionnera « Ajouter une nouvelle forêt » puis un nom nous sera demandé pour le nom de domaine racine.
5. Ensuite, un mot de passe et un nom de domaine NETBIOS nous sera demandé.
6. On aura ensuite la possibilité de définir les dossiers où seront stockés les fichiers liés à l'Active Directory.
7. Pour finir, il faudra confirmer que les informations entrées sont correctes et on pourra finaliser l'installation.

ETAPE 2 : Configuration du serveur DNS sur Windows 10

La suite de la configuration se fera sur Windows 10 qui devra être dans le même sous-réseau.

1. Il faudra mettre l'adresse IP du Windows server en tant que serveur DNS préféré en effectuant un clic droit sur l'icône réseau puis en sélectionner « Ouvrir le centre réseau et partage ».
2. Après cela, sélectionner « Ethernet » puis propriétés. Il vous suffira ensuite plus qu'à sélectionner « Protocole Internet version 4 » et à mettre l'adresse IP du Windows server en Serveur DNS préféré.

ETAPE 3 : Connexion de Windows 10 au domaine

1. Ensuite, il faudra ouvrir l'explorateur de fichier puis effectuer un clic droit sur « Ce PC » puis sélectionner modifier les paramètres. Sur la nouvelle fenêtre, on sélectionnera « Modifier », on sélectionnera « Domaine » en bas de la page puis on saisira le nom de domaine racine précédemment défini sur le Windows server.
2. Si la configuration a été correctement effectuée, le nom d'utilisateur et le mot de passe du compte administrateur du Windows seront demandés. Une fois connecté, la machine Windows 10 fera partie du domaine créé sur le Windows server.

6.5 RDP

ETAPE 1 : Configuration via l'explorateur de fichier

1. Dans un premier temps il va falloir ouvrir l'explorateur de fichier et effectuer un clic droit sur « Ce Pc » puis sélectionner propriétés.
2. Ensuite il va falloir sélectionner « Paramètres système avancés », on va sélectionner l'onglet « Utilisation à distance » et cocher « Autoriser les connexions à distance à cet ordinateur ».

ETAPE 2 : Configuration avec le pare feu Windows

1. Maintenant on va se rendre sur le pare feu Windows puis sélectionner la section « règles de trafic entrant » puis sélectionner « Nouvelle règle ».
2. Il va falloir sélectionner « Port » étape sélectionnez « TCP » puis on va mettre « 3389 » en Port.
3. Pour la prochaine étape il va falloir laisser « Autoriser la connexion » cocher. Ensuite pour l'étape suivante afin d'empêcher des attaques frauduleuses décocher tout sauf Domaine.
4. Pour finaliser la configuration il ne reste plus qu'à donner un nom à cette règle.

6.6 DHCP

Etape 1 : Prérequis avant l'installation

1. Pour commencer, nous devons configurer la machine virtuelle en utilisant les paramètres adéquats pour son bon fonctionnement. Le plus important de la configuration va être la partie réseau :
2. Il va falloir deux interfaces réseau, la première en accès par pont pour notre réseau étendu WAN, permettant de communiquer avec l'extérieur. En second, notre réseau local LAN, sans utiliser l'accès à internet.

Etape 2 : Installation de pfsense

On peut passer à l'installation de Pfsense en faisant, installation simplifiée, pour les débutants, en choisissant le disque que l'on souhaite.

Etape 3 : Configuration de l'adresse LAN du pfsense

1. On arrive sur l'interface Pfsense, avec plusieurs commandes affectées à des chiffres permettant de configurer notre pfSense.
2. En premier, il faut être bien sûr que le WAN est sur l'interface réseau en accès par pont et le LAN sur l'interface en réseau interne.
3. On configure le réseau local LAN en entrant son adresse IP choisie, la mise en place d'un réseau LAN IPV6 n'est pas nécessaire.

Etape 4 : Configuration du serveur DHCP

1. Ensuite, lors de la mise en place d'adresse LAN et WAN, il est demandé si vous voulez activer le serveur DHCP en LAN, vous devez taper Y.
2. Vous devez taper le début de la rangée d'adresse IP que vous voulez et taper la fin de rangées d'adresses IP, puis valider. Le pfSense fera les changements et les machines configurées en DHCP sur le réseau auront une adresse IP assignée au serveur DHCP.

6.7 Configuration du portail captif

Etape 1 : Accès à l'interface web de pf sense

1. Pour commencer la configuration il faut accéder à l'interface pfSense sur son navigateur en tapant l'adresse IP LAN du pfSense donc 20.0.0.254 dans cet exemple.
2. Le navigateur affiche un problème de sécurité, il faut accepter le risque et poursuivre. On accède au dashboard de pfSense en ayant entré les informations de connexions admin et pfsense pour le mot de passe.

Etape 2 : Configuration du portail captif

1. Nous pouvons passer à la mise en place d'un portail captif, Dans la section services/Portail Captif/LAN/Configuration, on choisit l'interface LAN et la méthode d'authentification « Use an authentication backend ».
2. Maintenant on peut créer notre utilisateur du portail captif avec les paramètres que l'on souhaite. Lorsque que l'utilisateur sera sur la page de connexion pfsense, il rentrera ses identifiants et il sera connecté. Le portail captif est en place, avec un utilisateur créé, la mise en place est donc terminée.

6.8 TrueNas Core

Etape 1 : Prérequis avant l'installation de TrueNas

Pour commencer, il faut configurer la machine virtuelle TrueNas Core avec une carte réseau en réseau interne, c'est très important.

Etape 2 : Installation de TrueNas

1. On peut lancer TrueNas Core, on arrive sur l'interface d'installation de TrueNas, on choisit le disque d'installation. On choisit le boot via BIOS, on ne crée pas de partition swap dans ce cas-là
2. L'installation se poursuit, on redémarre la machine virtuelle, ensuite s'affiche l'interface TrueNas. On peut changer le root password et ensuite dans la machine virtuelle windows on rentre l'adresse du TrueNas dans le navigateur et on arrive sur l'interface de connexion.

Etape 3 : Configuration du TrueNas

1. Dans l'onglet Network/Interface, on désactive le DHCP, on rentre une adresse statique puis cliquer sur valider.
2. Maintenant nous aller créer l'espace de stockage des fichiers en cliquant sur Storage/Pools sur le menu TrueNas. On ajoute les deux disques, dans ce cas-ci, ils seront en miroir. Cliquer sur valider et sauvegarder.
3. Maintenant, il faut partager ce stockage, dans la rubrique Sharing/Windows Share (SMB).

Etape 4 : Configuration d'un utilisateur pour le partage réseau TrueNAS

1. La prochaine étape consistera à créer un utilisateur autorisé à se connecter au partage réseau du TrueNAS.
2. Une fois cette étape accomplie, l'utilisateur pourra accéder à TrueNAS en entrant l'adresse IP, par exemple 20.0.0.12, dans son navigateur.
3. Ensuite, il lui suffira d'entrer les informations de connexion de l'utilisateur créé dans TrueNAS Core pour accéder au partage réseau.

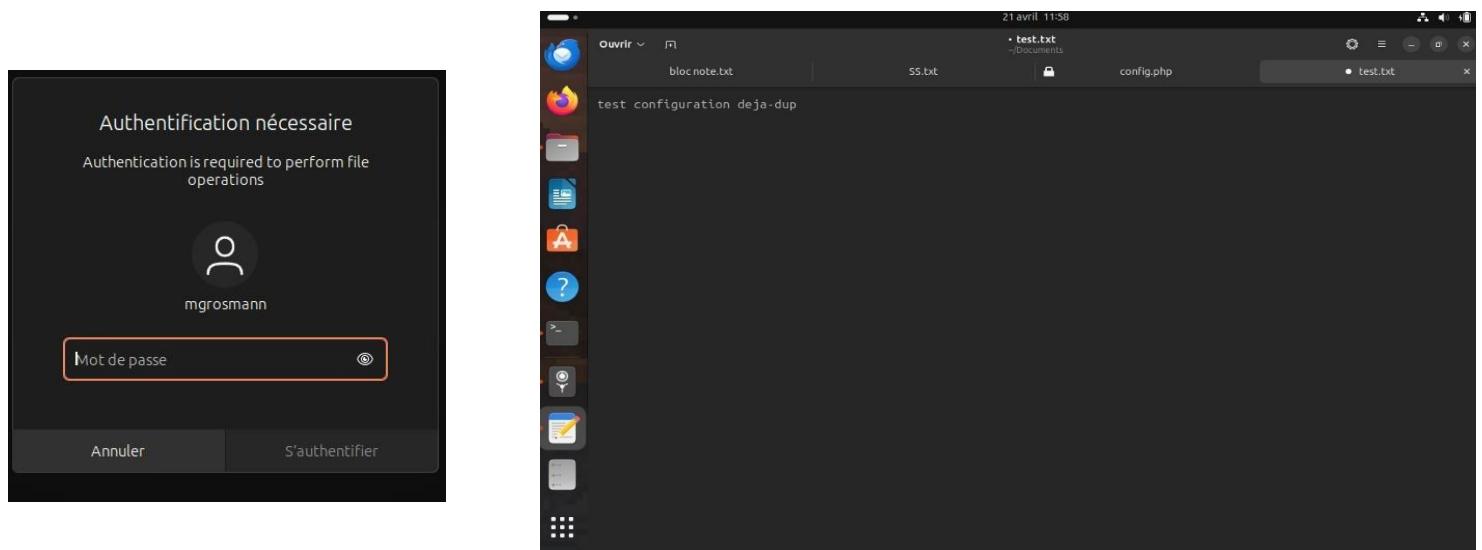
7. Jeu de tests :

7.1 DEJA-DUP :

Pour commencer le test on va créer un fichier « test.txt » il faudra remplacer « mgrosmann » par votre nom d'utilisateur

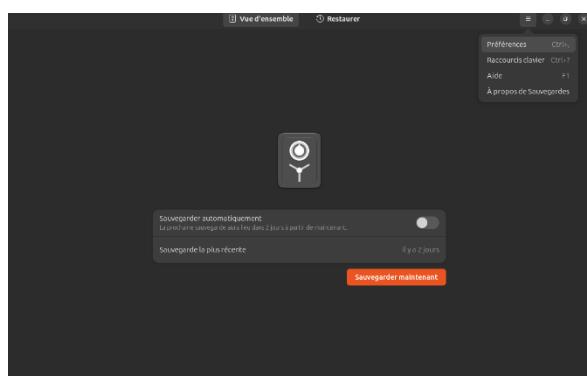
```
root@mgrosmann-pc:~# cd /home/mgrosmann/Documents
root@mgrosmann-pc:/home/mgrosmann/Documents# touch test.txt
```

On va éditer le fichier, cela nécessitera le mot de passe de l'administrateur :

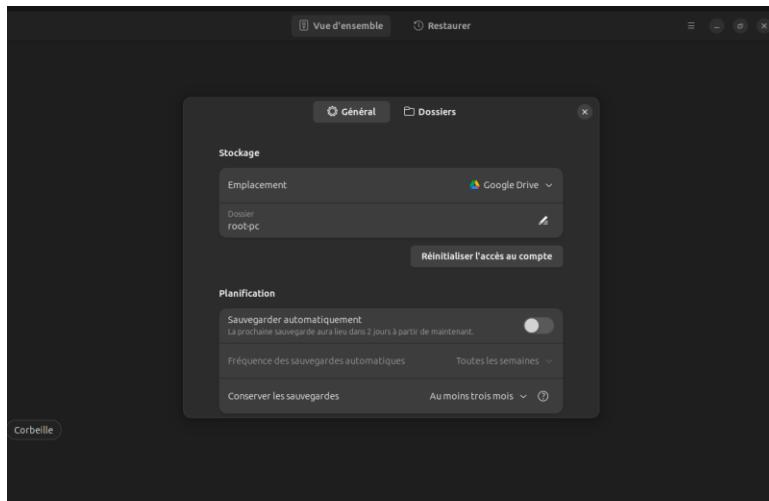


Lançons DEJA-DUP et avant de sauvegarder il y a des configurations à effectuer.

Sélectionner les 3 petits points puis « préférences »

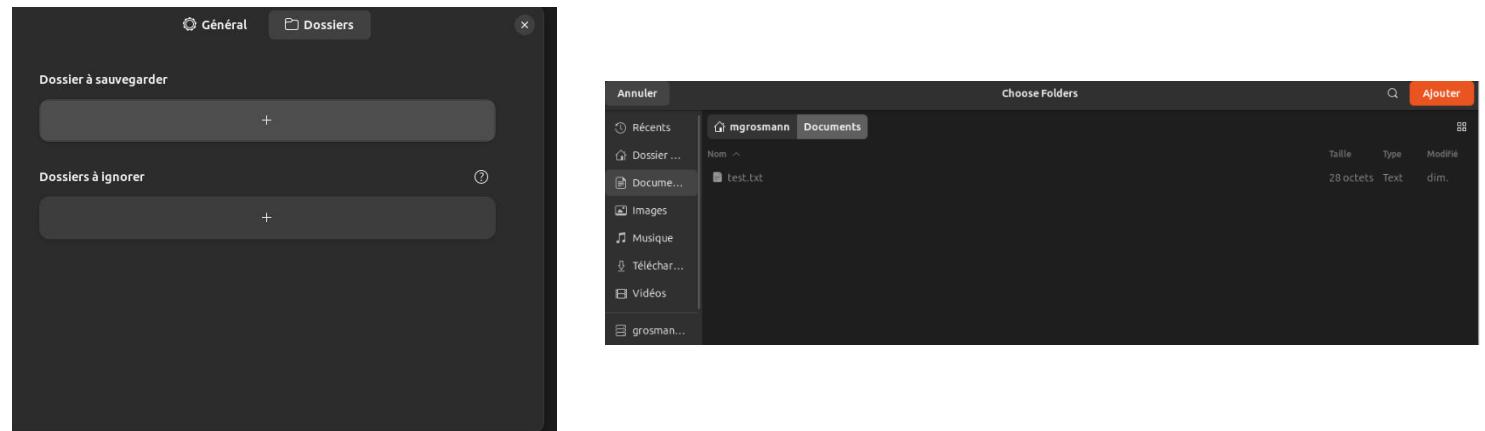


On tombe sur un menu où on peut voir le moyen utilisé pour stocker notre archive. On sélectionnera « Dossier » en haut de la page afin de définir le dossier à restaurer.

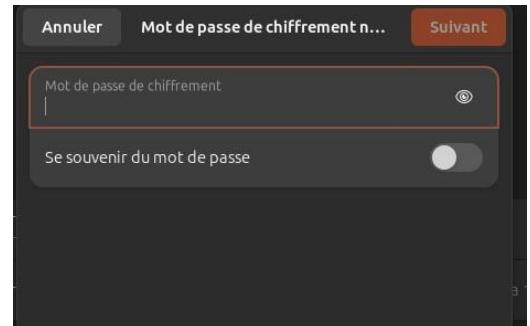
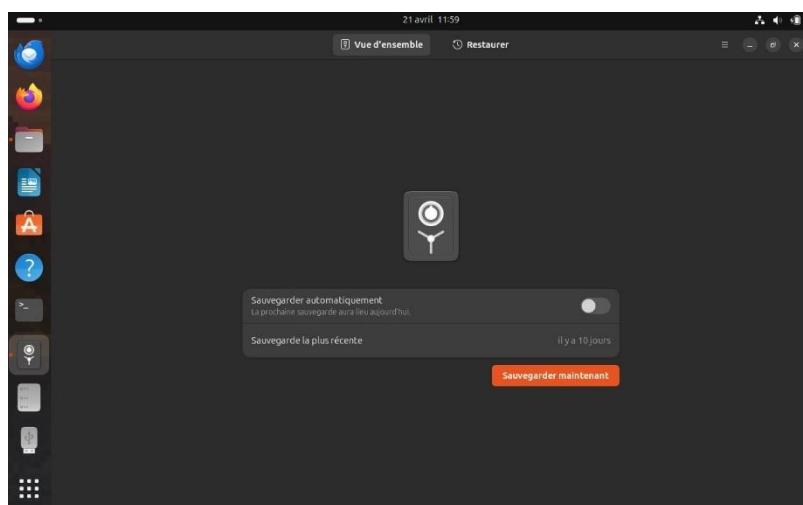


Une fois que nous sommes dans la section « Dossier » on appuie sur + dans la partie « dossier à sauvegarder » afin d'ajouter le dossier Documents.

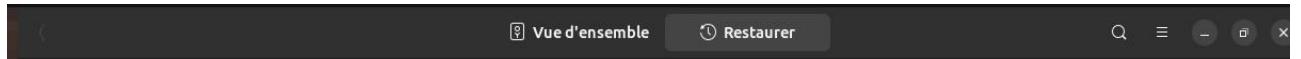
On sélectionne ensuite le dossier Documents puis on sélectionne Ajouter.



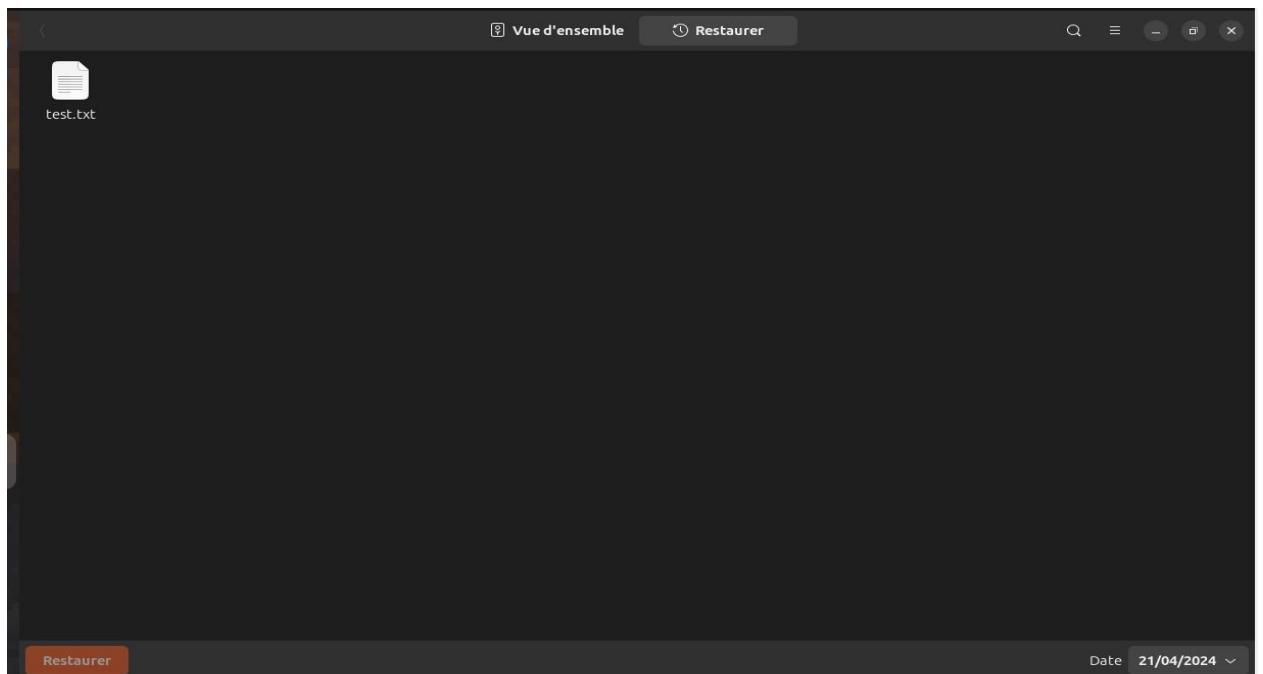
Après cela on sélectionne « sauvegarder maintenant », si vous avez sélectionné cette option un mot de passe vous sera demandé



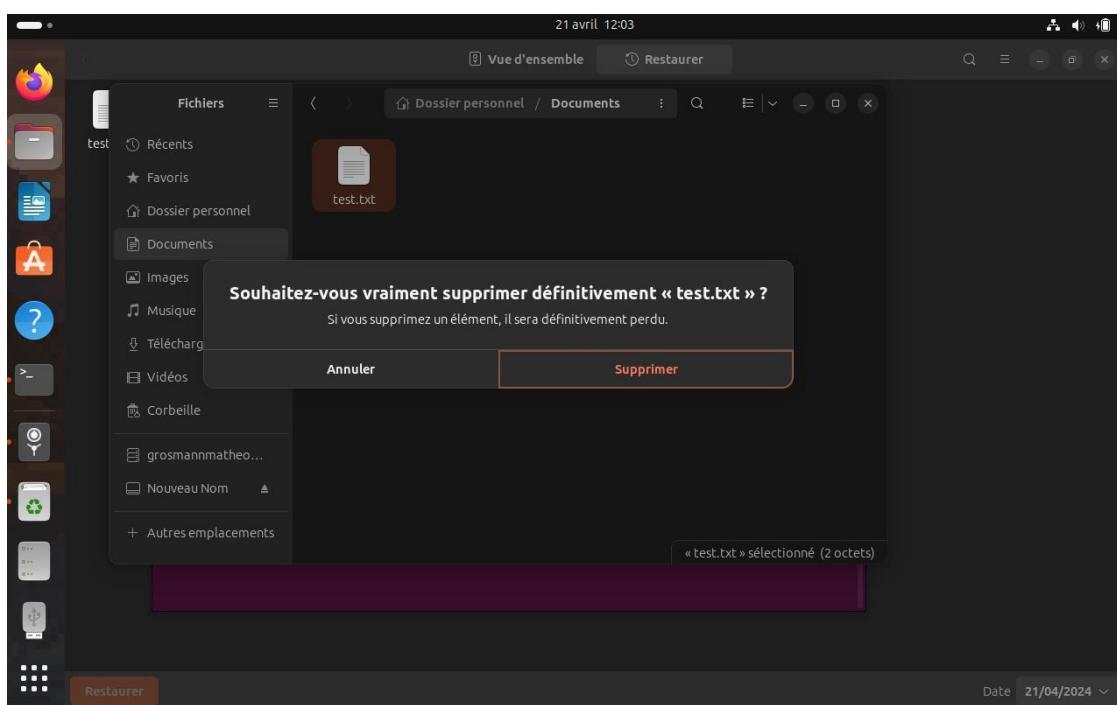
Sur la barre du haut sélectionner restaurer :



Vous pourrez voir le fichier test.txt contenu dans le dossier Documents qu'on a choisi pour la sauvegarde.

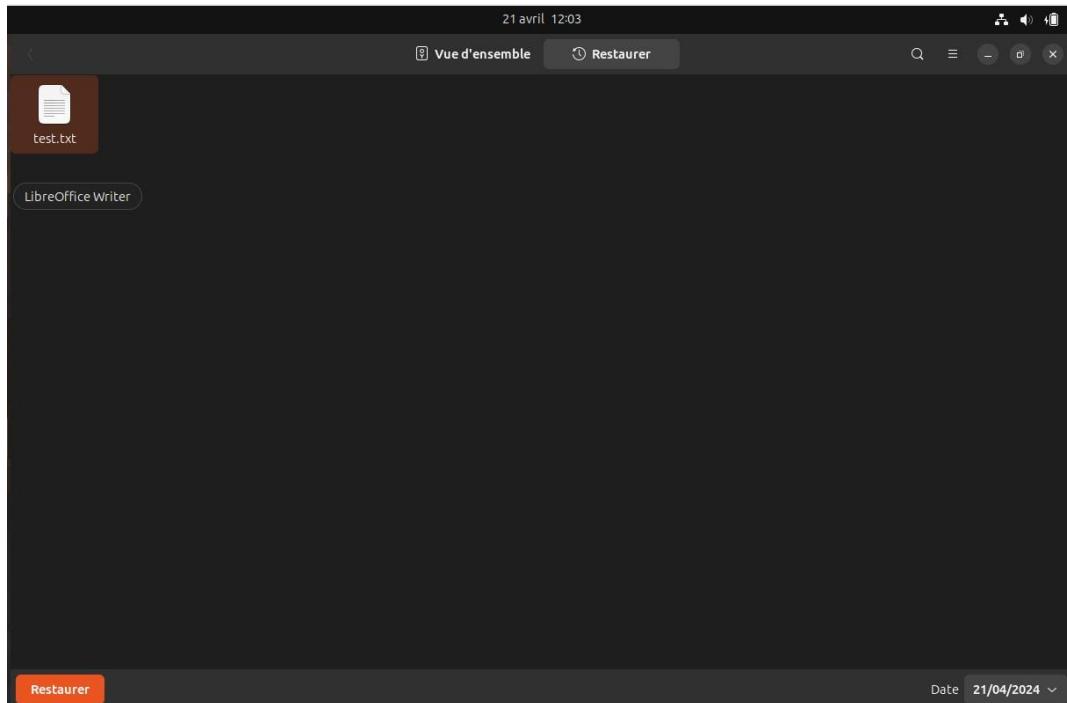


Pour vérifier que la configuration de DEJA-DUP on va supprimer le fichier test.txt

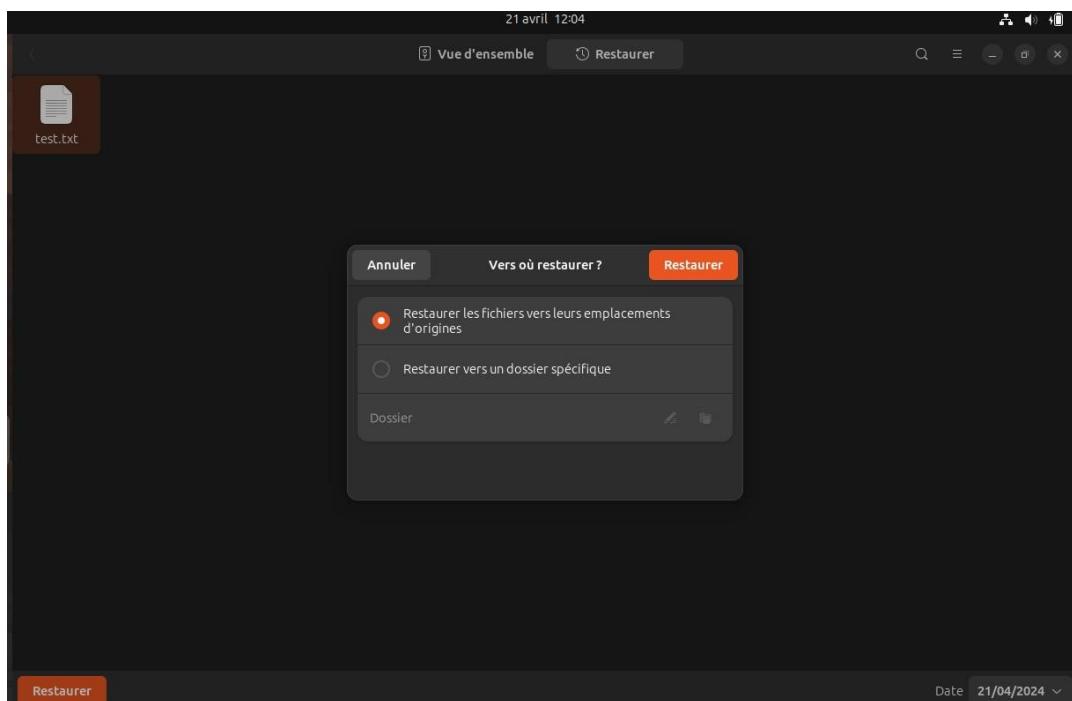


Le dossier Documents maintenant vide procérons à la restauration.

On va sélectionner le fichier « test.txt » et ensuite sélectionner « Restaurer »



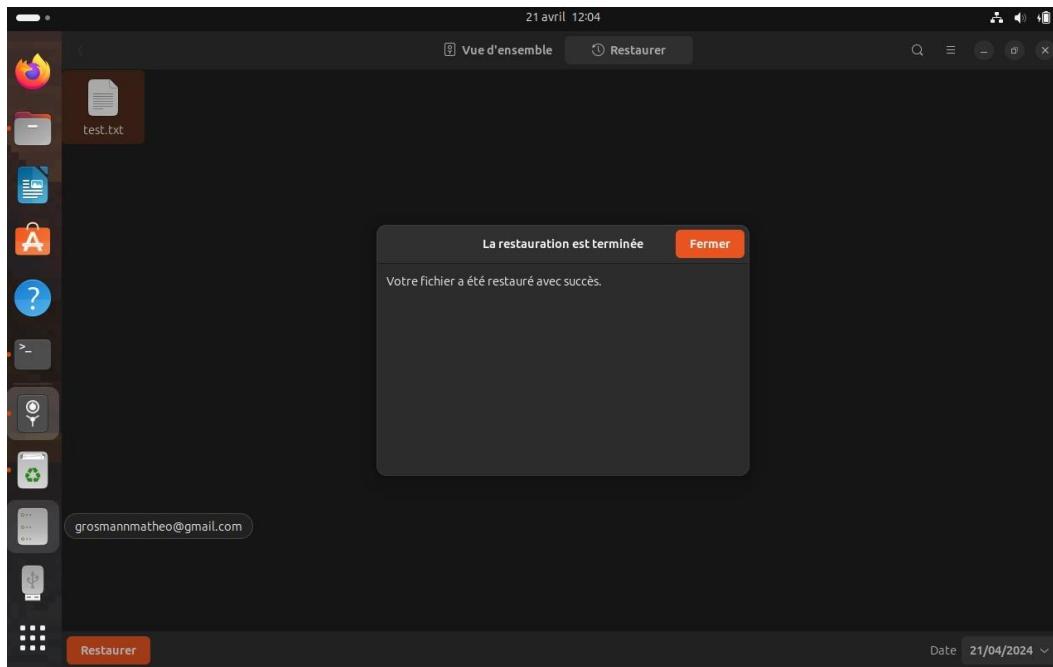
On a le choix entre restaurer dans le dossier d'origine (ici Documents) ou dans un dossier spécifique (dossier pour les backups), on fera le choix de restaurer dans le dossier d'origine.



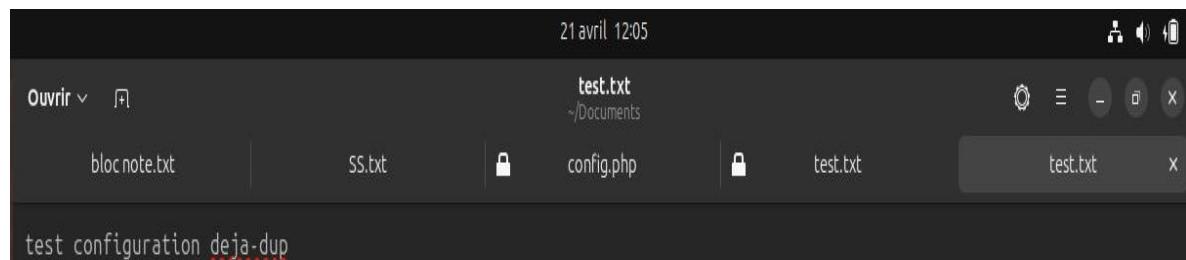
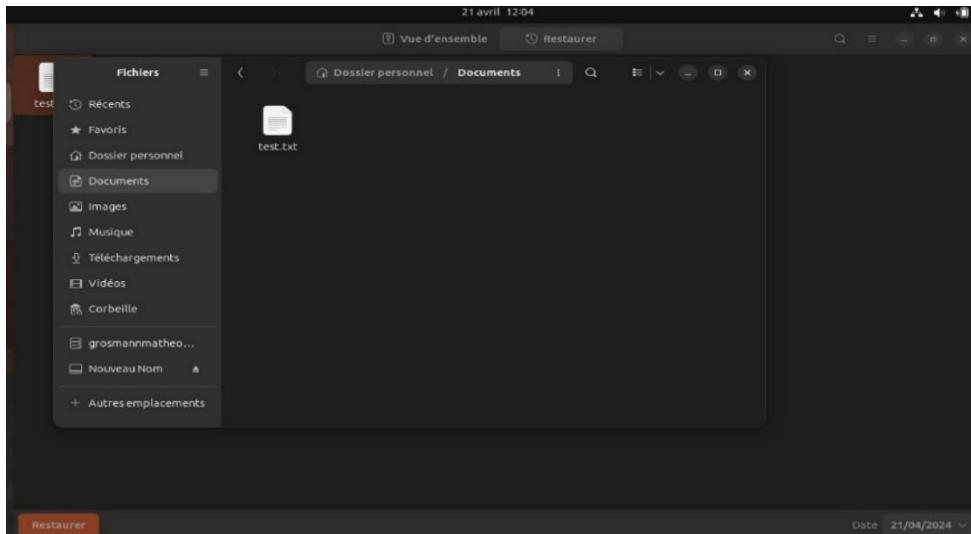
Le mot de passe de chiffrement sera demandé :



Lorsque la restauration aura été finalisé un message s'affiche :



On va dans le dossier Documents et on constate que le fichier « test.txt » est Restauré ainsi que son contenu.



