

28/09/2018

Microsoft Windows Serveur

Support de formation



Table des matières

Introduction :	4
Les versions de Windows Server 2008	4
Gérer les disques et les partitions :	4
Gérer les systèmes de fichier Fat16, Fat32, NTFS, NTFS V5, EFS :	5
Différence entre les versions 2003 et 2008 :	6
Server Core	6
Les rôles <i>Active Directory</i>	7
Terminal Services.....	7
Windows PowerShell.....	7
Auto-réparation NTFS	8
Hyper-V	8
la Sauvegarde de Windows Server	8
Quelles sont les principales évolutions ?	8
INSTALLATION DU SERVEUR 2008 EN MODE GRAPHIQUE :	9
LE MODE CORE :	14
ROUTAGE/ NAT	20
ROUTEUR	20
NAT	20
Installation d'une maquette fonctionnelle pour mettre en place un routage réseau avec NAT.....	20
Réglage à faire sur le SRV1.....	22
Réglage à faire sur le SRV2.....	30
DNS	38
Définition	38
Introduction au DNS.....	38
Notions de base d'un DNS.....	38
Base de données distribuée.....	40
Requêtes itératives et récursives.....	40
Zones et serveurs DNS :	41
Les différents types de zone :.....	41
Configuration des prérequis pour l'installation d'un serveur DNS	41
Installation du rôle DNS sur le Serveur 1.....	43
Les différents enregistrements DNS pour la zone directe.....	47
Les différents enregistrements DNS pour la zone inversée	49
FQDN	49
La commande NSLOOKUP.....	49
Ajout d'une machine dans la base de données	50
DHCP [DYNAMIC HOST CONFIGURATION PROTOCOL]	52
Définition.....	52

Rôle	52
Fonctionnement.....	52
APIPA	53
Le Bail	54
Renouvellement de bail.....	54
Installation.....	55
Paramétrage DHCP	57
Nouvelle étendue.....	57
Exclusion.....	58
Durée du bail	58
Paramètres DHCP	59
Paramétrage DNS	59
Visualisions de l'entendue	60
Réservations.....	61
AUTRES STATUS DHCP	62
COMMANDES UTILES	62
Création d'une deuxième étendue	62
Agent de Relais DHCP (DHCP RELAY).....	63
Installation de l'agent de relais DHCP	64
ACTIVE DIRECTORY.....	66
<i>Définition :</i>	66
Forêt Active Directory	66
Domaine Active Directory.....	66
La structure logique	67
La structure physique.....	69
Catalogue global.....	69
Modifications dans les groupes	69
Présentation des maîtres d'opérations :	71
Rôle du contrôleur de schéma.....	71
Maître d'attribution de nom de domaine.....	71
Emulateur CPD (PDC).....	71
Maître RID	71
Maître d'infrastructure	72
Installation.....	72
Gestion des utilisateurs.....	79
STRUCTURE ACTIVE DIRECTORY	80
Création d'une structure personnalisée :	81
Création des comptes utilisateurs	83
Création de groupe	83
DOSSIER PARTAGES.....	86
Connexion d'un poste client au domaine Active Directory.....	95

GPO [GROUP POLICY OBJECT]	98
Exemples de GPO	99
Mise à jour de la GPO sur le poste client.....	101
WINDOWS DEPLOYMENT SERVICES (WDS):.....	108
WDS sur Windows Server 2008	108
WSUS.....	119
Définition WSUS.....	119
Installation de WSUS (remplacer les noms de domaine par celui de l'exercice.)	119
Configuration de WSUS :.....	121

Introduction :

Microsoft Windows Server 2008 est un [système d'exploitation](#) de [Microsoft](#) orienté [serveur](#). Il est le successeur de [Windows Server 2003](#) sorti 5 ans plus tôt et le prédecesseur de [Windows Server 2008 R2](#). La sortie internationale du produit quant à elle a eu lieu le [27 février 2008](#). À l'instar de [Windows Vista](#), Windows Server 2008 est basé sur le *Kernel* (noyau) [Windows NT](#) version 6.0.

Windows Server 2008 R2 est le système d'exploitation qui succède à [Windows Server 2008](#). Il est "la version serveur" de [Windows 7](#), dont il partage le noyau, [Windows NT](#) 6.1. Il est important de noter que Windows Server 2008 R2 est le premier système d'exploitation de Microsoft à être **disponible uniquement en 64 bits**, et ce, afin de préparer au mieux le passage au tout 64 bits, en effet le prochain système d'exploitation client de Microsoft ne sera lui aussi plus disponible qu'en 64 bits.

Les versions de Windows Server 2008

- Édition Standard
- Édition Enterprise
- Édition DataCenter
- Édition Itanium
- Édition Web
- Édition Small Business Server
- Édition HPC (High Performance Computing).

Gérer les disques et les partitions :

Parmi les évolutions apportées par Windows Server 2008 à la gestion des disques et des volumes, l'une des plus attendues est probablement la possibilité de redimensionner de manière dynamique les volumes. Au-delà de la possibilité d'étendre des volumes sans perte de données qui avait été introduite avec Windows Server 2003, il est maintenant possible de réduire leur taille.

L'opération de réduction est possible soit de manière graphique via la console **Gestion des disques** soit en mode ligne de commande via **DISKPART**, dans les deux cas l'opération est réalisée sans interruption de service ou perte de données.

Gérer les systèmes de fichier Fat16, Fat32, NTFS, NTFS V5, EFS :

FAT 16 :

Limitations	
Taille maximale de fichier	4 Go (mais limité par la taille du disque)
Nombre maximal de fichiers	65518
Taille maximale du nom de fichiers	8.3 (comme FAT12) (étendu à 255 en VFAT)
Taille maximale de volume	2 Go (voire 4 Go)
Caractères autorisés dans les noms de fichiers	tous les caractères sur 8 bits (étendu à tout Unicode en VFAT) sauf / \ : * ? " < >

FAT 32 :

Limitations	
Taille maximale de fichier	4 Go
Nombre maximal de fichiers	supérieur à 250 millions
Taille maximale du nom de fichiers	255 caractères
Taille maximale de volume	2 To (8 To en théorie)

EFS : L'**Encrypting File System** est une fonctionnalité apparue avec la troisième version des systèmes de fichiers [NTFS](#) disponible depuis [Microsoft Windows 2000](#). Cette technologie permet d'enregistrer des fichiers [chiffrés](#) (cryptées) sur ce système de fichiers, ce qui protège les informations personnelles des attaques de personnes ayant un accès direct à l'ordinateur.

L'[authentification](#) de l'utilisateur et les [listes de contrôle d'accès](#) peuvent protéger les fichiers d'un accès non autorisé pendant l'exécution du [système d'exploitation](#). Mais elles sont facilement contournables si un attaquant obtient un accès physique à l'ordinateur. Une solution est de [chiffrer](#) les fichiers sur les disques de cet ordinateur. EFS réalise cette opération en utilisant la [cryptographie symétrique](#), et assure que le déchiffrement des fichiers est pratiquement impossible sans posséder la bonne clé. Cependant, EFS ne prévient pas les [attaques](#)

par force brute contre les mots de passe des utilisateurs. Autrement dit, le chiffrement de fichier ne procure pas une bonne protection si le mot de passe utilisateur est facilement trouvable.

Différence entre les versions 2003 et 2008 :

- réécriture de la couche réseau ([IPv6](#) et connectivité sans-fil en natif) ;
- amélioration du déploiement, de la récupération et de l'installation basée sur une image source ;
- amélioration des outils de diagnostic, de supervision, de traçabilité des évènements et de rapports ;
- apport de nouvelles fonctionnalités de sécurité telles que [Bitlocker](#), amélioration du [pare-feu](#) Windows avec la configuration sécurisée par défaut ;

Bitlocker : **BitLocker Drive Encryption** est une spécification de protection des données développée par Microsoft, et qui fournit le chiffrement de partition.

BitLocker est inclus dans les versions *Professionnelle*, *Entreprise* et *Intégrale* de Windows Vista¹ ainsi que dans Windows Server 2008 et Windows 7 pour les versions *Entreprise* et *Intégrale*.

BitLocker fournit trois modes d'opération². Les deux premiers modes requièrent un composant matériel cryptographique appelé TPM (Trusted Platform Module) (version 1.2 ou supérieure) et évidemment un BIOS compatible :

- **Transparent operation mode:** Mode d'opération transparent ; l'utilisateur n'a pas à s'identifier lors de la phase de pré-boot (avant l'exécution du BIOS) ;
- **User authentication mode:** Ce mode requiert que l'utilisateur s'identifie (par exemple avec un périphérique USB).

Le troisième mode ne requiert pas de composant matériel TPM :

- **USB-Key (clé USB)** : cela nécessite que l'accès à un périphérique USB soit possible AVANT le chargement du système d'exploitation (c'est une contrainte sur le BIOS)

Pour que BitLocker fonctionne, il faut que le disque contienne au moins deux partitions formatées NTFS :

- le volume système avec au moins 1,5 gigaoctets ;
- le volume de boot qui contient Vista ou 7.

Server Core

Il s'agit probablement de la nouveauté la plus notable proposée par Windows Server 2008 : l'option d'installation Server Core installe uniquement le strict minimum. Exit par exemple l'[Windows Explorer](#) (donc plus d'interface graphique, à l'instar d'[Ubuntu Server](#) par exemple) (*Il faut savoir qu'il existe une version alternante qui n'installe pas la partie graphique dans Ubuntu.*). Il ne contient pas non plus le [Framework .NET](#), [Internet Explorer](#), ou toute autre fonctionnalité qui n'est pas indispensable au bon fonctionnement du noyau. La configuration et la maintenance s'effectueront alors en ligne de commande ou en se connectant à distance à la machine au travers d'un logiciel qui, lui, pourra offrir une interface graphique.

Cette installation apporte plusieurs avantages :

- Réduction tout d'abord des ressources nécessaires ;
- Réduction de la maintenance et de la gestion, puisque seuls les éléments nécessaires pour les rôles définis sont à installer et configurer ;

- Réduction enfin de la surface d'exposition aux attaques, directement lié au nombre réduit d'applications et services exécutées sur le serveur ;

Une machine Server Core peut être configurée pour assurer plusieurs rôles de base :

- Services de domaine [Active Directory](#) (AD DS)
- Services AD LDS (Active Directory Lightweight Directory Services)
- Serveur [DHCP](#)
- Serveur [DNS](#)
- [Serveur de fichiers](#)
- Serveur d'impression
- Services de diffusion multimédia en continu

Ainsi que les fonctionnalités facultatives suivantes :

- Sauvegarde
- Chiffrement de lecteur [BitLocker](#)
- Équilibrage de la charge réseau
- Service [WINS](#) (Windows Internet Name Service)

Les rôles *Active Directory*

Active Directory comprend désormais les services d'identité, de certificats et de gestion numérique des droits. Jusqu'à [Windows Server 2003](#), *Active Directory* a permis aux administrateurs réseaux de gérer centralement les ordinateurs interconnectés, de définir des stratégies pour un ensemble ou groupe d'utilisateurs, et de déployer centralement de nouvelles applications à une multitude d'ordinateurs.

Les services de Certificats et d'Identité permettent aux administrateurs de gérer les comptes utilisateurs et les certificats numériques qui leur permettent d'accéder à certains services et systèmes. *Federation management services* permet aux entreprises de partager des données d'authentification avec des partenaires et clients de confiance, permettant ainsi à un consultant d'utiliser son propre compte utilisateur et mot de passe afin d'ouvrir une session sur le réseau de son client. *Identity Integration Feature Pack* est inclus à *Active Directory Metadirectory Services (ADMS)*. Chacun de ces services représente un rôle serveur.

Terminal Services

Windows Server 2008 apporte des améliorations majeures à [Terminal Services](#). Terminal Services est désormais compatible avec le protocole de [bureau à distance](#) en version 6.0 **Remote Desktop Protocol 6.0**. L'amélioration la plus notable consiste en la capacité à partager une application au travers d'une connexion de *bureau à distance*, à la place du *bureau* entier. Cette fonctionnalité est nommée **Terminal Services Remote Programs**.

Windows PowerShell

Windows Server 2008 est le premier système d'exploitation qui intègre [Windows PowerShell](#), le nouveau [shell](#) extensible en ligne de commande de Microsoft qui inclut des fonctionnalités de technologie de *scripting*. **PowerShell** repose sur de la programmation orientée objet et sur la version 2.0 du *Framework*.

Microsoft .NET, et inclut plus de 120 outils d'administration système, avec une convention de nommage et une syntaxe consistante, et la capacité intégrée d'opérer avec des données standards de gestion telles que la base de registre Windows, les magasins de certificats, ou [**Windows Management Instrumentation \(WMI\)**](#).

WMI est un système de gestion interne de Windows qui prend en charge la surveillance et le contrôle de ressource système via un ensemble d'interfaces. Il fournit un modèle cohérent et organisé logiquement des états de Windows.

Le langage de script *PowerShell* a été conçu spécifiquement pour l'administration IT, et peut être utilisé en lieu et place de **cmd.exe** et **Windows Script Host**.

Auto-réparation NTFS

Dans les versions antérieures de Windows, si le système d'exploitation détecte une corruption dans le système de fichiers d'un volume [**NTFS**](#), celui-ci marque le volume comme « *impropre* » ; pour corriger les erreurs sur le volume, celui-ci devait être *déconnecté*. Avec la fonctionnalité Auto-réparation NTFS, un processus réparateur NTFS est lancé en arrière-plan et effectue une réparation ciblée des structures endommagées, en ne laissant que les fichiers ou dossiers endommagés comme indisponibles et non pas l'intégralité du volume.

Hyper-V

Hyper-V est un hyperviseur de système virtuel, formant la partie centrale de la stratégie de [**virtualisation**](#) de Microsoft. Il permet de virtualiser des serveurs au niveau de la couche *Kernel* du système d'exploitation. Il peut être vu comme le partitionnement d'un unique serveur physique en plusieurs petits ensembles d'ordinateurs. Hyper-V inclut la possibilité d'opérer en tant qu'hôte hyperviseur de virtualisation [**Xen**](#) (logiciel libre d'hypervision), permettant ainsi aux systèmes d'exploitation avec la fonction Xen activée d'être virtualisés. Cette fonctionnalité n'était pas initialement intégrée à Windows Server 2008, mais était disponible trois mois après la sortie mondiale de Windows Server 2008, uniquement sur les versions 64 bits de Windows Server 2008.

la Sauvegarde de Windows Server

Windows Server 2008 R2

Quelles sont les principales évolutions ?

L'utilitaire de sauvegarde de Windows Server a été considérablement amélioré dans Windows Server® 2008 R2. Il inaugure des fonctionnalités qui autorisent un contrôle accru quant au choix des éléments à sauvegarder et des emplacements de sauvegarde. Il offre également une prise en charge étendue de la ligne de commande et de Windows PowerShell™ pour la gestion à distance des sauvegardes.

Windows Server 2008 R2 bénéficie des évolutions suivantes, qui se traduisent par des améliorations en termes de flexibilité, d'efficacité et de facilité de gestion sur le plan de la création et de la gestion des sauvegardes, et de l'exécution des récupérations.

- Aptitude à sauvegarder/exclure des fichiers individuels et à inclure/exclure des types de fichiers et des chemins d'accès au niveau d'un volume
- Amélioration des performances et de l'utilisation des sauvegardes incrémentielles
- Options étendues de stockage des sauvegardes
- Amélioration des options et des performances de sauvegarde et de récupérations de l'état du système

- Prise en charge étendue de la ligne de commande
- Prise en charge étendue de Windows PowerShell

INSTALLATION DU SERVEUR 2008 EN MODE GRAPHIQUE :

www.ToutWindows.com

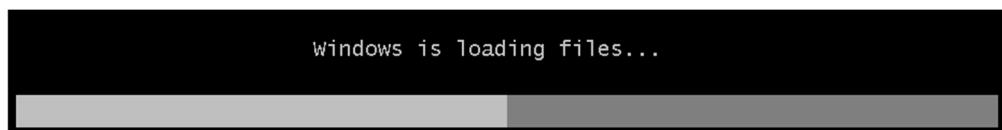
1 - Matériel nécessaire :

Un PC avec un lecteur de DVD et mini 512 Mo de RAM.

2 - Boot :

Insérez le DVD dans le lecteur et redémarrez le PC

Après avoir appuyé sur une touche, Windows PE est chargé :



Choisissez la langue, le format de date et monnaie et le clavier :

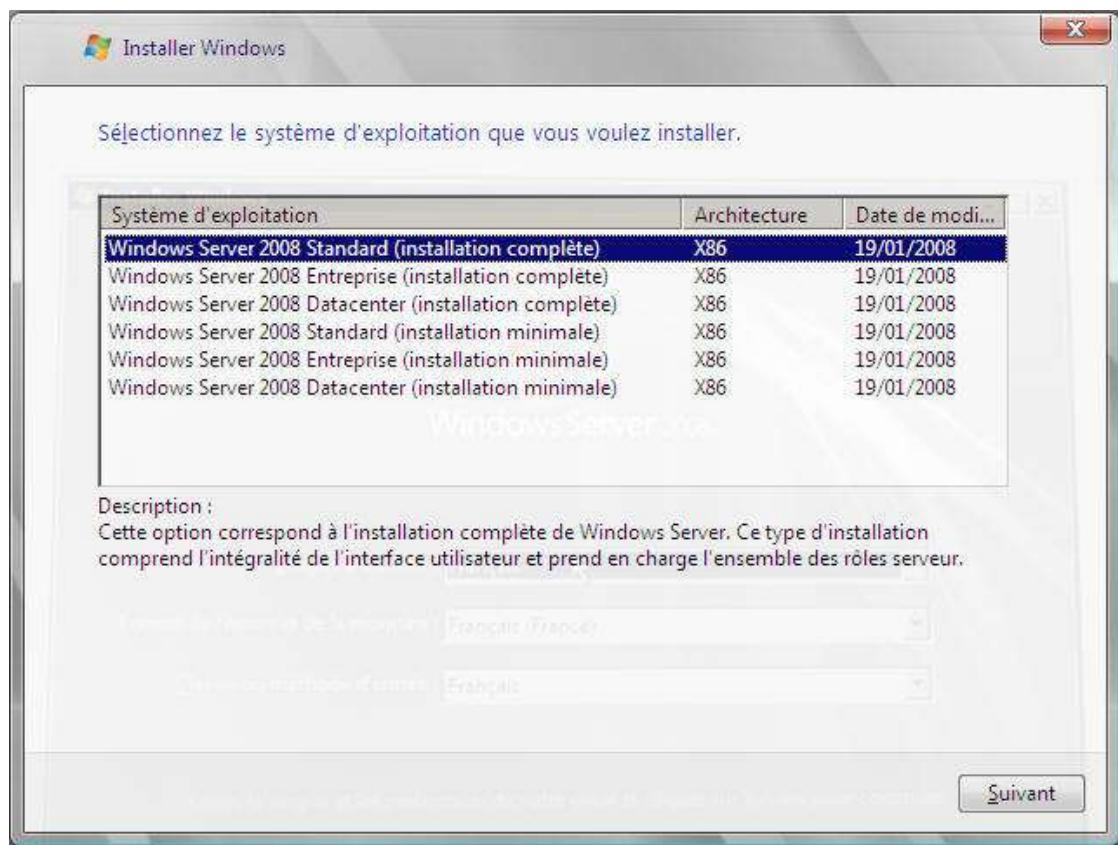


Choisissez Installer :

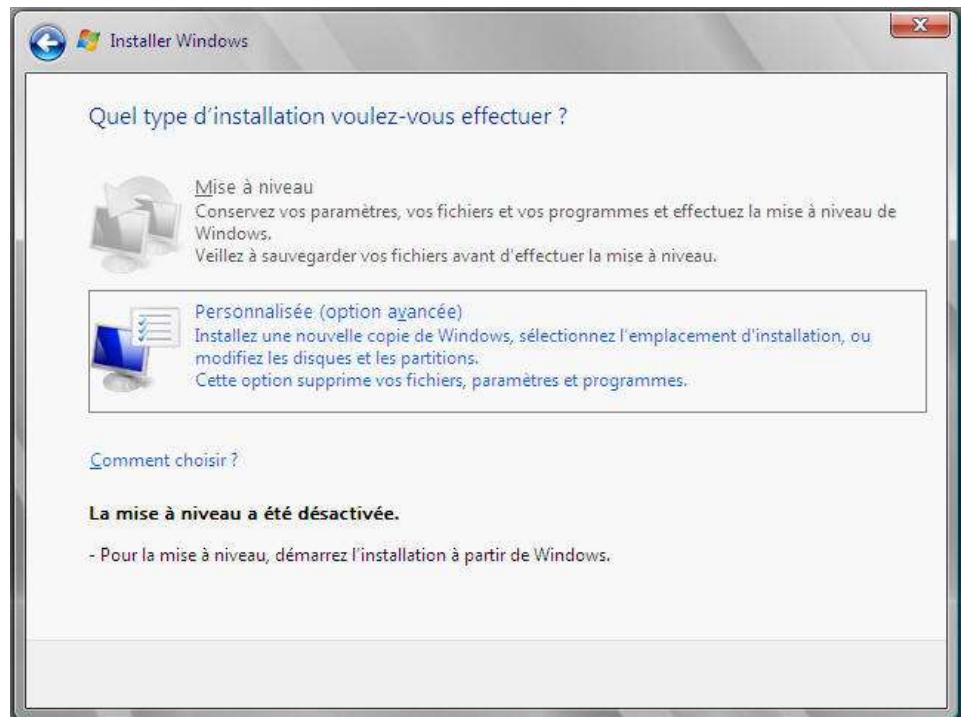


Saisissez la clef de produit, ou pas de clef pour une évaluation.

Si vous n'avez pas saisi de clef, alors vous devez choisir la version de Windows à Installer, sinon celle-ci est imposée par la clef et vous n'avez le choix qu'entre la version Core (traduite installation minimale) ou l'installation complète.



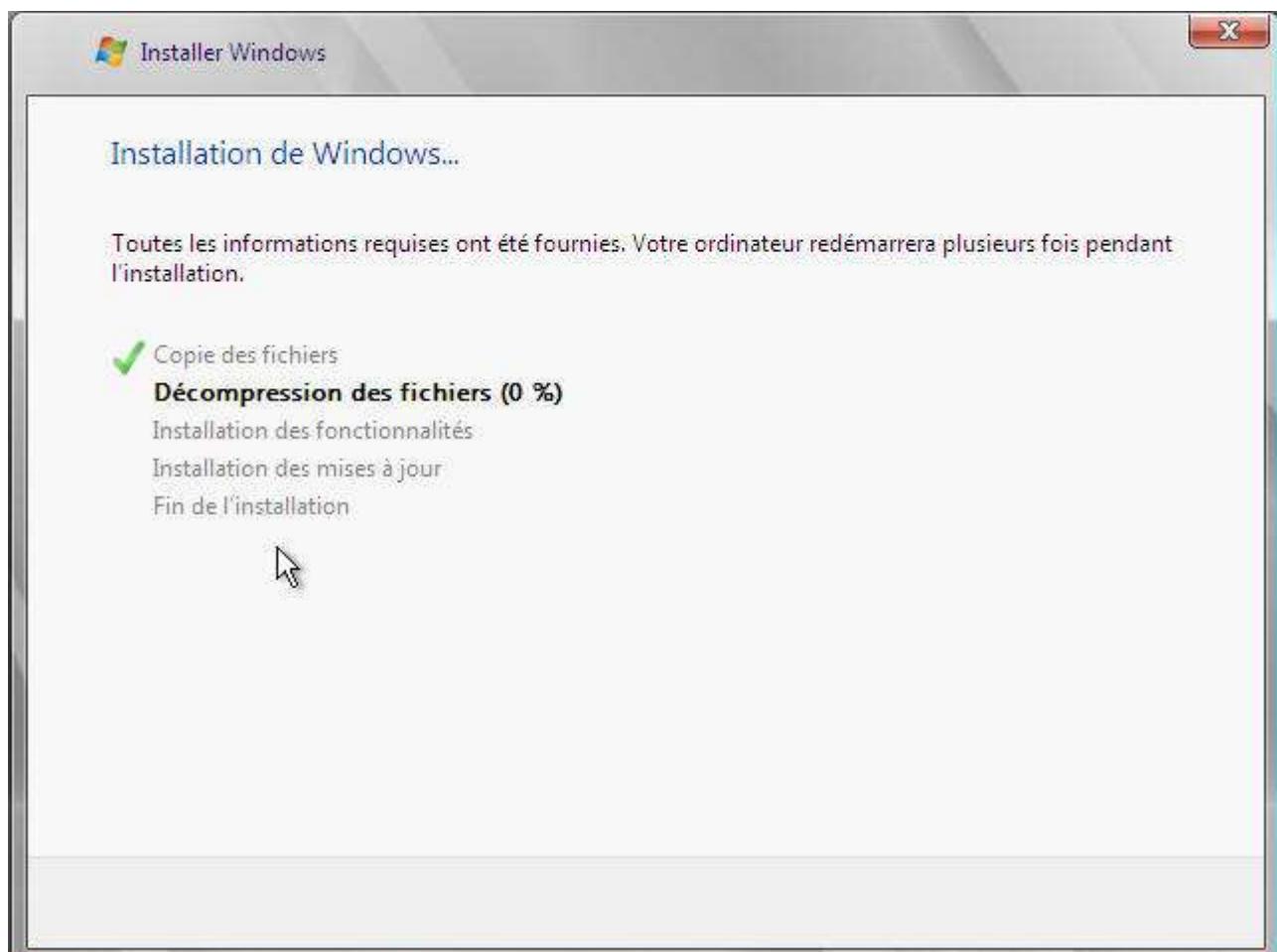
Choisissez le type d'installation (le choix Upgrade est disponible uniquement avec un lancement du programme depuis une version de Windows installée sur le disque dur).



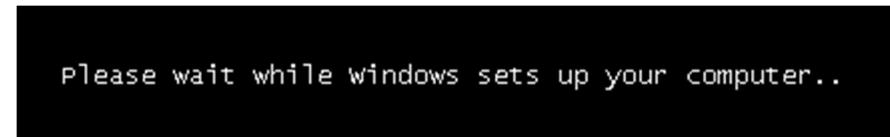
Le choix Options de lecteur vous permet d'accéder aux fonctions de création ou extension de partition, ou formatage.



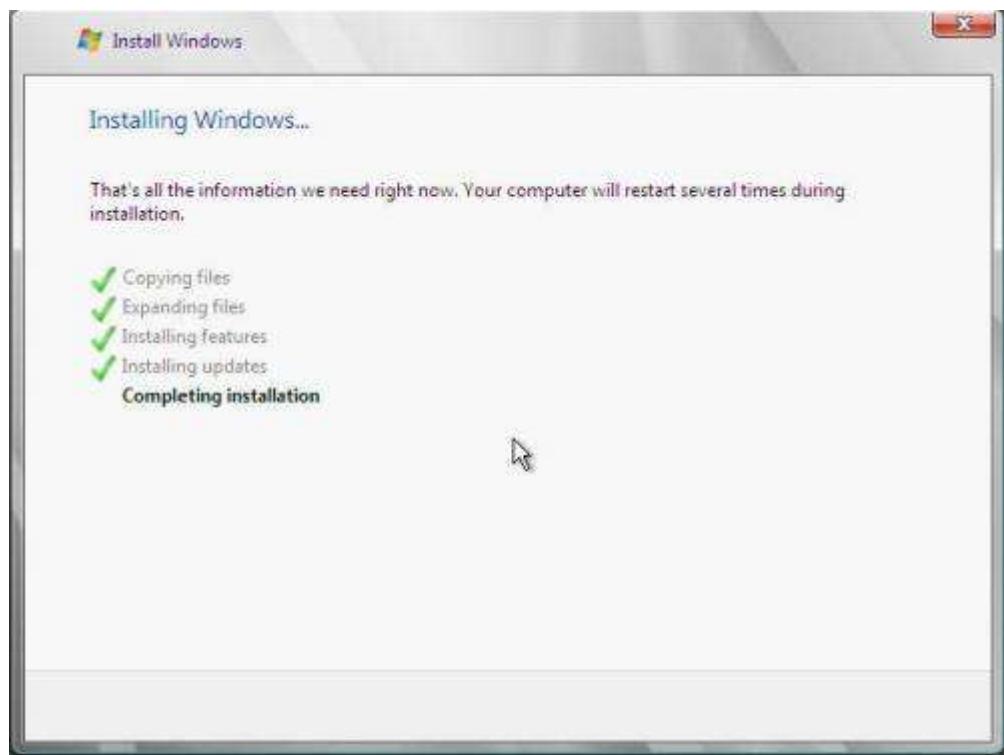
Un appui sur Suivant lance l'installation.



Puis un premier redémarrage :

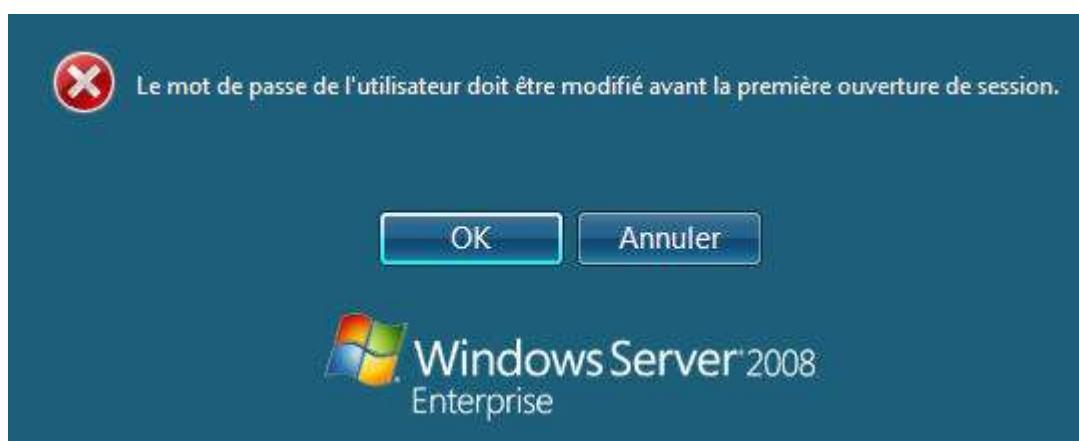


Finalisation de l'installation :



Second boot :

Windows impose de mettre un mot de passe

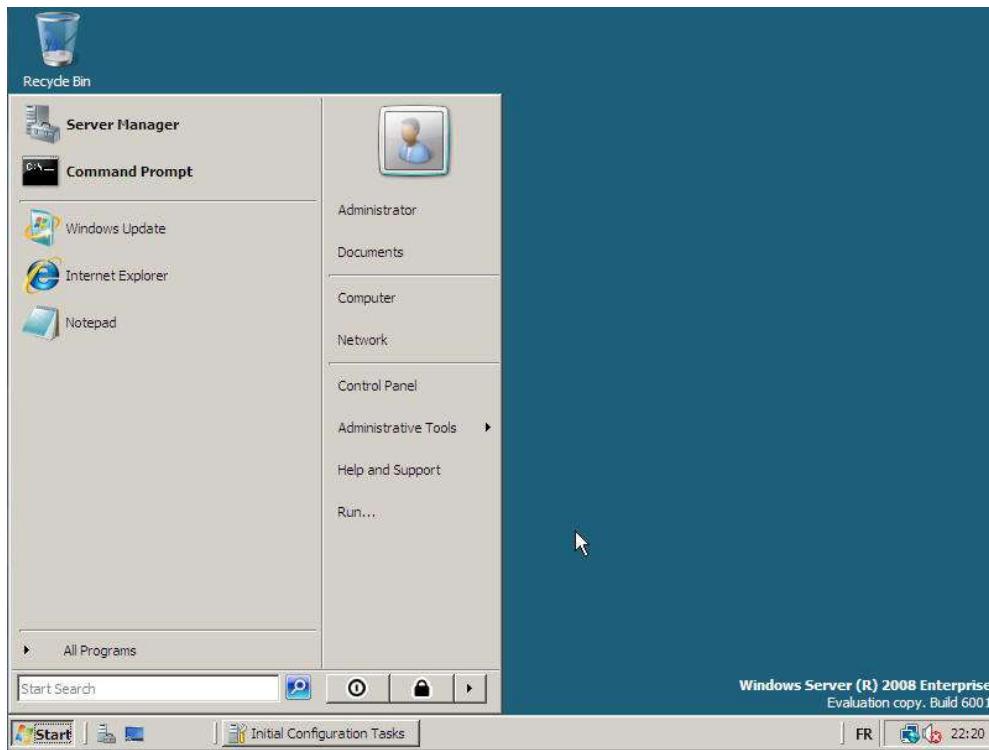


Pendant le démarrage, Windows indique les différentes tâches effectuées :

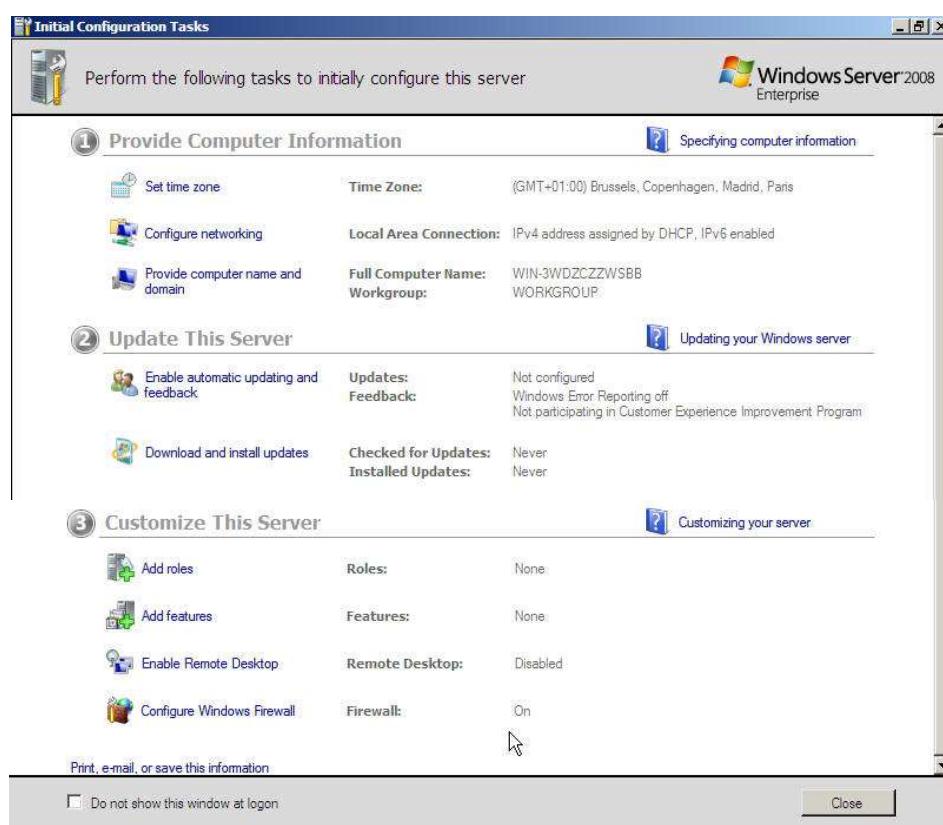
Applying user settings

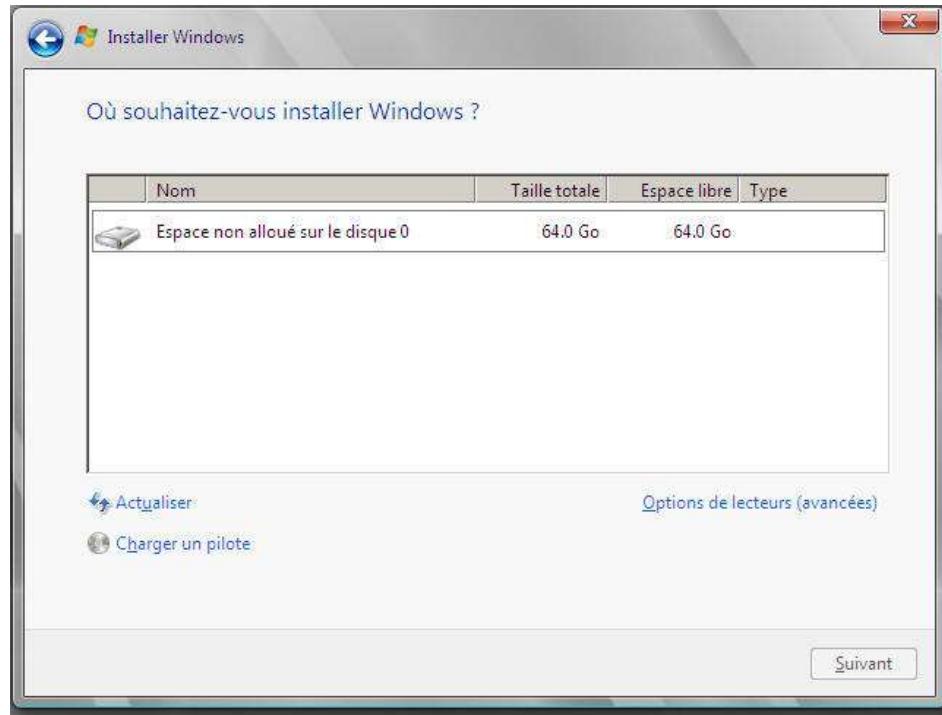
Preparing your desktop

C'est terminé :



et du nouvel assistant de configuration initiale :



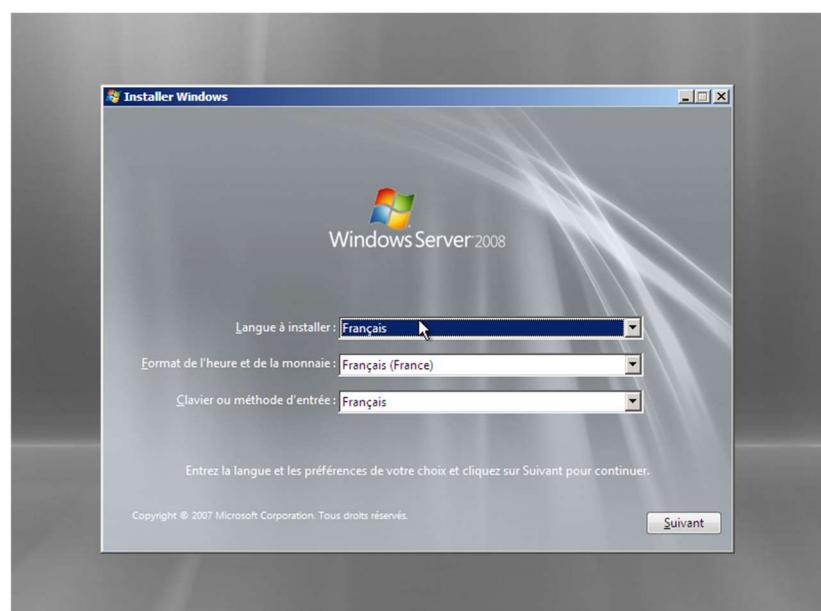


LE MODE CORE :

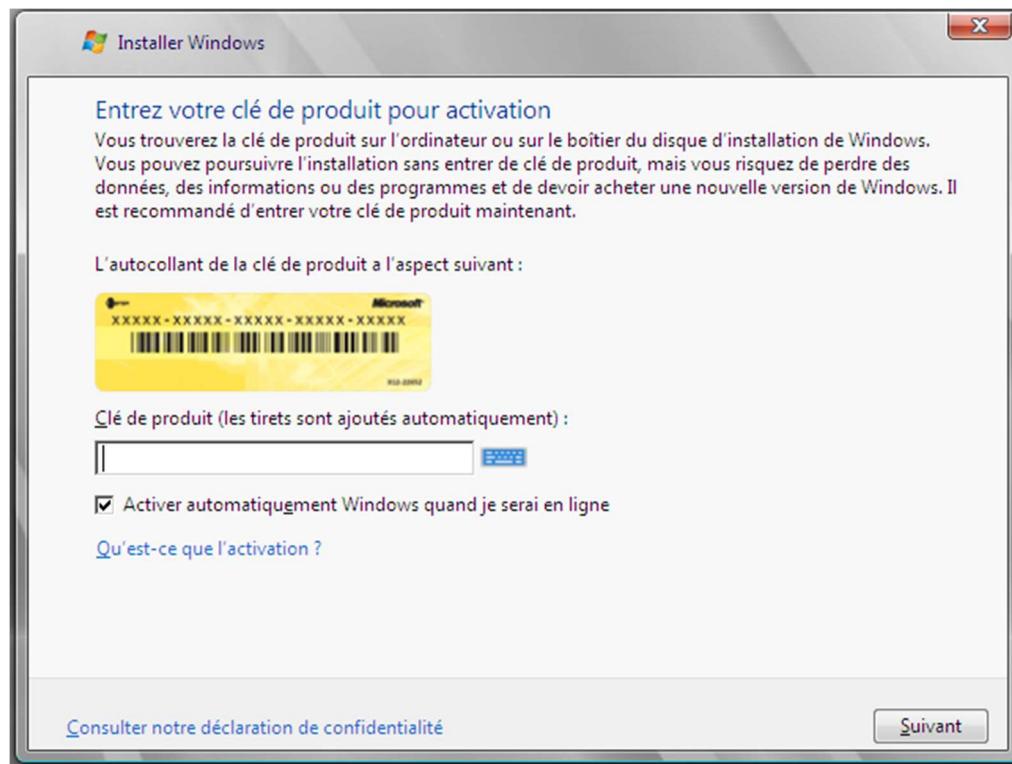
La version "Core" est une version allégée pourvu d'options d'installations et de configurations minimales. La configuration des composants se fait en **ligne de commande uniquement**. Cette version est en effet dépourvu d'Internet Explorer, de panneau de configuration et autres outils de configuration graphiques.

