

AP Resto.fr (AD,DHCP,TFTP) - Mission 1

Les tâches à faire :

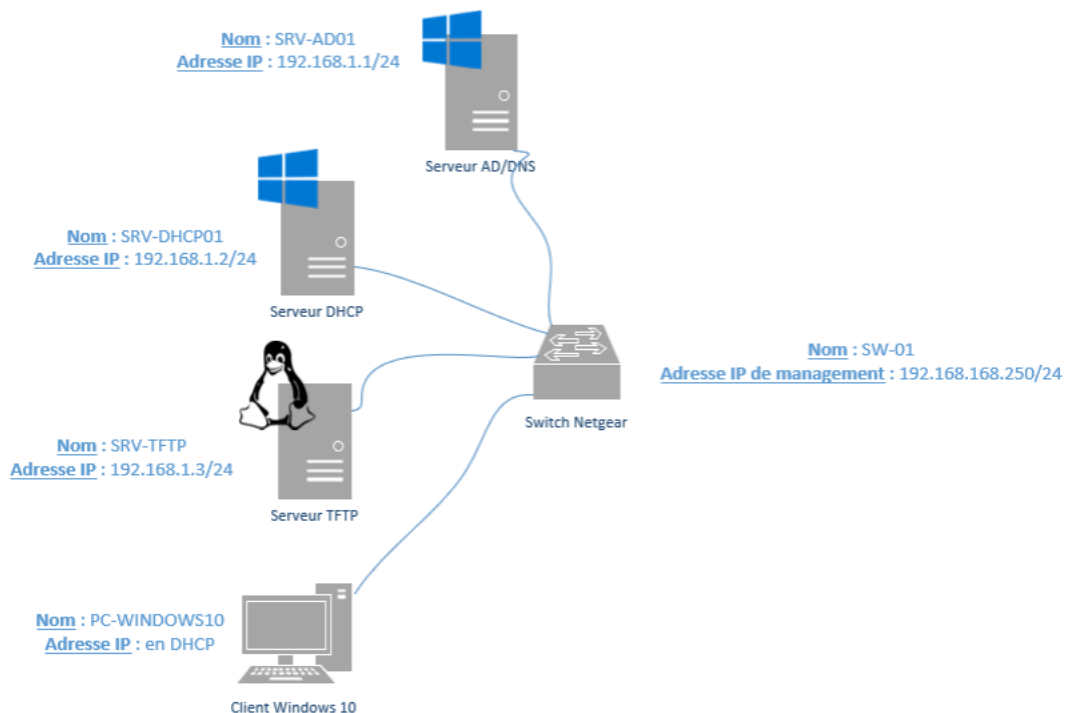
Serveur AD/DNS : Active Directory (AD) est un service d'annuaire qui fonctionne sur Microsoft Windows Server reposant sur un service de nommage des ordinateurs (service DNS). Dans Active Directory, les données sont stockées sous forme d'objets. Ceux-ci comprennent les utilisateurs, les groupes, les ordinateurs... Active Directory permet aux administrateurs de gérer et de contrôler de manière centralisée la configuration des ordinateurs et des utilisateurs. Les comptes utilisateurs ne seront donc plus des comptes locaux mais des comptes du domaine AD

Tous les serveurs et PC sous Windows de r3st0.fr devront être joints à votre domaine Active Directory et tous vos postes et serveurs devront être enregistrés dans les zones de noms DNS (zone de recherche directe et zone de recherche inversée).

Serveur DHCP : Le protocole DHCP (Dynamic Host Configuration Protocol) est un protocole client/serveur qui fournit automatiquement à un hôte IP (Internet Protocol) son adresse IP et d'autres informations de configuration associées (serveur DNS à contacter, suffixe DNS à utiliser...). Cette solution va permettre aux ordinateurs portables de l'entreprise d'être fonctionnels à la fois à leur domicile ainsi que dans les murs de l'entreprise sans manipulation particulière.

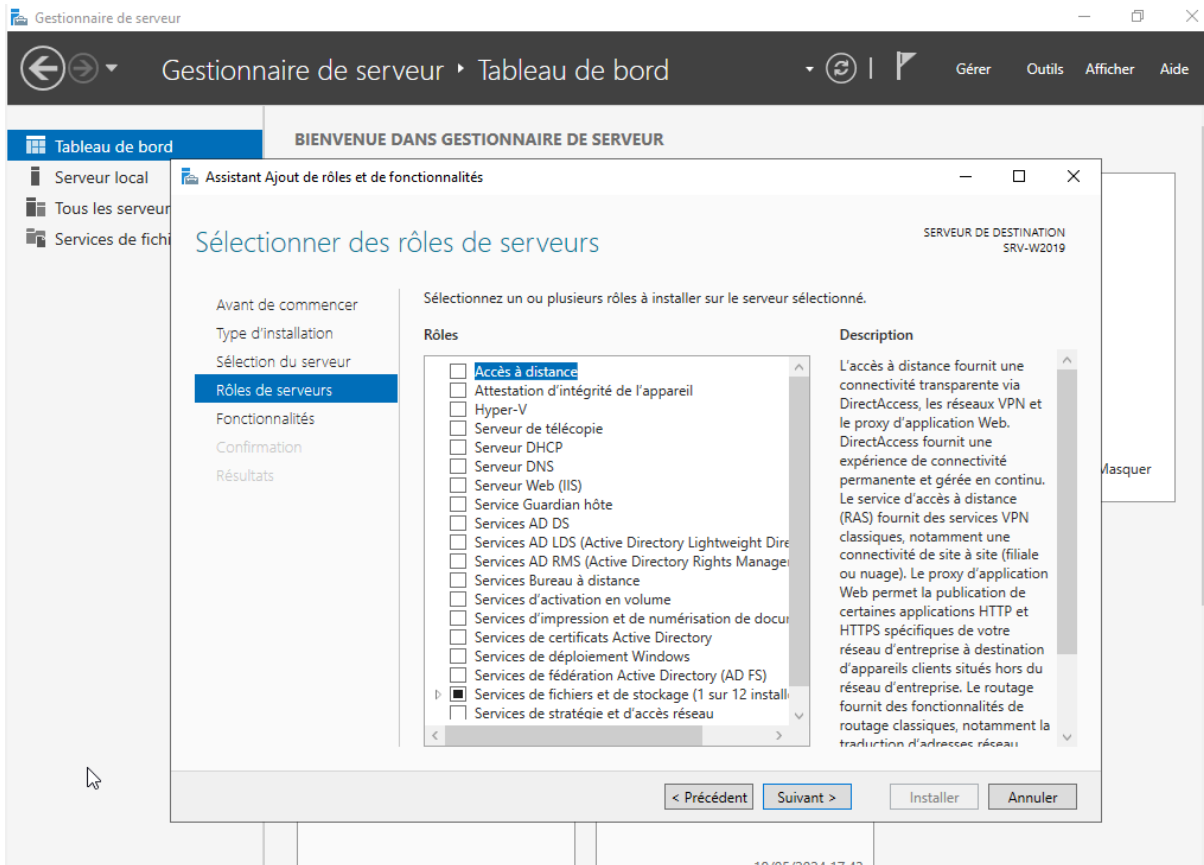
Serveur TFTP pour sauvegarder les équipements réseaux : Le protocole TFTP (Trivial File Transfer Protocol) est principalement utilisé pour des transferts de fichiers automatisés entre des machines. Ce serveur va donc servir à réaliser des sauvegardes et restaurations du fichier de configuration des commutateurs.

Schéma de la maquette :

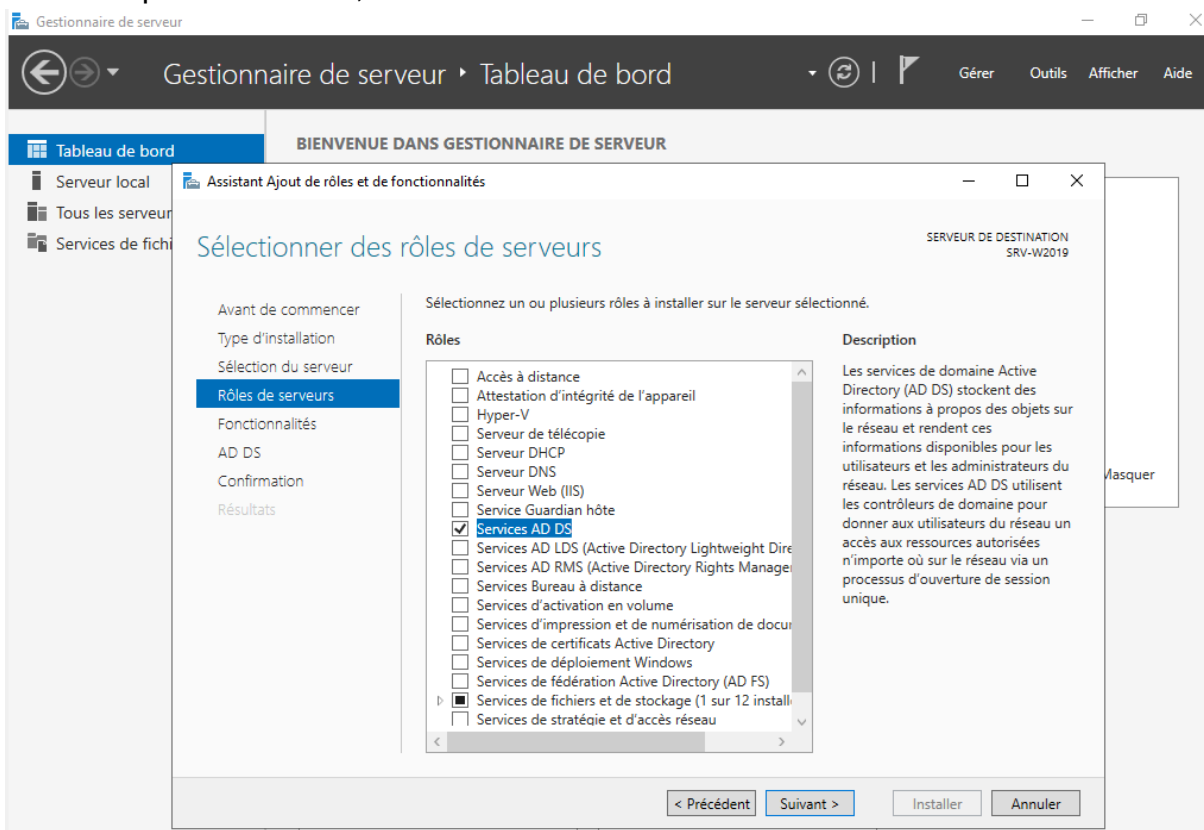


Mise en place du serveur AD :

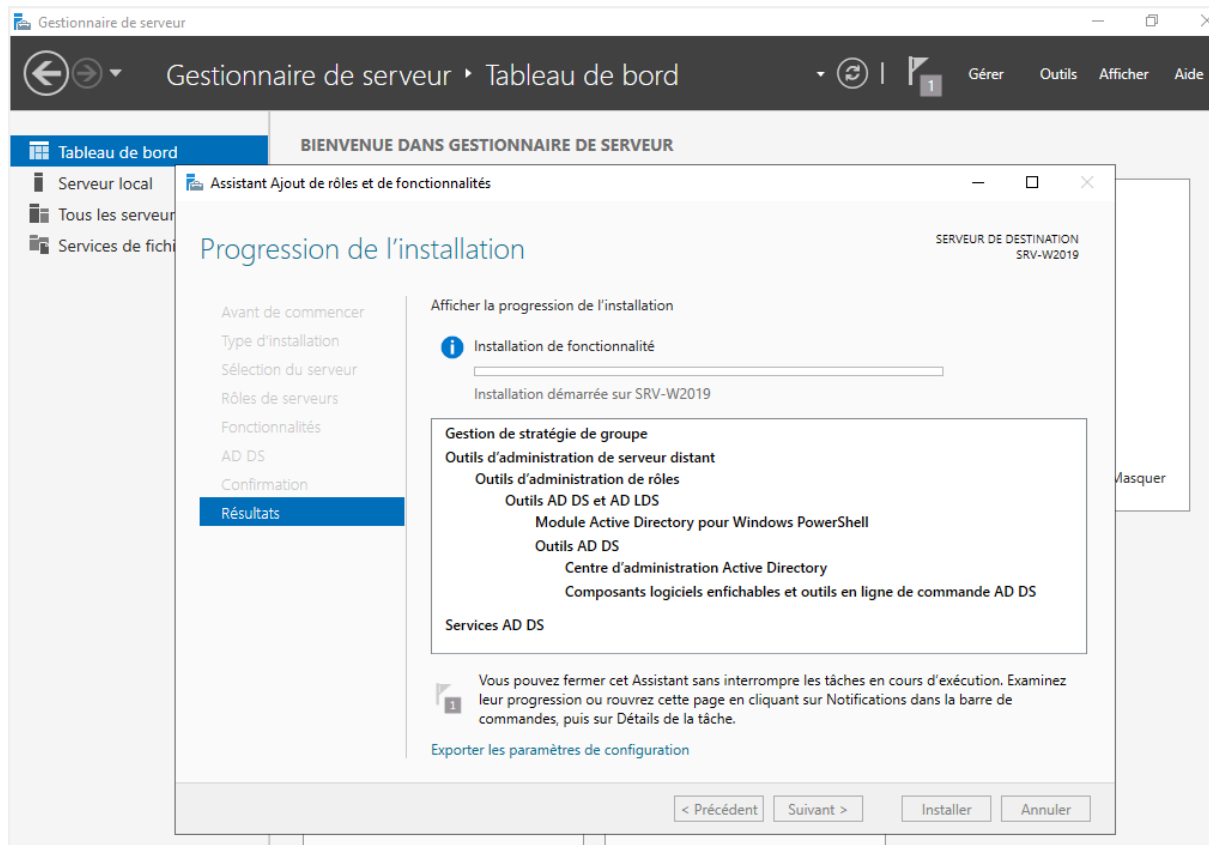
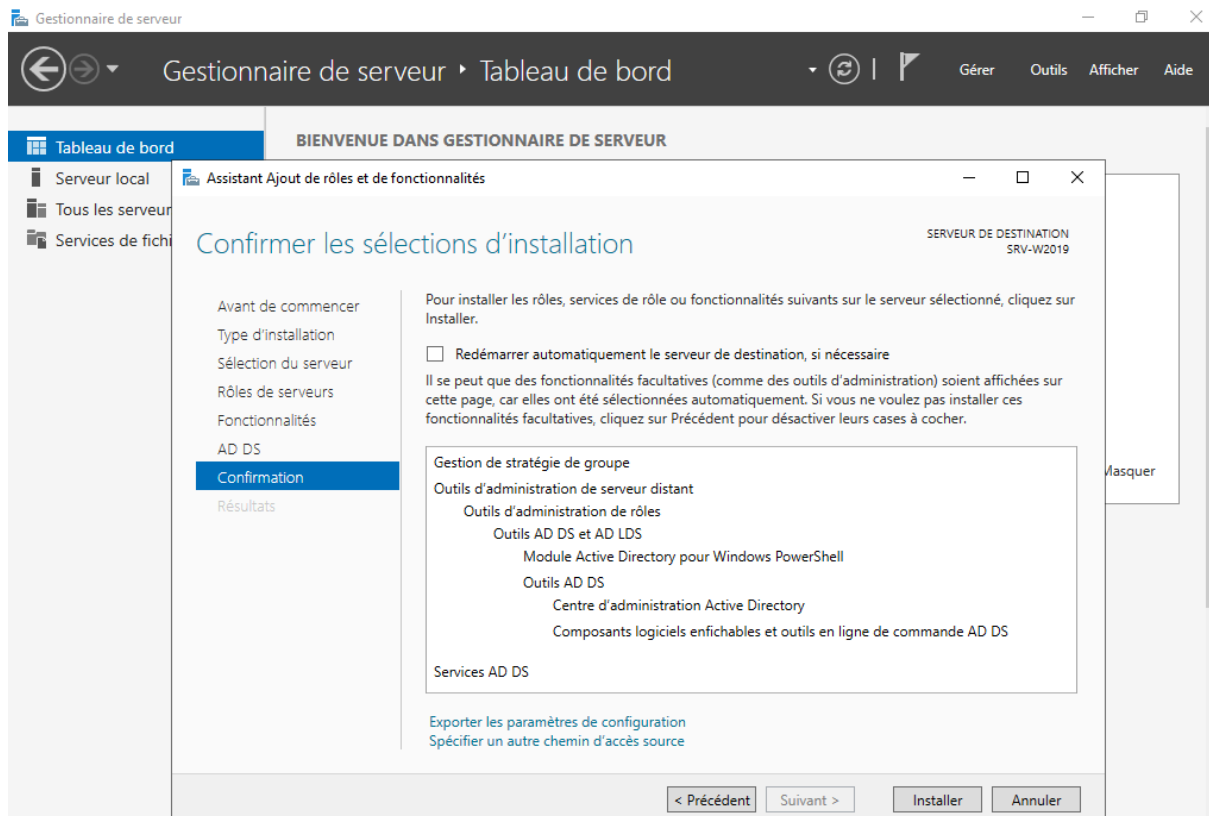
Tout d'abord il faut installer le service "AD DS" pour le serveur. Pour cela il faut se rendre dans : Gestionnaire de serveur > Gérer > Ajouter des rôles et fonctionnalités > Rôles de Serveurs .



Une fois que cela est fait, cocher la case "Service AD DS" :



Puis aller directement dans l'onglet "Confirmation" et cliquer sur le bouton "installer" :



Afficher la progression de l'installation

i Installation de fonctionnalité

Configuration requise. Installation réussie sur SRV-W2019.