7.2 Postfix :

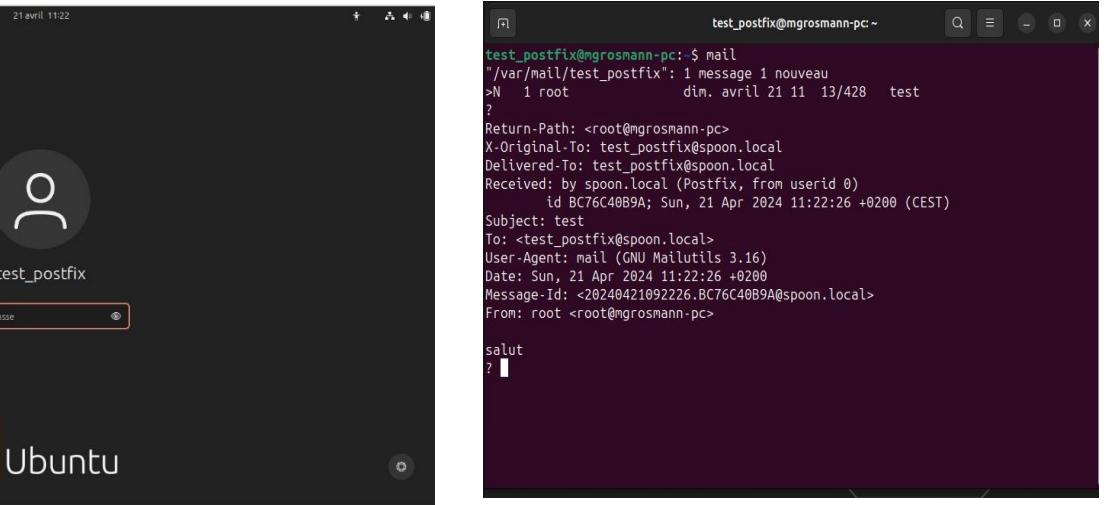
Pour tester la configuration de postfix on va créer un utilisateur pour cette essai avec la commande suivante :

```
root@mgrosmann-pc:~# sudo adduser test_postfix
```

On va ensuite lui envoyer un mail avec la commande suivante :

```
root@mgrosmann-pc:~# echo "salut" | mail -s "test" test_postfix@spoon.local
```

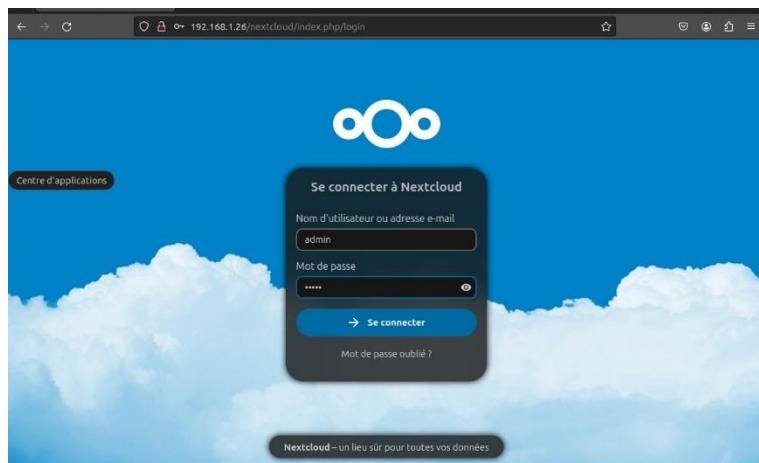
On se connecte ensuite sur « test_postfix » et on exerce la commande « mail » pour voir les mails reçus :



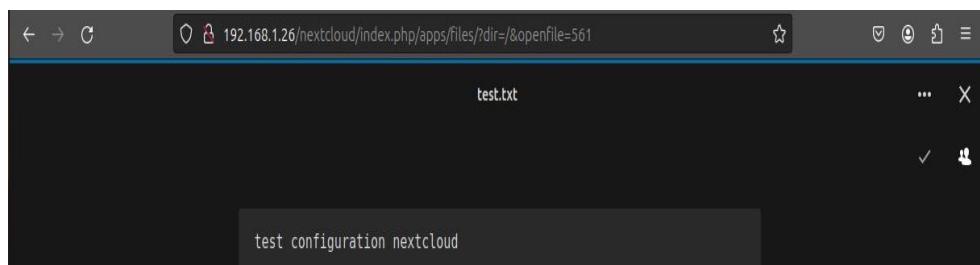
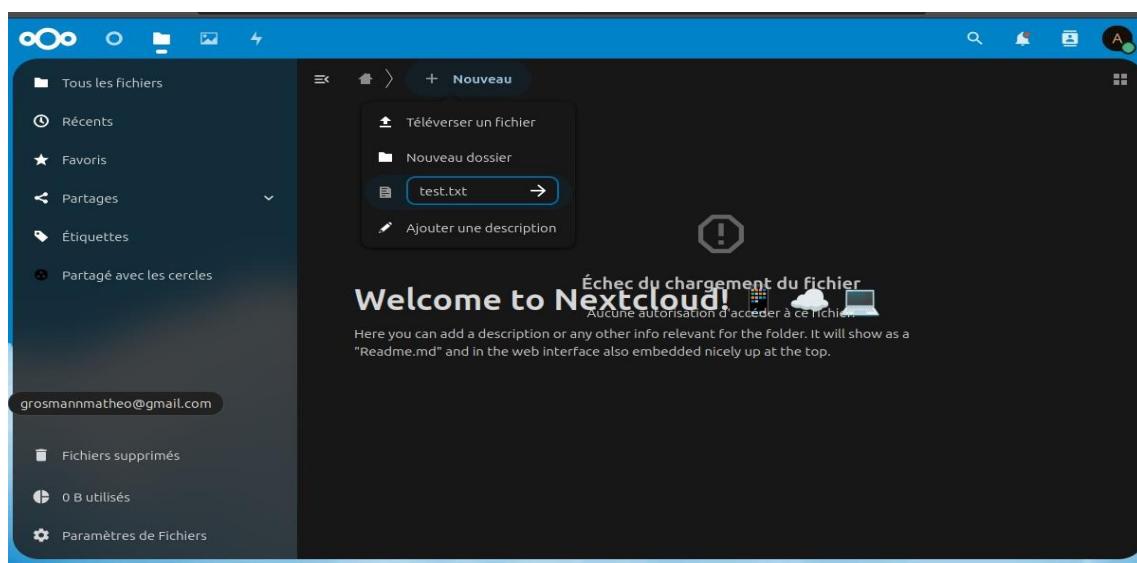
7.3 Nextcloud :

Pour ce test on va créer un fichier test.txt sur une machine ubuntu sur nextcloud

Premièrement on se connecte :



On crée et édite le fichier test.txt :

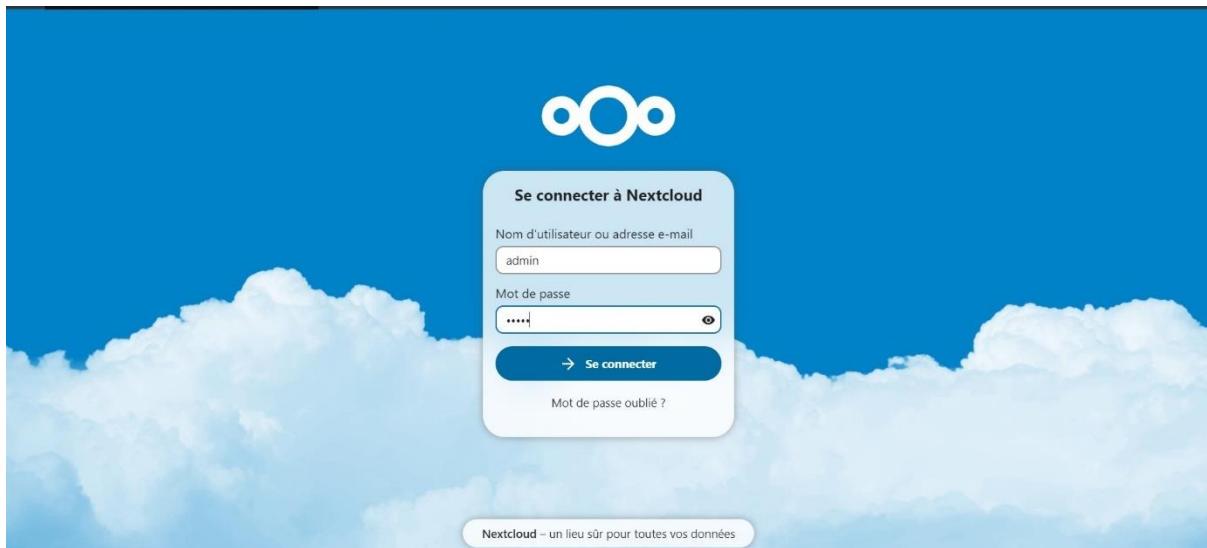


Ensuite on va se connecter sur nextcloud avec le même compte mais sur une machine windows :

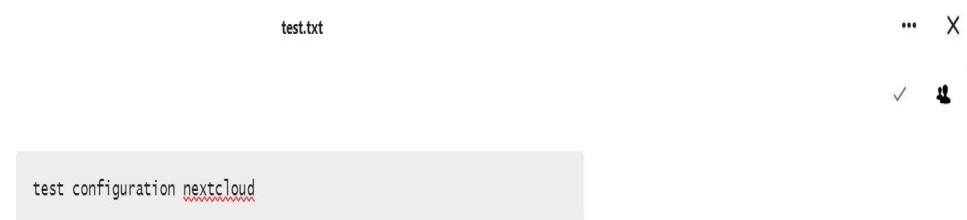
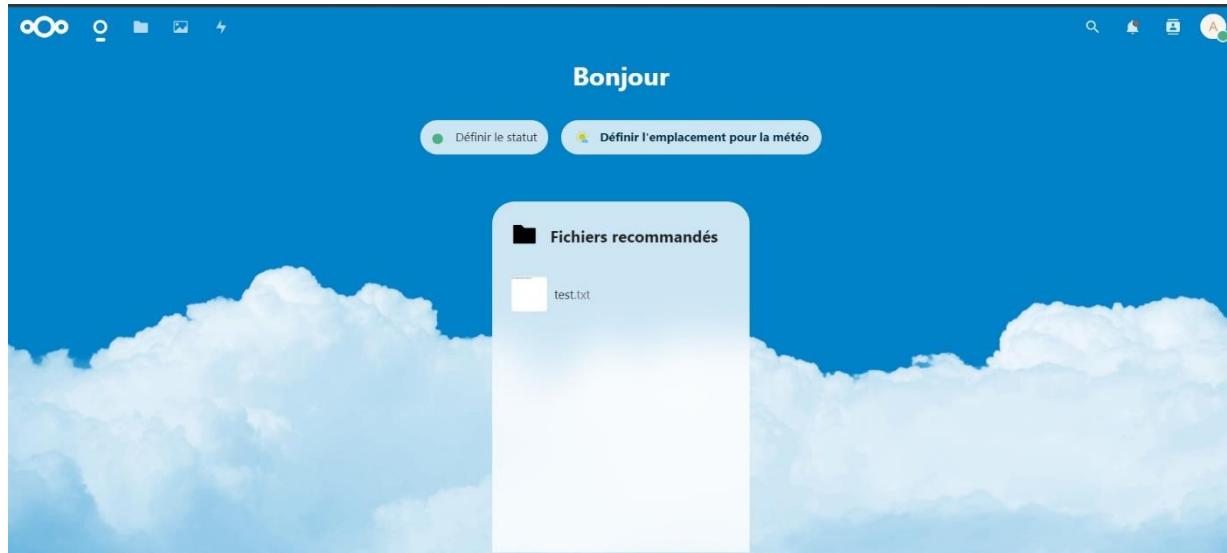
Il avant tout s'assurer que dans le fichier config.php dans la zone « trusted_domains » on ait ajouté l'adresse ip des machines (la machine windows dans l'exemple) à qui on autorise l'accès au cloud local Nextcloud.

Vous pouvez l'éditez afin d'y ajouter l'adresse ip des machines que vous souhaitez autoriser l'accès grâce à la commande : « sudo nano /var/www/nextcloud/config/config.php »

```
GNU nano 7.2          /var/www/nextcloud/config/config.php *
<?php
$CONFIG = array (
    'instanceid' => 'ocp0ravrbwvp',
    'passwordsalt' => 'ipKtuFrOF0lOXAWYNW1erzkbDdmsvE',
    'secret' => 'nzyMNPwLxNg92KGW/2IHtSygLrGPtRbnjF35h1iIGdQHhWS0',
    'trusted_domains' =>
        array (
            0 => '192.168.1.88',
            1 => '192.168.1.26',
        ),
    'datadirectory' => '/var/www/nextcloud/data',
    'dbtype' => 'mysql',
    'version' => '27.1.7.2',
    'overwrite.cli.url' => 'http://192.168.2.163/nextcloud',
    'dbname' => 'cloud_local',
    'dbhost' => 'localhost',
    'dbport' => '',
    'dbtableprefix' => 'oc_',
    'mysql.utf8mb4' => true,
    'dbuser' => 'oc_admin',
)
Sauver l'espace modifié ?
O Oui       Annuler
N Non
```



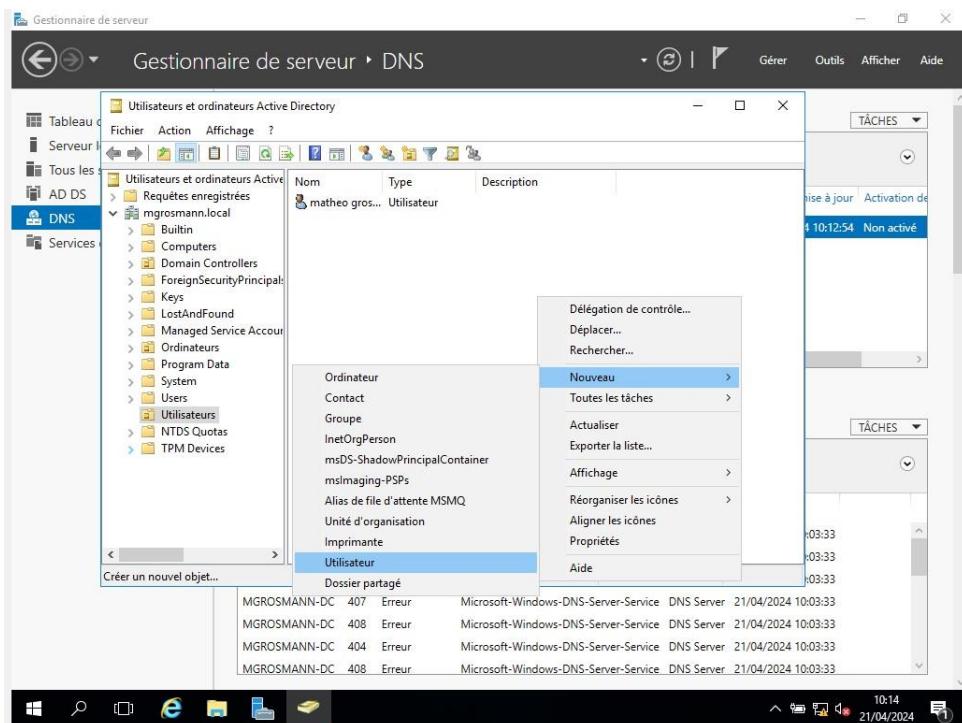
Sur la page d'accueil on peut voir le fichier « test.txt » et si on l'ouvre on peut même accéder à son contenu.



7.4 Active Directory :

Afin de vérifier que l'Active Directory nous allons créer un utilisateur et tenter de se connecter à son compte sur windows 10

Pour se faire on va ouvrir la fenêtre « Utilisateurs et ordinateurs Active Directory » puis on va effectuer un clic droit, Nouveau puis sélectionner Utilisateur



On le nommera « test »

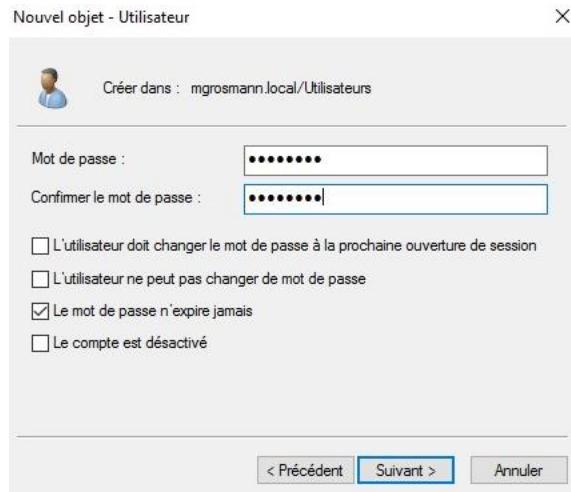
Nouvel objet - Utilisateur

Créer dans : mgrosmann.local/Utilisateurs

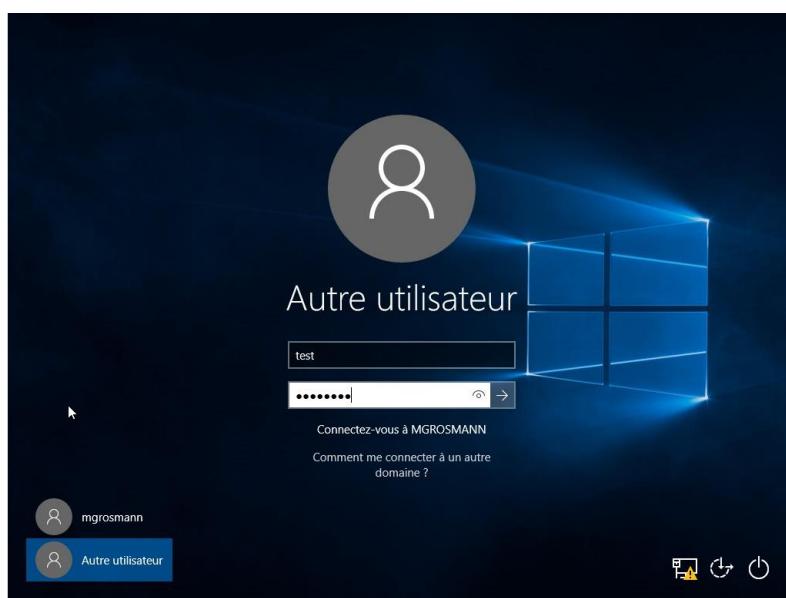
Prénom :	t	Initiales :	
Nom :	est		
Nom complet :	t est		
Nom d'ouverture de session de l'utilisateur :			
test		@mgrosmann.local	▼
Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :			
MGROSMANN\		test	

< Précédent Suivant > Annuler

On entre un mot de passe et on coche la case « le mot de passe n'expire jamais » puisqu'il s'agit d'un test même si pour des raisons de sécurité il vaudrait mieux cocher la case « L'utilisateur doit changer le mot de passe à la prochaine ouverture de session »



On bascule sur la machine windows 10 et on entre l'identifiant et le mot de passe pour vérifier que l'Active Directory est correctement configuré

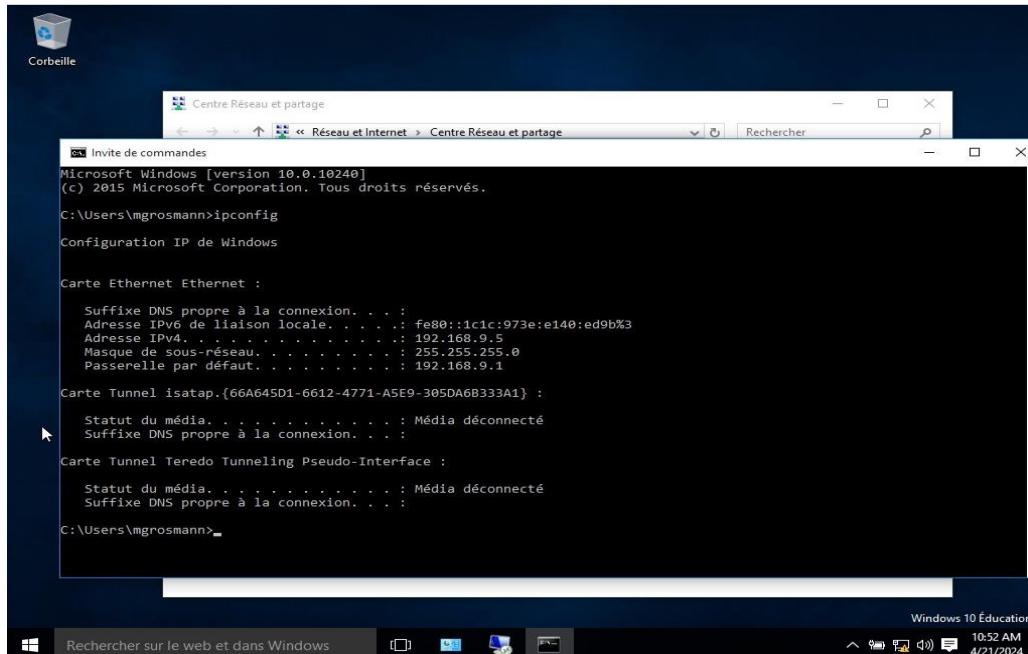


Connexion réussi avec le compte créé sur l'Active Directory

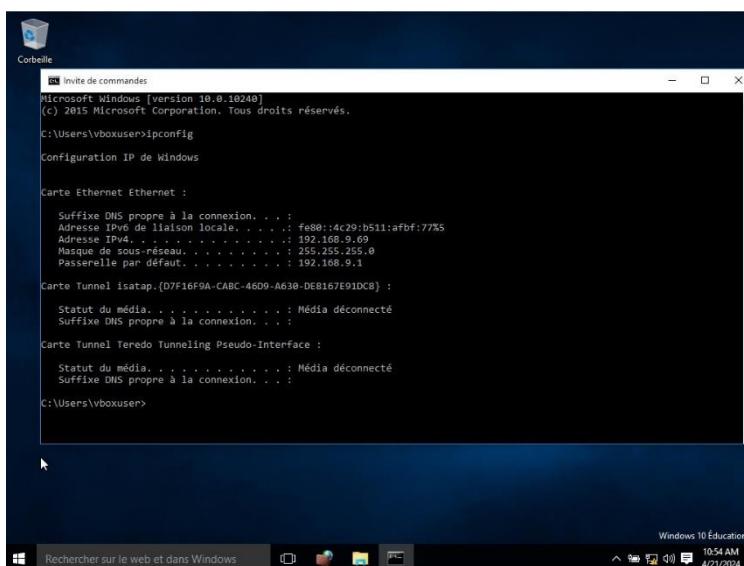
7.5 Connexion RDP

Pour vérifier la connexion RDP on va effectuer une connexion à distance entre deux machine windows 10 qui sont situés dans le même réseau :

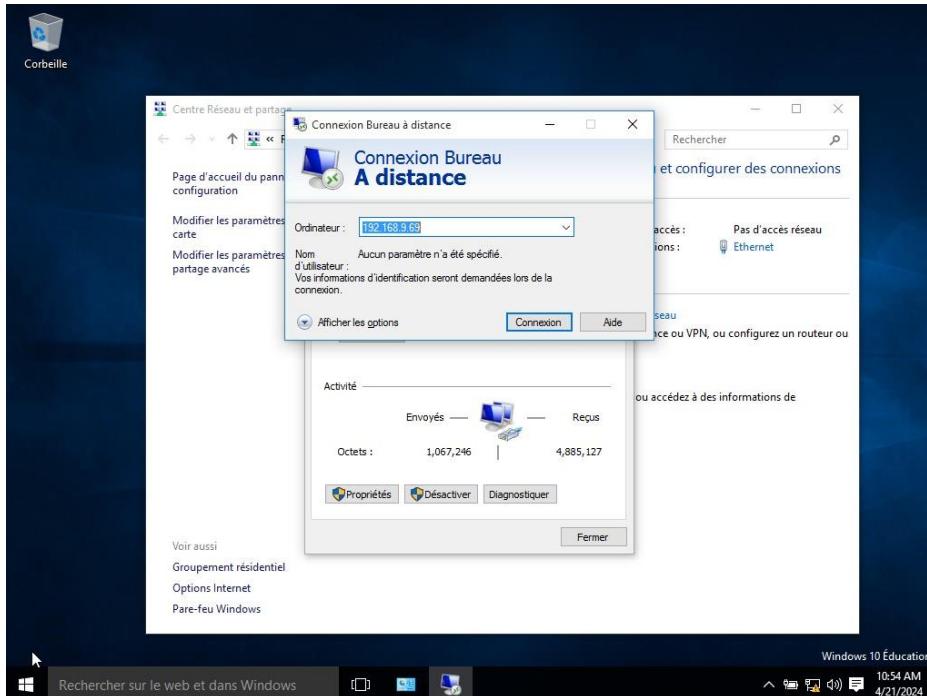
Une machine windows 10 ayant pour adresse IP « 192.168.9.5 » qui sera la machine cliente



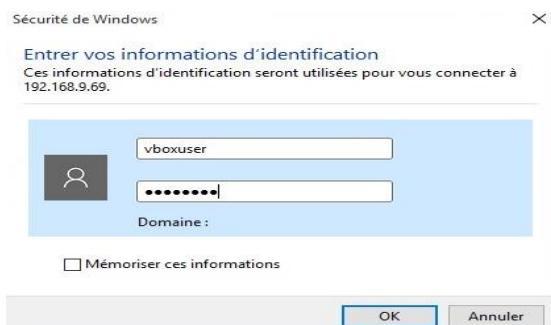
Une machine Windows 10 ayant pour adresse IP « 192.168.9.69 » qui sera la machine cible et qui a été configuré pour pouvoir être contrôlé à distance.



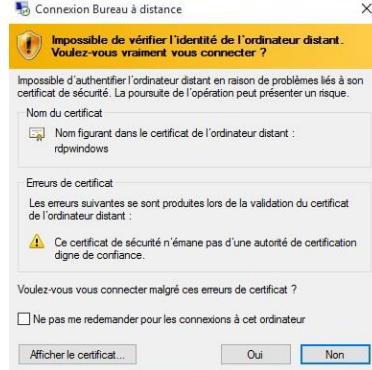
Sur la machine cliente on lance le logiciel rdp et on indique l'adresse ip de la machine cible dans la zone « Ordinateur »



On entre l'identifiant et le mot de passe du compte de la machine cible



Avant la connexion nous avons un message d'avertissement qui demande une confirmation de notre part



Après avoir sélectionné oui nous voilà maintenant connecter à distance sur la machine cible depuis la machine cliente

```
Corbeille
Invite de commandes
Microsoft Windows [Version 10.0.19360]
(c) 2015 Microsoft Corporation. Tous droits réservés.

C:\Users\vboxuser>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :
    Suffixe DNS propre à la connexion. . . . . : 
    Adresse IPv6 de liaison locale. . . . . : fe80::4c29:b511:afb7:7785
    Adresse IPv4. . . . . : 192.168.9.69
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . : 192.168.9.1

Carte Tunnel Istanap (DF710F9A-CABC-4B09-A630-0E8107E91DC8) :
    Statut du média. . . . . : Média déconnecté
    Suffixe DNS propre à la connexion. . . . . : 

Carte Tunnel Teredo Tunneling Pseudo-Interface :
    Statut du média. . . . . : Média déconnecté

C:\Users\vboxuser>
```

7.6 Serveur DHCP

Pour vérifier que le serveur DHCP fonctionne correctement on va changer le sous réseau de l'adresse IP LAN du pf sense et on va entrer une nouvelle plage d'adresses IP.

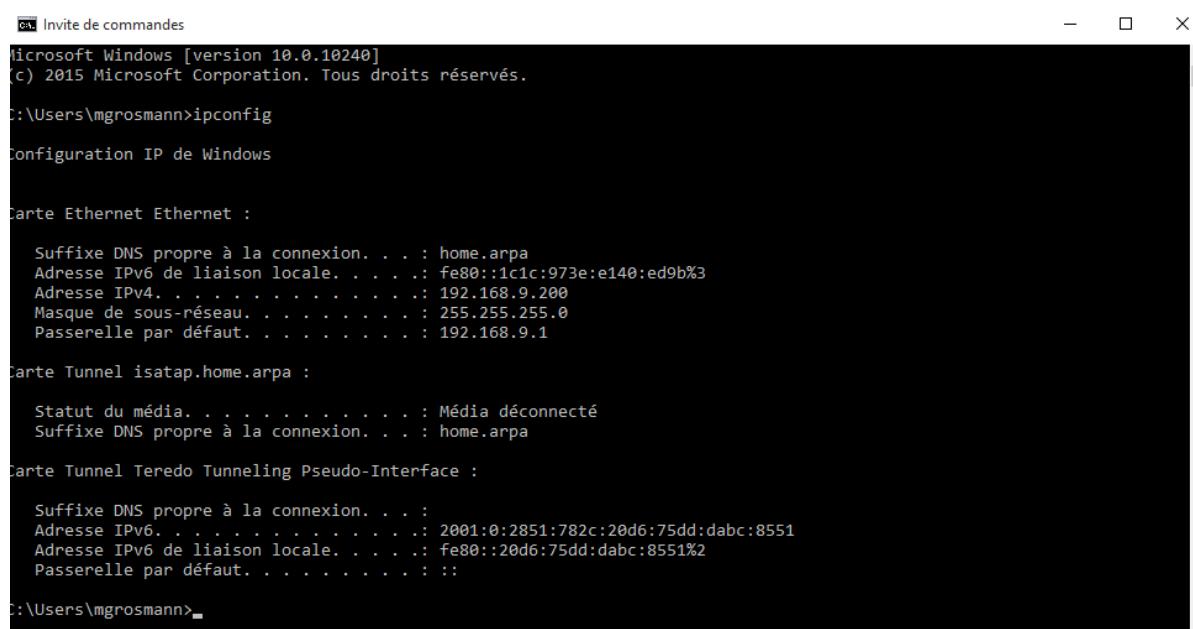
La nouvelle adresse IP LAN sera « 192.168.9.1 »

```
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 192.168.9.1
```

La nouvelle plage d'adresses IP ira de « 192.168.9.200 » à « 192.168.9.210 »

```
Do you want to enable the DHCP server on LAN? (y/n) y  
Enter the start address of the IPv4 client address range: 192.168.9.200  
Enter the end address of the IPv4 client address range: 192.168.9.210
```

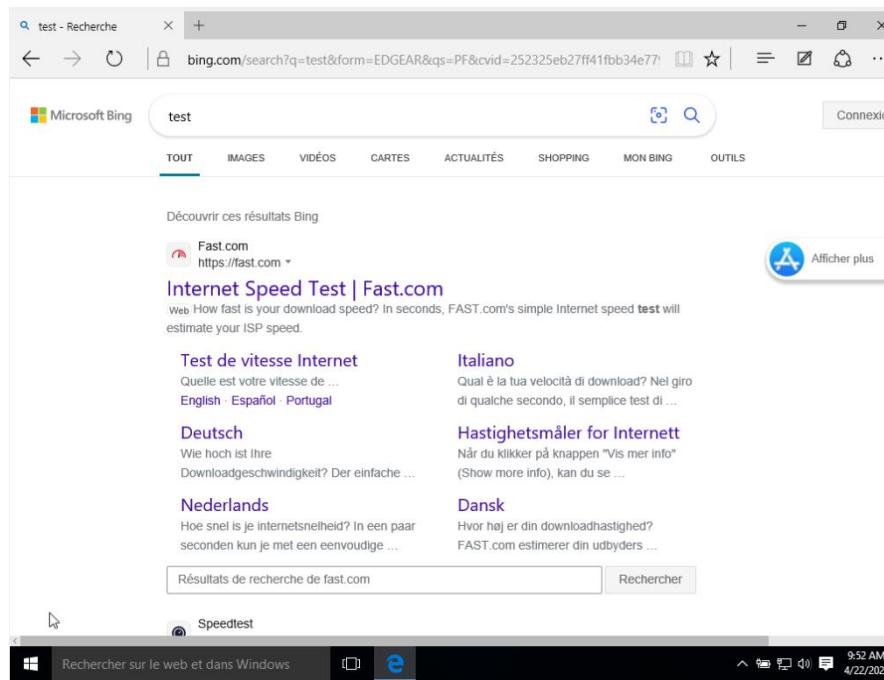
Lançant maintenant la machine Windows 10 et vérifiant la configuration IP grâce à la commande « ipconfig » sur l'invite de commande.



```
C:\ Invité de commandes  
Microsoft Windows [version 10.0.10240]  
(c) 2015 Microsoft Corporation. Tous droits réservés.  
C:\Users\mgrosmann>ipconfig  
Configuration IP de Windows  
  
Carte Ethernet Ethernet :  
  
    Suffixe DNS propre à la connexion... : home.arpa  
    Adresse IPv6 de liaison locale... : fe80::1c1c:973e:e140:ed9b%3  
    Adresse IPv4... : 192.168.9.200  
    Masque de sous-réseau... : 255.255.255.0  
    Passerelle par défaut... : 192.168.9.1  
  
Carte Tunnel isatap.home.arpa :  
  
    Statut du média... : Média déconnecté  
    Suffixe DNS propre à la connexion... : home.arpa  
  
Carte Tunnel Teredo Tunneling Pseudo-Interface :  
  
    Suffixe DNS propre à la connexion... :  
    Adresse IPv6... : 2001:0:2851:782c:20d6:75dd:dabc:8551  
    Adresse IPv6 de liaison locale... : fe80::20d6:75dd:dabc:8551%2  
    Passerelle par défaut... :  
C:\Users\mgrosmann>
```

Le serveur DHCP a correctement affecté automatiquement la configuration en attribuant « 192.168.9.200 » comme adresse IP soit une adresse IP compris dans la plage d'adresse IP disponible en ayant automatiquement mis l'adresse LAN du pf sense « 192.168.9.1 » en passerelle par défaut.

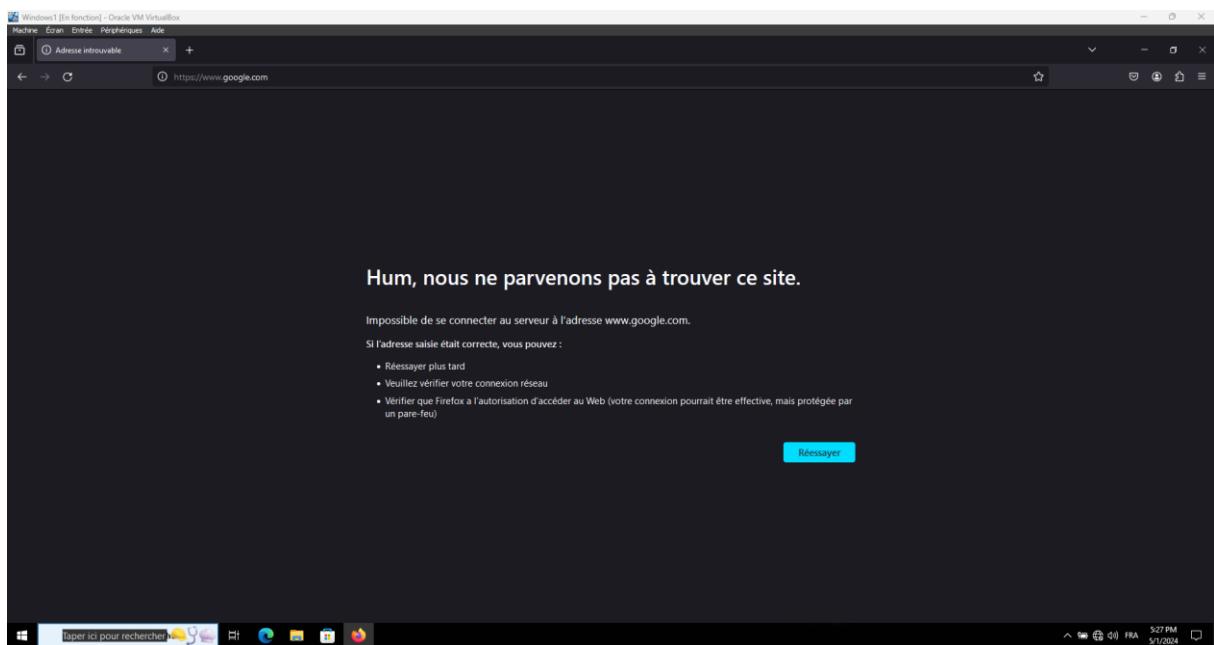
Maintenant vérifions la connexion au réseau.