Cette version est idéale pour les composants d'infrastructures comme Active Directory, LDAP, Diffusion, Exchange, IIS ou encore DNS, DHCP, etc... mais ne conviendra pas pour des applications comme Powershell, le .NET n'étant pas implémenté.

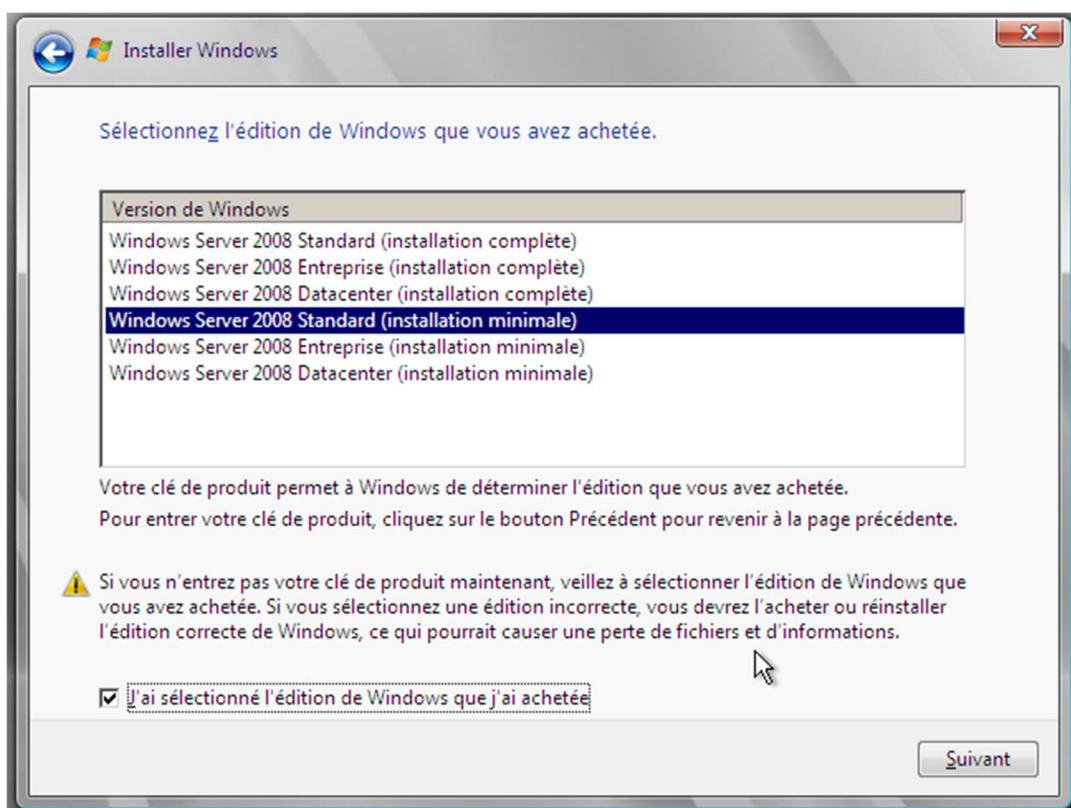
Le choix de l'installation du mode "Core" se fera durant l'installation. Il faut savoir que ce choix est irréversible !



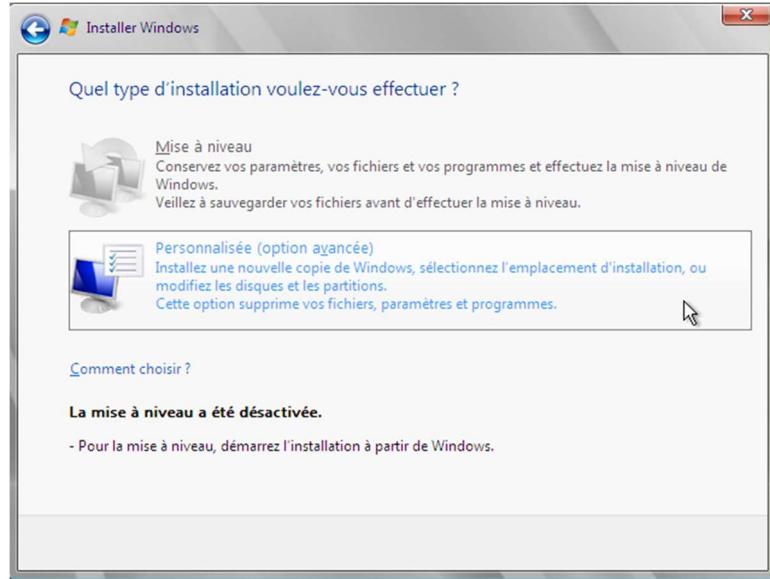
Une fois les paramètres régionaux sélectionnés nous passons à la fenêtre de licence. Lors de cette installation je reste en mode évaluation (30 jours) en ne rentrant aucune information d'enregistrement.



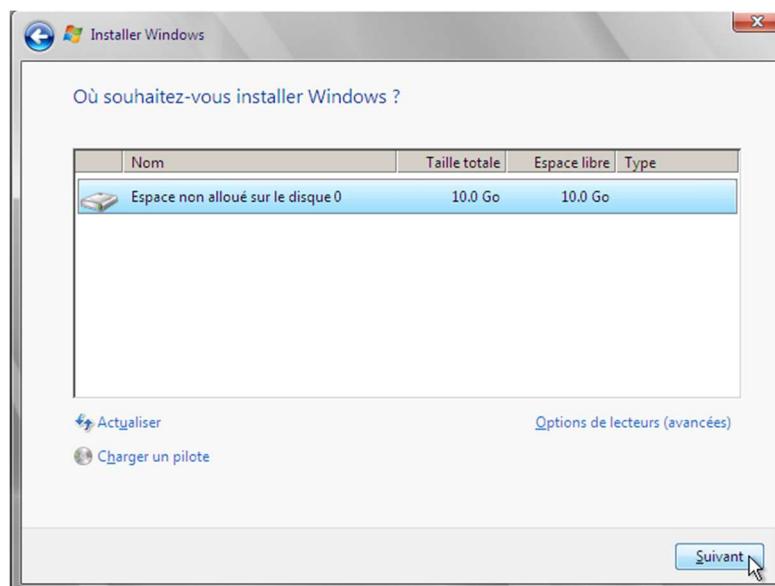
C'est à cette étape nous allons sélectionner l'édition "Core", appelée minimale dans l'installation en français. J'ai sélectionné ici la version "Core" standard:



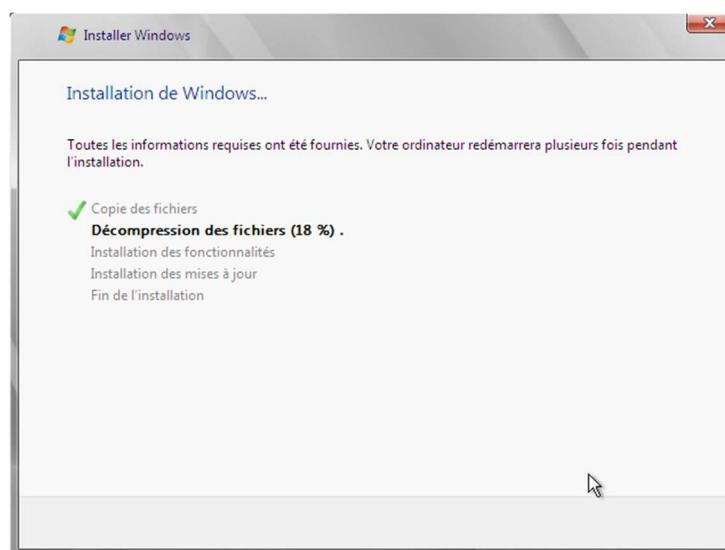
La mise à niveau n'est disponible qu'à partir d'un serveur en 2003, je continu donc en mode d'installation personnalisé:



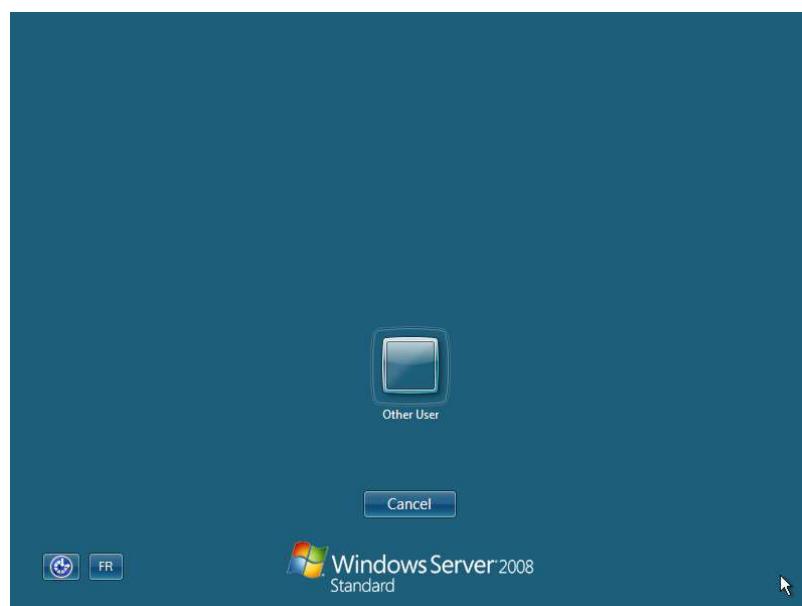
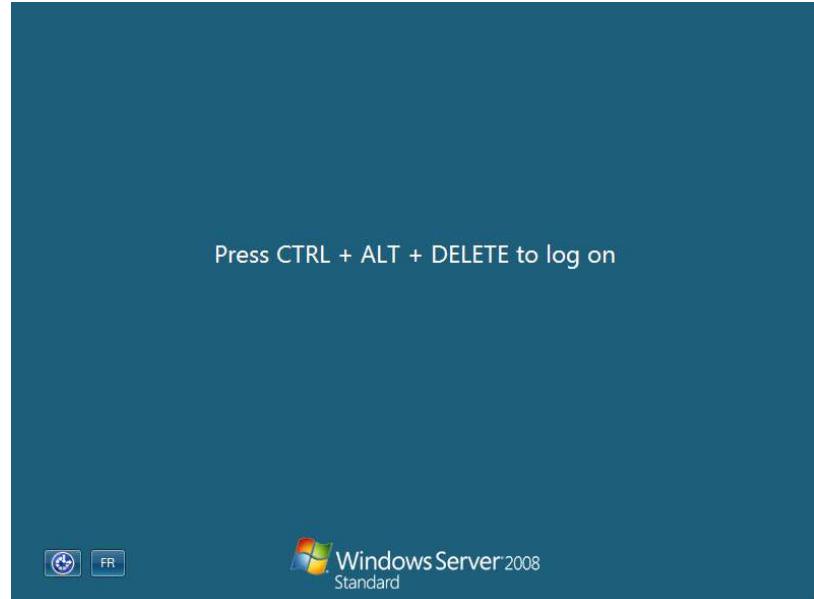
Je sélectionne ma partition système :



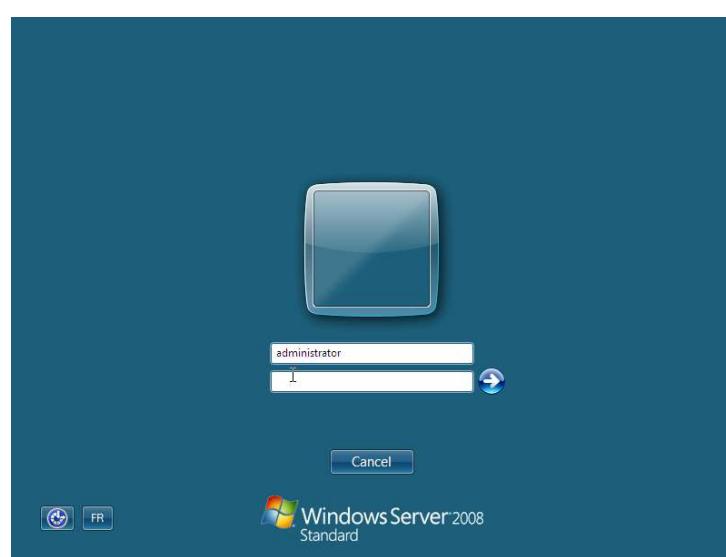
Et je lance enfin l'installation :



L'installation est relativement rapide en version "Core", une quinzaine de minutes environ. Pendant le processus d'installation le système redémarrera 2 fois. Une fois terminée nous arrivons enfin sur la mire Windows Serveur 2008 classique :



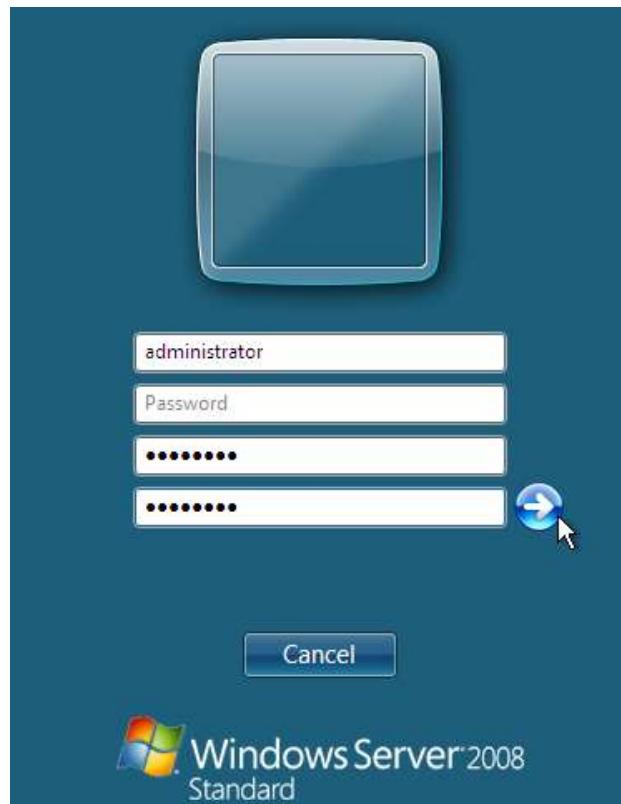
Tout comme la version standard de Windows, il faut s'authentifier avec le compte **administrator / administrateur** et sans mot de passe !



Nous devons changer le mot de passe.

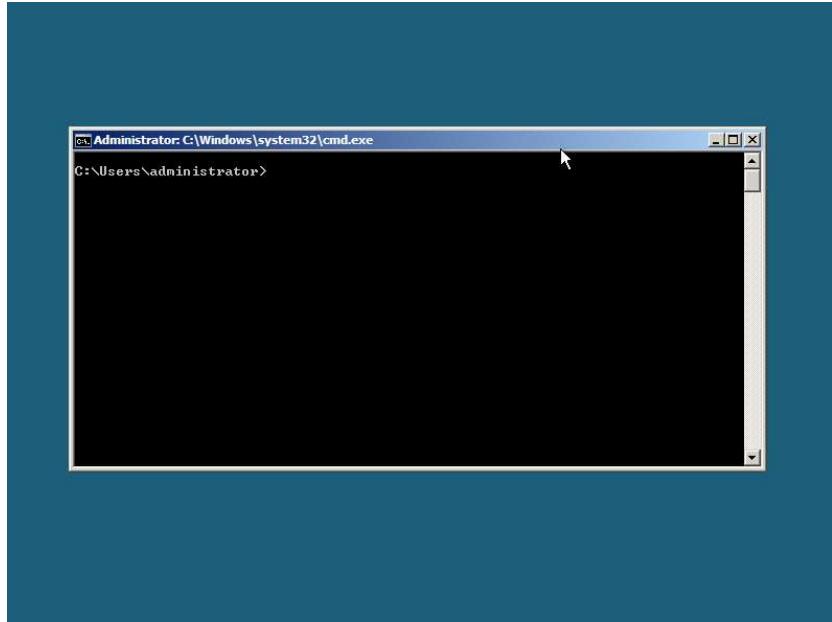


Et il doit être suffisamment long et compliqué pour être accepté (Majuscule, chiffre, etc..)



Cliquez sur **OK** et le bureau va se charger :





Et voilà c'est terminé !

La version "Core" ne contient qu'une simple invite de commande.

Voici pour les deux mots de configurations possibles.

ROUTAGE / NAT

ROUTEUR

Les services de stratégie et d'accès réseau vous permettent de fournir un accès réseau local et distant, ainsi que de définir et d'appliquer des stratégies pour l'authentification d'accès réseau. Nous allons voir la partie permettant de faire communiquer deux réseaux ou deux sous-réseaux entre eux. Grâce au rôle de routage réseau.

Le rôle d'un routeur est de rediriger les paquets qu'il reçoit en fonction d'une table de routage vers le routeur suivant jusqu'à atteindre le réseau local de destination. Chaque paquet comporte l'adresse d'origine et l'adresse de destination.

NAT

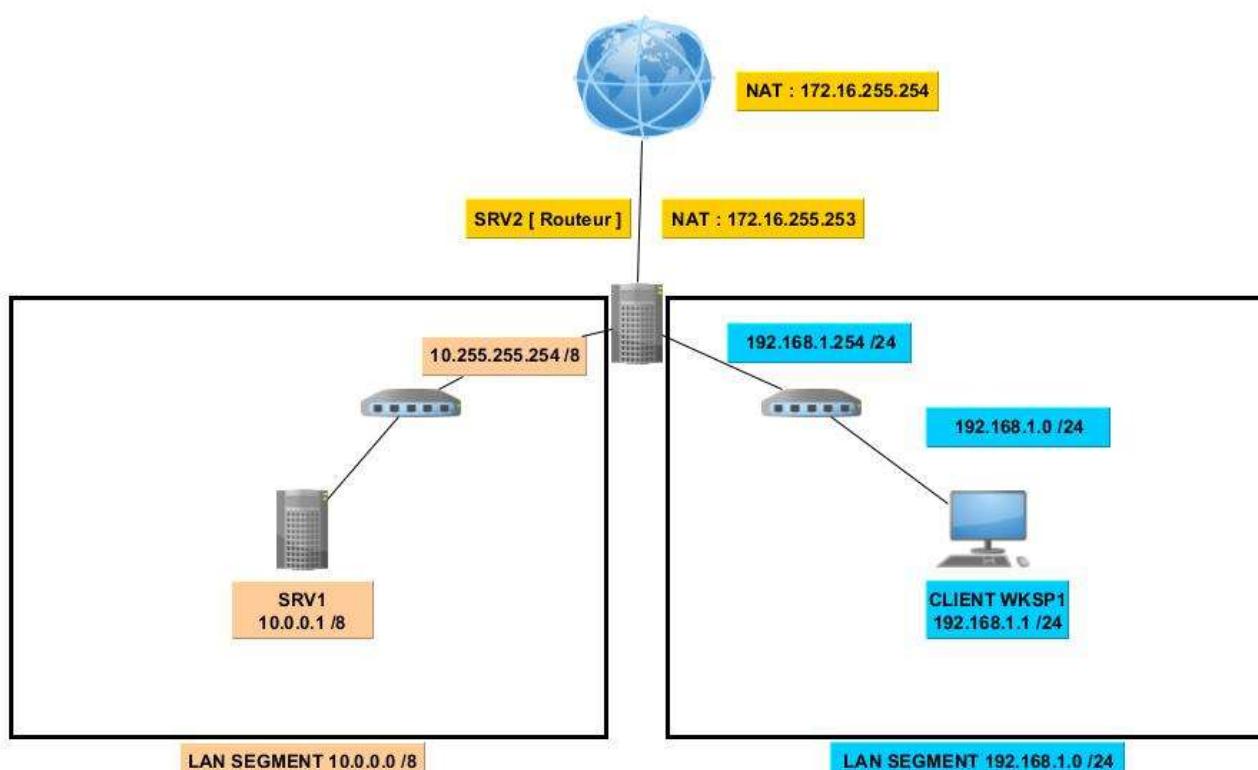
Dans le cas d'adresses privées, l'adresse d'origine est une adresse privée inconnue Internet. Le destinataire ne pourra pas répondre. Il faut donc remplacer l'adresse privée d'origine par une adresse publique. C'est le travail d'un routeur NAT (Network Address Translation) qui effectue la transformation des adresses. Pour aller plus loin vous pouvez vous informez sur « la notion de port ».

Lorsqu'une machine du réseau local envoie des paquets à un serveur à l'extérieur, l'adresse d'origine est une adresse privée. Le destinataire ne pourra pas répondre à cette adresse. Pour résoudre ce problème, le routeur NAT remplace l'adresse et le port d'origine par l'adresse Internet publique du routeur et un numéro de port libre choisi au hasard en notant adresse et ports associés à la machine locale

Installation d'une maquette fonctionnelle pour mettre en place un routage réseau avec NAT.

Pour cette maquette il nous faudra deux Windows Server 2008 R2 Entreprise ou Standard, ainsi qu'un poste client Windows 7 ou 10 en version Professionnel par exemple.

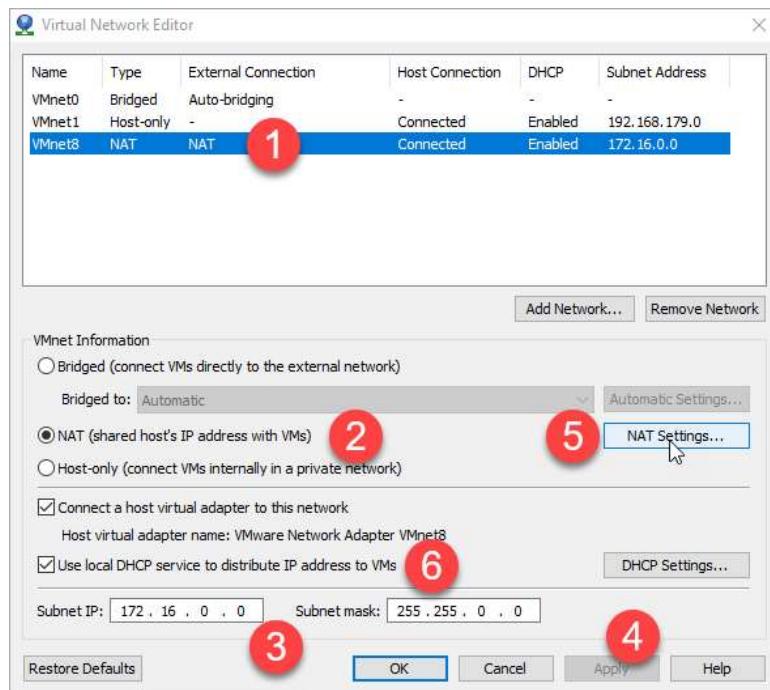
Plan de la maquette :



Réglage du NAT dans Vmware :

Aller dans **Edit > Virtual Network Editor** :

Puis renseigner les réglages comme la capture d'écran ci-dessous.



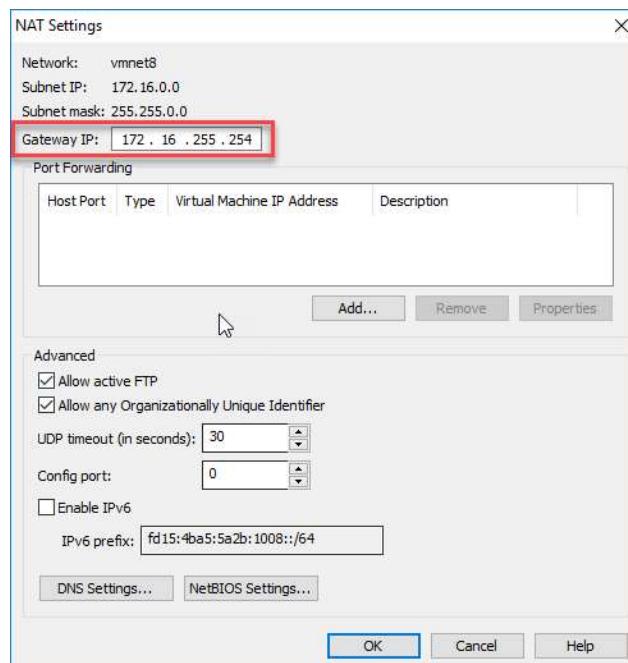
1 – NAT -> Cliquez sur l'interface NAT

2 – Vérifier que le Vmnet Information est bien réglé sur **NAT**.

3 – Renseigner l'adresse Subnet IP : **172.16.0.0** et Subnet mask sur **255.255.0.0**

4 – Cliquez sur **Apply** pour modifier les cartes virtuelles du serveur.

5 – Cliquez sur **NAT Settings**, renseignez la nouvelle IP.

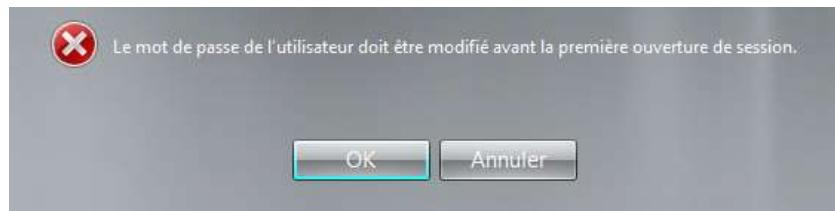


6 – Décochez « Use local DHCP service to distribute IP address to VMs ».

Réglage à faire sur le SRV1.

- Création du compte **administrateur** avec le mot de passe « **Respons11** »
- Mettre le nom du serveur.
- Activer une règle permettant de laisser passer les requêtes de **PING ICMP**.
- Régler la carte réseau sur le **LAN SEGMENT 10**.
- Régler l'IP du serveur.

1 - Crédation du compte **administrateur** avec le mot de passe « **Respons11** »

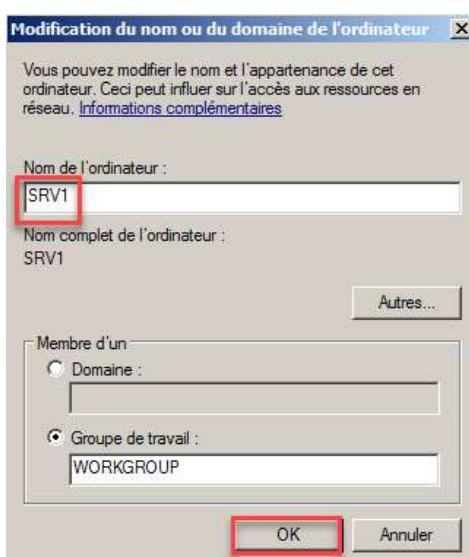


Renseigner le mot de passe du compte **administrateur : Respons11**



- **2 - Mettre le nom du serveur.**

Aller dans les propriétés systèmes : Panneau de configuration => Système
Ensuite cliquez sur **Modifier** puis changer le nom en **SRV1**. Cliquez sur **OK**.



Redémarrez la machine.

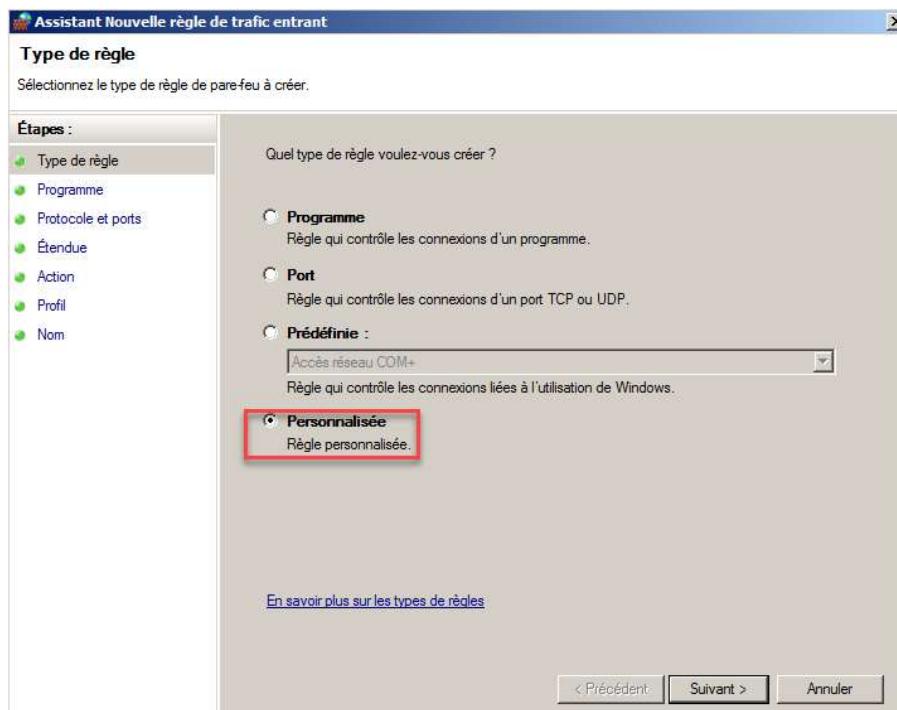
3 - Activer une règle permettant de laisser passer les requêtes de **PING ICMP**.

Aller dans la console de **gestion du pare-feu avec fonctions avancées de sécurité**.

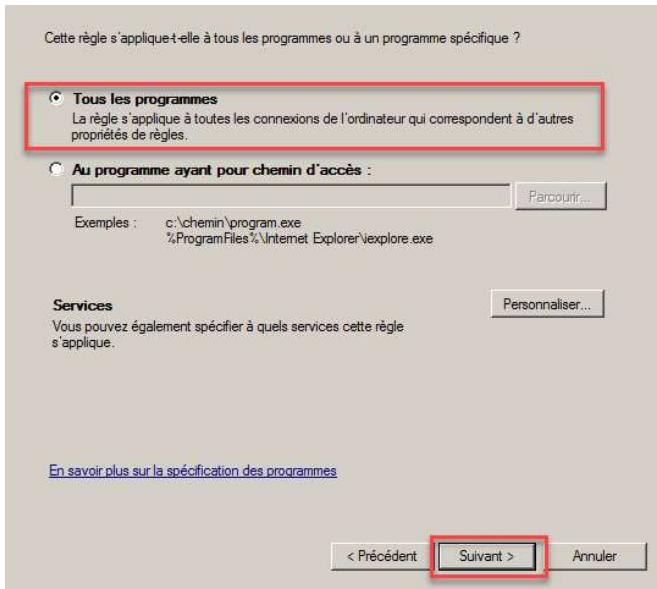
Allez sur **règles de trafic entrant** et faites un **clic droit** ensuite **clic gauche** sur **Nouvelle règle**.



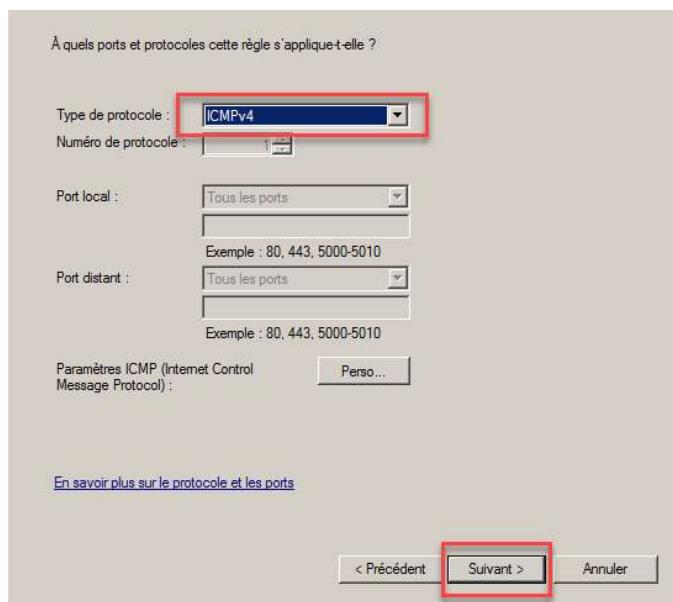
Cocher sur **Personnalisée**, puis cliquez sur **Suivant**.



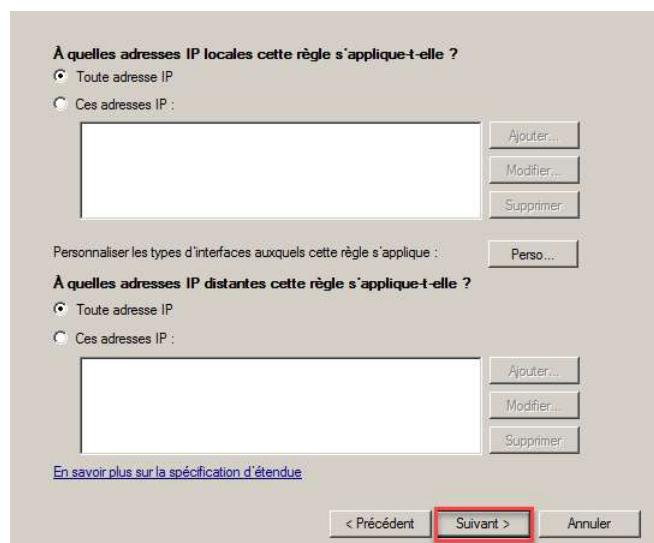
Laissez cocher sur **Tous les programmes** et cliquez sur **Suivant**, ce réglage permet d'autoriser le ping à tous les programmes pouvant en avoir besoin comme des logiciels permettant.