Installation + Configuration du service DNS :

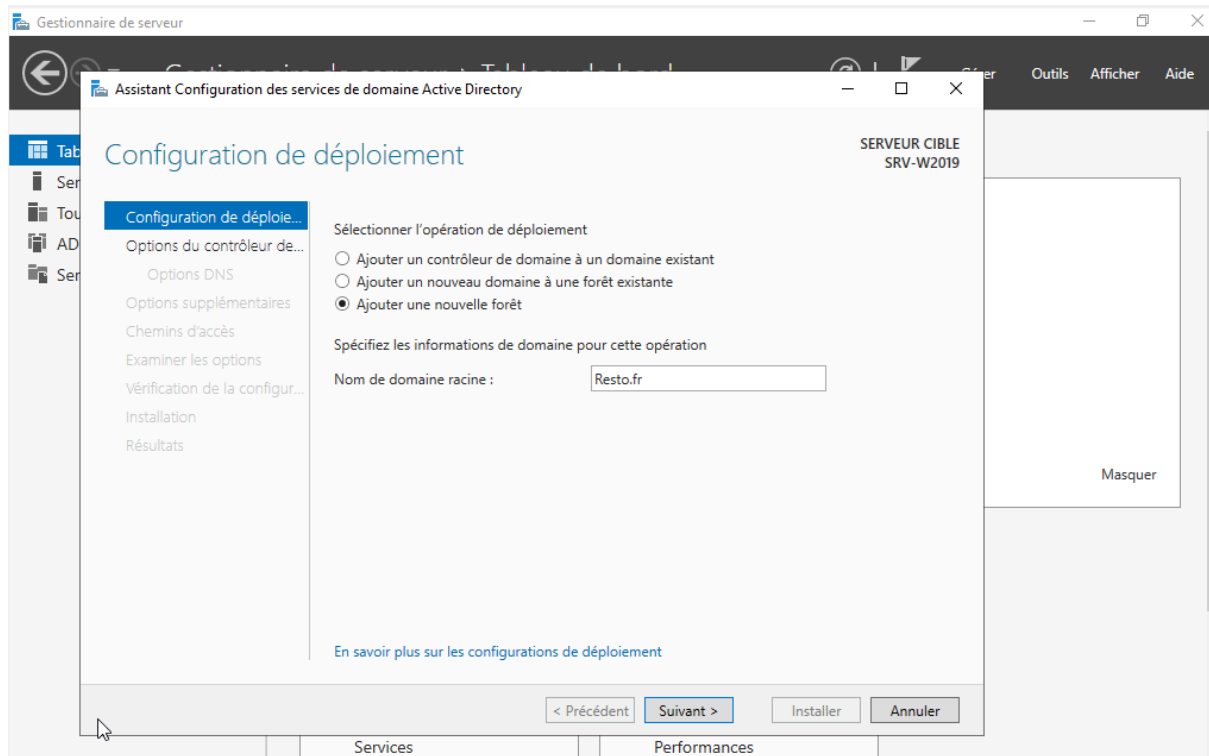
Suite à l'installation du service "AD DS" on peut à présent installer et configurer le service DNS qui va permettre à s'autre machine de pouvoir se connecter au serveur.

Pour cela il faut se rendre dans le tableau de bord du gestionnaire du serveur et aller dans "Notifications" qui serait symbolisé sous forme de drapeau et cliquer sur "Promouvoir ce serveur en contrôleur de domaine" :

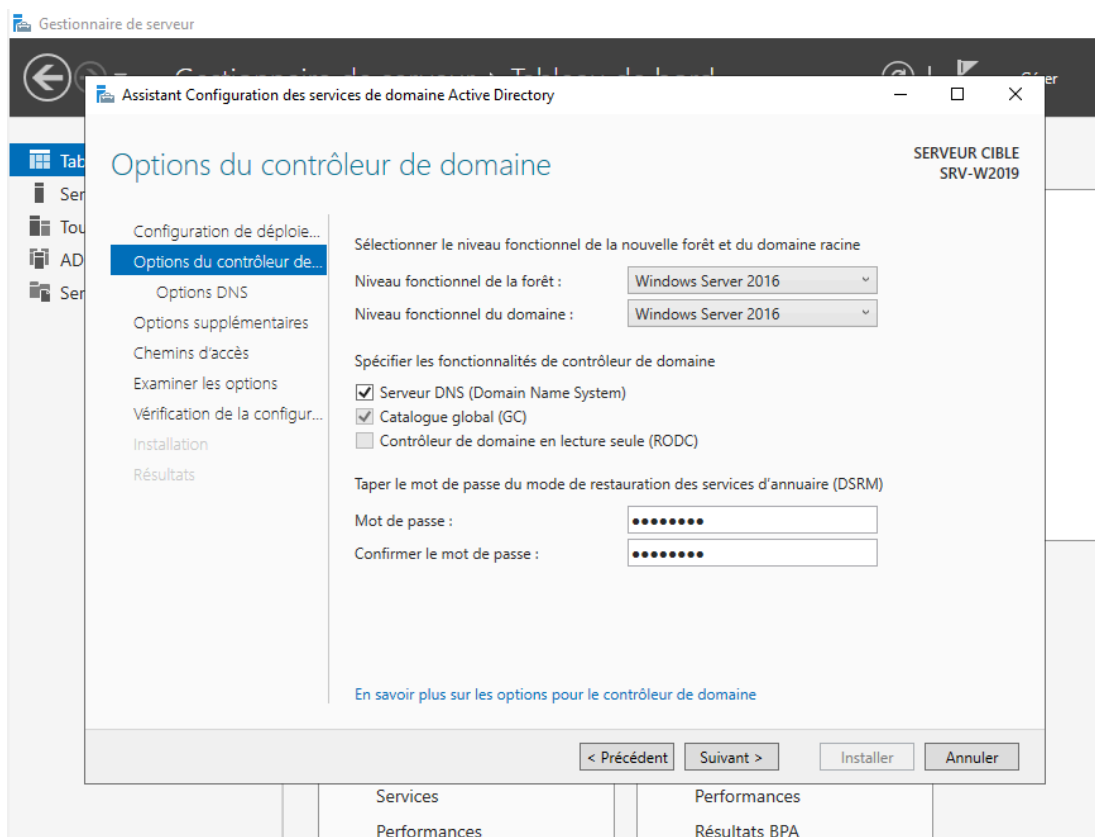
The screenshot shows the Windows Server Management console. The top navigation bar includes "Gestionnaire de serveur" and "Tableau de bord". A notification banner is visible, titled "Configuration post-déploiement", with a yellow warning icon. The notification content includes: "Configuration requise pour : Services AD DS à SRV-W2019", "Promouvoir ce serveur en contrôleur de domaine", "Installation de fonctionnalité", "Configuration requise. Installation réussie sur SRV-W2019.", "Ajouter des rôles et fonctionnalités", "Détails de la tâche", and "Connecter ce serveur aux services cloud". The main area shows "BIENVENUE DANS GESTIONNAIRE" with a "DÉMARRAGE RAPIDE" button and a "NOUVEAUTÉS" section. Below, the "Rôles et groupes de serveurs" section shows "AD DS" and "Services de fichiers et de stockage" with their respective management options.

Une fois arriver sur l'interface ils nous sera proposées plusieurs options et nous sélectionnerons "Ajouter une nouvelle forêt " et renommerons la forêt par Resto.fr.

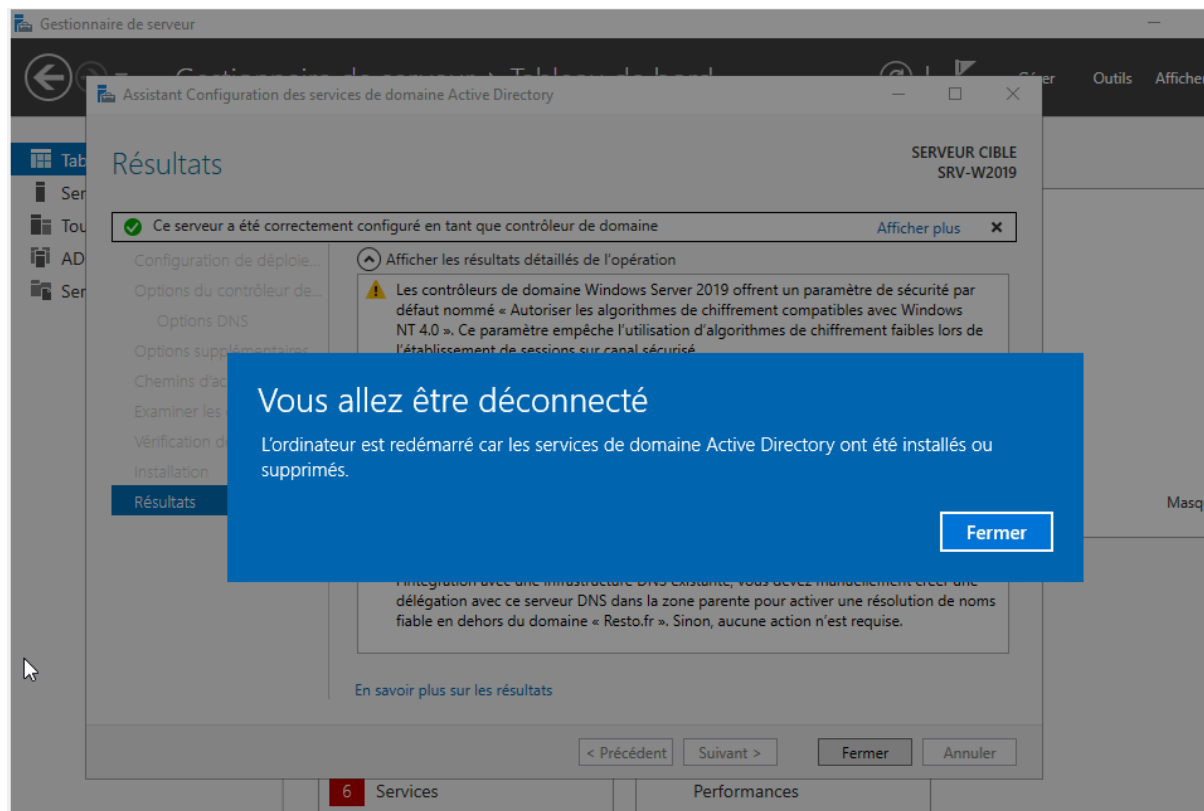
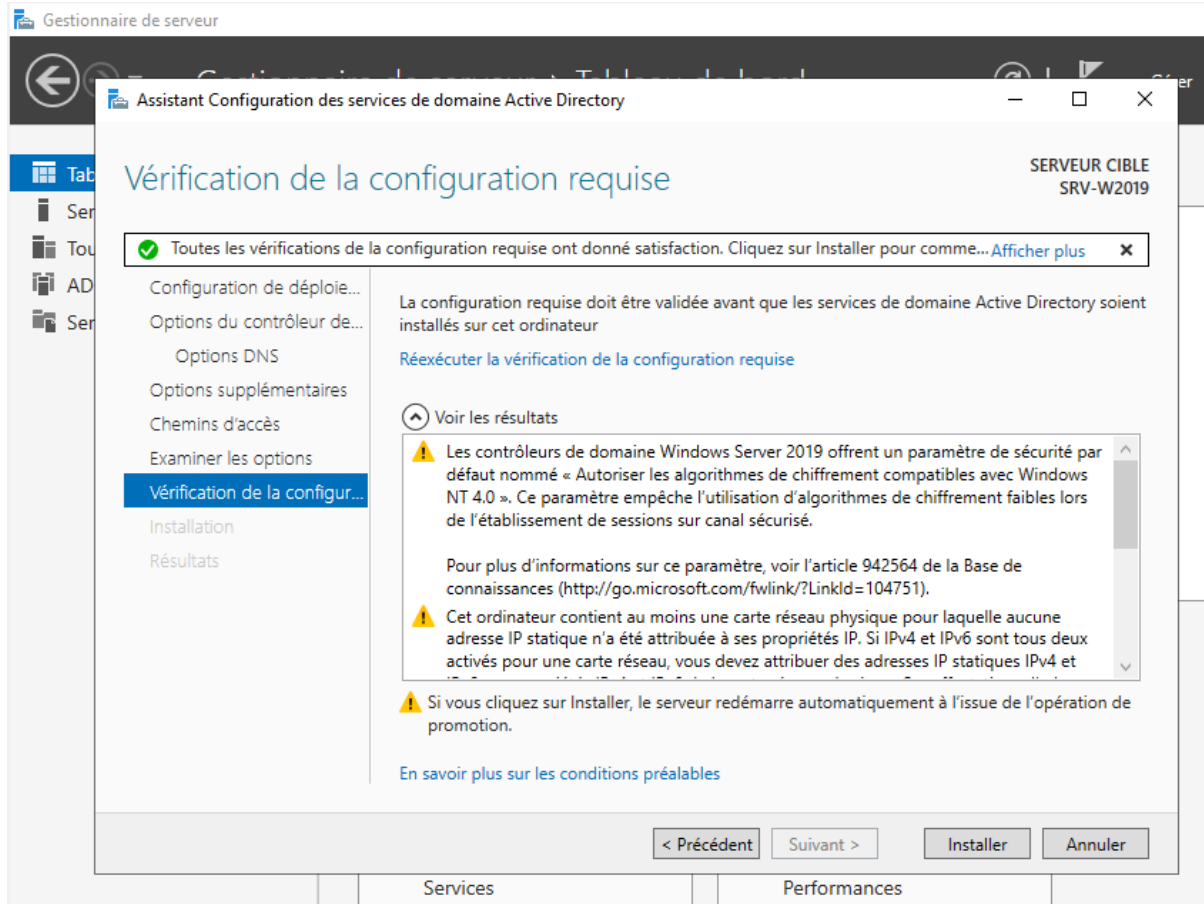
Une nouvelle forêt AD (Active Directory) sert à gérer et organiser les utilisateurs, les ordinateurs et les ressources d'une entreprise. Elle facilite la sécurité, le partage de fichiers et la gestion des accès au sein du réseau informatique.

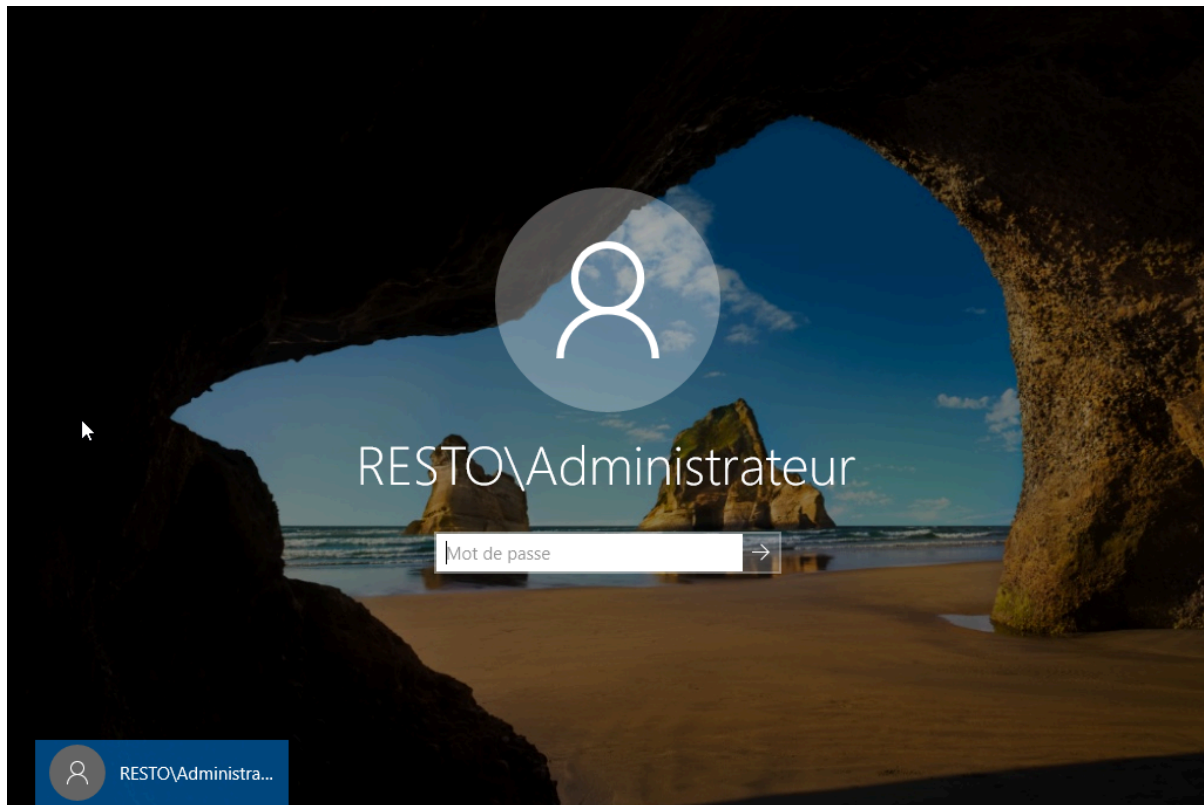


Par la suite un mot de passe nous sera demandé ici : "Btssio64" :



Cliquer sur suivant jusqu'à l'onglet "Vérification de la configuration requise" puis lancer l'installation. Le serveur va redémarrer de lui même afin que la nouvelle configuration soit prise en compte :

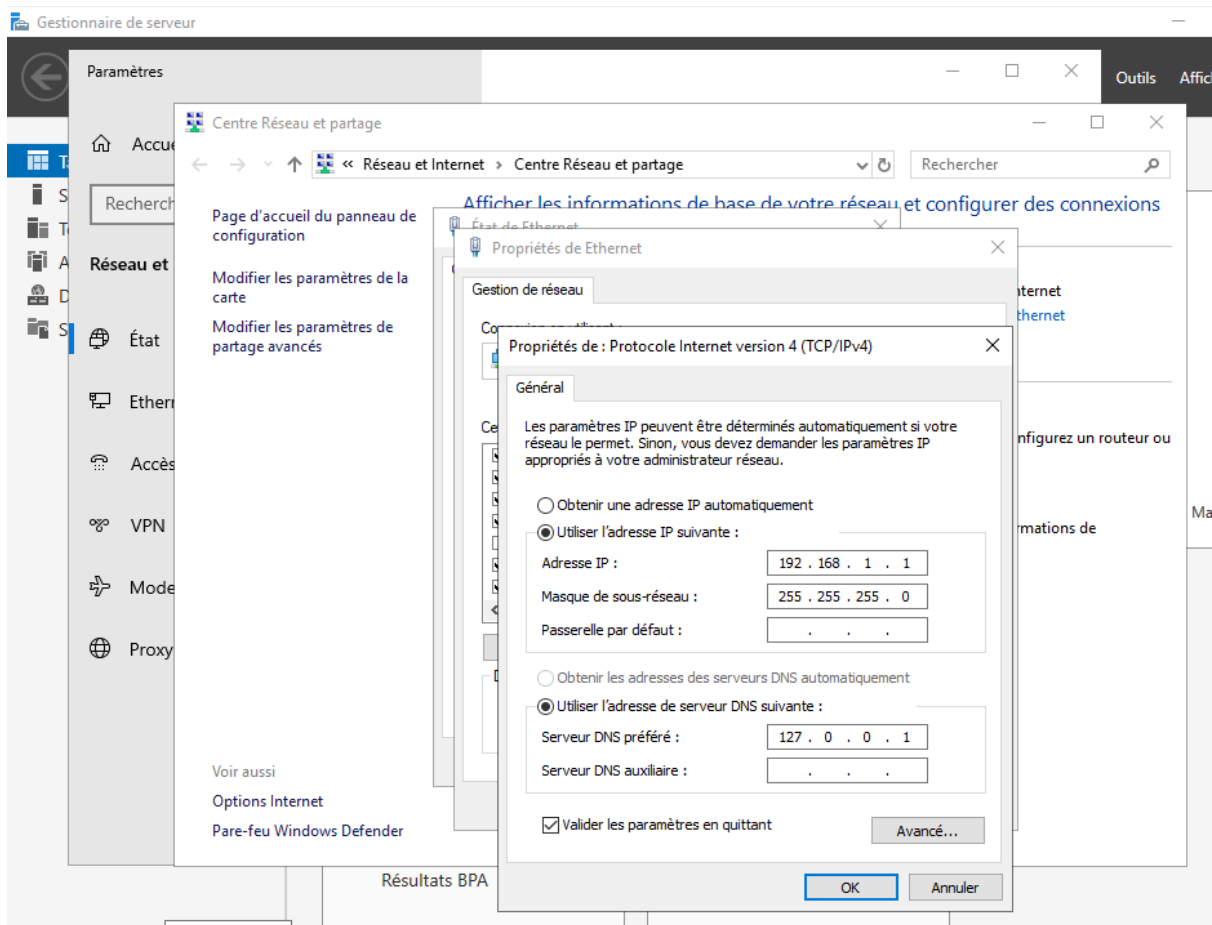




Configuration de l'ip du serveur resto.fr

Dans le schémas de la maquette réseaux il faut mettre le serveur resto.fr en 192.168.1.1/24 pour cela il faut se rendre dans : “Ouvrir les paramètres réseau et internet” > “Centre Réseau et partage” > “ Ethernet ” >” Propriétés “ > “ Protocole Internet Version 4 (TCP/IPv4) “ .