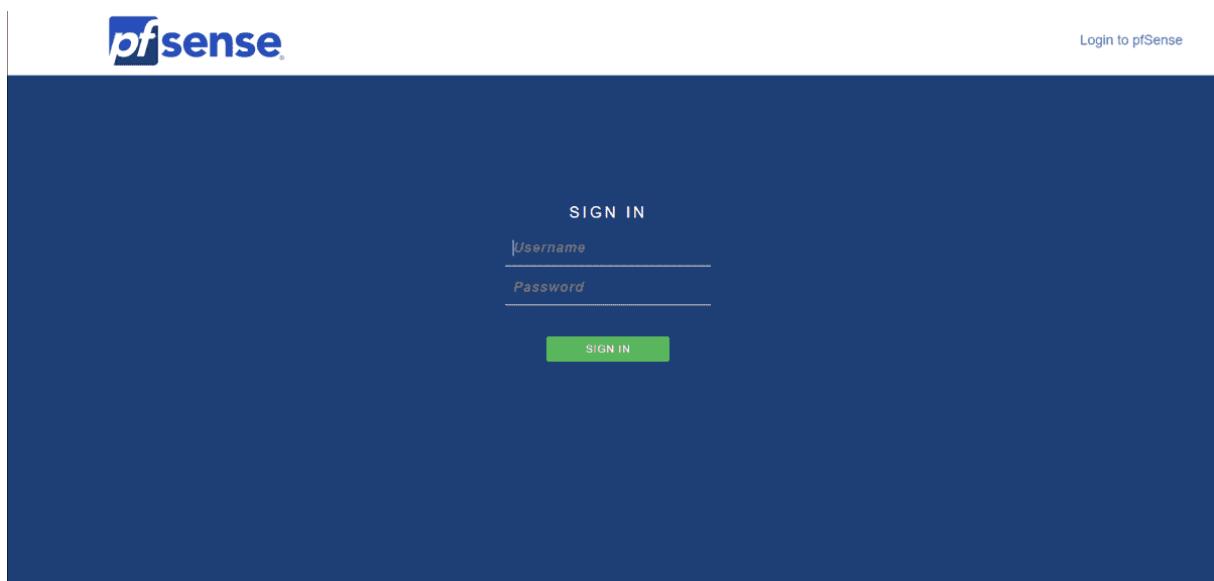
On peut bien effectuer une recherche internet, la serveur DHCP fonctionne correctement.

7.7 Portail Captif

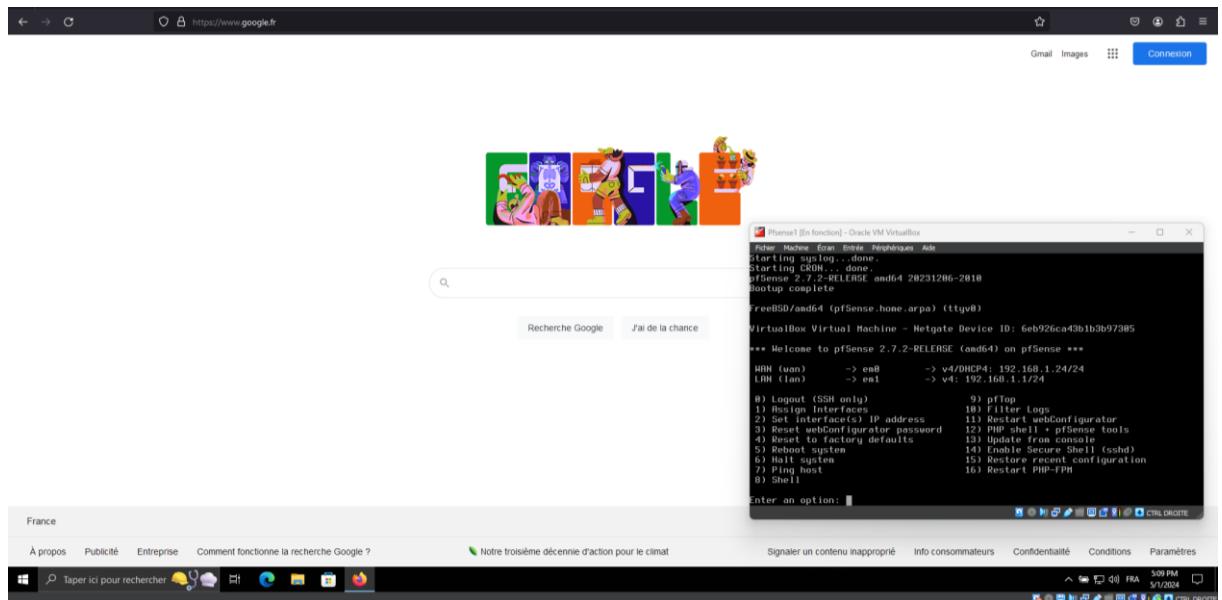
Pour tester si notre pfSense marche, on fait une recherche sur internet quand le pfSense est éteint, on voie que la machine windows n'a pas accès à internet.



On arrive sur la page de connexion du pfsense. On se connecte avec l'identifiant « thomas » précédemment créer.

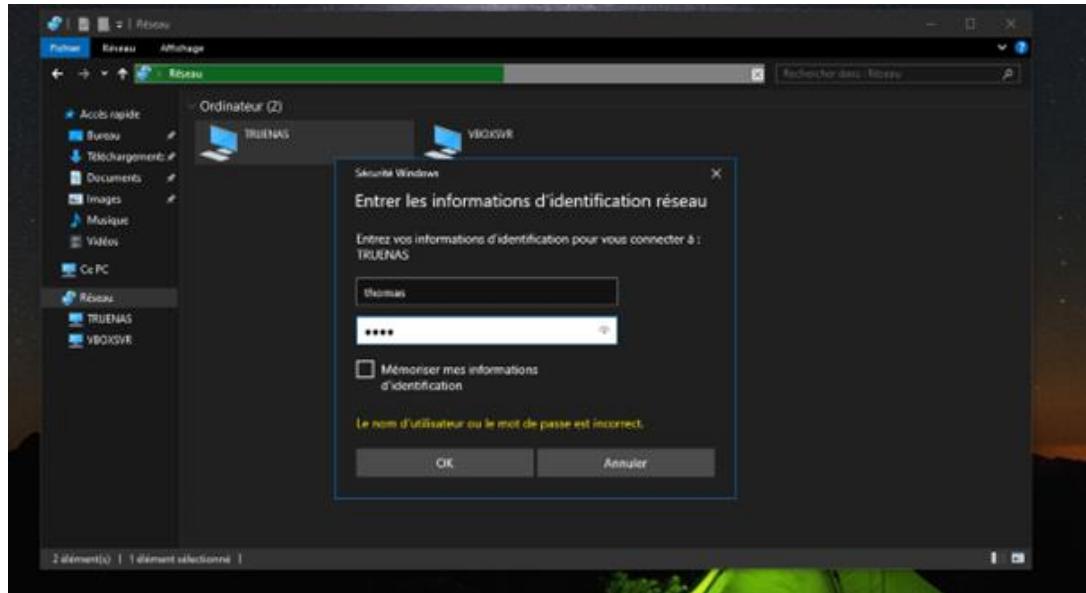


Quand le pfSense est allumé, la machine windows accède à internet, le pfSense est donc opérationnel

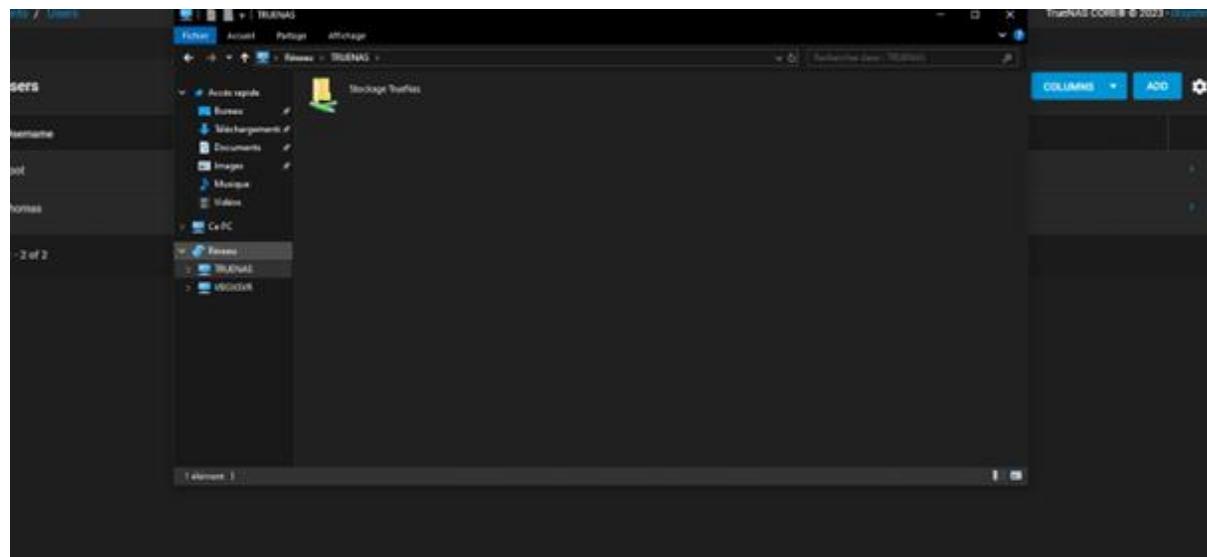


7.8 TrueNAS

Après avoir configurer notre truenas, on peut tester s'il marche, nous allons nous connecter avec l'utilisateur thomas pour le test :



Après avoir rentré l'adresse ip du truenas, il apparait et il faut rentre les identifiants d'un utilisateur, dans cet exemple, ceux de l'utilisateur thomas.



On voit maintenant que l'utilisateur à bien accès au stockage de Truenas.

8. Manuel technique :

8.1 Installation du logiciel de système de sauvegarde : DEJA DUP

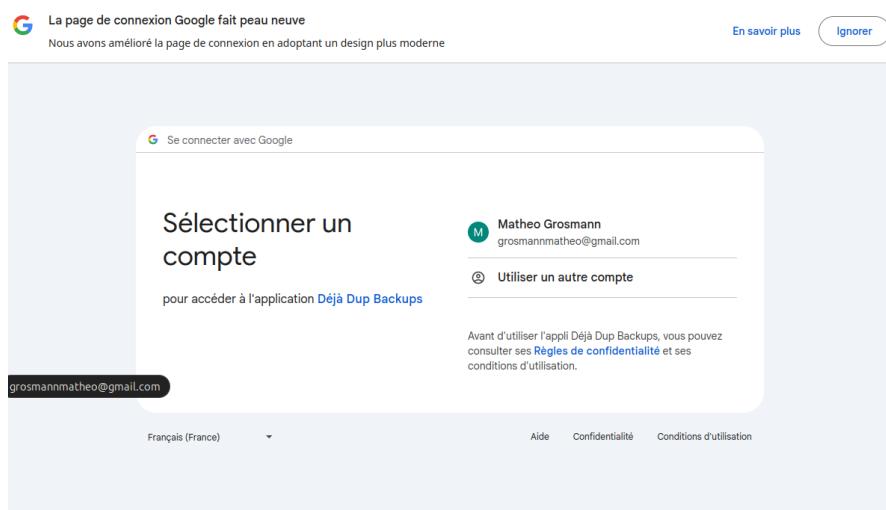
Il faut commencer par mettre à jour la liste des paquets disponibles avec :

```
root@mgrosmann-pc:~# sudo apt update
```

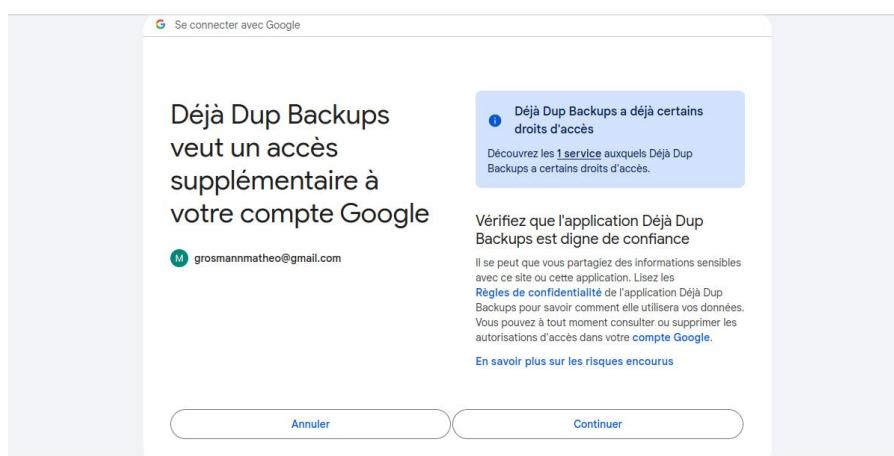
Ensuite on peut commencer à l'installer sur le terminal sur ubuntu:

```
root@mgrosmann-pc:~# sudo apt install deja-dup
```

Ensute on lance deja-dup on se connecte afin de pouvoir stocker notre archive:



Nous avons ici fait le choix d'utiliser google pour stocker notre archive.



Par la suite il faut autoriser certain les accès dont deja-dup a besoin.

Ensuite on nous demandera si on veut demander un mot de passe pour l'archive, pour la sécurisation des données il est préférable d'autoriser et d'entrer un mot de passe qui sera demandé pour ouvrir l'archive.



Suite à cela l'archive sera sur votre drive et vous serez en capacité à la restaurer en cas d'accident.

8.2 Configuration d'un serveur de messagerie sur ubuntu : Postfix

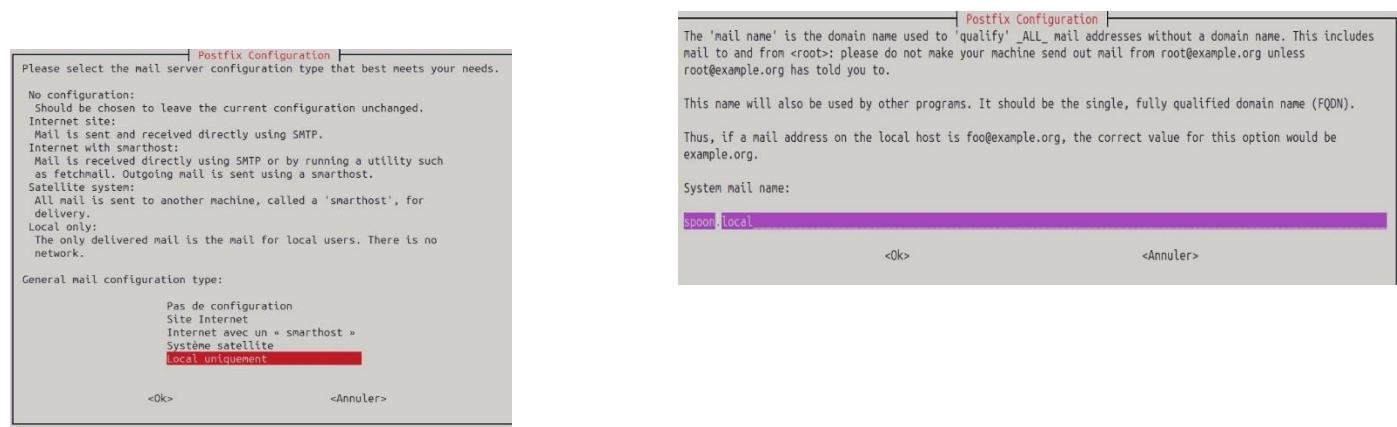
Après avoir mis à jour la liste des paquets avec la commande « sudo apt update » vue précédemment on utilise la commande suivante pour installer postfix :

```
root@mgrosmann@mgrosmann-pc:~$ sudo apt install postfix
```

On arrivera donc sur 2 qui nous intéresse

Pour le premier d'entre eux on sélectionnera « Local uniquement »

Pour le deuxième il faut rentrer un nom de système mail, nous avons le choix entre en créer en fictif ou déjà existant mais on fera la choix d'un créer un.



On va ensuite éditer le fichier de configuration avec la commande suivante uniquement dans le cas où certaines lignes sont erronées ou incomplètes :

```
mgrosmann@mgrosmann-pc:~$ sudo nano /etc/postfix/main.cf
```

Il devrait ressembler à ça

```
# fresh installs.
compatibility_level = 3.6

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls CAPath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = spoon.local
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = spoon.local, $myhostname, mgrosmann-pc, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = loopback-only
default_transport = error
relay_transport = error
inet_protocols = all
```

Si la configuration est correcte vous pouvez fermer le fichier en utilisant « ctrl+x » et utiliser la commande suivante pour redémarrer Postfix :

```
mgrosmann@mgrosmann-pc:~$ sudo systemctl restart postfix
```

La configuration est maintenant terminée même si pour pouvoir recevoir des messages il faut installer la commande mail avec la commande suivante :

```
mgrosmann@mgrosmann-pc:~$ sudo apt install mailutils
```

8.3 Configuration d'un serveur cloud local : Nextcloud

Pour configurer Nextcloud il faut d'abord commencer par installer SQL sur le terminal ubuntu

On installe le serveur MySQL avec la commande a condition d'avoir deja effectué la commande « sudo apt update » afin de mettre à jour la liste des paquets :

```
root@mgrosmann-pc:~# sudo apt install mysql-server
```

Puis on lance MySQL avec :

```
mgrosmann@mgrosmann-pc:~$ sudo mysql
```

On crée une base de données et l'utilisateur pour se connecter sur Nextcloud comme ceci :

```
CREATE DATABASE nextcloud;
CREATE USER 'nextcloud'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Avant d'installer Nextcloud il faut d'abord installer apache avec la commande suivante :

```
root@mgrosmann-pc:~# sudo apt install apache2
```

Maintenant qu'apache est installé, passons à l'installation de Nextcloud, il faut saisir la commande suivante :

```
wget https://download.nextcloud.com/server/releases/nextcloud-?.zip
```

A la place du « ? » vous saisissez la syntaxe de la version de votre choix

Vous allez ensuite extraire l'archive vers le répertoire var/www afin de vous permettre d'y accéder depuis internet grâce à la commande :

```
sudo unzip nextcloud-?.zip -d/var/www
```

Il faut ensuite modifier des autorisations a Nextcloud afin qu'il puisse modifier les fichiers grâce à la commande :

```
root@mgrosmann-pc:~# sudo chown -R www-data:www-data /var/www/nextcloud~
```

Vous allez ensuite modifier le fichier « nextcloud.conf » avec la commande :

```
root@mgrosmann-pc:~# sudo nano /etc/apache2/sites-available/nextcloud.conf
```

Le fichier doit ressembler à ça :

```
Alias /nextcloud "/var/www/nextcloud/"  
<Directory /var/www/nextcloud/>  
    Options +FollowSymlinks  
    AllowOverride All  
  
    <IfModule mod_dav.c>  
        Dav off  
    </IfModule>  
  
    SetEnv HOME /var/www/nextcloud  
    SetEnv HTTP_HOME /var/www/nextcloud  
</Directory>
```

Vous devez activer le fichier de configuration avec la commande :

```
root@mgrosmann-pc:~# sudo a2ensite nextcloud.conf
```

Pour sauvegarder la configuration il faut redémarrer le serveur apache

```
root@mgrosmann-pc:~# sudo systemctl restart apache2
```

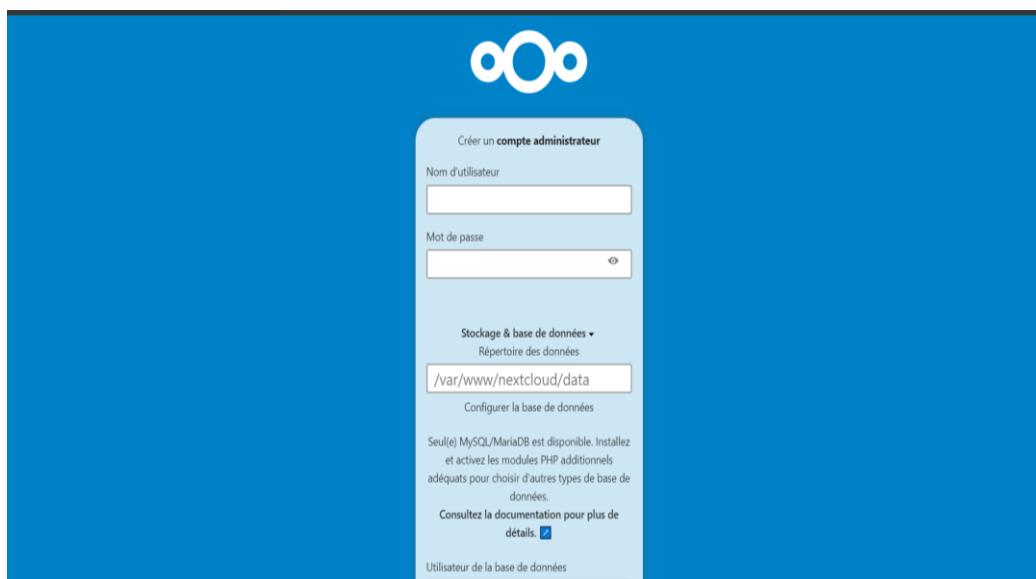
Par la suite pour nextcloud il faut installer php-curl :

