Compte rendu Stage Apo’G

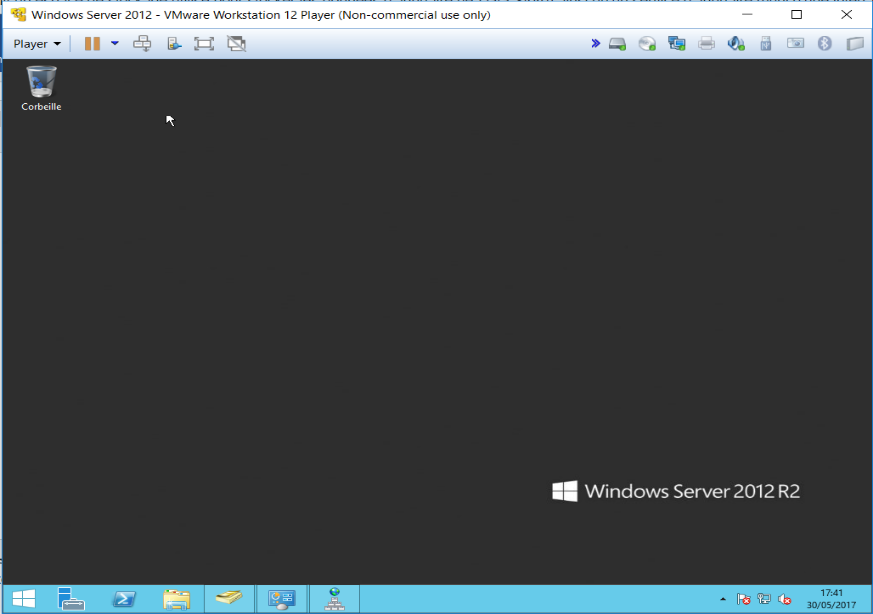
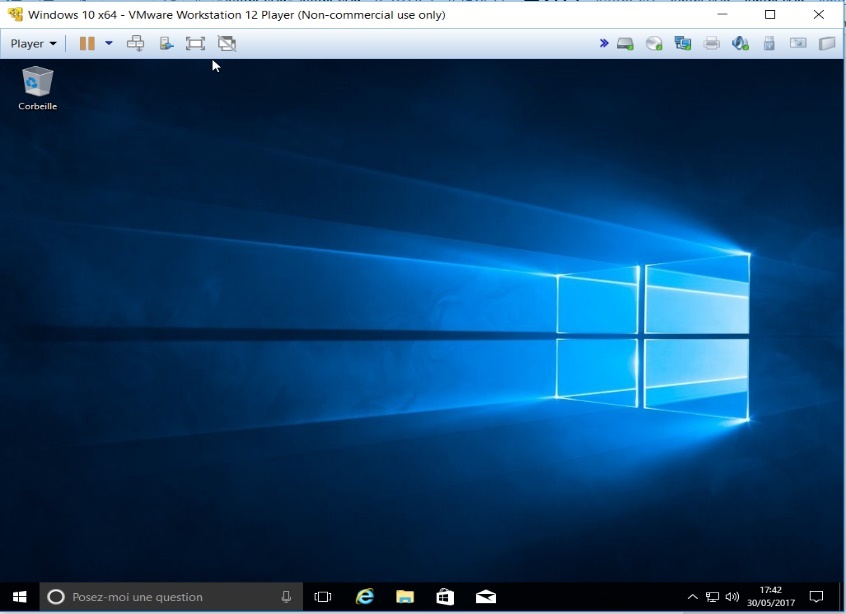
--------------------------------------------------------------------------------------------------------------------------------------

Tout d’abord nous allons installer VMware afin de virtualiser nos machines Windows et Windows server 2012.

Notre projet est de mettre en œuvre un service d’annuaire LDAP (Lightweight Directory Access Protocol) pour les systèmes d’exploitation Windows, Active Directory.

L’objectif principal d’Active Directory est de fournir des services centralisés d’identification à un réseau d’ordinateurs qui utilisent le système Windows. Active Directory permet également l’attribution et l’application de stratégies, distributions de logiciels et installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d’un réseau administré tels que les comptes utilisateurs, serveurs, postes de travail, dossiers partagés, imprimantes, etc.

Nous allons installer les services Active Directory sur un serveur Windows 2012 : L’utilité de Windows Server 2012 est de créer un domaine pour mettre en réseau des postes de travail. Ce serveur sera donc contrôleur de domaine, il aura en plus les rôles de serveur DNS et DHCP.

Dans un premier temps nous allons installer Windows Server 2012 R2 et une machine Windows 10 (le client)

Windows Server 2012 Windows Client

Installation de notre machine client Windows :

* Create a New Virtual Machine, Sélection de L’iso Windows et installation

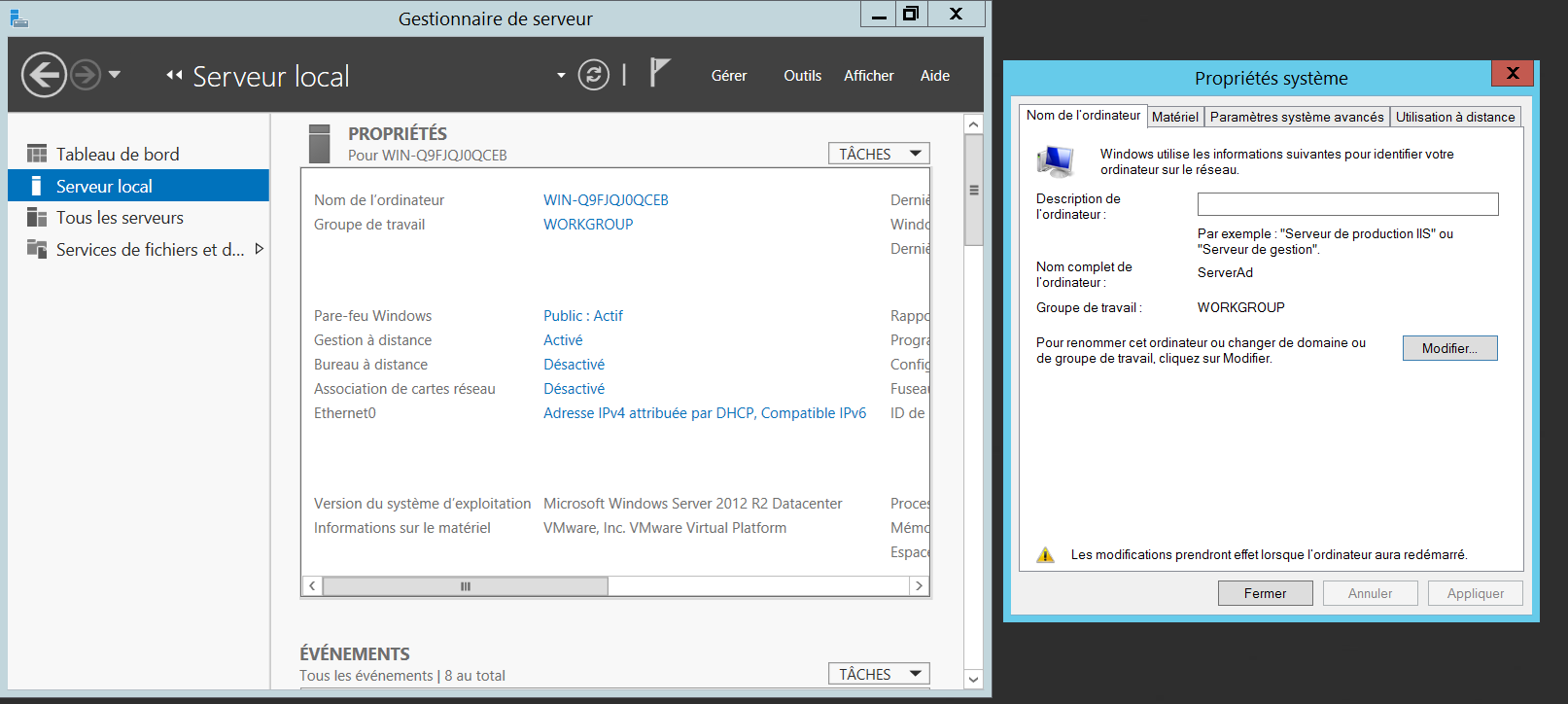
**D:\Stage\ISO Windows\Windows .** Ensuite nous allons suivre la procédure d’installation.

Installation Windows Server avec VMware :

* Create a New Virtual Machine, On sélectionne L’iso de Windows server :

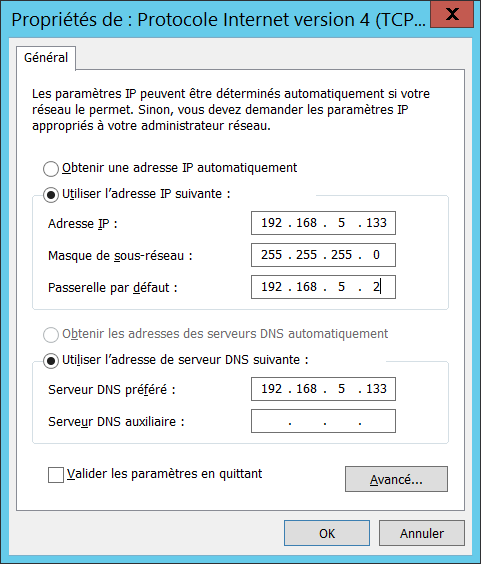
**D:\Stage\ISO Windows\fr\_windows\_server\_2012\_r2\_with\_update\_x64\_dvd\_4048488.iso**

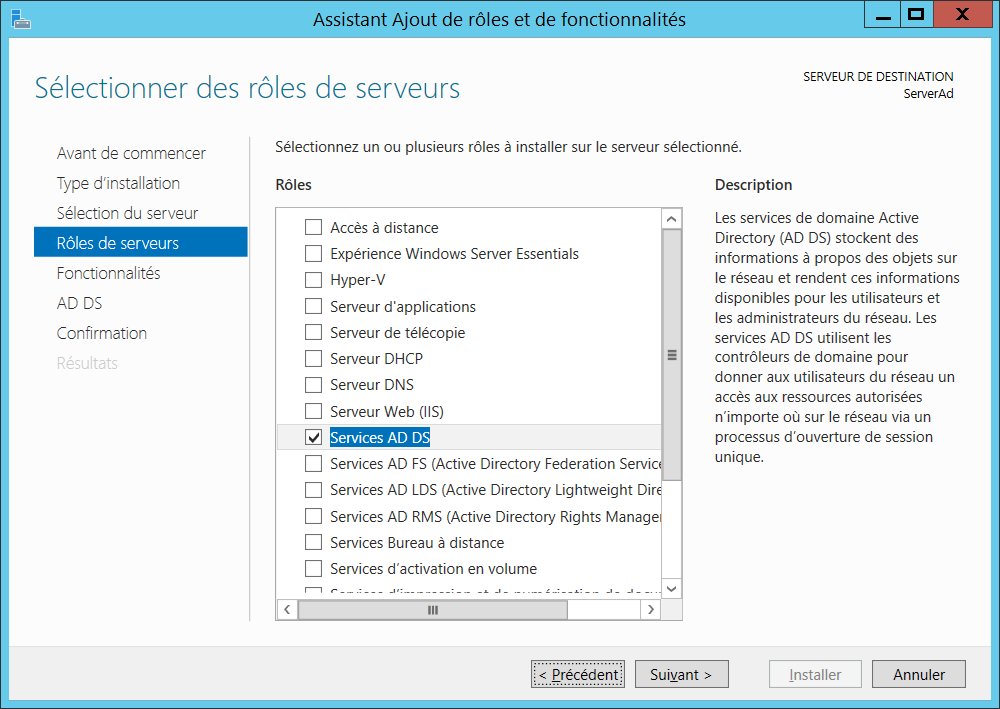
Après avoir installé nos deux machines nous allons mettre en place notre contrôleur de domaine.