- Sélectionner “ Utiliser l'adresse IP suivante “ et mettre dans “ Adresse ip “ 192.168.1.1.
- Ensuite dans “ Masque de sous-réseau “ 255.255.255.0 ” qui correspond au /24 .

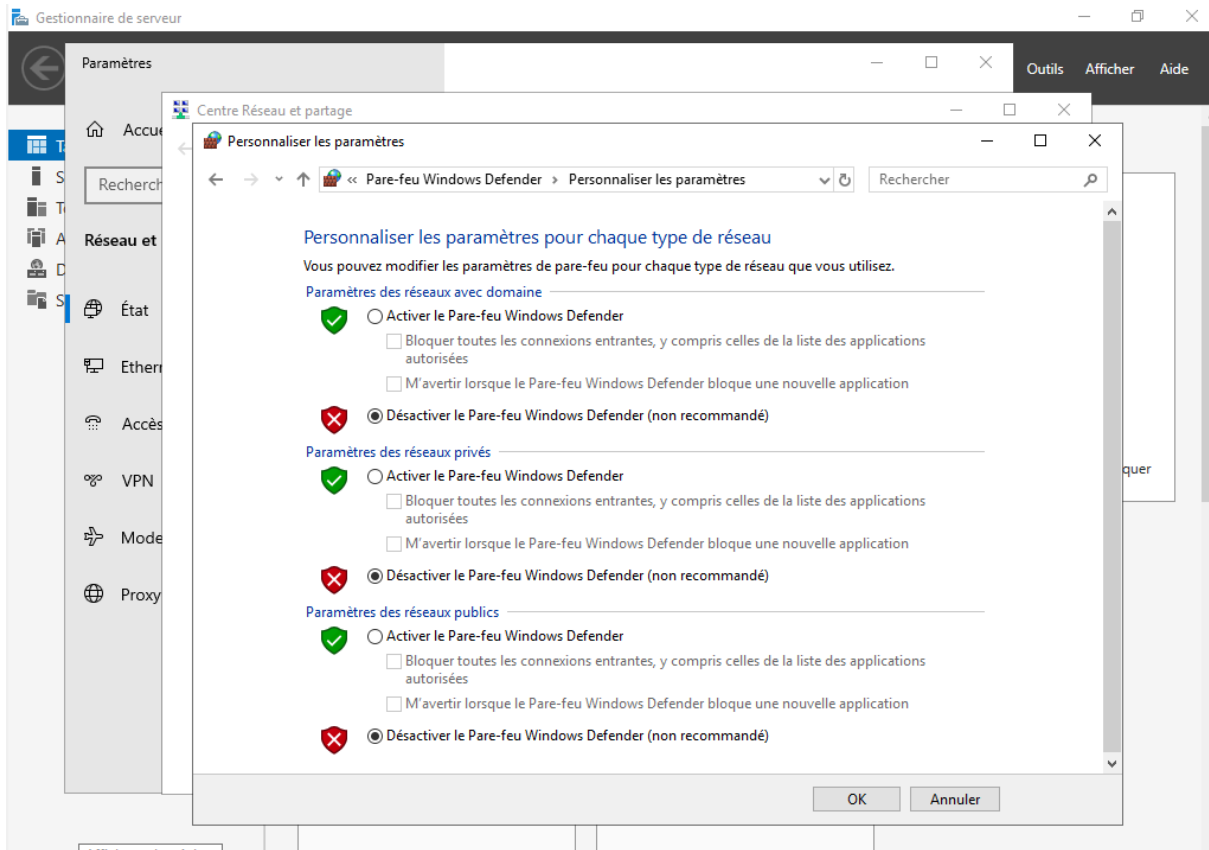


Désactivation du pare-feu :

Il faut désactiver la sécurité du pare-feu car si nous ne le faisons pas cela peut empêcher notre machine de recevoir les paquets lors des pings qui lui sont dédiés.

Pour cela il faut se rendre dans " Pare-feu Windows Defender" > " Activer ou désactiver le Pare-feu Windows Defender " .

Pour finir enlever tous la sécurité du Pare-feu de Windows Defender :



Création d'un compte utilisateur pour le PC-Windows 10 sur le serveur resto.fr :

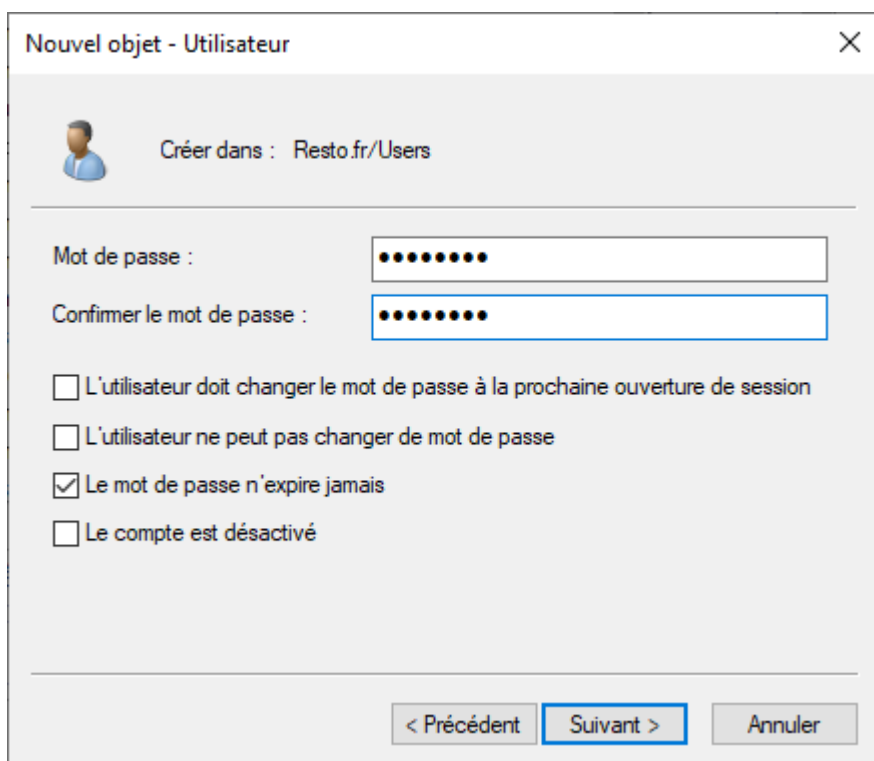
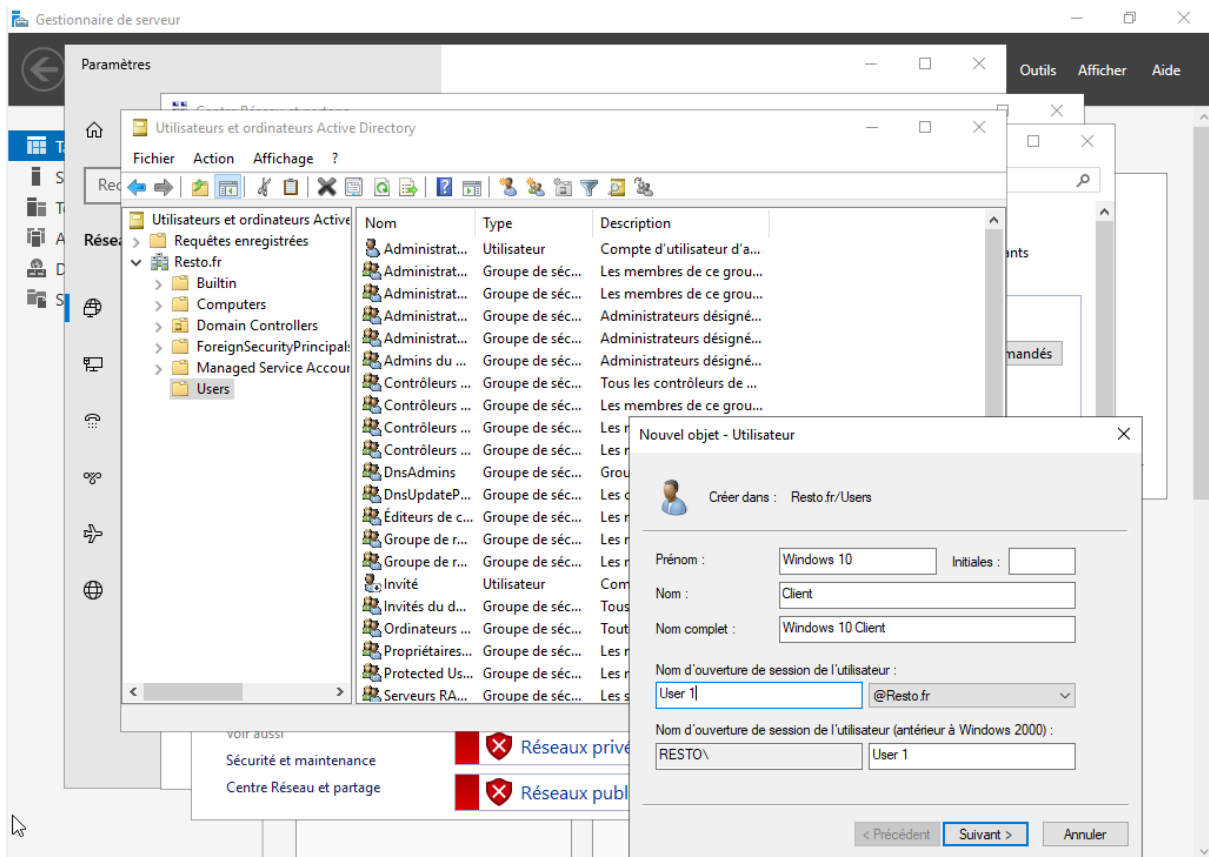
Maintenant il faut créer un compte utilisateur sur le serveur resto.fr pour qu'il puisse le rejoindre par la suite.

Pour cela il faut se rendre dans " Utilisateurs et ordinateur Active Directory " > " Users " .

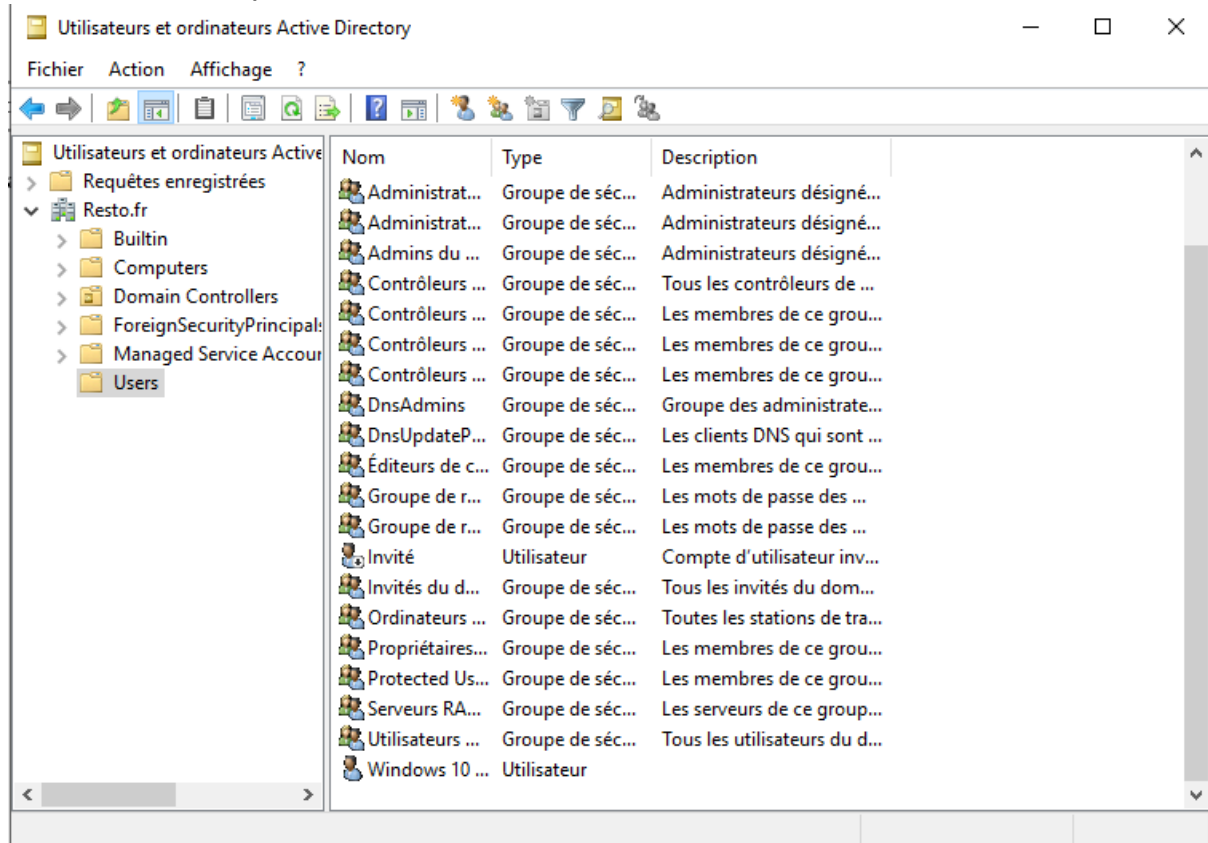
Ensuite il faut faire un clic droit sur le dossier Users et aller dans : " Nouveau " > " Utilisateur " .

Il faudra spécifier le “ Prénom” (**Windows 10**) , “ Nom” (**Client**) et “ Nom d’ouverture de session de l’utilisateur” (**Windows 10 Client**).

Ensuite il faut mettre le **mot de passe de l’utilisateur** pour son ouverture de session .
(**Btsio64**)



L'utilisateur est à présent créé dans le domaine :



Mise en place du serveur DHCP et tests avec le client Windows 10 :

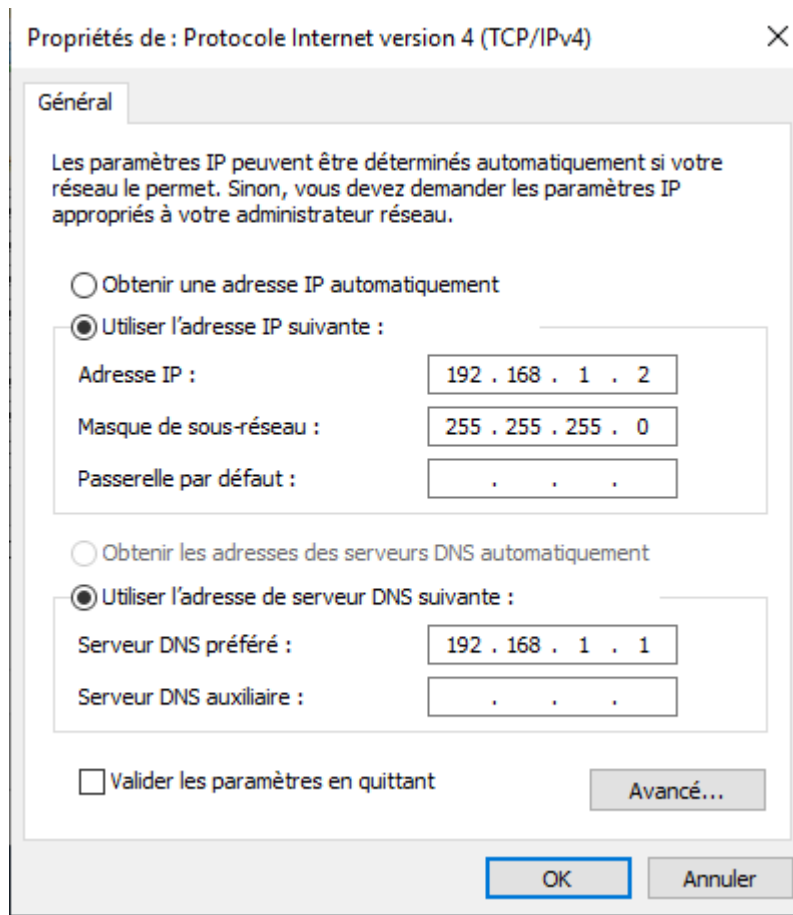
Configuration de l'ip du serveur DHCP de resto.fr :

Dans le schémas de la maquette réseaux il faut mettre le serveur DHCP de resto.fr en 192.168.1.2/24 pour cela il faut se rendre dans : "Ouvrir les paramètres réseau et internet" > "Centre Réseau et partage" > " Ethernet " > " Propriétés " > " Protocole Internet Version 4 (TCP/IPv4) " .