```
root@mgrosmann-pc:~# sudo apt install php-curl
```

Il faudra redémarrer le serveur apache précédemment cité.

Pour vous rendre sur votre cloud local saisissez 192.168.XXX.XXX(votre adresse ip trouvable avec la commande « ifconfig ») suivi de /nextcloud

Vous devrez tomber sur cette interface :



Connectez-vous avec l'utilisateur ajouté dans la base de données en descendant dans le bas de la page :

Utilisateur de la base de données

Mot de passe de la base de données

Nom de la base de données

Hôte de la base de données

localhost

Veuillez spécifier le numéro du port avec le nom de l'hôte (ex: localhost:5432).

Installer

Besoin d'aide ? [Lire la documentation](#)

Vous arriverez donc sur une page ressemblant à ça :

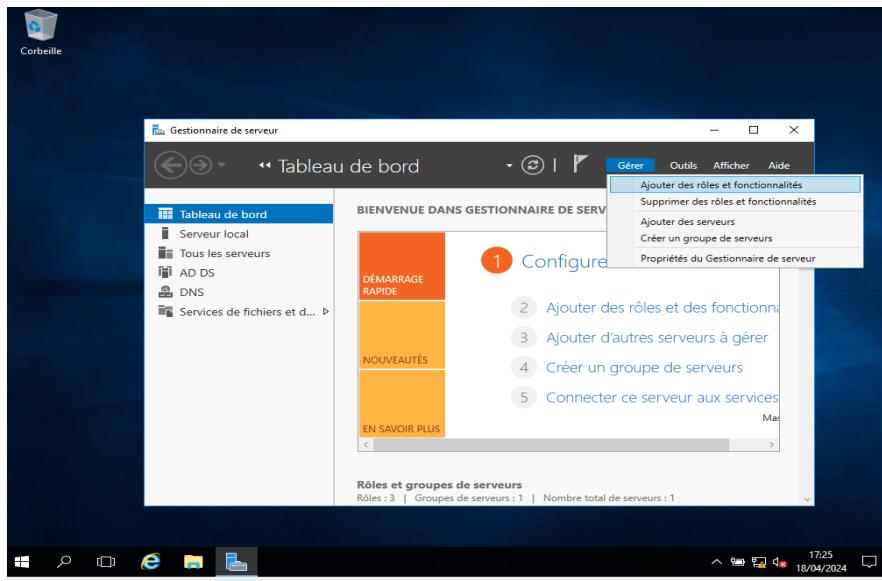
The screenshot shows the Nextcloud web interface. On the left, there's a sidebar with navigation links: All files, Recent, Favorites, Shares, Tags, Shared to Circles, Deleted files, 36.5 MB of 5 GB used, and Files settings. The main area displays a welcome message: "Welcome to Nextcloud! 📁 🌐 🖥️". Below it, there's a note: "Here you can add a description or any other info relevant for the folder. It will show as a 'Readme.md' and in the web interface also embedded nicely up at the top." A "Reconnect" button is visible. The file list table has columns for name, size, and modified date. The files listed are:

Name	Size	Modified
Documents	1.1 MB	21 days ago
Photos	5.4 MB	21 days ago
Templates	10.2 MB	21 days ago
Reasons to use Nextcloud.pdf	954 KB	21 days ago
Templates credits.md	2 KB	21 days ago
test.md	0 KB	seconds ago

8.4 Configuration d'un active directory: Windows server

Pour configurer un Active Directory il faudra une version de Windows server 2016.

Dans le gestionnaire de serveur qui s'ouvre automatiquement au démarrage sélectionner « Gérer » puis « ajouter des rôles et des fonctionnalités



Il faudra laisser les choix par défauts et sélectionner votre serveur.

The 'Avant de commencer' window displays the following text:

Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.

For suppression des rôles, des services de rôle ou des fonctionnalités :

Démarrer l'Assistant de Suppression de rôles et de fonctionnalités

Avant de continuer, vérifiez que les travaux suivants ont été effectués :

- Le compte d'administrateur possède un mot de passe fort
- Les paramètres réseau, comme les adresses IP statiques, sont configurés
- Les dernières mises à jour de sécurité de Windows Update sont installées

Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaites, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.

Cliquez sur Suivant pour continuer.

Ignorer cette page par défaut

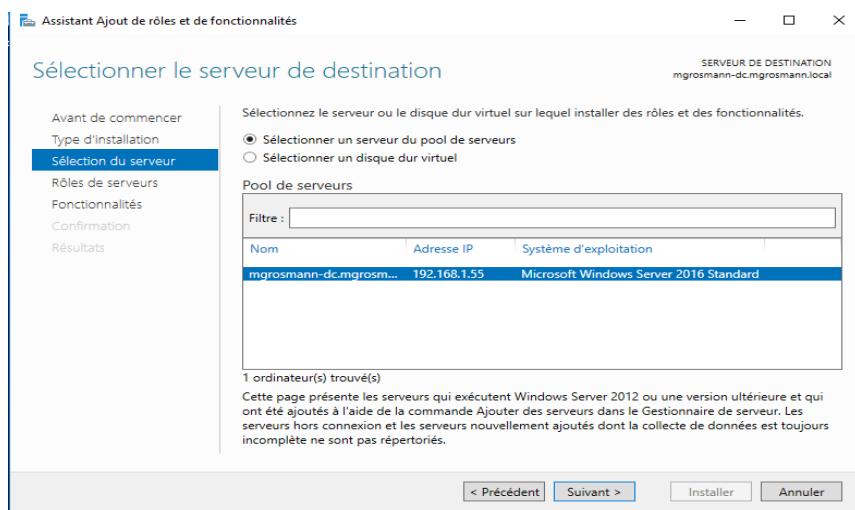
The 'Sélectionner le type d'installation' window displays the following text:

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

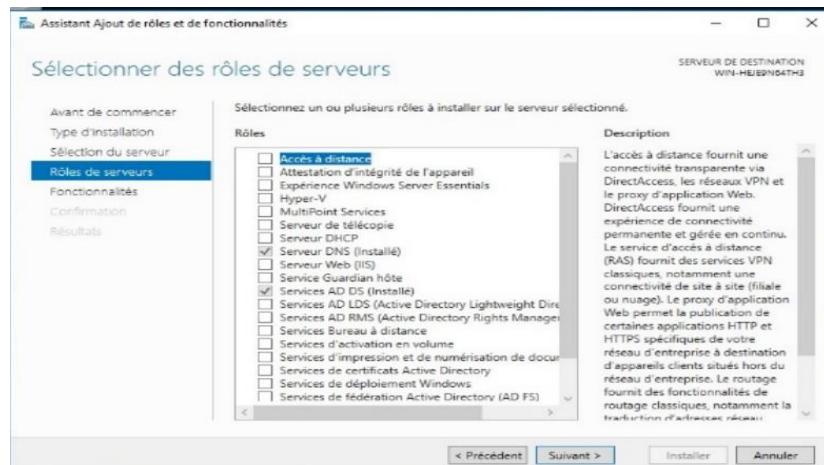
Installation basée sur un rôle ou une fonctionnalité
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

Installation des services Bureau à distance
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

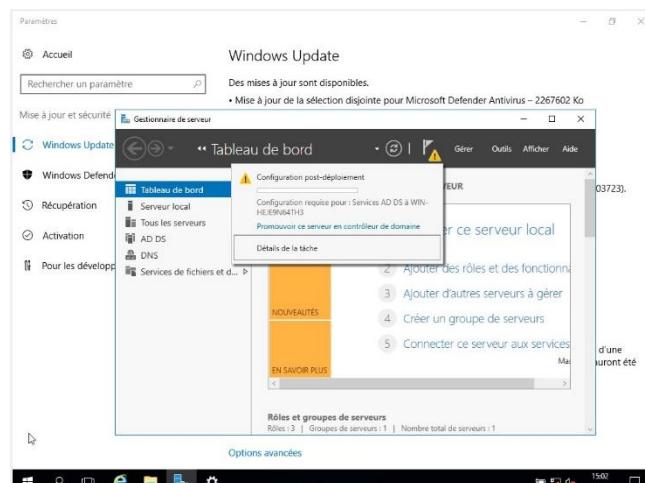
< Précédent Suivant > Installer Annuler



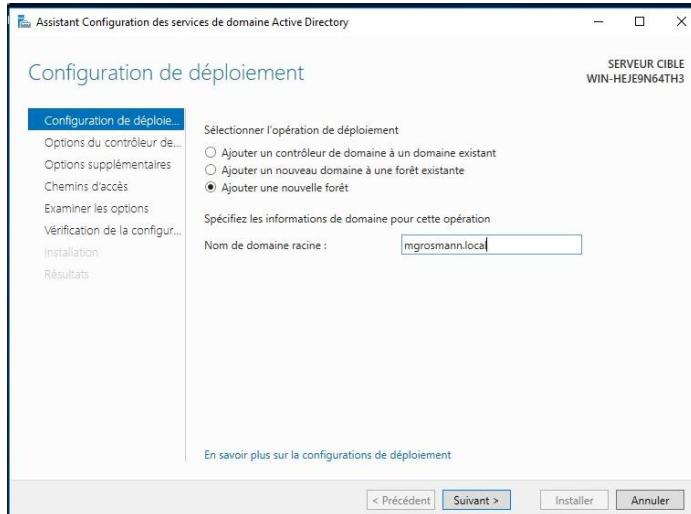
Il faudra ensuite sélectionner « AD DS » et « DNS »



Suite à cela il faudra sélectionner le drapeau en haut de la fenêtre afin de promouvoir ce serveur en domaine de contrôle et un chargement se produira.



Vous arriverez sur une nouvelle fenêtre, il faudra sélectionner « ajouter une nouvelle forêt » et entrer un nom pour le nom de domaine racine.



Après cela un mot de passe et nom de domaine NETBIOS sera demandé :

The image contains two side-by-side screenshots of the 'Assistant Configuration des services de domaine Active Directory'.

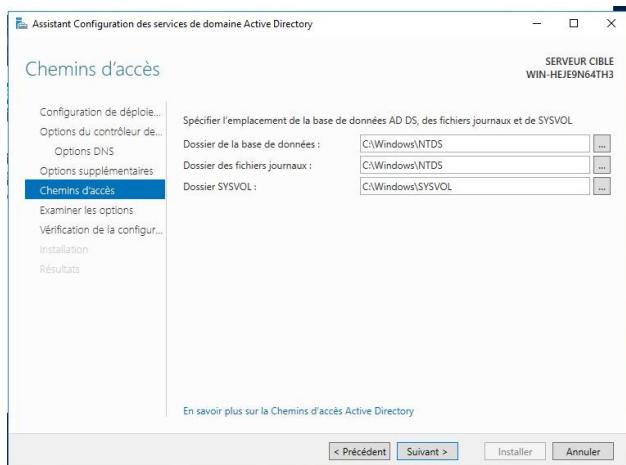
Left Screenshot (Options du contrôleur de domaine):

- Title: 'Assistant Configuration des services de domaine Active Directory'.
- Section: 'Options du contrôleur de...'. The 'Options du contrôleur de...' tab is selected.
- Sub-section: 'Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine'.
 - Niveau fonctionnel de la forêt : Windows Server 2016
 - Niveau fonctionnel du domaine : Windows Server 2016
- Section: 'Spécifier les fonctionnalités de contrôleur de domaine'.
 - Serveur DNS (Domain Name System)
 - Catalogue global (GC)
 - Contrôleur de domaine en lecture seule (RODC)
- Section: 'Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)'.
 - Mot de passe : [redacted]
 - Confirmer le mot de passe : [redacted]
- Buttons at the bottom: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

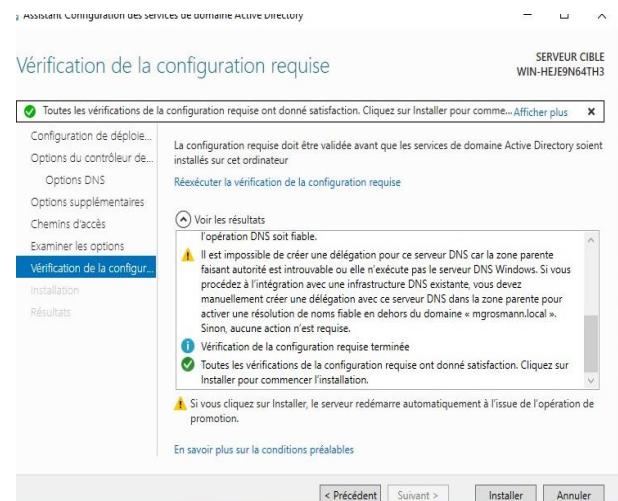
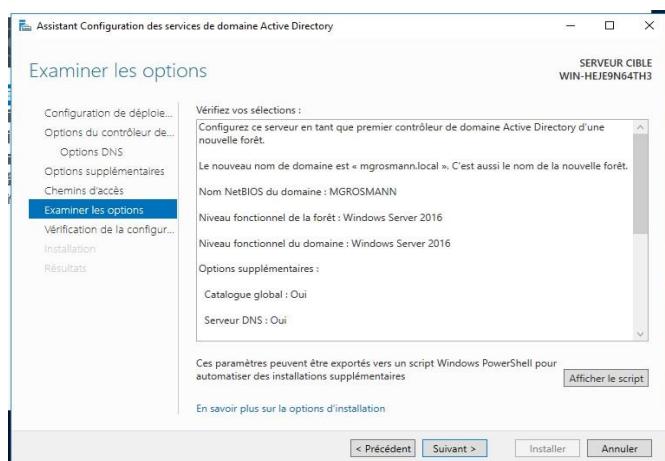
Right Screenshot (Options supplémentaires):

- Title: 'Assistant Configuration des services de domaine Active Directory'.
- Section: 'Options supplémentaires'. The 'Options supplémentaires' tab is selected.
- Section: 'Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire'.
 - Le nom de domaine NetBIOS : MGROSMANN
- Section: 'Configuration de déploiement' (disabled).
 - Options du contrôleur de...
 - Options DNS
 - Chemins d'accès
 - Examiner les options
 - Vérification de la config...
 - Installation
 - Résultats
- Buttons at the bottom: '< Précédent', 'Suivant >', 'Installer', and 'Annuler'.

Pour finir vous aurez le choix de définir les dossiers où seront stockés les fichiers liés à l'active directory



Afin de finaliser l'installation il faudra confirmer que les informations sont correctes et si oui procéder a l'installation.

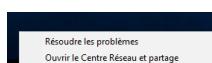


Vous serez déconnectez quand l'installation sera finalisée.

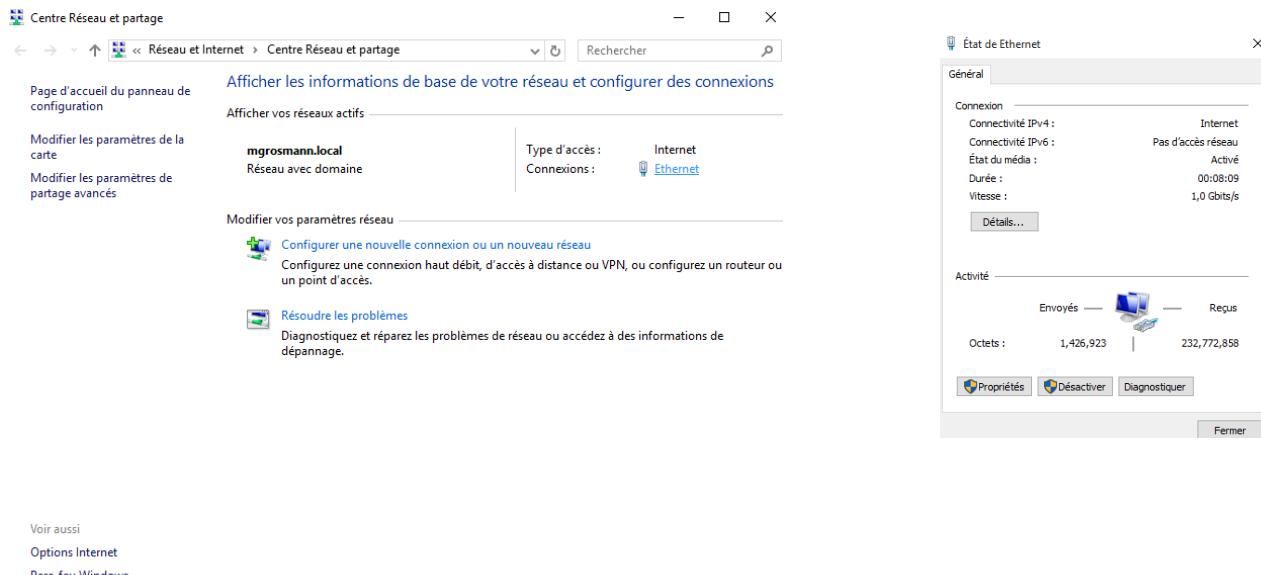
Passons maintenant à la configuration sur Windows 10 qui doit obligatoirement se situé dans le même réseau.

Avant toute chose il est impératif de définir en serveur DNS préféré l'adresse IP du Windows server .

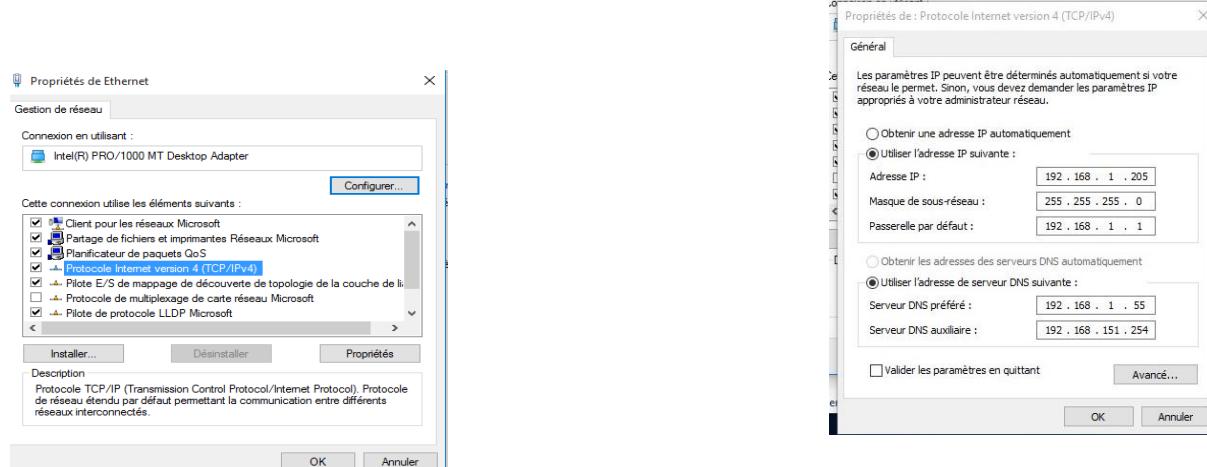
Pour cela : effectuer un clic droit sur l'icône réseau, sélectionner « ouvrir le centre réseau et partage,



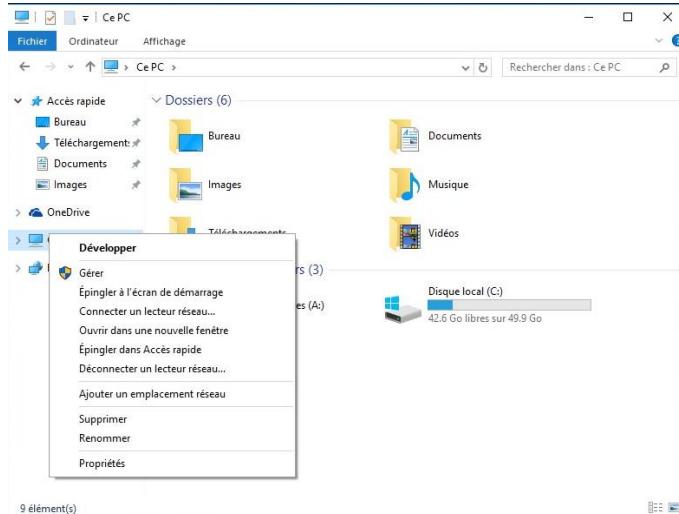
Ensuite sélectionner « Ethernet puis propriétés sur la nouvelle fenêtre générée



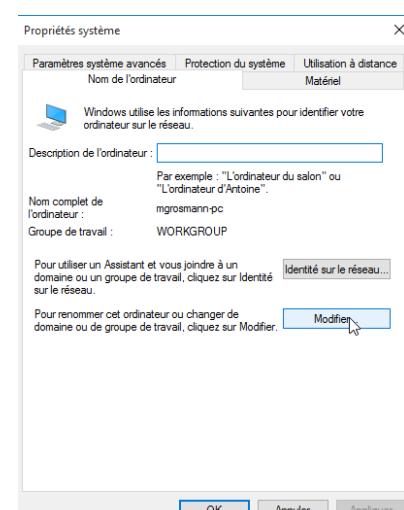
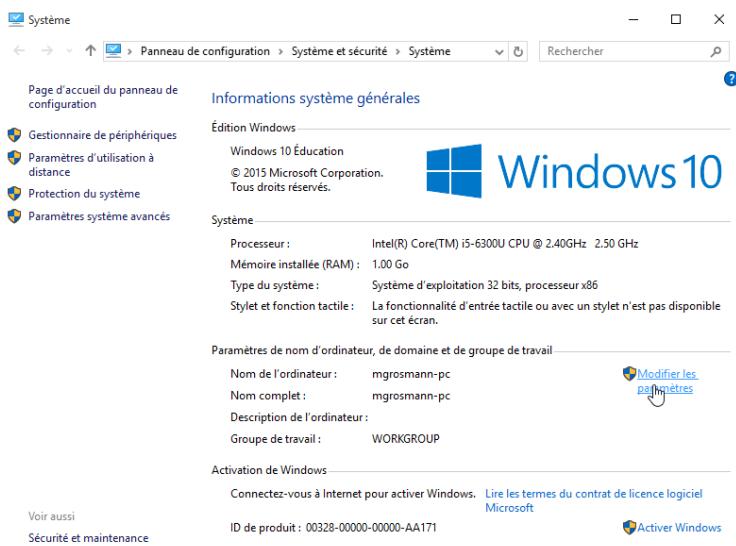
Ensuite il ne reste plus qu'à sélectionner « protocole internet Version 4 » et à définir l'adresse IP du Windows server en serveur DNS préféré



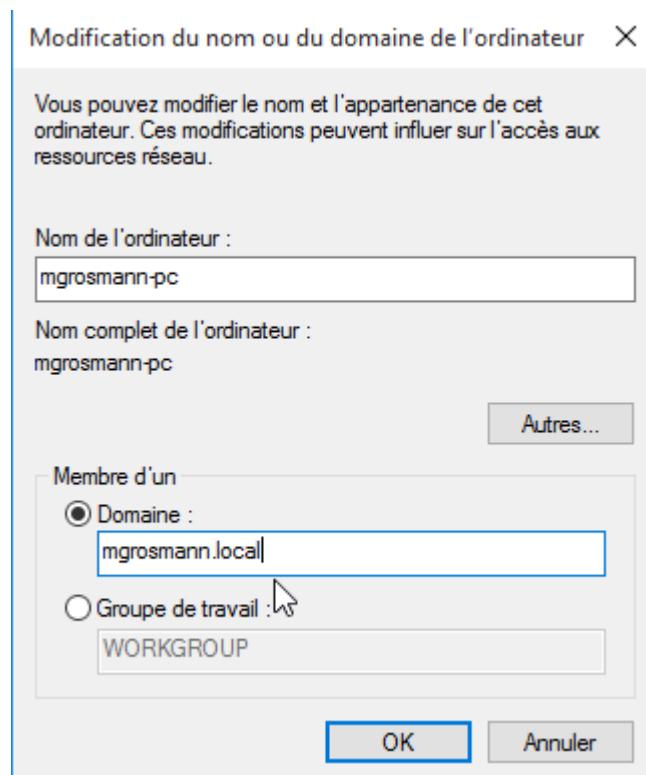
Il faudra ouvrir un explorateur de fichier, effectuer un clic droit sur ce pc puis propriétés



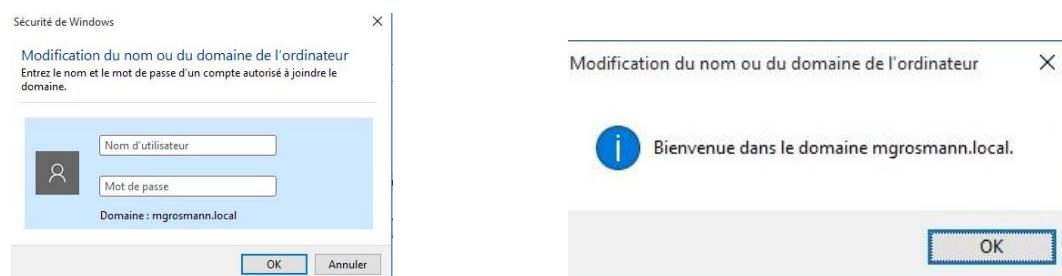
Il faudra ensuite sélectionner « modifier les paramètres » puis sur la nouvelle fenêtre « modifier »



Vous devrez ensuite sélectionner « Domaine » en bas de la page puis saisir le nom de domaine racine défini sur le Windows server

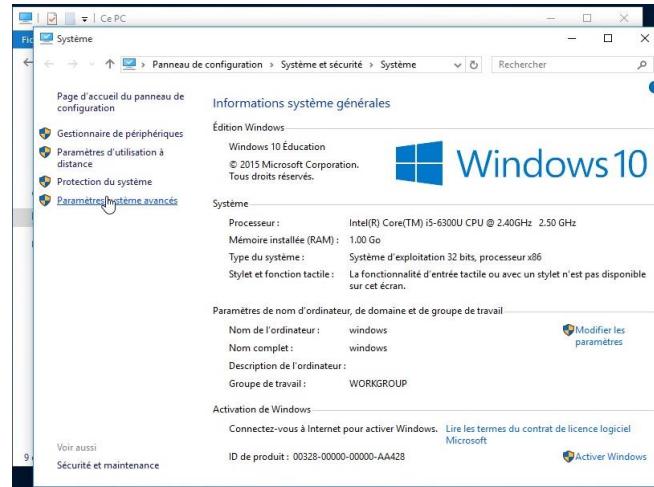
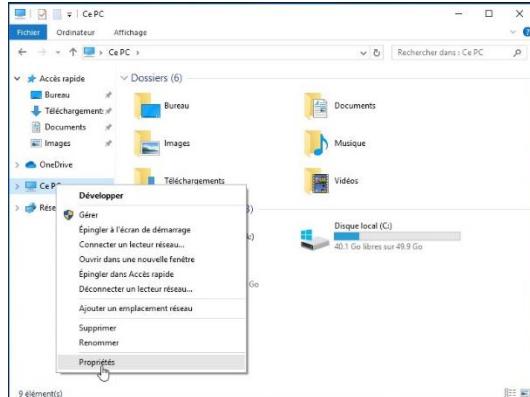


Si la configuration est correcte il faudra se connecter avec le compte administrateur du Windows server afin d'ajouter le domaine à la machine Windows 10.

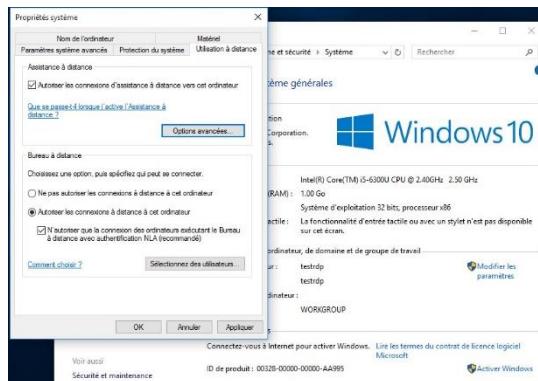


8.5 Configuration D'une connexion à Distance : RDP

Pour commencer il faut ouvrir l'explorateur de fichier et effectuer un clic droit sur « Ce Pc » puis sélectionner propriétés ensuite sélectionner « Paramètres système avancés »

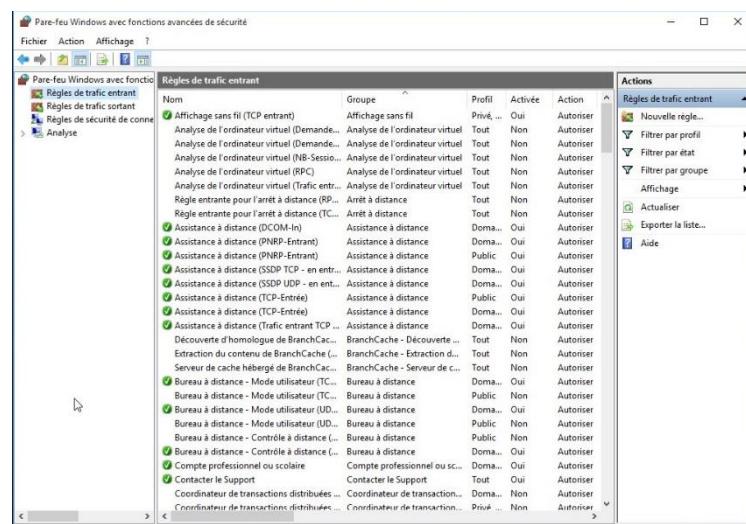


Après cela allez sur l'onglet « Utilisation à Distance » et cocher « Autoriser les connexions à distance à cet ordinateur »

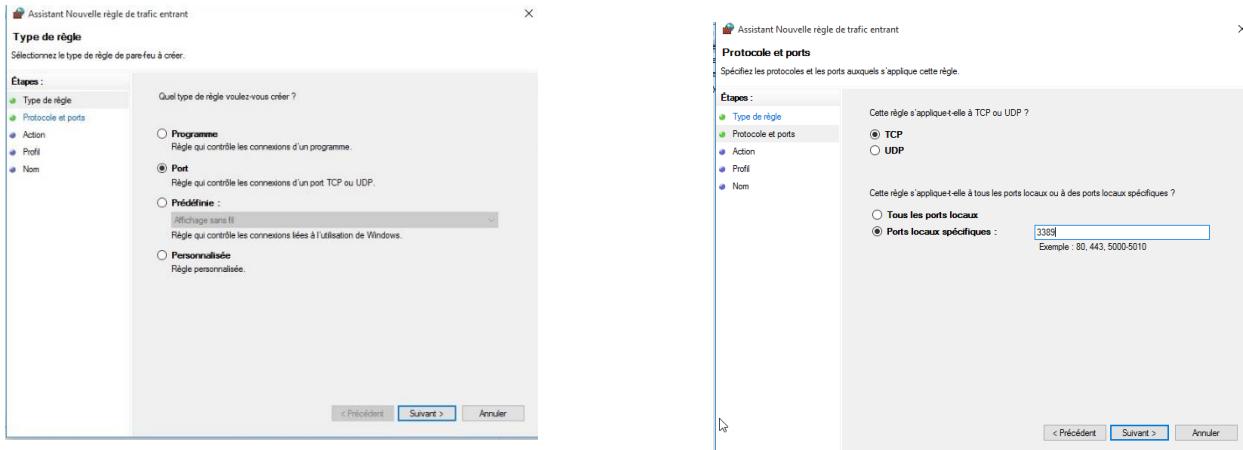


Maintenant nous allons rajouter une règle de pare feu pour permettre cette connexion à distance.

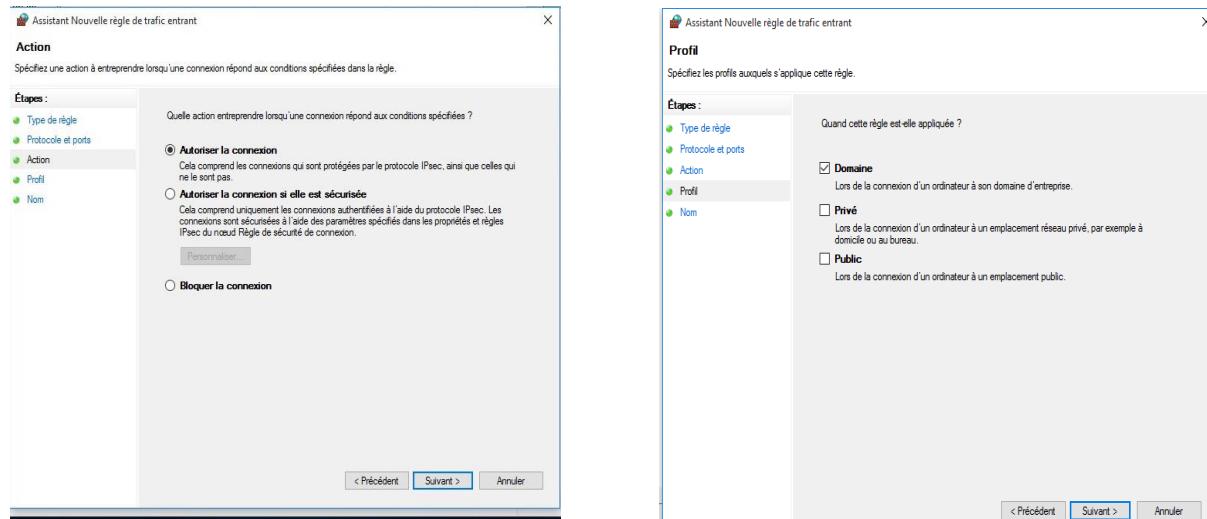
Aller sur le pare feu Windows et aller sur la section « règles de trafic entrant » puis sélectionner « Nouvelle règle »



Sélectionnez « Port » puis sur la nouvelle étape sélectionnez « TCP » puis mettez « 3389 » en Port



Pour la prochaine étape il faut laisser « Autoriser la connexion » cocher puis pour l'étape suivante afin d'empêcher des attaques frauduleuses décocher tout sauf Domaine



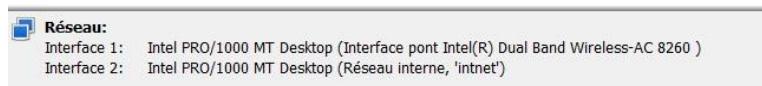
Il nous reste plus qu'à donner un nom à cette règle et la configuration sera désormais finalisé.

8.6 Configuration d'un Serveur DHCP : Pf sense

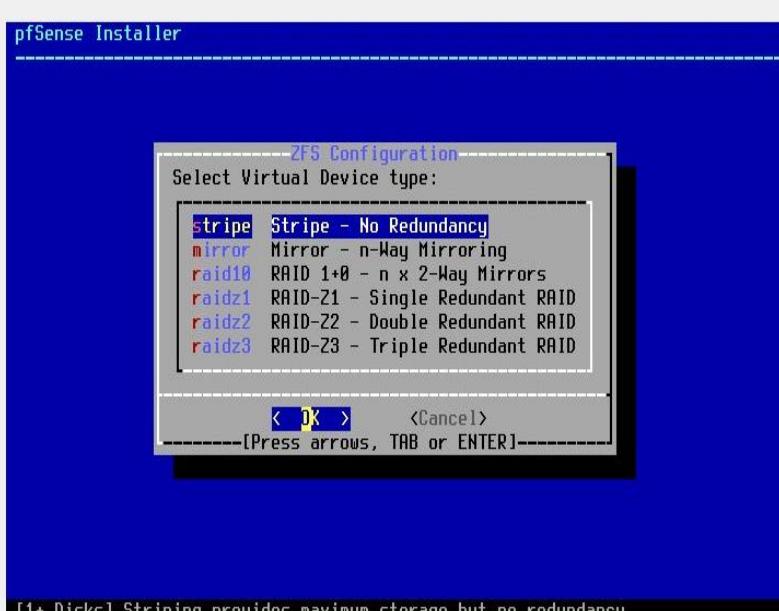
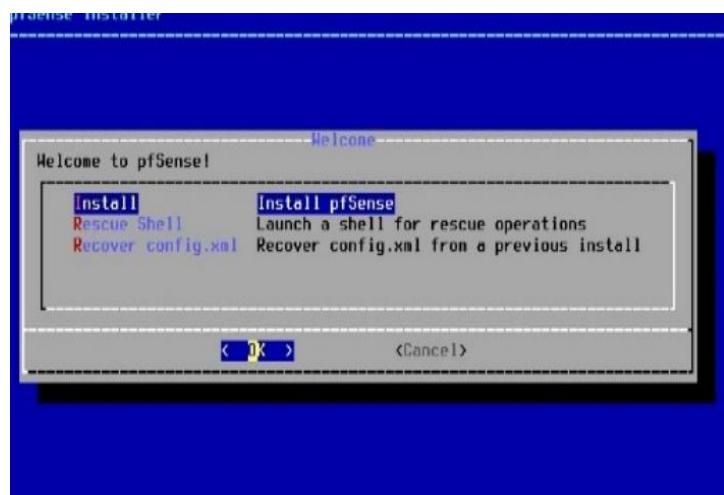
Avant de commencer l'installation assurez d'avoir deux cartes réseaux :

Une en accès par pont permettant de se connecter à l'extérieur en WAN a partir de la carte réseau de l'ordinateur

Une deuxième en réseau interne afin de communiquer avec les autres machines virtuelles.



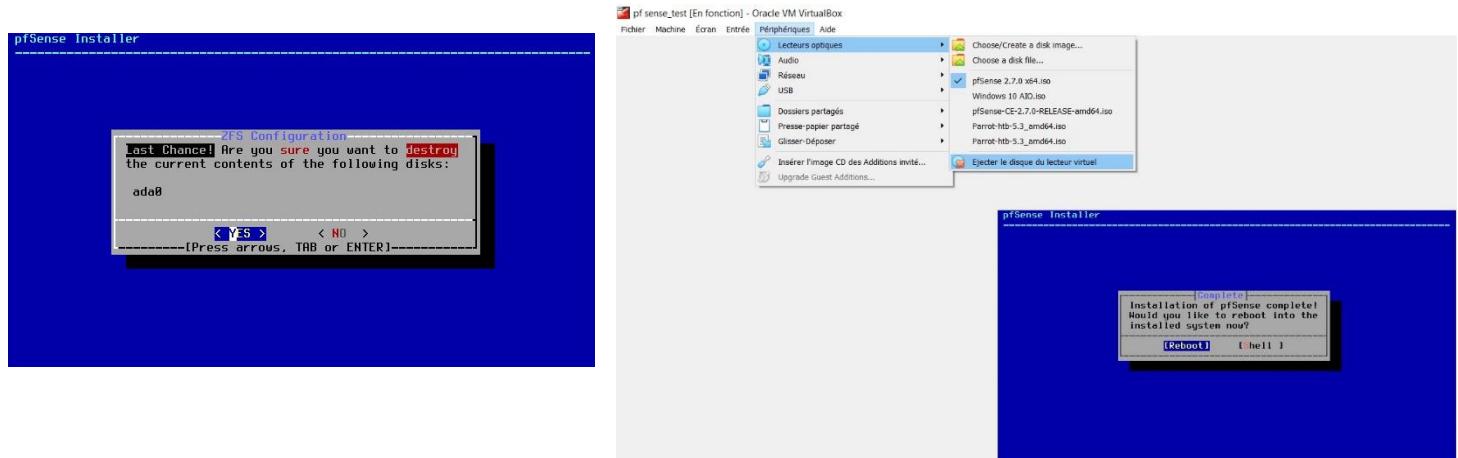
Pour le début de l'installation de Pf-Sense il va falloir laisser les choix par défauts :



Ensuite vous allez sélectionnez sur espace afin de confirmer le disque dur sur lequel vous allez installer pf sense



Vous allez devoir confirmer que vous souhaitez détruire le contenu du disque pour l'installation puis vous allez pouvoir redémarrer tout en pensant à éjecter le disque



A la fin du redémarrage vous tomberez sur un écran ressemblant à ça :

```

starting syslog...done.
starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 723cce0c0008d842a68e

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0          -> v4/DHCP4: 192.168.1.49/24
LAN (lan)      -> em1          -> v4: 192.168.1.1/24

 0) Logout (SSH only)          9) pfTop
 1) Assign Interfaces          10) Filter Logs
 2) Set interface(s) IP address 11) Restart webConfigurator
 3) Reset webConfigurator password 12) PHP shell + pfSense tools
 4) Reset to factory defaults 13) Update from console
 5) Reboot system              14) Enable Secure Shell (sshd)
 6) Halt system                15) Restore recent configuration
 7) Ping host                  16) Restart PHP-FPM

Enter an option: 

```

Pour configurer le serveur DHCP ou il faut configurer l'adresse LAN qu'elle soit dans le même réseau ou non que l'adresse WAN.

Pour modifier les adresses IP WAN ou LAN il faut entrer 2, dans notre cas on veut modifier l'adresse LAN donc il faut entrer 2.

```
LHN (lan)      -> em1      -> v4: 192.168.1.1/24
8) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
```

Ensuite vous aurez le choix entre avoir une adresse automatique avec le DHCP ou en entrer une manuellement, il faut en saisir une manuellement.

On peut laisser « 192.168.1.1 » si l'adresse WAN est dans un sous réseau différent, dans notre cas on va changer le sous réseau

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.15.1
```

Il faudra mettre 24 en CIDR ensuite.

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0 = 16
     255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Ensute on nous demandera une « upstream gateway adress » ou une adresse passerelle en amont. Par défaut on n'en mettra aucune

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Viens la configuration du DHCP.

On désactivera la DHCP6 et entrera aucune adresse ipv6

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n
```

```
Enter the new LAN IPv6 address. Press <ENTER> for none:
```

```
>
```

Ensuite on active le serveur DHCP sur le LAN et on indique la plage d'adresse IP que le serveur distribue en indiquant la première et dernière adresse IP.

```
Do you want to enable the DHCP server on LAN? (y/n) y
```

```
Enter the start address of the IPv4 client address range: 192.168.15.10
```

```
Enter the end address of the IPv4 client address range: 192.168.15.20
```

```
Disabling IPv6 DHCPD...
```

Pour finaliser la configuration on laisse le protocole HTTPS pour le site web pfsense.

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

La configuration est à présent terminée même si on peut encore la personnaliser sur l'interface web depuis Windows 10.

Si la configuration est correcte vous aurez une adresse IP qui sera automatique dans le même sous réseau que le pf-sense.

Vous pouvez vérifier en lançant l'invite de commande et en utilisant la commande ipconfig :

```
microsoft Windows [version 10.0.10240]
(c) 2015 Microsoft Corporation. Tous droits réservés.

C:\Users\vboxuser>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :
  Suffrage DNS propre à la connexion. . . . . : home.arpa
  Adresse IPv6 de liaison locale. . . . . : fe80::1c1c:973e:e140:ed9b%3
  Adresse IPv4. . . . . : 192.168.15.10
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . : 192.168.15.1

Carte Tunnel isatap.home.arpa :
  Statut du média. . . . . : Média déconnecté
  Suffrage DNS propre à la connexion. . . . . : home.arpa

Carte Tunnel Teredo Tunneling Pseudo-Interface :
  Suffrage DNS propre à la connexion. . . . . :
  Adresse IPv6. . . . . : 2001:0:2851:782c:20d6:75dd:dabc:8551
  Adresse IPv6 de liaison locale. . . . . : fe80::20d6:75dd:dabc:8551%
  Passerelle par défaut. . . . . :
```

Vous allez maintenant entrer l'adresse LAN du pf sense pour pouvoir accéder à l'interface web en entrant « admin » comme identifiant et « pfsense » comme mot de passe



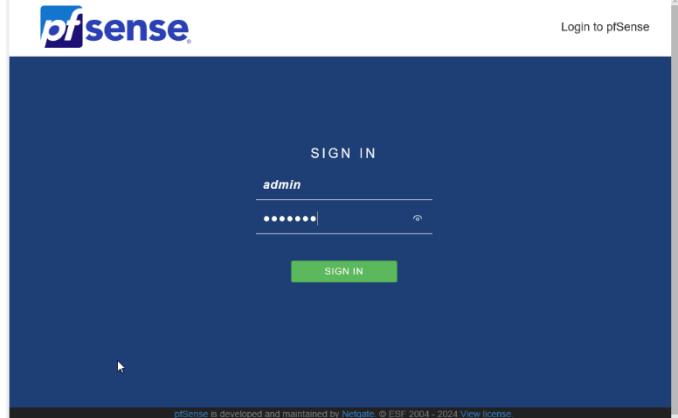
Le certificat de sécurité de ce site web présente un problème

Nous vous recommandons de fermer cette page web et de quitter ce site.

Le certificat de sécurité et l'URL du site ne correspondent pas. Ce problème peut indiquer une tentative de duplicité ou d'interception des données envoyées au serveur.

Atteindre plutôt la page d'accueil

Poursuivre sur cette page web (non recommandé)



Une fois connecter il faut se rendre sur « services » puis « DHCP server »

Range	192.168.15.10	192.168.15.20
From	To	

On peut observer la plage d'adresse ip précédemment configurer qu'on peut modifier si on le souhaite.

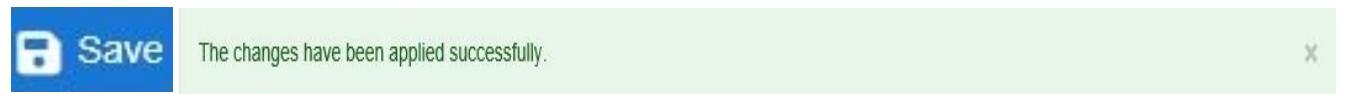
La partie intéressante de la configuration est la configuration du délai d'expiration.

En effet puisqu'elle n'est pas configurable depuis la machine pf sense.

Par défaut elle dure minimum 7200 secondes(2h) et au maximum 86400 secondes(24h)

Default lease time	<input type="text" value="7200"/>	This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.
Maximum lease time	<input type="text" value="86400"/>	This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.

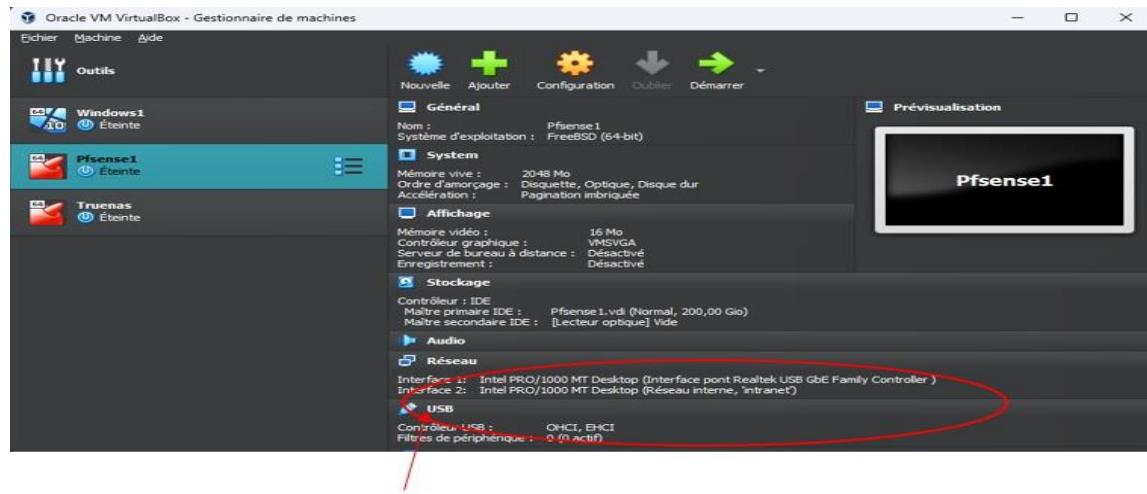
La configuration est maintenant terminée pour sauvegarder les changements il faut sélectionner « Save » en bas de la page afin de sauvegarder les changements. Vous aurez un message de confirmation.



8.7 Installation pfSense et mise en place d'un portail captif

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD.

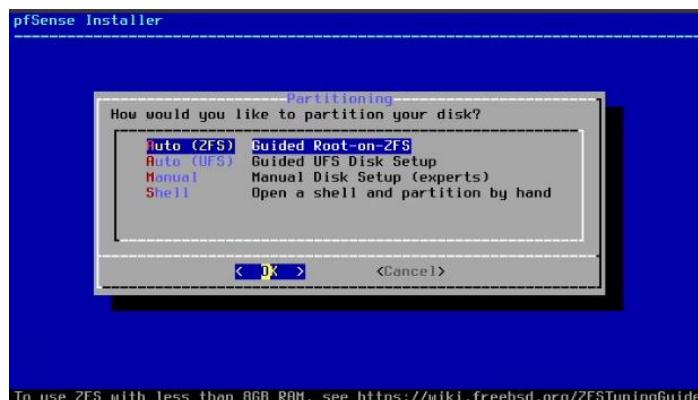
Pour commencer, il faut configurer notre machine virtuelle avec différents paramètres nécessaires au bon fonctionnement de pfSense.

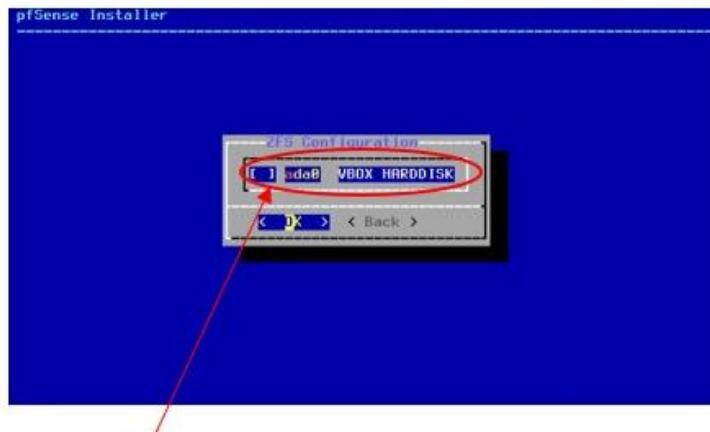


Le plus important de la configuration :

- L'interface 1 sera affectée au WAN du pfSense, qui permet de communiquer avec l'extérieur.
- L'interface 2 sera affecté au LAN, donc au réseau interne.

Après cela, nous pouvons passer à l'installation de pfSense :





Disque où sera installé pfSense

Après avoir affecté l'interface 1 au WAN et l'interface 2 au LAN, il faut maintenant entrer l'adresse IP LAN ainsi que le masque.

Adresse IPV4 LAN