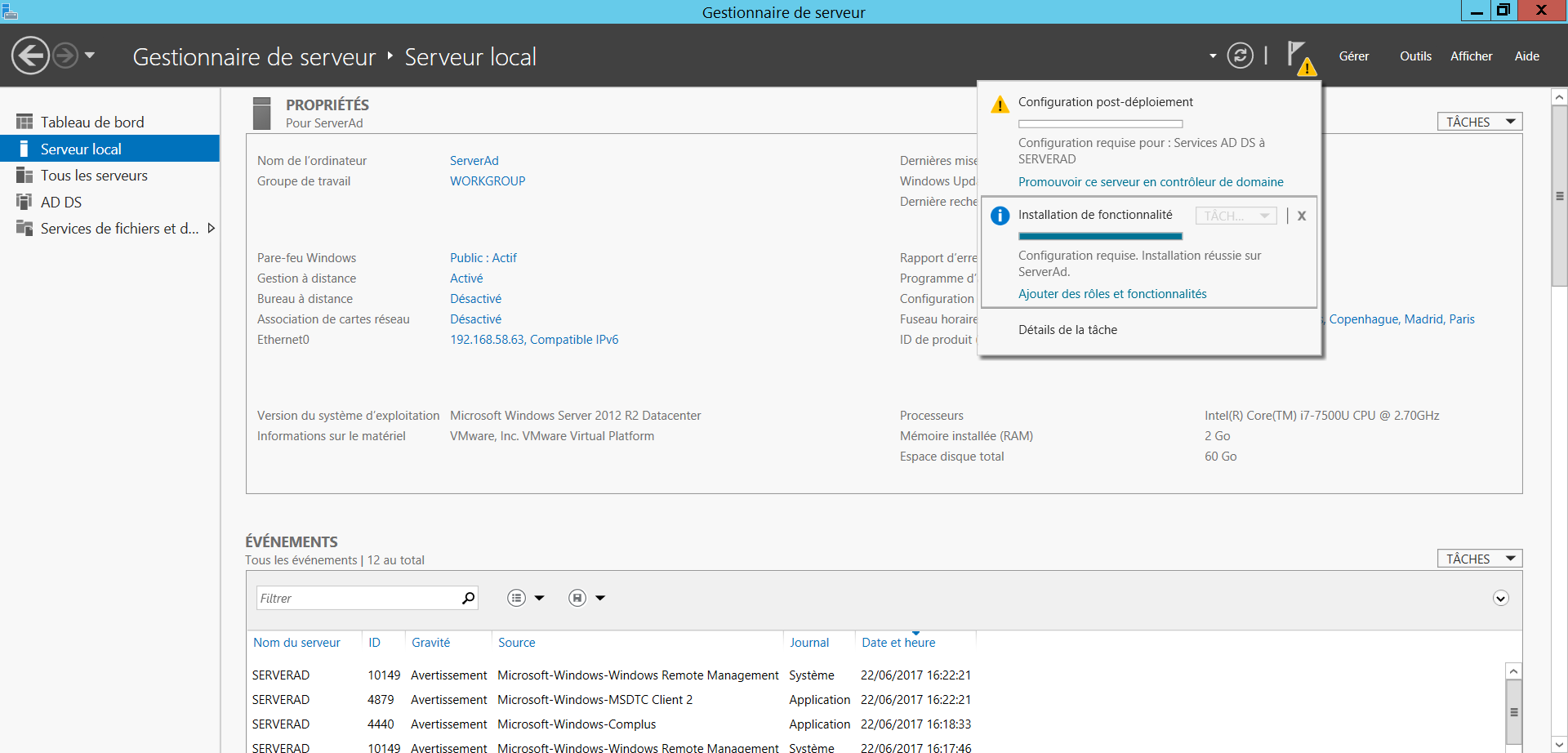
Important ! il faut renommer notre machine Windows Server avant de le déclarer comme contrôleur de domaine. Avant Windows Server 2008 il était impossible de changer le nom du serveur une fois qu’il était devenu contrôleur de domaine ; les systèmes Windows récent le permettent mais il est très dur de le changer après.

Une fois la modification de notre nom de machine fait nous allons redémarrer. Le nom est bien modifié en ServerAd.

Nous attribuons une adresse IP Fixe à notre Windows Server 2012 :

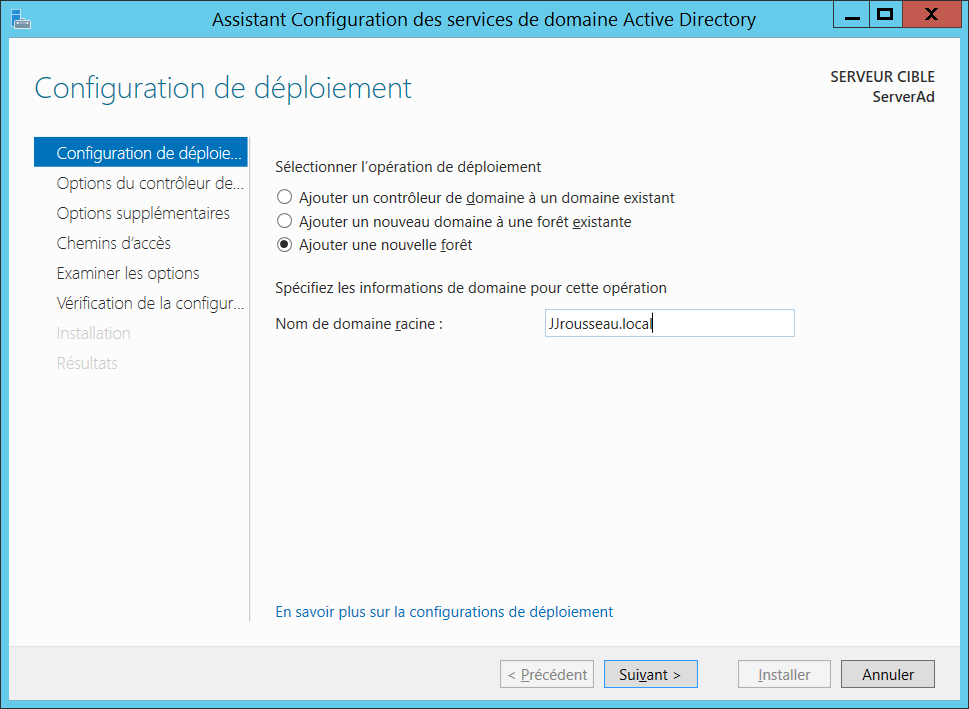
Pourquoi attribuer une IP Fixe ? Il est recommandé par Microsoft que les contrôleurs de domaines est une IP fixe, de plus le DNS doit avoir une IP fixe.

Nous allons maintenant installer le rôle active directory et transformer notre serveur en contrôleur de domaine. Sélection de Service AD DS :

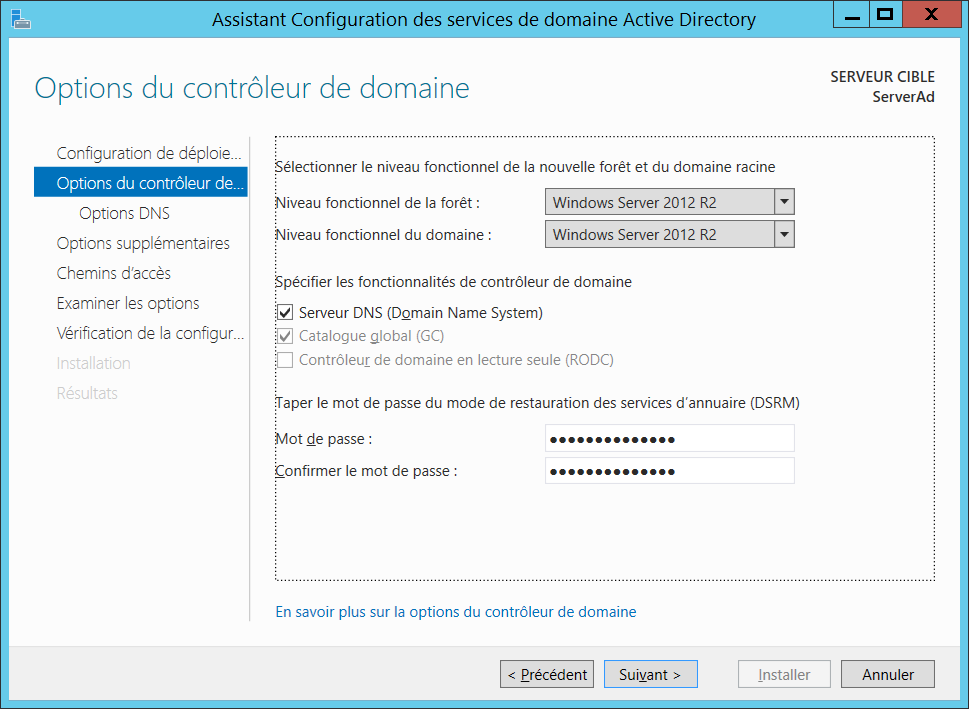
Une fois l’active Directory installé, Nous allons promouvoir ce serveur en contrôleur de domaine :

L’accès à l’assistant de configuration est maintenant possible et il est possible de configurer notre contrôleur de domaine.

Une fois la configuration terminée nous constatons que la connexion se fera sur notre domaine.

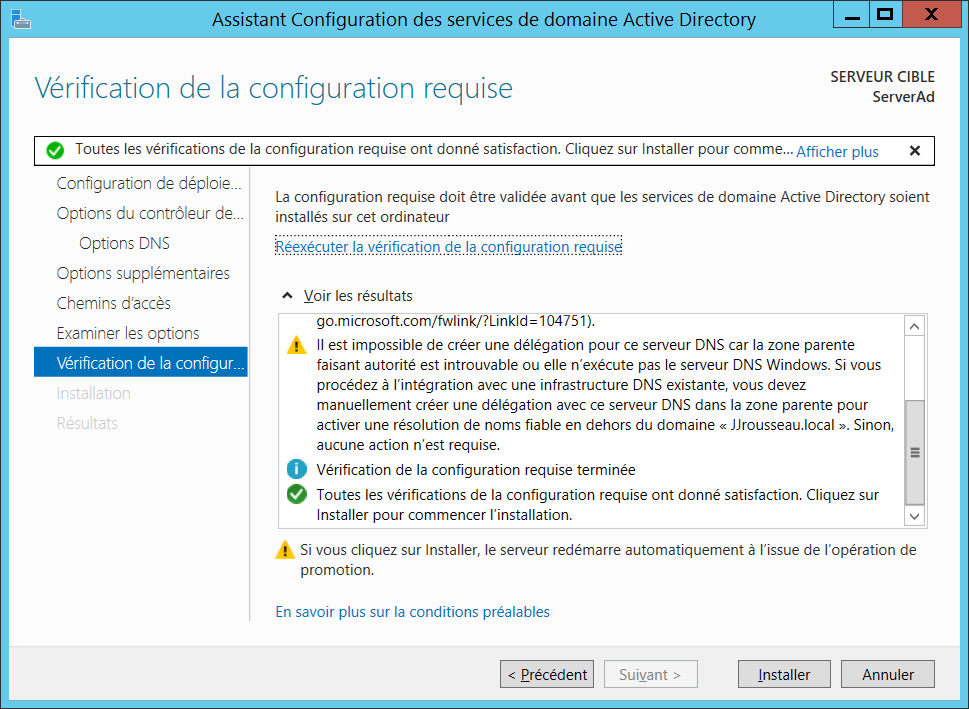
Nous allons créer une nouvelle forêt pour notre domaine :

Une forêt est une structure hiérarchique d’un ou plusieurs domaines indépendants (c’est l’ensemble de tous les sous domaines Active Directory).

Afin de restaurer dans le futur notre annuaire nous allons définir un mot de passe important.