Sélectionner " Utiliser l'adresse IP suivante " et mettre dans " Adresse ip " 192.168.1.2.

Ensuite dans " Masque de sous-réseau " 255.255.255.0 " qui correspond au /24 .

Pour finir spécifier l'IP du serveur DNS qui est 192.168.1.1 .

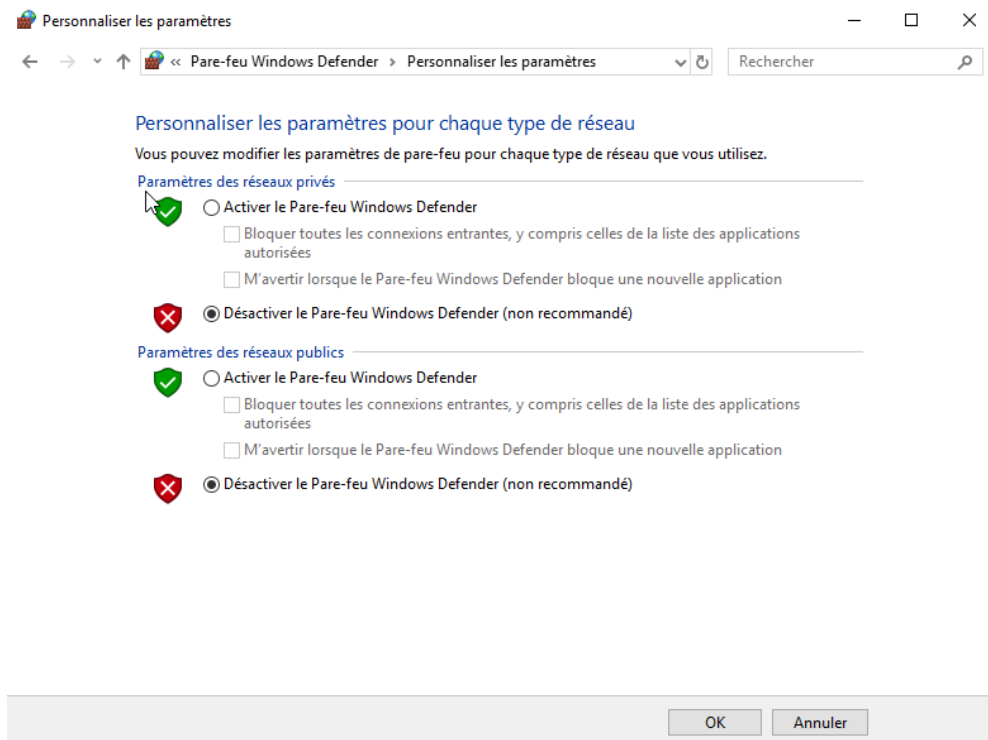


Désactivation du pare-feu :

Il faut désactiver la sécurité du pare-feu car si nous ne le faisons pas cela peut empêcher notre machine de recevoir les paquets lors des pings qui lui sont dédiés.

Pour cela il faut se rendre dans " Pare-feu Windows Defender" > " Activer ou désactiver le Pare-feu Windows Defender " .

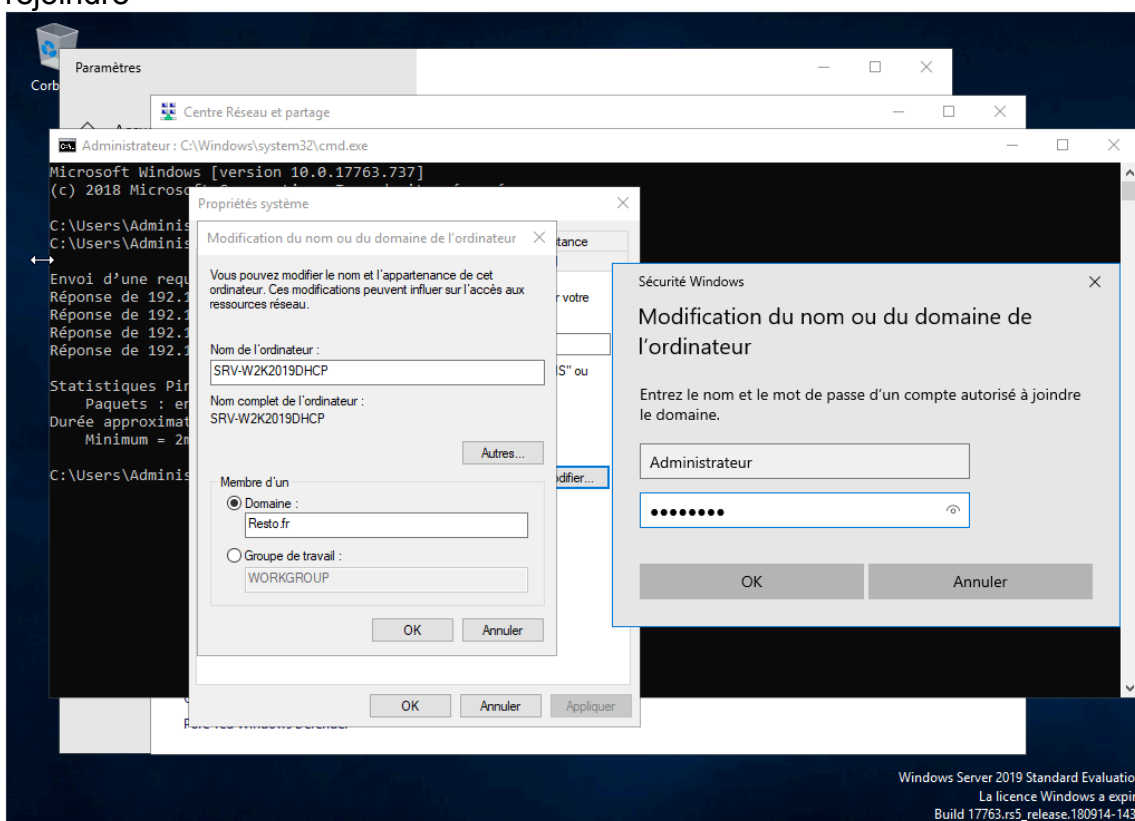
Pour finir enlever tous la sécurité du Pare-feu de Windows Defender :

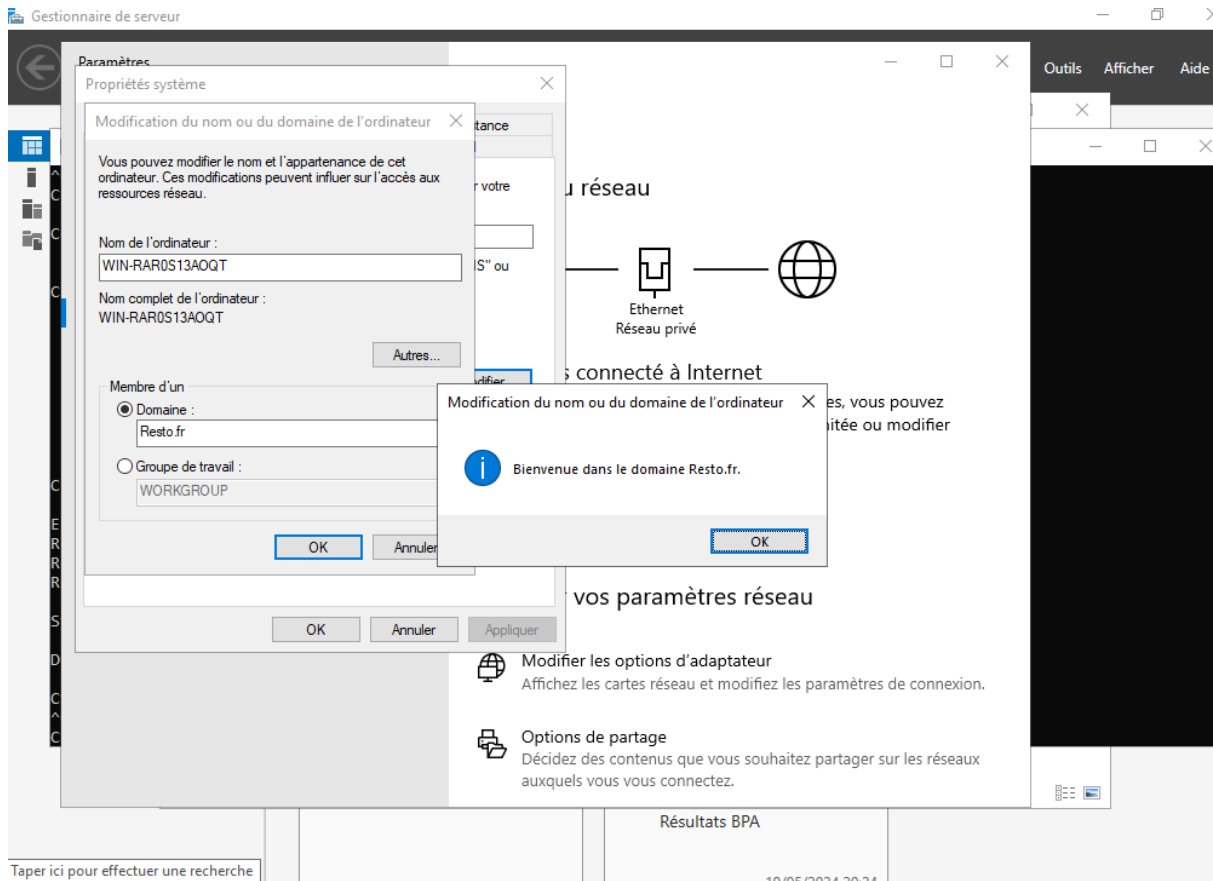


Rejoindre le domaine Resto.fr :

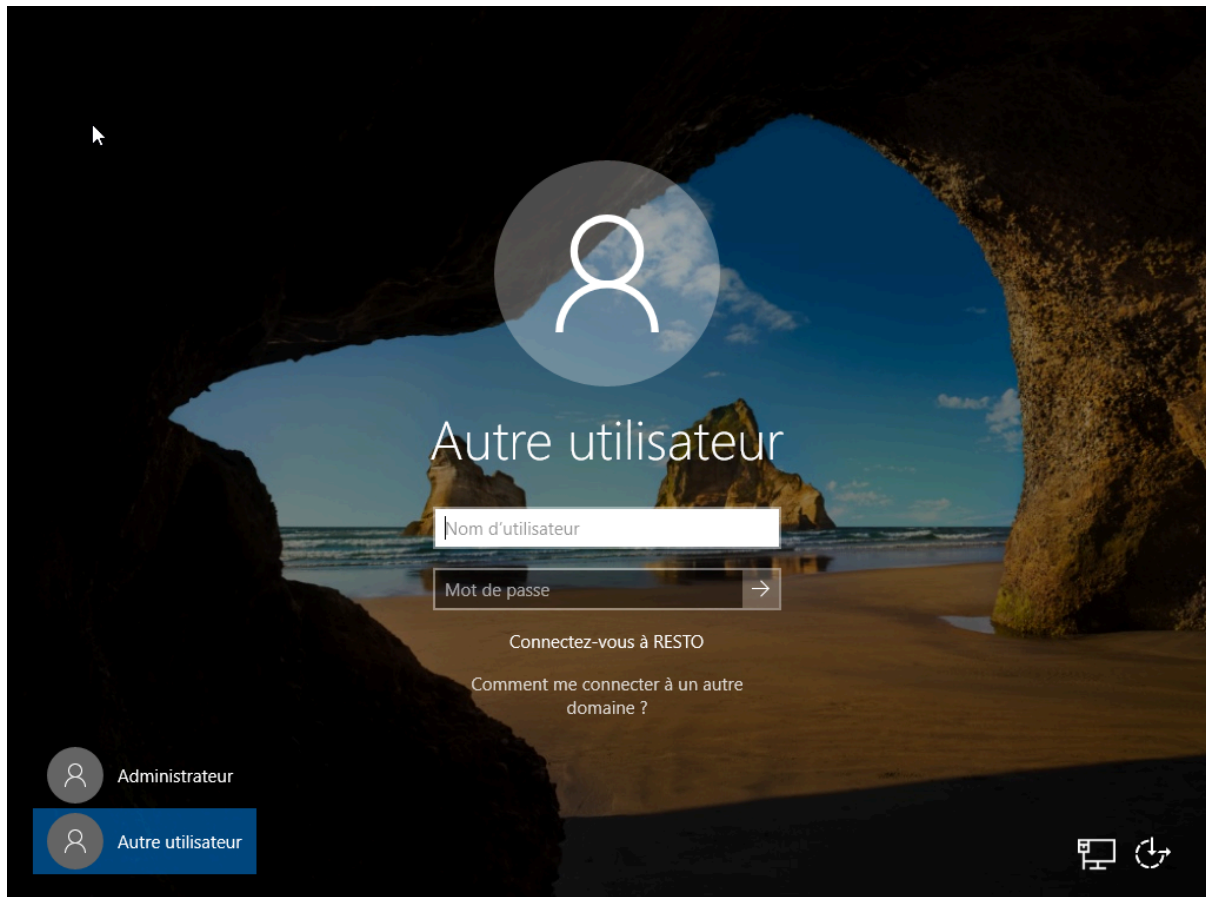
Le serveur DHCP doit rejoindre le domaine Resto.fr, pour cela il faut se rendre dans : " Paramètres " > " Informations système " > " Modifier les paramètres " > " Modifier " .

Ensuite sélectionner " Domaine " et rentrer le nom de domaine que vous voulez rejoindre



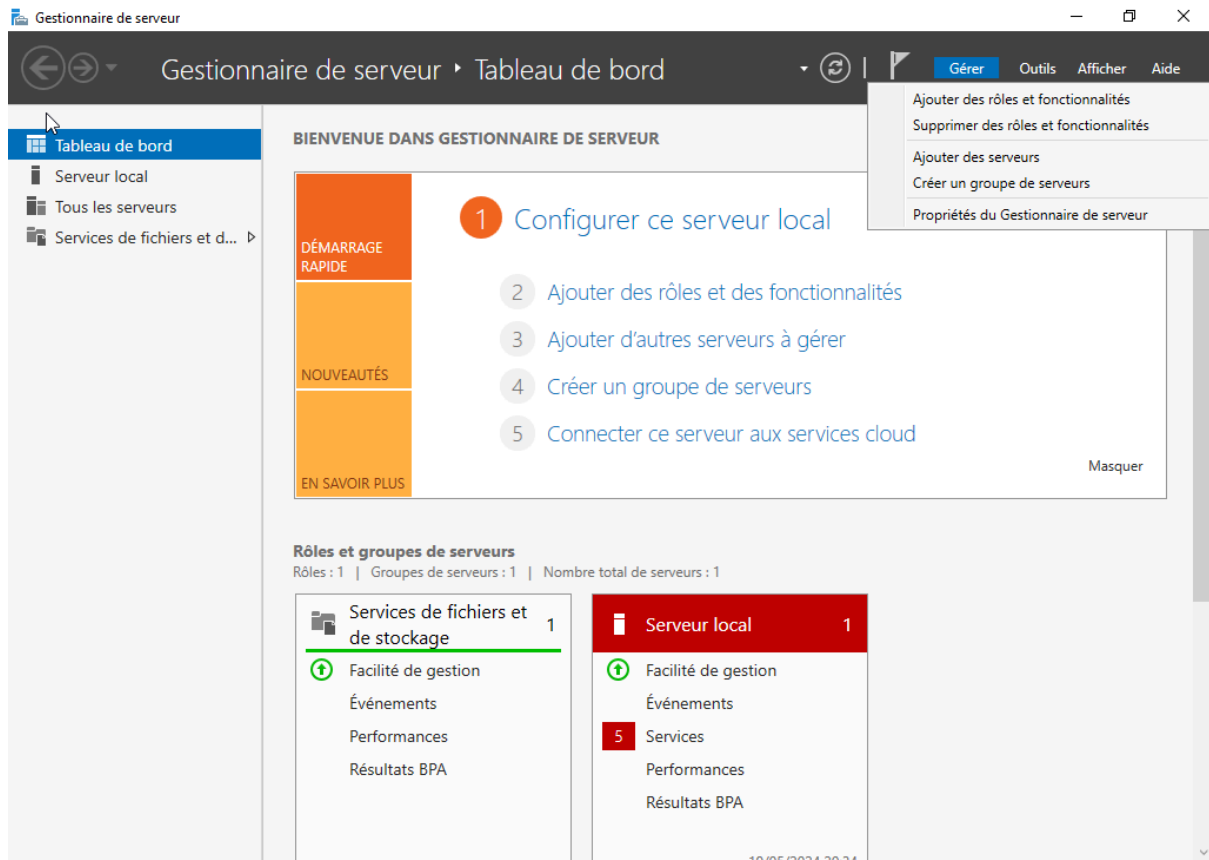


Il faut à présent redémarrer le serveur dhcp pour qu'on puisse rejoindre le domaine Resto.fr :

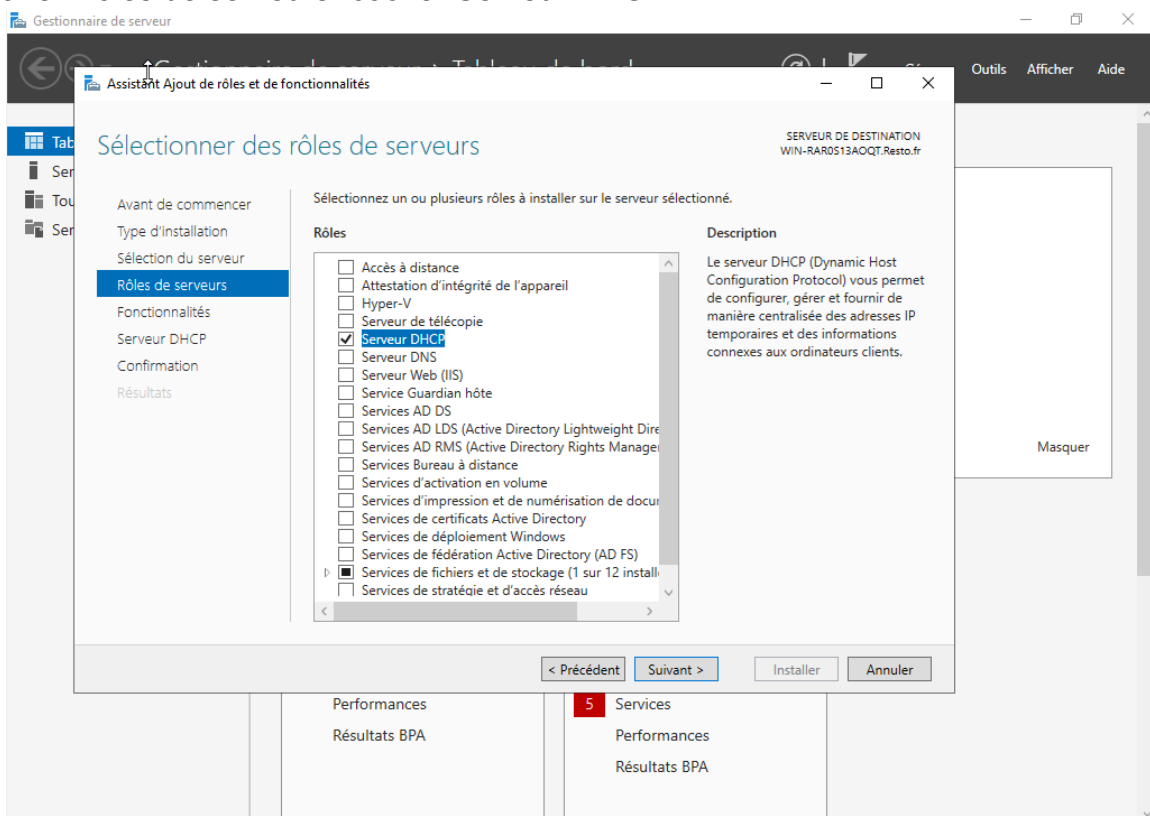


Installation du DHCP :

Le DHCP est une fonctionnalité, donc nous allons d'abord l'installer, et pour effectuer cela nous devons cliquer sur :
"Gérer" puis ajouter des rôles et fonctionnalités.