```
Available interfaces:  
1 - WAN (em0 - dhcp, dhcp6)  
2 - LAN (em1)  
Enter the number of the interface you wish to configure: 2  
Configure IPv4 address LAN interface via DHCP? (y/n) n  
Enter the new LAN IPv4 address. Press <ENTER> for none:  
> 20.0.0.254  
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.  
e.g. 255.255.255.0 = 24  
255.255.0.0 = 16  
255.0.0.0 = 8  
Enter the new LAN IPv4 subnet bit count (1 to 32):  
> 24  
For a WAN, enter the new LAN IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>  
Configure IPv6 address LAN Interface via DHCP6? (y/n) ■
```

Masque

Mise en place d'un DHCP :

```
> 20.0.0.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 20.0.0.10
Enter the end address of the IPv4 client address range: 20.0.0.30
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Plages d'adresses IP

Nous avons cet affichage

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv1)

login: root
Password:
Login incorrect
login: admin
Password:
VirtualBox Virtual Machine - Netgate Device ID: f9f63a42ed0e45ef5865

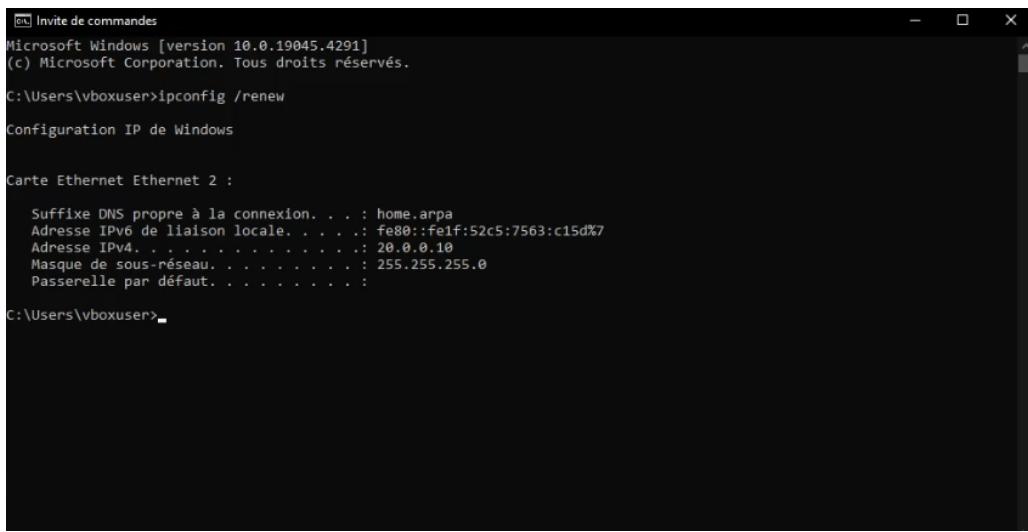
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.0.13/24
LAN (lan)      -> em1      -> v4: 20.0.0.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM

Enter an option: ■
```

Maintenant dans la machine Windows, taper dans le terminal ipconfig /renew



```
Microsoft Windows [version 10.0.19045.4291]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\vboxuser>ipconfig /renew

Configuration IP de Windows

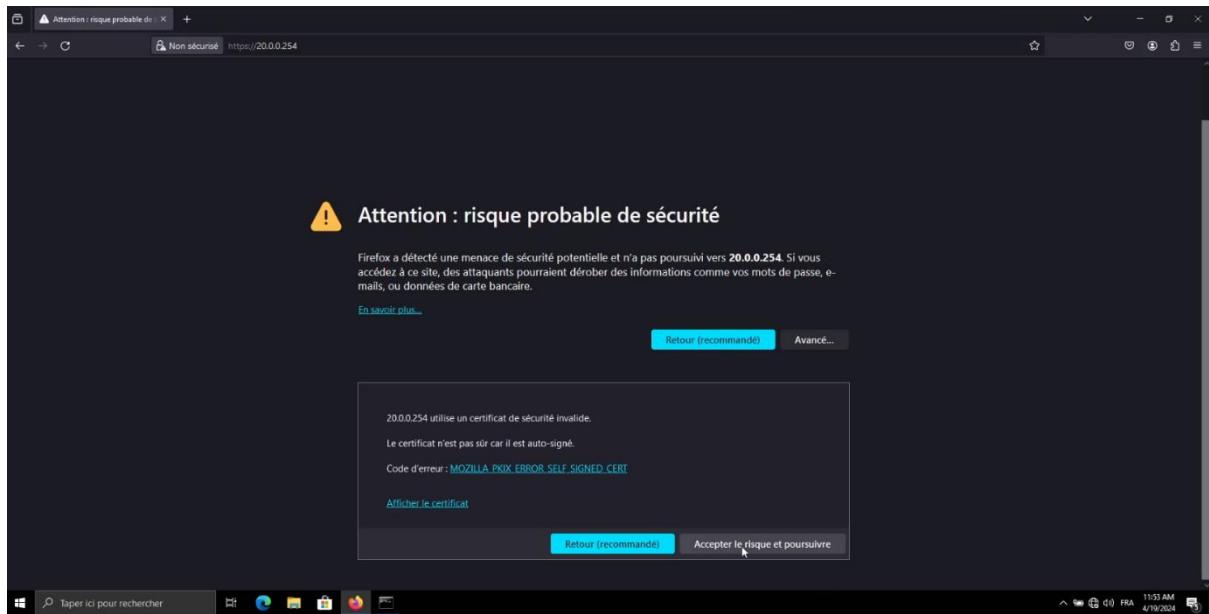
Carte Ethernet Ethernet 2 :

    Suffixe DNS propre à la connexion . . . : home.arpa
    Adresse IPv6 de liaison locale . . . . . : fe80::fe1f:52c5:7563:c15d%7
    Adresse IPv4 . . . . . : 20.0.0.10
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :

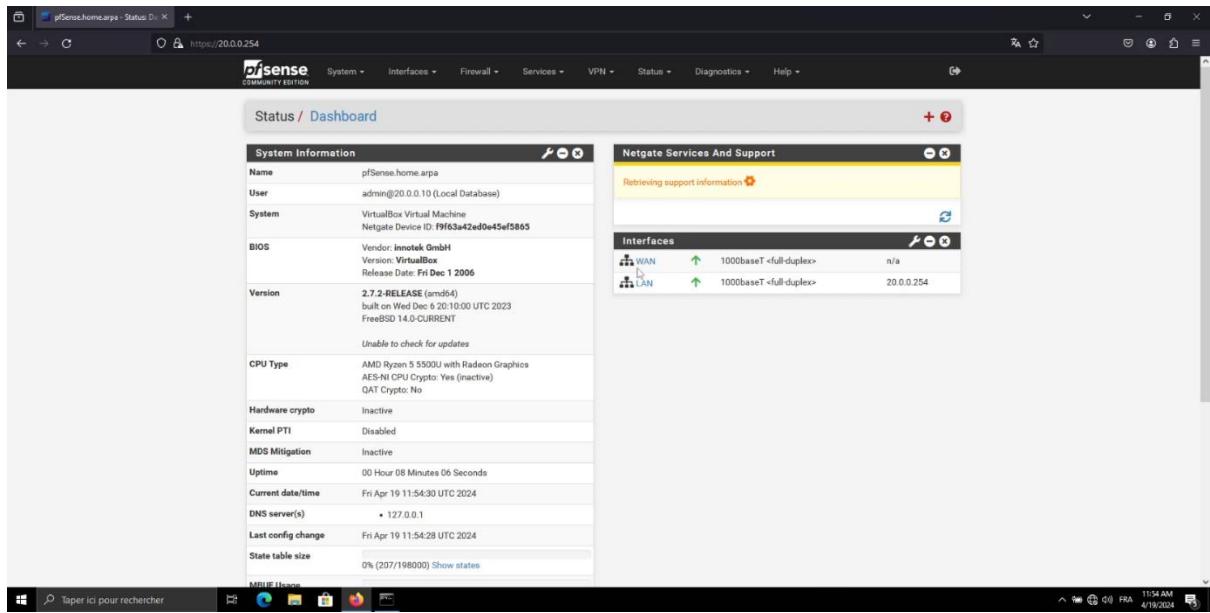
C:\Users\vboxuser>
```

L'adresse IPV4 sera affectée sur la plage d'adresses IP fournies par le pfSense.

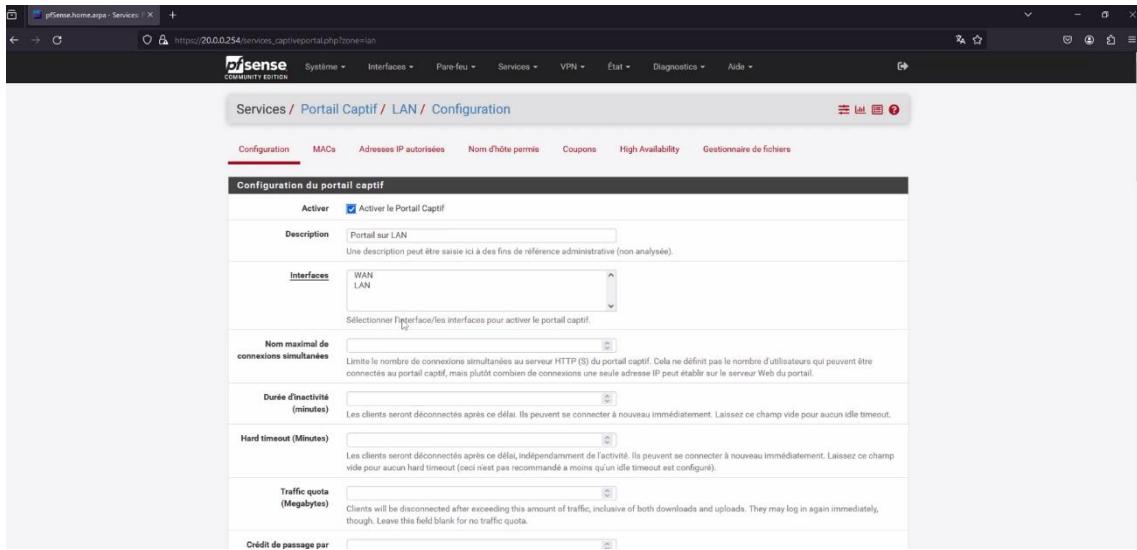
A présent tout est configuré et on peut accéder à l'interface pfSense sur son navigateur en tapant l'adresse IP LAN du pfSense



On accède au dashboard de pfSense en ayant entré les informations de connexions admin et pfsense pour le mot de passe.



Nous pouvons passer à la mise en place d'un portail captif



Dans la section services/Portail Captif/LAN/Configuration, on choisit l'interface LAN et la méthode d'authentification « Use an authentication backend ».

Maintenant on peut créer notre utilisateur du portail captif avec les paramètres que l'on souhaite. Lorsque que l'utilisateur sera sur la page de connexion pfSense, il rentrera ses identifiants et il sera connecté.

pfSense home page - Système +

https://20.0.0.254/system_usermanager.php?action=new

Système / Gestionnaire d'usagers / Utilisateurs / Modifier

Utilisateurs **Groupes** **Paramètres** **Serveurs d'authentification**

Propriétés utilisateur

Défini par	USER
Désactivé	<input type="checkbox"/> Cet utilisateur ne peut pas s'authentifier
Nom d'utilisateur	Thomas
Mot de passe	*****
Nom complet	Thomas Poussin
Date d'expiration	Laissez vide si le compte ne doit pas expiration, 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	admins
	Pas un membre de Membre de
	Gérez vers la liste "Membre de" Gérez vers la liste "Non membre de"
Certificat	Aucune autorité de certification privée n'a été trouvée. Une autorité de certification privée est requise pour créer un nouveau certificat d'utilisateur.

Système / Gestionnaire d'usagers / Utilisateurs

Utilisateurs **Groupes** **Paramètres** **Serveurs d'authentification**

Utilisateurs

Nom d'utilisateur	Nom complet	État	Groupes	Actions
Thomas	thomas_poussin	✓		Modifier Supprimer
admin	System Administrator	✓	admins	Modifier Supprimer

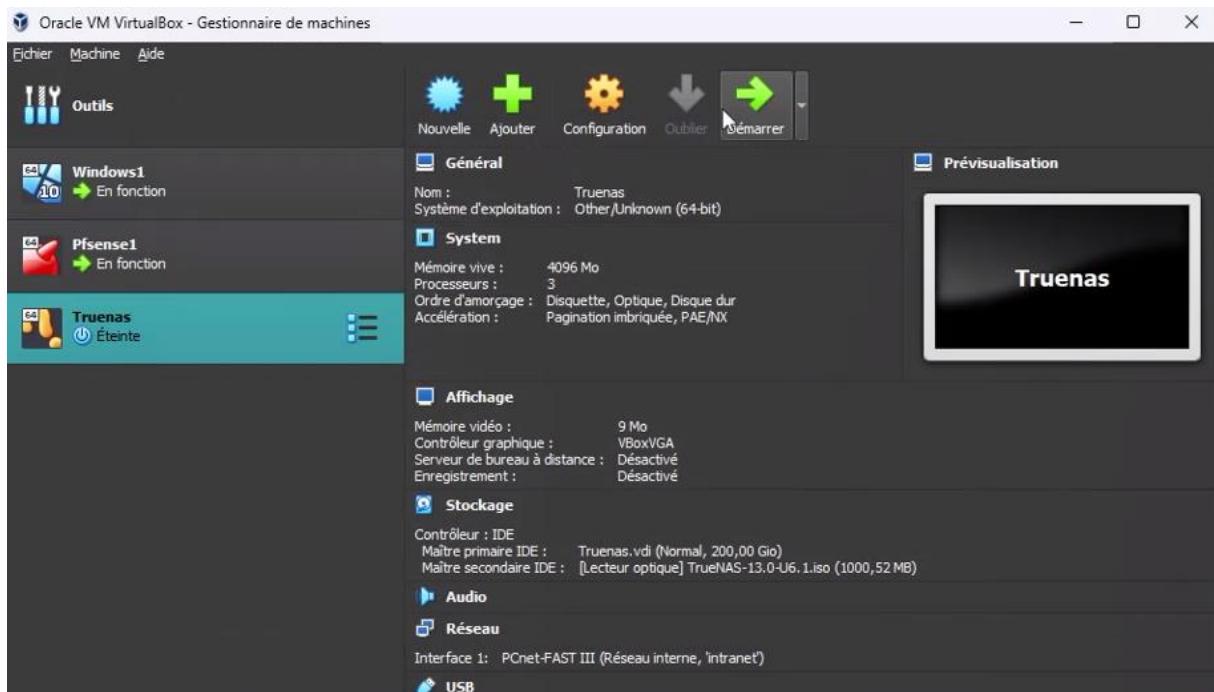
[Ajouter](#) [Supprimer](#)

Utilisateurs du portail captif

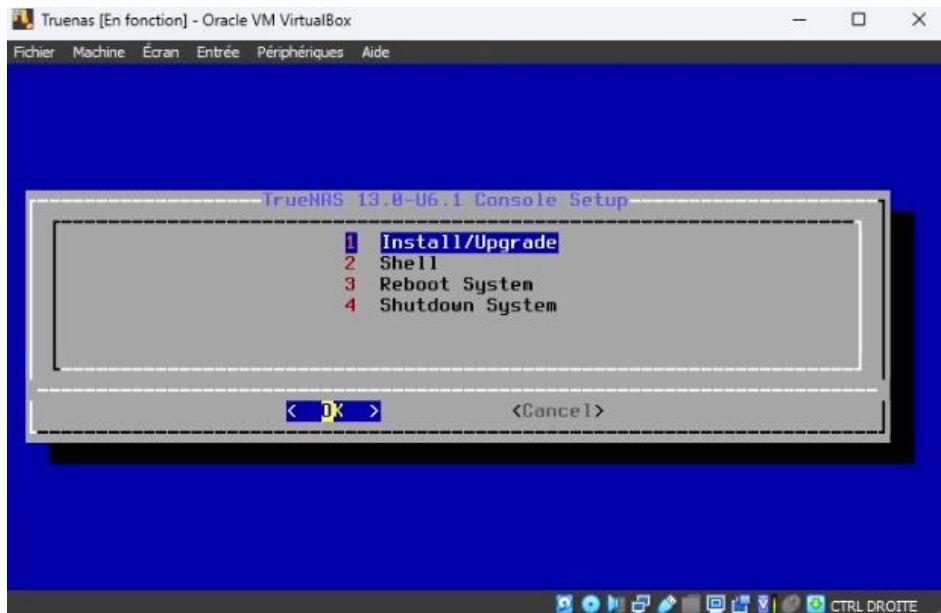
8.8 Rapport technique installation serveur fichier TrueNAS Core

TrueNAS est un système d'exploitation sous licence libre, basé sur FreeBSD et la distribution Linux Debian, destiné aux serveurs de stockage en réseau NAS. Nous allons donc mettre en place un système de serveur de stockage.

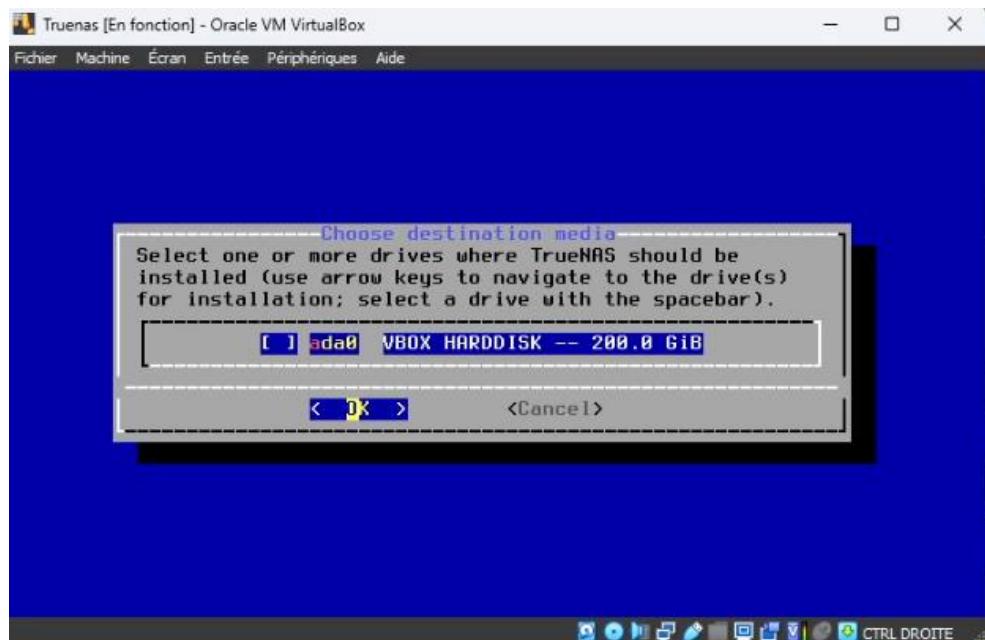
Pour commencer la configuration nécessaire pour la machine virtuelle TrueNAS Core :



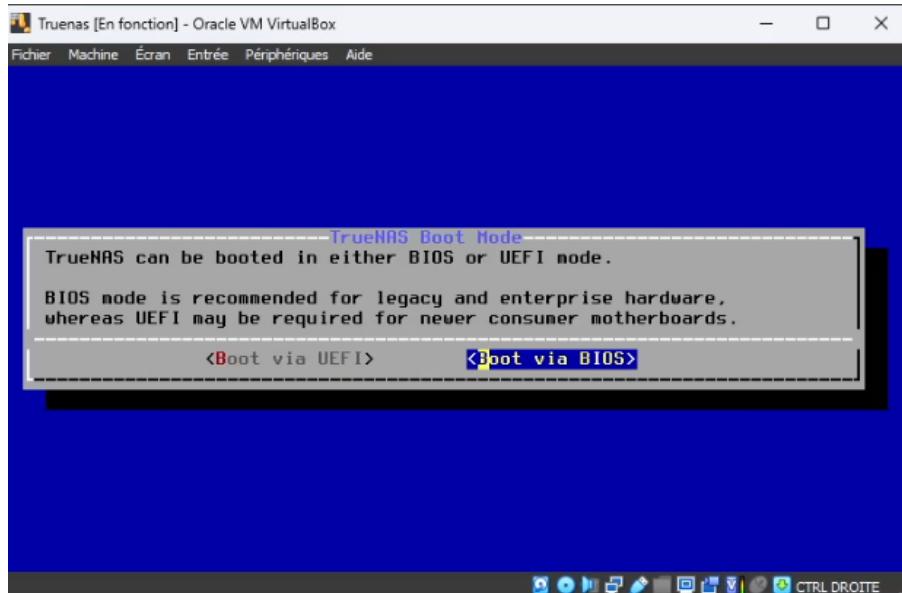
On arrive sur l'interface d'installation de TrueNas



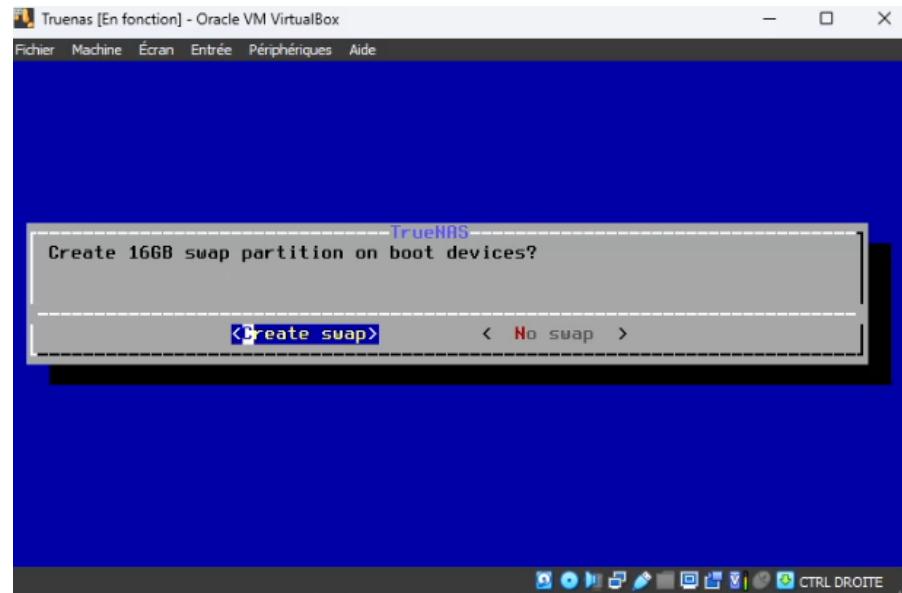
Le disque sélectionné pour l'installation



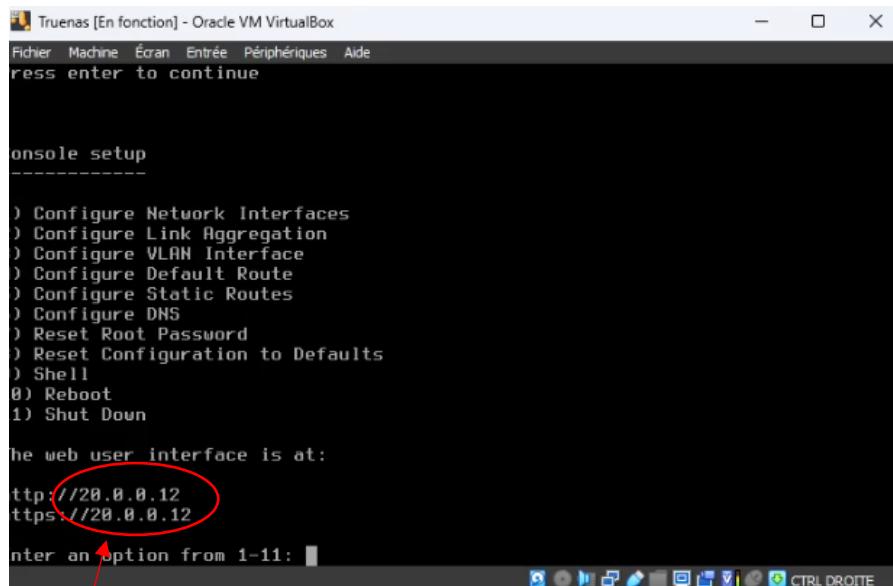
On boot via le BIOS



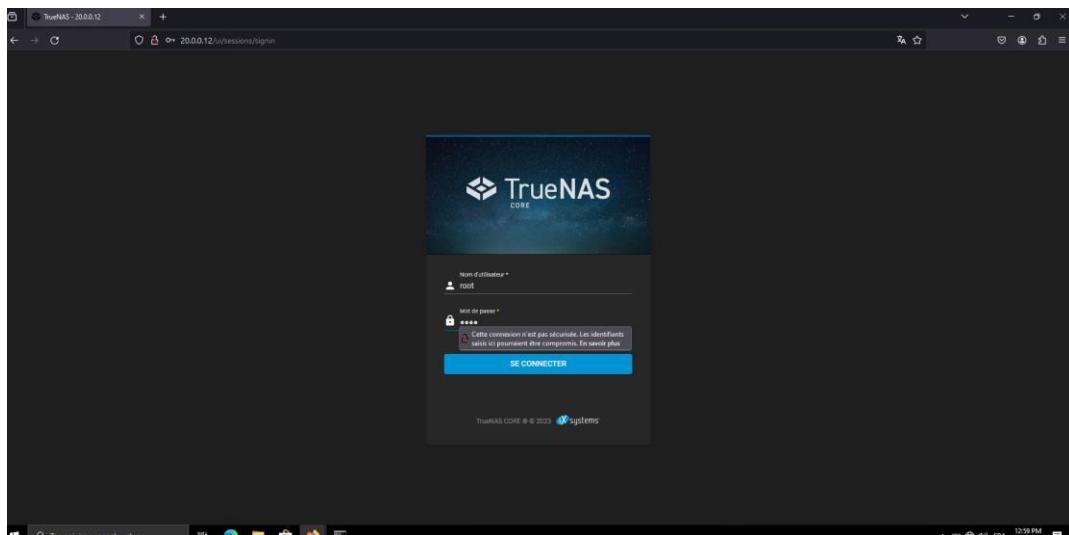
On ne crée pas de partition swap dans ce cas-là



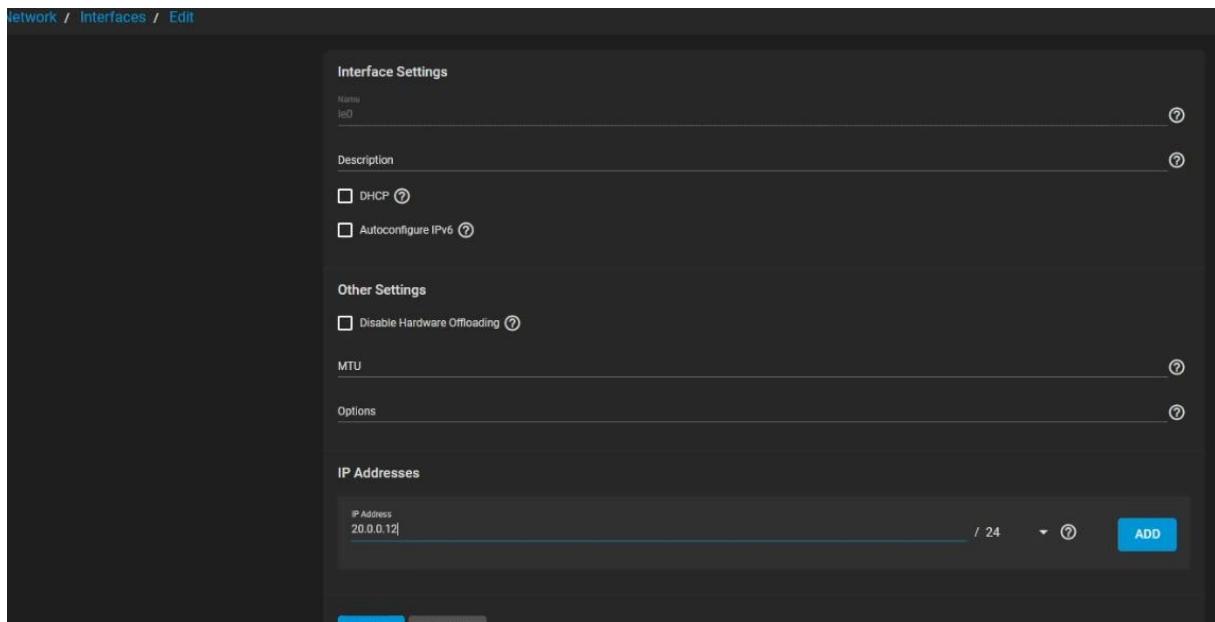
L'installation se poursuit, on redémarre la machine virtuelle, ensuite s'affiche cette interface :



On peut changer le root password et ensuite dans la machine virtuelle windows on rentre l'adresse du TrueNAS dans le navigateur et on arrive sur cette interface de connexion.



Dans l'onglet Network/Interface, on désactive le DHCP, on rentre une adresse statique puis cliquer sur valider.



Maintenant nous allons créer l'espace de stockage des fichiers en cliquant sur Storage/Pools sur le menu TrueNas.

Name * Truenas

RESET LAYOUT SUGGEST LAYOUT ADD VDEV

Available Disks

No data to display

0 selected / 0 total

Filter disks by name Filter disks by capacity

Data VDevs

ada1 UNKNOWN 200 GiB

ada2 UNKNOWN 200 GiB

0 selected / 2 total

Mirror

Estimated raw capacity: 198 GiB

Estimated total raw data capacity: 198 GiB

CREATE CANCEL

On ajoute les deux disques, dans ce cas-ci, ils seront en miroir. Cliquer sur valider et sauvegarder.

Maintenant, il faut partager ce stockage, dans la rubrique Sharing/Windows Share (SMB)

Basic

Path * /mnt/Truenas

/mnt

Truenas

Name Stockage TrueNas

Purpose Default share parameters

Enabled

SUBMIT CANCEL ADVANCED OPTIONS

Cliquer sur valider puis activer le service

Ensuite, il faut créer un utilisateur qui pourra se connecter au partage réseau du TrueNas.

Identification

Full Name *
Thomas

Username *
thomas

Email

Password *

Confirm Password *

User ID and Groups

User ID *
1000

New Primary Group [?](#)

Primary Group

Auxiliary Groups
wheel

Directories and Permissions

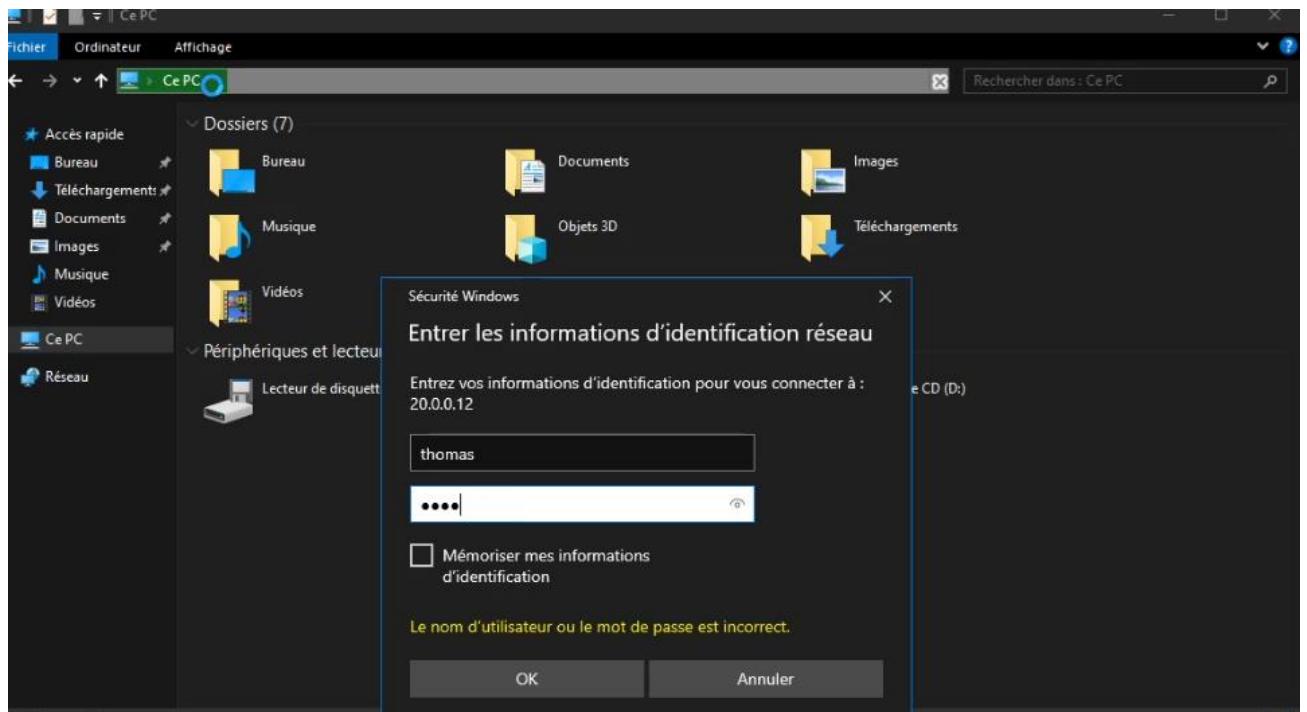
Home Directory
/nonexistent

/mnt

Authentication

SSH Public Key

Tout est prêt et l'utilisateur peut accéder à TrueNAS en tapant l'adresse 20.0.0.12 dans cet exemple, rentrer les informations de connexion de l'utilisateur créé dans TrueNAS Core et il accède au partage réseau.



9. Manuel utilisateur :

9.1 Installation du logiciel de système de sauvegarde : DEJA DUP

Tout d'abord il faut savoir que sur Ubuntu est basé sur le noyau d'exploitation Linux qui reste assez différent de Windows 10.

Il faut également savoir que principalement tout se fait grâce au terminal.

Pour installer DEJA DUP, le logiciel qui va nous permettre de restaurer des fichiers perdus on va utiliser une commande qui va mettre à jour la liste des paquets qu'on peut installer notamment celui de DEJA DUP.

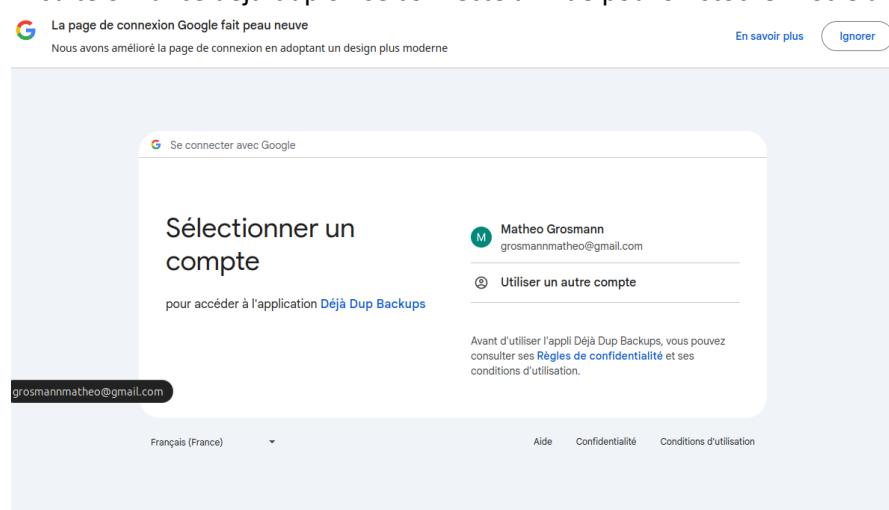
Pour cela il faut entrer la commande suivante :