Il est possible de restaurer notre Active Directory seulement si nous avons une sauvegarde de ce dernier. Il est donc nécessaire de bien garder le mot de passe de restauration qui est très important et aussi d’effectuer des sauvegardes de notre Active Directory régulièrement. Exemple d’un logiciel permettant de sauvegarder notre Active Directory : BackupExec qui est un logiciel de sauvegarde et de restauration de données qui fournit des fonctionnalités de sauvegarde et d’archivage pour les environnements Windows.

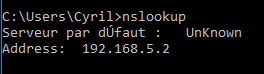
Après les différentes étapes nous installerons notre domaine Active Directory :

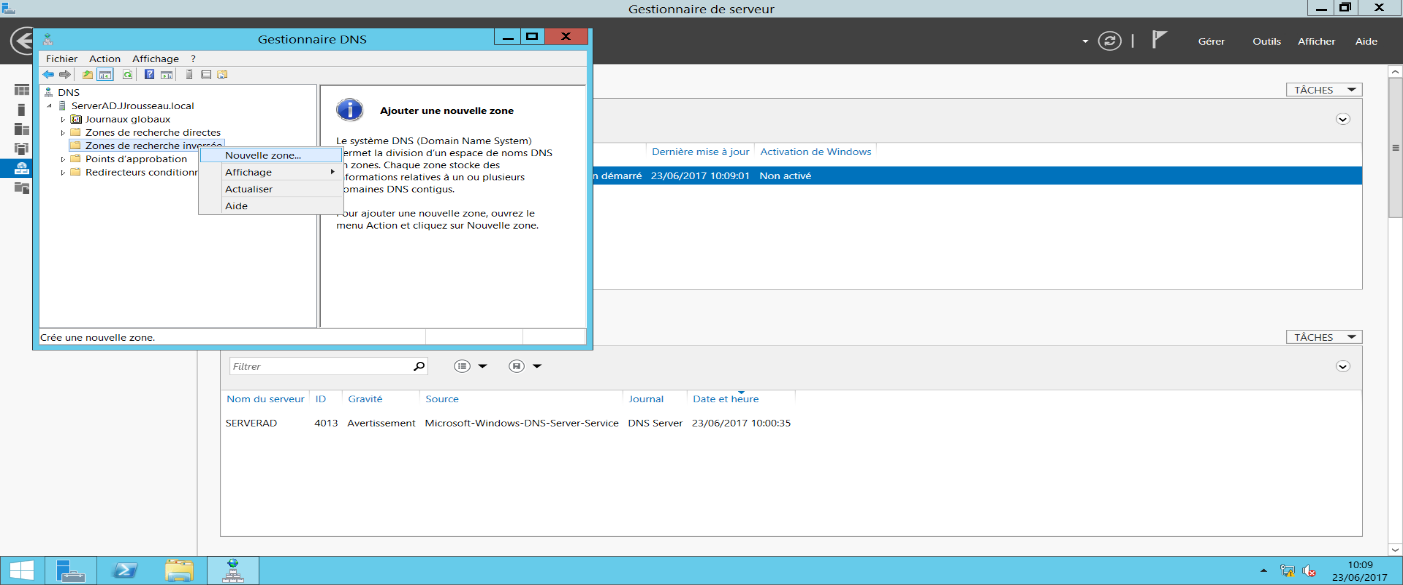


L’active Directory est désormais installée, nous allons maintenant configurer la zone inverse de notre DNS afin d’obtenir le FQDN de notre serveur à partir de son IP ou de tous les postes de travails.

Un serveur DNS est vital sur un réseau Active Directory. S’il tombe en panne, les machines du réseau seront incapables de communiquer avec le contrôleur de domaine.

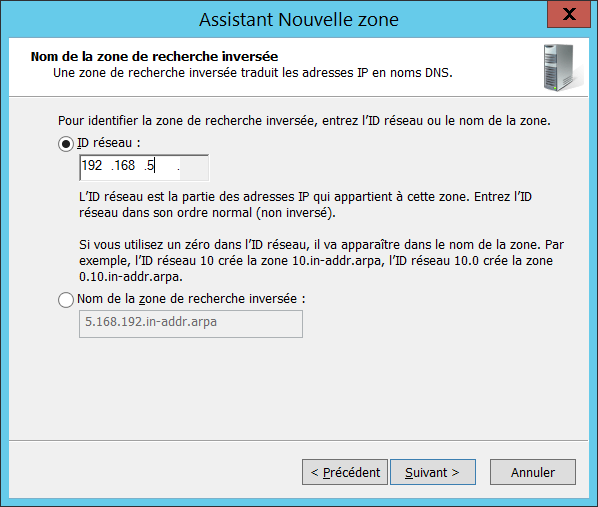
Nous pouvons constater voir que la zone n’est pas encore configurée :

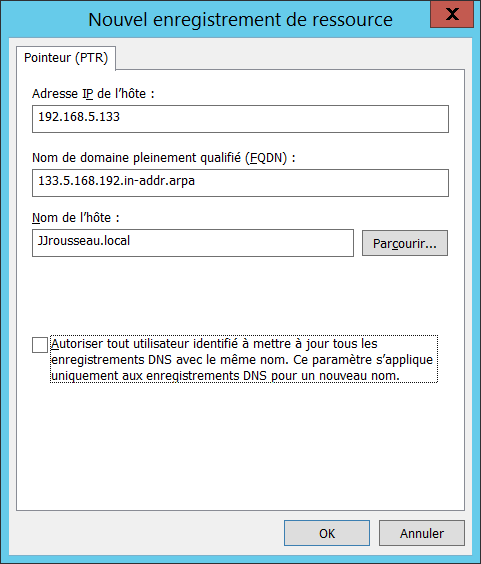


Pour cela la première chose à faire est de configurer le DNS en y ajoutant une nouvelle zone inverse :

Le type de la zone sera « zone principale », ensuite nous sélectionnerons : vers tous les serveurs DNS exécutés sur des contrôleurs de domaine dans ce domaine : JJrousseau.local -> Zone inverse IPV4.

Nous allons maintenant entrer l’ID réseau pour lequel nous souhaitons créer la zone de recherche inverse :

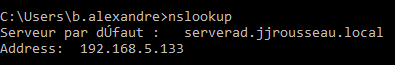


La zone inverse est maintenant configurée.

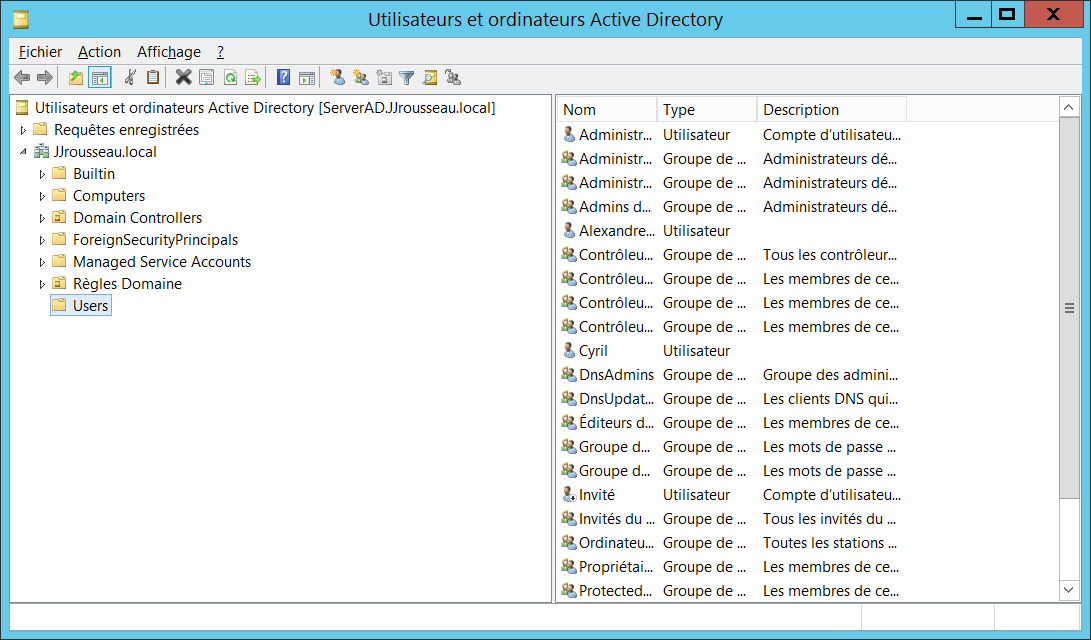
Ensuite il faut ajouter sur la zone inverse un enregistrement PTR manuellement.

Un enregistrement de type PTR permet de résoudre une adresse IP en nom et permet d’associer la dernière partie d’une adresse IP à une adresse FQDN. L’adresse IP est écrite « à l’envers » et se termine par : in-addr.arpa.

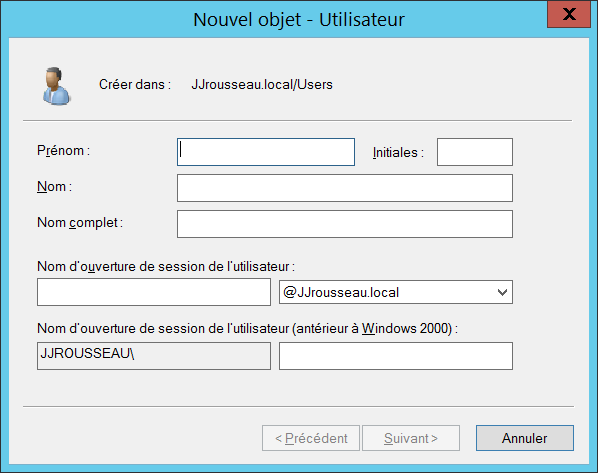
Une fois la zone inverse faite nous remarquons que le DNS repond bien.



Pour crée un utilisateur il faudra se rendre comme indiqué ci-dessous :



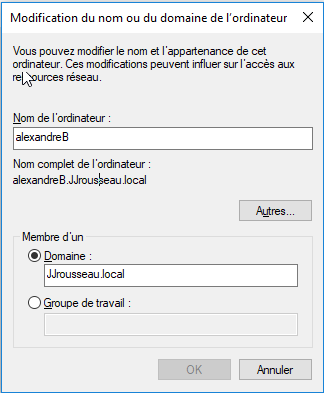
Nous allons sur Users, puis nouveau utilisateur. Il est important de bien sélectionner notre domaine pour que nos utilisateurs puissent se connecter sur notre domaine.