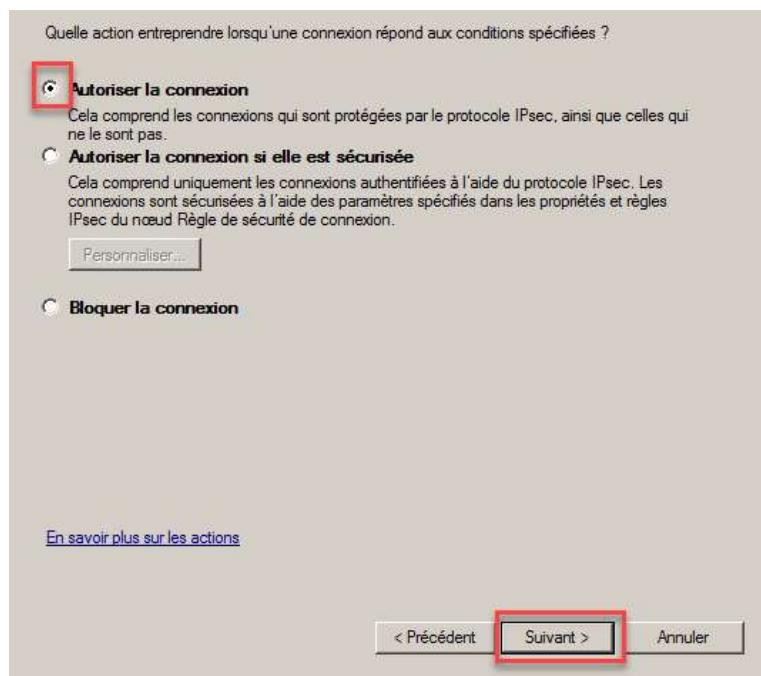
Dans type de protocole choisir ICMPv4 et cliquez sur Suivant, ce réglage permet d'autoriser le ping (ICMPv4).



Il faut ici spécifier à quelles adresses locales s'applique cette règle. Ici nous voulons que nous puissions pinger toutes les machines et que cette machine soit joignable par la requête de ping depuis n'importe quelle machine du réseau. Cliquer ensuite sur Suivant.



Cette fenêtre nous permet de choisir l'action à entreprendre en cas de connexion. Nous allons **autoriser la connexion**. Cliquer ensuite sur **Suivant**.



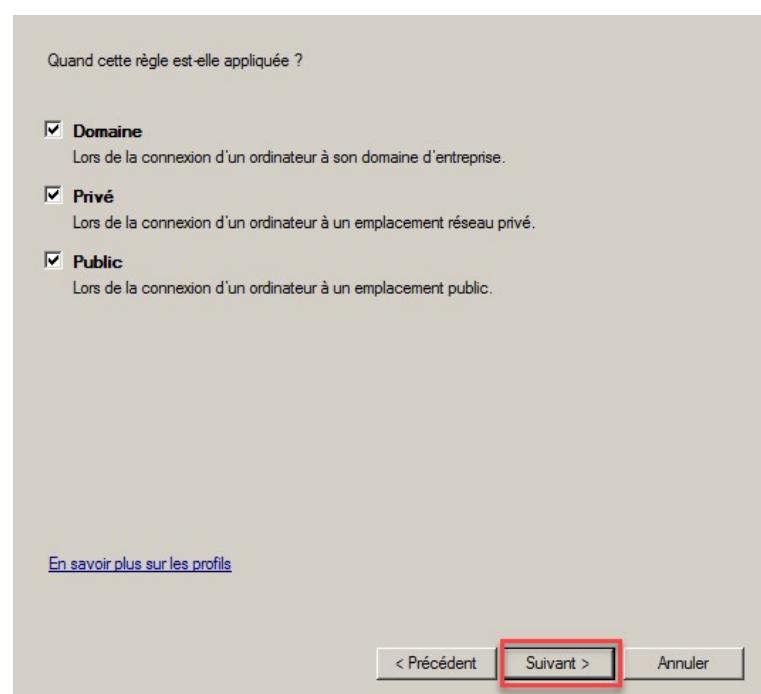
Le déblocage du ping par le pare-feu est soumis à une règle d'emplacement réseau, selon le contexte utilisé, on peut ou non autoriser le ping dans :

Un réseau d'entreprise avec un domaine Active Directory

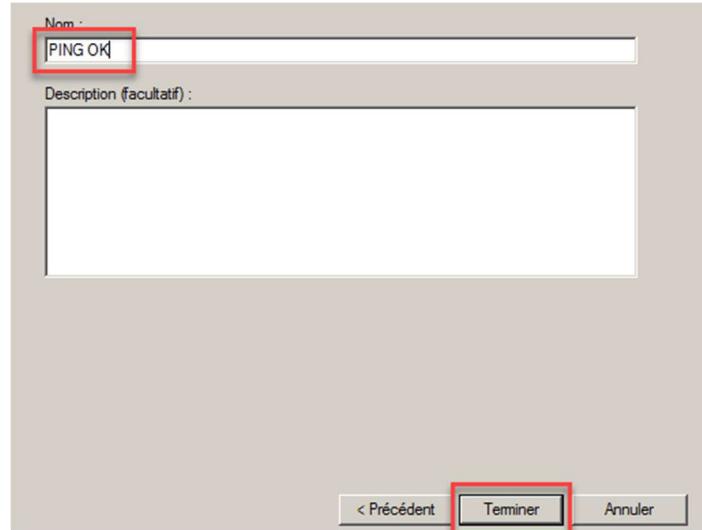
Un réseau privé : A la maison ou dans une entreprise n'utilisant pas un domaine.

Un réseau public comme un cybercafé, une gare, ou alors un accès wifi visteur HOTSPOT, etc.

Cliquez simplement sur **Suivant**.



J'ai nommé ma règle PING OK. Cliquer sur **Terminer**, une fois votre règle nommée.



Une fois la règle créée, faites la même chose pour **la règle de Traffic sortant**.

REGLAGE DE L'ADRESSE IP SUR LA CARTE RESEAU

Dans le gestionnaire de serveur cliquer sur **Afficher les connexions réseau**.

Gestionnaire de serveur (SRV1)

Résumé serveur

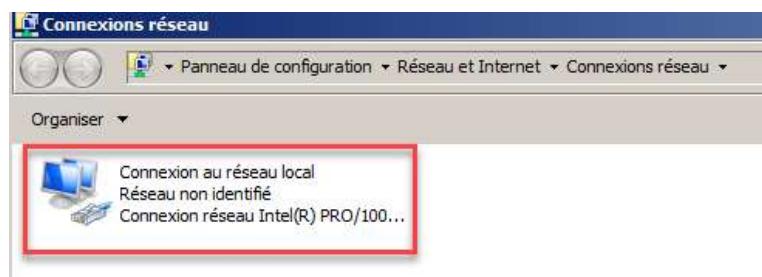
Informations sur l'ordinateur

Nom complet de l'ordinateur :	SRV1
Groupe de travail :	WORKGROUP
Connexion au réseau local :	Adresse IPv4 attribuée par DHCP, Compatible IPv6

Aide récapitulative sur le serveur

- Activer Windows
- Modifier les propriétés système
- Afficher les connexions réseau**
- Configurer le Bureau à distance
- Configurer la gestion à distance du Gestionnaire de serveur

Voici votre réseau, vous pouvez cliquer sur le **bouton droit pour renommer** la carte réseau. Par exemple mettre son adresse IP pourrait vous permettre de ne pas se mettre la même IP sur plusieurs machines. Ensuite double cliquer sur **le nom de la carte réseau**.

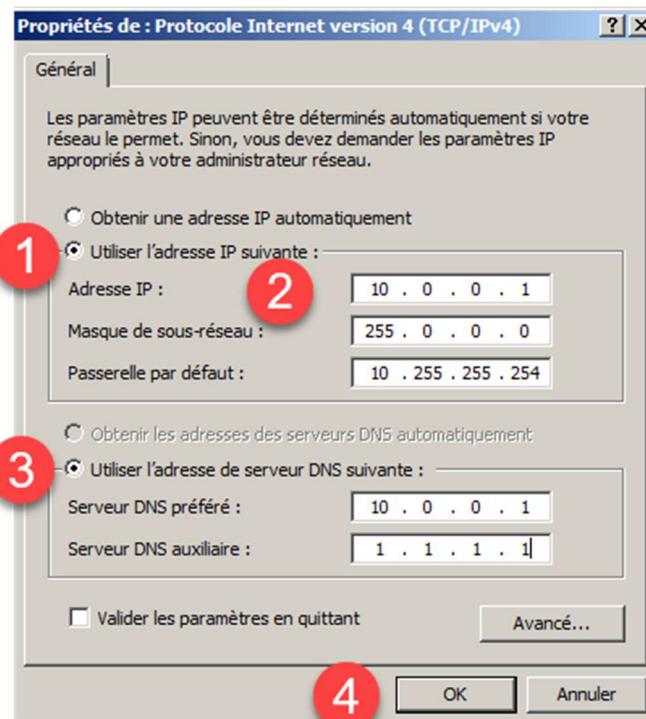


Cliquer sur **Propriétés** pour accéder aux réglages réseaux.



Penser à décocher la prise en charge du **Protocole Internet version 6**. Nous l'utiliserons plus tard avec un serveur de messagerie.

Ensuite sélectionner **Protocole Internet version 4** et cliquer sur **Propriétés**.



Cocher **Utiliser l'adresse IP suivante** :

Renseigner l'adresse IP 10.0.0.1

Le masque de sous-réseau : 255.0.0.0

La passerelle par défaut : 10.255.255.254

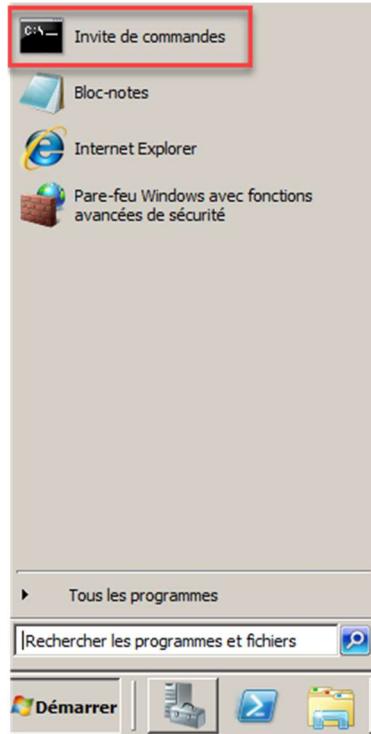
Cocher **Utiliser l'adresse de serveur DNS suivante** :

Serveur DNS préféré : 10.0.0.1

Serveur DNS auxiliaire : 1.1.1.1

Cliquer sur **OK** une fois les informations correctement saisies. Puis **Fermer** deux fois.

La méthode de vérification la plus efficace est de passer par l'invite de commande. Cliquer sur **Démarrer**, puis **Invite de commandes**.



Une fois dans l'invite de commande, taper la commande **IPCONFIG /ALL**.

Vous pouvez vous afficher les informations voulues.

```
Administrator : C:\Windows\system32\cmd.exe
C:\Users\Administrateur>IPCONFIG /ALL
Configuration IP de Windows
  Nom de l'hôte . . . . . : SRU1
  Suffixe DNS principal . . . . . : 
  Type de noeud. . . . . : Hybride
  Routage IP activé . . . . . : Non
  Proxy WINS activé . . . . . : Non

Carte Ethernet Connexion au réseau local :
  Suffixe DNS propre à la connexion. . . . . : Connexion réseau Intel(R) PRO/1000 M
  Description. . . . . : Connexion réseau Intel(R) PRO/1000 M
  Adresse physique . . . . . : 00-0C-29-5E-59-8D
  DHCP activé. . . . . : Non
  Configuration automatique activée. . . . . : Oui
  Adresse IPv4. . . . . : 10.0.0.1<préféré>
  Masque de sous-réseau. . . . . : 255.0.0.0
  Passerelle par défaut. . . . . : 10.255.255.254
  Serveurs DNS. . . . . : 10.0.0.1
  NetBIOS sur Tcpip. . . . . : Activé

Carte Tunnel isatap.<C3CC04D2-42D8-4031-85C0-DC9D1A8C7901> :
  Statut du média. . . . . : Média déconnecté
  Suffixe DNS propre à la connexion. . . . . : 
  Description. . . . . : Carte Microsoft ISATAP
  Adresse physique . . . . . : 00-00-00-00-00-00-E0
  DHCP activé. . . . . : Non
  Configuration automatique activée. . . . . : Oui

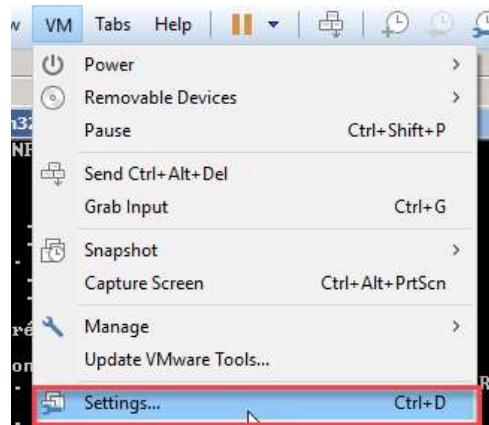
Carte Tunnel Connexion au réseau local* :
  Statut du média. . . . . : Média déconnecté
  Suffixe DNS propre à la connexion. . . . . : 
  Description. . . . . : Microsoft Teredo Tunneling Adapter
  Adresse physique . . . . . : 00-00-00-00-00-00-E0
  DHCP activé. . . . . : Non
  Configuration automatique activée. . . . . : Oui

C:\Users\Administrateur>
```

On peut voir que les informations voulues sont les bonnes.

Maintenant il faut vérifier le réglage sur VMWARE du type de connexion avec notre carte Virtuelle.

Aller dans **VM** puis **Settings**



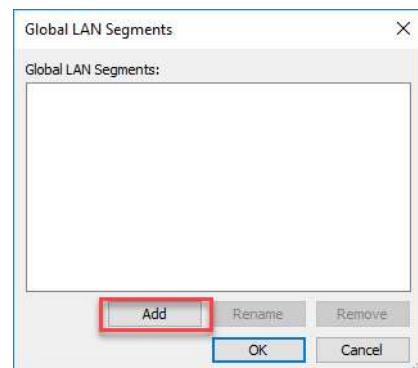
Sélectionner Network Adapter

Device	Summary
Memory	2 GB
Processors	1
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Using file C:\Users\Prof\Downloads\...
Floppy	Auto detect
Network Adapter	LAN Segment

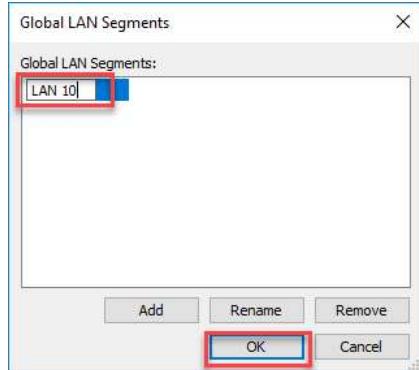
Cocher LAN segment puis cliquer sur LAN Segments.



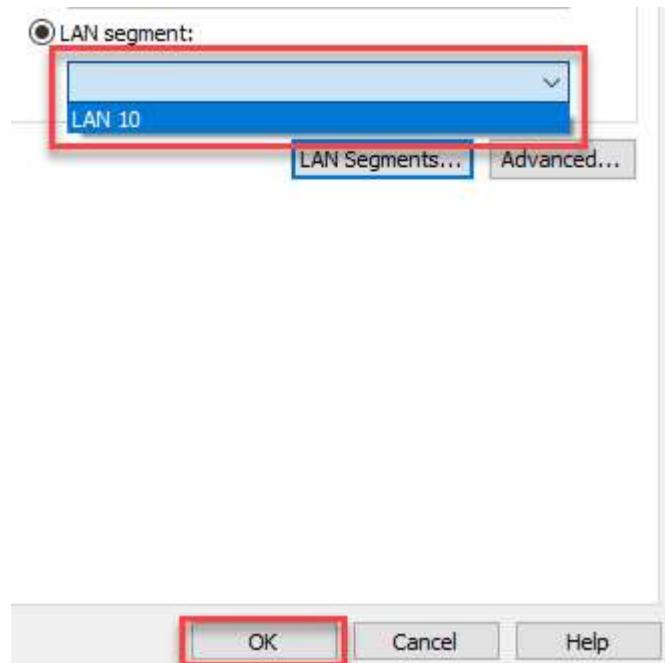
Cliquer Add.



Nommer le LAN Segment en **LAN 10**. Cliquer sur **OK**.



Cliquer sur le menu déroulant **LAN segment** et sélectionner **sur LAN 10** puis cliquer sur **OK**.



Réglage à faire sur le SRV2.

- Création du compte **administrateur** avec le mot de passe « **Respons11** »
- Mettre le nom du serveur.
- Activer une règle permettant de laisser passer les requêtes de **PING ICMP**.
- Régler la carte réseau sur le **LAN SEGMENT 10**.
- Régler l'IP du la carte réseau.
- Rajouter une seconde carte réseau et la régler sur le **LAN SEGMENT 192.168.1**
- Régler l'IP de la seconde carte réseau.
- Ajouter une troisième carte réseau et la régler sur **NAT**.

Reprenez le mode opératoire du serveur 1 en changeant le nom en SRV2.

Les adresses IP seront les suivants :

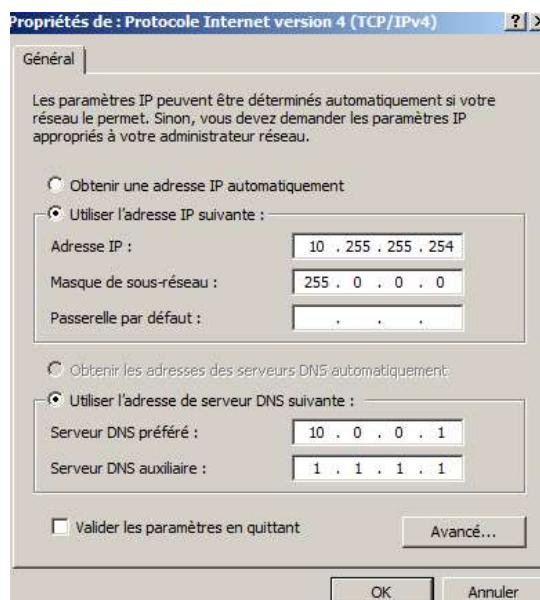
LAN10 : 10.255.255.254

LAN192.168.1 192.168.1.254

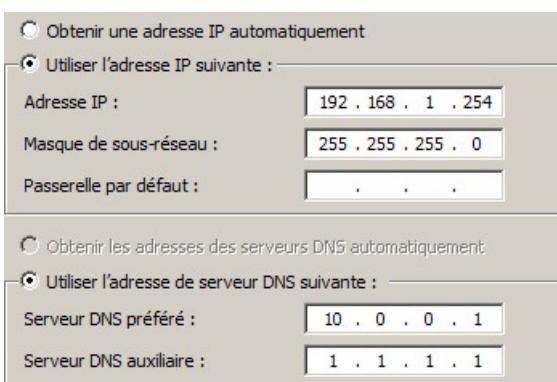
NAT 172.16.255.253

Ce qui doit nous donner ceci :

LAN 10 :



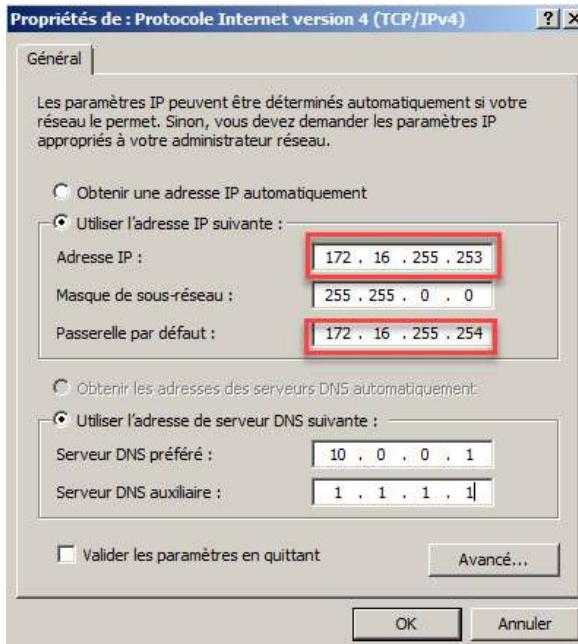
LAN192.168.1



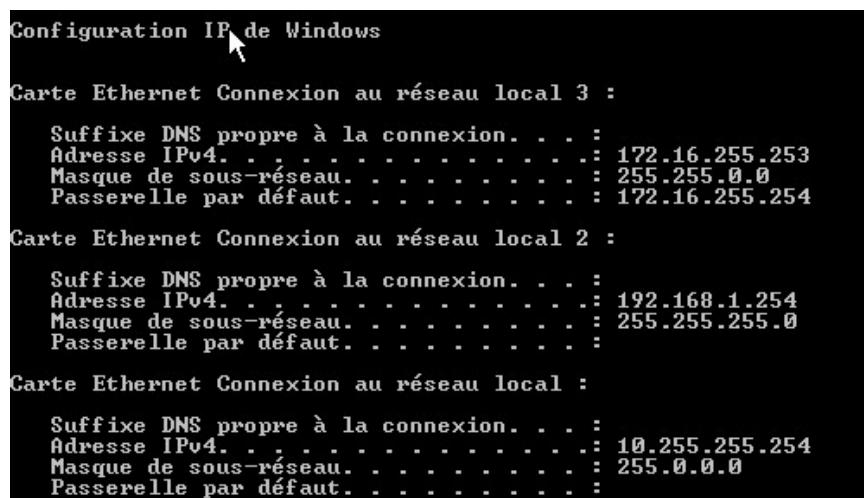
NAT

Memory	2 GB
Processors	1
Hard Disk (SCSI)	80 GB
CD/DVD (IDE)	Using file C:\Users\Prof\Downloads\...
Floppy	Auto detect
Network Adapter	LAN Segment
Network Adapter 2	LAN Segment
Network Adapter 3	NAT
USB Controller	Present
Sound Card	Auto detect
Printer	Present
Display	Auto detect

Attention à bien suivre les informations ci-dessous.

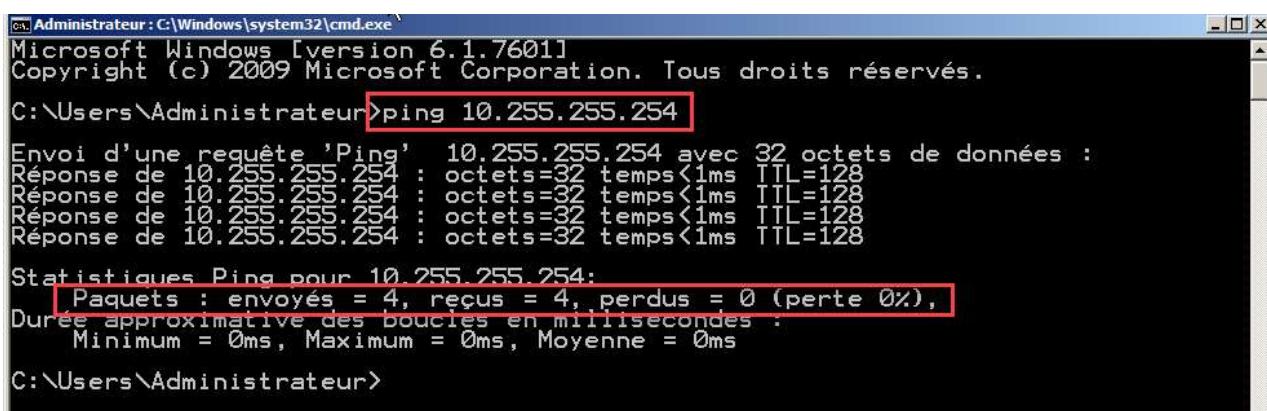


Voilà après la commande ipconfig ce que nous devrions avoir.



Une fois les 3 interfaces de crées, nous allons tester la communication du SRV1 vers SRV2.

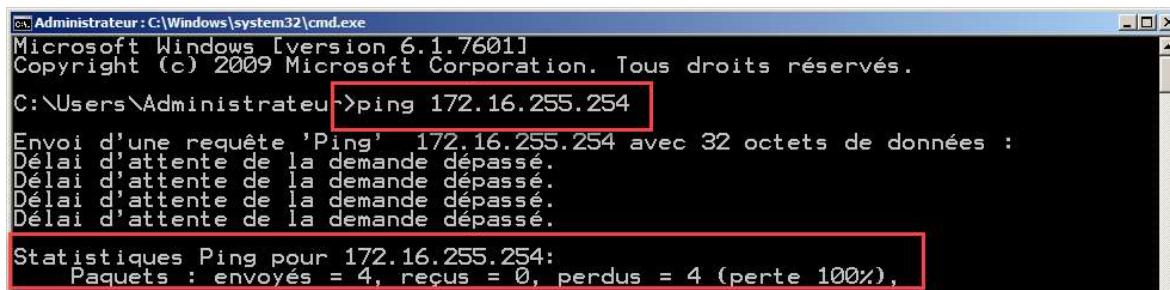
Aller sur la machine SRV1. Ouvrez l'invite de commande. Taper la commande ping 10.255.255.254. Cela permet de tester la connectivité vers cette adresse IP.



Si le paquet est reçus, c'est que nous pouvons joindre cette carte réseau et recevoir le retour. En cas d'erreur vérifier le pare-feu, les LANS segments, les IP.

Faisons le test sur les autres interfaces :

172.16.255.254



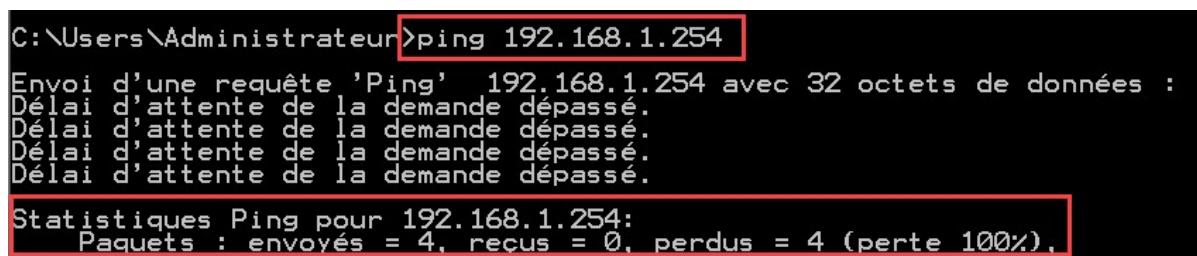
```
c:\Administrator : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\Administrateur>ping 172.16.255.254

Envoi d'une requête 'Ping' à 172.16.255.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.

Statistiques Ping pour 172.16.255.254:
Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

192.168.1.254



```
C:\Users\Administrateur>ping 192.168.1.254

Envoi d'une requête 'Ping' à 192.168.1.254 avec 32 octets de données :
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.1.254:
Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%).
```

Les deux autres interfaces ne répondent pas à la requête de ping.

La question est pourquoi ?

Si on regarde l'adresse réseau des deux autres interfaces, on peut constater qu'elles ne sont pas sur le même segment que le Serveur 1.

Par défaut un message ne peut être envoyé que dans un même réseau logique. Pour permettre d'envoyer un message dans un autre réseau, il faut utiliser le routage. Pour faire du routage, il est nécessaire d'avoir un routeur qui est équipement de la couche 3 du modèle OSI. Son rôle va être d'aiguiller et relayer les paquets entre les différents réseaux au(x) bon(s) destinataire(s). Pour pouvoir communiquer avec un routeur il faut une passerelle par défaut renseigner dans les machines émettrices et de destination. Cette passerelle permettra d'accéder à la table de routage du routeur.

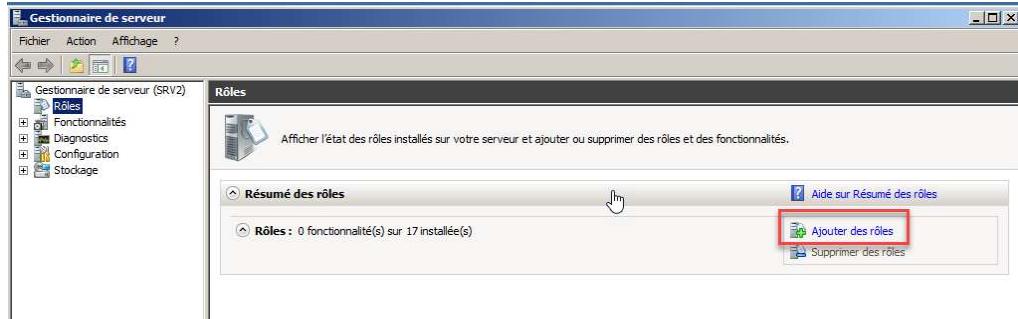
Elle permet de définir les réseaux connectés sur différentes cartes réseaux du routeur, ainsi que le protocole de routage utilisé pour l'acheminement des paquets et sa métrique.

La machine émettrice aura besoin de son adresse IP et MAC et de l'adresse IP de destination.

Voici comment mettre en place un routeur sur un Windows Serveur.

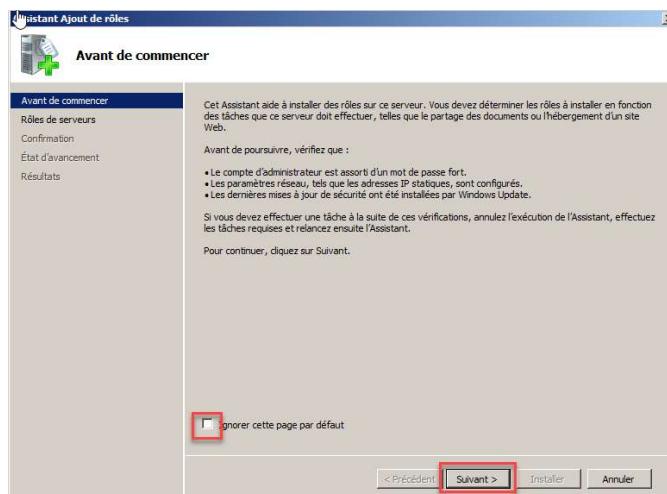
Il faut aller sur le SRV2.

Aller dans le **Gestionnaire de Serveur**, puis dans **Rôles** et cliquer sur **Ajouter des rôles**.

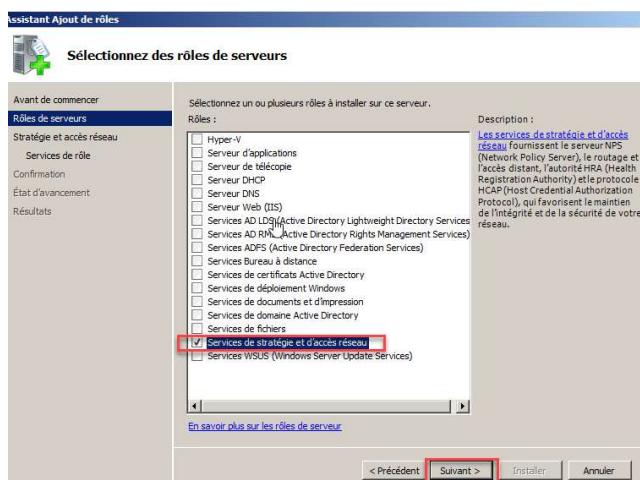


Avant l'installation de tout rôle il faut que le serveur soit en IP Fixe, les mises à jours de sécurité soient installées (production), et que le serveur possède un mot de passe fort. **Respons11** correspond à cette politique de mot de passe fort.

Vous pouvez cocher **Ignorer cette page par défaut** et cliquer sur **Suivant**.



Cocher **Services de stratégie et d'accès réseau** puis cliquer sur **Suivant**. Attention ce rôle est nommé **Accès a distance** depuis Windows Serveur 2012.



La prochaine fenêtre est l'introduction aux **services de stratégie et d'accès réseau**. Cliquer sur **Suivant**.

Ensuite cocher Routage.



Un pop-up apparaît pour vous notifyez des dépendances nécessaires aux fonctionnements du rôle de routage. Cliquer sur **Ajouter les services de rôle requis**. Puis cliquer sur **Suivant** et enfin **Installer**.

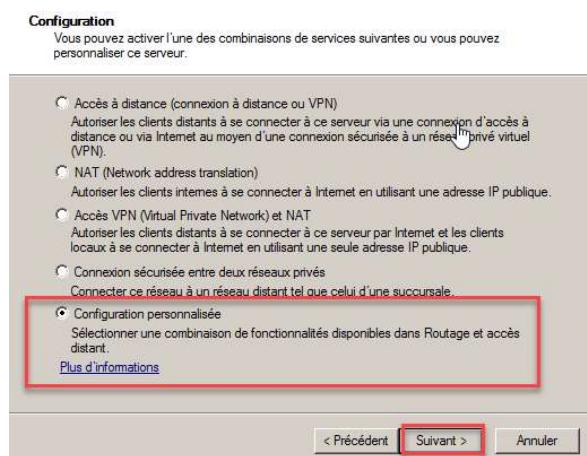


Lancer maintenant la console de **Routage et accès distant**. Cliquer sur **Démarrer** puis **Outils d'administration** et enfin **Routage et accès distant**.

Cliquer droit sur **SRV2 (local)**, puis clique gauche sur **Configurer et activer le routage et l'accès à distance**.

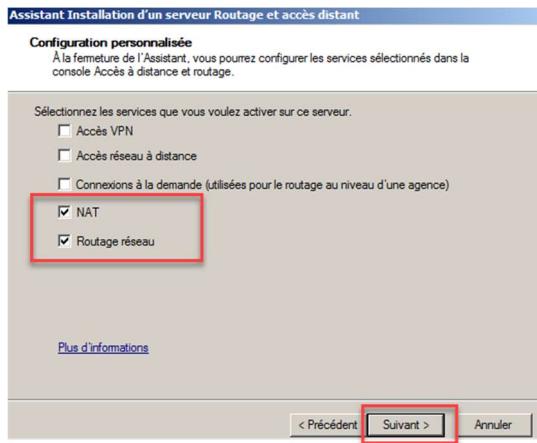


Cliquer sur **Suivant** pour accéder au paramétrage du routage. Cocher **Configuration personnalisée** et cliquer sur **Suivant**.



Nous allons faire une pierre deux coups, nous allons mettre un routeur en place pour connecter les réseaux 10 et 192.168.1 ensemble et en même temps définir la carte NAT 172.16.255.253 en temps que passerelle NAT. Cette passerelle nous permettra de fournir l'accès externe Internet aux deux autres réseaux.

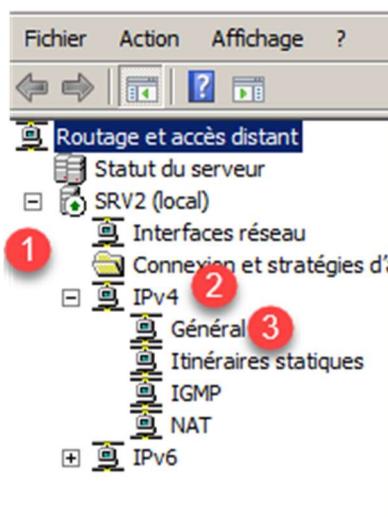
Cocher **NAT** et **Routage réseau**, puis cliquer sur **Suivant** et **Terminer**.



Cliquer sur **Démarrer le service**.



Une fois dans la console de gestion de routage et accès distant. Faites un clic sur la croix à gauche de **SRV2(local)**. Un menu se déroule, cliquer à gauche sur **IPv4**, et enfin sur général.



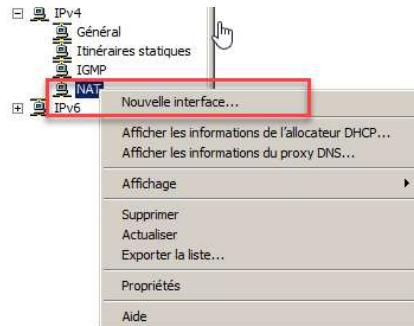
Voici l'information concernant les interfaces du routeur.

Général								
Interface	Type	Adresse IP	Octets entrants	Octets sortants	Filtres statiques	État d'administration	État opérationnel	
Interne	Interne	Non disponible	-	-	Désactivé	Inconnu	Non opérationnel	
Connexion au réseau local 3	Dédiée	172.16.255.253	158 413	23 345	Désactivé	Monter	Opérationnel	
Connexion au réseau local 2	Dédiée	192.168.1.254	0	20 736	Désactivé	Monter	Opérationnel	
Connexion au réseau local	Dédiée	10.255.255.254	42 114	24 544	Désactivé	Monter	Opérationnel	
Bouclage	Bouclage	127.0.0.1	0	0	Désactivé	Monter	Opérationnel	

C'est une table dynamique, il n'y a pas besoin de créer des routes statiques.

Pour la translation NAT, il faut définir une interface.

Clic droit sur **NAT**, puis **Nouvelle interface**.



Sélectionner l'interface **Connexion au réseau local 3**, cliquer sur **OK**. Nous avions défini sur notre maquette que le NAT serait sur la carte ayant l'IP 172.16.255.253.

Cocher **Interface sur Interface publique connectée à Internet**. Cocher **Activer NAT sur cette interface**. En Effet notre serveur est connecté directement Internet. Cliquer sur **OK** pour finir.

Retour sur le SRV1 pour mettre en place le test.

Refaire les tests de ping vers l'interface 192.168.1.254 et le serveur Dns Google [8.8.8.8].