```
root@mgrosmann-pc:~# sudo apt update
```

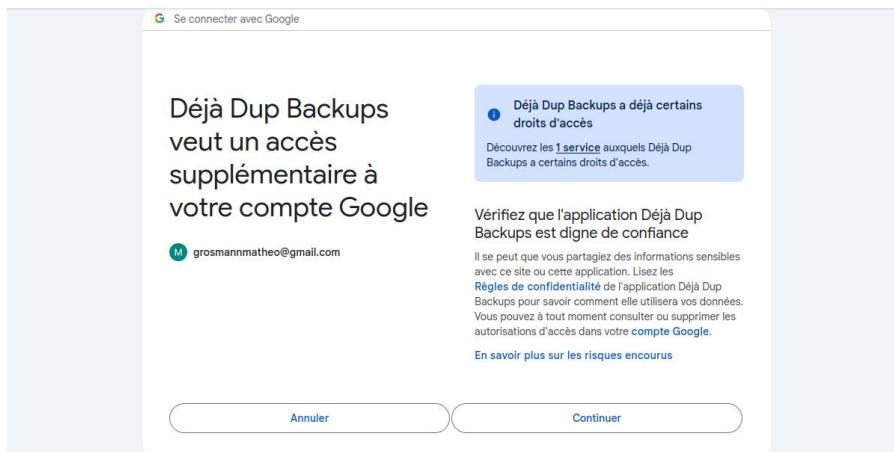
Maintenant qu'on a mis à jour la liste des paquets on va pouvoir installer déjà-dup

```
root@mgrosmann-pc:~# sudo apt install deja-dup
```

Ensuite on lance deja-dup on se connecte afin de pouvoir stocker notre archive :



Vous aurez le choix entre plusieurs options afin de conserver votre archive comme des options de connexion avec google ou Microsoft ou le stocker localement sur votre disque dur. Dans cet exemple on a choisi google



Par la suite il faut autoriser certain les accès dont deja-dup a besoin.

Ensuite on nous demandera si on veut demander un mot de passe pour l'archive, pour la sécurisation des données il est préférable d'autoriser et d'entrer un mot de passe qui sera demandé pour ouvrir l'archive.



À la suite de cela l'archive sera sur votre drive et vous serez en capacité à la restaurer en cas d'accident.

9.2 Configuration d'un serveur de messagerie sur ubuntu : Postfix

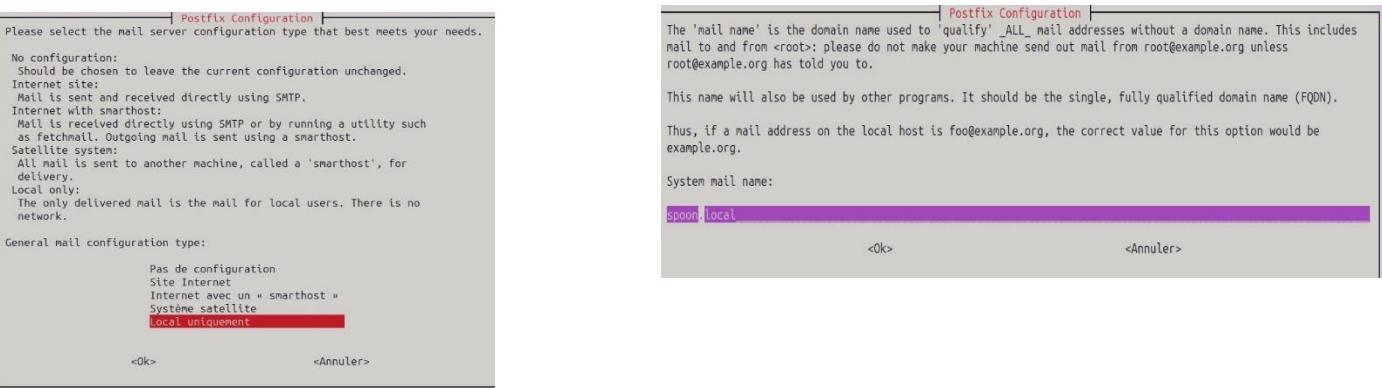
Après avoir mis à jour la liste des paquets avec la commande « sudo apt update » vue précédemment pour DEJA DUP on utilise la commande suivante pour installer Postfix :

```
root@mgrosmann@mgrosmann-pc:~$ sudo apt install postfix
```

On arrivera donc sur diverses menu dont seulement 2 qui nous intéresse

Pour le premier d'entre eux on sélectionnera « Local uniquement » parce qu'on souhaite configurer un serveur de messagerie au sein du réseau local afin de limiter les failles de sécurités.

Pour le deuxième il faut rentrer un nom de système mail comme @gmail.com ou @lasalle63.fr, nous avons le choix entre en créer en fictif ou déjà existant mais on fera la choix d'un créer un.



On va ensuite éditer le fichier de configuration « main.cf » qui se situe dans etc/postfix

« .cf » est une extension de fichier texte comme « .txt » et qui sert principalement pour stocker des données de configuration.

Il va falloir le faire en ligne de commande car il faut être administrateur et cela n'est pas possible depuis l'explorateur de fichier contrairement à l'os Windows 10 qui permet de le faire.

```
mgrosmann@mgrosmann-pc:~$ sudo nano /etc/postfix/main.cf
```

Il devrait ressembler à ça :

```
# fresh installs.
compatibility_level = 3.6

# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_tls_security_level=may

smtp_tls_CPath=/etc/ssl/certs
smtp_tls_security_level=may
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = spoon.local
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = /etc/mailname
mydestination = spoon.local, $myhostname, mgrosmann-pc, localhost.localdomain, localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [:1]:128
mailbox_size_limit = 0
recipient_delimiter = +
inet_interfaces = loopback-only
default_transport = error
relay_transport = error
inet_protocols = all
```

Si la configuration est correcte vous pouvez fermer le fichier en utilisant « ctrl+x » et utiliser la commande suivante pour redémarrer Postfix :

```
mgrosmann@mgrosmann-pc:~$ sudo systemctl restart postfix
```

La configuration est maintenant terminée même si pour pouvoir recevoir des messages il faut installer la commande mail avec la commande suivante :

```
mgrosmann@mgrosmann-pc:~$ sudo apt install mailutils
```

9.3 Configuration d'un serveur cloud local : Nextcloud

Pour configurer Nextcloud il faut d'abord commencer par installer un serveur SQL sur le terminal Ubuntu.

Le langage MySQL est un langage de programmation permettant de manipuler les bases de données. L'utilisation de ce langage est obligatoire pour la configuration de Nextcloud.

On commence par mettre à jour la liste des paquets avec « sudo apt update » puis on installe le serveur MySQL avec la commande :

```
root@mgrosmann-pc:~# sudo apt install mysql-server
```

Puis on lance MySQL avec :

```
mgrosmann@mgrosmann-pc:~$ sudo mysql
```

On crée une base de données et l'utilisateur pour se connecter sur Nextcloud comme ceci :

```
CREATE DATABASE nextcloud;
CREATE USER 'nextcloud'@'localhost' IDENTIFIED BY 'password';
GRANT ALL PRIVILEGES ON nextcloud.* TO 'nextcloud'@'localhost';
FLUSH PRIVILEGES;
EXIT;
```

Sur la première ligne on crée une base de données nommée « Nextcloud ». Elle sera utilisée par Nextcloud afin de configurer le cloud local

Sur la deuxième ligne on crée un utilisateur « nextcloud » local grâce à la syntaxe « '@localhost' » et on définit comme mot de passe 'password' grâce à la commande « IDENTIFIED BY ». On utilisera cet identifiant et ce mot de passe pour se connecter sur nextcloud

Pour que l'utilisateur nextcloud possède tous les droits on utilise la commande « GRANT ALL PRIVILEGES ». « on nextcloud » permet de définir sur quel base de données on applique ces droits et « TO'nextcloud'@'localhost' » permet d'indiquer quel utilisateur bénéficiera de ces droits.

La quatrième ligne force le serveur à rechargé les droits pour appliquer les changements.

On a fini la configuration sur SQL on utilise la commande « EXIT » pour quitter le serveur MySQL

Avant d'installer Nextcloud il faut d'abord installer apache avec la commande suivante :

```
root@mgrosmann-pc:~# sudo apt install apache2
```

L'installation d'apache va nous permettre de configurer un site web sur notre adresse ip et par la même occasion le cloud local Nextcloud.

Maintenant qu'apache est installé, passons à l'installation de Nextcloud, il faut saisir la commande suivante :

```
wget https://download.nextcloud.com/server/releases/nextcloud-?.zip
```

La commande wget permet de télécharger un fichier/archive stocké(e) sur un site.

A la place du « ? » vous saisissez la syntaxe de la version de votre choix

Vous allez ensuite extraire l'archive vers le répertoire var/www afin de vous permettre d'y accéder depuis internet grâce à la commande :

```
sudo unzip nextcloud-?.zip -d /var/www
```

La commande « sudo unzip » permet de dézipper une archive depuis le terminal.

La commande « -d » permet de définir où les fichiers extraits de l'archive doivent être stockées.

Il faut le faire depuis le terminal puisqu'il faut être administrateur pour déposer des fichiers dans le répertoire /var/www et on ne peut pas être administrateur sur l'explorateur de fichiers.

Si on le dépose dans le répertoire /var/www c'est pour que le serveur cloud local Nextcloud soit accessible depuis notre adresse IP suivi de « /nextcloud ». Il s'agit du répertoire qui gère le site web de notre machine Ubuntu.

Il faut ensuite modifier des autorisations à nextcloud afin qu'il puisse modifier les fichiers grâce à la commande :

```
root@mgrosmann-pc:~# sudo chown -R www-data:www-data /var/www/nextcloud~
```

La commande « sudo chown -R » permet de donner les droits à nextcloud d'écrire dans le répertoire « /var/www/nextcloud » qui gère l'interface web de notre nextcloud.

Pour ce qui est de « www-data :www-data » www-data est un utilisateur système utilisé par des serveurs comme apache (qu'on utilise pour sql) qui se situe dans le groupe du même nom « www-data ». Cette commande permet de définir les droits de l'utilisateur « www-data » qui est dans le groupe « www-data ».

Vous allez ensuite modifier le fichier « nextcloud.conf » avec la commande :

```
root@mgrosmann-pc:~# sudo nano /etc/apache2/sites-available/nextcloud.conf
```

« .conf » est une extension semblable à « .cf » qui sert à stocker des données de configuration.

Le fichier doit ressembler à ca :

```
Alias /nextcloud "/var/www/nextcloud/"

<Directory /var/www/nextcloud/>
    Options +FollowSymlinks
    AllowOverride All

    <IfModule mod_dav.c>
        Dav off
    </IfModule>

    SetEnv HOME /var/www/nextcloud
    SetEnv HTTP_HOME /var/www/nextcloud
</Directory>
```

Vous devez activer le fichier de configuration avec la commande :

```
root@mgrosmann-pc:~# sudo a2ensite nextcloud.conf
```

Pour sauvegarder la configuration il faut redémarrer le serveur apache

```
root@mgrosmann-pc:~# sudo systemctl restart apache2
```

Par la suite pour nextcloud il faut installer php-curl :

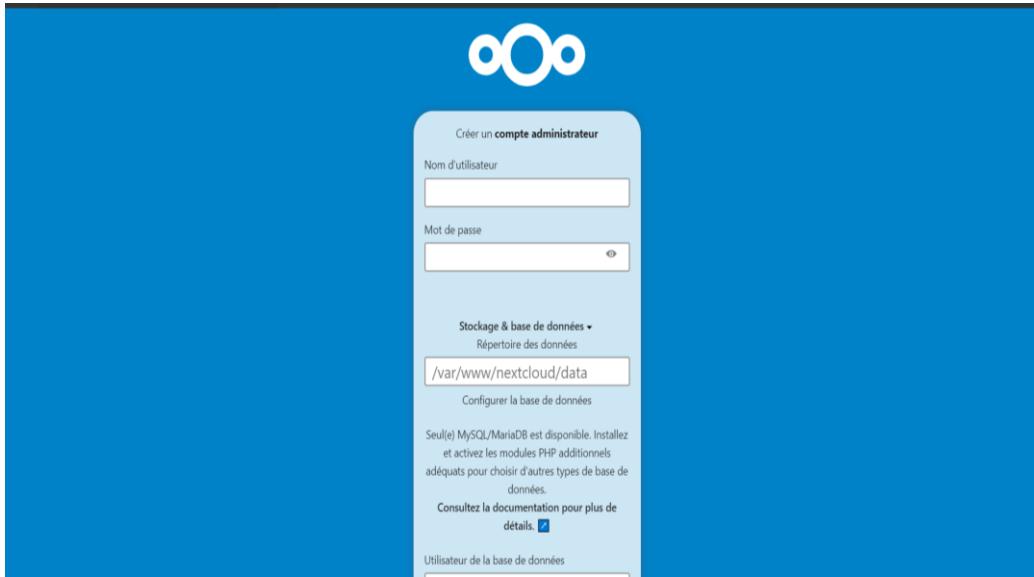
```
root@mgrosmann-pc:~# sudo apt install php-curl
```

L'extension php-curl ou PHP C-url va permettre à Nextcloud d'effectuer des requêtes http vers d'autres serveurs

Il faudra redémarrer le serveur apache précédemment cité.

Pour vous rendre sur votre cloud local saisissez 192.168.XXX.XXX(votre adresse ip trouvable avec la commande « ifconfig ») suivi de /nextcloud

Vous devrez tomber sur cette interface :



Connectez-vous avec l'utilisateur ajouté dans la base de données en descendant dans le bas de la page :

Utilisateur de la base de données

Mot de passe de la base de données

Nom de la base de données

Hôte de la base de données

localhost

Veuillez spécifier le numéro du port avec le nom de l'hôte (ex: localhost:5432).

Installer

Besoin d'aide ? [Lire la documentation](#)

Vous arriverez donc sur une page ressemblant à ça :

All files

Recent

Favorites

Shares

Tags

Shared to Circles

Deleted files

36.5 MB of 5 GB used

Files settings

Welcome to Nextcloud!

File could not be loaded. Please check your internet connection. **Reconnect**

Here you can add a description or any other info relevant for the folder. It will show as a "Readme.md" and in the web interface also embedded nicely up at the top.

Name	Size	Moamea
Documents	1.1 MB	21 days ago
Photos	5.4 MB	21 days ago
Templates	10.2 MB	21 days ago
Reasons to use Nextcloud.pdf	954 KB	21 days ago
Templates credits.md	2 KB	21 days ago
test.md	0 KB	seconds ago

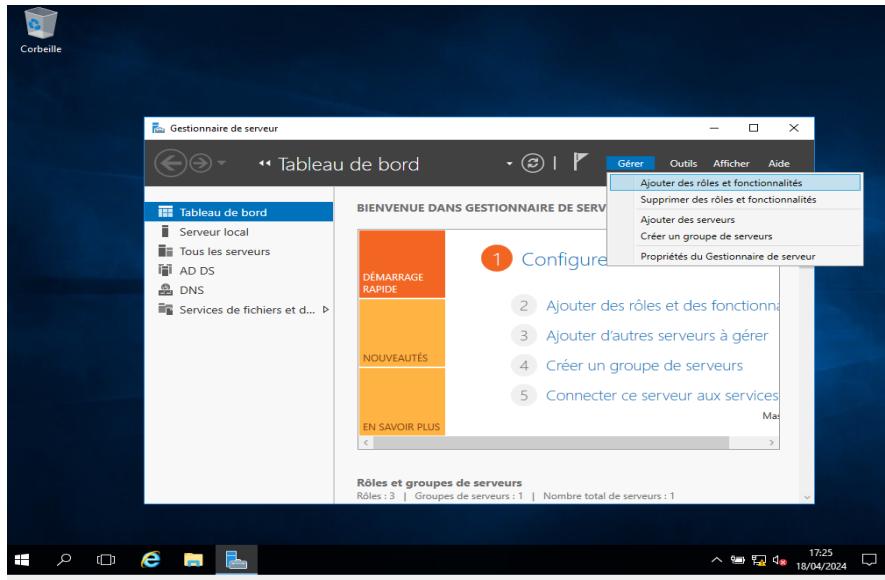
9.4 Configuration d'un active directory: Windows server

Premièrement Windows Server est un système d'exploitant semblable à Windows 10 permettant de gérer des tâches administratives vis-à-vis de la gestion des serveurs et des services de réseau.

Un Active Directory est un service d'annuaire permettant de stocker des informations sur des objets tels que les utilisateurs, les groupes et ordinateurs. Ils permettent aussi de créer un « domaine » où sera stocké les objets précédemment cités.

Pour configurer un Active Directory il faudra une version de Windows server 2016.

Dans le gestionnaire de serveur qui s'ouvre automatiquement au démarrage sélectionner « Gérer » puis « ajouter des rôles et des fonctionnalités



Il faudra laisser les choix par défauts et sélectionner votre serveur.

Avant de commencer

Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.

Pour supprimer des rôles, des services de rôle ou des fonctionnalités : Démarrer l'Assistant de Suppression de rôles et de fonctionnalités

Avant de continuer, vérifiez que les travaux suivants ont été effectués :

- Le compte d'administrateur possède un mot de passe fort
- Les paramètres réseau, comme les adresses IP statiques, sont configurés
- Les dernières mises à jour de sécurité de Windows Update sont installées

Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.

Cliquez sur Suivant pour continuer.

Ignorer cette page par défaut

< Précédent Suivant > Installer Annuler

Selectionner le type d'installation

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

Installation basée sur un rôle ou une fonctionnalité Configuez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.

Installation des services Bureau à distance Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent Suivant > Installer Annuler

Selectionner le serveur de destination

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

Sélectionner un serveur du pool de serveurs

Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :	Nom	Adresse IP	Système d'exploitation
	mgrosmann-dc.mgrosmann.local	192.168.1.55	Microsoft Windows Server 2016 Standard

1 ordinateur(s) trouvé(s)

Cette page présente les serveurs qui exécutent Windows Server 2012 ou une version ultérieure et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors connexion et les serveurs nouvellement ajoutés dont la collecte de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

Il faudra ensuite sélectionner « AD DS » et « DNS »

Selectionner des rôles de serveurs

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

Rôles

Accès à distance	Description
Attestation d'intégrité de l'appareil	L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et générée en continu. Le service d'accès à distance (RAS) fournit des services VPN (réseau virtuel privé) et de connectivité de site à site (filiale ou nuplex). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réseau.
Expérience Windows Server Essentials	
Hyper-V	
MultiPoint Services	
Serveur de télécopie	
Serveur DHCP	
<input checked="" type="checkbox"/> Serveur DNS (Installé)	
Server Web (IIS)	
Service Guardian hôte	
<input checked="" type="checkbox"/> Services AD DS (Installé)	
Services AD LDS (Active Directory Lightweight Directory Services)	
Services AD RMS (Active Directory Rights Management Services)	
Services Bureau à distance	
Services d'activation en volume	
Services de certification Active Directory	
Services de déploiement Windows	
Services de fédération Active Directory (AD FS)	

< Précédent Suivant > Installer Annuler

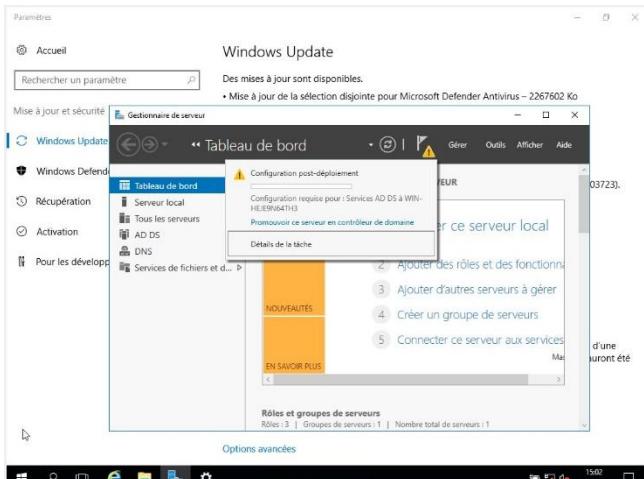
L'AD DS ou Active Directory Domain est un élément principal de l'active directory.

C'est grâce à lui que l'Active Directory va pouvoir stocker les informations sur l'objet.

Le DNS ou Domain Name System permet de traduire des noms de domaines en adresse IP.

Dans un Active Directory il va associer les noms de domaines des machines à leurs Adresses IP correspondantes.

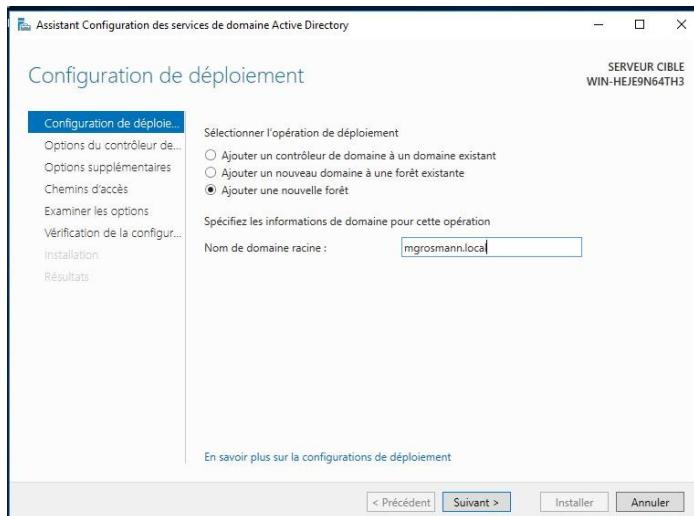
Suite à cela il faudra sélectionner le drapeau en haut de la fenêtre en fait de promouvoir ce serveur en domaine de contrôle et un chargement se produira.



Le fait de promouvoir ce serveur en domaine de contrôle va notamment permettre d'ajouter des objets comme les utilisateurs au sein du domaine.

Vous arriverez sur une nouvelle fenêtre, il faudra sélectionner « ajouter une nouvelle forêt » et entrer un nom pour le nom de domaine racine.

Dans un Active Directory, une « forêt » est l'endroit où sera stocker tous les domaines de l'Active Directory.



Après cela un mot de passe et nom de domaine NETBIOS sera demandé :

Le nom de domaine est simplement le nom du domaine qu'on est en train de créer.

The image contains two side-by-side screenshots of the 'Assistant Configuration des services de domaine Active Directory' wizard.

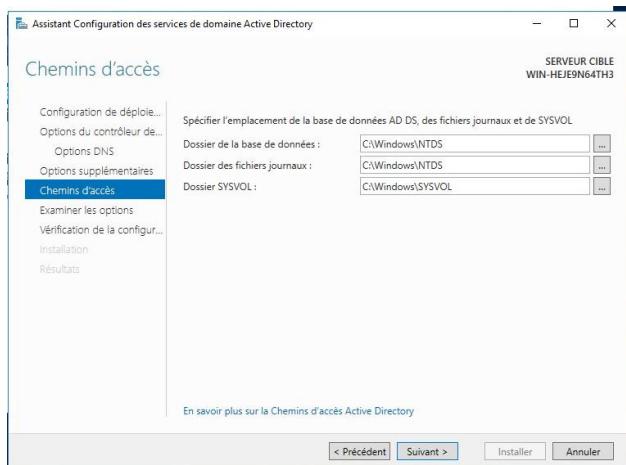
Left Window (Options du contrôleur de domaine):

- Title: 'Assistant Configuration des services de domaine Active Directory' - 'Options du contrôleur de domaine'.
- Section: 'Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine'.
 - Niveau fonctionnel de la forêt: Windows Server 2016
 - Niveau fonctionnel du domaine: Windows Server 2016
- Section: 'Spécifier les fonctionnalités de contrôleur de domaine'.
 - Serveur DNS (Domain Name System)
 - Catalogue global (GC)
 - Contrôleur de domaine en lecture seule (RODC)
- Section: 'Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)'.
 - Mot de passe:
 - Confirmer le mot de passe:
- Bottom: '< Précédent', 'Suivant >', 'Installer', 'Annuler'.

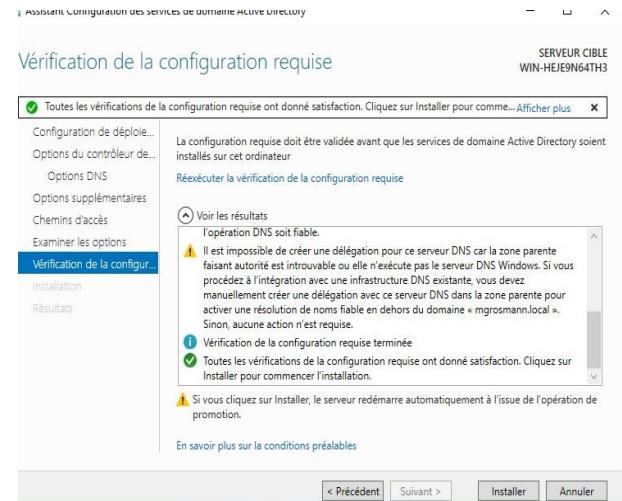
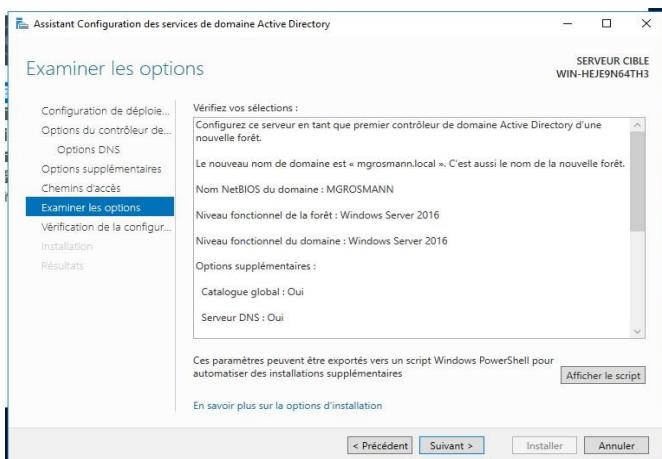
Right Window (Options supplémentaires):

- Title: 'Assistant Configuration des services de domaine Active Directory' - 'Options supplémentaires'.
- Section: 'Vérifiez le nom NetBIOS attribué au domaine et modifiez-le si nécessaire'.
 - Le nom de domaine NetBIOS: MGROSMANN
- Bottom: '< Précédent', 'Suivant >', 'Installer', 'Annuler'.

Pour finir vous aurez le choix de définir le dossier où seront stockés les fichiers liés à l'active directory



Afin de finaliser l'installation il faudra confirmer que les informations sont correctes et si oui procéder à l'installation.



Vous serez déconnectez quand l'installation sera finalisée.

Passons maintenant à la configuration sur Windows 10.

La machine Windows server 2016 et Windows 10 doivent tous deux être en réseau interne afin que les deux machines puissent se voir et que la machine Windows 10 puisse faire partie du domaine créé sur Windows server. Cela nécessite aussi que les 2 machines soient dans le même sous-réseau (ex : 192.168.1.0)

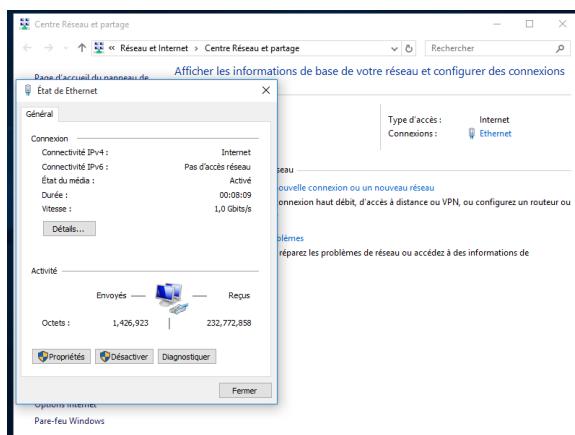
Avant toute chose il est impératif de définir en serveur DNS préféré l'adresse IP du Windows server.

A chaque fois que sur la machine Windows 10 tentera une connexion sur un compte créer sur l'Active Directory, il devra récupérer les informations via le Windows server.

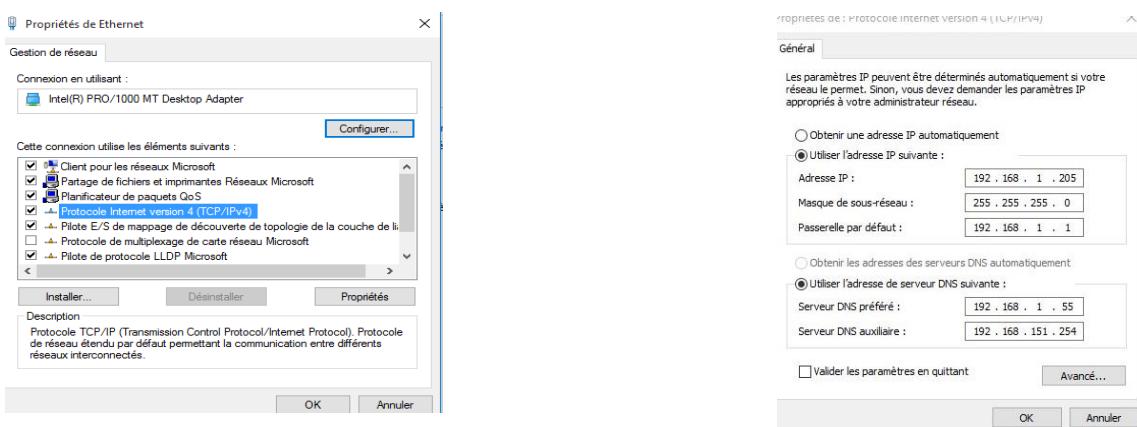
Pour cela : effectuer un clic droit sur l'icône réseau, sélectionner « ouvrir le centre réseau et partage,



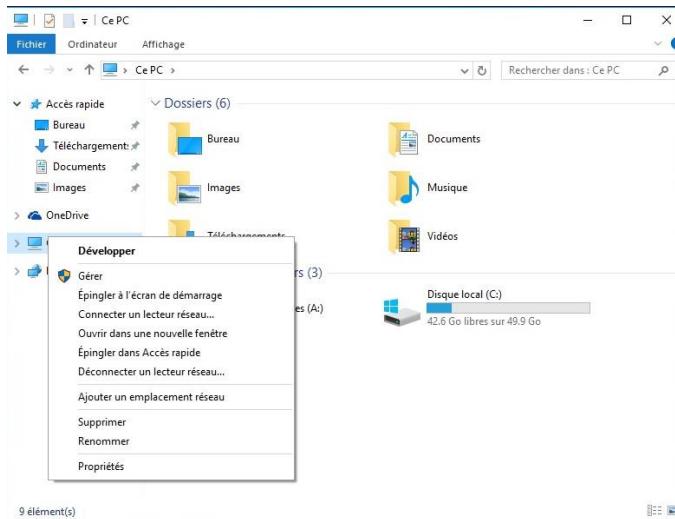
Ensuite sélectionner « Ethernet puis propriétés sur la nouvelle fenêtre générée



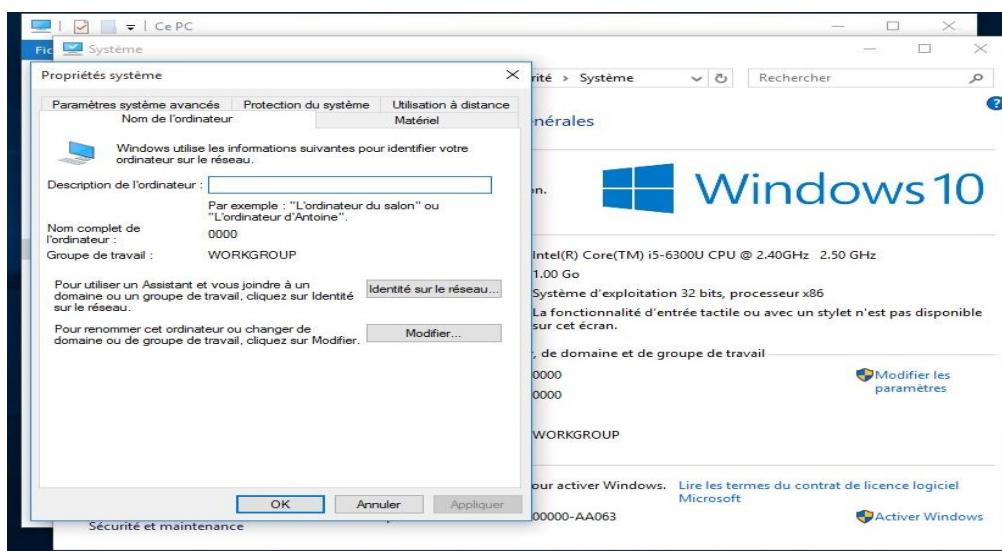
Ensute il ne reste plus qu'a sélectionner « protocole internet Version 4 » et à définir l'adresse IP du Windows server en serveur DNS préféré



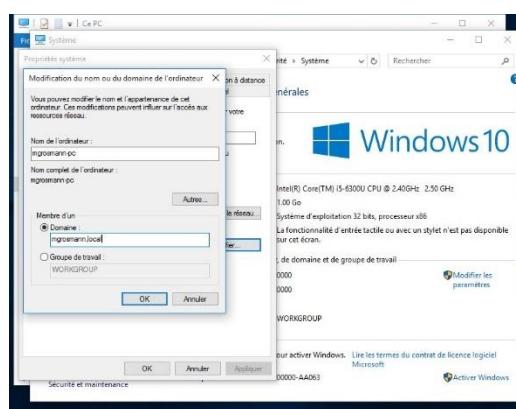
Il faudra ouvrir un explorateur de fichier, effectuer un clic droit sur ce pc puis propriétés



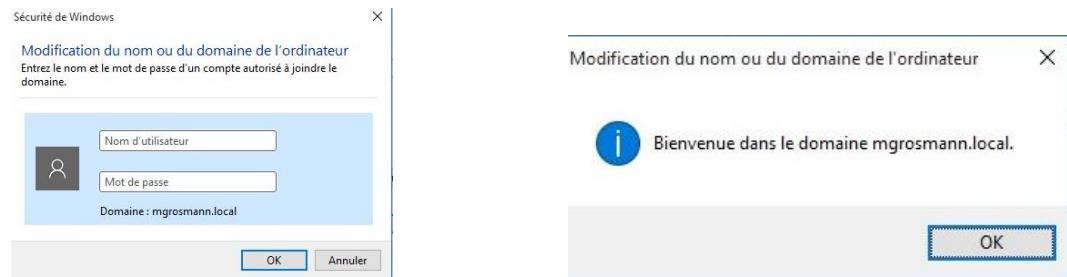
Il faudra ensuite sélectionner « modifier les paramètres » puis sur la nouvelle fenêtre « modifier »



Vous devrez ensuite sélectionner nom de domaine puis saisir le nom de domaine racine défini sur le Windows server

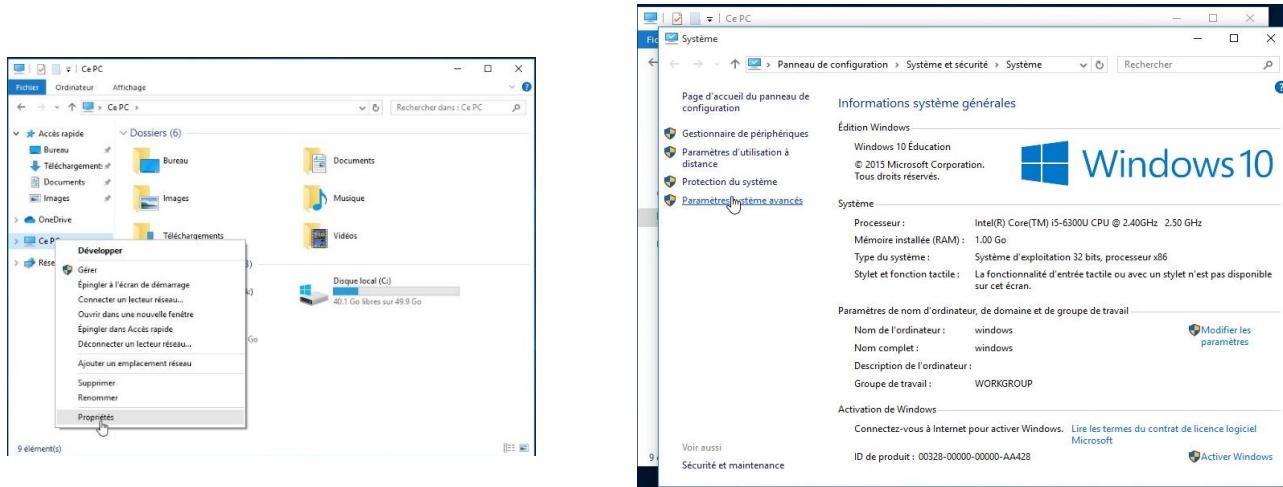


Si la configuration est correcte il faudra se connecter avec le compte administrateur du Windows server afin d'ajouter le domaine a la machine Windows 10.

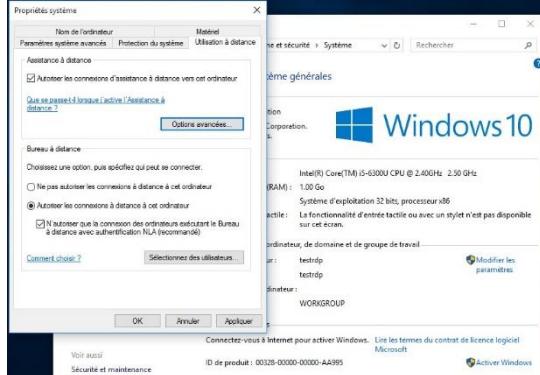


9.5 Configuration D'une connexion à Distance : RDP

Pour commencer il faut ouvrir un explorateur de fichier et effectuer un clic droit sur « Ce Pc » puis sélectionner propriétés ensuite sélectionner « Paramètres système avancés »



Après cela allez sur l'onglet « Utilisation à Distance » et cocher « Autoriser les connexions à distance à cet ordinateur »



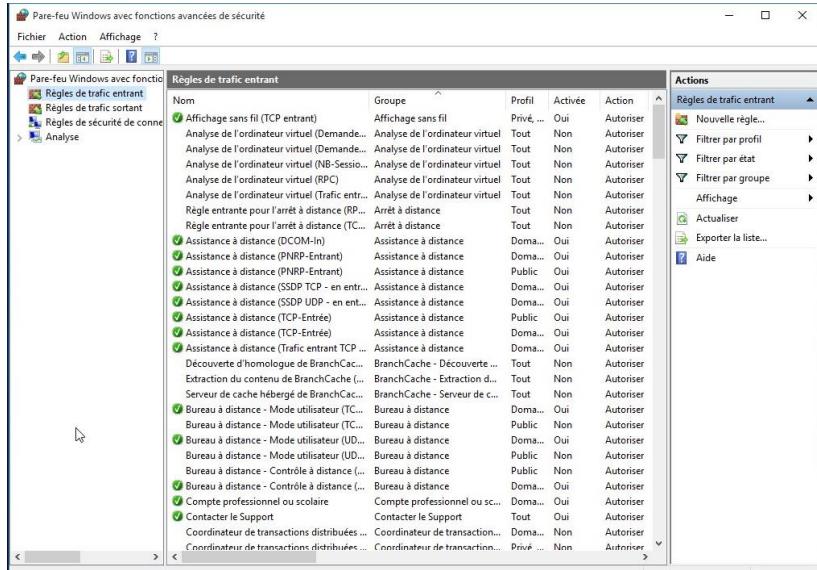
Maintenant nous allons rajouter une règle de pare feu pour permettre cette connexion à distance.

Le Pare-Feu Windows protège votre ordinateur des attaques frauduleuses, Il est fortement conseillé de le laisser activer.

Par défaut le port 3389 qui est utilisé pour les connexions à distance RDP n'est pas ouvert.

On va donc ajouter une règle pour permettre le contrôle à distance.

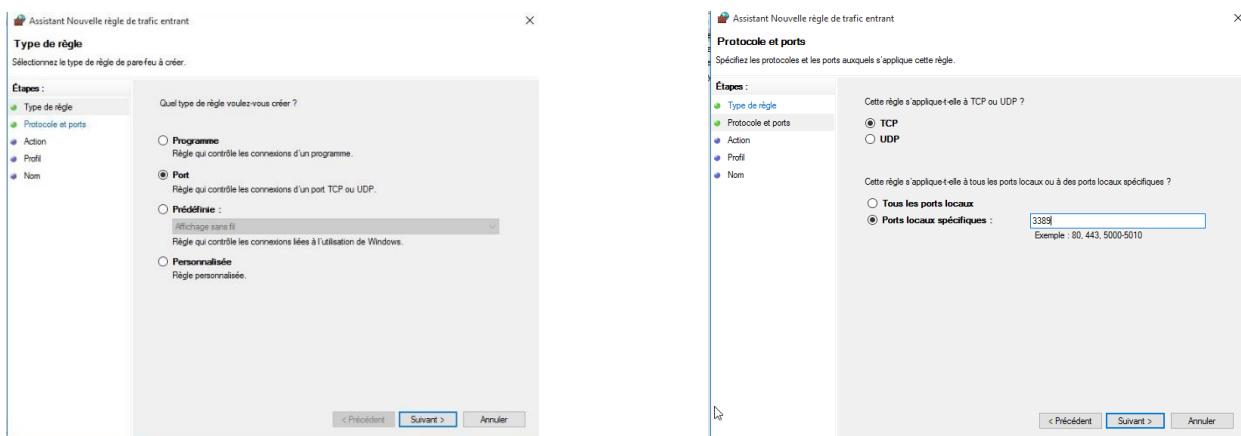
Aller sur le pare feu Windows et aller sur la section « règles de trafic entrant » puis sélectionner « Nouvelle règle »



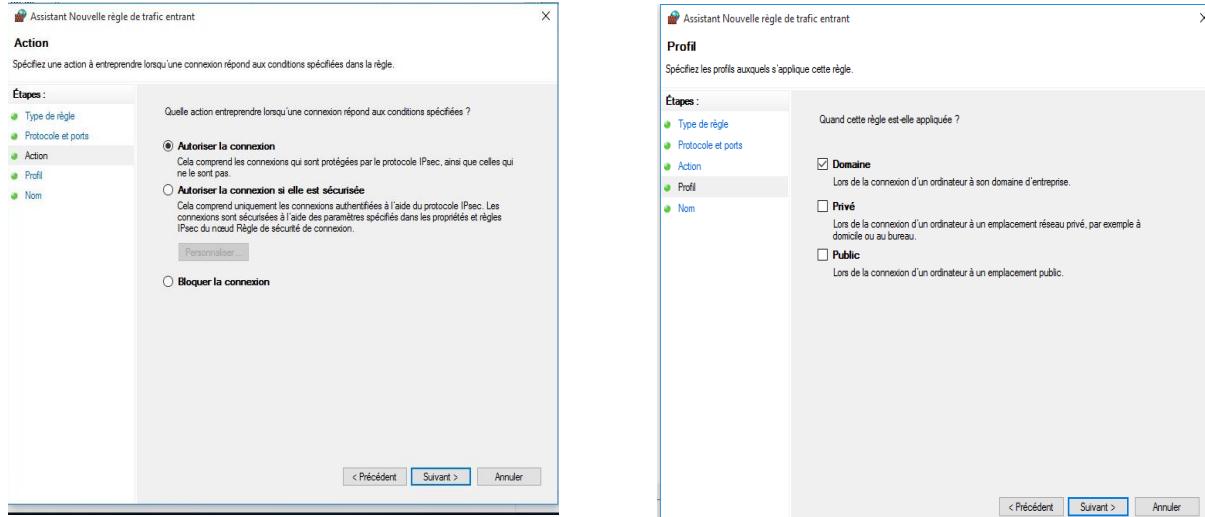
Sélectionnez « Port » puis sur la nouvelle étape sélectionnez « TCP » puis mettez « 3389 » en Port

LE TCP ou Transmission Control Protocol est un protocole de transfert permettant une transmission sans faille des données.

Dans une règle RDP il est préférable de choisir le TCP car il est plus fiable que l'UDP mais surtout plus adapté puisque c'est un protocole plus orienté pour la connexion contrairement à l'UDP.



Pour la prochaine étape il faut laisser « Autoriser la connexion » cocher puis pour l'étape suivante afin d'empêcher des attaques frauduleuses décocher tout sauf Domaine



Il vous reste plus qu'à donner un nom à cette règle et la configuration sera désormais finalisé.

9.6 Configuration d'un Serveur DHCP : Pf sense

Pf sense est un système d'exploitation basée sur un autre système d'exploitation : FreeBSD.

Il permet la mise en place de routeur ou pare-feu. Associé à une machine Windows 10, Ubuntu ou autre il va permettre de donner un accès à internet tout en filtrant les connexions pour protéger une machines des cyber-attaques.

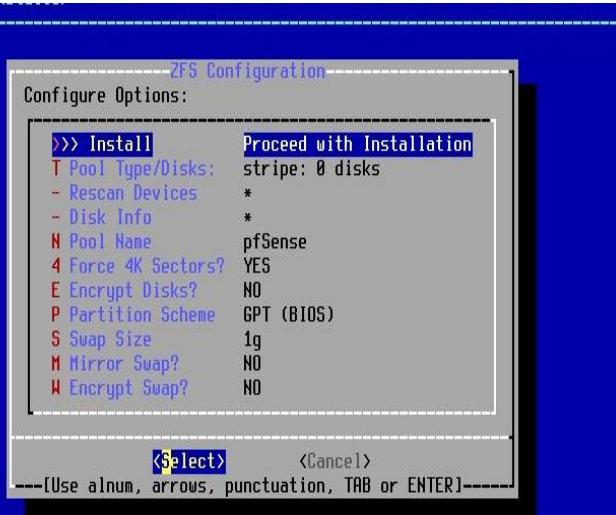
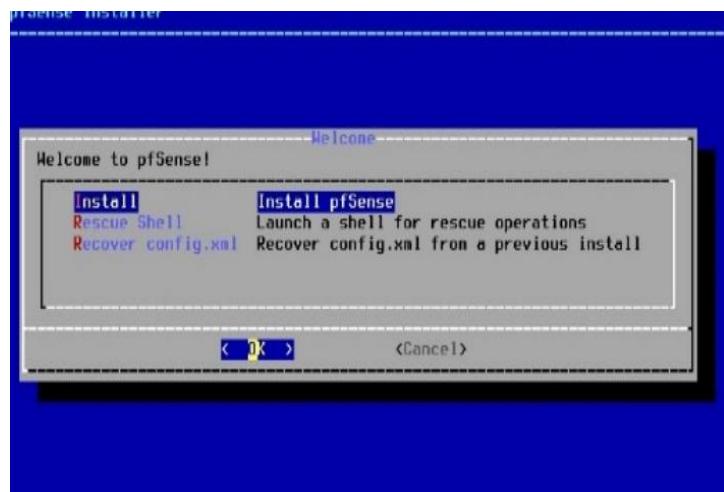
Avant de commencer l'installation assurez d'avoir deux cartes réseaux :

Une en accès par pont permettant de se connecter à l'extérieur en WAN à partir de la carte réseau de l'ordinateur

Une deuxième en réseau interne afin de communiquer avec les autres machines virtuelles.



Pour le début de l'installation de Pf-Sense il va falloir laisser les choix par défauts :



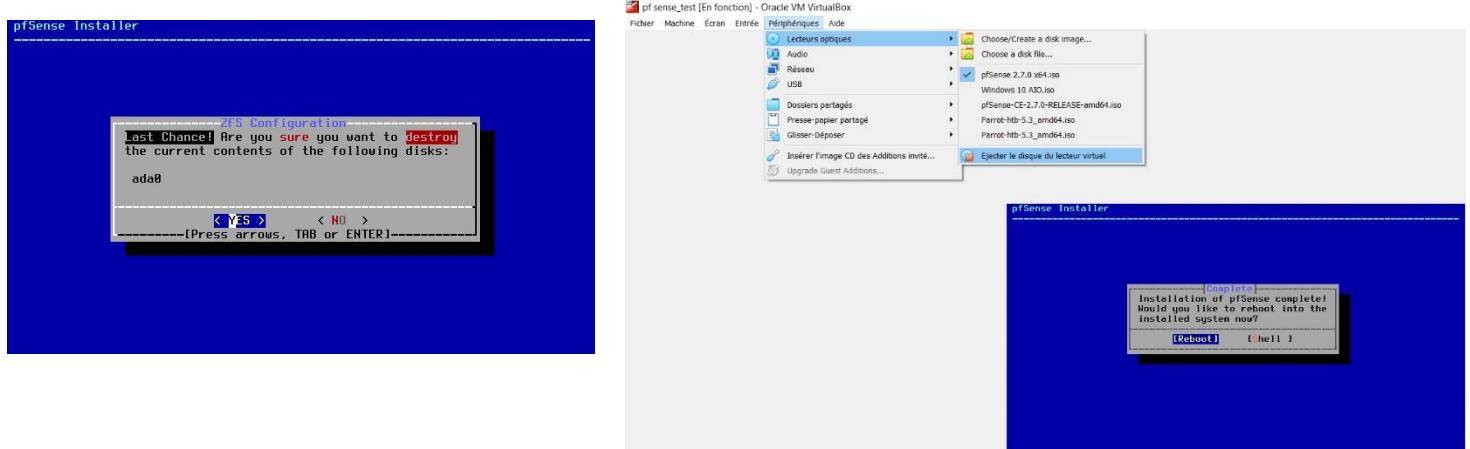
Pendant l'installation vous avez l'opportunité de pf sense de créer un RAID afin d'améliorer la tolérance à la panne (ex : RAID 1) ou les performances (RAID 0)

Ensute vous allez sélectionnez sur espace afin de confirmer le disque dur sur lequel vous allez installer pf sense



Vous allez devoir confirmer que vous souhaitez détruire le contenu du disque pour l'installation puis vous allez pouvoir redémarrer tout en pensant à éjecter le disque

Le disque doit être éjecter puisqu'il permet l'installation de pf sense mais maintenant que l'installation est finie il n'est plus nécessaire.



A la fin du redémarrage vous tomberez sur un écran ressemblant à ça :