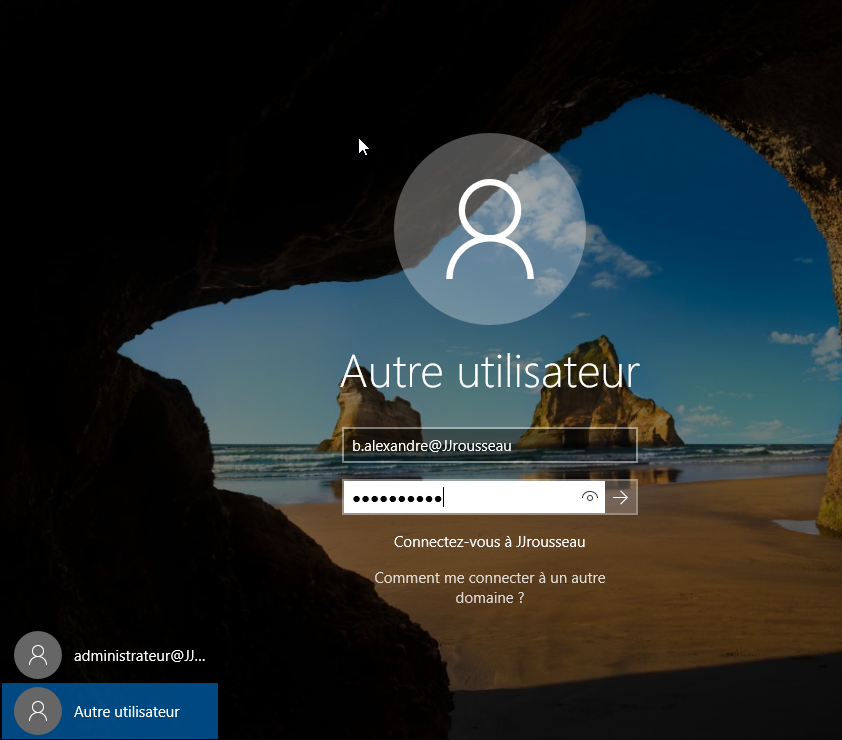


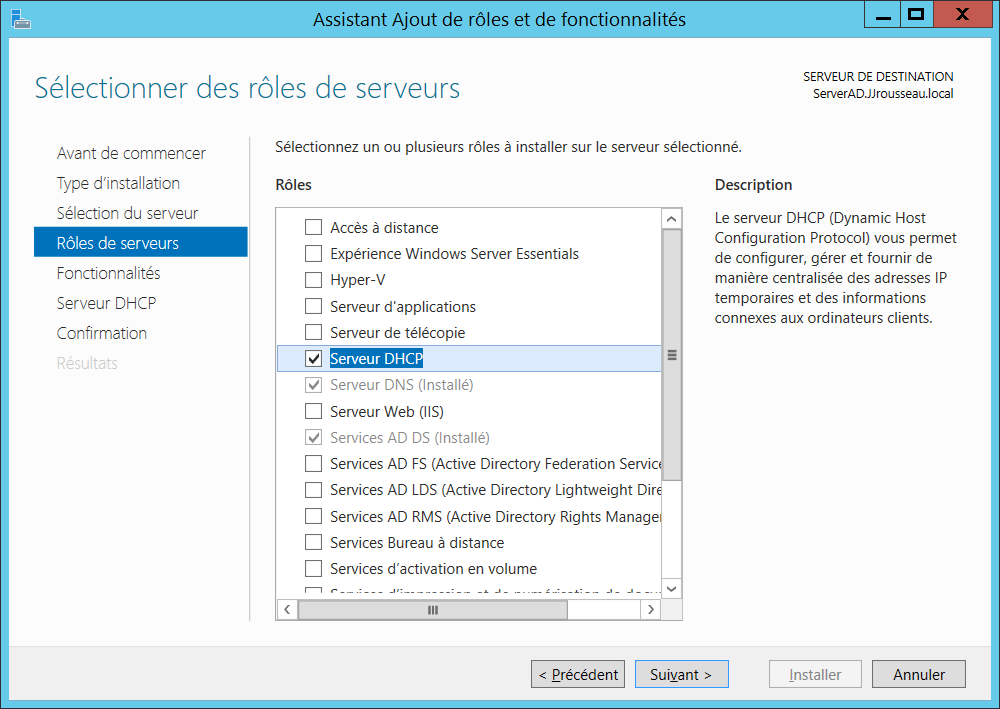
Une fois l’utilisateur crée on peut modifier ses droits etc …

Pour se connecter à notre domaine nous associons notre machine Windows au domaine JJrousseau pour que l’utilisateur crée qui souhaite se connecter sur notre domaine puissent le faire.

Nous nous rendons donc dans paramètre système -> Information système -> modifier les paramètres puis mettre le nom de notre domaine, ici ce sera JJrousseau.local.



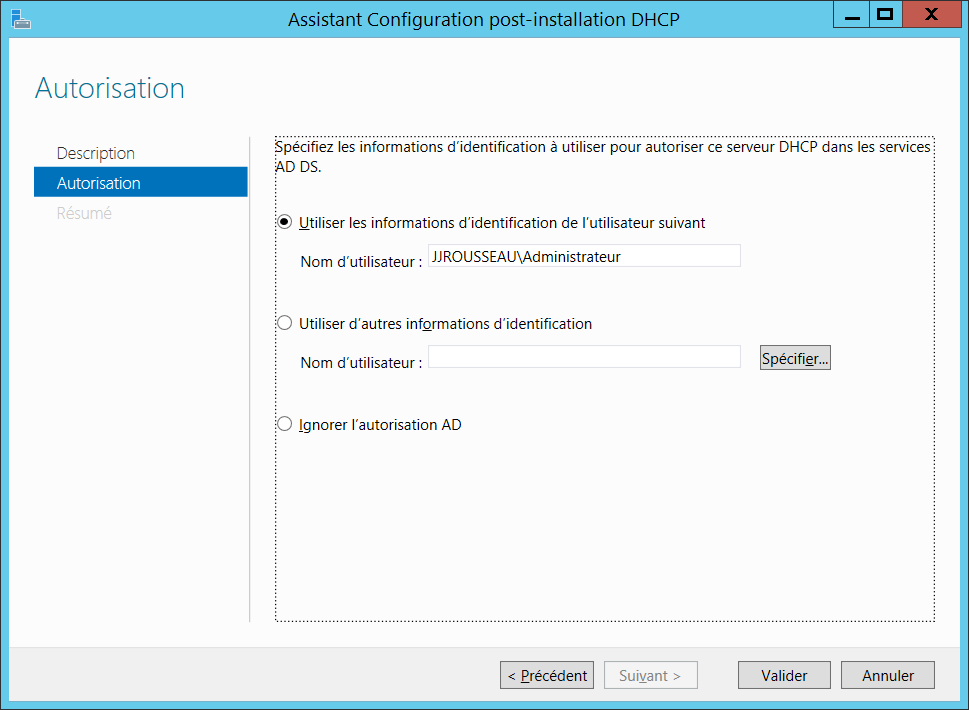
Nous allons désormais ouvrir notre session avec l’utilisateur crée sur notre domaine JJrousseau :

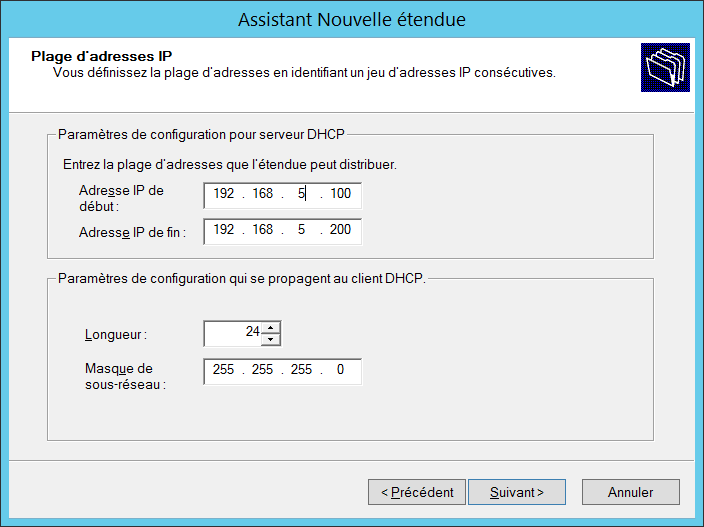
Afin d’ installer un DHCP suivre les étapes suivantes :

Un serveur DHCP a pour rôle de distribuer des adresses IP à des clients pour un durée déterminée, au lieu d’affecter manuellement à chaque hôte une adresse statique, passerelle par défaut …

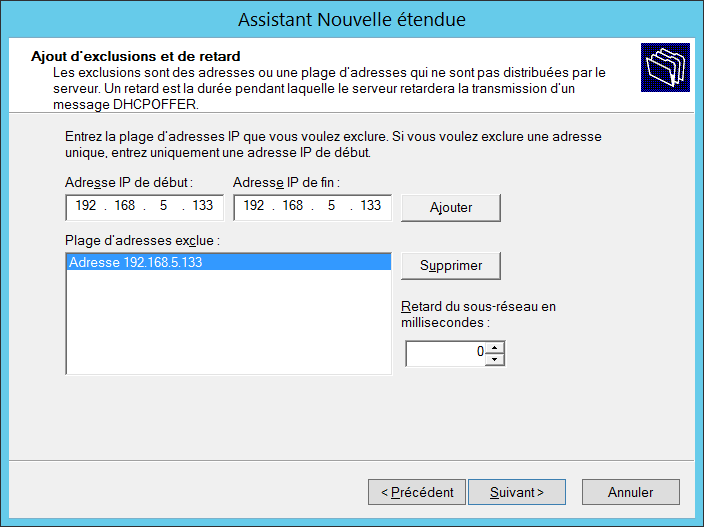
Le DHCP alloue à un client, un bail d’accès au réseau pour une durée déterminée. Cela permet de libérer les adresses et de les rendre de nouveau disponible.

L’installation du DHCP s’effectue et une fois finit nous allons terminer la configuration DHCP :

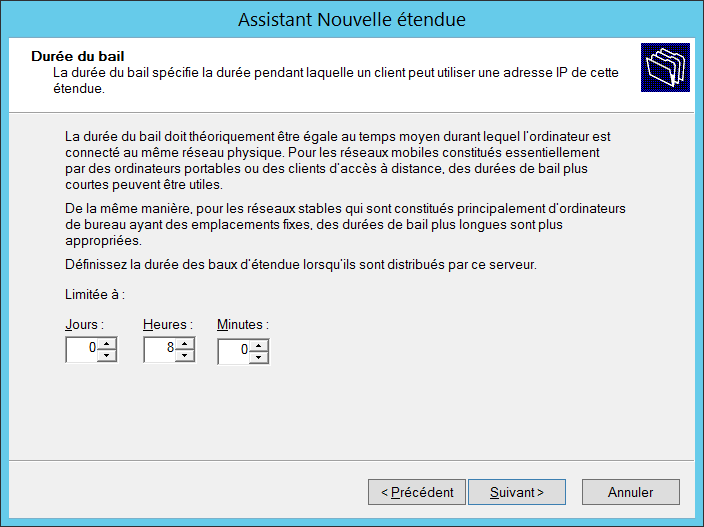


Ensuite sur Gestionnaire DHCP puis dans l’onglet IPv4, nous faisons une nouvelle étendue et on la nommera.

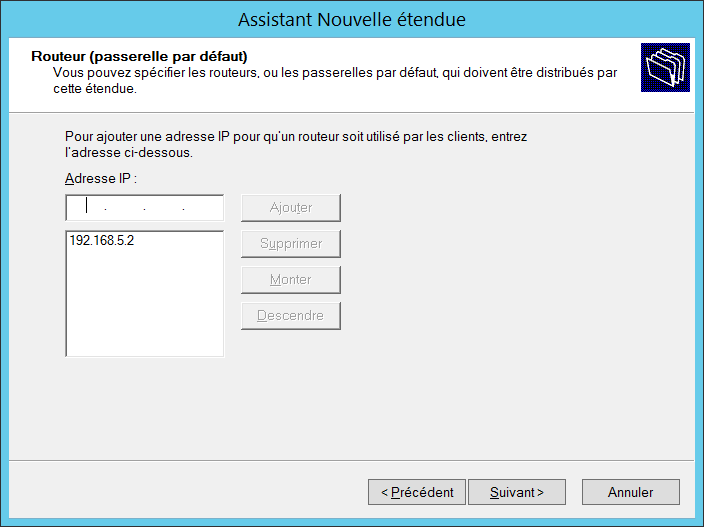
La plage d’adresse est définie nous allons maintenant exclure l’adresse IP de notre serveur afin de ne pas rentrer en conflit avec ce dernier.



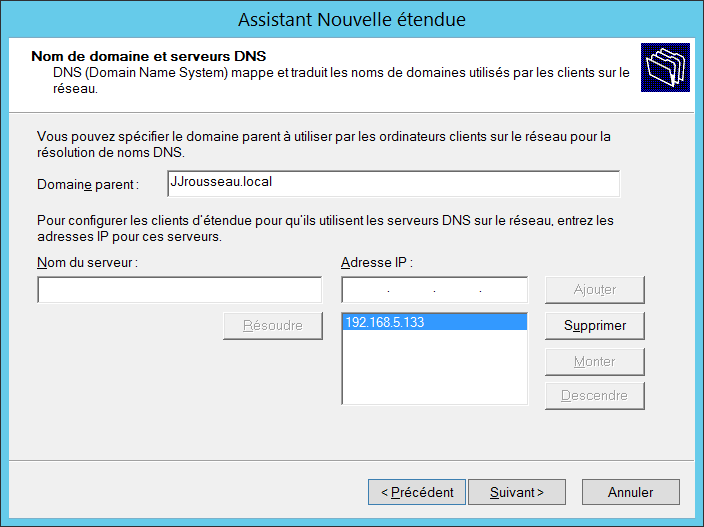
L’adresse IP de notre serveur n’entrera pas en conflit avec nos machines.