```

C:\Users\Administrateur>ping 192.168.1.254
Envoi d'une requête 'Ping' 192.168.1.254 avec 32 octets de données
Réponse de 192.168.1.254 : octets=32 temps<1ms TTL=127
Statistiques Ping pour 192.168.1.254:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
C:\Users\Administrateur>ping 8.8.8.8
Envoi d'une requête 'Ping' 8.8.8.8 avec 32 octets de données
Réponse de 8.8.8.8 : octets=32 temps=5 ms TTL=128
Statistiques Ping pour 8.8.8.8:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 5ms, Maximum = 5ms, Moyenne = 5ms

```

test de connectivité vers l'interface 192.168.1.254

test de connectivité vers le serveur de google 8.8.8.8

DNS

Définition :

Le Domain Name System, généralement abrégé DNS, qu'on peut traduire en « système de noms de domaine », est un service permettant d'établir une correspondance entre un nom de domaine et une adresse. Il s'agit donc d'un système essentiel pour la navigation sur internet. On devrait saisir les adresses IP à longueur de temps et les connaître par cœur. Le DNS à un peu le rôle d'un répertoire téléphonique, pour trouver un contact on utilise généralement le nom de la personne et non son numéro pour trouver son nom. Cela reviendra à retenir tous les numéros par cœur et savoir à qui correspond le numéro mais de tête. Le système DNS simplifie tout ce processus. Il permet aussi la résolution inverse avec l'IP on peut trouver le domaine lié à cette IP.

Le système DNS a vu le jour avec l'explosion d'utilisation du réseau ARPANET pour faciliter la mise en réseau des ressources partagées.

En effet il existe une table de conversion local, mais il faut faire la mise à jour manuellement sur tous les postes du réseau. C'est le fichier Hosts de Windows. Ce fichier associe sur chaque ligne une adresse IP et le nom d'hôte de l'ordinateur.

Introduction au DNS

Ce système propose :

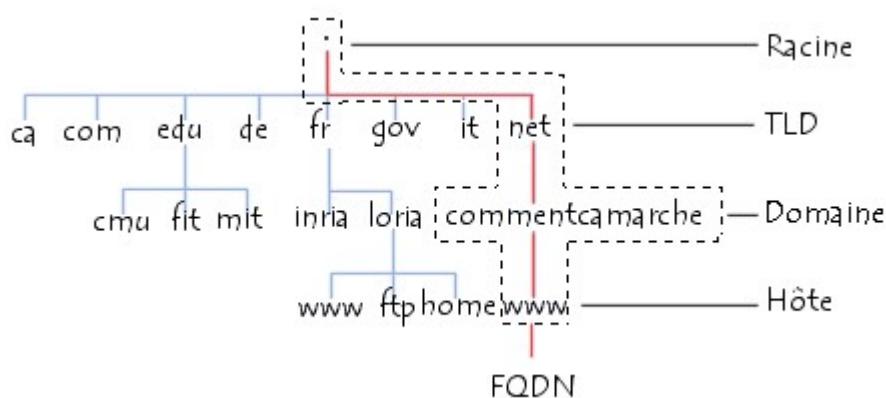
Un espace de noms hiérarchique permettant de garantir l'unicité d'un nom dans une structure arborescente, à la manière des systèmes de fichier Unix.

Un système de serveurs distribués permettant de rendre disponible l'espace de noms.

Un système de clients permettant de « résoudre » les noms de domaines, c'est-à-dire interroger les serveurs afin de connaître l'adresse IP correspondant à un nom.

L'espace de noms :

La structure du système DNS s'appuie sur une structure arborescente dans laquelle sont définis des domaines de niveau supérieurs (appelés TLD, pour Top Level Domains), rattachés à un nœud racine représenté par un point.



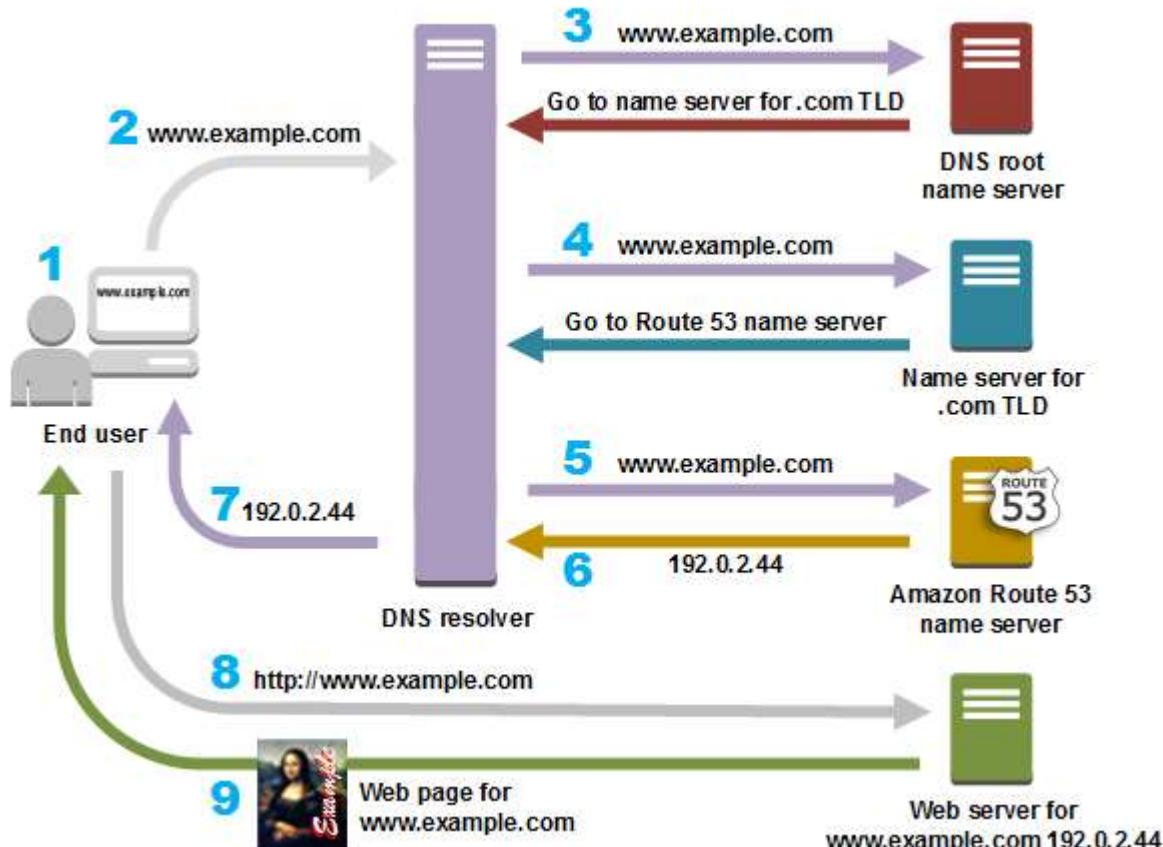
Le Dns racine est le niveau le plus haut dans la structure hiérarchique

Notions de base d'un DNS

Tous les ordinateurs sur Internet, depuis votre smartphone ou ordinateur portable jusqu'aux serveurs qui proposent du contenu aux plus grandes boutiques en ligne, communiquent entre eux à l'aide de numéros. Ces numéros sont appelés adresses IP. Lorsque vous ouvrez un navigateur et accédez à un site web, vous n'avez pas à mémoriser et à saisir de long numéro. Il vous suffit simplement d'entrer un nom de domaine comme exemple.com pour arriver au bon endroit.

Un service DNS comme Amazon Route 53 est un service distribué dans le monde entier qui traduit des noms lisibles par l'homme, comme www.exemple.com, en adresses IP au format numérique de type 192.0.2.1 que les ordinateurs utilisent

pour s'interconnecter. Le système DNS d'Internet fonctionne comme un annuaire téléphonique en gérant le mappage entre les noms et les nombres. Les serveurs DNS traduisent des demandes de noms en adresses IP, en contrôlant à quel serveur un utilisateur final va se connecter quand il saisit un nom de domaine dans son navigateur. Ces demandes sont appelées requêtes.



1. Un utilisateur ouvre un navigateur web, saisit **www.example.com** dans la barre d'adresse et appuie sur Entrée.
2. La demande pour **www.example.com** est acheminée vers un résolveur DNS, qui est généralement géré par le fournisseur d'accès à Internet (FAI) de l'utilisateur, par exemple, un fournisseur d'accès à Internet par câble, un fournisseur d'accès DSL à large bande ou un réseau d'entreprise.
3. Le résolveur DNS du FAI transmet la demande pour **www.example.com** à un serveur de noms racine DNS.
4. Le résolveur DNS du fournisseur d'accès à Internet transmet, à nouveau, la demande pour **www.example.com**, mais cette fois-ci, aux serveurs de noms TLD pour les domaines **.com**. Le serveur de noms de domaines **.com** répond à la demande avec les noms des quatre serveurs de noms Amazon Route 53 qui sont associés au domaine **example.com**.
5. Le résolveur DNS du fournisseur d'accès à Internet choisit un serveur de noms Amazon Route 53 et transmet la demande pour **www.example.com** à ce serveur de noms.
6. Le serveur de noms Amazon Route 53 recherche l'enregistrement **www.example.com** dans la zone hébergée **example.com**. Il obtient la valeur associée, par exemple l'adresse IP d'un serveur web, **192.0.2.44**, puis il renvoie l'adresse IP au résolveur DNS.
7. Enfin, le résolveur DNS du fournisseur d'accès à Internet possède l'adresse IP dont l'utilisateur a besoin. Le résolveur renvoie cette valeur au navigateur web. Le résolveur DNS met également en cache (stocke) l'adresse IP de **example.com** pendant un laps de temps défini, afin qu'il puisse répondre plus rapidement lors du prochain accès à **example.com**. Pour en savoir plus, consultez la page dédiée au paramètre Durée de vie (TTL).
8. Le navigateur web envoie une demande pour **www.example.com** à l'adresse IP figurant dans le résolveur DNS. C'est là que se trouve votre contenu, par exemple, sur un serveur web s'exécutant sur une instance Amazon EC2 ou sur un compartiment Amazon S3 configuré comme un point de terminaison de site web.

9. Le serveur web ou une autre ressource à l'adresse 192.0.2.44 retourne la page web de www.example.com vers le navigateur web, et celui-ci affiche la page.

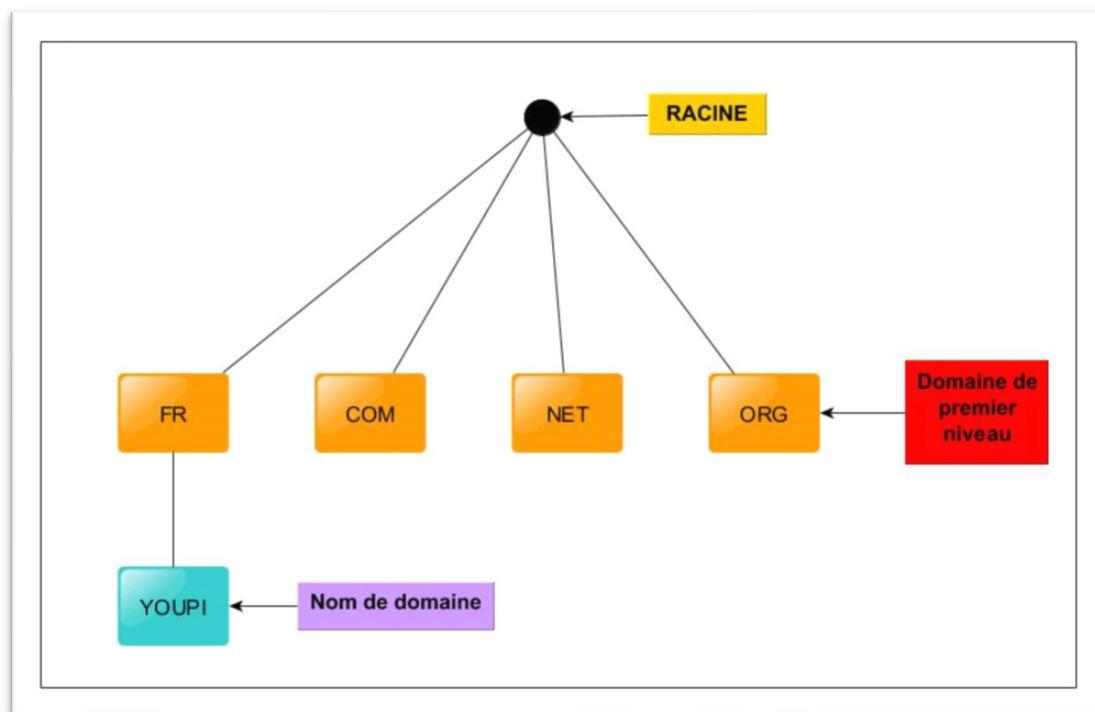
Base de données distribuée.

DNS est construit sur un système hiérarchique. Les serveurs situés en haut de la hiérarchie, appelés serveurs racine sont représentés par un point. Ils permettent la redirection des requêtes vers les serveurs DNS de premier niveau (org, net, fr, com – TLD).

Situés en dessous des serveurs racines, les serveurs ayant autorité sur les domaines de premier niveau permettent la gestion des zones fr, net... Chacun de ces domaines est géré par un organisme (AFNIC...)

Au second niveau se trouvent les noms de domaine qui sont réservées par les entreprises ou des particuliers. Ces noms de domaine sont réservés chez un fournisseur d'accès, qui peut également héberger un serveur web ou tout simplement fournir un nom de domaine.

Chaque niveau est composé de serveur DNS différents qui ont chacun autorité sur leur zone. Il est possible pour une entreprise ou un particulier de rajouter des enregistrements ou des sous-domaines pour le nom de domaine qu'il a réservé (mail.youpi.fr qui me permet de transférer tout mon trafic mail vers mon routeur, plus précisément à destination de mon IP Public)



Chaque serveur DNS ne peut résoudre que les enregistrements de sa zone, le serveur de la zone FR, peut résoudre l'enregistrement youpi, mais il ne sait pas résoudre le nom de domaine test.youpi.fr.

Requêtes itératives et récursives

Lors de la tentative de résolution d'un nom, le serveur DNS peut utiliser deux types de requêtes pour tenter d'effectuer une résolution pour des noms qui ne sont pas présents dans sa base de données.

Requêtes itératives :

Le poste client envoie à son serveur DNS une requête afin de résoudre le nom www.youpir.fr. Le serveur interroge le serveur racine. Ce dernier le redirige vers le serveur ayant autorité sur la zone FR. L'interrogation de ce dernier permet de connaître l'adresse IP du serveur DNS ayant autorité sur la zone youpi. L'interrogation du serveur DNS ayant autorité sur la zone youpi permet la résolution du nom www.youpir.fr. Le serveur DNS internet répond à la demande qu'il a reçue au préalable de son client.

Requêtes récursives :

Le poste client souhaite résoudre le nom www.youpi.fr. Il envoie la demande à son serveur DNS. N'ayant pas autorité sur la zone youpi.fr, le serveur a besoin d'un serveur externe pour effectuer la résolution. La demande est donc transmise au redirecteur configuré par l'administrateur (le serveur DNS du FAIT qui possède un cache plus important par exemple.) Si la réponse n'est pas contenue dans son cache, le serveur DNS du FAI effectue une requête itérative puis transmet la réponse au serveur qui lui a transmis la demande. Ce dernier peut donc maintenant répondre à son client.

Zones et serveurs DNS :

Une zone DNS est une portion d'un nom de domaine dont le responsable est le serveur DNS. On dit qu'il a autorité sur la zone. Ce dernier gère la zone ainsi que les différents enregistrements dont elle dispose.

Les différents types de zone :

Il est possible de créer dans un serveur DNS trois types de zones :

- une zone principale
- une zone secondaire
- une zone stub

La zone principale possède des droits de lecture et d'écriture sur l'ensemble des enregistrements qu'elle contient. Ce type de zone peut être intégré à Active Directory ou simplement contenu dans un fichier texte. Dans le cas où la zone n'est pas intégrée à l'annuaire Active Directory, il est nécessaire de configurer le transfert de zone.

La zone secondaire est une copie d'une zone principale. L'écriture sur ce type de zone est impossible, seule la lecture est autorisée. Il est impossible de l'intégrer à Active Directory, un transfert de zone est donc obligatoire.

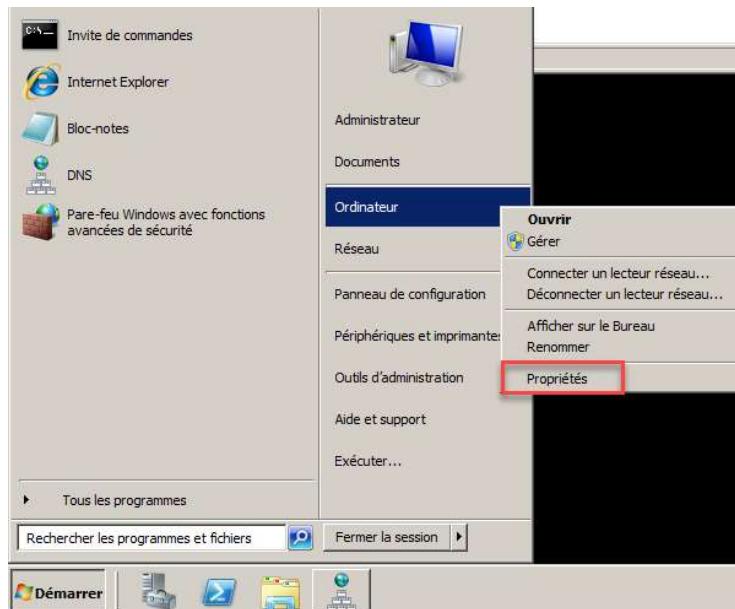
La zone stub est une copie d'une zone, néanmoins cette dernière contient uniquement les informations nécessaires à l'identification du serveur DNS qui a autorité sur la zone qu'il vient d'être rajoutée

Configuration des prérequis pour l'installation d'un serveur DNS

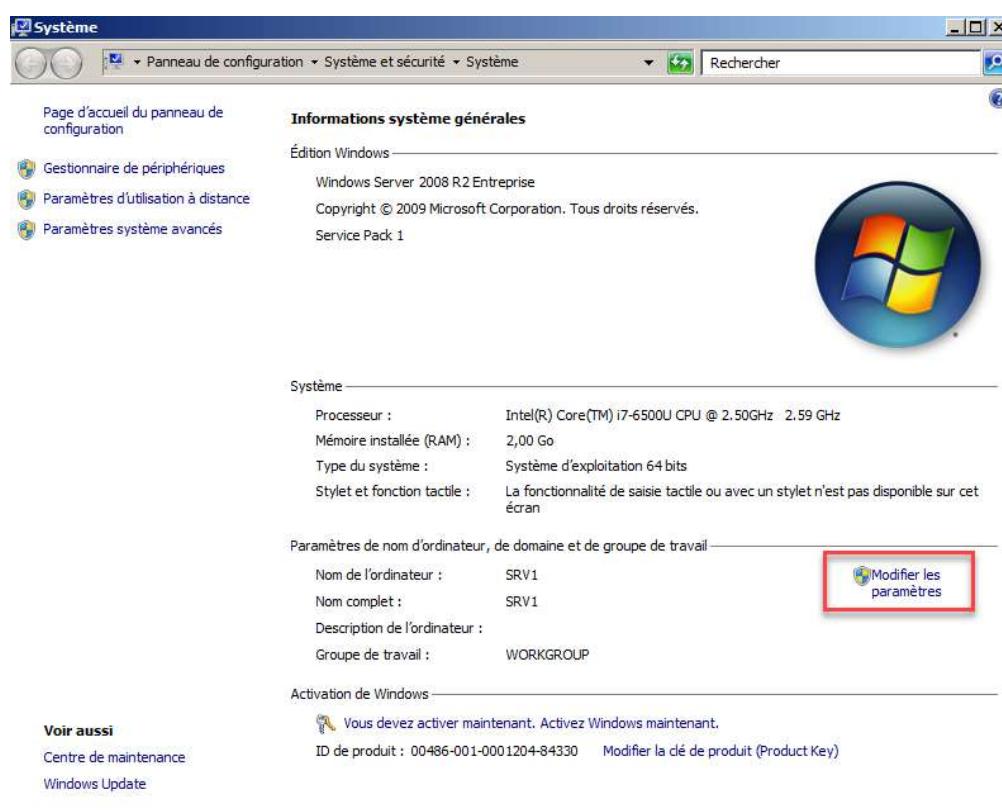
Pour que notre DNS soit fonctionnel, il nous faut lui indiquer le nom de la zone DNS qu'il va devoir héberger et l'adresse IP pour trouver cette base de données.

Pour ce faire il faut lui indiquer le suffixe DNS pour déclarer la zone DNS dans laquelle le serveur va appartenir.

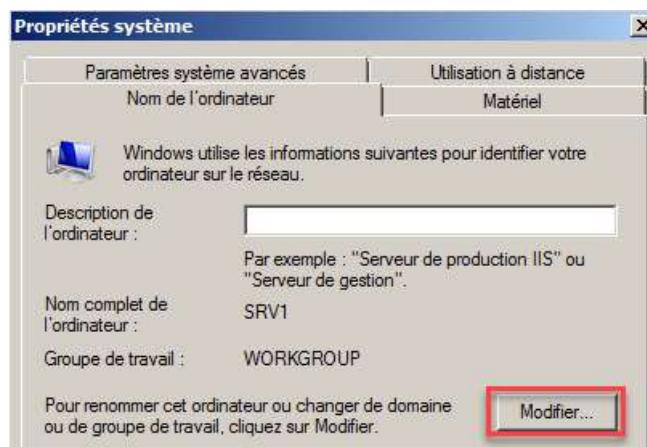
Faites un clic droit sur **Ordinateurs** puis un clic simple sur **Propriétés**.



Ensuite cliquer sur **Modifier les paramètres** qui se trouve à droite du nom de votre Serveur.



Ensuite cliquer sur **Modifier**.

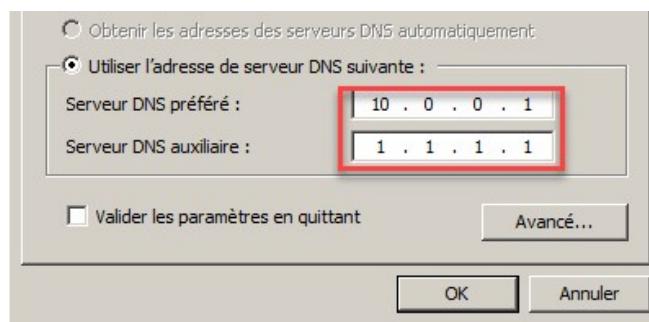


Puis cliquer sur **Autres**.



Nous utiliserons le suffixe **formation.local**. Une fois validé, l'ordinateur va devoir démarrer pour application la modification.

Une fois redémarrer, aller dans la configuration d'adressage IP du serveur. Vérifier que les adresses IP 10.0.0.1 et 1.1.1.1 aient été bien modifier précédemment.



Installation du rôle DNS sur le Serveur 1

Aller sur SRV1, ouvrir le **gestionnaire de serveur**, puis **Rôles, Ajouter des rôles**.

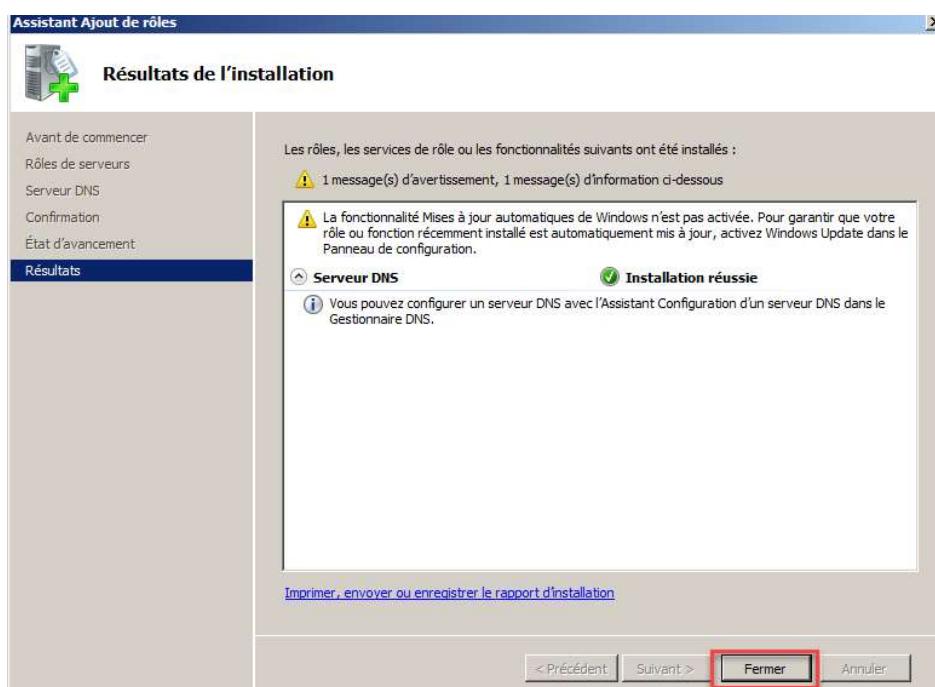


Cocher **Serveur DNS**, puis cliquer sur **Suivant**.



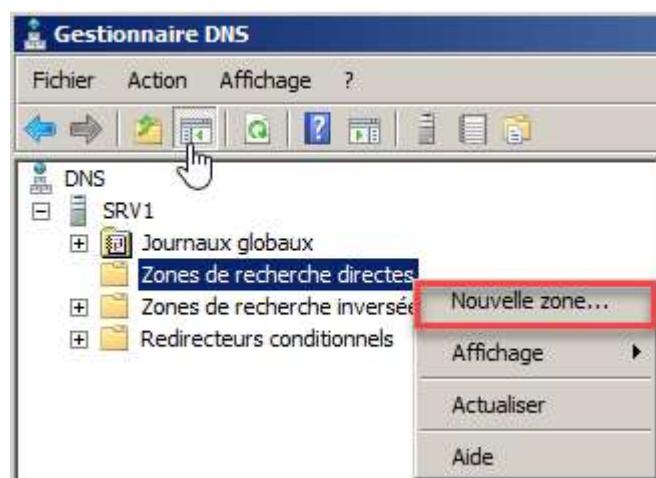
Cliquer à nouveau sur **Suivant**, puis **Installer** pour valider l'installation du rôle.

Une fois l'installation terminée cliquer sur **Fermer**.

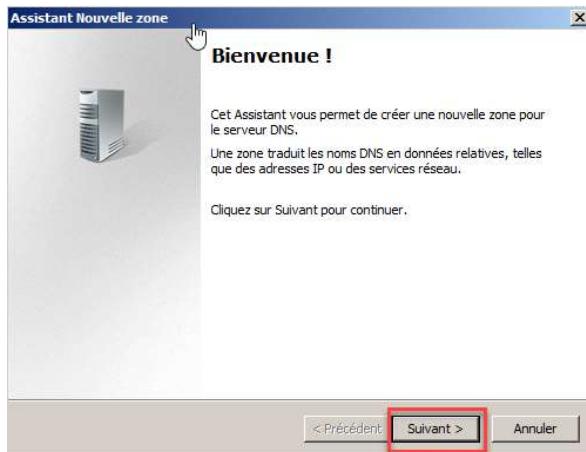


Ouvrir la console de gestion DNS (elle se trouve dans **outils d'administrations** ou dans le **gestionnaire de serveur**.)

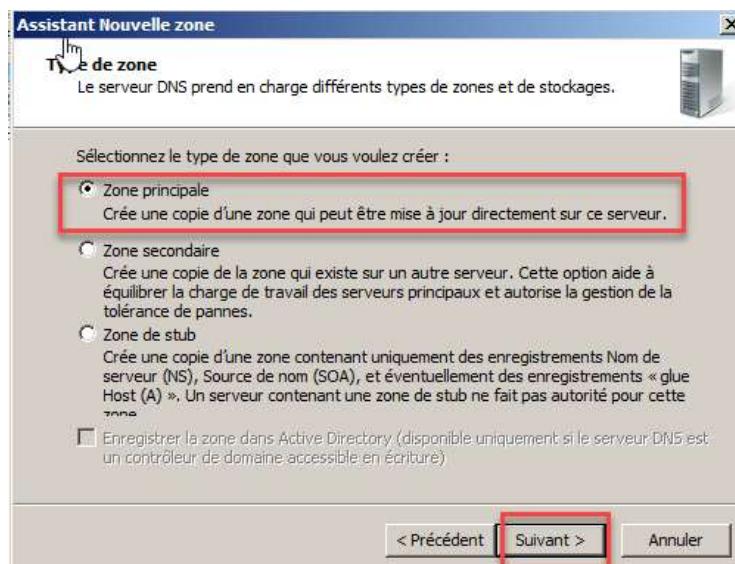
Sélectionner la zone de recherche directe et faites un clic droit **nouvelle zone**.



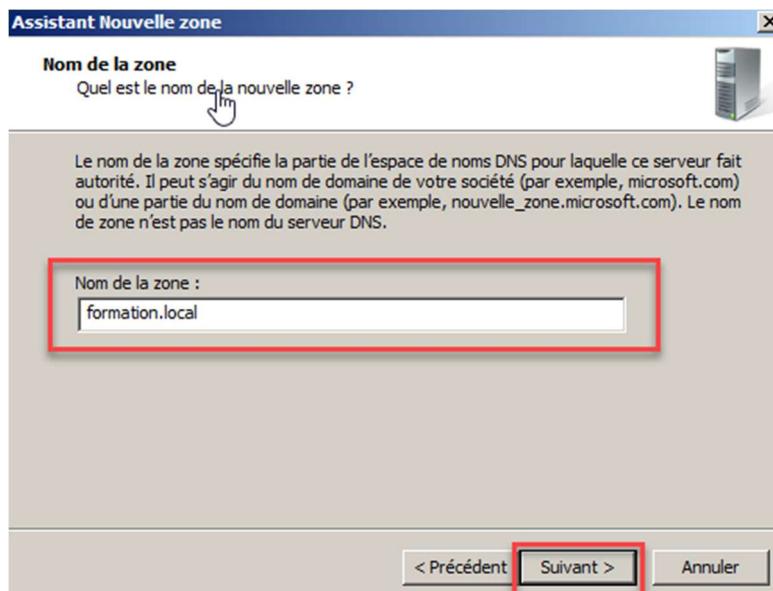
Cliquer sur **Suivant**.



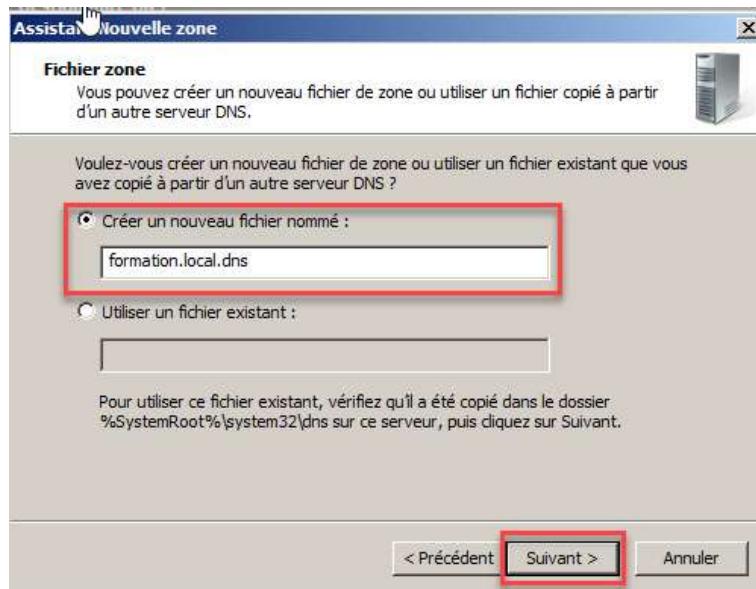
Dans notre cas ce sera la première zone de notre infrastructure, nous laisserons donc cocher **zone principale**. Voir au-dessus pour la différence entre les différents types de zones. Puis cliquer sur **Suivant**.



Renseigner le nom de la zone de recherche principale directe : **formation.local**, puis cliquer sur **Suivant**.



Valider en cliquant sur **Suivant** le nom de fichier d'enregistrement DNS **formation.local.dns**. Il sera stocké dans le répertoire Windows\System32\dns\



Cocher **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées**. Ce type de mise à jour permet à un terminal de remonter très rapidement et automatiquement dans la base de données afin qu'il puisse utiliser le serveur DNS pour résoudre des requêtes. Sans mise à jour dynamique il faudrait créer un enregistrement manuel pour tous les équipements devant utiliser le DNS. Ce serait une perte de temps énorme surtout si les IP sont dynamiques pour ses postes, il faudrait le modifier régulièrement.

Cliquer ensuite sur **Suivant**.

Viens ensuite l'écran permettant d'avoir un récapitulatif avant la validation. Cliquer sur **Terminer**.



Ensuite aller dans la zone de recherche directe **formation.local**.

Vous devriez voir plusieurs enregistrements.

Nom	Type	Détails
(identique au dossier parent)	Source de nom (SOA)	[1], srv1.formation.local., h...
(identique au dossier parent)	Serveur de noms (NS)	srv1.formation.local.
srv1	Hôte (A)	10.0.0.1

Vu notre configuration il nous faut trois enregistrements. Si le dernier srv1 / Hôte (A) / 10.0.0.1 n'apparaît pas, vérifier le suffixe DNS.

Les différents enregistrements DNS pour la zone directe

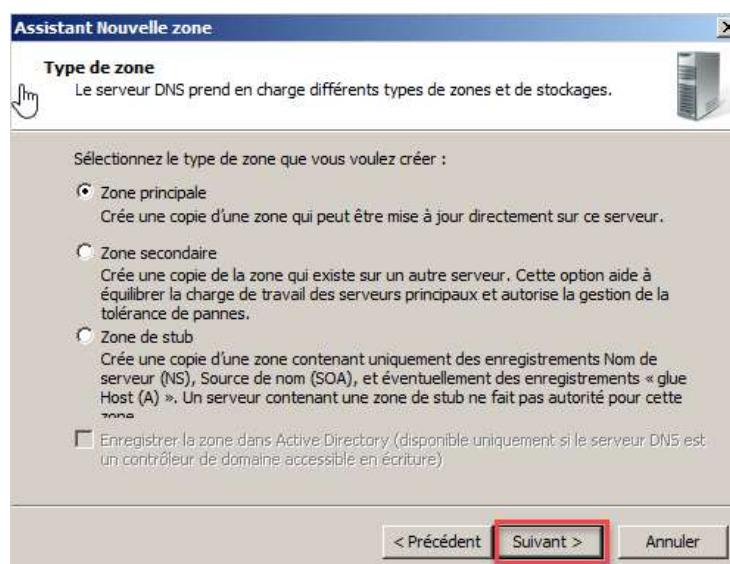
ENREGISTREMENTS	EXPLICATIONS
SOA (Start of Authority)	L'enregistrement donne les informations générales de la zone (serveur principal, courrier de contact, durée d'expiration)
NS (Name Server)	Définit les serveurs de noms du domaine
A [IP V4] AAAA [IP V6] (Address Record)	Permet de faire correspondre un nom de poste en adresse IP v4 ou IP v6 selon le nom de l'enregistrement A / AAAA
CNAME (Canonical Name)	Un alias est créé vers le nom d'un autre poste. Le poste concerné est accessible sur son nom ainsi que sur son alias
MX (Mail Exchange)	Définit les serveurs de courrier pour le domaine.
SRV	Permet de définir un serveur spécifique pour une application, notamment pour la répartition de charge

Nous allons créer une zone indirecte qui permettra de faire de la résolution inverse. Cette fois de l'adresse IP v4 | v6 vers le nom. Cette zone n'est pas essentielle pour le fonctionnement de Active Directory mais elle contribue à faciliter la recherche sur un domaine.

Aller dans la console de gestion DNS puis faites un clic droit sur **Zones de recherche inversée** et un clic simple sur **Nouvelle zone**.



Ensuite cliquer sur **Suivant**, pour passer à l'écran de configuration. Laisser cocher **Zone Principale** et cliquer sur **Suivant**.



Nous laissons cocher **Zone de recherche inversée en IP v4**, vu que nous avons configurer que l'adresse IP v4 au niveau de la carte réseau. Cliquer ensuite sur **Suivant**.

Pour éviter des problèmes, utiliser que la partie Network ID de l'adresse IP.

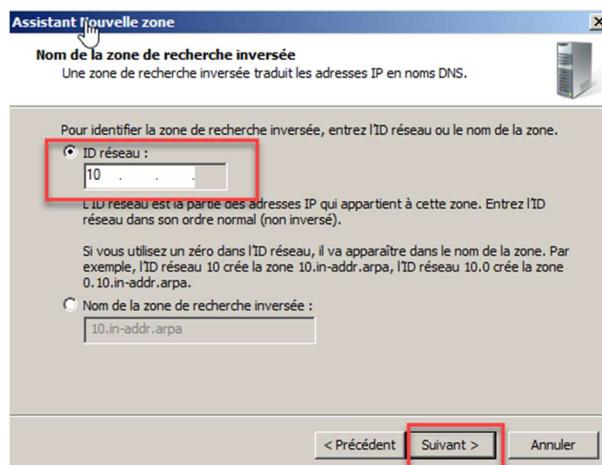
En effet, sur mon adresse IP 10.0.0.1 si je mets 10.0.0 en ID réseau, seul les postes allant de 10.0.0.1 à 10.0.0.254 pourront entrer dans ma base de données DNS, les autres ne pourrons pas l'utiliser.

Or avec mon adresse de classe A je suis sensé pouvoir avoir plus de 16 Millions d'ordinateurs utilisant mon DNS.

10.0.0.1 à 10.255.255.254 soit 2^{24} ordinateur -2 [réseau et broadcast].

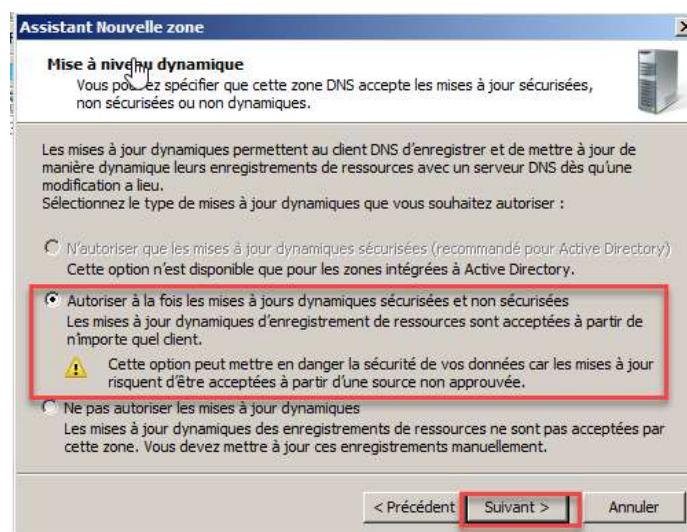
De même que pour une classe B on mettra l'ID Réseau par exemple 172.16 et non 172.16.x.

Et pour finir une classe C on mettra les trois premiers octets qui définissent le réseau, qu'il y est des sous réseaux ou non.



Laisser le nom par défaut du fichier de la zone inversée et cliquer sur **Suivant**.

Pareil que tout à l'heure pour les mises jours dynamiques. Cocher **Autoriser à la fois les mises à jour dynamiques sécurisées et non sécurisées** puis cliquer sur **Suivant** et **Terminer**.



Cette fois nous trouvons que deux enregistrements, un troisième doit être forcer à la main pour apparaître.

Pour forcer sa remonter ouvrir **l'invite de commande** et taper la commande **ipconfig /registerdns**

```

Administrator : C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.
C:\Users\Administrateur>ipconfig /registerdns
Configuration IP de Windows
L'inscription des enregistrements de ressource DNS pour toutes les cartes de
cet ordinateur a été initiée. Toute erreur sera signalée dans l'Observateur
d'événements dans 15 minutes.
C:\Users\Administrateur>_

```

Aller sur la zone de recherche inversée et faites actualiser [F5 par exemple]. Voici le troisième enregistrement. Si vous avez fait une erreur au niveau de l'adresse IP du DNS préferé vous ne le verrai pas remonter.

No	Nom	Type	Données
	(identique au dossier parent)	Source de nom (SOA)	[2], srv1.formation.local., 1
	(identique au dossier parent)	Serveur de noms (NS)	srv1.formation.local.
	10.0.0.1	Pointeur (PTR)	srv1.formation.local.

Les différents enregistrements DNS pour la zone inversée

ENREGISTREMENTS	EXPLICATIONS
SOA (Start of Authority)	L'enregistrement donne les informations générales de la zone (serveur principal, courrier de contact, durée d'expiration)
NS (Name Server)	Définit les serveurs de noms du domaine
PTR [Pointer Record]	Associe une adresse IP à un nom, il est le contraire d'un enregistrement de type A.
CNAME (Canonical Name)	Un alias est créé vers le nom d'un autre poste. Le poste concerné est accessible sur son nom ainsi que sur son alias

FQDN

Full Qualified Domain Name (nom de domaine complètement qualifié) est un nom de domaine qui révèle la position absolue d'un nœud dans l'arborescence DNS en indiquant tous les domaines de niveau supérieur jusqu'à la racine. Par exemple : srv1.formation.local est un FQDN.

Srv1 est le nom NetBIOS du poste. Formation.local est le suffixe DNS. Donc le FQDN est le nom NetBIOS suivi d'un point et du nom de la zone DNS sur laquelle il est enregistré.

La commande NSLOOKUP

Nslookup est une commande qui permet la recherche d'enregistrement dans le DNS. Exécutée par défaut, la console affiche le nom et l'adresse IP du serveur de noms primaire. Il est par la suite possible d'interroger le serveur.

Ouvrir l'invite de commande, et taper NSLOOKUP.