```
Starting syslog...done.
Starting CRON... done.
pfSense 2.7.0-RELEASE amd64 Wed Jun 28 03:53:34 UTC 2023
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 723cce0c0008d842a68e

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.1.49/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■
```

Pour configurer le serveur DHCP ou il faut configurer l'adresse LAN qu'elle soit dans le même réseau ou non que l'adresse WAN.

L'adresse IP du LAN ou Local Area Network correspond à l'adresse IP utilisé dans un réseau local

L'adresse IP du Wan ou Wide Area Network correspond à l'adresse IP utilisé dans un réseau étendu afin de se connecter vers l'extérieur (Internet par exemple).

Le DHCP ou Dynamic Host Configuration Protocol permet d'attribuer une adresse IP automatiquement à une machine dans un réseau parmi celles disponibles et pas encore utilisé. Cette solution permet d'offrir une connexion internet sans devoir configurer une adresse IP manuellement mais aussi d'éviter les conflits d'Adresse IP.

Pour modifier les adresses IP WAN ou LAN il faut entrer 2, dans notre cas on veut modifier l'adresse LAN donc il faut entrer 2, ensuite vous aurez le choix entre avoir une adresse automatique avec le DHCP ou en entrer une manuellement, il faut en saisir une manuellement.

```
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 2
```

On peut laisser « 192.168.1.1 » si l'adresse WAN est dans un sous réseau différent, dans notre cas on va changer le sous réseau

```
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.15.1
```

Le sous réseau correspond au 3^{ème} octet d'une adresse IP (par exemple dans l'adresse IP « 192.168.1.5 » le sous réseau est 1)

Il faudra mettre 24 en CIDR ensuite.

Le CIDR est défini par le nombre de bit disponible et le masque de sous réseau.

Dans cette exemple il reste 8 bit donc le CIDR est de 24.

```
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8
Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24
```

Ensuite on nous demandera une « upstream gateway adress » ou une adresse passerelle amont. Par défaut on n'en mettra aucune

Une adresse passerelle en amont est l'adresse IP de la passerelle qui se trouve du côté du réseau le plus éloigné du réseau local.

```
For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
```

Viens la configuration du DHCP.

On désactivera la DHCP6 et entrera aucune adresse ipv6

```
Configure IPv6 address LAN interface via DHCP6? (y/n) n
Enter the new LAN IPv6 address. Press <ENTER> for none:
>
```

Ensuite on active le serveur DHCP sur le LAN et on indique la plage d'adresse IP que le serveur distribue en indiquant la première et dernière adresse IP.

La plage d'adresse IP correspond à un certain groupe d'adresse IP qui commence avec une adresse IP de départ (sur le capture au-dessus 192.168.15.10) et avec une adresse IP de fin (sur le capture au-dessus 192.168.15.20)

```
Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 192.168.15.10
Enter the end address of the IPv4 client address range: 192.168.15.20
Disabling IPv6 DHCPD...
```

Pour finaliser la configuration on laisse le protocole HTTPS pour le site web pfsense.

```
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Le protocole https ou Hyper Text Transfer Protocol Security est une extension du protocole http. Il propose une sécurisation des données supérieure au protocole https.

Actuellement Le protocole http est assez minoritaire, les sites internet privilégiant le protocole https.

La configuration est à présent terminée même si on peut encore la personnaliser sur l'interface web depuis Windows 10.

Si la configuration est correcte vous aurez une adresse IP qui sera automatique dans le même sous réseau que le pf-sense.

Vous pouvez vérifier en lançant l'invite de commande et en utilisant la commande ipconfig :

```
Microsoft Windows [version 10.0.10240]
(c) 2015 Microsoft Corporation. Tous droits réservés.

C:\Users\vboxuser>ipconfig

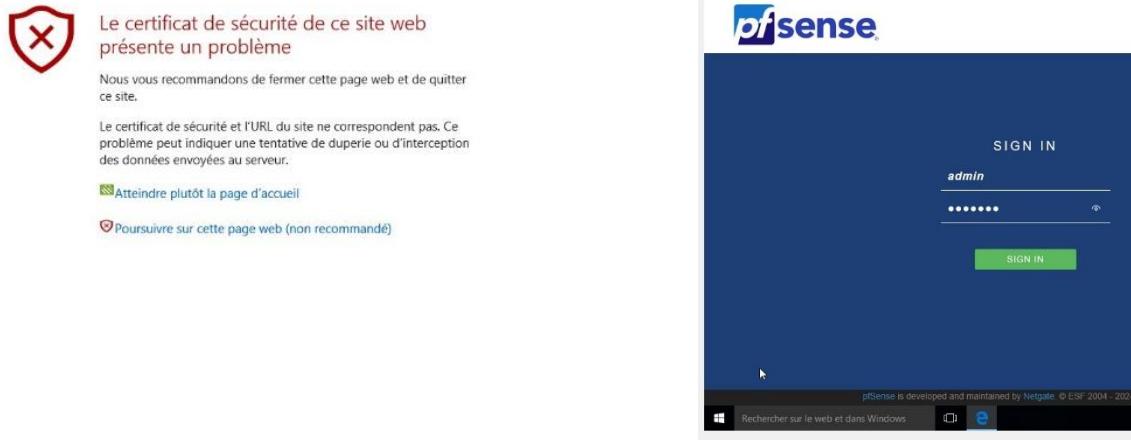
Configuration IP de Windows

Carte Ethernet Ethernet :
  Suffixe DNS propre à la connexion... : home.arpa
  Adresse IPv6 de liaison locale... : fe80::1c1c:973e:e140:ed9b%3
  Adresse IPv4... : 192.168.15.10
  Masque de sous-réseau... : 255.255.255.0
  Passerelle par défaut... : 192.168.15.1

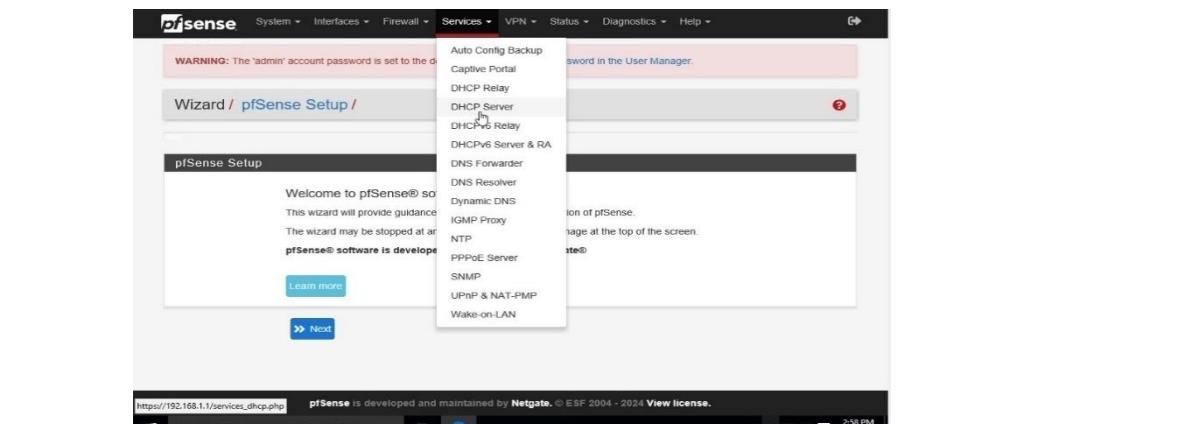
Carte Tunnel isatap.home.arpa :
  Statut du média... : Média déconnecté
  Suffixe DNS propre à la connexion... : home.arpa

Carte Tunnel Teredo Tunneling Pseudo-Interface :
  Suffixe DNS propre à la connexion... :
  Adresse IPv6... : 2001:0:2851:782c:20d6:75dd:dabc:8551
  Adresse IPv6 de liaison locale... : fe80::20d6:75dd:dabc:8551%2
  Passerelle par défaut... :
```

Vous allez maintenant entrer l'adresse LAN du pf sense pour pouvoir accéder a l'interface web en entrant « admin » comme identifiant et « pfsense » comme mot de passe



Une fois connecter il faut se rendre sur « services » puis « DHCP server »




On peut observer la plage d'adresse IP précédemment configurer qu'on peut modifier ou non.

La partie intéressante de la configuration est la configuration du délai d'expiration.

En effet puisqu'elle n'est pas configurable depuis la machine pf sense.

Par défaut elle dure minimum 7200 secondes(2h) et au maximum 86400 secondes(24h)

Default lease time	<input type="text" value="7200"/>
This is used for clients that do not ask for a specific expiration time. The default is 7200 seconds.	
Maximum lease time	<input type="text" value="86400"/>
This is the maximum lease time for clients that ask for a specific expiration time. The default is 86400 seconds.	

Le délai d'expiration correspond au temps auquel une machine peut conserver l'adresse IP que lui attribuer le serveur DHCP. Après ce délai, le serveur DHCP lui attribuera une nouvelle adresse IP.

La configuration est maintenant terminée pour sauvegarder les changements il faut sélectionner « Save » en bas de la page afin de sauvegarder les changements. Vous aurez un message de confirmation.



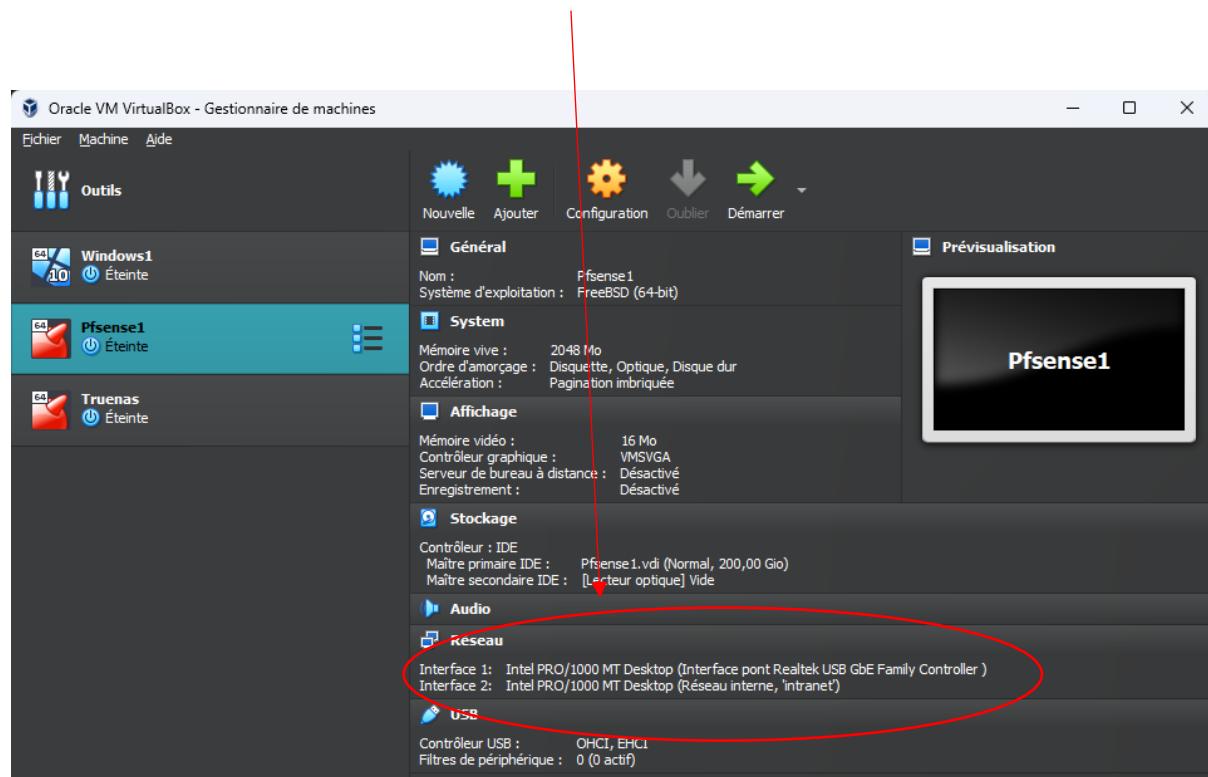
9.7 Rapport Détailé portail captif pfSense

Le portail captif est une application chargée de contrôler et de gérer de manière automatisée l'accès des utilisateurs aux réseaux wifi ; qu'ils soient publics ou privés. Ainsi, les portails captifs sont couramment utilisés dans les réseaux à accès ouvert. Ces mêmes réseaux wifi disponibles dans les magasins, les centres commerciaux, les hôpitaux, les aéroports, etc.

Le portail captif permet donc aux administrateurs du réseau wifi de fournir un accès à l'internet. Au préalable, l'utilisateur doit y renseigner les informations permettant de l'identifier. Par le biais de son nom, de son numéro de téléphone, de son adresse électronique ou encore de ses réseaux sociaux.

Pour commencer, nous devons configurer la machine virtuelle en utilisant les paramètres adéquats pour son bon fonctionnement. Le plus important de la configuration va être la partie réseau :

Il va falloir deux interfaces réseau, la première en accès par pont pour notre réseau étendu WAN, permettant de communiquer avec l'extérieur. En second, notre réseau local LAN, sans utiliser l'accès à internet.

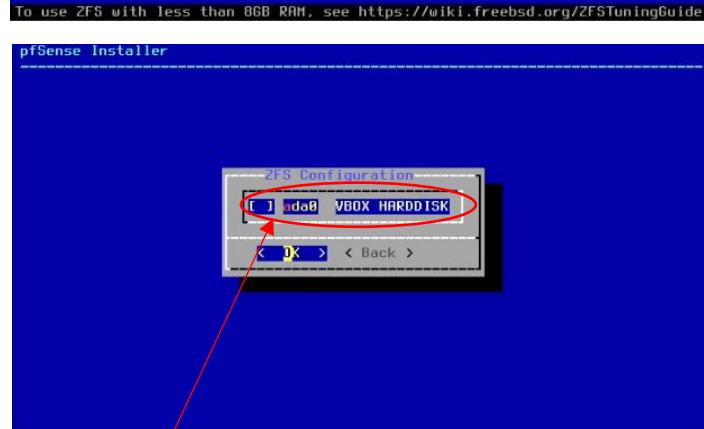
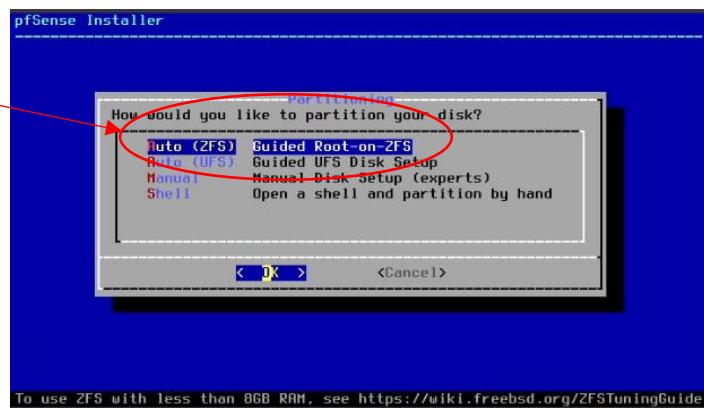


Nous pouvons dès à présent démarrer la machine virtuelle.

Passons à l'installation de pfSense



Une installation simplifiée,
pour les débutants



Disque où sera installé pfSense

Après avoir éjecté le disque d'installation, on peut démarrer notre pfSense

```

FreeBSD/amd64 (pfSense.home.arpa) (ttyv1)

login: root
Password:
Login incorrect
login: admin
Password:
VirtualBox Virtual Machine - Netgate Device ID: f9f63a42ed8e45ef5865

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 192.168.0.13/24
LAN (lan)      -> em1      -> v4: 20.0.0.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: ■

```

On arrive sur cette interface, avec plusieurs commandes affectées à des chiffres permettant de configurer notre pfSense. En premier, il faut être bien sûr que le WAN est sur l'interface réseau en accès par pont et le LAN sur l'interface en réseau interne. On peut voir sur la capture d'écran que c'est bien le cas.

On configure le réseau local LAN en entrant son adresse IP choisie (20.0.0.254 dans l'exemple ci-dessous), son masque (255.255.255.0 ou /24 dans l'exemple ci-dessus également), la mise en place d'un réseau LAN IPV6 n'est pas nécessaire.

Adresse IPV4 LAN

```

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1)

Enter the number of the interface you wish to configure: 2
Configure IPv4 address LAN interface via DHCP? (y/n) n
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 20.0.0.254

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0 = 16
      255.0.0.0 = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) ■

```

Masque

Mise en place d'un DHCP :

```
> 20.0.0.254
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
      255.255.0.0   = 16
      255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) y
Enter the start address of the IPv4 client address range: 20.0.0.10
Enter the end address of the IPv4 client address range: 20.0.0.30
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Plages d'adresses IP

La mise en place d'un DHCP permettra aux machines connectées au pfSense de prendre des adresses IP comprises dans la plage donnée ci-dessus. Par exemple, si une machine est connectée au pfSense, son adresse IP sera 20.0.0.10, la machine suivante 20.0.0.11, la machine d'après 20.0.0.12 etc...

Ce sera possible jusqu'à ce qu'une machine prenne l'adresse 20.0.0.30, après cela non car la plage d'adresses IP affectables sur le DHCP s'arrête à 20.0.0.30, dans l'exemple donné.

Maintenant le pfSense est configuré, nous pouvons passer côté machine. Pour appliquer les paramètres IP du pfSense, il faut taper la commande ipconfig /renew dans le terminal.