La durée du bail sera définie à 8 h :

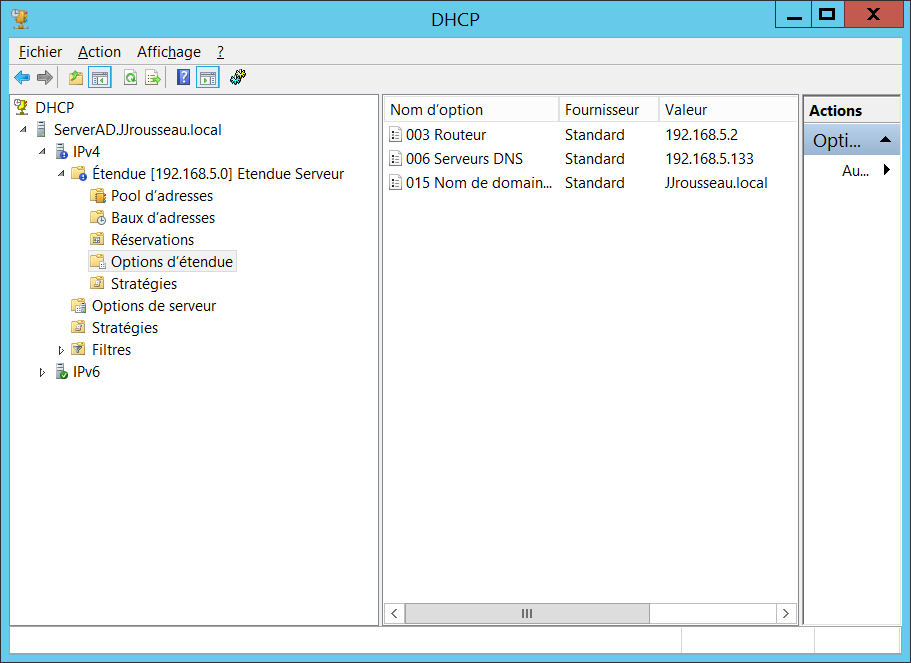
Ce sera le temps pendant lequel le PC est autorisé à utiliser cette adresse sans la renouveler.

La passerelle par défaut :

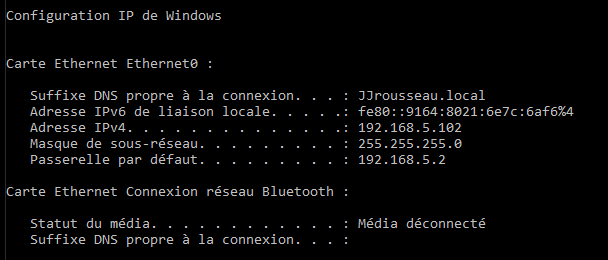
Une passerelle par défaut permet de faire la liaison entre deux réseaux par exemple local et internet, afin de faire l’interface entre des protocoles réseau différents.

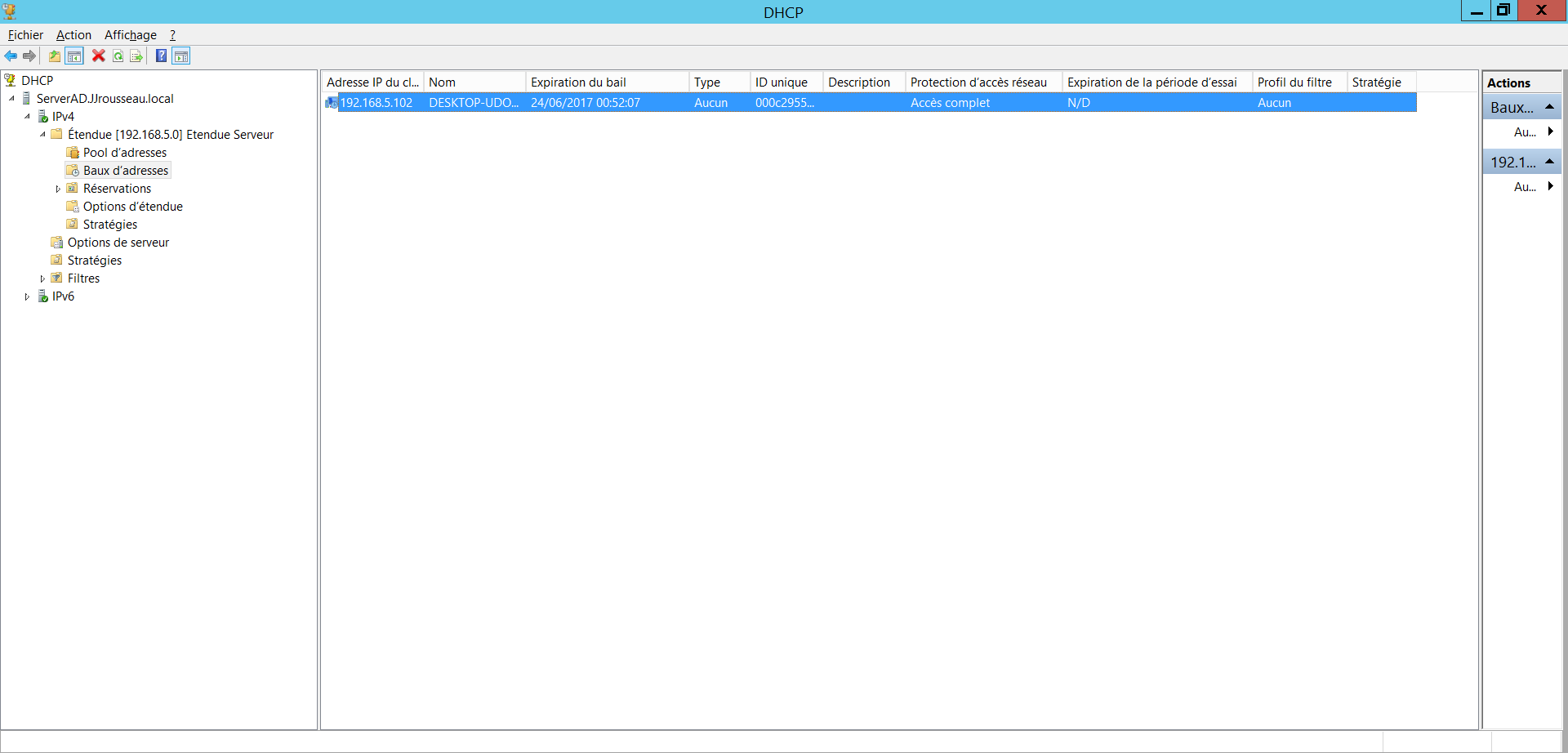


Il faut renseigner l’IP de notre DNS : 192.168.5.133

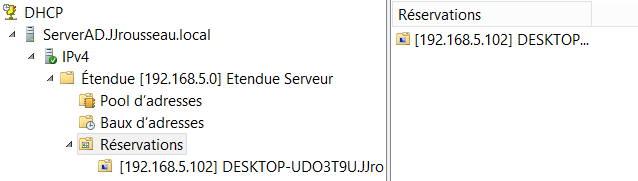
Le DHCP est maintenant configuré nous allons donc vérifier sur la machine cliente si elle a récupéré un bail DHCP.

Nous constatons que notre DHCP à bien attribuer une @IP à notre machine du domaine : **JJrousseau**



Pour aller plus loin : Pour réserver une @IP à notre machine afin que le DHCP ne la change pas au bout de 8h on va la réserver :

Nous ajoutons à la réservation :



La réservation à bien été effectué.

La base de notre serveur est maintenant créée nous allons maintenant gérer des règles que l’on pourra appliquer à des utilisateurs, groupes ou unités d’organisations présent dans notre service Active Directory, d’où le principe d’avoir configuré un domaine sur notre serveur.

Les règles seront des GPO (Group Policy Object ou stratégies de groupe). Voici quelques exemples de GPO :

- Mapper des lecteurs réseaux

- Déployer un certificat

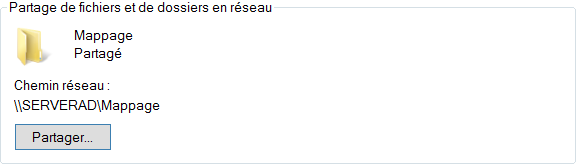
- Modifier des droits

- Empêcher d’effectuer certaines modifications (par exemple fond d’écran du bureau, installer programmes, ajouter des imprimantes…)

L’avantage des GPO est qu’il n’y a pas besoin de passer sur tous les postes pour déployer ces règles etc...

**Mappage d’un lecteur réseau par GPO :**

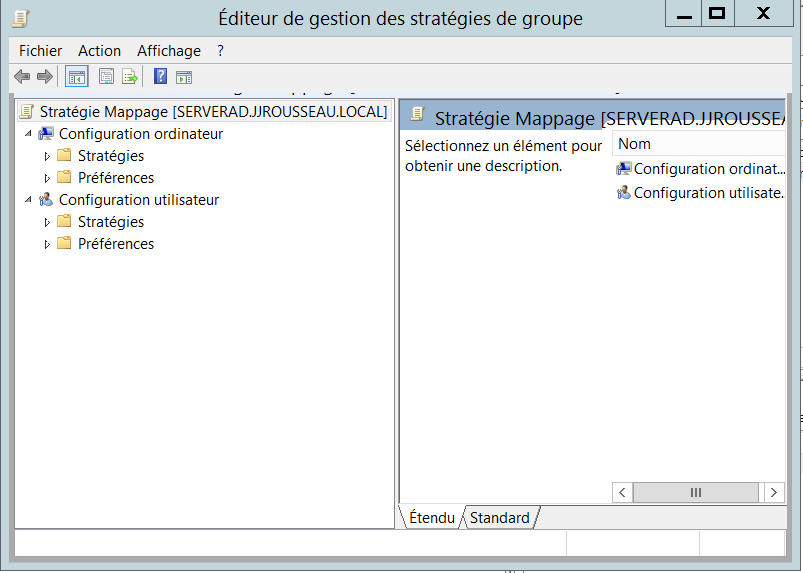
A l’aide d’une GPO nous allons partager des fichiers à l’aide d’un lecteur réseau qui sera disponible sur tous les postes sans avoir à le faire sur chaque poste et chaque utilisateur aura accès ou non au lecteur réseau dès l’ouverture de la session.

Tout d’abord nous créons un dossier, ici il sera nommé « Mappage ». Nous nous rendons sur propriété et dans partage on fait partager. Il faut ensuite sélectionner les utilisateurs qui verront le dossier.

Nous allons créer une GPO pour mapper ce lecteur :

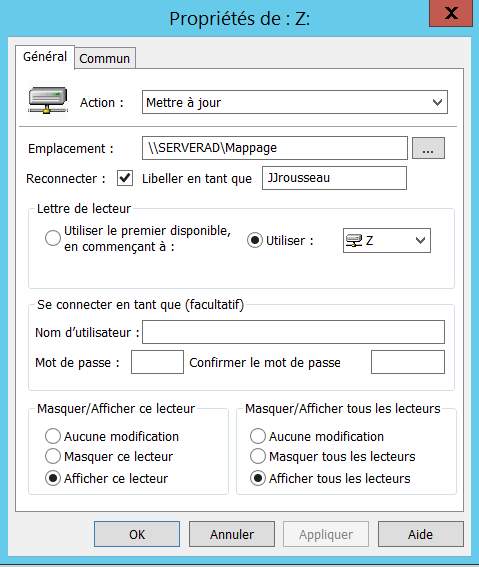
Outils d’administration -> Gestion des stratégies de groupe -> Clic droit sur notre domaine : JJrousseau.local -> Clic droit et nous créons un objet GPO dans ce domaine et nous le nommons Mappage.