```
C:\Administrator : C:\Windows\system32\cmd.exe - NSLOOKUP  
C:\Users\Administrateur>NSLOOKUP  
Serveur par défaut : srv1.formation.local  
Address: 10.0.0.1  
>
```

cette ligne correspond à l'adresse du NS

L'adresse IP par défaut du serveur qui possède les enregistrement

Vous deviez avoir quelque chose comme ça. Si vous avez **UNKNOW** ou **Timeout** vérifier toute votre configuration DNS.

Test de résolution par le nom :

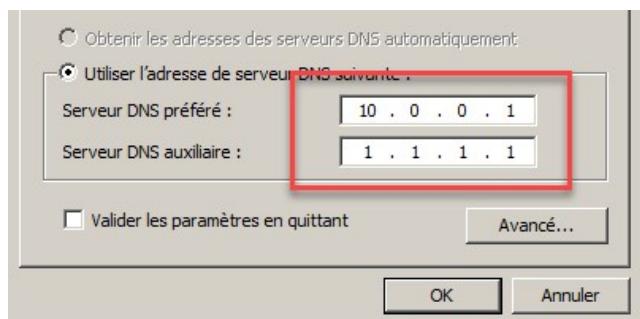
```
srv1  
Serveur : srv1.formation.local  
Address: 10.0.0.1  
Nom : srv1.formation.local  
Address: 10.0.0.1  
> _
```

Test de résolution par l'adresse IP :

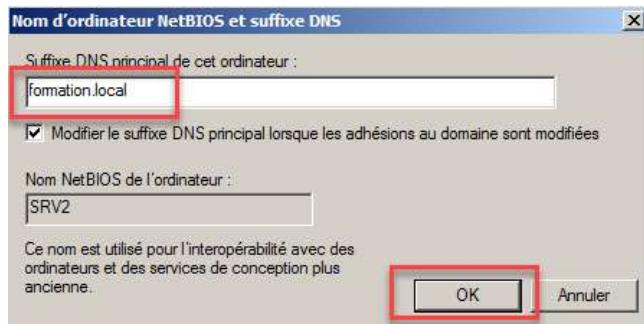
```
> 10.0.0.1  
Serveur : srv1.formation.local  
Address: 10.0.0.1  
Nom : srv1.formation.local  
Address: 10.0.0.1
```

Ajout d'une machine dans la base de données.

Sur le SRV2, vérifier les adresses de serveur DNS sont bien les suivantes :



Ensuite indiquer le suffixe DNS et redémarrer.



Retourner sur le SRV1 pour regarder l'évolution des enregistrements DNS.

Nous constatons trois nouveaux enregistrements dans la zone de recherche directe. Ce sont les trois IP du serveur 2

Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[6], srv1.formation.local., h...
(identique au dossier parent)	Serveur de noms (NS)	srv1.formation.local.
srv1	Hôte (A)	10.0.0.1
SRV2	Hôte (A)	10.255.255.254
SRV2	Hôte (A)	172.16.255.253
SRV2	Hôte (A)	192.168.1.254

Sur la zone de recherche inversée c'est un peu différent. Il n'y a qu'un seul enregistrement pour le SRV2 vu qu'une seule des cartes réseaux appartient à la zone de recherche inversée 10.

Nom	Type	Données
(identique au dossier parent)	Source de nom (SOA)	[3], srv1.formation.local., h...
(identique au dossier parent)	Serveur de noms (NS)	srv1.formation.local.
10.0.0.1	Pointeur (PTR)	srv1.formation.local.
10.255.255.254	Pointeur (PTR)	srv2.formation.local.

```
C:\Users\Administrateur>nslookup
Serveur par défaut : srv1.formation.local
Address: 10.0.0.1
> srv2
Serveur : srv1.formation.local
Address: 10.0.0.1
Nom : srv2.formation.local
Addresses: 10.255.255.254
          172.16.255.253
          192.168.1.254
> 10.255.255.254
Serveur : srv1.formation.local
Address: 10.0.0.1
Nom : srv2.formation.local
Address: 10.255.255.254
> 172.16.255.254
Serveur : srv1.formation.local
Address: 10.0.0.1
*** srv1.formation.local ne parvient pas à trouver 172.16.255.254 : Non-existent
>
```

Voici la réponse de recherche SRV2 dans la zone de recherche directe

Test de la résolution
 10.255.255.254 -> srv2
 172.16.255.254 -> X
 il n'y a pas d'enregistrement dans la zone inversée pour cette ip.

DHCP [DYNAMIC HOST CONFIGURATION PROTOCOL]

Définition

Le serveur DHCP est un protocole important dans une infrastructure réseau. Son rôle est la distribution de configuration IP, permettant aux équipements connectés au réseau de dialoguer entre eux.

Rôle

Le DHCP permet d'automatiser la configuration des interfaces réseaux, sans lui il serait obligatoire de le faire manuellement sur tous les postes du réseau.

Une configuration IP inclut une adresse IP, un masque de sous-réseau et une passerelle et éventuellement d'autres informations comme un suffixe DNS et les adresses des DNS préférés, une durée de bail, l'adresse d'un serveur déploiement et le fichier pour lancer le logiciel de déploiement.

Ce protocole fonctionne avec IPv4 et aussi avec IPv6.

Fonctionnement

Par défaut un ordinateur est équipé d'une carte réseau (filaire ou sans-fil), cette carte possède une adresse physique. On l'appelle l'adresse MAC : Media Access Control. Cette adresse permet d'identifier une machine sur le réseau de façon électrique. Elle est codée sur 48 bits en hexadécimal. Chaque carte possède un numéro unique au monde.

Pour avoir votre adresse MAC, vous avez deux commandes permettant de la trouver.

ipconfig /all mais elle affiche aussi beaucoup d'autres informations réseaux. Le plus simple est d'utiliser **getmac /v** qui est spécifique aux adresses MAC.

```
C:\Users\Administrateur>getmac /v
Nom de la connexio Carte réseau      Adresse physique
=====
Connexion au réseau Connexion réseau 00-0C-29-5E-59-8D
-4031-85C0-DC9D1A8C7901}
```

Voici l'adresse 00 :0C :29 :5E :59 :8D.

```
C:\Users\Administrateur>getmac /v
Nom de la connexio Carte réseau      Adresse physique
=====
Connexion au réseau Connexion réseau 00-0C-29-5E-59-8D
-4031-85C0-DC9D1A8C7901}
```

Diagramme expliquant la structure de l'adresse MAC :

- Le premier bloc (3 octets) indique le fabricant sous forme de numéro et le modèle de la carte réseau.
- Le deuxième bloc indique le numéro de série de cette carte réseau.

L'ordinateur n'ayant pas encore d'adresse IP va envoyer en diffusion **Broadcast** un datagramme (paquet de données) **[DHCP DISCOVER]** qui s'adresse au port 67 de n'importe quel serveur à l'écoute sur ce port. Dans ce datagramme figure par exemple l'adresse physique [MAC] du client.



1 - L'ordinateur n'ayant pas encore d'adresse IP va envoyer en diffusion **Broadcast** un datagramme (paquet de données) **[DHCP DISCOVER]** qui s'adresse au port 67 de n'importe quel serveur à l'écoute sur ce port. Dans ce datagramme figure par exemple l'adresse physique **[MAC]** du client.

2 – Le serveur à reçu ce datagramme, s'il est en mesure de proposer une adresse sur le réseau auquel appartient le client, envoie une offre DHCP **[DHCP OFFER]** à l'attention du client en utilisant le port 68, identifié par son adresse physique. Cette offre comporte l'adresse IP du serveur, ainsi que l'adresse IP et le masque de sous-réseau qu'il propose au client. Un client peut recevoir plusieurs offres si plusieurs serveurs DHCP sont actifs sur le réseau.

3 – Le client retient l'offre la plus rapide qui lui parvient, et diffuse sur le réseau un datagramme de requête DHCP **[DHCP REQUEST]** en **broadcast**. Ce datagramme comporte l'adresse IP du serveur et celle qu'il lui a été proposé. Elle permet de demander au serveur choisi, de valider l'assignation de cette adresse, et ils informent également les autres serveurs que leurs offres n'ont pas été retenue.

4 – Le serveur DHCP envoie un datagramme d'accusé de réception **[DHCP ACK pour ACKNOWLEDGEMENT]** qui assigne au client son adresse IP et son masque de sous-réseau, la durée du bail de cette adresse et éventuellement d'autres paramètres comme l'adresse de la passerelle, ...)

APIPA

Dans le meilleur des cas, le serveur donnera toujours une adresse IP, mais on peut rencontrer une panne sur ce serveur. Dans ce cas l'ordinateur qui démarre, va tenter d'envoyer plusieurs paquets **DISCOVER**. Au bout de trois paquets, il va basculer sur une adresse **APIPA [Automatic Private Internet Protocol Addressing]**. C'est un protocole qui permet à un système d'exploitation de s'attribuer automatiquement une adresse IP, lorsqu'aucun serveur DHCP n'est joignable.

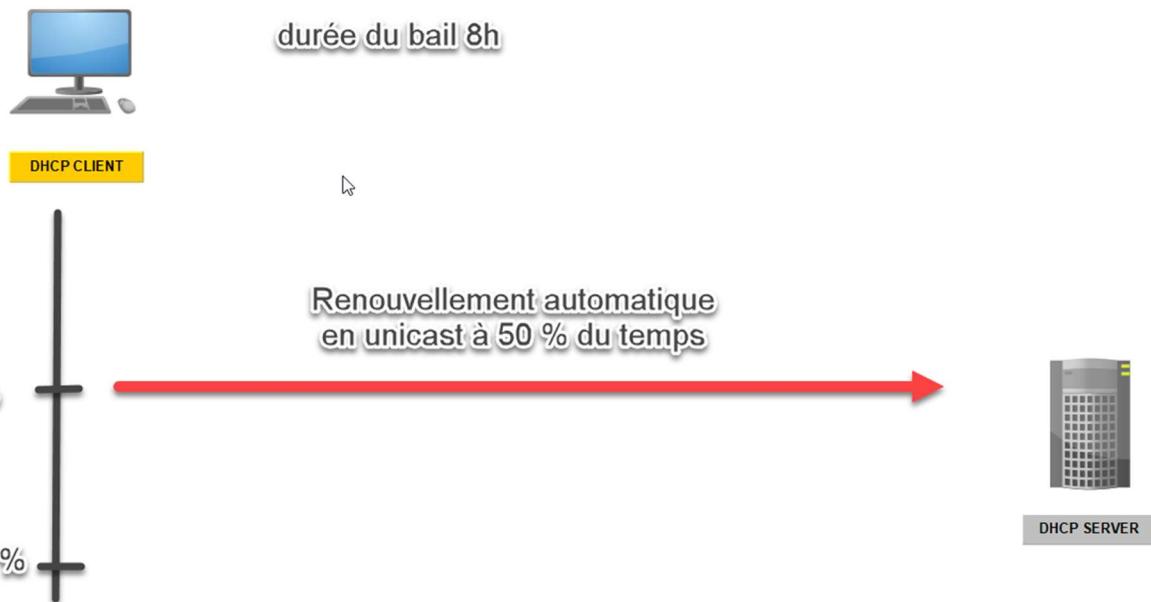
APIPA utilise la plage d'adresse 169.254.0.0 /16 à 169.254.255.255. Cette adresse est une adresse de secours. Elle ne possède pas de passerelle, ni serveur DNS, vous serez isolé sur réseau local.

Le Bail

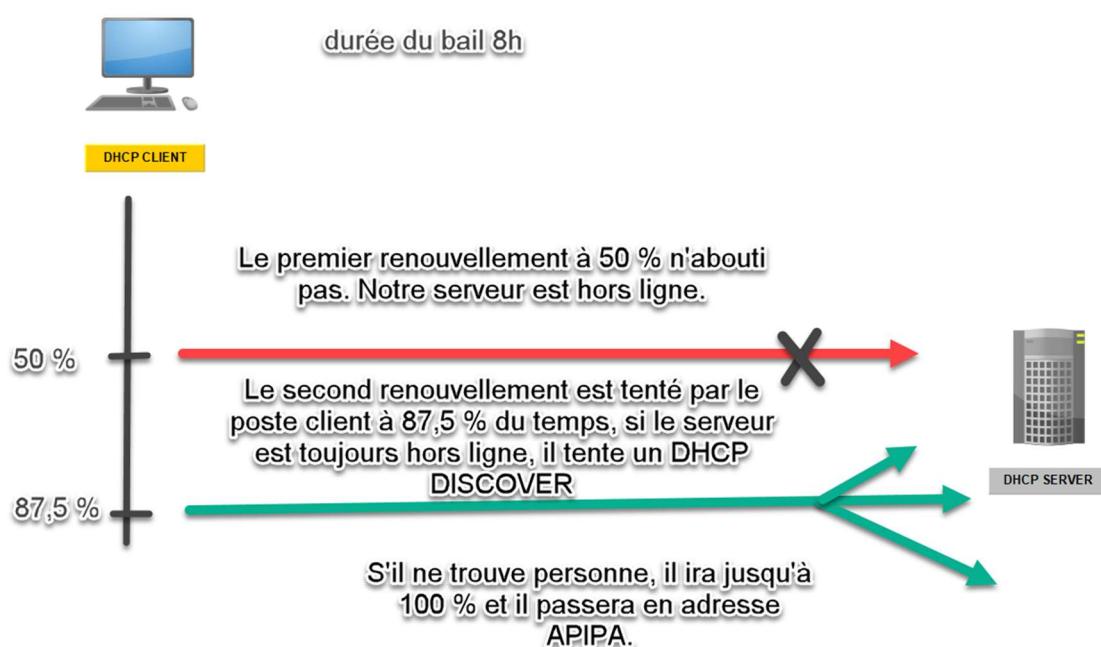
Les adresses IP dynamiques sont fournies pour une durée limitée (durée du bail ou lease time). Elle est transmise dans l'accusé de réception qui clôture la transaction DHCP.

La durée du bail va influer sur la mise à disposition d'adresse plus utilisé par les postes clients. Mais en raccourcissant ce bail, on augmente l'envoi de broadcast sur le réseau pour trouver une adresse.

Renouvellement de bail



En cas de soucis :



Installation

Aller dans le **gestionnaire de serveur** sur le SRV1. Cliquer sur **Rôles**, puis **Ajouter de rôles**.



Cocher ensuite **Serveur DHCP**, puis cliquer sur **Suivant**.

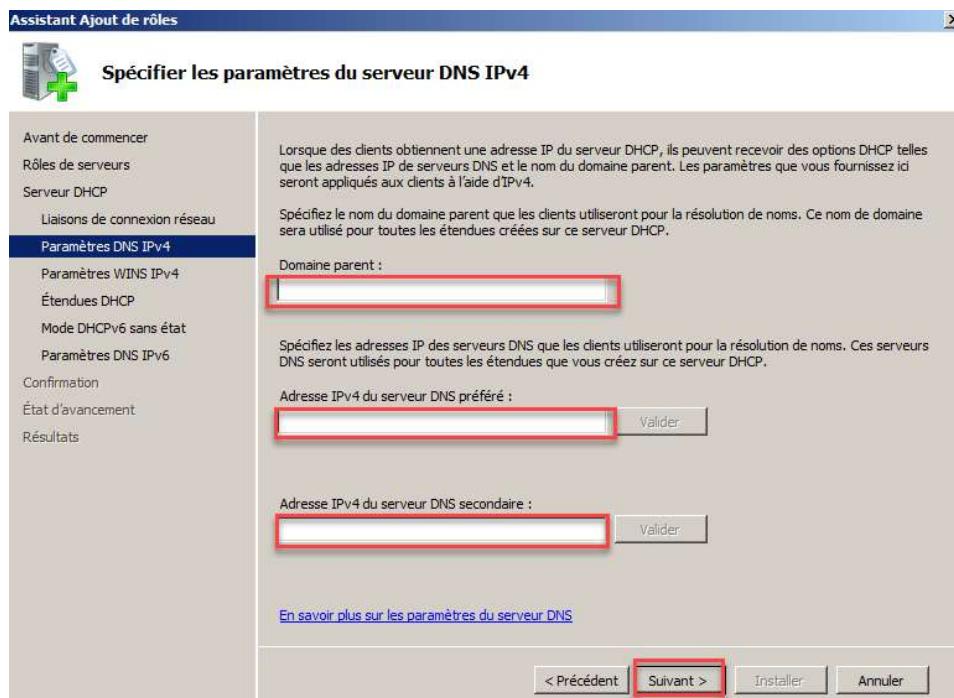


Pour rappel, il faut que votre serveur possède une adresse IP FIXE pour être en capacité d'assigner des adresses dynamiques aux terminaux. Vous devez aussi planifier aussi votre plan d'adressage de votre réseau ou sous réseau.

Cliquer ensuite sur **Suivant**. Sélectionner la carte réseau qui va être utilisé pour traiter les clients DHCP en écoutant le ports 67 et utilisant le port 68 pour lui répondre. Cliquer sur **Suivant**, une fois l'interface sélectionnée.

Vous pouvez spécifiez des paramètres serveurs DNS IP v4 sur votre serveur. Dans le cas où votre serveur doit envoyer des informations sur plusieurs réseaux ou sous-réseaux effacer les informations déjà sélectionnées. Nous le ferons manuellement ensuite. Le risque est que ce paramétrage s'applique sur toutes les étendues DHCP, ce qui peut ne pas correspondre aux infrastructures.

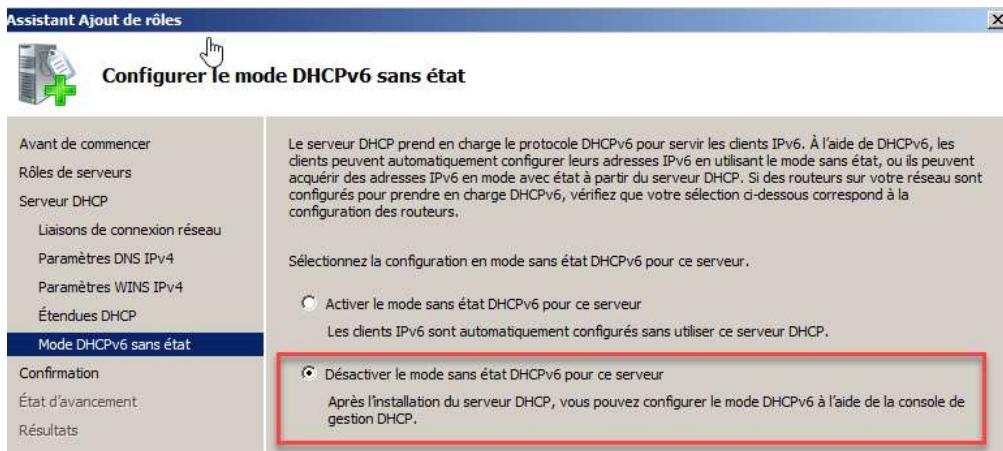
Suivez la capture suivante, et cliquer sur **Suivant**.



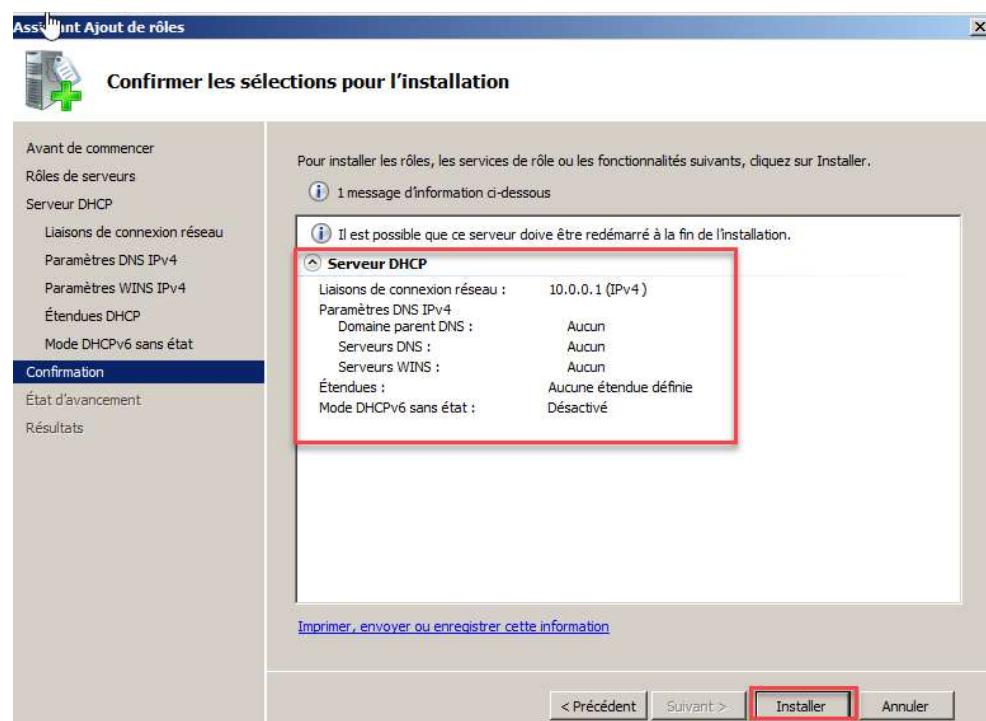
Cocher sur **WINS n'est pas requis pour les applications sur ce réseau**, puis cliquer sur **Suivant**.



Lancer le chant vite pour les **Ajouter ou modifier les étendues DHCP** et cliquer sur **Suivant**.
Décocher le mode sans état DHCPv6 pour ce serveur et cliquer sur **Suivant**.



Cliquer sur **Installer** pour lancer l'installation du rôle et de son paramétrage basique.

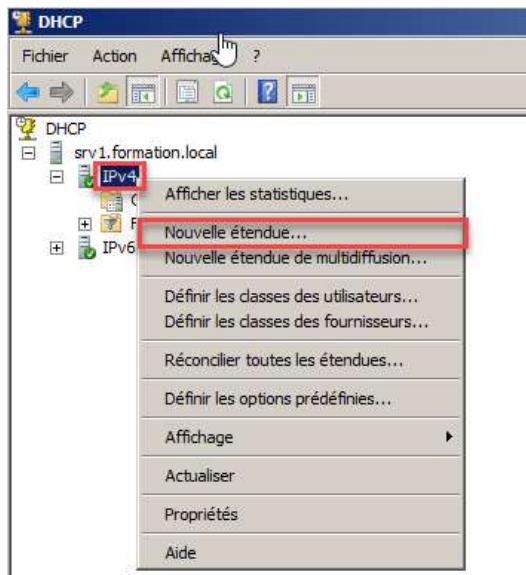


Paramétrage DHCP

Lancer la console de gestion du serveur DHCP. Vous la trouverez dans les **outils d'administration** ou dans le **gestionnaire de serveur**.

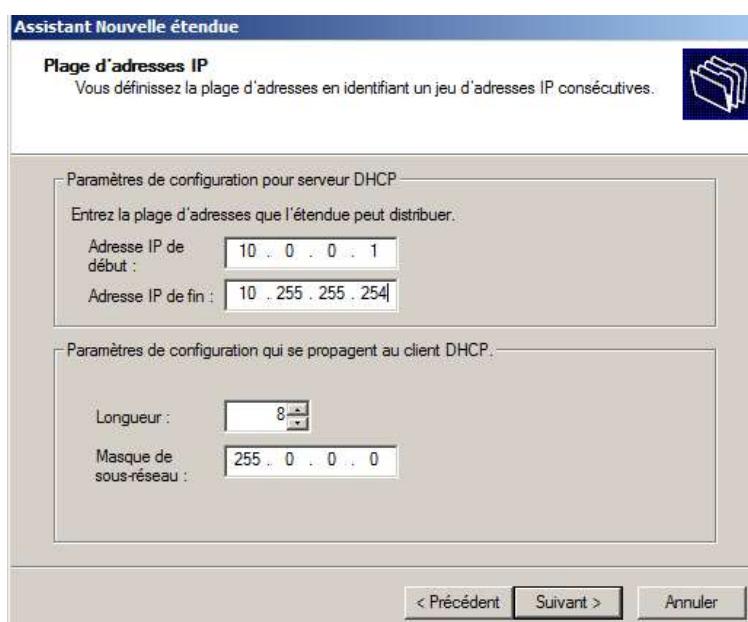
Nouvelle étendue

Ensuite clic droit sur **IPv4**, puis clic simple sur **Nouvelle étendue**. Cliquer ensuite sur **Suivant**.



Renseigner le nom de l'étendue voulu, le nom à pour but de vous y retrouver dans l'ensemble des étendues de votre serveur DHCP, cela peut être l'adresse IP du réseau ou bien un service en particulier [INFRA|COMPTA|SAV]. Dans notre exemple j'ai choisi **LAN 10 Serveurs**, cliquer ensuite sur **Suivant**.

Renseignez les informations correspondant à la capture d'écran ci-dessous, puis cliquer sur **Suivant**. Nous devons choisir la première et la dernière adresses IP à distribuer par cette étendue. Vous devez aussi spécifiez le masque pour indiquer aux postes clients s'il y a des sous-réseaux.



Exclusion

Nous avons utilisé toutes les adresses disponibles pour le réseau 10 dans notre étendue, or les deux adresses IP 10.0.0.1 et 10.255.255.254 sont déjà affecté en statique.

10.0.0.1 est l'adresse IP du SRV1

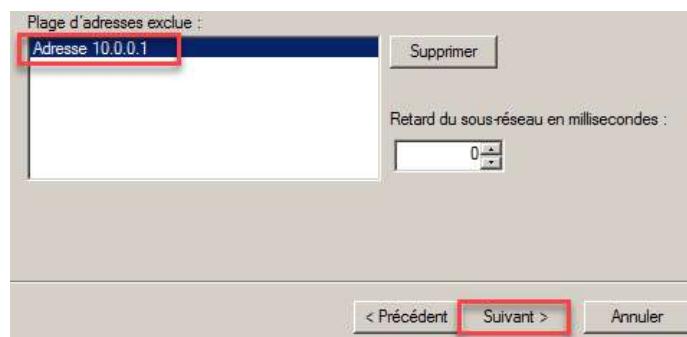
10.255.255.254 est une des adresses IP du SRV2.

Si nous ne bloquons pas ses deux adresses nous aurons un conflit d'adresse IP ce qui entraînera un dysfonctionnement de mon réseau.

Nous allons exclure l'adresse 10.0.0.1 du POOL DHCP (plage d'adresse de l'étendue), pour qu'il ne tente pas de la proposer. Entrer l'adresse IP **10.0.0.1** dans l'adresse IP de début. Pas besoin de mettre une IP de fin pour bloquer une seule adresse. Cela permet de bloquer une plage d'adresse IP d'un coup. Cliquer ensuite sur **Ajouter**.

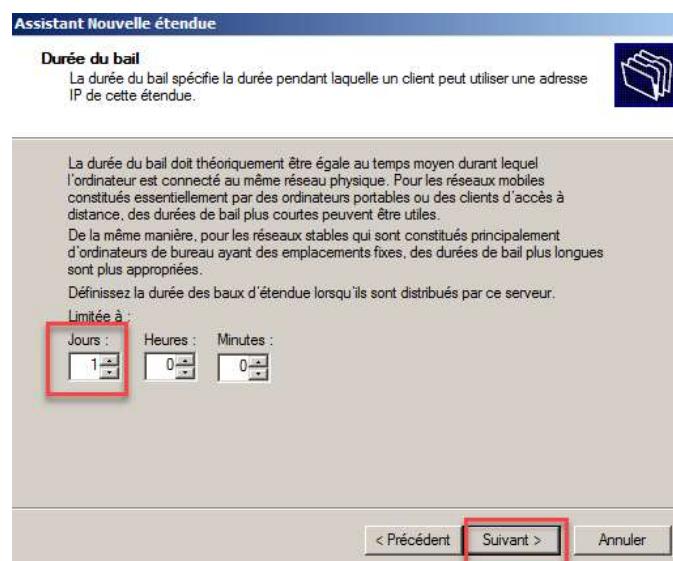


L'adresse IP apparaît dans la plage d'adresse exclue, cliquer maintenant sur **Suivant**.



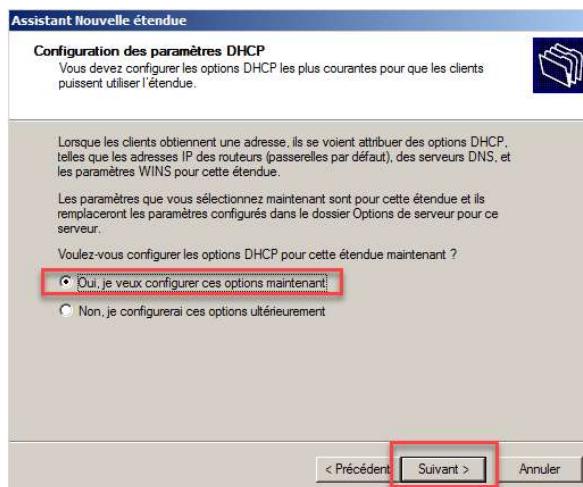
Durée du bail

Changer la durée du Bail à 1 journée. Cliquer sur **Suivant**.



Paramètres DHCP

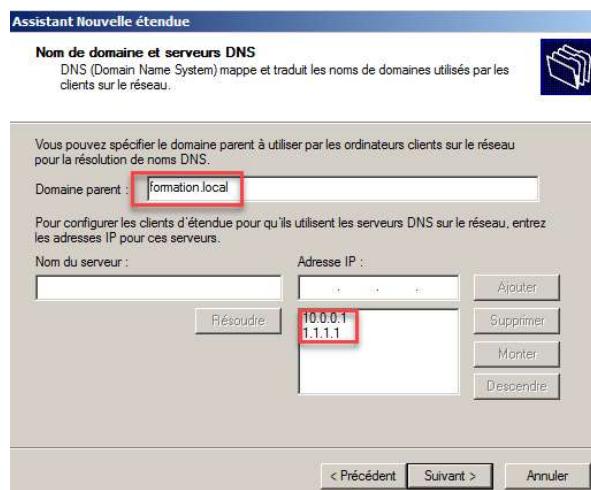
Cocher **Oui, je veux configurer ces options maintenant** pour attribuer des options de passerelle par défaut, suffixe DNS et adresses des serveurs DNS. Cliquer sur **Suivant**.



Ajouter l'adresse IP **10.255.255.254** qui correspond à l'adresse IP de la carte réseau du SRV2 qui est aussi notre ROUTEUR/NAT. Cela permettra aux clients d'interroger la table de routage pour éventuellement trouver son réseau de destination. Cliquer sur **Ajouter** pour valider l'adresse et cliquer sur **Suivant**.

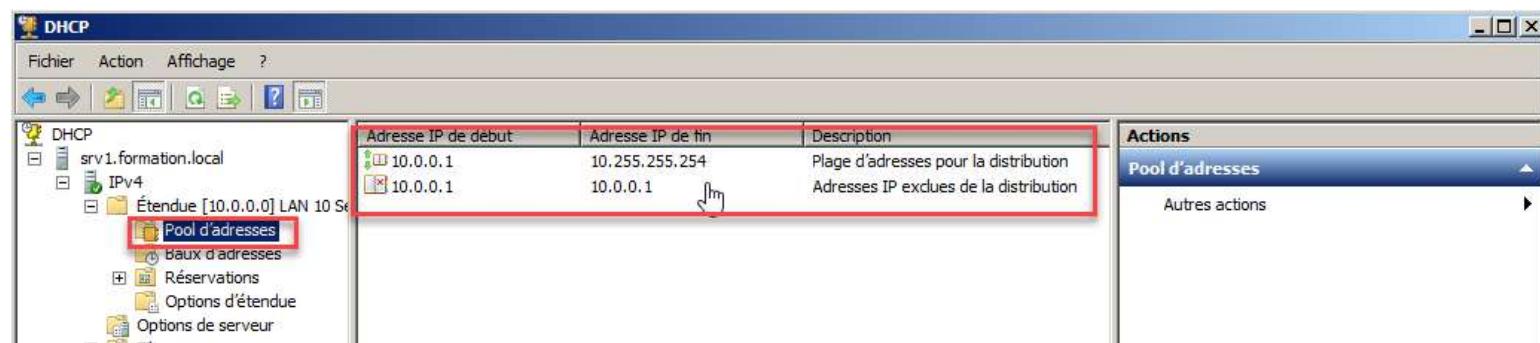
Paramétrage DNS

Renseigner les informations permettant aux clients d'interroger notre DNS. (voir capture ci-dessous) et cliquer sur **Suivant**. Pensez à cliquer sur Ajouter pour les adresses IP des serveurs DNS.



Cliquer sur **Suivant** pour le réglage des serveurs WINS, nous utilisons le DNS. Laissez cocher **Oui, je veux activer cette étendue maintenant** et cliquer sur **Suivant** et **Terminer**.

Visualisations de l'entendue



Cliquer sur Etendue / Pool d'adresses. Nous voyons la plage d'adresses et l'adresse exclue. Je vais prendre un poste client pour vérifier le fonctionnement de mon serveur DHCP. Mettez-le sur le bon LAN SEGMENT LAN 10.

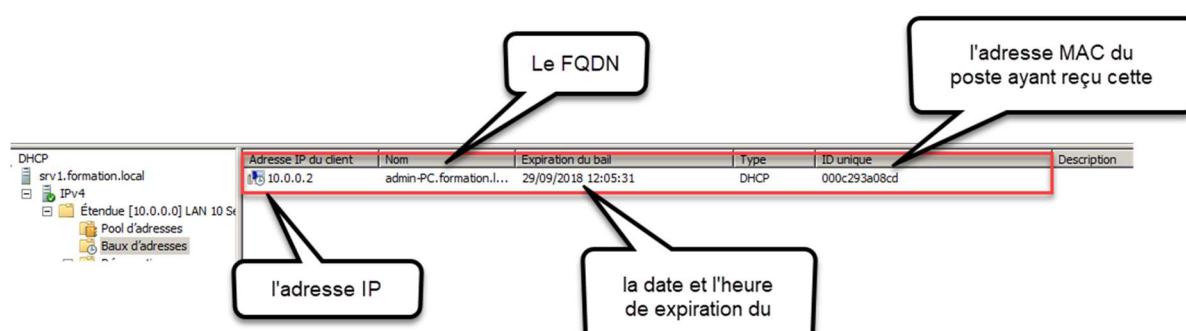
No.	Time	Source	Destination	Protocol	Length	Info	Transaction ID	0xe896260
1	0.000000	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover	Transaction ID	0xe896260
2	0.001036	10.0.0.1	255.255.255.255	DHCP	350	DHCP Offer	Transaction ID	0xe896260
3	0.001917	0.0.0.0	255.255.255.255	DHCP	354	DHCP Request	Transaction ID	0xe896260
4	0.002715	10.0.0.1	255.255.255.255	DHCP	355	DHCP ACK	Transaction ID	0xe896260

J'ai bien recu les 4 paquets, et mon adresse IP.