Dans "Rôles de serveurs" cocher Serveur DHCP.



Ensuite faire suivant jusqu'à Installer.

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
WIN-RAR0S13AOQT.Resto.fr

Confirmer les sélections d'installation

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Serveur DHCP
Confirmation
Résultats

Pour installer les rôles, services de rôle ou fonctionnalités suivants sur le serveur sélectionné, cliquez sur Installer.

Redémarrer automatiquement le serveur de destination, si nécessaire

Il se peut que des fonctionnalités facultatives (comme des outils d'administration) soient affichées sur cette page, car elles ont été sélectionnées automatiquement. Si vous ne voulez pas installer ces fonctionnalités facultatives, cliquez sur Précédent pour désactiver leurs cases à cocher.

Outils d'administration de serveur distant
Outils d'administration de rôles
Outils du serveur DHCP

Serveur DHCP

Exporter les paramètres de configuration
Spécifier un autre chemin d'accès source

< Précédent Suivant > Installer Annuler

Assistant Ajout de rôles et de fonctionnalités

SERVEUR DE DESTINATION
WIN-RAR0S13AOQT.Resto.fr

Progression de l'installation

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveur
Fonctionnalités
Serveur DHCP
Confirmation
Résultats

Afficher la progression de l'installation

i Installation de fonctionnalité

Sélectionner le serveur de destination en requise. Installation réussie sur WIN-RAR0S13AOQT.Resto.fr.

Serveur DHCP
Lancer l'Assistant Post-installation DHCP
Terminer la configuration DHCP

Outils d'administration de serveur distant
Outils d'administration de rôles
Outils du serveur DHCP

1 Vous pouvez fermer cet Assistant sans interrompre les tâches en cours d'exécution. Examinez leur progression ou rouvrez cette page en cliquant sur Notifications dans la barre de commandes, puis sur Détails de la tâche.

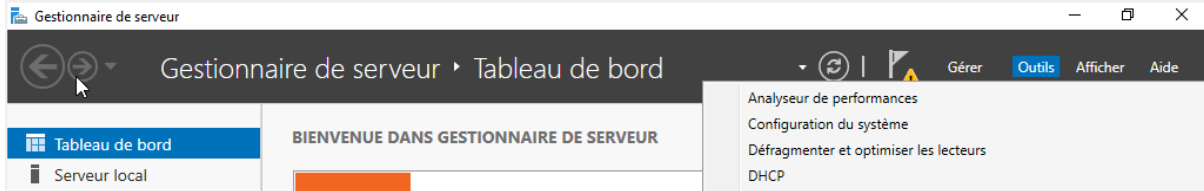
Exporter les paramètres de configuration

< Précédent Suivant > Fermer Annuler

Configuration :

Maintenant nous allons configurer le DHCP.

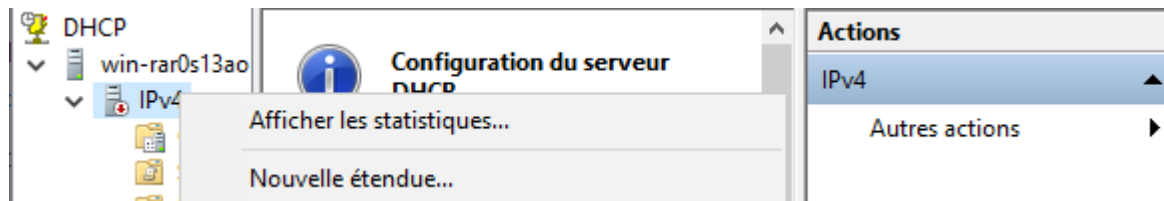
Pour cela cliquer sur “Outils” en haut à droite et DHCP



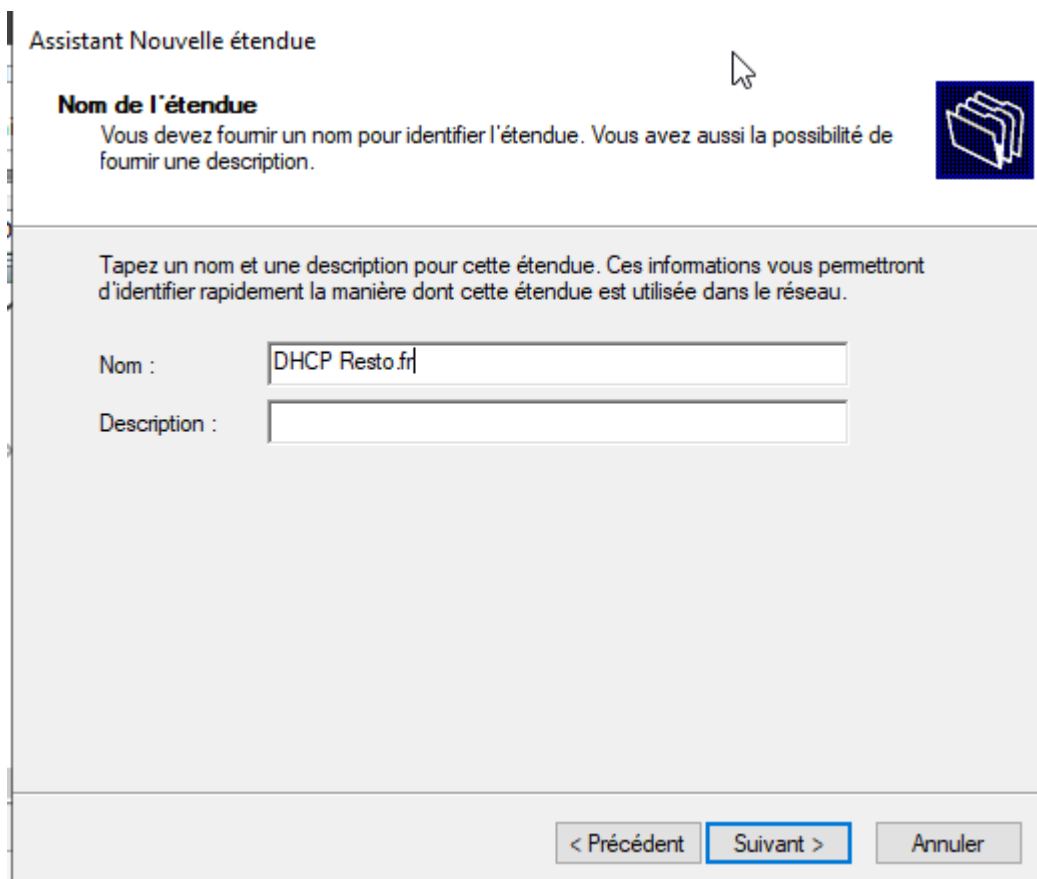
Étendue :

Nous allons créer/mettre en place une étendue d'adresse IP, c'est les IPs qui seront automatiquement attribués à un utilisateurs qui se connecte en DHCP à notre AD.

Clique gauche sur “IPv4” ensuite Nouvelle étendue comme ci-dessous. *****



La première étape est de choisir le nom de notre étendue, ici “ DHCP Resto.fr”

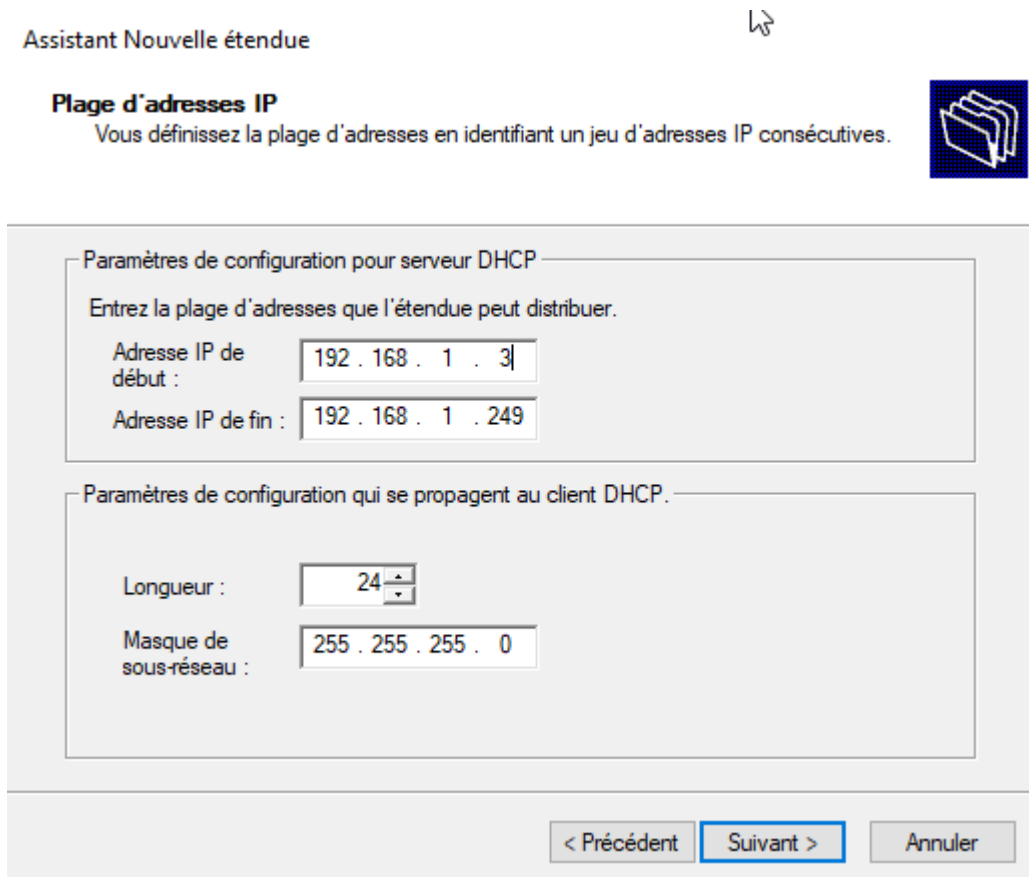
A screenshot of the 'Assistant Nouvelle étendue' wizard. The title is 'Assistant Nouvelle étendue'. The main heading is 'Nom de l'étendue'. Below it, the text says: 'Vous devez fournir un nom pour identifier l'étendue. Vous avez aussi la possibilité de fournir une description.' To the right is a folder icon. Below this, a larger text block says: 'Tapez un nom et une description pour cette étendue. Ces informations vous permettront d'identifier rapidement la manière dont cette étendue est utilisée dans le réseau.' There are two input fields: 'Nom :' with the text 'DHCP Resto.fr' and 'Description :' which is empty. At the bottom, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'. The 'Suivant >' button is highlighted with a blue border.

La partie la plus **importante**, la plage IP nous allons choisir les ip de notre étendue.
La première ip et la dernière qui sera attribuée.

Dans notre exemple les utilisateurs pourront avoir une ip entre 192.168.1.3/24 et 192.168.1.249/24

Automatiquement le masque sous-réseau sera attribué.

Une fois fini cliquer sur “Suivant”



Assistant Nouvelle étendue

Plage d'adresses IP
Vous définissez la plage d'adresses en identifiant un jeu d'adresses IP consécutives.

Paramètres de configuration pour serveur DHCP

Entrez la plage d'adresses que l'étendue peut distribuer.

Adresse IP de début : 192 . 168 . 1 . 3

Adresse IP de fin : 192 . 168 . 1 . 249

Paramètres de configuration qui se propagent au client DHCP.

Longueur : 24

Masque de sous-réseau : 255 . 255 . 255 . 0

< Précédent Suivant > Annuler

Il nous sera demandé si nous souhaitons que certaines IP ne soient pas attribuées, étant donné que cela ne nous intéresse pas nous cliquons sur suivant .

Ajout d'exclusions et de retard

Les exclusions sont des adresses ou une plage d'adresses qui ne sont pas distribuées par le serveur. Un retard est la durée pendant laquelle le serveur retardera la transmission d'un message DHCP OFFER.



Entrez la plage d'adresses IP que vous voulez exclure. Si vous voulez exclure une adresse unique, entrez uniquement une adresse IP de début.

Adresse IP de début : . . Adresse IP de fin : . .

Plage d'adresses exclue :

Retard du sous-réseau en millisecondes :

La durée du bail représente la durée pendant laquelle la machine possèdera une adresse IP de l'étendue.

Durée du bail

La durée du bail spécifie la durée pendant laquelle un client peut utiliser une adresse IP de cette étendue.



La durée du bail doit théoriquement être égale au temps moyen durant lequel l'ordinateur est connecté au même réseau physique. Pour les réseaux mobiles constitués essentiellement par des ordinateurs portables ou des clients d'accès à distance, des durées de bail plus courtes peuvent être utiles.

De la même manière, pour les réseaux stables qui sont constitués principalement d'ordinateurs de bureau ayant des emplacements fixes, des durées de bail plus longues sont plus appropriées.

Définissez la durée des baux d'étendue lorsqu'ils sont distribués par ce serveur.

Limitée à :

Jours : Heures : Minutes :

Ensuite nous cliquons sur suivant afin de pouvoir configurer les adresses IP des routeurs, configurer le DNS, WINS pour l'étendue

Nous renseignons la passerelle par défaut qui sera distribuée par l'étendue à toutes les machines du domaine en + de leurs adresses IP respectives.

Assistant Nouvelle étendue

Routeur (passerelle par défaut)
Vous pouvez spécifier les routeurs, ou les passerelles par défaut, qui doivent être distribués par cette étendue.

Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP :

<input type="text" value="."/>	Ajouter
192.168.1.1	Supprimer
	Monter
	Descendre

< Précédent **Suivant >** Annuler

Puis, nous laisserons le nom de domaine de l'AD tel que nous l'avons préalablement défini :

Assistant Nouvelle étendue

Nom de domaine et serveurs DNS
DNS (Domain Name System) mappe et traduit les noms de domaines utilisés par les clients sur le réseau.

Vous pouvez spécifier le domaine parent à utiliser par les ordinateurs clients sur le réseau pour la résolution de noms DNS.