Sur la règle Mappage nous faisons modifier :



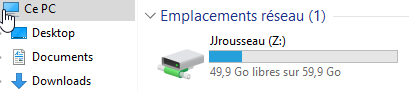
Clic sur modifier et dans configuration utilisateur > Préférences > Paramètres Windows > Mappages de lecteurs.

Clic droit puis nouveau Lecteur mappé et faire comme ci-dessous :



Après ces manipulations on clic droit sur la règle puis il l’ appliquer, il est aussi possible d’ajouter des utilisateurs.

On redémarre la session du client et l’on constate ceci :



Le lecteur réseau est bien connecté sur l’utilisateur du domaine.

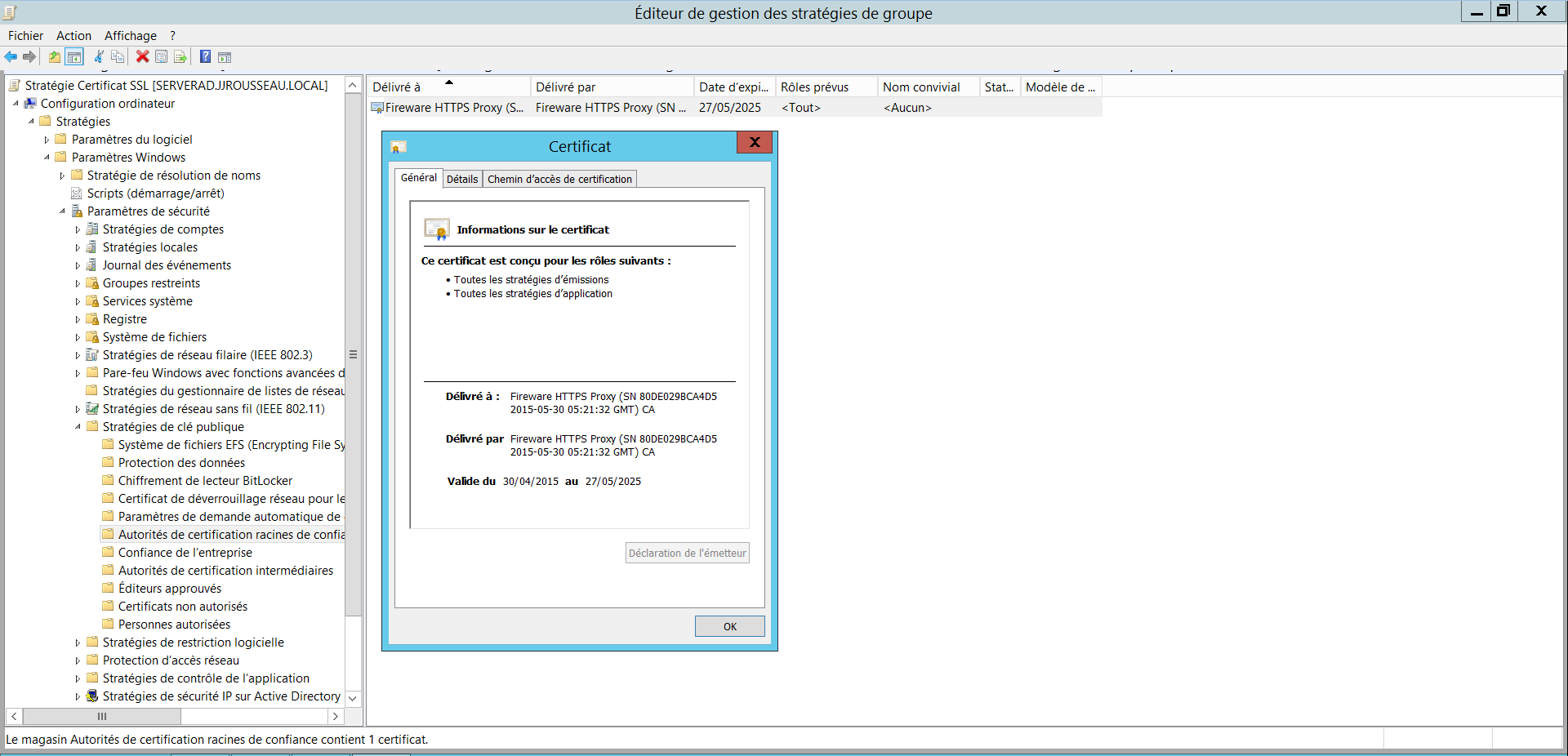
Toutefois si le dossier n’apparait pas nous pouvons faire la commande suivante : **gpupdate /force**

**Déploiement de certificat SSL par GPO :**

Un certificat SSL est un fichier de données qui lie une clé cryptographique donc crypté aux informations d’une organisation ou d’un individu. On peut remarquer si le certificat est bien actif avec le cadenas et le protocole https (port 443) sur les navigateurs et permet d’assurer une connexion sécurisée entre le serveur web et le navigateur.

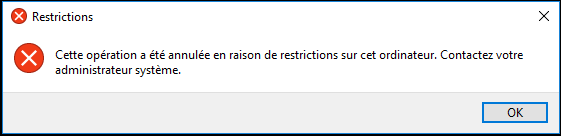
Comme précédemment nous allons créer une GPO que nous appellerons certificat SSL :

Dans gestion de stratégies de groupe -> clic droit sur Certificat SSL et modifier ensuite se rendre sur configuration ordinateur -> Paramètres Windows -> Paramètres de sécurité -> Stratégies de clé publique -> Autorités de certification racine et importer le certificat qui ici est en PEM.

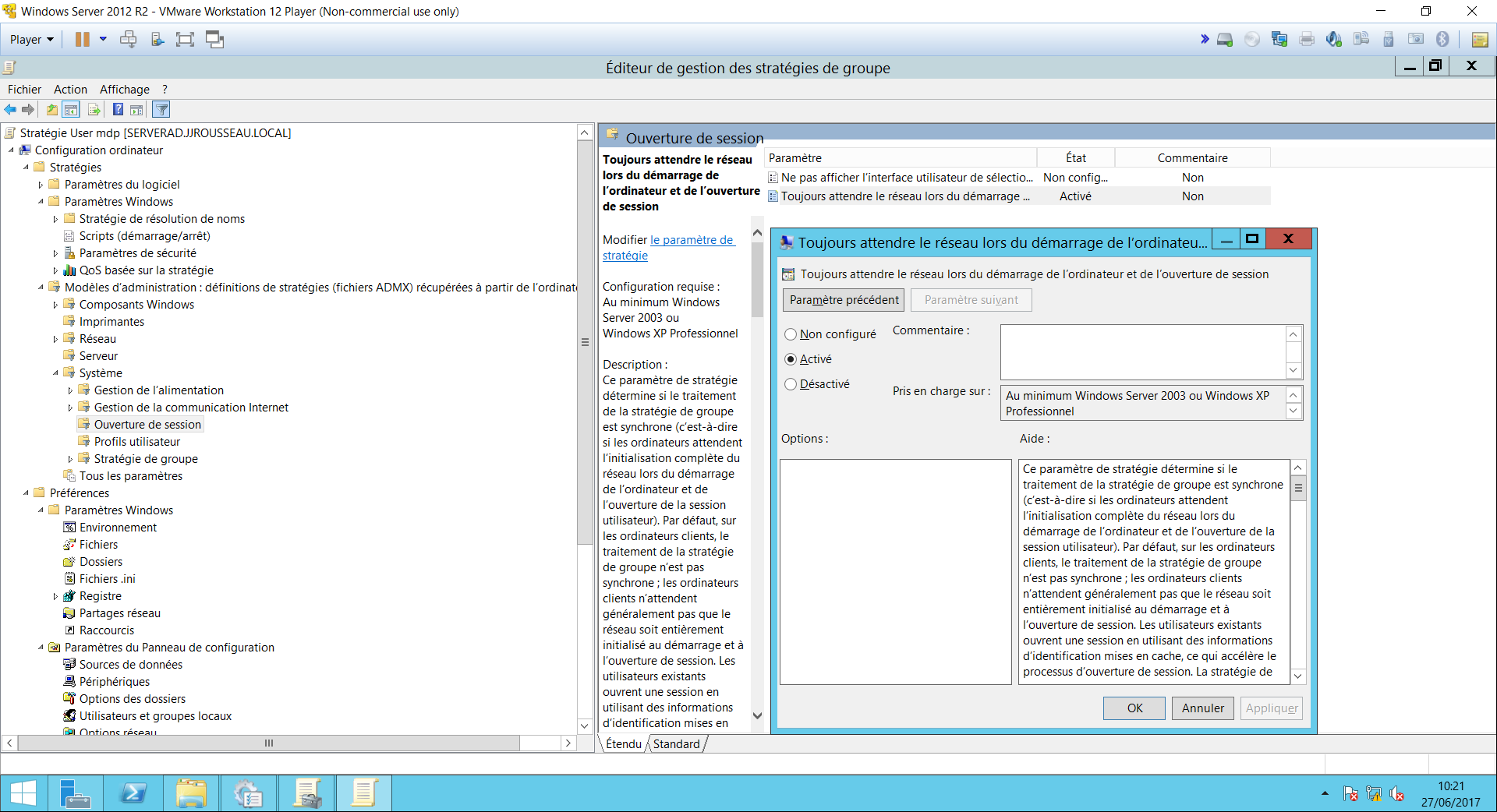
On obtient donc :

**Empêcher l’accès au panneau de configuration :**

On crée une GPO que l’on nommera « Panneau de Configuration » -> Modifier -> configuration utilisateur -> Modèles d’administration -> Panneau configuration ensuite on va sur Interdire l’accès au Panneau de configuration et à l’application paramètre du PC.

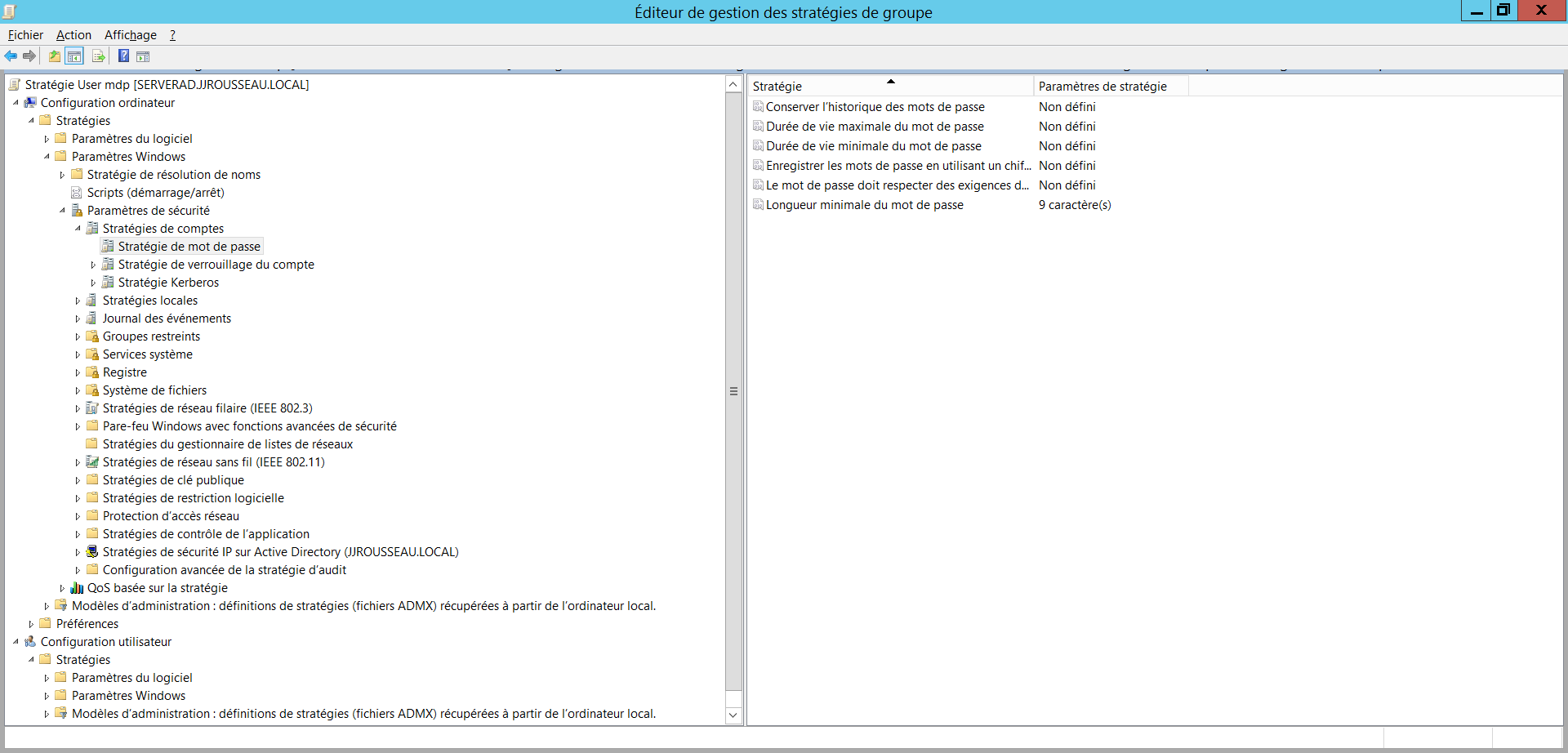
Les utilisateurs du domaine ne pourront donc pas modifier les paramètres du PC :