```
C:\Users\admin>ipconfig
Configuration IP de Windows

Carte Ethernet Connexion réseau Bluetooth :
  Statut du média : Média déconnecté
```

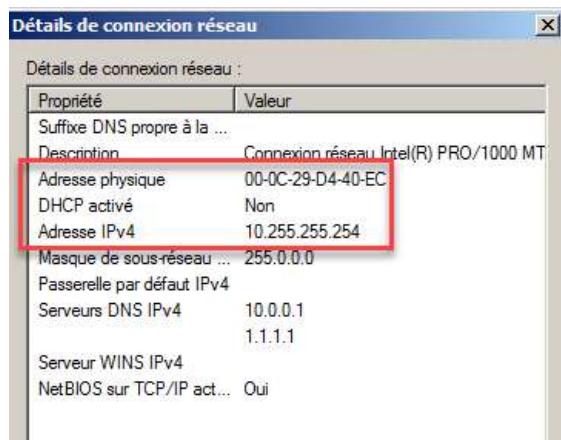
On peut voir que l'assignation de l'adresse IP est bien enregistrer dans mon serveur.



Réservations

On peut également fixer une adresse IP de manuel automatique sans passer par de l'adressage manuel. Il faut avoir l'adresse MAC de la carte réseau et l'adresse IP à bloquer. Quand le poste fera sa demande d'adressage avec son paquet DISCOVER, le serveur regardera dans ses réservations et trouvera l'adresse MAC du poste et enverra toujours l'adresse IP qui avait été fixé.

Je dois récupérer l'adresse MAC de ma carte réseau en 10.255.255.254.

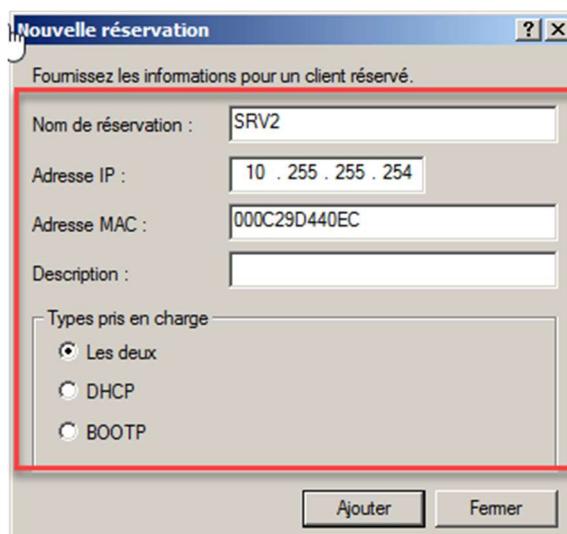


00:0C:29:D4:40:EC

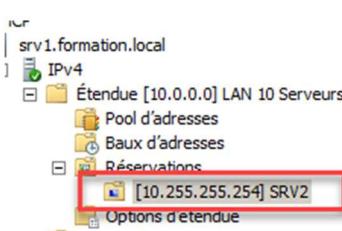
Aller sur le SRV1 et dans la console de gestion DHCP.

Faites un clic droit sur **Réservations** puis clic simple sur **Nouvelle réservation**.

Renseignez les informations dans les différents champs. Types pris en charge : DHCP seul, un poste avec un système reçoit une adresse IP. Le BOOTP permet à une machine sans disque dur ou sans OS de recevoir une adresse IP, l'adresse d'un serveur capable de lui fournir un système et le fichier charge en mémoire pour exécution. Cliquer sur **Ajouter**.



Aller dans l'adresse IP pour voir les informations de réservations.



NOM D'OPTION	Fournisseur	Valeur	Classe
003 Routeur	Standard	10.255.255.254	Aucun
006 Serveurs DNS	Standard	10.0.0.1, 1.1.1.1	Aucun
015 Nom de domaine DNS	Standard	formation.local	Aucun

AUTRES STATUS DHCP

- **DHCPNAK** (réponse du serveur pour signaler au client que son bail est échu ou si le client annonce une mauvaise configuration réseau)
- **DHCPDECLINE** (le client annonce au serveur que l'adresse est déjà utilisée)
- **DHCPRELEASE** (le client libère son adresse IP)
- **DHCPINFORM** (le client demande des paramètres locaux, il a déjà son adresse IP)

COMMANDES UTILES

Deux commandes sont utiles avec un DHCP.

Ipconfig /release : permet de libérer le client du bail

Ipconfig /renew : permet de faire une demande d'attribution d'IP ou de renouvellement de bail. **DISCOVER**.

Création d'une deuxième étendue

Nom de l'étendue

Entrez 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.

Nom : LAN 192.168.1. CLIENTS

Description :

Plage de distribution

Paramètres de configuration pour serveur DHCP

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

Adresse IP de début : 192.168.1.1

Adresse IP de fin : 192.168.1.254

Paramètres de configuration qui se propagent au client DHCP.

Longueur : 24

Masque de sous-réseau : 255.255.255.0

Exclusion

Entrez uniquement une adresse IP de debut.

Adresse IP de début : Adresse IP de fin : Ajouter

Plage d'adresses exclue :

Adresse 192.168.1.1
Adresse 192.168.1.254

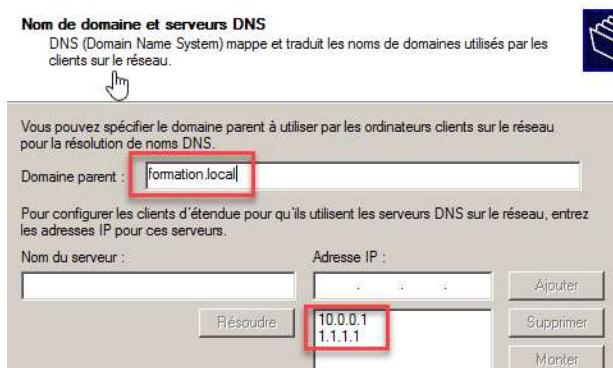
Supprimer

Passerelle par défaut

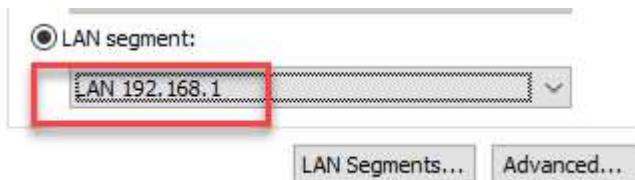
Pour ajouter une adresse IP pour qu'un routeur soit utilisé par les clients, entrez l'adresse ci-dessous.

Adresse IP : Ajouter
 Supprimer

Intégration des options de nom de domaine

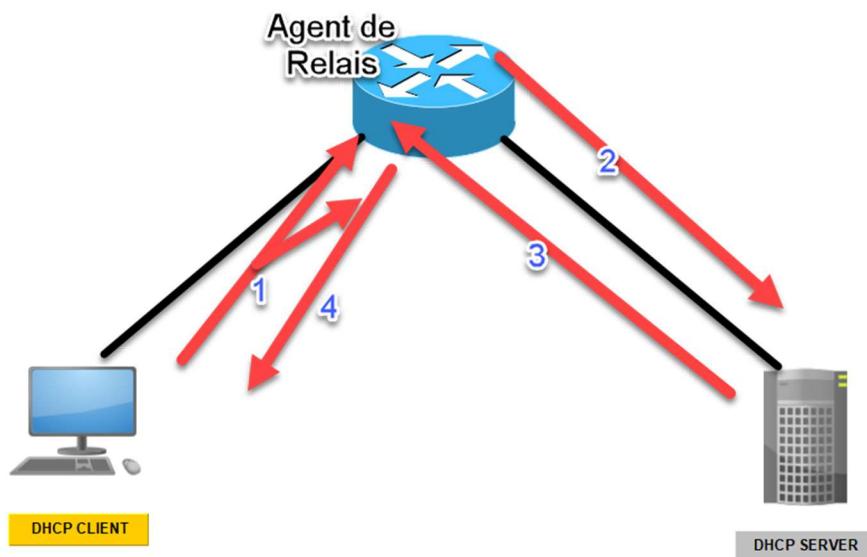


Test sur le poste client. Passer le client en LAN SEGMENT 192.168.1



Notre client ne pourra jamais recevoir d'adresse IP s'il reste câblé sur le réseau 192.168.0. En effet pour obtenir une adresse IP il passe par un **Broadcast** qui est bloqué par le routeur afin d'éviter d'inonder tous les réseaux présents derrière le routeur.

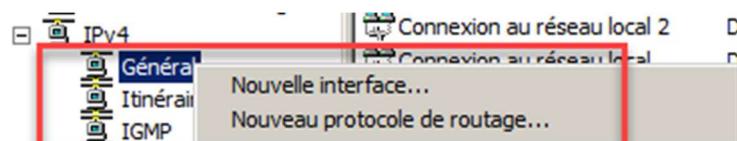
Agent de Relais DHCP (DHCP RELAY)



- 1 – Le client effectue sa demande en **Broadcast** pour trouver un serveur.
- 2 – L'agent de relais reçoit la demande qu'il reçoit sur le port 67 et demande une adresse IP au Serveur DHCP dont il connaît l'adresse.
- 3 – Le serveur fournit l'adresse à l'agent
- 4 – L'agent de relais transmet l'adresse au client.

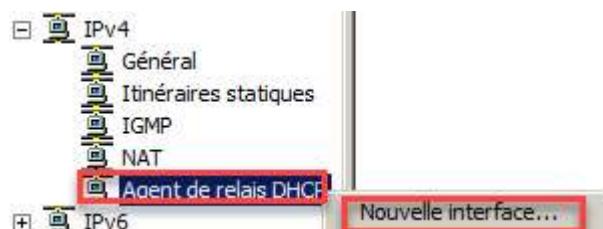
Installation de l'agent de relais DHCP

Aller sur dans la console de routage et d'accès distance. Sélectionné **IPv4, Général** et faites un clic droit **Nouveau protocole de routage**.

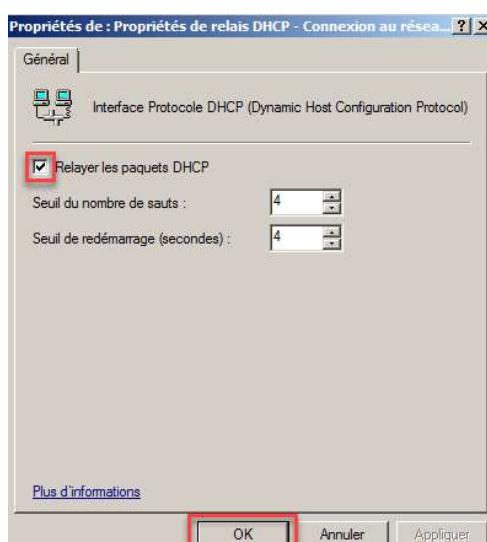


Sélectionner **l'agent de relais DHCP** et cliquer sur **OK**.

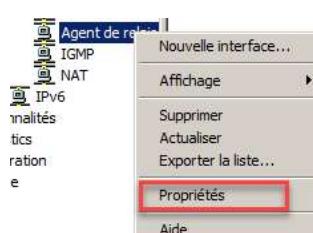
Faites un clic droit sur **Agent de relais DHCP**, puis clic simple sur **Nouvelle interface**.



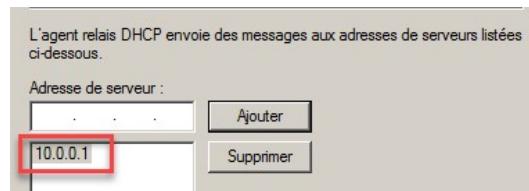
Sélectionner **Connexion au réseau local 2**, cliquer sur **OK**.



Sélectionner l'agent de relais DHCP, clic droit **propriétés**.



Ajout de l'adresse IP du serveur DHCP 10.0.0.1 et cliquer sur **Ajouter**.



Voici l'interface installé.

Interface	Mode de relais	Requêtes reçues	Réponses reçues	Requêtes rejetées	Répon
Connexion au réseau local 2	Activé	0	0	0	0

Sur mon poste client voici les informations reçues.

Carte Ethernet Connexion au réseau local :

Suffixe DNS propre à la connexion. : formation.local
Adresse IPv6 de liaison locale. : fe80::b18c:f6de:da0:900f%11
Adresse IPv4. : 192.168.1.2
Masque de sous-réseau. : 255.255.255.0
Passerelle par défaut. : 192.168.1.254

Notre DHCP est fonctionnel.

ACTIVE DIRECTORY

Définition :

Active Directory est un service d'annuaire utilisé pour stocker des informations relatives aux ressources réseau sur un domaine.

Une structure *Active Directory* (AD) est une organisation hiérarchisée d'objets. Les objets sont classés en trois grandes catégories : les ressources (par exemple les imprimantes), les services (par exemple le courrier électronique) et les utilisateurs (comptes utilisateurs et groupes). L'AD fournit des informations sur les objets, il les organise et contrôle les accès et la sécurité.

Forêt Active Directory

Une forêt est une collection d'un ou plusieurs domaines Active Directory qui partagent la même structure logique, le même schéma d'annuaire (définitions de classes et d'attributs), la même configuration d'annuaire (informations de site et de réPLICATION) et le même catalogue global (fonctionnalités de recherche à l'échelle de la forêt). Les domaines d'une même forêt sont automatiquement liés par des relations d'approbation transitives bidirectionnelles.

Domaine Active Directory

Un domaine est une partition dans une forêt Active Directory. Le partitionnement des données permet aux organisations de répliquer des données uniquement là où cela est nécessaire. Définition simplifiée : Ensemble d'ordinateurs autour d'un serveur 2000/2003/2008 partageant une base de données commune. Un domaine est une zone de sécurité.

Ainsi, l'annuaire peut s'adapter globalement sur un réseau disposant d'une bande passante limitée. En outre, le domaine prend en charge un certain nombre d'autres fonctions de base relatives à l'administration, dont les suivantes :

- Identité d'utilisateur à l'échelle du réseau. Un domaine permet à une identité d'utilisateur d'être créée une fois et d'être référencée sur n'importe quel ordinateur joint à la forêt dans laquelle se trouve le domaine. Les contrôleurs de domaine qui constituent le domaine servent à stocker de manière sécurisée les comptes d'utilisateurs et les informations d'identification des utilisateurs (telles que les mots de passe ou les certificats).
- Authentification. Les contrôleurs de domaine assurent des services d'authentification pour les utilisateurs et fournissent des données d'autorisation supplémentaires, telles que les appartenances aux groupes d'utilisateurs, qui peuvent être utilisées pour contrôler l'accès aux ressources du réseau.
- Relations d'approbation. Les domaines peuvent étendre les services d'authentification aux utilisateurs de domaines situés en dehors de leur forêt au moyen d'approbations. Permet à l'utilisateur d'un domaine « Y » d'accéder aux ressources d'un domaine « X » et inversement
- RéPLICATION. Le domaine définit une partition de l'annuaire qui contient les informations requises pour assurer des services de domaine, puis réplique ces informations entre les contrôleurs de domaine. Ainsi, tous les contrôleurs de domaine sont homologues dans un domaine et sont gérés comme une seule unité.

Domaine : Installation d'Active directory via un utilitaire DCpromo.exe

Pour l'installation d'AD prérequis :

- TCP/IP

- NTFS (partition)
- DNS serveur

Structure D'AD :

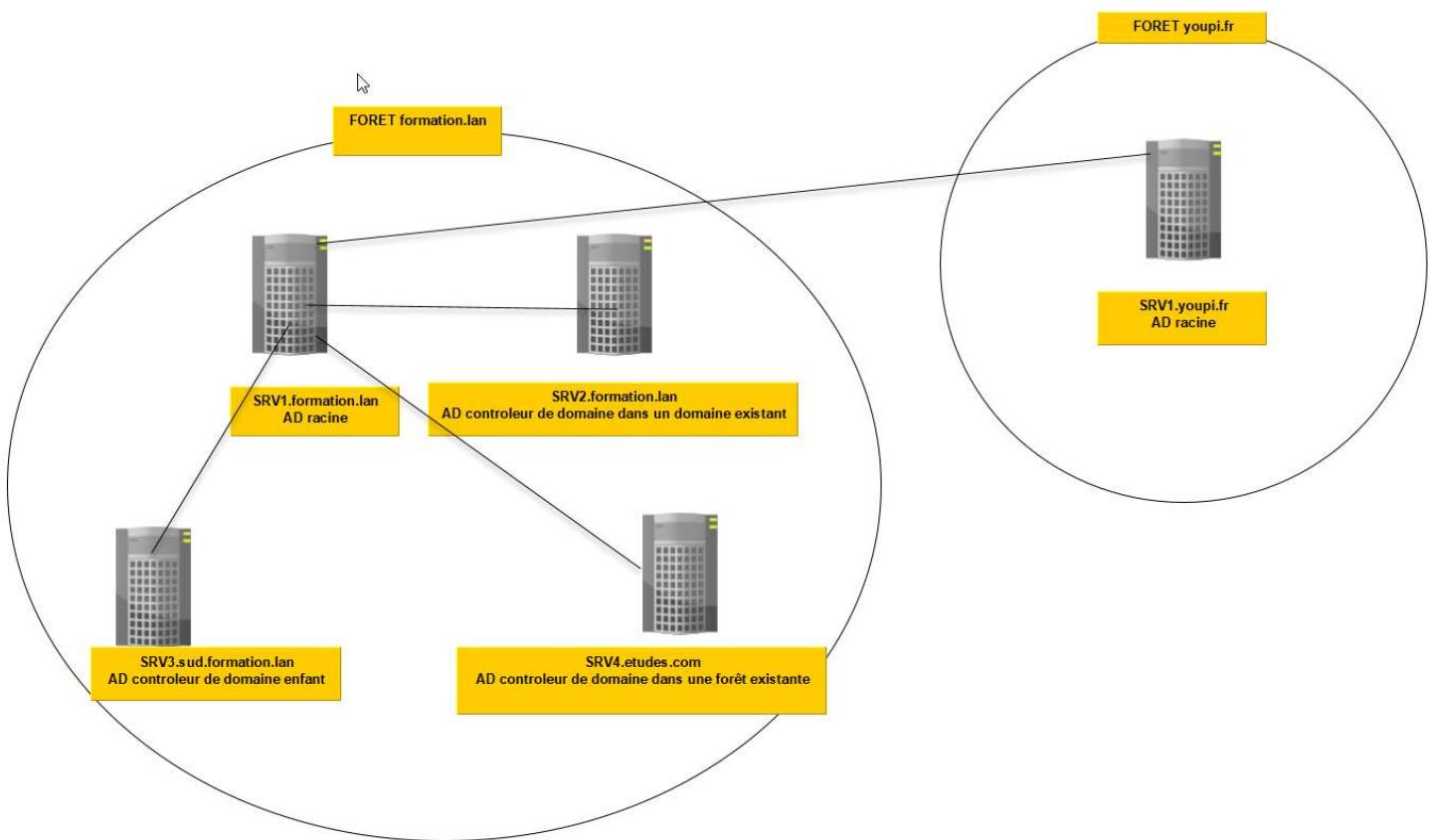
- Forêt
 - Arborescences
 - Domaine

4 cas pour être contrôleur de domaine :

- CD père créateur de la forêt
- CD père dans une forêt existante
- CD enfant d'un père dans une forêt existante
- CD supplémentaire dans un domaine existant

Nom de domaine Active Directory = Nom de domaine DNS

Arborescence : ensemble de Contrôleur de domaine portant de noms de domaine contigus. (Touchant)



La structure logique

La structure logique d'un réseau est l'ensemble de ses éléments intangibles (objets, domaines, arbres et forêts).

Dans Active Directory, une ressource réseau est un objet, c'est-à-dire un ensemble d'attributs distinct et nommé. Les attributs de l'objet sont ses caractéristiques dans l'annuaire. Les objets peuvent être organisés en classes : les classes sont des groupements logiques d'objets. Utilisateurs, Groupes, et Ordinateurs sont des exemples de classes d'objets.

Au plus bas niveau, certains objets représentent des entités individuelles de votre réseau, un utilisateur ou un ordinateur par exemple. On les appelle objets Feuille : ils ne peuvent pas contenir d'autres objets. Cependant, afin de faciliter leur gestion et de simplifier l'organisation de l'annuaire, vous avez la possibilité de placer les objets Feuille dans d'autres objets appelés objets conteneurs. Ces objets conteneurs peuvent eux-mêmes contenir d'autres objets conteneurs sous un format compilé (ou hiérarchisé).

Le type d'objet conteneur le plus courant est l'Unité d'Organisation (OU). Vous pouvez utiliser une OU afin de catégoriser les objets d'un domaine selon un schéma de regroupement administratif logique. Attention, la structure et la hiérarchie d'une OU dans un domaine ne dépend de la structure d'aucun autre domaine.

Tous les objets d'un réseau, Feuille ou Conteneurs, ne peuvent exister que dans un seul domaine. Les domaines regroupent des objets apparentés ensemble afin de refléter le réseau de votre organisation. Chaque domaine créé enregistre exclusivement les informations concernant les objets qu'il contient. Actuellement, le nombre limite d'objets que vous pouvez maintenir dans un domaine est d'un million.

Chaque domaine représente une limite de sécurité. Dans chaque domaine, l'accès aux objets est contrôlé par des entrées de contrôle d'accès (ACE) enregistrées dans les listes du contrôle d'accès (ACL). Ces paramètres de sécurité ne peuvent pas être transmis d'un domaine à un autre. Dans Active Directory, un domaine peut aussi être appelé partition. Un domaine étant la partition physique de la base de données Active Directory, vous pouvez structurer les vôtres par fonction commerciale (RH, Ventes, ou Comptabilité) ou par emplacement (géographique ou relatif à la fonction). Il est à noter que si chaque domaine représente une limite de sécurité, la limite absolue de sécurité, notamment quant aux droits dont disposent les administrateurs se trouve au niveau de la forêt Active Directory. La prise en compte de cette règle est importante dans les réflexions concernant l'isolation et la compartimentation des fonctions administratives entre différents administrateurs.

En regroupant plusieurs domaines parents pour permettre un partage des ressources global, vous créez un Arbre. Un arbre peut n'être composé que d'un seul domaine ; vous pouvez également regrouper des domaines multiples au même emplacement dans une structure hiérarchisée. Les domaines d'un arbre sont reliés les uns aux autres de façon transparente par l'intermédiaire de relations d'approbation dans les deux sens avec une sécurité basée sur le système d'authentification Kerberos. Ces approbations sont toutes deux permanentes (elles ne peuvent être supprimées) et transitives. En d'autres termes, si le domaine A approuve le domaine B qui approuve le domaine C, alors le domaine A approuve le domaine C.

Tous les domaines d'un arbre partagent une définition formelle de tous les types d'objets appelée Schéma. Par ailleurs, le catalogue global (GC) est partagé par tous les domaines de n'importe quel arbre. Le GC fait office de dépôt central pour les objets d'un arbre.

Chaque arbre est également représenté par un espace de noms contigu. Par exemple, si le domaine racine de votre société est "société.com" et si vous créez des domaines séparés pour vos divisions Vente et Service-après-vente, leurs noms de domaine deviennent "ventes.société.com" et "SAV.société.com". Ce sont des domaines enfants. Dans un environnement autre que Windows NT 4.0, chaque domaine génère des relations d'approbation.

Au niveau le plus élevé, des arbres disparates peuvent être regroupés ensemble pour former une forêt. Une forêt vous permet de combiner des divisions différentes dans une organisation voire de regrouper des organisations différentes. Ces organisations n'ont pas besoin de partager le même schéma de noms et peuvent fonctionner de façon indépendante tout en communiquant entre elles. Tous les arbres d'une forêt partagent le même schéma, le même catalogue global et le même conteneur de configuration. Là aussi, le système d'authentification Kerberos établit les relations d'approbation entre les arbres.

La structure physique

Les contrôleurs et sites de domaine sont les seuls éléments de base constituant la structure physique d'une configuration de Réseau local (LAN).

Contrairement à un environnement Windows NT 4.0, un réseau constitué exclusivement d'ordinateurs fonctionnant sous Windows 2000 n'a pas de contrôleurs principaux de domaine (PDC) ni de contrôleur secondaire de domaine (BDC). Tous les serveurs participant à l'administration du réseau dans un environnement Windows 2000 sont considérés comme des contrôleurs de domaine. Un contrôleur de domaine (DC) stocke une copie de la base de données de l'annuaire et le processus de réPLICATION est automatique entre les contrôleurs dans le domaine.

Les réseaux d'entreprise s'étendent de plus en plus sur des sites géographiques multiples, par conséquent les implications de la conception et de la structure d'un réseau étendu sont très importantes lorsqu'on comprend l'impact que la réPLICATION de la base de données d'annuaire peut avoir sur les contrôleurs de domaine et les performances du réseau.