Domaine parent :

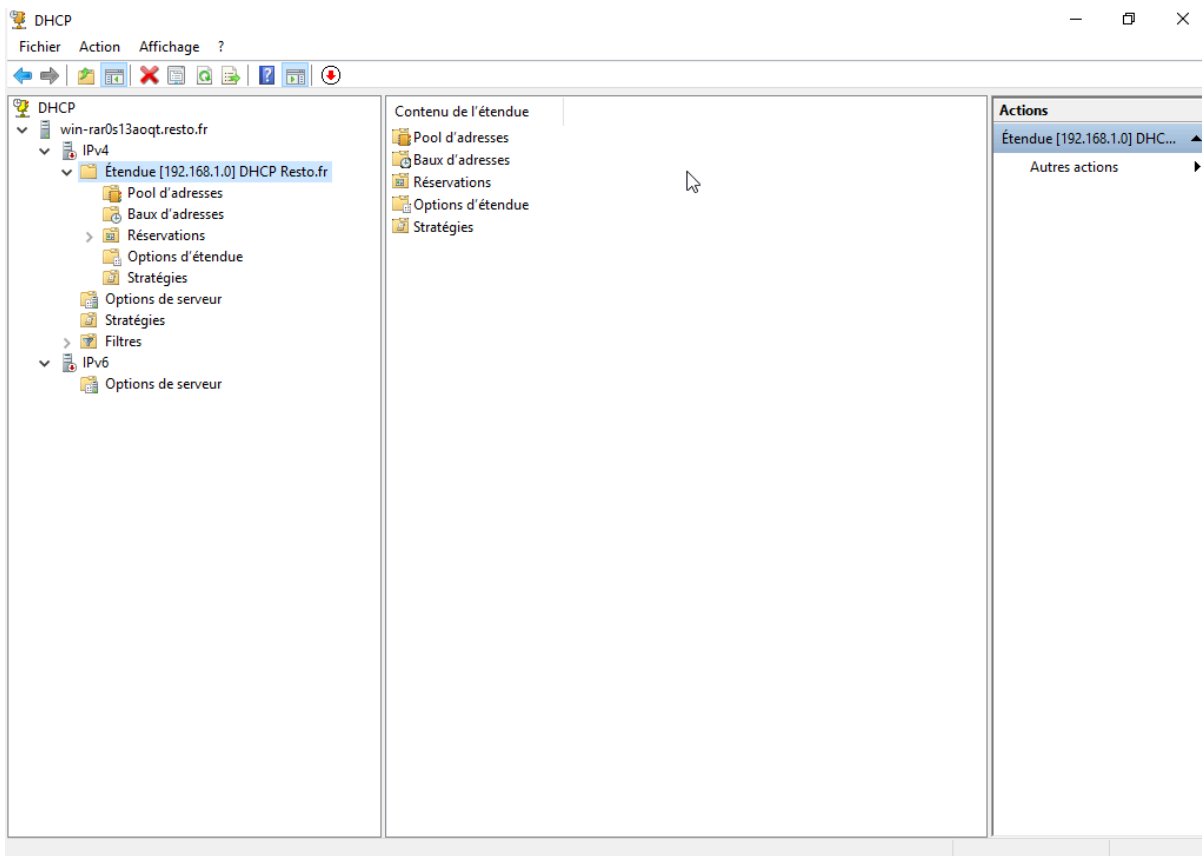
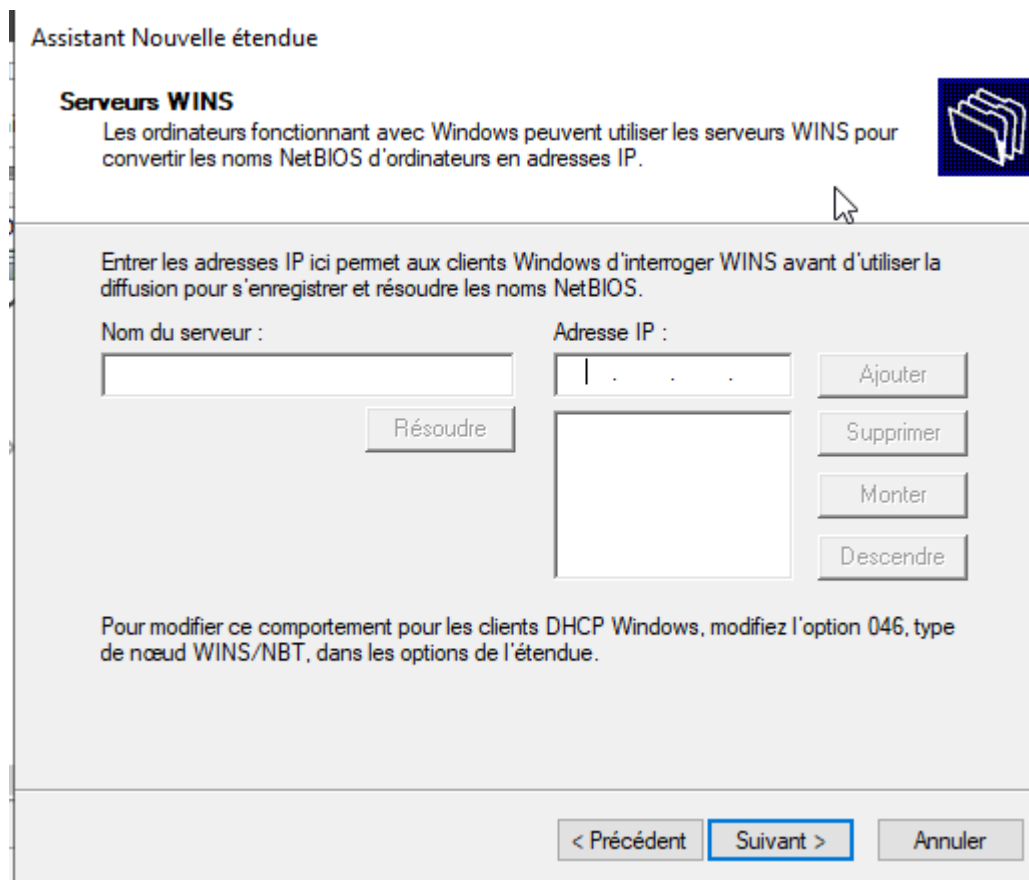
Pour configurer les clients d'étendue pour qu'ils utilisent les serveurs DNS sur le réseau, entrez les adresses IP pour ces serveurs.

<input type="text"/>	Adresse IP :	<input type="text" value="."/>	Ajouter
		192.168.1.1	Supprimer
			Monter
			Descendre

Résoudre

< Précédent **Suivant >** Annuler

Nous n'utilisons pas d'ip pour le WINS, donc "Suivant"



Test du DHCP sur la windows 10 :

Maintenant que le dhcp à été activé il faut le tester nous allons commencer par lui attribuer son ip, sa passerelle ainsi que l'ip du serveur Resto.fr.

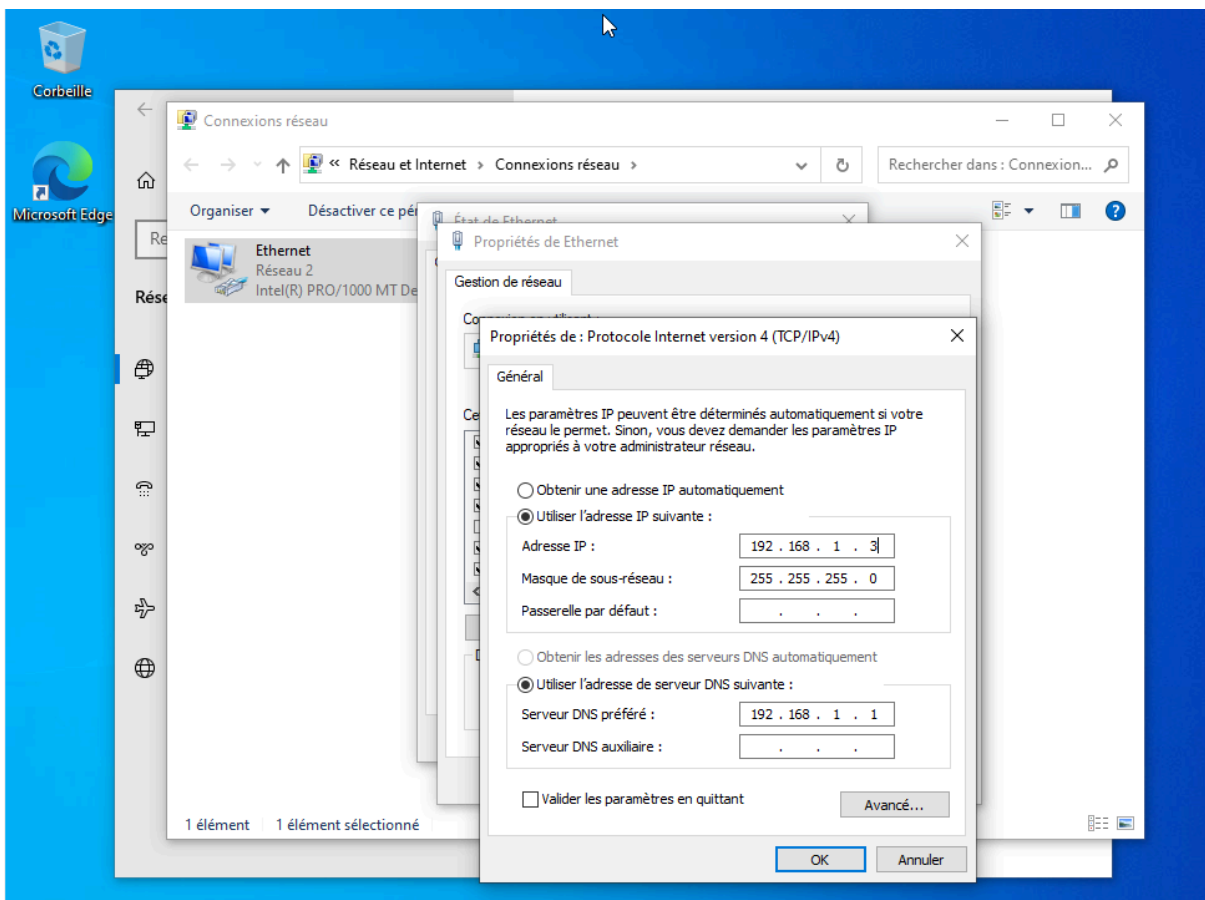
Configuration de l'ip du serveur DHCP de resto.fr :

Dans le shémas de la maquette réseaux il faut mettre la windows client de resto.fr en 192.168.1.3/24 pour cela il faut se rendre dans : "Ouvrir les paramètres réseau et internet" > "Centre Réseau et partage" > "Ethernet" > "Propriétés" > "Protocole Internet Version 4 (TCP/IPv4)" .

Sélectionner "Utiliser l'adresse IP suivante" et mettre dans "Adresse ip" 192.168.1.2.

Ensuite dans "Masque de sous-réseau" 255.255.255.0 " qui correspond au /24 .

Pour finir spécifier l'IP du serveur DNS qui est 192.168.1.1 .

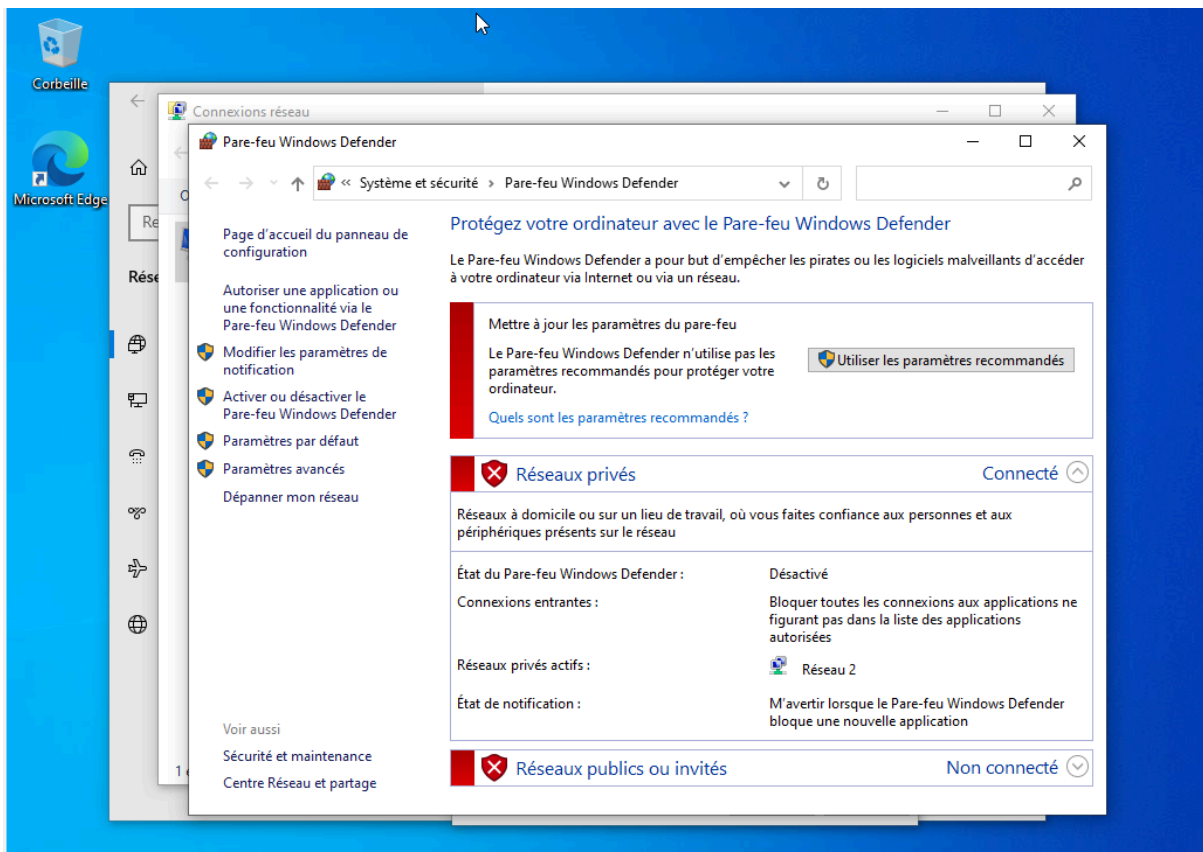


Désactivation du pare-feu :

Il faut désactiver la sécurité du pare-feu car si nous ne le faisons pas cela peut empêcher notre machine de recevoir les paquets lors des pings qui lui sont dédiés.

Pour cela il faut se rendre dans “ Pare-feu Windows Defender” > “ Activer ou désactiver le Pare-feu Windows Defender “ .

Pour finir enlever tous la sécurité du Pare-feu de Windows Defender :

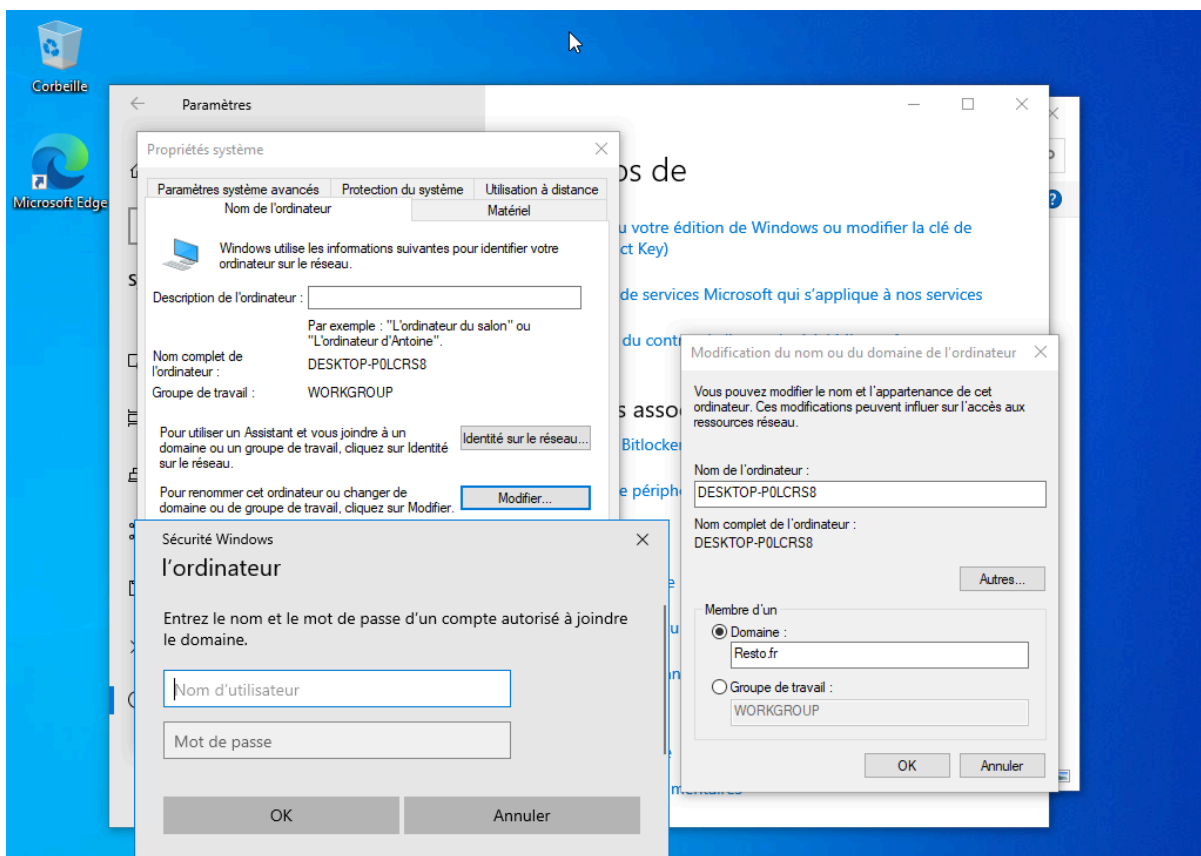
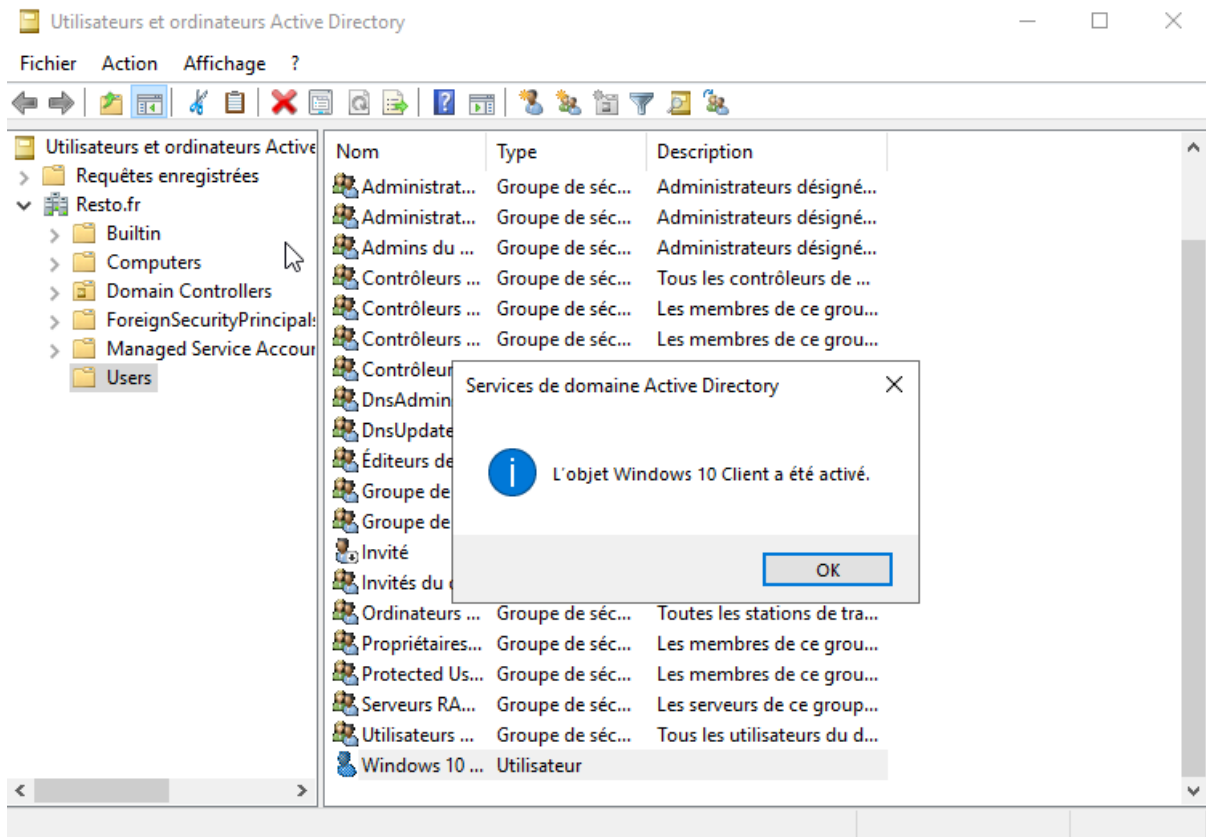