Nous pouvons constater que l’utilisateur n’a pas accès et ne peut donc rien modifier.

**Toujours attendre le réseau au démarrage et à la connexion : **

Cette règle est très importante si on fait une GPO il est possible que lors de la connexion des utilisateurs, celle-ci ne soit pas appliquer, elle permet donc de ne pas avoir à se reconnecter plusieurs fois pour que la GPO soit appliqué.

Les GPO sont le cœur de notre Active directory afin de gérer tout notre domaine, une dernière règle que l’on va voir les mots de passes.



Dans notre gestion de stratégie de groupe on peut voir que l’on peut gérer tout. Ici on peut définir la longueur de mot de passe, sa durée de vie et quelles exigences il doit respecter.

Une fois les règles configurer, il est possible de choisir à qui s’appliquera la règle.

**VISIOCONFERENCE**

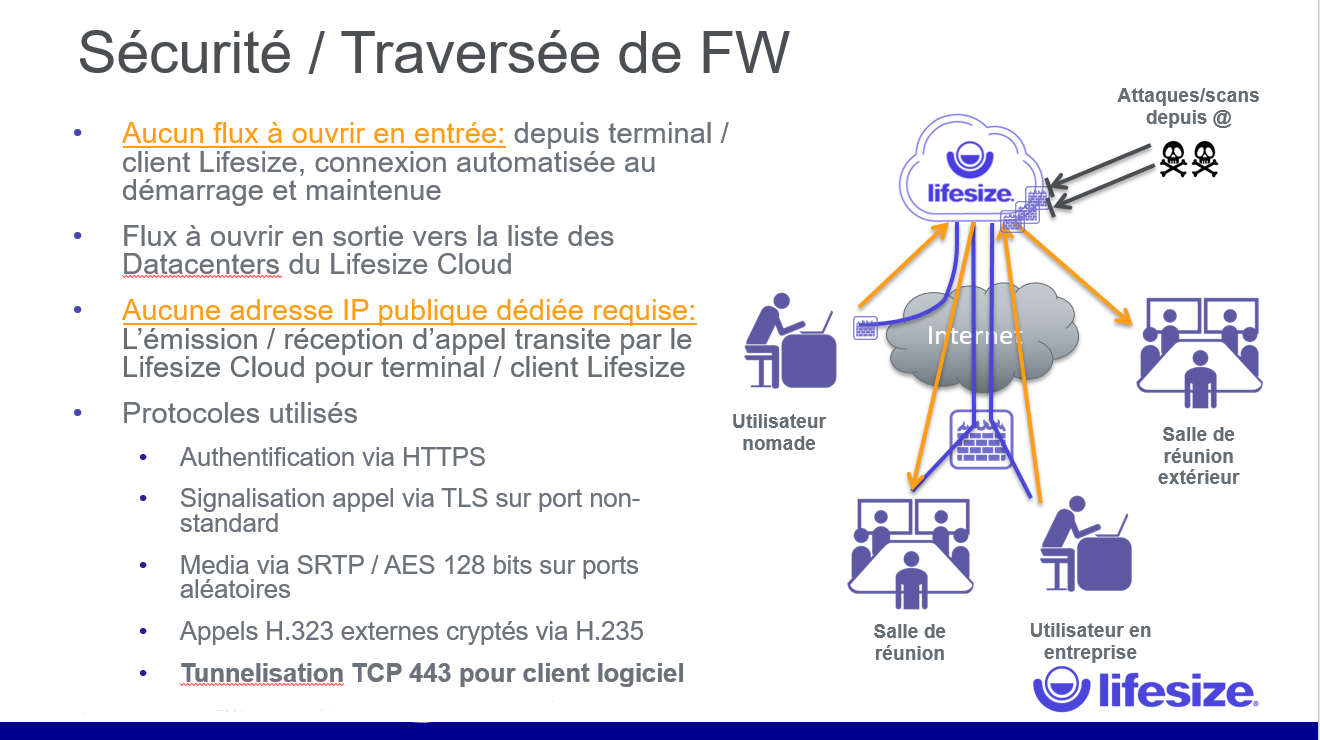
La visioconférence c’est quoi ? C’est un moyen de communication de plus en plus utilisé par les entreprises. De par son aspect pratique, la visioconférence intéresse les entreprises souhaitant communiquer à distance avec d’autres entreprise ou personnes sans avoir à se déplacer.

Cela permet donc aux entreprises d’organiser des réunions de travail, conférences et formation sans se déplacer.

J’ai pu assister à une réunion entreprise sur paris afin de présenter la solution de visioconférence Lifesize Cloud.

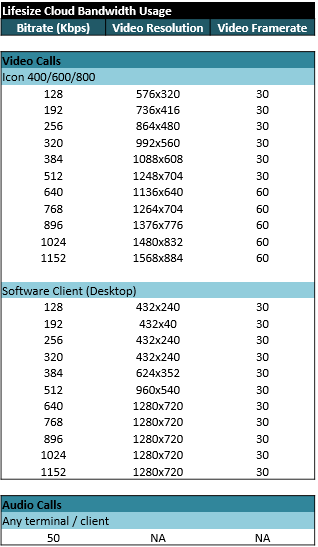
Lifesize propose différentes solutions de cloud s’adaptant à la vision conférence sous forme d’abonnements allant de Room, Premium et Entreprise chacun disposant d’offre en fonction de l’utilisation. Il est possible de faire de la visioconférence avec différents terminaux : smartphone, poste traditionnels (Windows...), Navigateur internet…

Concernant la sécurité voire schéma ci-dessous :



L’interopérabilité avec Windows et un point important de la visioconférence cela permet au différentes solutions Windows tel que Office 365 d’être utilisé.

Concernant le débit à avoir il faut disposer de la fibre afin d’avoir la meilleur qualité vidéo possible :



La visioconférence est donc très utile et très sécurisée. Cela permet de réduire les coûts de déplacement, tout en ayant des réunions fréquentes et des réunions sécurisées car les flux sont cryptés et l’utilisation de la visioconférence est facile d’utilisation.

**Téléphone IP**

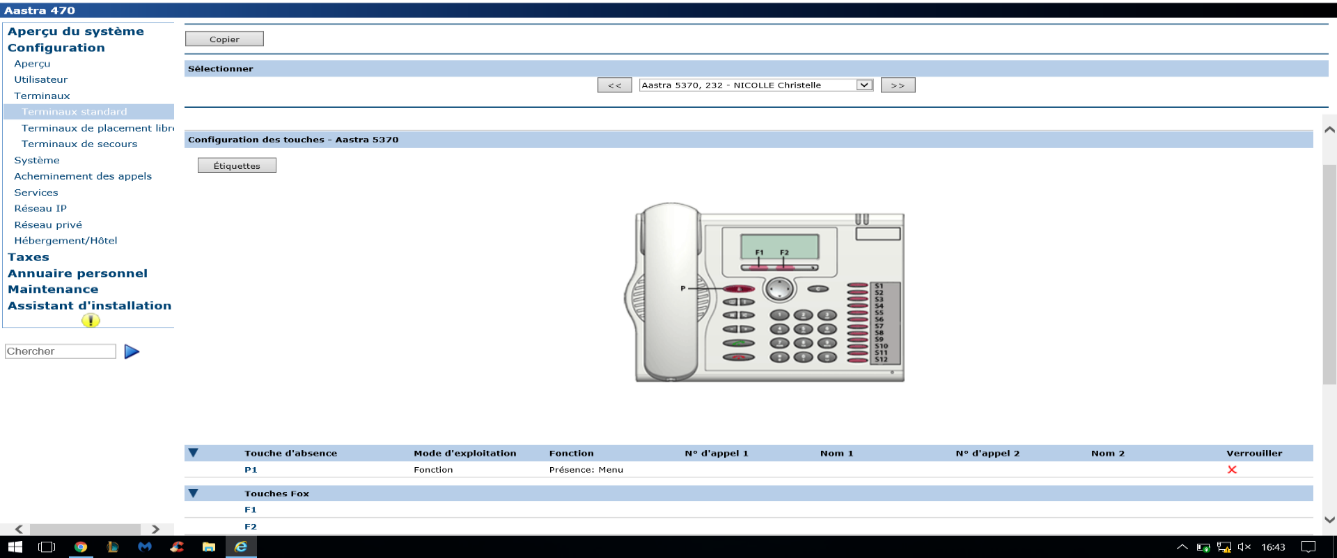
La téléphonie sur IP permet la transmission des communications vocales via des réseaux au protocole IP et permet la convergence de tous les postes informatiques d’une entreprise en un seul réseau unifié.