```
invite de commandes
Microsoft Windows [version 10.0.19045.4291]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\vboxuser>ipconfig /renew

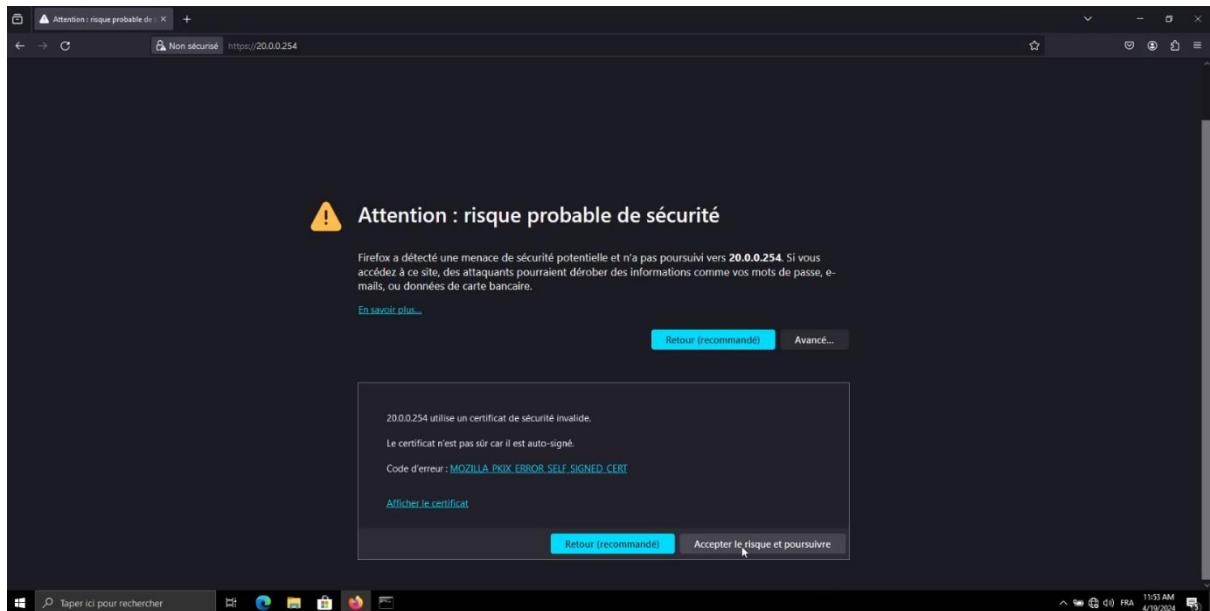
Configuration IP de Windows

Carte Ethernet Ethernet 2 :

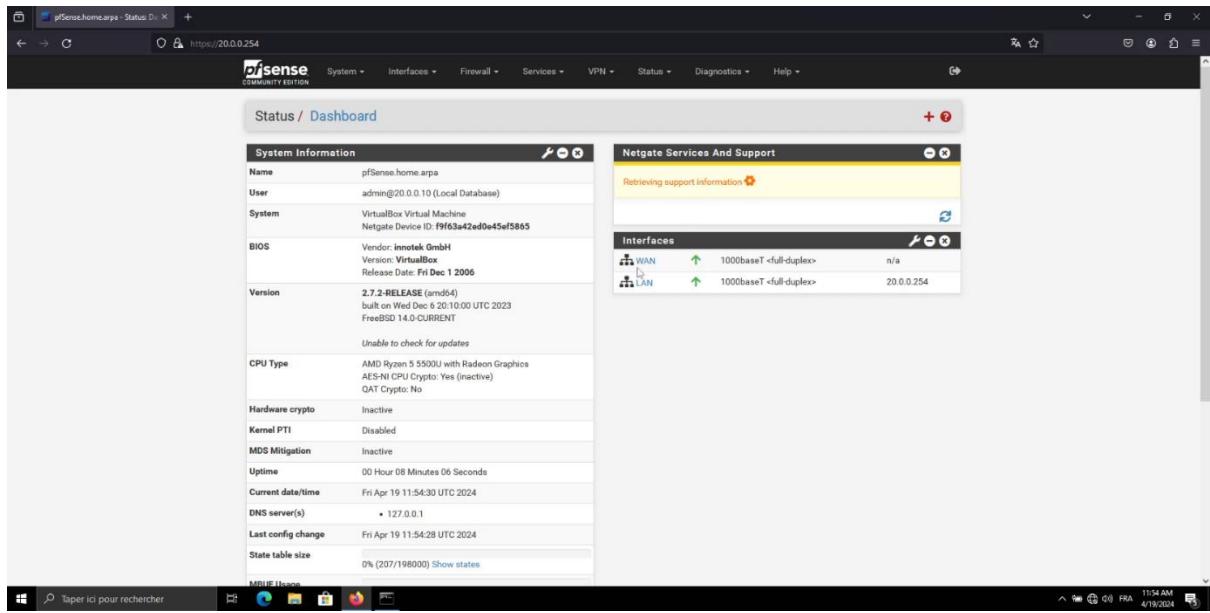
    Suffixe DNS propre à la connexion . . . : home.arpa
    Adresse IPv6 de liaison locale. . . . . : fe80::fe1f:52c5:7563:c15d%7
    Adresse IPv4. . . . . : 20.0.0.10
    Masque de sous-réseau. . . . . : 255.255.255.0
    Passerelle par défaut. . . . . :
```

Ici apparaissent les paramètres IP de la machine, on voit bien qu'elle a appliqué ceux du pfSense.

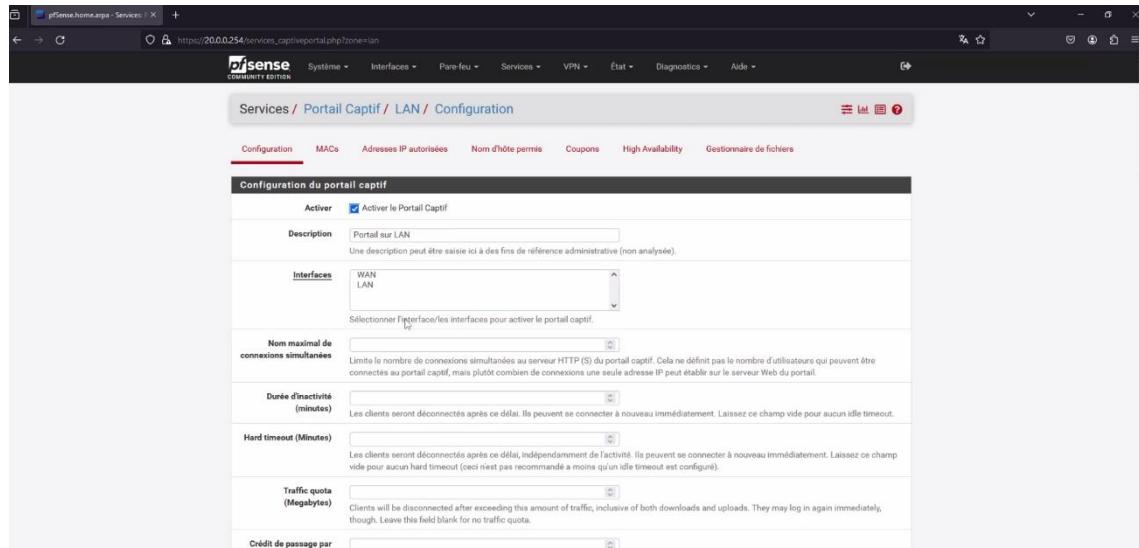
A présent tout est configuré et on peut accéder à l'interface pfSense sur son navigateur en tapant l'adresse IP LAN du pfSense donc 20.0.0.254 dans cet exemple. Le navigateur affiche un problème de sécurité, il faut accepter le risque et poursuivre.



On accède au dashboard de pfSense en ayant entré les informations de connexions admin et pfsense pour le mot de passe.



Nous pouvons passer à la mise en place d'un portail captif



Dans la section services/Portail Captif/LAN/Configuration, on choisit l'interface LAN et la méthode d'authentification « Use an authentication backend ».

Maintenant on peut créer notre utilisateur du portail captif avec les paramètres que l'on souhaite. Lorsque que l'utilisateur sera sur la page de connexion pfSense, il rentrera ses identifiants et il sera connecté.

pfSense.home.apa - Système +

https://20.0.0.254/system_usermanager.php?act=new

Propriétés utilisateur

Défini par	USER
Désactivé	<input type="checkbox"/> Cet utilisateur ne peut pas s'authentifier
Nom d'utilisateur	Thomas
Mot de passe	*****
Nom complet	Thomas Poussin
Date d'expiration	Laissez vide si le compte ne doit pas expiration, 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	admins <input type="checkbox"/> Pas un membre de <input type="checkbox"/> Membre de Déplacez vers la liste "Membre de" Déplacez vers la liste "Non membre de" <small>Maintenez la touche CTRL (PC)/COMMAND (Mac) enfoncée pour sélectionner plusieurs éléments.</small>
Certificat	Aucune autorité de certification privée n'a été trouvée. Une autorité de certification privée est requise pour créer un nouveau certificat d'utilisateur.

Système / Gestionnaire d'usagers / Utilisateurs

Utilisateurs	Groupes	Paramètres	Serveurs d'authentification															
Utilisateurs																		
<table border="1"> <thead> <tr> <th>Nom d'utilisateur</th> <th>Nom complet</th> <th>État</th> <th>Groupes</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Thomas</td> <td>thomas_pouss</td> <td>✓</td> <td></td> <td> </td> </tr> <tr> <td><input type="checkbox"/> admin</td> <td>System Administrator</td> <td>✓</td> <td>admins</td> <td></td> </tr> </tbody> </table>	Nom d'utilisateur	Nom complet	État	Groupes	Actions	<input checked="" type="checkbox"/> Thomas	thomas_pouss	✓		 	<input type="checkbox"/> admin	System Administrator	✓	admins				
Nom d'utilisateur	Nom complet	État	Groupes	Actions														
<input checked="" type="checkbox"/> Thomas	thomas_pouss	✓		 														
<input type="checkbox"/> admin	System Administrator	✓	admins															
				 Ajouter Supprimer														

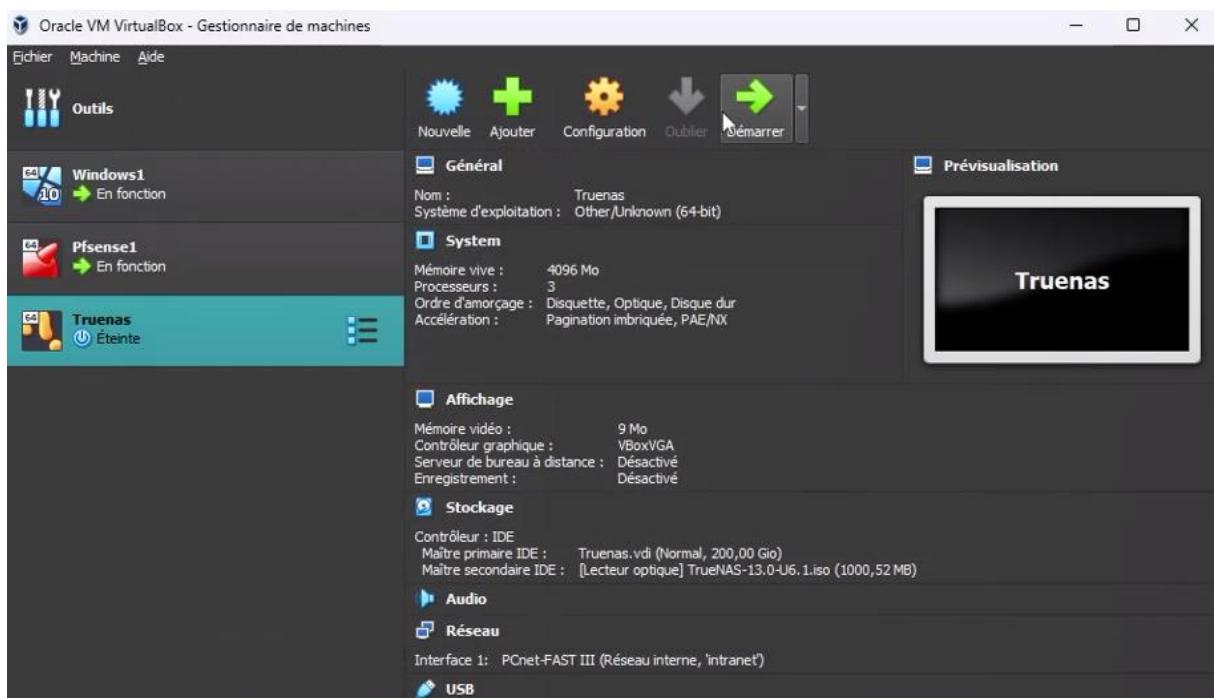
Utilisateurs du portail captif

Le portail captif est en place, avec un utilisateur créé, la mise en place est donc terminée.

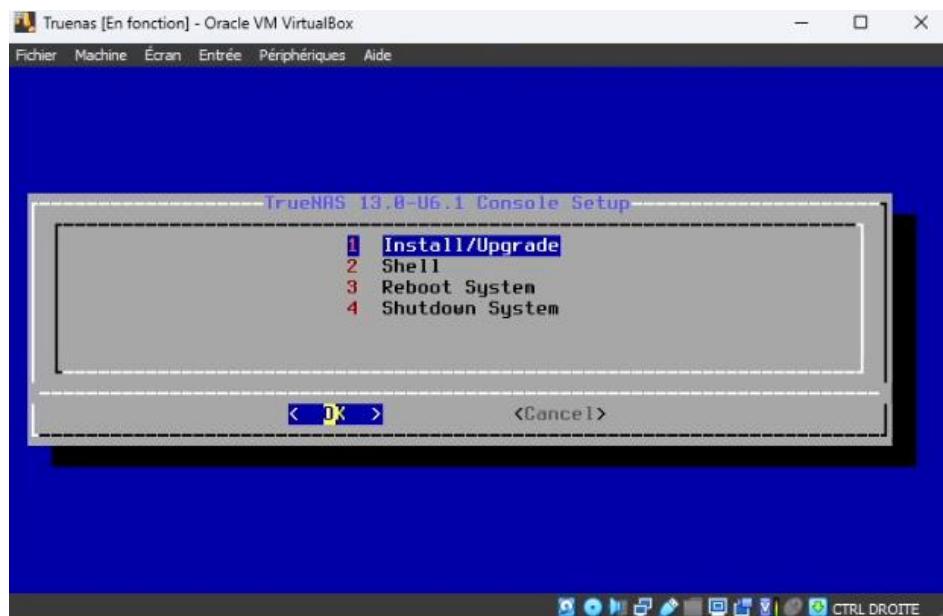
9.8 Rapport technique installation serveur fichier TrueNAS Core

TrueNAS est un système d'exploitation sous licence libre, basé sur FreeBSD et la distribution Linux Debian, destiné aux serveurs de stockage en réseau NAS. Nous allons donc mettre en place un système de serveur de stockage.

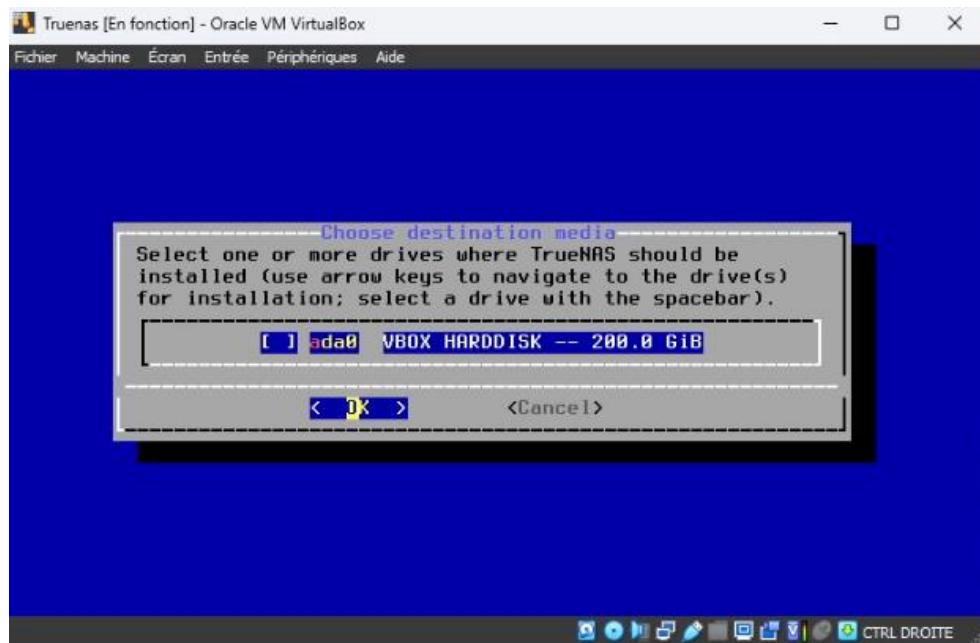
Pour commencer la configuration nécessaire pour la machine virtuelle TrueNAS Core :



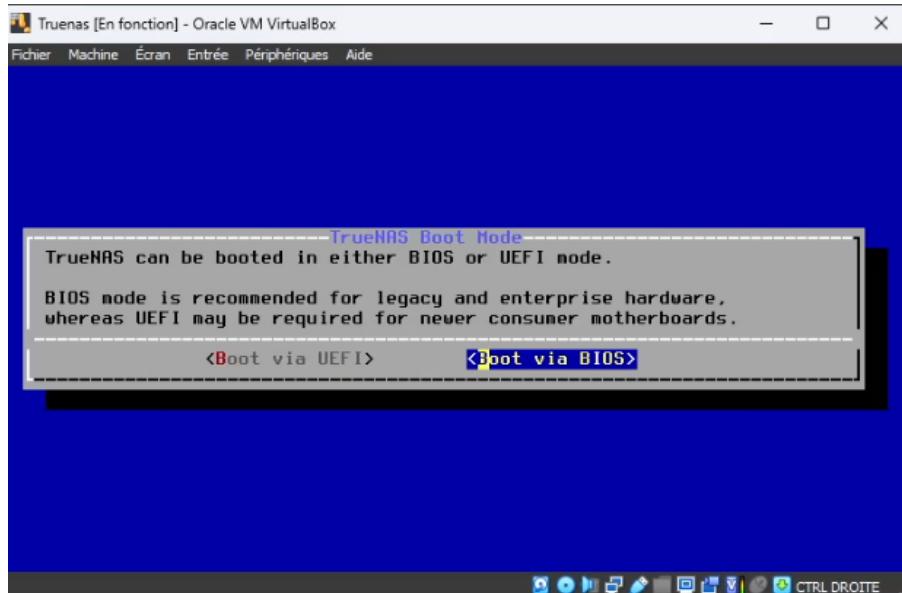
On arrive sur l'interface d'installation de TrueNAS



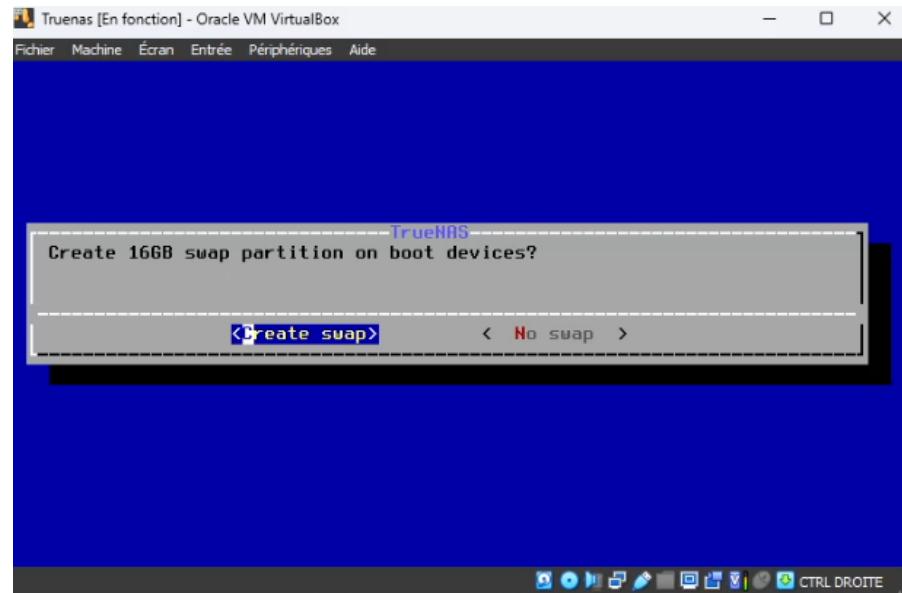
Le disque sélectionné pour l'installation



On boot via le BIOS



On ne crée pas de partition swap dans ce cas-là



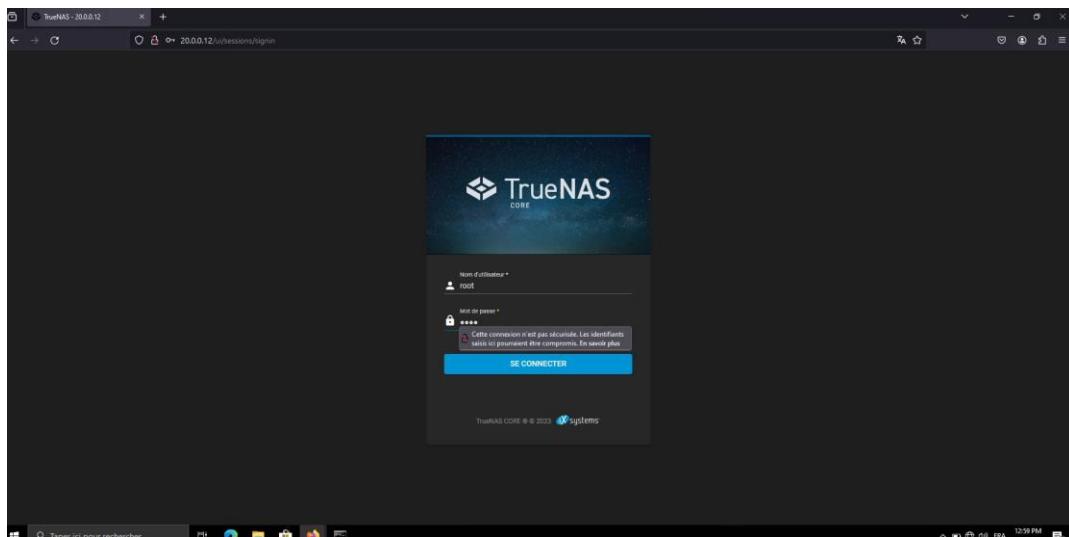
L'installation se poursuit, on redémarre la machine virtuelle, ensuite s'affiche cette interface :

```
Truenas [En fonction] - Oracle VM VirtualBox
Fichier Machine Écran Entrée Périphériques Aide
ress enter to continue

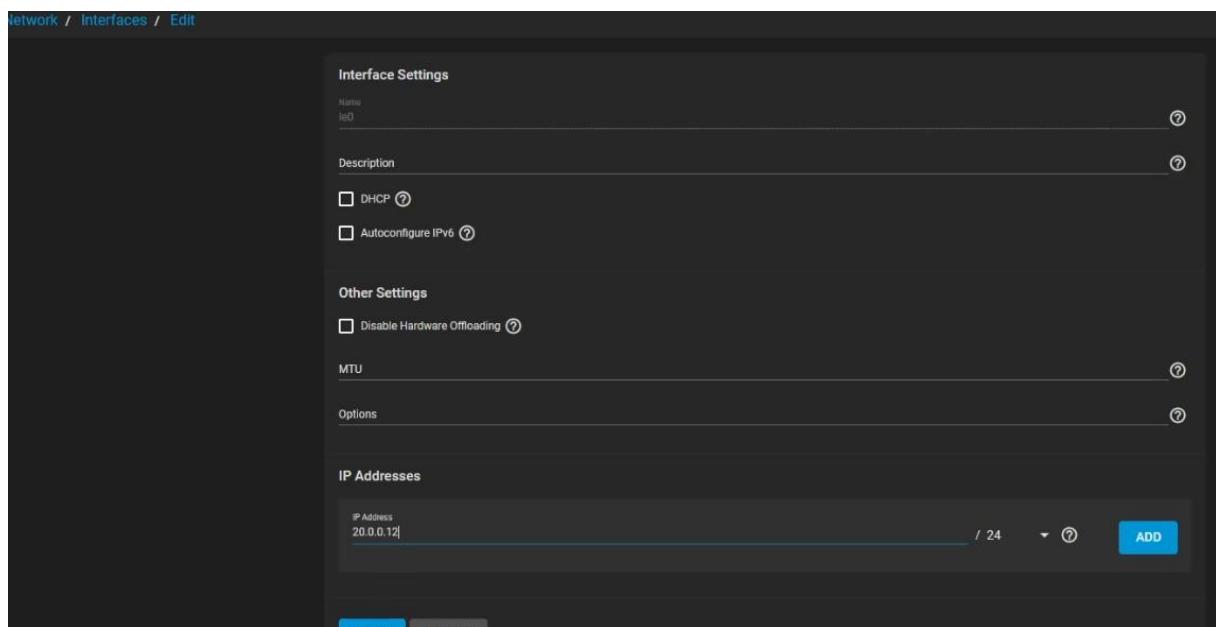
onsole setup
-----
) Configure Network Interfaces
) Configure Link Aggregation
) Configure VLAN Interface
) Configure Default Route
) Configure Static Routes
) Configure DNS
) Reset Root Password
) Reset Configuration to Defaults
) Shell
0) Reboot
1) Shut Down

he web user interface is at:
http://20.0.0.12
https://20.0.0.12
ntrer une option from 1-11: ■
```

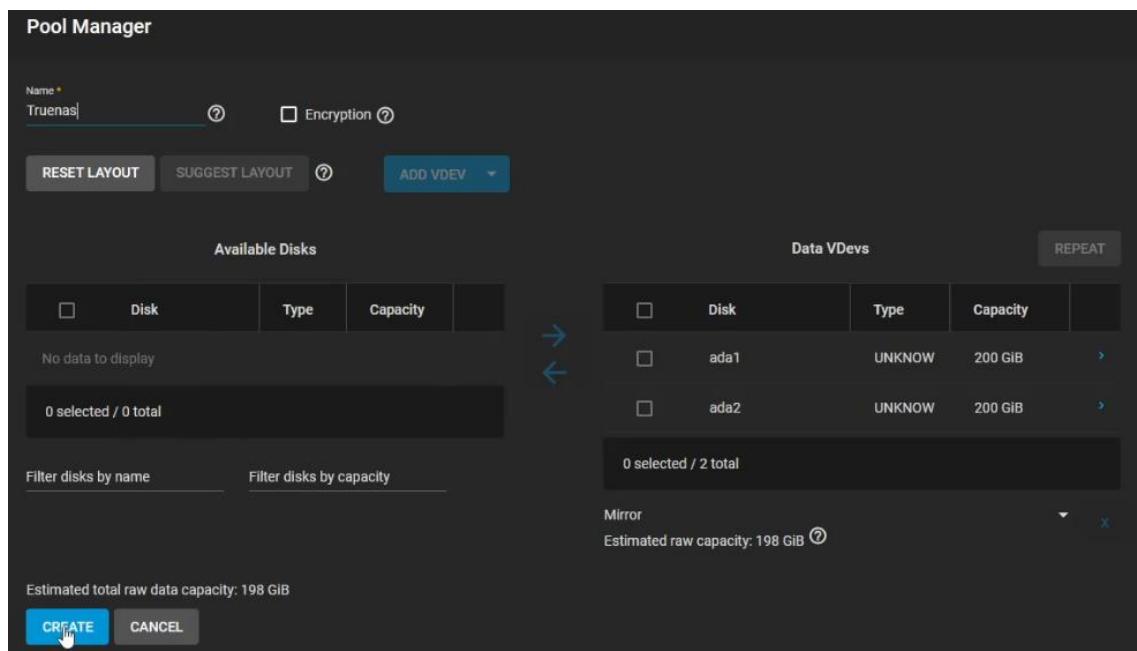
On peut changer le root password et ensuite dans la machine virtuelle windows on rentre l'adresse du TrueNAS dans le navigateur et on arrive sur cette interface de connexion.



Dans l'onglet Network/Interface, on désactive le DHCP, on rentre une adresse statique puis cliquer sur valider.

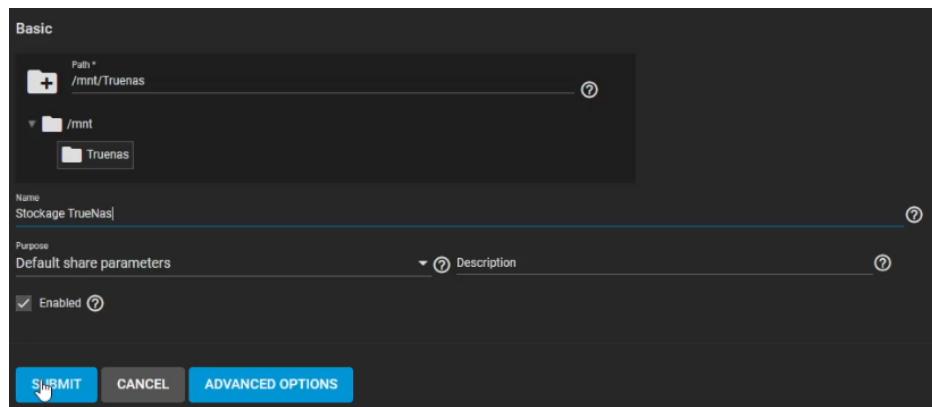


Maintenant nous allons créer l'espace de stockage des fichiers en cliquant sur Storage/Pools sur le menu TrueNas.



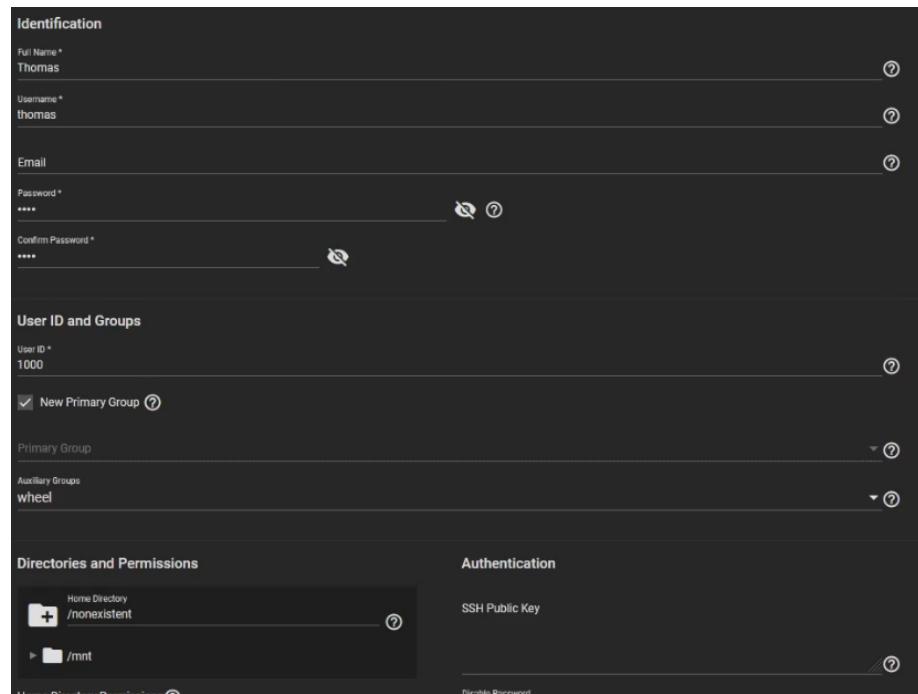
On ajoute les deux disques, dans ce cas-ci, ils seront en miroir. Cliquer sur valider et sauvegarder.

Maintenant, il faut partager ce stockage, dans la rubrique Sharing/Windows Share (SMB)

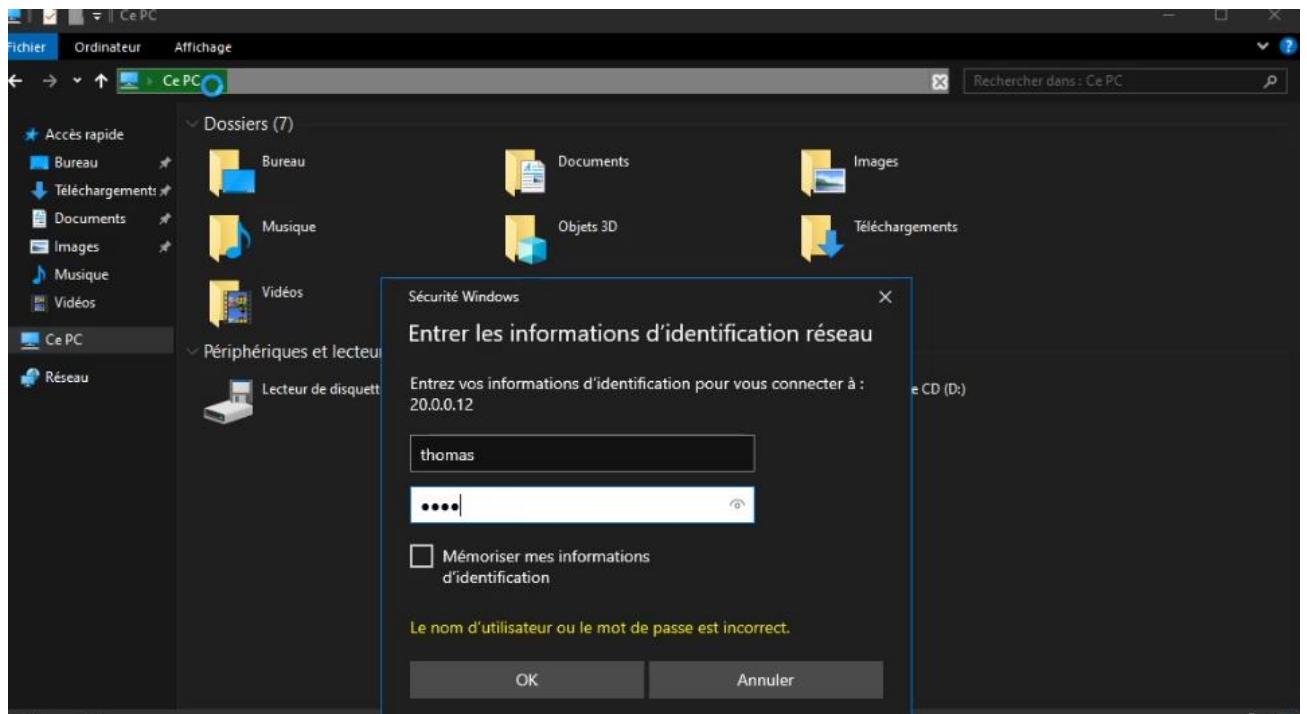


Cliquer sur valider puis activer le service

Ensuite, il faut créer un utilisateur qui pourra se connecter au partage réseau du TrueNas.



Tout est prêt et l'utilisateur peut accéder à TrueNAS en tapant l'adresse 20.0.0.12 dans cet exemple, rentrer les informations de connexions de l'utilisateur créé dans TrueNAS Core et il accède au partage réseau.



10. Références bibliographiques (liste des sources documentaires)

Service mis en place	Sources documentaires
DEJA DUP	https://doc.ubuntu-fr.org/deja-dup
Postfix	https://doc.ubuntu-fr.org/installer_postfix_en_local_pour_un_poste_de_travail
Nextcloud	https://linuxgenie.net/how-to-install-nextcloud-on-ubuntu-22-04/
Active Directory	https://www.readandexecute.com/how-to/server-2016/active-directory/how-to-server-2016installing-active-directory-server-2016/
RDP	https://support.microsoft.com/fr-fr/windows/utilisation-du-bureau-%C3%A0-distance-5fe128d5-8fb1-7a23-3b8a-41e636865e8c
DHCP DNS	https://www.pc2s.fr/pfsense-installation-et-configuration/
Portail captif	https://www.youtube.com/watch?v=JmCadrWt1ag
True Nas	https://www.youtube.com/watch?v=rF0aeRcd3ks

11. Conclusion sur le travail réalisé ou restant à faire :

Nous pouvons conclure que les services que nous avons mis en place représentent une avancée significative pour l'infrastructure de la société SPOON. Ces services sont essentiels pour toute entreprise, quelle que soit sa taille, ses objectifs ou sa capacité financière.

Parmi ces services, l'Active Directory a été configuré pour stocker tous les utilisateurs de l'entreprise dans un seul annuaire. Il y a également le serveur DHCP attribue automatiquement des adresses IP aux utilisateurs, permettant un accès à Internet sans nécessiter une configuration manuelle. Cependant, l'accès à Internet nécessitera une authentification sur le portail captif pour confirmer l'identité de l'utilisateur.

Dans le contexte actuel, où les cyber-attaques notamment les ransomwares sont de plus en plus fréquentes, il est crucial de sauvegarder les ressources de l'entreprise. Pour cela, le logiciel de sauvegarde DEJA-DUP pour archiver et restaurer des données importantes. De même, le cloud local Nextcloud offre un stockage sécurisé des ressources, tandis que le serveur de fichiers TrueNAS assure une gestion et stockage efficace des données.

D'autres services, bien que moins prioritaires, sont également essentiels. La connexion RDP permet le contrôle à distance des machines, favorisant ainsi le télétravail. Le logiciel Postfix assure une communication sécurisée entre les utilisateurs et qui a été configuré comme serveur de messagerie locale.

Parmi le travail restant à faire, nous avons la téléphonie IP, qu'on peut associer à la même catégorie que Postfix et RDP. Il offre une utilité différente en permettant les appels téléphoniques via une connexion Internet plutôt qu'un réseau téléphonique.