Catalogue global

Le catalogue global contient un réPLICA partiel de chacun des domaines Windows 2000 de l'annuaire : il est construit automatiquement par le système de réPLICATION d'Active Directory. Les utilisateurs peuvent ainsi trouver des objets dans l'arbre d'un domaine Active Directory en spécifiant un ou plusieurs attributs de l'objet recherché. Le catalogue contient également le schéma et la configuration des partitions de l'annuaire. Tout cela signifie que le catalogue global comporte un réPLICA de chacun des objets de l'annuaire Active Directory ; mais ces réPLICAS ne possèdent qu'une petite partie des attributs des objets d'origine. Les attributs repris dans le catalogue global sont les attributs les plus communément utilisés dans les opérations de recherche (les nom et prénoms de l'utilisateur, les noms de connexion par exemple) ainsi que les attributs requis pour localiser le réPLICA complet de l'objet.

En utilisant ces informations basiques, les utilisateurs peuvent retrouver les objets qui les intéressent rapidement alors qu'ils ne connaissent pas leur domaine et sans pour cela devoir utiliser un espace de noms contigu étendu. Si l'objet est introuvable dans le catalogue global, alors l'utilitaire de recherche peut réclamer votre partition de domaine local pour plus d'informations.

Vous pouvez utiliser le gestionnaire de schéma pour modifier le schéma et définir les attributs qui doivent être stockés dans le catalogue global. Ce dernier étant répliqué sur les modifications apportées à tous les serveurs du Catalogue global, il est recommandé de limiter la quantité d'attributs stockés dans la partition locale pour des raisons de performances comme de maintenance.

Modifications dans les groupes

Active Directory introduit également de nouveaux groupes dans le processus de planification logique. Dans l'environnement Windows NT 4.0, deux types de groupe de base étaient disponibles à un administrateur réseau : local et global. En restant dans les limites inhérentes à ce type de structure, Windows 2000 offre une flexibilité et une fonctionnalité accrues aux administrateurs réseau, avec les groupes suivants :

- Groupes à portée locale (également appelés groupes locaux)
- Groupes à portée locale dans le domaine (groupes locaux de domaine)
- Groupes à portée globale (groupes globaux)
- Groupes à portée universelle (Groupes universels)

Désormais les groupes globaux peuvent contenir d'autres groupes globaux. Les groupes globaux servent toujours à collecter les utilisateurs ; en plus de cela, le fait de pouvoir placer un groupe dans un autre permet à

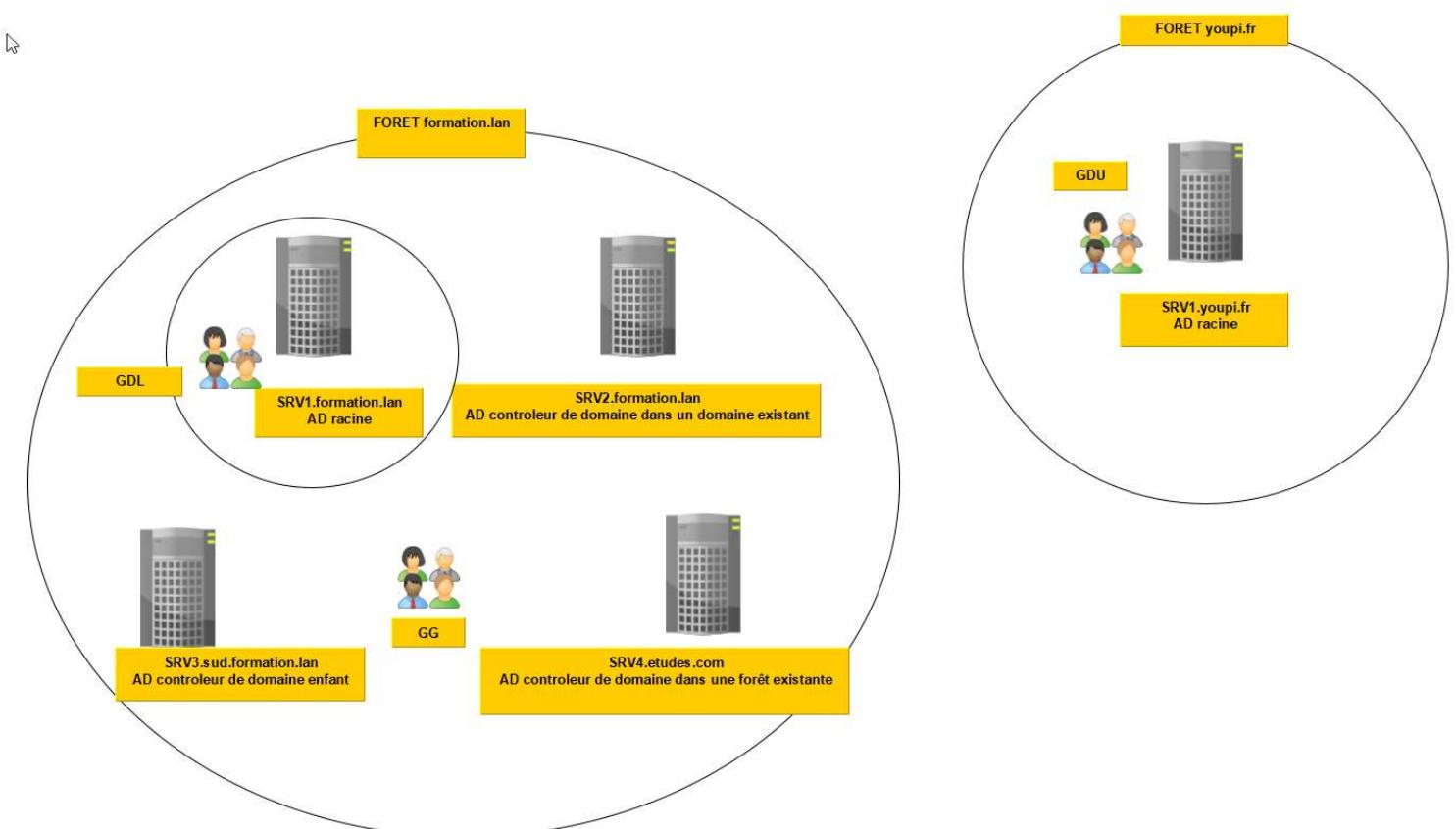
l'administrateur de les placer où il le souhaite dans une forêt afin de faciliter la maintenance du réseau. Cependant, les groupes globaux ne peuvent contenir les utilisateurs et groupes d'un seul domaine dans la forêt Active Directory.

De nombreux réseaux comportant des serveurs Windows NT 4.0 et Windows 2000, vous devez déterminer le nombre et les types de domaines de votre réseau et savoir si ces domaines sont en mode mixte ou natif avant de créer des groupes :

- Domaine en mode mixte. Par défaut, le système d'exploitation Windows 2000 s'installe dans une configuration réseau en mode mixte. Un domaine en mode mixte comprend un groupe d'ordinateurs en réseau fonctionnant avec des contrôleurs de domaine Windows NT 4.0 et Windows 2000. (Cela peut également être le cas lorsque vous avez des ordinateurs fonctionnant uniquement avec des contrôleurs de domaine Windows 2000.)
- Domaine en mode natif. Vous pouvez convertir un domaine au mode natif lorsqu'il ne contient que des contrôleurs de domaine Windows 2000 Server.

Le groupe universel (nouveauté sous Windows 2000) peut contenir tous les autres groupes et utilisateurs de n'importe quel arbre dans la forêt, et vous pouvez l'utiliser à l'aide de n'importe quelle liste de contrôle d'accès (ACL) dans la forêt.

Les groupes globaux, locaux de domaine et universels peuvent être combinés pour contrôler l'accès aux ressources réseau. En fait, les groupes globaux permettent d'organiser les utilisateurs dans des conteneurs administratifs qui représentent leurs domaines respectifs. Les groupes universels contiennent les groupes globaux des différents domaines, ce qui permet une gestion encore plus précise de la hiérarchie des domaines lors de l'octroi d'autorisations. Vous pouvez ajouter des groupes locaux aux groupes universels puis leur attribuer des autorisations d'accès à des groupes locaux de domaine (emplacement " physique " des ressources). Ainsi, les administrateurs peuvent ajouter ou enlever des utilisateurs de chaque groupe global d'un domaine afin de contrôler l'accès aux ressources dans l'entreprise sans pour cela avoir besoin d'opérer les modifications sur plusieurs sites.



Présentation des maîtres d'opérations :

Les modifications d'Active Directory peuvent être faites sur n'importe quel contrôleur de domaine. Il y a toutefois 5 exceptions pour lesquelles les modifications sont faites sur un et un seul contrôleur de domaine particulier : les 5 rôles des maîtres d'opérations.

Voici les cinq rôles des maîtres d'opérations :

- Contrôleur de schéma
- Maître d'attribution des noms de domaine
- Emulateur CPD
- Maître d'identificateur relatif
- Maître d'infrastructure.

Les deux premiers sont assignés au niveau de la forêt, les trois derniers au niveau du domaine. Ce qui implique s'il y a plusieurs domaines dans une forêt, autant de maîtres d'opérations pour les trois derniers rôles, que de domaines.

Par défaut le premier contrôleur de domaine d'une nouvelle forêt contient les cinq rôles.

Rôle du contrôleur de schéma

Il est le seul dans une forêt à pouvoir modifier le schéma. Il duplique les modifications aux autres contrôleurs de domaine dans la forêt lorsqu'il y a eu une modification du schéma. Le fait d'avoir un seul ordinateur qui gère le schéma évite tout risque de conflits.

Un seul groupe peut faire des modifications sur le schéma : le groupe « administrateurs du schéma ».

Maître d'attribution de nom de domaine

Seul le contrôleur de domaine ayant ce rôle, est habilité à ajouter un domaine dans une forêt. Si le maître d'opération d'attribution de nom de domaine n'est pas disponible, il est impossible d'ajouter ou de supprimer un domaine à la forêt.

Du fait de son rôle, le maître d'attribution de nom de domaine est aussi un serveur de catalogue global. En effet pour éviter tous problèmes, celui-ci doit connaître tous les noms des objets présents dans la forêt.

Emulateur CPD (PDC)

Ce rôle a été créé principalement dans un souci de permettre une compatibilité avec les versions antérieures de Windows 2000.

Rôle propre aux versions antérieures à Windows 2000 :

- Il permet la prise en charge des BDC Windows NT4.
- Il a la gestion des modifications des mots de passes pour des clients antérieurs à Windows 2000.

Autres Rôles :

- Authentification de secours : Lorsque vous avez modifié votre mot de passe sur votre ordinateur, et que vous vous connectez peu de temps après sur une autre machine, il se peut que la réPLICATION du changement de votre mot de passe n'ait pas encore été effectuée. Dans ce cas, le DC qui vérifie votre mot de passe va demander à l'émulateur CPD si votre mot de passe n'a pas été changé avant de vous refuser l'accès.
- Synchroniser l'heure de tous les DC en fonction de son horloge.
- Elimine les risques d'écrasement d'objets GPO : par défaut la modification de GPO se fait sur ce DC.

Maître RID

Un SID est composé de deux blocs : un identificateur de domaine et un RID (Identificateur unique dans le domaine).

Pour qu'il ne puisse y avoir deux DC qui assignent le même SID à deux objets différents, le maître RID distribue une plage de RID à chacun des DC. Lorsque la plage de RID a été utilisée, le DC demande une nouvelle plage de RID au maître RID.

Le maître RID a aussi la charge des déplacements inter-domaines, pour éviter la duplication de l'objet.

Maître d'infrastructure

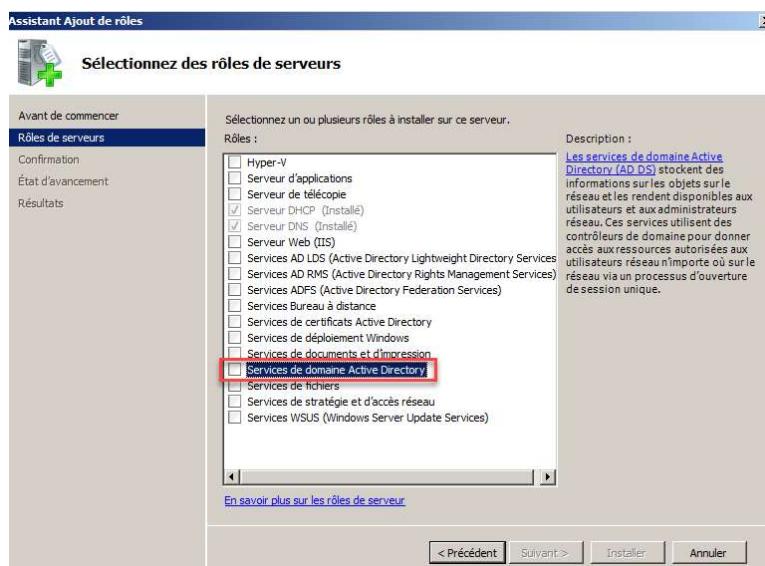
Le maître d'infrastructure sert à mettre à jour, dans son domaine, les références à des objets situés dans d'autres domaines. Si des modifications d'un objet du domaine surviennent (déplacement intra et extra domaine), alors si cet objet est lié à un ou plusieurs objets d'autres domaines, le maître d'infrastructure est responsable de la mise à jour vers les autres domaines. La mise à jour se fait par le biais d'une réPLICATION.

Un Maître d'infrastructure ne peut être aussi un serveur de catalogue global.

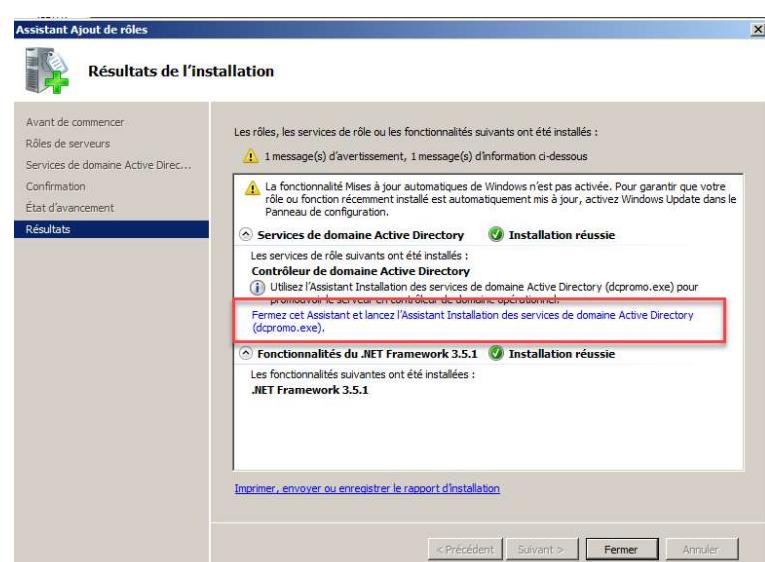
Installation

Pour l'installation d'active directory nous allons ajouter un deuxième disque dur sur SRV1. Ajouter un disque dur de 60 Go, formatez-le avec le système de fichiers NTFS.

Aller dans **le gestionnaire de serveur, Rôles, Ajouter des rôles**. Cocher **Services de domaine Active Directory**. Ajouter les fonctionnalités avancées. Puis **Suivant, suivant et Installer**.



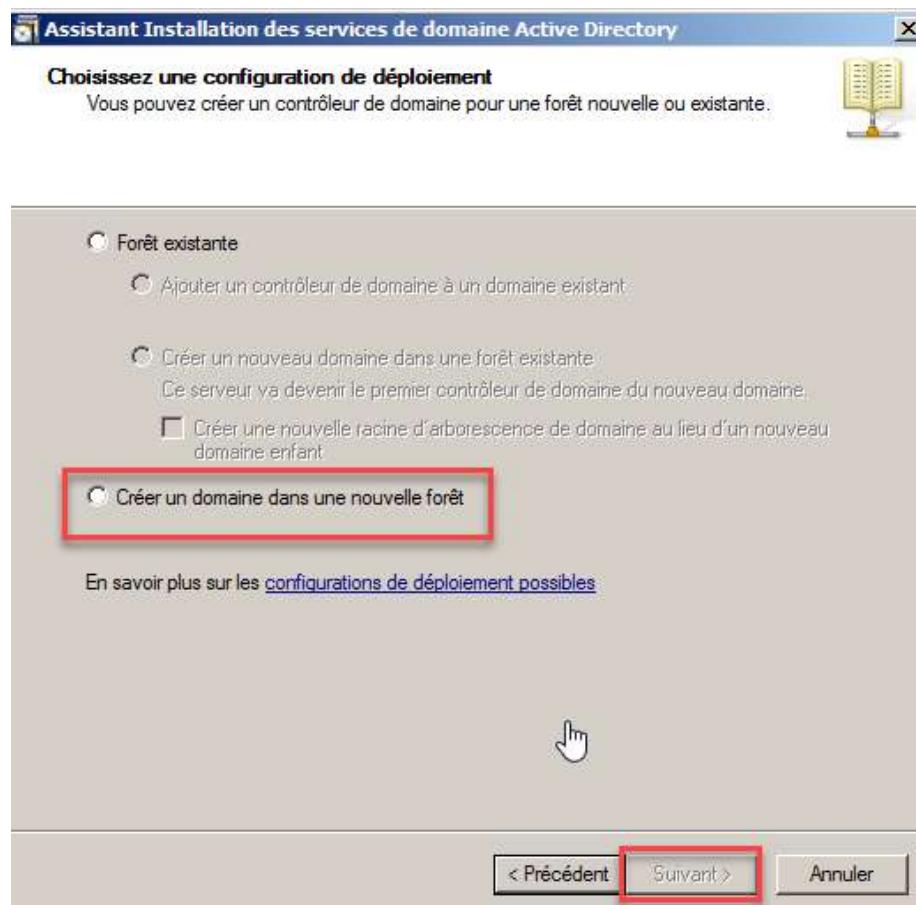
Une fois l'installation finie, cliquer sur le lien en bleu. Il permet de promouvoir notre serveur en Contrôleur de domaine.



L'assistant d'installation des services de domaine Active Directory se lance, cocher Utiliser l'installation en mode avancé, puis cliquer sur Suivant.



Cliquer à nouveau sur Suivant.



Types d'installations :

Forêt existante :

Ajouter un contrôleur de domaine à un domaine existant

Cela permet de créer ou rajouter un serveur répliquant les informations active directory d'un serveur déjà existant. (SRV2)

Créer un nouveau domaine dans une forêt existante.

Par défaut cela permet de créer un domaine de DNS Enfant d'un domaine existant. Il faut qu'une relation d'approbation hiérarchique soit établie. (délégation DNS – Redirecteur DNS) (SRV3)

Créer une nouvelle racine d'arborescence de domaine au lieu d'un nouveau domaine enfant

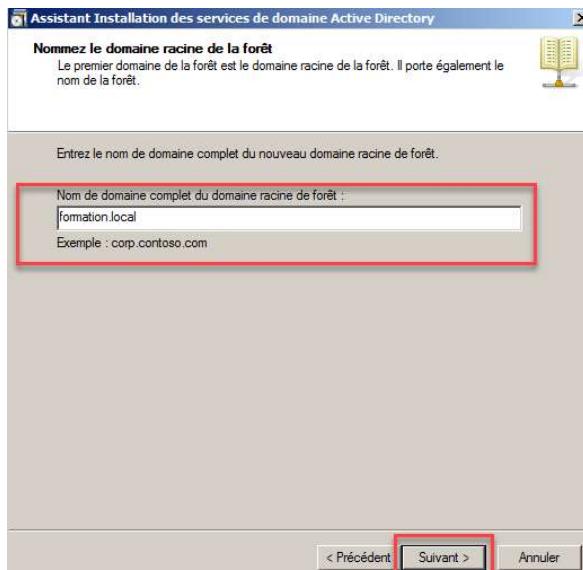
Permet de crée une nouvelle racine d'arborescence de domaine dans une forêt existante. (SRV4).

Créer un domaine dans une nouvelle forêt : Permet de créer un contrôleur de domaine racine et la forêt en même temps. (SRV1)

Nous allons créer la **forêt et le contrôleur de domaine racine** et cliquer sur **Suivant**.

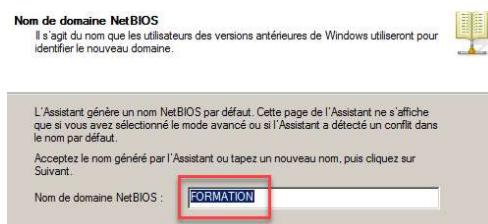


Entrer le nom du domaine racine de la forêt, on reprend ici le nom de la zone DNS. **formation.local**, puis cliquer sur **Suivant**.



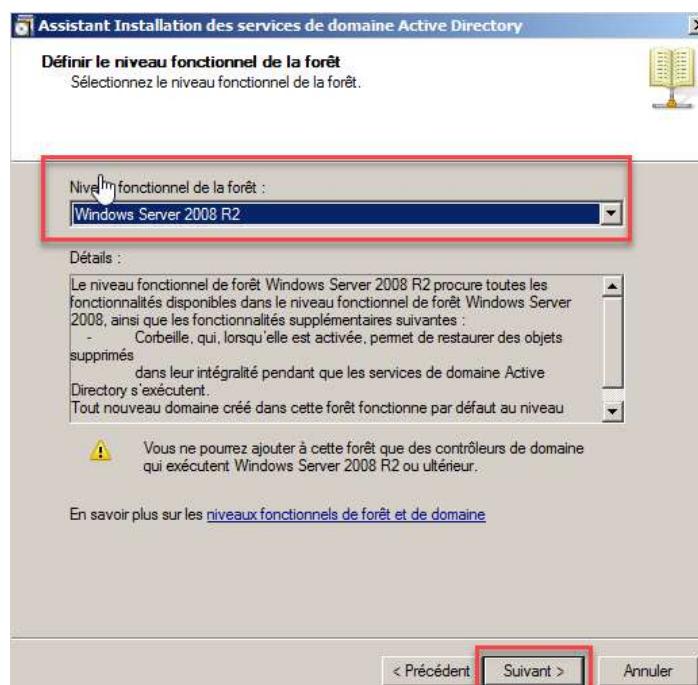
Une fenêtre apparaît pour informer de la vérification de la disponibilité du nom de forêt **formation.local**.

Cliquer sur **Suivant** pour le nom **NETBIOS** qui ne peut comporter que **8 caractères**, ne vous inquiétez pas si vous n'avez pas le . ni local. Cliquer simplement sur **Suivant**.



Définir le niveau fonctionnel de la forêt :

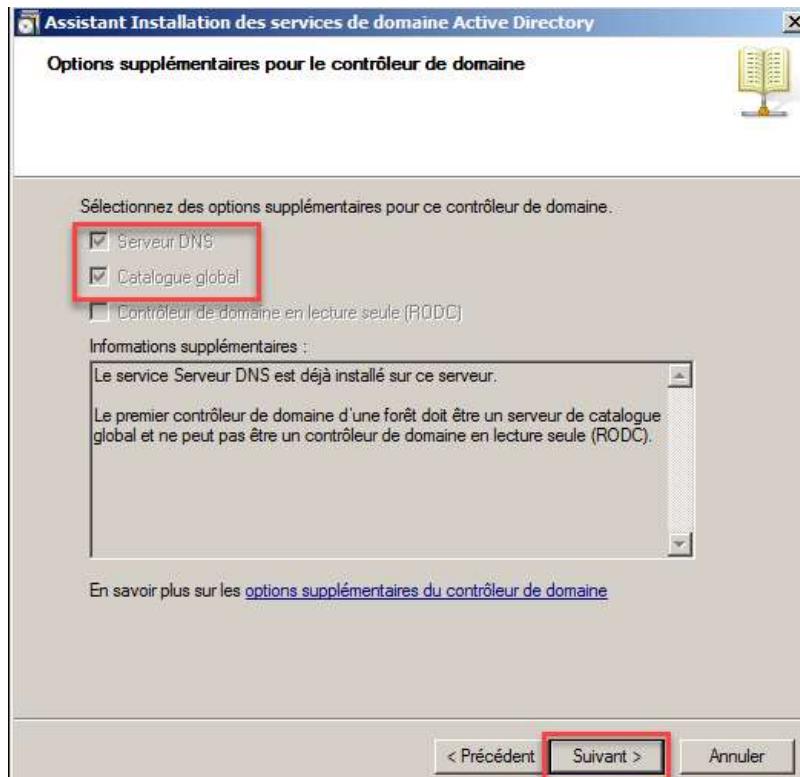
Choisissez le niveau le plus haut, il permet d'avoir toutes les fonctionnalités. Cependant tous les autres serveurs seront aussi en mode 2008 R2. Vu qu'il sera racine de mon système, il faudra le mettre à jour vers 2012 R2 par exemple pour migrer la forêt et ensuite migrer les autres serveurs. Cliquer ensuite sur **Suivant**.



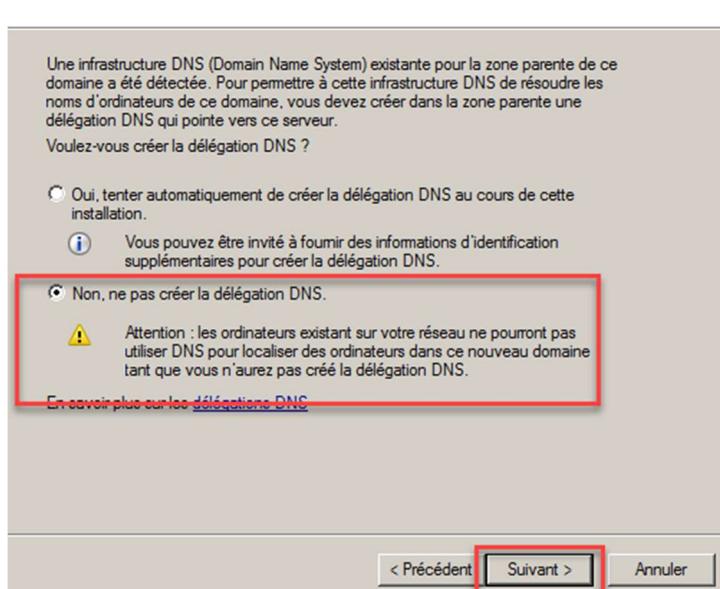
Serveur DNS, il est déjà coché vu que l'on a déjà installer et configurer le rôle DNS.

Le catalogue global permet de stocker l'ensemble des données du contrôleur de domaine, pour effectuer une recherche.

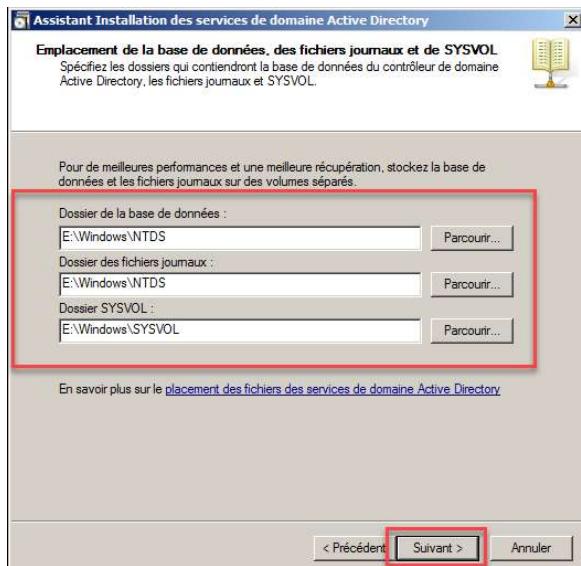
Contrôleur de domaine en lecture seule (RODC) permet une réPLICATION d'un contrôleur existante pour répliquer ses objets dans le but d'accélérer un accès local dans le cas où le serveur racine est distant. Seulement personne ne peut modifier sur le contrôleur de domaine en lecture seule. Cliquer sur **Suivant**



Cocher **Non, ne pas créer la délégation DNS**, vu que nous avons qu'un serveur contrôleur de domaine et pas de contrôleur de domaine enfant. Nous n'aurons pas besoin de délégation DNS. Cliquer ensuite sur **Suivant**.



Changer les chemins correspondants au disque dur prévu pour stocker nos données Active Directory.



Le dossier de la base de données : il contient la base stockant tous les objets.

Le dossier des fichiers journaux, stocke les journaux d'exploitations d'active directory.

Le dossier sysvol « system volume » sert à stocker les données qui doivent être répliquées entre les contrôleurs de domaine ou accessibles par les ordinateurs clients.

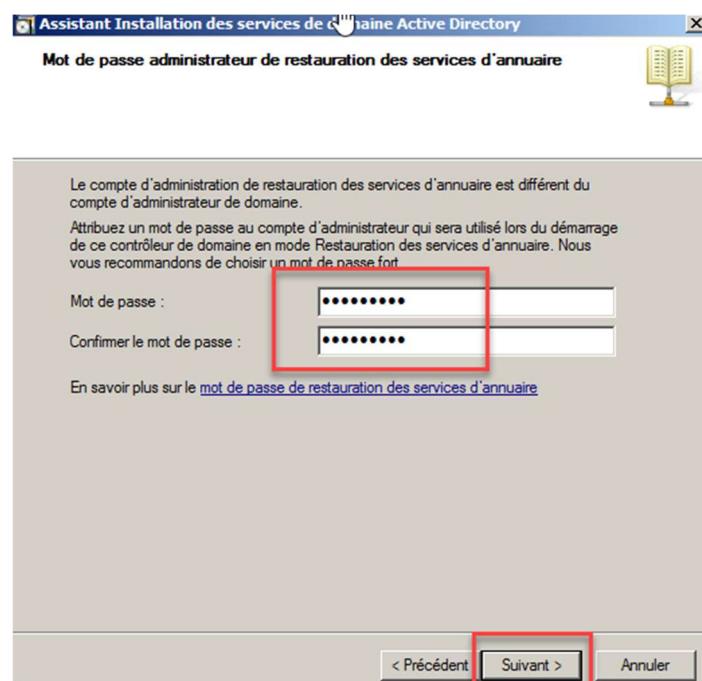
On trouve notamment les scripts de connexion et les stratégies de groupe (GPO).

Dans le dossier SYSVOL :

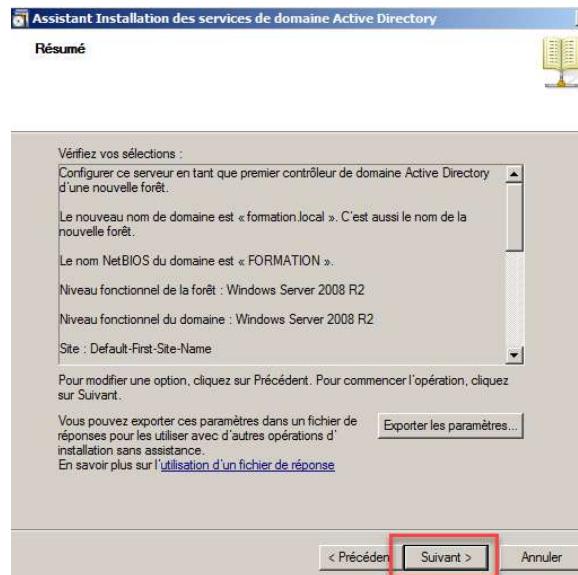
Domain : ce répertoire contient toutes les données à jour (GPO et scripts), réparties en deux sous dossiers : « Policies » et « scripts »

Polices : ce répertoire est stocké sous « domain », stocke toutes les GPOs du domaine. Un sous-dossier par GPO est créé où le nom du dossier correspond au GUID de l'objet GPO.

Cliquer sur **Suivant** une fois les changements effectués. Entrez le mot de passe qui permettra de désinstaller le contrôleur de domaine. Dans notre cas **Respons11**. Cliquer ensuite sur **Suivant**.



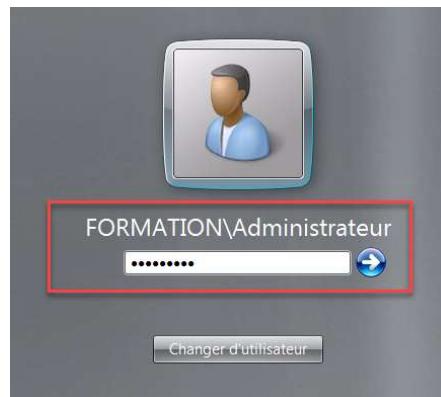
Cliquer ensuite sur **suivant** pour valider le récapitulatif.



Cocher **Redémarrer à la fin de l'opération**, une fois l'installation terminée le serveur redémarrera tout seul.

Un message d'avertissement concernant la présence d'un serveur DNS n'est pas une erreur, cliquer sur **OK**.

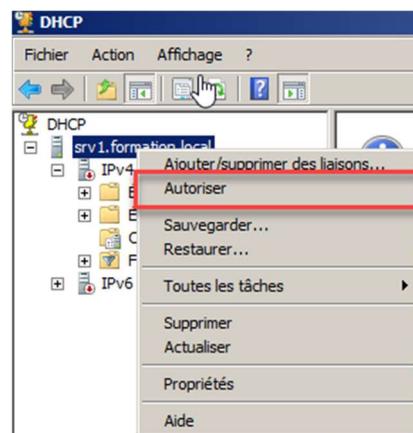
Une fois l'installation terminée, nous allons nous connecter en temps **qu'administrateur du contrôleur de domaine** et non plus **administrateur local**.



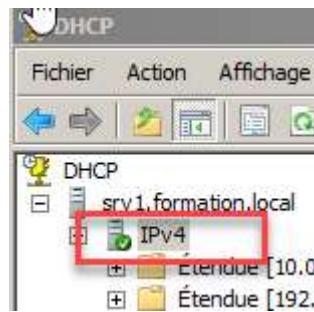
Le rôle DHCP avait été crée avec le compte **administrateur local**, nous avons basculer sur un domaine, il faut donc que **l'administrateur du domaine** l'autorise.

Ouvrir la console de gestion du rôle DHCP. Cliquer sur **srv1.formation.local**, faites un clic droit puis **Autoriser**.

Cliquer ensuite sur **Actualiser ou F5**.



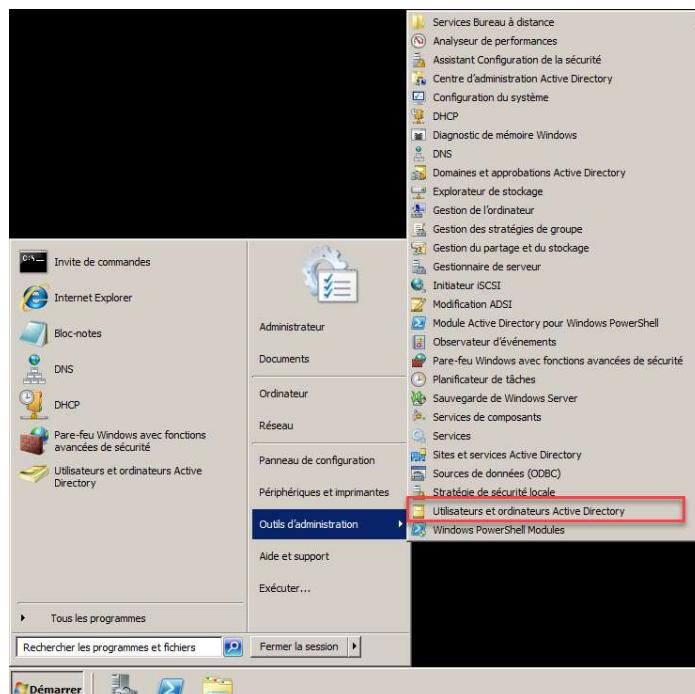
Rouge le service est éteint Vert il est actif



Gestion des utilisateurs