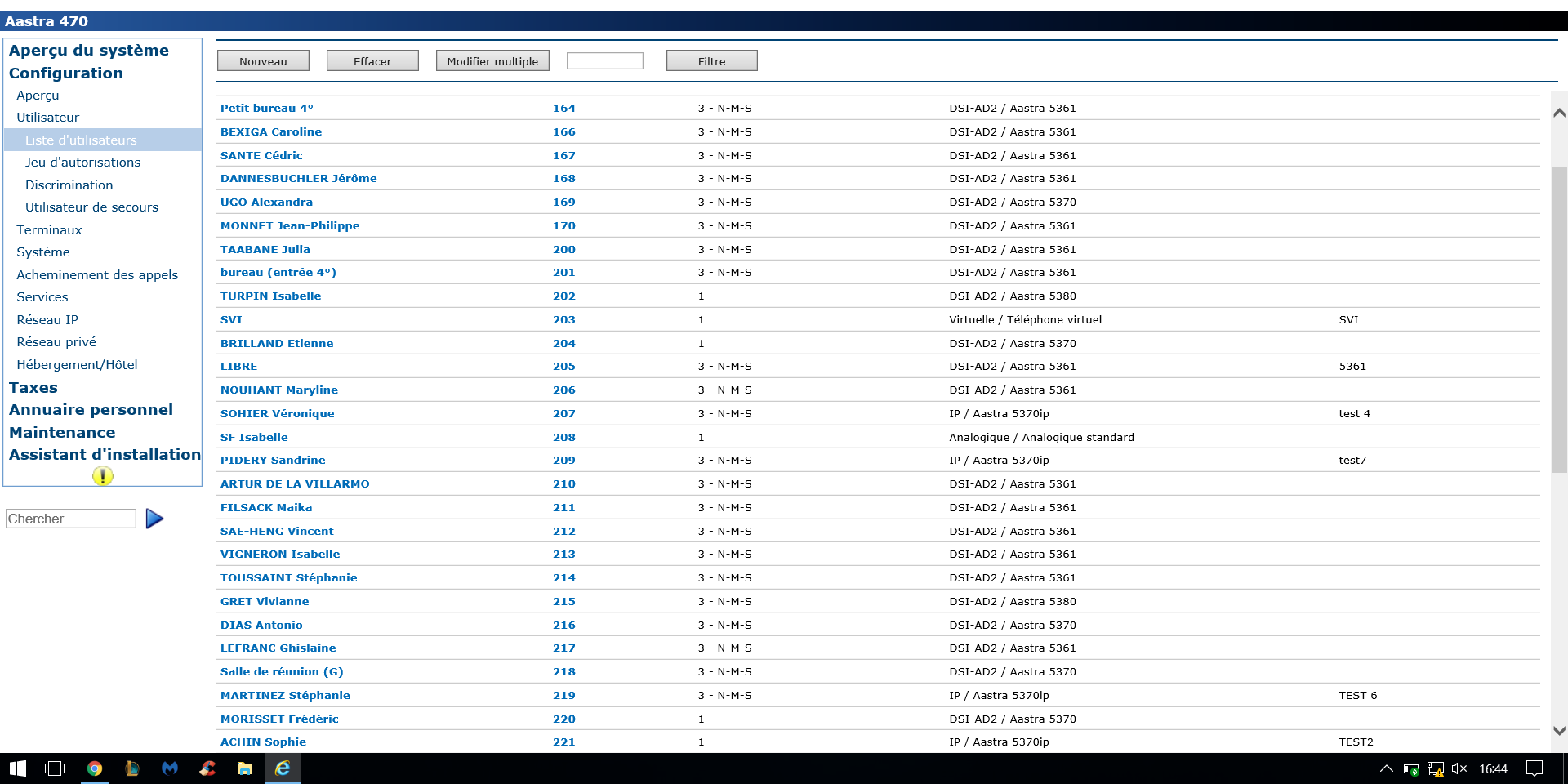
Les avantages de la téléphonie IP sont :

* Les coûts d’installation : Une économie sur les frais de câblage, si vous possédez déjà un réseau Internet d’entreprise. Pas d’achat de câbles et de frais de pose à faire.
* Concernant la mobilité : La téléphonie IP fonctionne en associant un utilisateur à un poste et non plus à une ligne. Un utilisateur peut désormais garder le même numéro de téléphone s’il est en déplacement ou s’il change de bureau
* L’évolutivité : Dans une architecture VoIP, il est très facile d’ajouter des postes supplémentaires ou d’agrandir le réseau, ce qui n’était pas le cas avec la téléphonie non -IP.

J’ai installé chez un client des postes téléphones IP et les est configuré :

Avec Aastra nous allons configurer les postes IP clients : Attribuer des IP au différents postes

Interface Système :

Pour finir après avoir attribué une IP et configuré nos postes IP nous allons par connexion FTP (Protocole de communication) afin de récupérer notre configuration.

Ici nous pouvons voir le nom de tous les clients associés à chaque poste du réseau.

L’adresse IP de nos postes peut aussi s’obtenir avec un DHCP, il suffit d’activer l’option DHCP

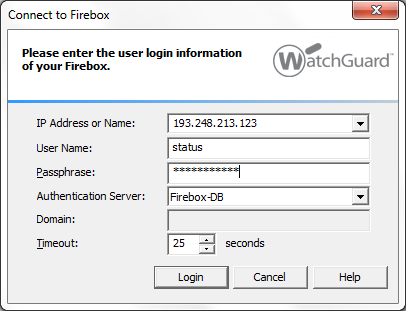
La configuration finale sera celle-ci : Nom de la personne, date, heure…

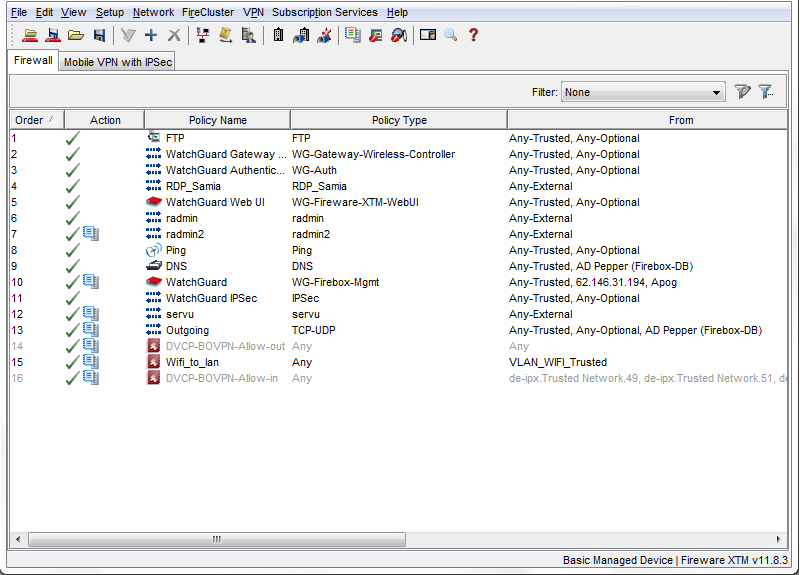


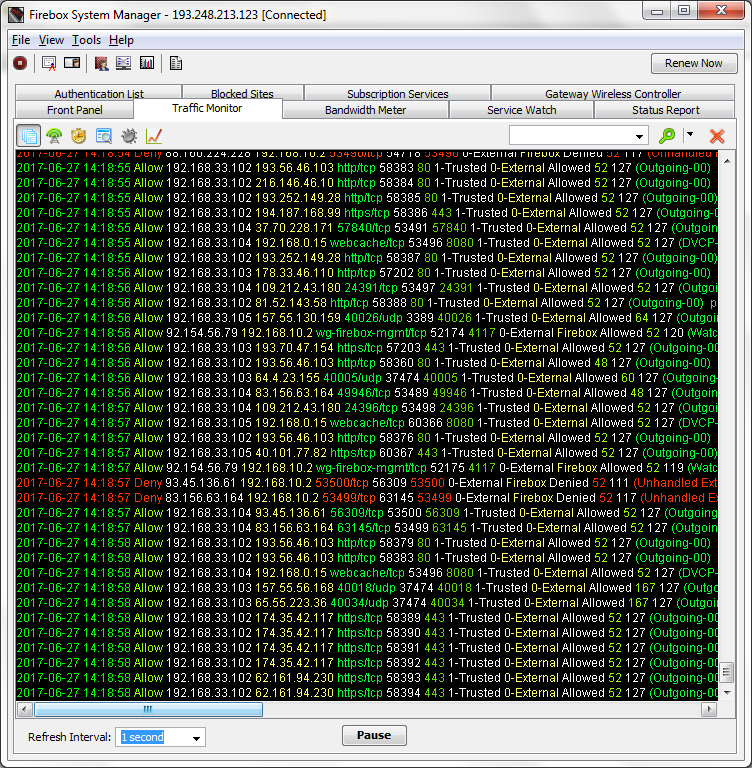
La connexion se fait par câble RJ45 qui se connectera à notre réseau.

**Watch Guard**

WatchGuard est conçu pour protéger les réseaux locaux connectés à internet à l’aide d’un boitier et son logiciel d’administration (Watch Guard LiveSecurity Control Center), il permet d’appliquer une politique de sécurité définie par l’entreprise ainsi que de nombreux outils : Monitoring pour visualiser la bande passante consommée, outils d’administration…

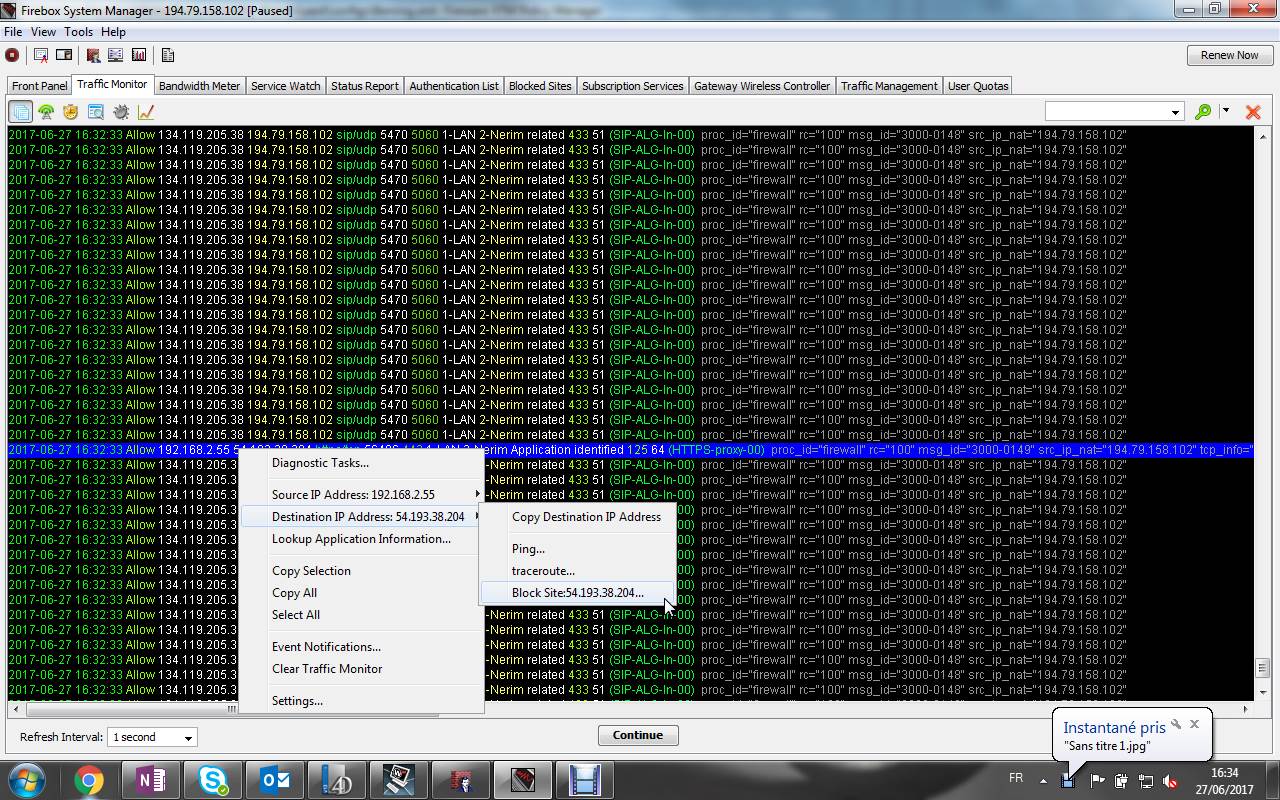
Tout d’abord pour se connecter sur notre Watch Guard on fait comme ci-dessous :

Ensuite ici on peut voir les différentes règles que l’on peut créer et gérer :

Les différents Flux sont gérés dans le Traffic Monitor, on peut apercevoir les requetés autorisés en vert et refusé en rouge et on voie exactement quel IP, quel protocole, d’où vient la connexion etc.

Mon boitier WatchGuard utilisé lors du stage est :

Si l’on souhaite bloquer un client on clic droit sur la ligne concernant notre client et l’on peut interdire tout le trafic c’est-à-dire que s’il fait des recherches sur le net il ne pourra pas ou alors on peut seulement bloquer l’IP du site que l’on refuse donc il pourra accéder au net mais pas au site.

Si on bloque une IP interne on bloquera tout le trafic vers le Wan.