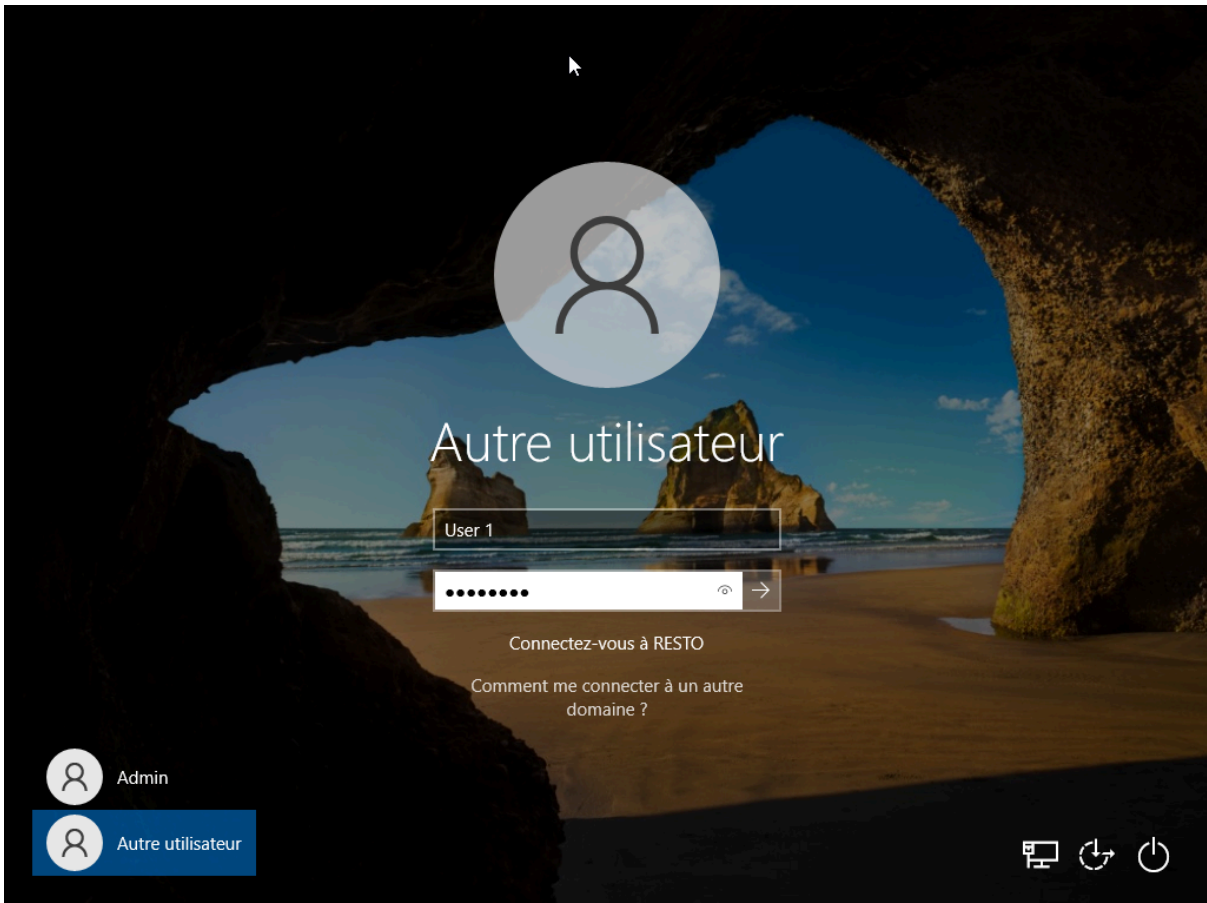
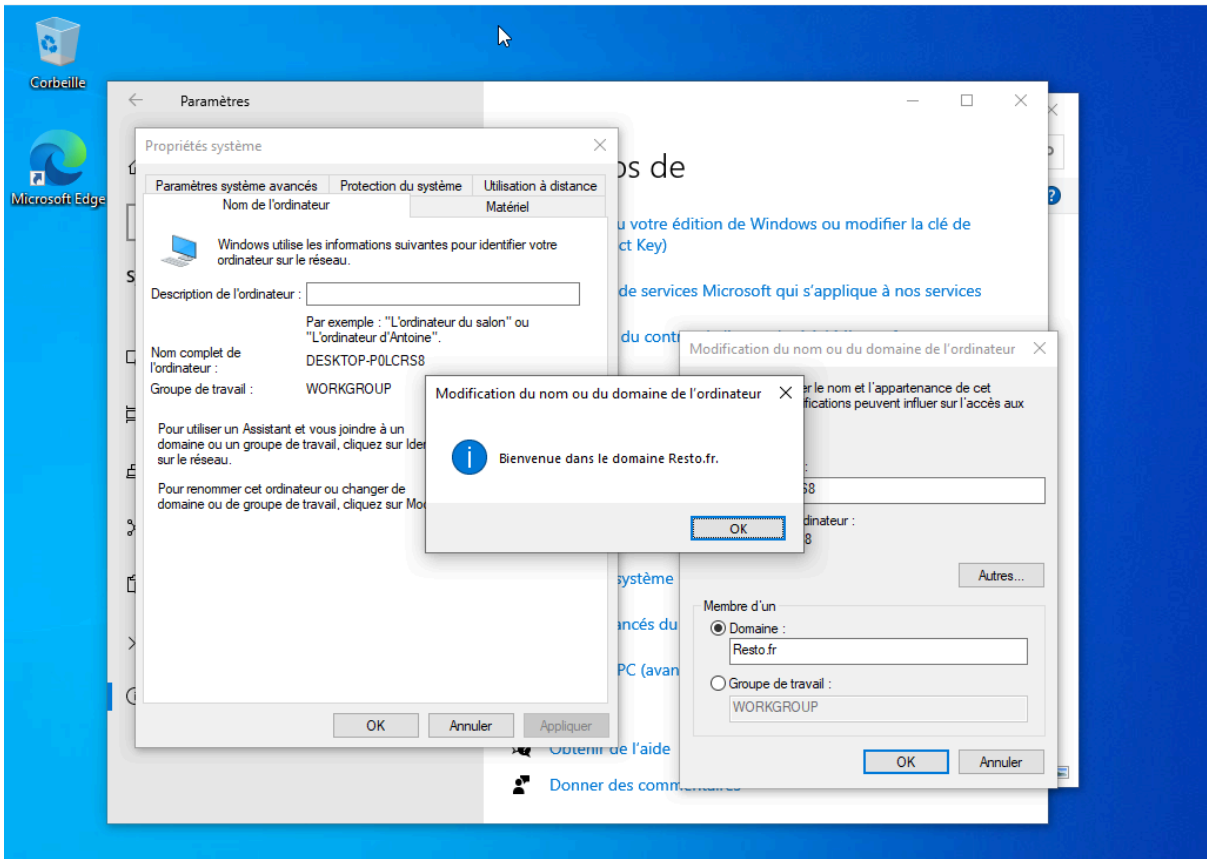
Rejoindre le domaine Resto.fr :

Le serveur DHCP doit rejoindre le domaine Resto.fr, pour cela il faut se rendre dans : “ Paramètres “ > “ Informations système “ > “ Modifier les paramètres “ > “ Modifier ” .

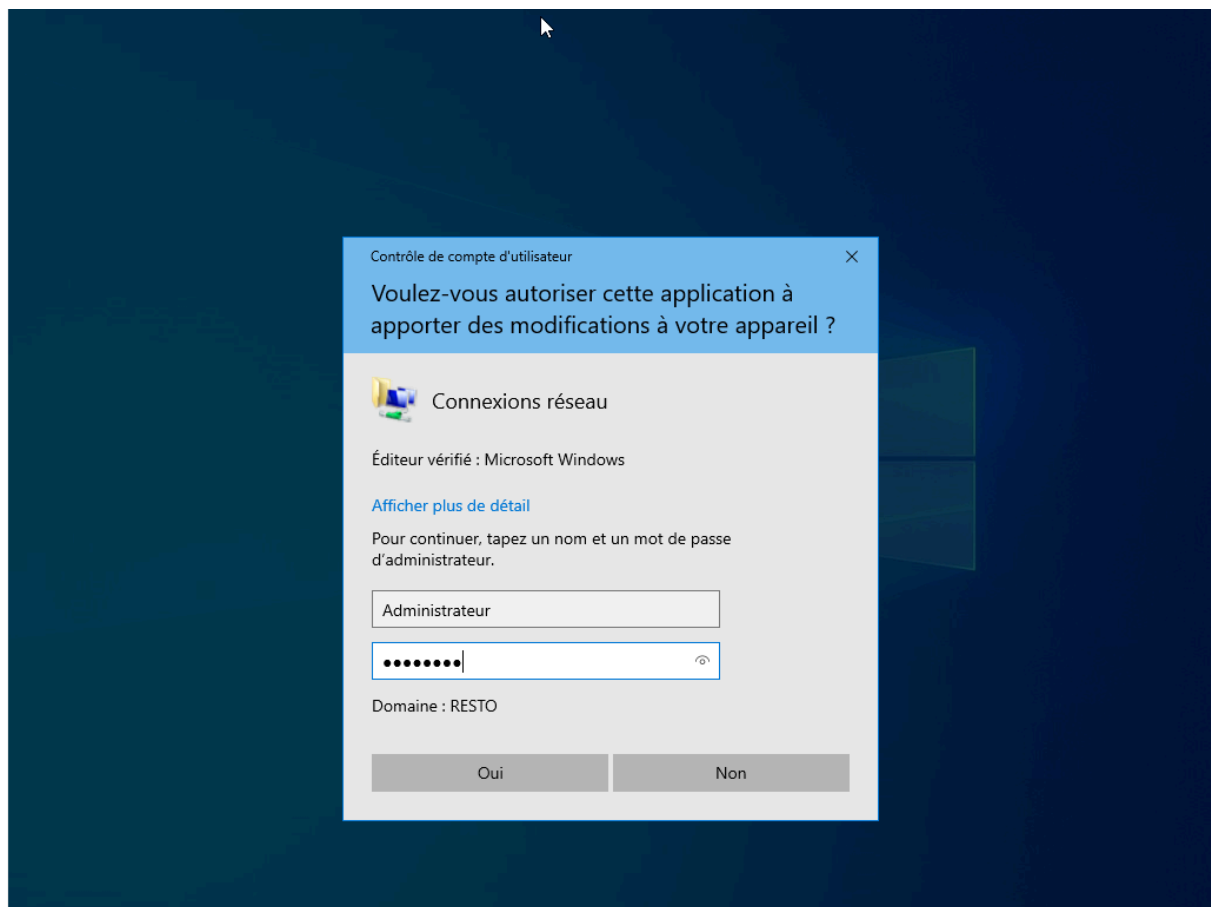
Ensuite sélectionner “ Domaine “ et rentrer le nom de domaine que vous voulez rejoindre.

Nous activons notre compte Windows 10 Client sur notre AD et nous rejoignons le domaine avec la machine Windows 10 Client en utilisant le login et le mot de passe qui est dédié à ce compte **“User 1” “Btssio64”** :

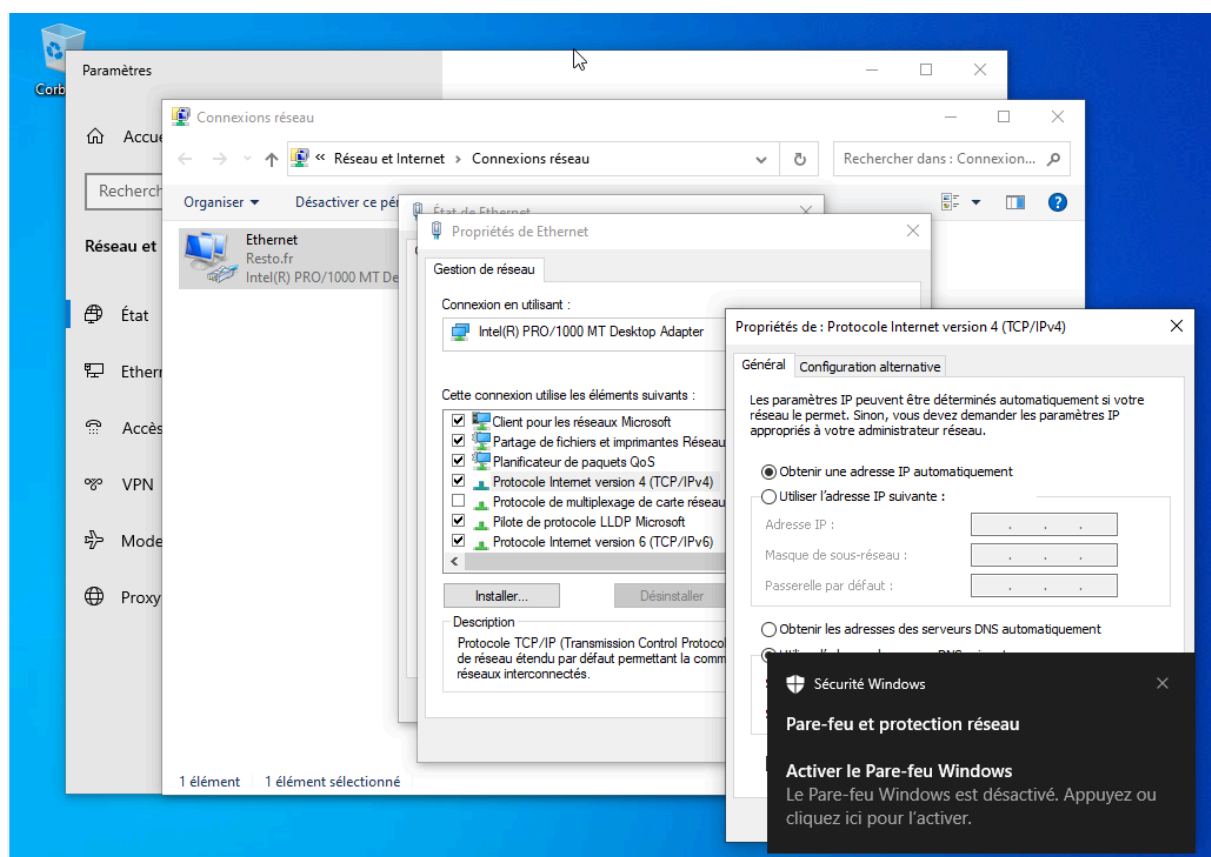


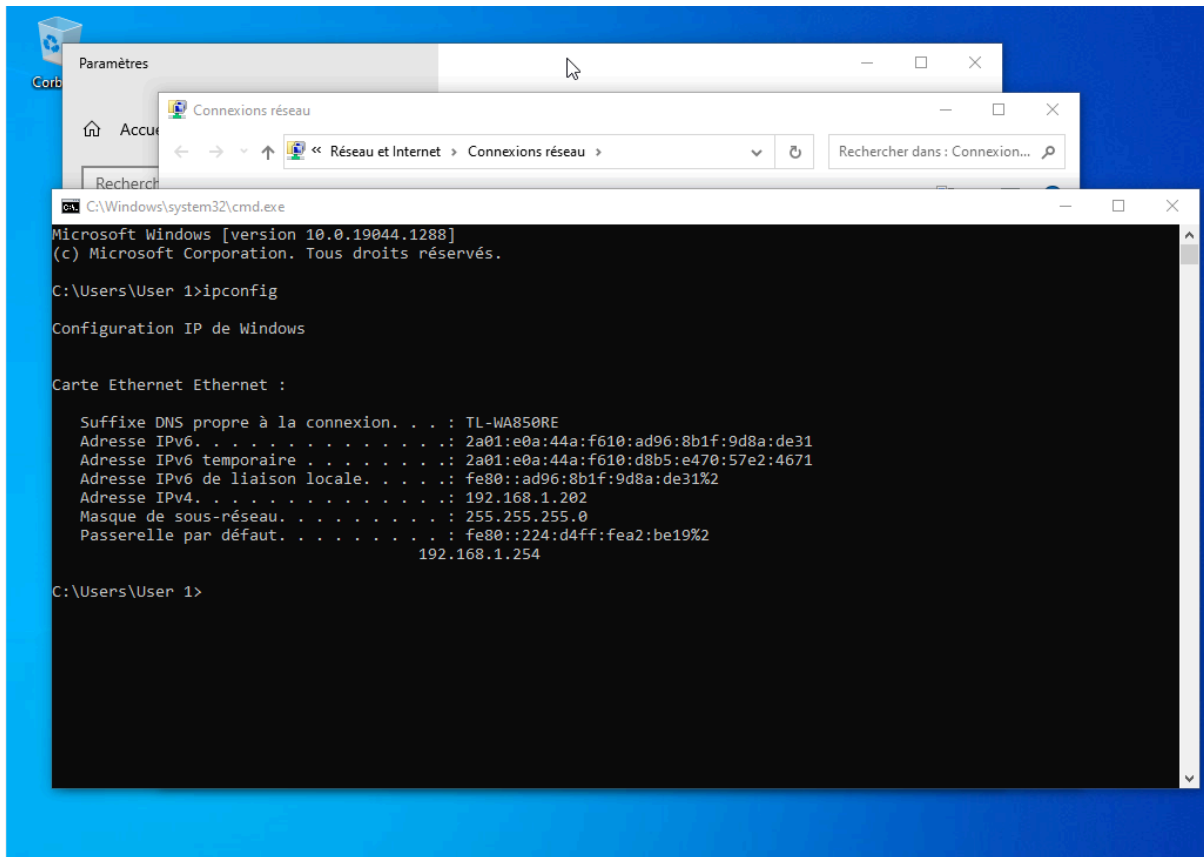


Afin d'effectuer les modifications sur la machine Windows 10 Client nous devons nous connecter en Admin car un simple utilisateur comme User 1 ici ne doit en aucun posséder des droits admins tel que le changement d'IP :



Avec cette machine Windows 10 Client et nos droits admins nous pouvons tester et vérifier le bon fonctionnement de notre serveur DHCP nouvellement créé :





```
C:\Users\User 1>ping 192.168.1.1

Envoi d'une requête 'Ping' 192.168.1.1 avec 32 octets de données :
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.1 : octets=32 temps=26 ms TTL=128
Réponse de 192.168.1.1 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.1 : octets=32 temps=76 ms TTL=128

Statistiques Ping pour 192.168.1.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 76ms, Moyenne = 26ms

C:\Users\User 1>ping 192.168.1.162

Envoi d'une requête 'Ping' 192.168.1.162 avec 32 octets de données :
Réponse de 192.168.1.162 : octets=32 temps=9 ms TTL=128
Réponse de 192.168.1.162 : octets=32 temps=1 ms TTL=128
Réponse de 192.168.1.162 : octets=32 temps=3 ms TTL=128
Réponse de 192.168.1.162 : octets=32 temps=1 ms TTL=128

Statistiques Ping pour 192.168.1.162:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 9ms, Moyenne = 3ms

C:\Users\User 1>
```

Vérifications effectuées et nous constatons le bon fonctionnement du DHCP

Mise en place et configuration de notre serveur TFTP sous Linux (Debian 12) :

Nous nous connectons en root sur notre serveur Linux :

```
Debian GNU/Linux 12 TemplateDebian12 tty1
TemplateDebian12 login: root
Password:
Linux TemplateDebian12 6.1.0-10-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.38-1 (2023-07-14) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon May 20 16:32:46 CEST 2024 on tty1
root@TemplateDebian12:~#
```

Nous modifions l'IP de la machine Linux afin que cette dernière corresponde au schéma réseau présent au début de ce doc :

192.168.1.3/24

```
root@TemplateDebian12:~# nano /etc/network/interfaces
```

```
GNU nano 7.2 /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.1.3
    netmask 255.255.255.0
    gateway 192.168.1.1

# This is an autoconfigured IPv6 interface
iface enp0s3 inet6 auto
```

```
root@TemplateDebian12:~# ifdown enp0s3
root@TemplateDebian12:~# ifup enp0s3
root@TemplateDebian12:~# systemctl restart networking
```

```

root@TemplateDebian12:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:12:33:67 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.3/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 2a01:e0a:44a:f610:a00:27ff:fe12:3367/64 scope global dynamic mngtmpaddr
        valid_lft 86378sec preferred_lft 86378sec
    inet6 fe80::a00:27ff:fe12:3367/64 scope link
        valid_lft forever preferred_lft forever

```

On change le miroir de notre machine Debian :

```

root@SRV-DEBIAN-01:~# nano /etc/apt/sources.list

```

```

GNU nano 7.2 /etc/apt/sources.list
deb http://deb.debian.org/debian/ bookworm main

```

Nous lançons la mise à jours des programmes et logiciels de la machine avec la commande suivante :

```

root@TemplateDebian12:~# apt update_

```

```

root@TemplateDebian12:~# apt upgrade_

```

```

Progression : [ 63%] [#####.....]

```

Installation de "ufw" :

UFW (Uncomplicated Firewall) est un outil de gestion de pare-feu conçu pour faciliter la configuration des règles de pare-feu sur les systèmes Linux.

```
root@TemplateDebian12:/# apt install ufw_
```

On effectue la commande suivante :

```
root@TemplateDebian12:/# ufw allow tftp
Rules updated
Rules updated (v6)
```

On installe le client TFTP avec la commande suivante :

```
root@TemplateDebian12:/# apt install tftpd-hpa
```

On installe le serveur TFTP avec la commande suivante :

```
root@TemplateDebian12:/# apt install tftp_
```

Maintenant nous allons ouvrir le port 69 qui correspond au port du tftp pour pouvoir configurer le serveur :

```
root@TemplateDebian12:/# nano /etc/default/tftpd-hpa
```

```
GNU nano 7.2 /etc/default/tftpd-hpa *
# /etc/default/tftpd-hpa

TFTP_USERNAME="tftp"
TFTP_DIRECTORY="/srv/tftp"
TFTP_ADDRESS="192.168.1.3:69"
TFTP_OPTIONS="--secure --create"
```

Nous modifions le propriétaire du fichier tftp à l'utilisateur tftp :

```
root@TemplateDebian12:/# chown tftp:tftp /srv/tftp
```

Puis nous redémarrons le service TFTP :

```
root@TemplateDebian12:/# systemctl restart tftpd-hpa
root@TemplateDebian12:/# _
```

Afin de s'assurer du bon fonctionnement nous nous connectons au serveur via la commande suivante :

```
root@TemplateDebian12:/# tftp 192.168.1.3
tftp> _
```

Nous effectuons des pings entre les différents serveurs afin de s'assurer du bon fonctionnement des VM :

```
root@TemplateDebian12:/# ping 192.168.1.162
PING 192.168.1.162 (192.168.1.162) 56(84) bytes of data.
64 bytes from 192.168.1.162: icmp_seq=1 ttl=128 time=0.522 ms
64 bytes from 192.168.1.162: icmp_seq=2 ttl=128 time=0.275 ms
^C
--- 192.168.1.162 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1027ms
rtt min/avg/max/mdev = 0.275/0.398/0.522/0.123 ms
root@TemplateDebian12:/# ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=128 time=0.376 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=128 time=0.365 ms
^C
--- 192.168.1.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1018ms
rtt min/avg/max/mdev = 0.365/0.370/0.376/0.005 ms
root@TemplateDebian12:/#
```

Pour l'épreuve E5 nous rajouterons un glpi

Installation de GLPI version 9.5.0

Tout d'abord nous lançons la mise à jours des programmes et logiciels de la machine avec la commande suivante :

```
root@SRV-DEBIAN-01:/# apt-get update
```

```
root@SRV-DEBIAN-01:/# apt upgrade_
```

Ensuite il faut installer mariadb à l'aide de la commande suivante :

```
root@SRV-DEBIAN-01:/# apt install mariadb-server
```

Après il faut se connecter à la base de donnée à l'aide de la commande suivante.

```
root@SRV-DEBIAN-01:/# mysql -u root -p_
```

```
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.5.23-MariaDB-0+deb11u1 Debian 11

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

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

MariaDB [(none)]> _
```

Il faut à présent créer une base de donnée qui s'appellera glpi :

```
MariaDB [(none)]> CREATE DATABASE glpi;_
```

Pour savoir si la base donnée nommée glpi a bien été créée il faut taper la commande suivante :

```
MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| glpi     |
| information_schema |
| mysql    |
| performance_schema |
+-----+
4 rows in set (0,000 sec)
```

La prochaine étape est de créer un compte administrateur qui aura tous les droits et de lui rajouter un mot de passe dans la base de donnée de glpi à l'aide des commandes suivantes :

```
MariaDB [(none)]> CREATE USER 'glpi'@'localhost' IDENTIFIED BY 'glpi';_
```

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON glpi.* TO 'glpi'@'localhost' WITH GRANT OPTION;
```



```
MariaDB [(none)]> FLUSH PRIVILEGES;
```

Une fois que les droits ont été bien appliqués, il faut installer un serveur web(apache2) + php pour faire un serveur LAMP(Linux, Apache, Mariadb et PHP) à l'aide de la commande suivante :

```
MariaDB [(none)]> exit
Bye
root@SRV-DEBIAN-01:/# apt install apache2 php
```

Une fois cela fait il faut installer d'autre extension php avec la commande suivante :

```
apt install php-mysql, php-mysqli,php-json, php-mbstring, php-simplexml, php-xml,
php-cgi, php-cli, php- common, php-gd, php-imap, php-ldap, php-apcu,
php-xmlrpc,php-cas, php-curl.
```

(il faut le faire 1 par 1 pour chaque extension pour pas se tromper)

Une fois que les commandes on été faites il faut redémarrer le serveur apache et vérifier si il tourne correctement à l'aide des commandes suivantes :

```
root@SRV-DEBIAN-01:/# systemctl restart apache2
```

```
root@SRV-DEBIAN-01:/# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-05-21 14:23:10 CEST; 48min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 31476 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 31480 (apache2)
     Tasks: 11 (limit: 2340)
    Memory: 37.9M
       CPU: 590ms
   CGroup: /system.slice/apache2.service
           └─31480 /usr/sbin/apache2 -k start
             └─31481 /usr/sbin/apache2 -k start
               └─31482 /usr/sbin/apache2 -k start
                 └─31483 /usr/sbin/apache2 -k start
                   └─31484 /usr/sbin/apache2 -k start
                     └─31485 /usr/sbin/apache2 -k start
                       └─31597 /usr/sbin/apache2 -k start
                         └─31601 /usr/sbin/apache2 -k start
                           └─31602 /usr/sbin/apache2 -k start
                             └─31603 /usr/sbin/apache2 -k start
                               └─31604 /usr/sbin/apache2 -k start

mai 21 14:23:10 SRV-DEBIAN-01 systemd[1]: Starting The Apache HTTP Server...
mai 21 14:23:10 SRV-DEBIAN-01 apachectl[31479]: AH00558: apache2: Could not reliably determine the
mai 21 14:23:10 SRV-DEBIAN-01 systemd[1]: Started The Apache HTTP Server.
lines 1-25/25 (END)
```

Maintenant il faut télécharger glpi avec la commande suivante :

```
root@SRV-DEBIAN-01:/# wget https://github.com/glpi-project/glpi/releases/download/9.5.0/glpi-9.5.0.t
gz
```

Après avoir téléchargé le fichier, vous devez le décompresser à l'aide de la commande suivante :

```
root@SRV-DEBIAN-01:/# tar -xzf glpi-9.5.0.tgz
```

Déplacez les fichiers extraits vers le répertoire de votre serveur web à l'aide de la commande suivante :

```
root@SRV-DEBIAN-01:/# mv glpi /var/www/html/glpi_
```

Il faut à présent configurer les permissions de fichiers pour que le serveur puisse lire et écrire grâce au commande suivantes :

```
root@SRV-DEBIAN-01:/# chown -R www-data:www-data /var/www/html/glpi_
```

```
root@SRV-DEBIAN-01:/# chmod -R 755 /var/www/html/glpi
```

Maintenant il faut continuer la procédure d'installation via un navigateur web en entrant l'ip du serveur glpi qu'on va configurer au préalables à l'aide des commandes suivantes :

```
cd /etc/network
```

```
root@SRV-DEBIAN-01:/etc/network# nano interfaces
```

```
GNU nano 5.4 interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

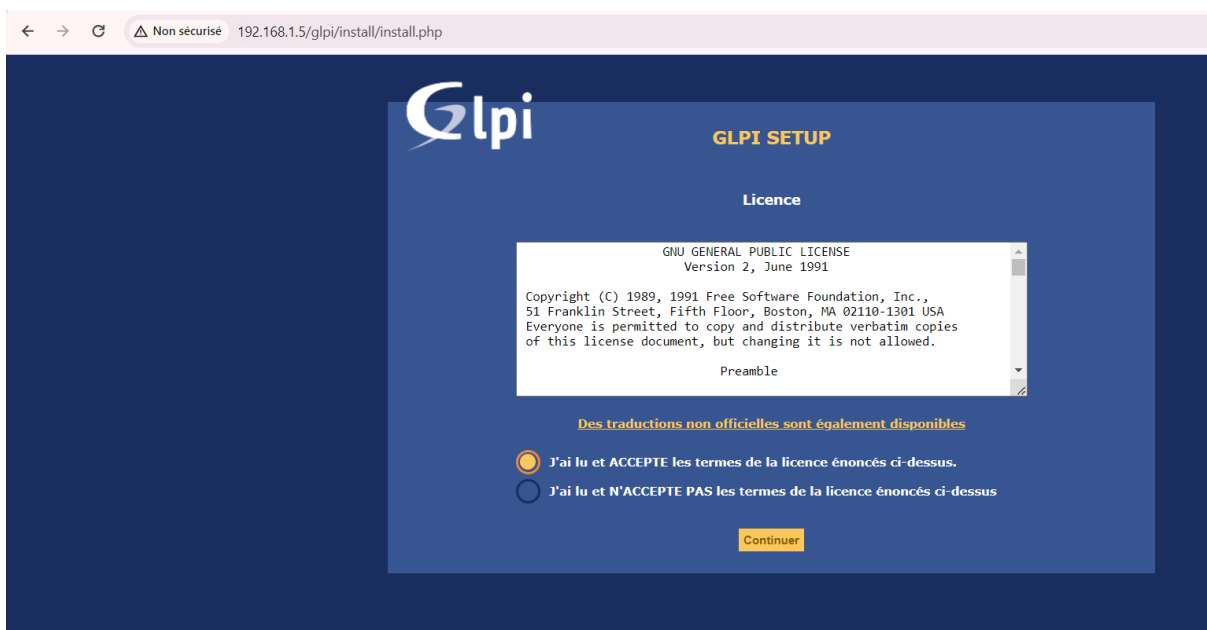
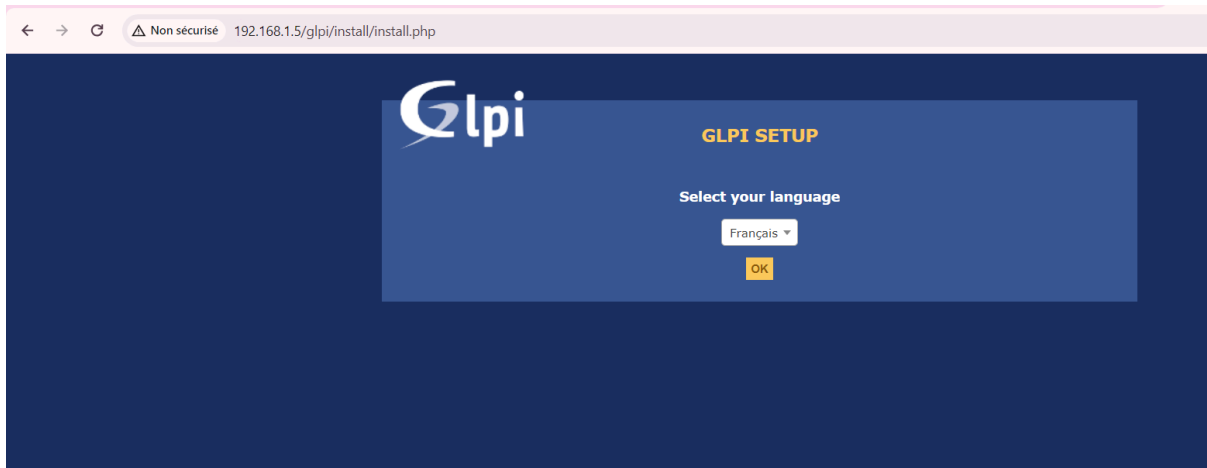
# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
    address 192.168.1.5
    netmask 255.255.255.0
    gateway 192.168.1.1
```

Pour activer l'interface réseaux :

```
root@SRV-DEBIAN-01:/etc/network# ifup enp0s3_
```

```
root@SRV-DEBIAN-01:/etc/network# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default c
000
    link/ether 08:00:27:8b:e0:a7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.5/24 brd 192.168.1.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 2a02:8428:3918:f701:a00:27ff:fe8b:e0a7/64 scope global dynamic mngtmpaddr
        valid_lft 724sec preferred_lft 724sec
    inet6 fe80::a00:27ff:fe8b:e0a7/64 scope link
        valid_lft forever preferred_lft forever
root@SRV-DEBIAN-01:/etc/network#
```

Direction le navigateur web pour pouvoir continuer la procédure d'installation en entrant l'ip du serveur glpi :



On choisit l'option Installer :



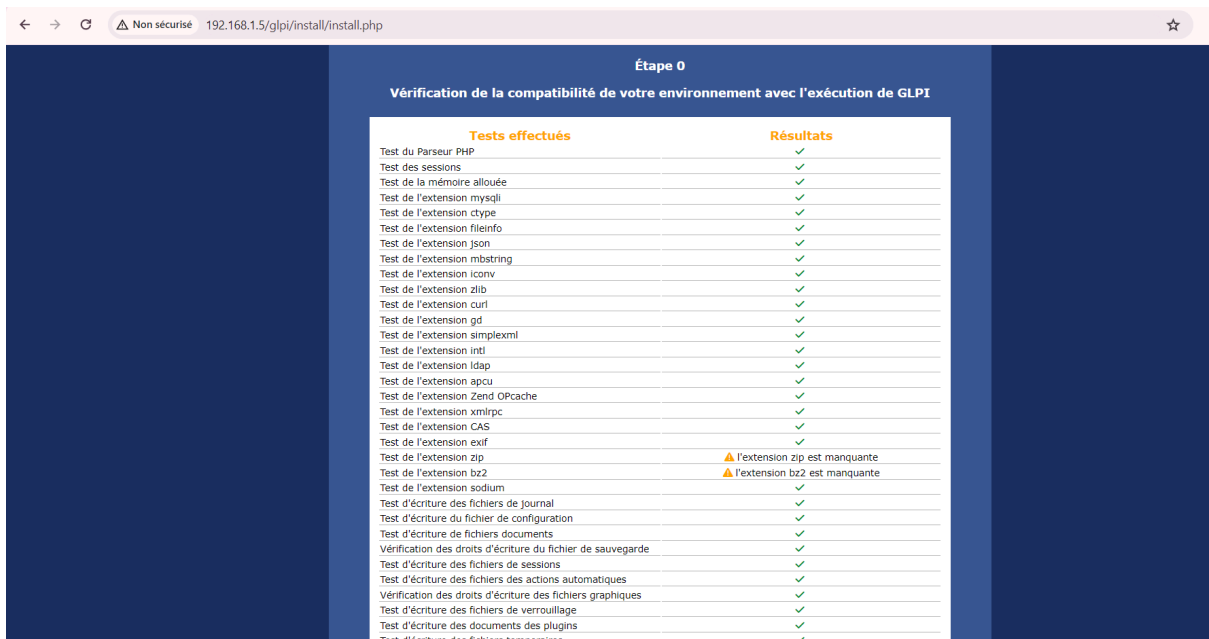
Lors de l'installation il y a une erreur car il manque une extension non installée intl :



```
root@SRV-DEBIAN-01:/etc/network# apt install php-intl_
```

```
root@SRV-DEBIAN-01:/etc/network# systemctl restart apache2_
```

Une fois que l'installation de l'extension intl + redémarrer le serveur apache on revient sur le navigateur web pour constater le changement les autres extensions qui sont pas installés ne sont pas dérangerant pour la suite :



il faut rentrer le nom du serveur sql l'utilisateur ainsi que son mot de passe :



la connexion à réussie on choisit la base de donnée glpi :





Nous voici sur la page d'administration :