L'installation d'active directory à permis d'installer de nombreux outils de gestion. Ouvrez la console **Utilisateurs et ordinateurs Active Directory**.

Démarrer -> Tous les programmes -> Outils d'administrations -> Utilisateurs et ordinateurs Active Directory.



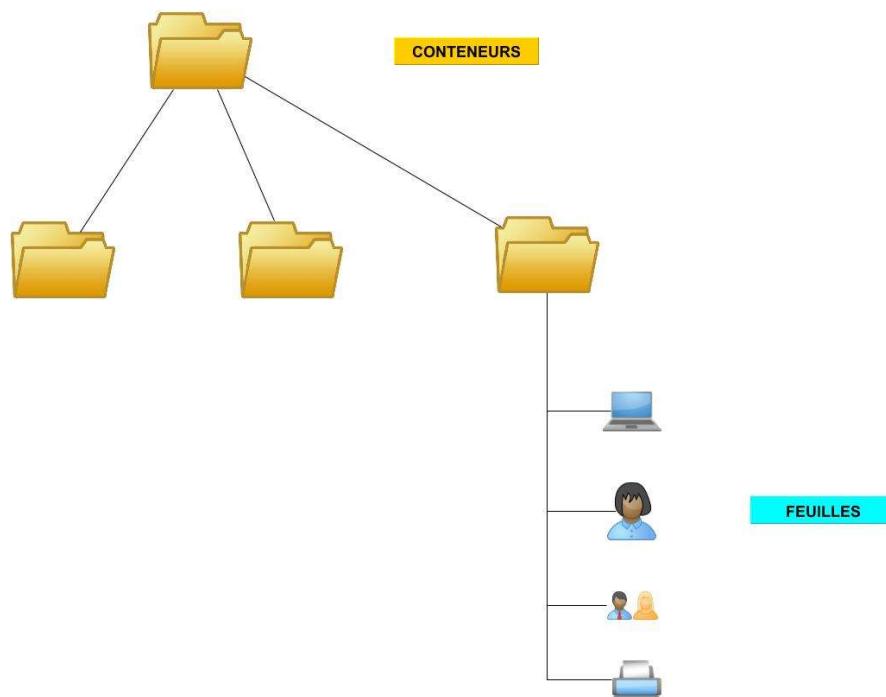
Dérouler **formation.local**.



STRUCTURE ACTIVE DIRECTORY

Les objets d'Active Directory (Utilisateurs, Groupes, Ordinateurs, etc.) correspondent à des classes, c'est-à-dire des catégories d'objets possédant les mêmes attributs. Ainsi un objet est une « instantiation » d'une classe d'objet, c'est-à-dire un ensemble d'attributs avec des valeurs particulières.

Lorsqu'un objet contient d'autres objets, on le qualifie de **conteneur**. Les conteneurs permettent de regrouper les objets dans une optique d'organisation. A l'inverse si l'objet est au plus bas niveau de la hiérarchie, il est qualifié de **feuille**. Il existe par défaut déjà des **unités d'organisation ou OU**.



La hiérarchie composée de l'ensemble des conteneurs (noeuds) et des feuilles est appelée **arbre**.

La notion d'arbre est étroitement liée à la notion de domaine, permettant de circonscrire des ressources informatiques dans un même périmètre de sécurité.

Voici les conteneurs présents d'origine :

Built-in : Ce sont des groupes qui permettent d'assigner des autorisations d'administration, ou de gestion de la sécurité. Leur étendue est toujours de type local.

Computers : C'est le conteneur par défaut pour les ordinateurs intégrés au domaine.

Domain Controllers : C'est le conteneur qui stocke les contrôleurs de domaine en tant qu'objet active directory

ForeignSecurityPrincipals : Ce conteneur liste les domaines approuvés par une relation d'approbation entre deux ou plusieurs forêts.

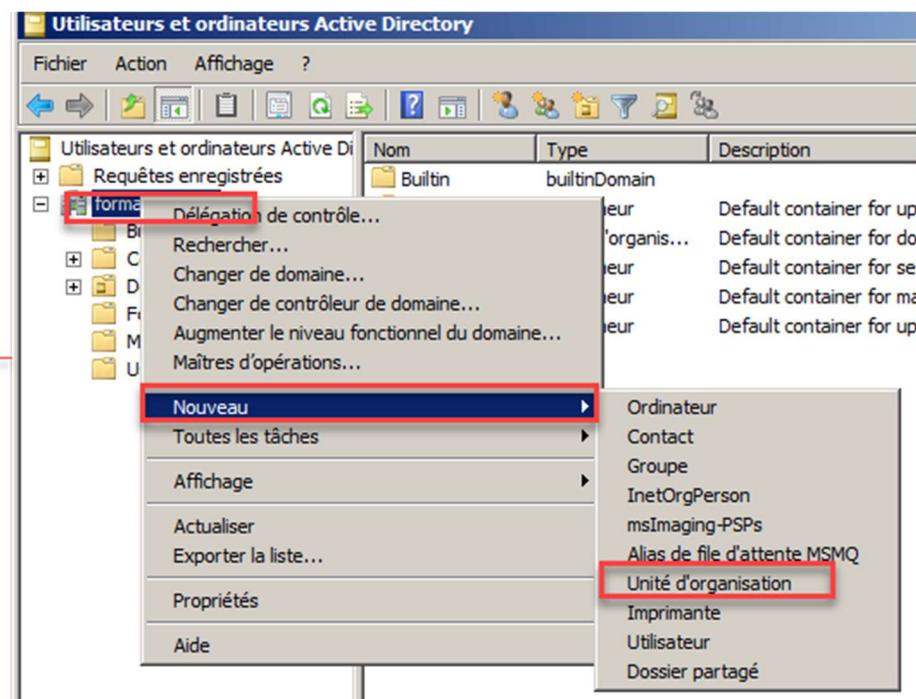
Managed Service Accounts : C'est un nouveau conteneur qui force le changement de mot de passe des utilisateurs placés dans cette unité d'organisation tous les 30 jours.

Users : Conteneur stockant par défaut les comptes utilisateurs.

Création d'une structure personnalisée :

Aller dans la console gestion **utilisateurs et ordinateurs active directory**.

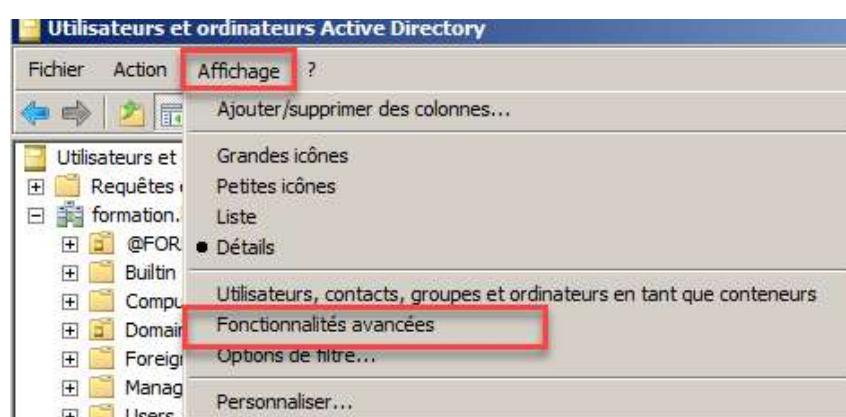
Clic droit sur **formation.local**, puis clic simple sur **nouveau** et enfin **Unité d'organisation**.



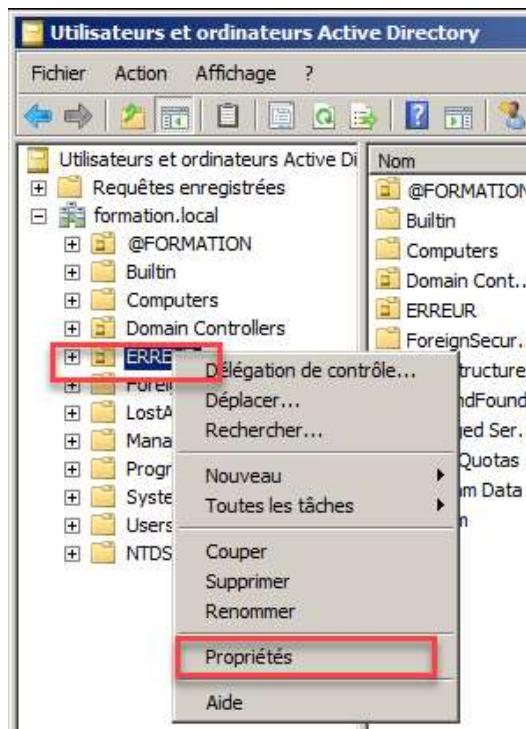
Renseigner le nom **@formation**, l'arobase permet de faire monter l'ou tout en haut de la liste des ou. Laisser cocher la protection contre la suppression accidentelle. Cliquer ensuite sur **OK**.



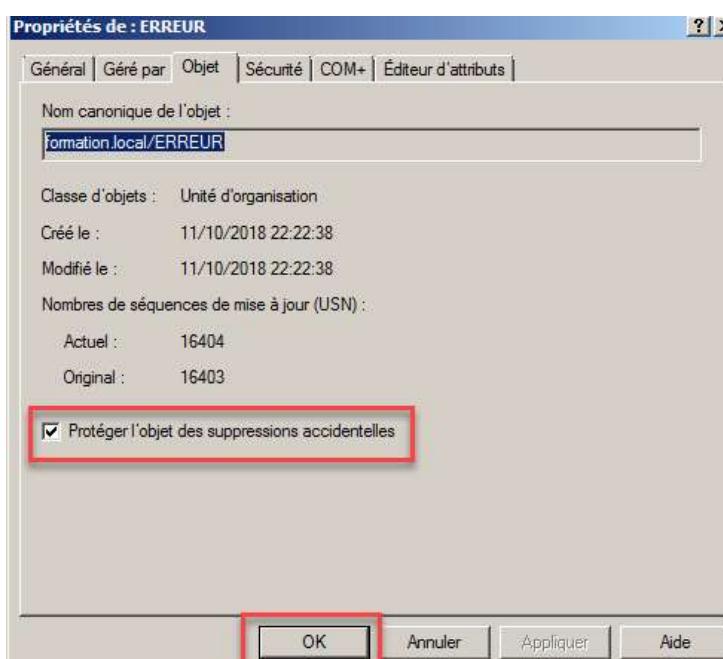
En cas d'erreur de saisi, pour retirer la protection contre la suppression accidentelle. Cliquer sur **Affichage** et **Fonctionnalités avancées**.



La structure des OU est plus fournis. Faire un clic droit sur l'ou à renommer ou supprimer.

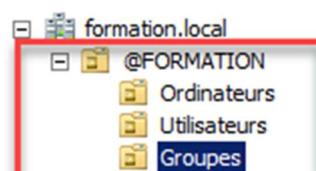


Cliquer sur l'onglet **Objet**, puis décocher **Protéger l'objet des suppressions accidentelles**. Cliquer ensuite sur **OK**.



Une fois la modification effectuer, penser à décocher l'affichage des fonctionnalités avancées.

Crée trois OU dans l'OU @formation.



L'OU « ordinateurs » permettra de stocker les ordinateurs du services formations.

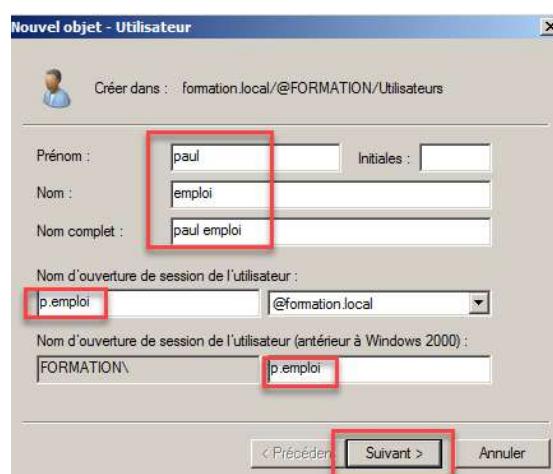
L'OU « groupes » permettra de stocker les groupes du services formations.

L'OU « utilisateurs » permettra de stocker les utilisateurs du services formations.

Création des comptes utilisateurs

Aller dans l'OU « utilisateurs », faites un clic droit **Nouveau et Utilisateur**.

Renseigner la fiche de l'utilisateur, puis cliquer sur **suivant**. Le nom d'ouverture de session de l'utilisateur est important pour l'utilisateur pour ouvrir sa session.



Entrer un mot de passe fort : **Azerty11**, dès que l'utilisateur se connectera pour la première fois, il devra choisir un nouveau mot de passe. Cliquer sur **Suivant et Terminer**.

Créer ensuite les utilisateurs présents dans la capture d'écran.

Nom	Type
john attends	Utilisateur
justine ptiteg...	Utilisateur
paul emploi	Utilisateur
sam soul	Utilisateur

Création de groupe

L'utilisation d'un objet **groupe** permet d'affecter une stratégie ou un accès à l'ensemble des utilisateurs présents dans ce groupe. Les groupes peuvent avoir une portée différente. Relisez cette partie [ici](#).

Aller dans **groupes** puis **Nouveau** et enfin **Groupe**.

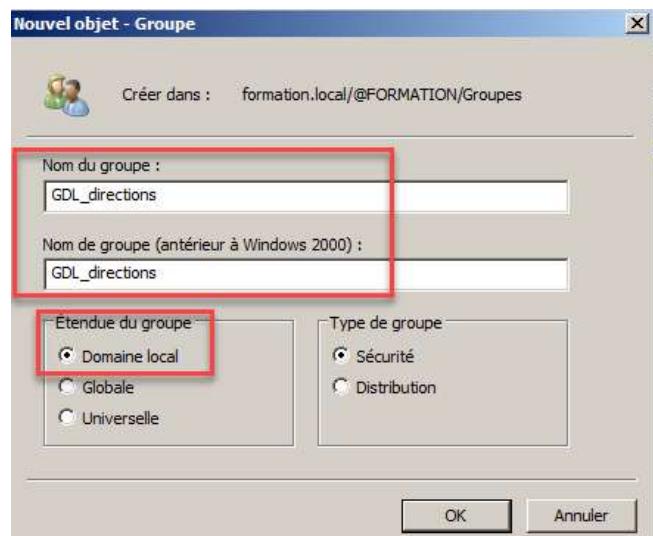


Deux types de groupes :

Groupes de distribution : permet d'utiliser un groupe pour l'appliquer à un serveur de messagerie.

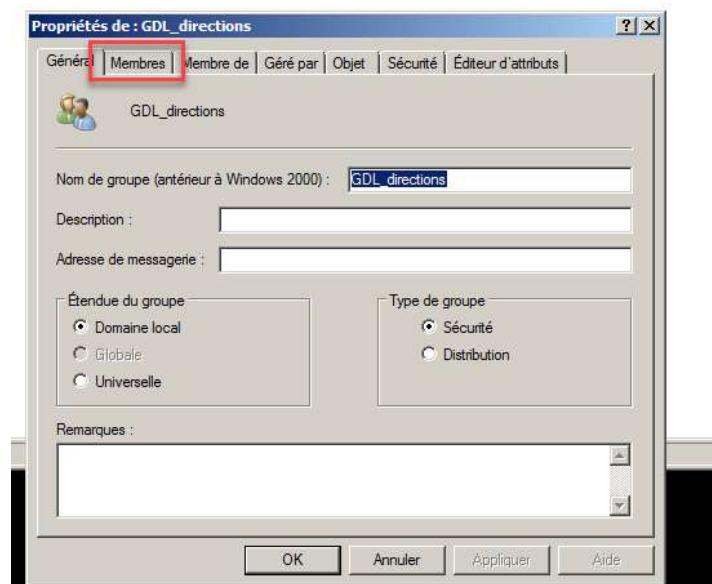
Groupes de sécurité : permet d'affecter des droits d'accès (ACL = access control list) sur un répertoire.

Dans notre cas ce sera uniquement des **groupes de sécurités**. Suivez l'exemple avec la capture d'écran. Cliquer sur **OK** pour valider. Notre groupe sera visible uniquement sur ce contrôleur et non pas sur la forêt. Le nommage permet d'avoir une information sur la portée du groupe.

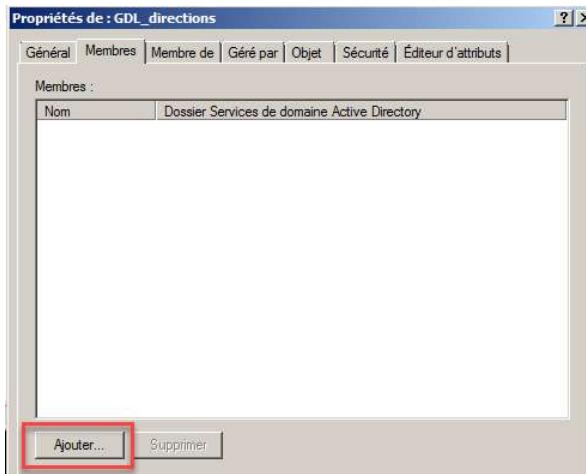


Double clic sur le groupe, puis dans l'onglet **membre**.

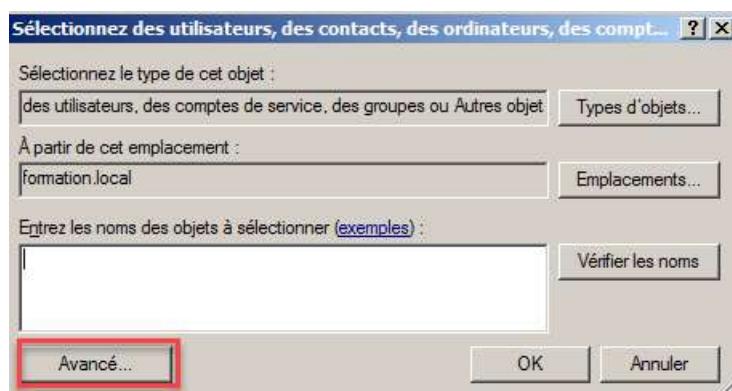
Nom	Type	Description
GDL_directions	Groupe de sécu...	



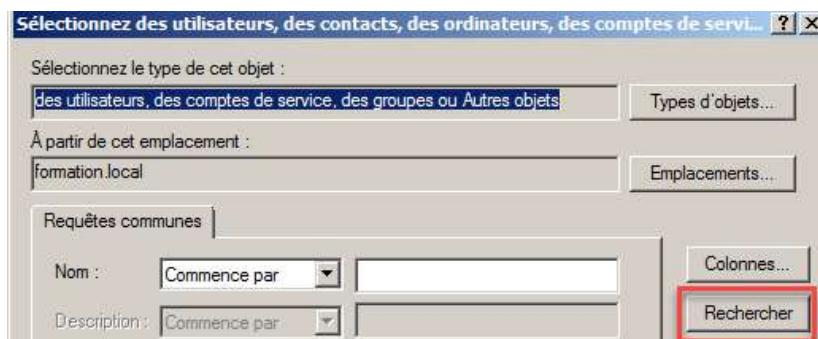
Cliquez sur **Ajouter**.



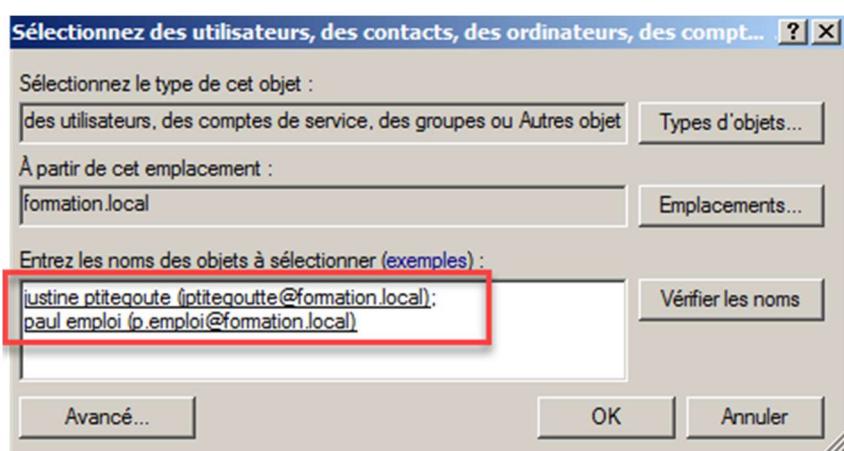
Cliquer sur **Avancé**.



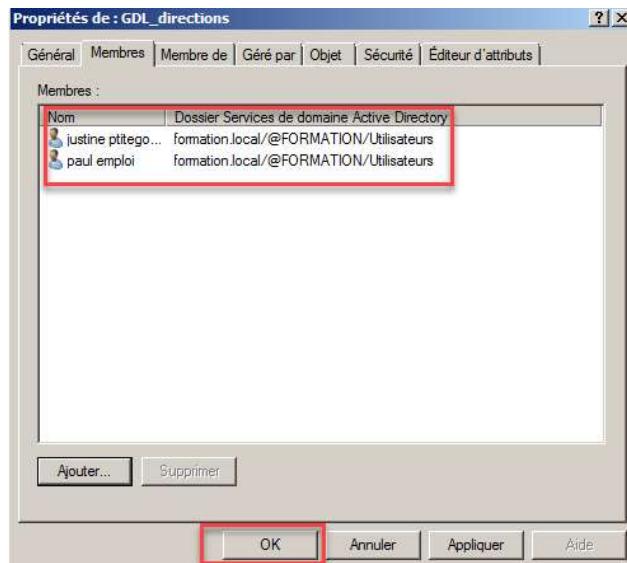
Cliquer sur **Rechercher** pour afficher l'ensembles des objets active directory (groupes ou utilisateurs)



Sélectionner **paul emploi** et **justine ptitegoutte** et valider avec **OK**. Nous voyons bien les deux utilisateurs dans les objets selectionner. Cliquer sur **OK**.



Les deux utilisateurs apparaissent en maintenant dans les membres du groupe, cliquer sur **OK**.



DOSSIER PARTAGES

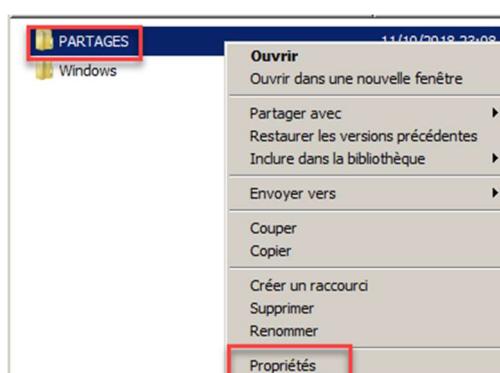
Une fois la structure des utilisateurs et groupes, nous allons procéder à la création d'un répertoire accessible par l'utilisateur sur son poste de travail depuis le réseau.

Création de la structure de partage.

Aller dans l'explorateur de fichier, dans le disque E. crée la structure suivante.



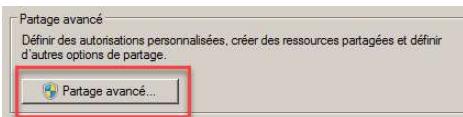
Nous allons mettre en place le partage Windows. Il va permettre de rendre visible le dossier **PARTAGES** du serveur par le réseau sur les utilisateurs de notre domaine. Sélectionner le dossier **PARTAGES** et faites un clic droit **Propriétés**.



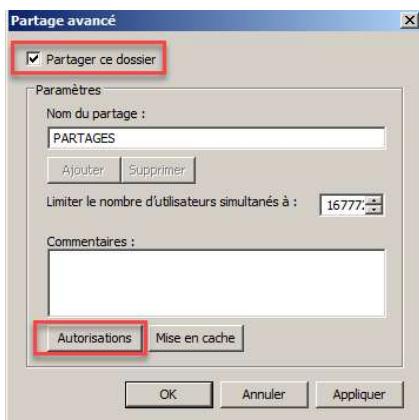
Ensuite cliquer sur l'onglet **Partage**.



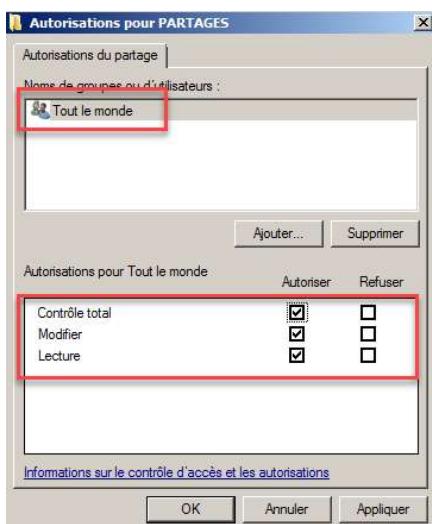
Cliquer sur **Partage avancé**.



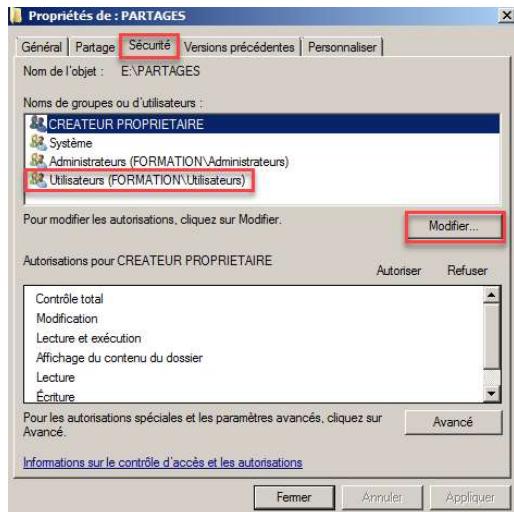
Cocher **Partager ce dossier** puis cliquer sur **Autorisations**.



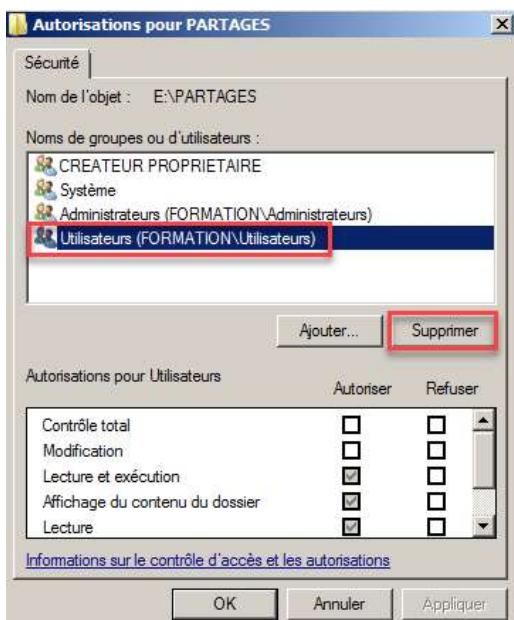
Cocher les **Autorisations : Contrôle total** pour le groupe Tout le monde. Ne vous inquiétez pas nous spécifierons les droits de façon plus précises dans l'onglet **sécurité** qui à la priorité sur l'onglet **Partages**. Cliquer sur **OK**, une fois le contrôle total cocher.



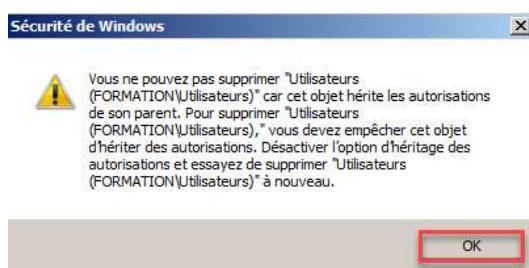
Cliquer ensuite sur **OK** puis sur l'onglet sécurité. Cliquer sur **Modifier** et sélectionner le groupe **Utilisateurs**.



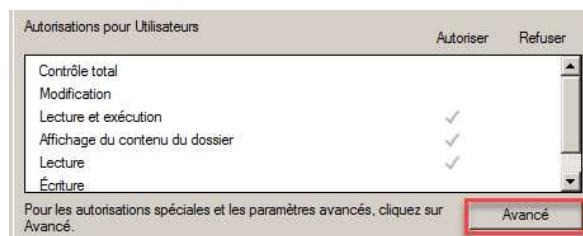
Cliquer sur **Supprimer**.



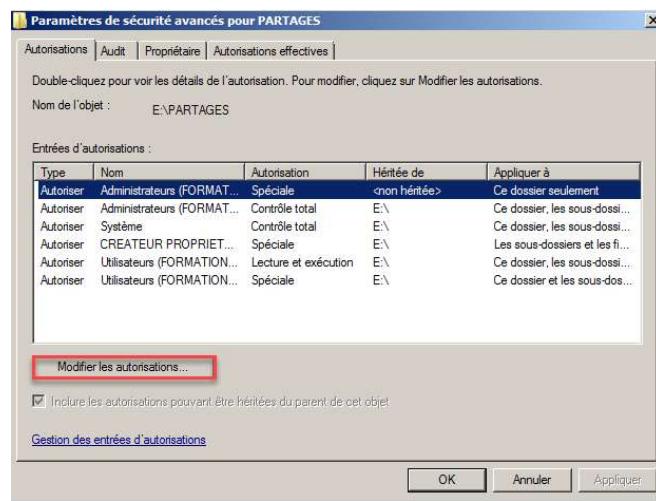
Nous ne pouvons pas supprimer le groupe **Utilisateurs**, il hérite des droits du dossier parents. Cliquer sur **OK**.



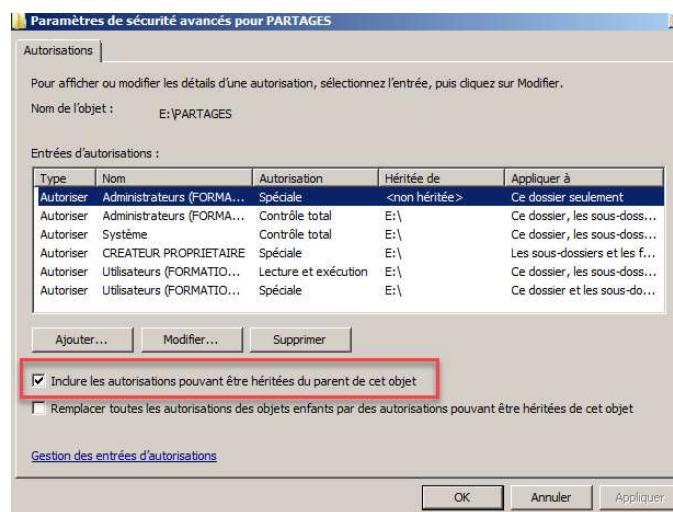
Cliquer ensuite sur **OK**, puis sur **Avancé**.



Cliquer sur **Modifier les autorisations**.



Décocher **Inclure les autorisations pouvant être héritées du parent de cet objet.**



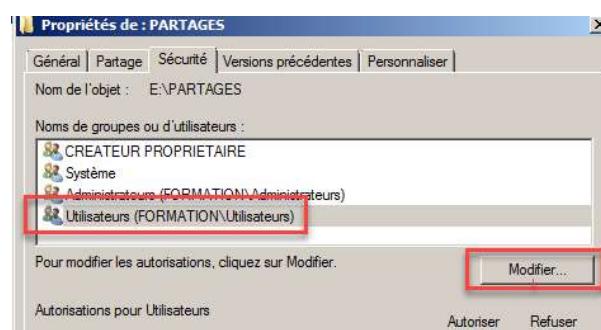
Trois choix apparaissent :

Ajouter, il permet de modifier manuellement les permissions déjà existantes.

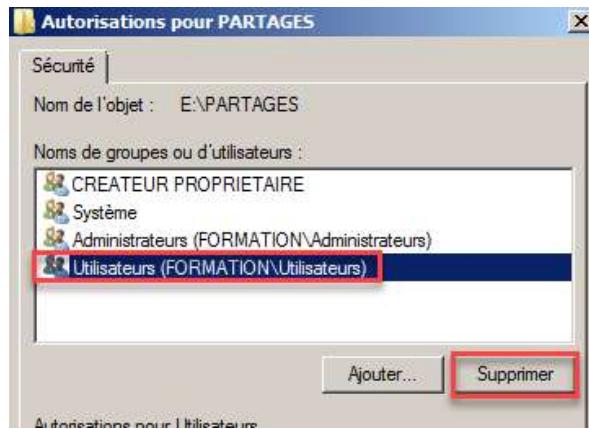
Supprimer, supprime toutes les autorisations déjà présentes dans l'onglet sécurité.

Annuler, si nous voulons annuler la demande de modification d'héritage.

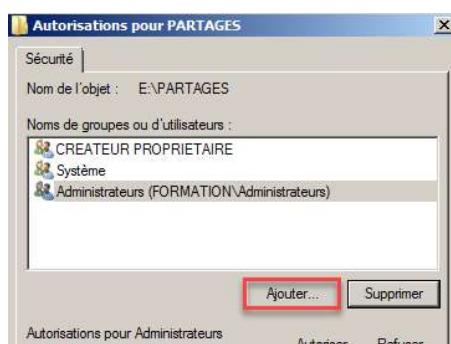
Cliquer sur **Ajouter** et cliquer sur **Appliquer**. Cliquer sur **OK**. Sélectionner le groupe **Utilisateurs** et cliquer sur **Modifier**.



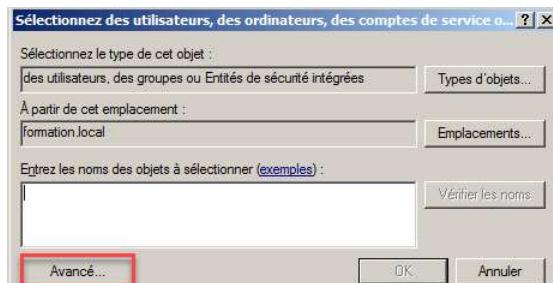
Sélectionner **Utilisateurs** et cliquer sur **Supprimer**.



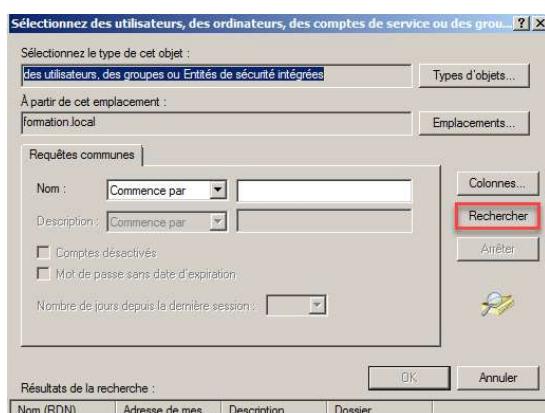
Cliquer sur Ajouter.



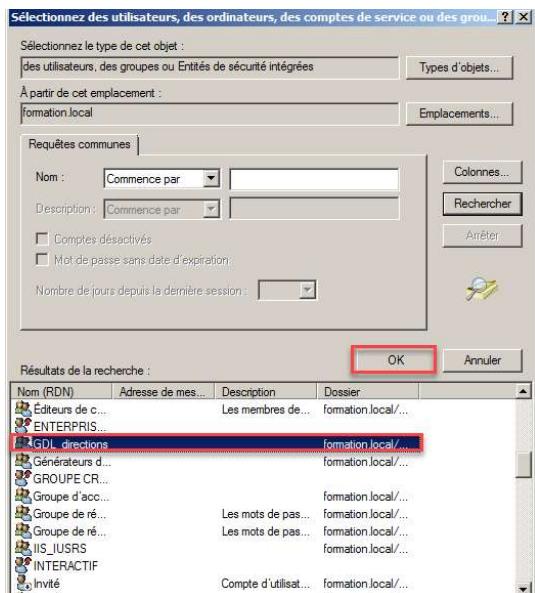
Cliquer sur Avancés.



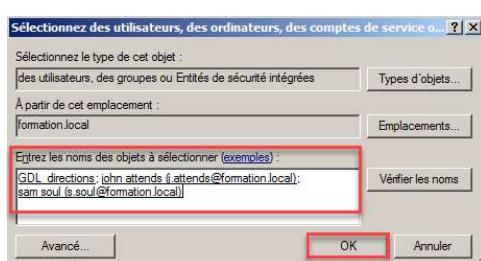
Cliquer sur Rechercher pour rechercher les utilisateurs.



Selectionner : le groupe **GDL_directions** et les utilisateurs **sam soul** et **john attends**, cliquer ensuite sur **OK**.



Cliquez sur OK.



Attribution des droits :

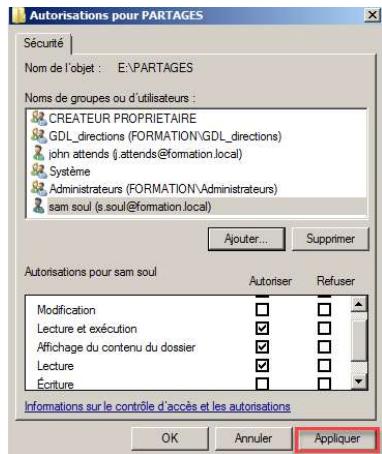
GDL directions : Lecture et exécution

John attends : Lecture et exécution

Sam soul : Lecture et exécution

Différences entre les droits :

Cliquer sur **Appliquer** et **OK** pour valider les droits par défaut.



Cliquer sur **Fermer**. Entrer dans le dossier **PARTAGES**. Faites un clic droit Propriété sur le répertoire **COMMUNS**. NE PAS ALLER DANS L'ONGLET PARTAGES. Cliquer plutôt sur l'onglet **Sécurité**. Puis **Modifier**.

Cocher les droits suivants en fonction des objets :

Objets Active Directory	Contrôle total	Modification	Lecture et exécution	Affichage du contenu du dossier	Lecture	Ecriture
GDL_directions	X	X	X	X	X	X
Sam soul			X	X	X	X
John attends			X	X	X	X

Cliquer ensuite sur **OK**. Pour le dossier **DIRECTION**, il faut retirer les droits hérités en allant dans le menu **avancé** et décocher **Inclure les autorisations pouvant être héritées du parent de cet objet**.

Respecter les droits suivants. Pour configurer pas d'accès, soit on refuse les accès ou alors on les retire de la liste. La deuxième option est la meilleure et la plus sûre.

Objets Active Directory	Contrôle total	Modification	Lecture et exécution	Affichage du contenu du dossier	Lecture	Ecriture	Pas d'accès
GDL_directions			X	X	X		
Sam soul							X
John attends							X

Cliquer sur **Fermer**. Entrer dans le dossier **COMMUNS** du dossier **DIRECTIONS**. Faites un clic droit Propriété sur le répertoire **COMMUNS**. NE PAS ALLER DANS L'ONGLET PARTAGES. Cliquer plutôt sur l'onglet **Sécurité**. Puis **Modifier**.

Cliquer ensuite sur **OK**. Pour le dossier **DIRECTION/COMMUNS**, il faut retirer les droits hérités en allant dans le menu **avancé** et décocher **Inclure les autorisations pouvant être héritées du parent de cet objet**.

Respecter les droits suivants. Pour configurer pas d'accès, soit on refuse les accès ou alors on les retire de la liste.

Objets Active Directory	Contrôle total	Modification	Lecture et exécution	Affichage du contenu du dossier	Lecture	Ecriture	Pas d'accès
GDL_directions							X
Sam soul							X
John attends							X
Paul Emploi			X	X	X	X	
Justine ptitegoutte			X	X	X	X	

Cliquer sur **Fermer**. Faites un clic droit Propriété sur le répertoire **JPETITEGOUTTE**. NE PAS ALLER DANS L'ONGLET PARTAGES. Cliquer plutôt sur l'onglet Sécurité. Puis Modifier.

Cliquer ensuite sur **OK**. Pour le dossier **JPETITEGOUTTE**, il faut retirer les droits hérités en allant dans le menu avancé et décocher **Inclure les autorisations pouvant être héritées du parent de cet objet**.

Respecter les droits suivants. Pour configurer pas d'accès, soit on refuse les accès ou alors on les retire de la liste.

Objets Active Directory	Contrôle total	Modification	Lecture et exécution	Affichage du contenu du dossier	Lecture	Ecriture	Pas d'accès
GDL_directions							X
Sam soul							X
John attends							X
Paul Emploi							X
Justine ptitegoutte	X	X	X	X	X	X	

Cliquer sur **Fermer**. Faites un clic droit Propriété sur le répertoire **PEMPLOI**. NE PAS ALLER DANS L'ONGLET PARTAGES. Cliquer plutôt sur l'onglet Sécurité. Puis Modifier.

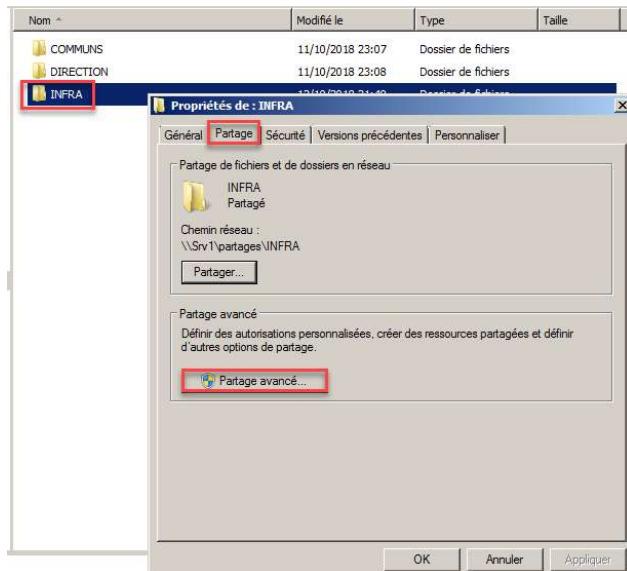
Cliquer ensuite sur **OK**. Pour le dossier **PEMPLOI**, il faut retirer les droits hérités en allant dans le menu avancé et décocher **Inclure les autorisations pouvant être héritées du parent de cet objet**.

Respecter les droits suivants. Pour configurer pas d'accès, soit on refuse les accès ou alors on les retire de la liste.

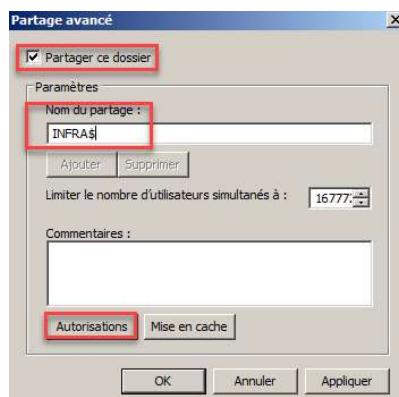
Objets Active Directory	Contrôle total	Modification	Lecture et exécution	Affichage du contenu du dossier	Lecture	Ecriture	Pas d'accès
GDL_directions							X
Sam soul							X
John attends							X
Paul Emploi	X	X	X	X	X	X	
Justine ptitegoutte							X

Nous allons rajouter un partage caché dans le dossier **PARTAGES**.

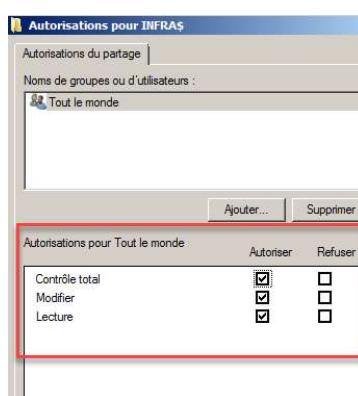
Crée un nouveau dossier à la racine du **disque E**, nommé le « **INFRA** », faites un clic droit **Propriétés**, aller dans l'onglet **PARTAGE**, puis **Partages avancés**.



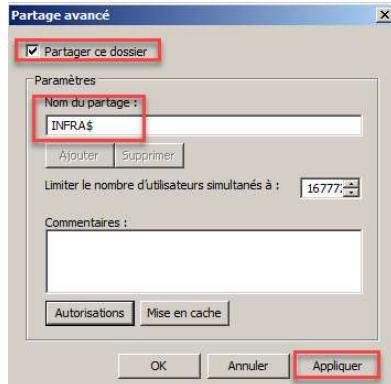
Cocher **Partager ce dossier**, puis dans Paramètres : **INFRA\$**, le fait de mettre un signe « \$ » permet de cacher le partage.



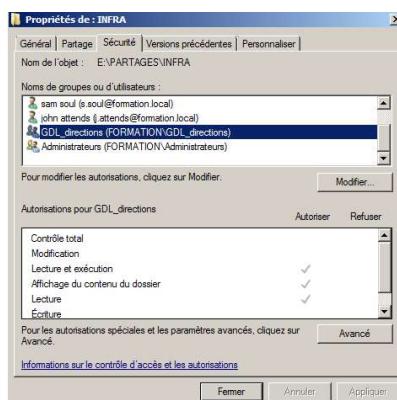
Cocher le contrôle total pour le groupe **Tout le monde**. Cliquer sur **OK**.



Cliquer sur **OK**.



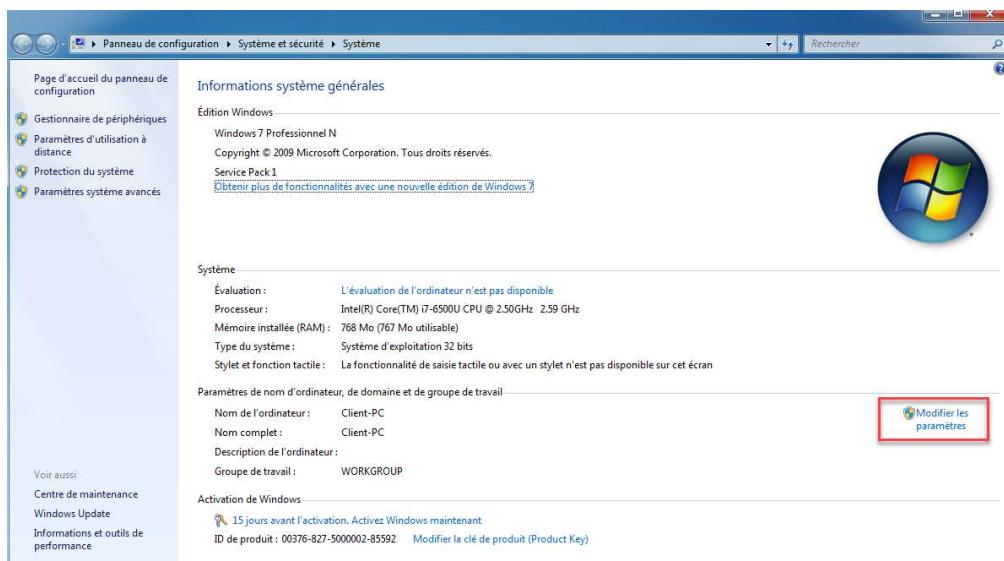
Vérification des autorisations dans l'onglet sécurité. Les quatre membres doivent avoir le droit de lecture et execution.



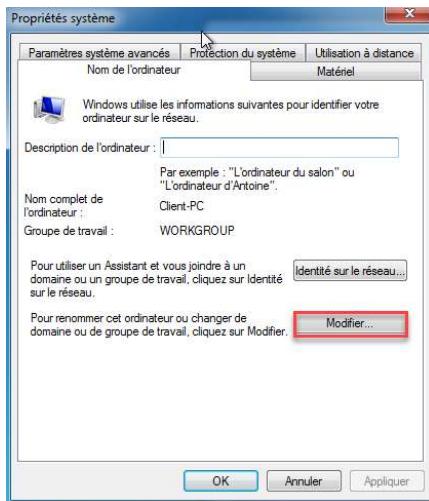
Connexion d'un poste client au domaine Active Directory.

Prenez un poste client et connecter le au domaine. Mettez le poste client sur le LAN 192.168.1.

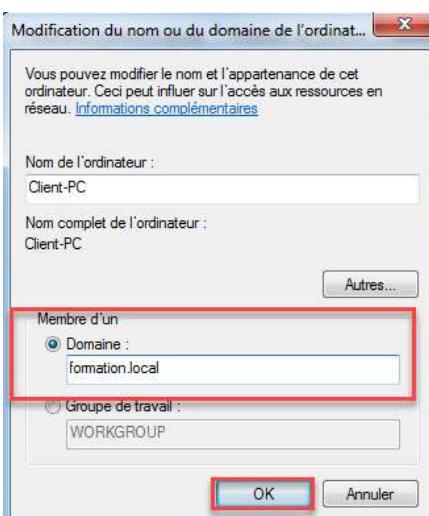
Aller dans les **Propriété système** puis cliquer sur **Modifier les paramètres**.



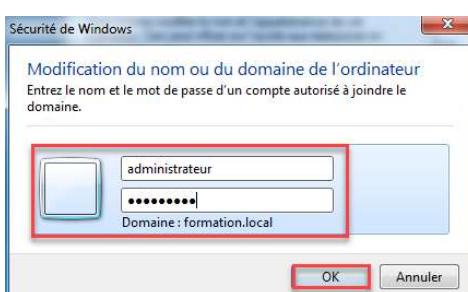
Cliquez sur **Modifier**.



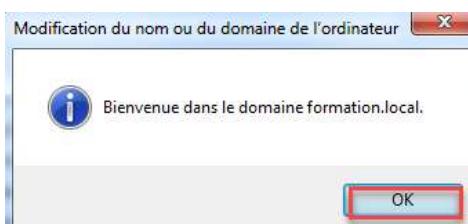
Cocher **Domaine** puis entrer le nom du domaine **formation.local**. Cliquer sur **OK**.



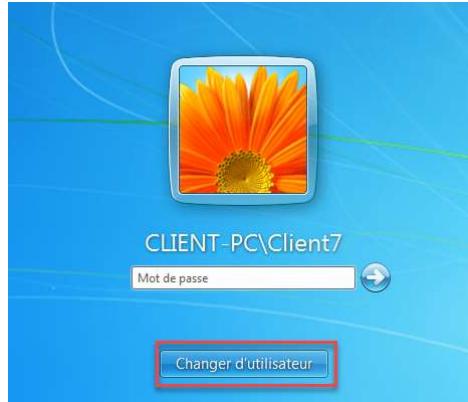
Entrer les identifiant et le mot de passe **Administrateur du domaine**.



Cliquer sur **OK**.



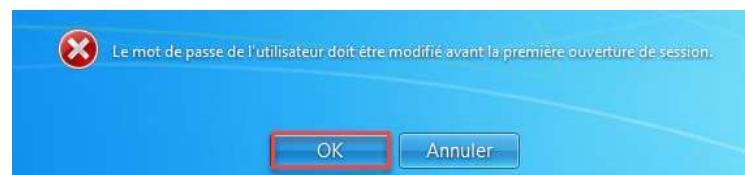
Redémarrer l'ordinateur. Cliquer sur **Changer d'utilisateur**. Utiliser un des comptes de la direction.



Cliquer sur **Autre utilisateur**. Entrer le l'identifiant, **p.emploi** et son mot de passe **Azerty11**. Cliquer sur la flèche pour valider.



Le mot de passe de l'utilisateur doit être modifié avant la première ouverture de session. Cliquer sur **OK**.



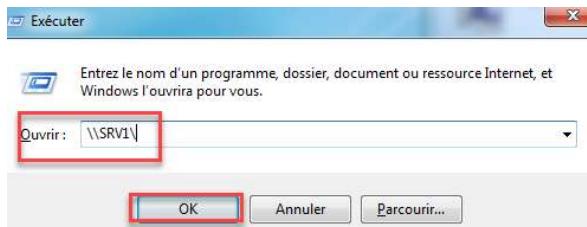
Entrer le nouveau mot de passe : Azerty12. Valider.



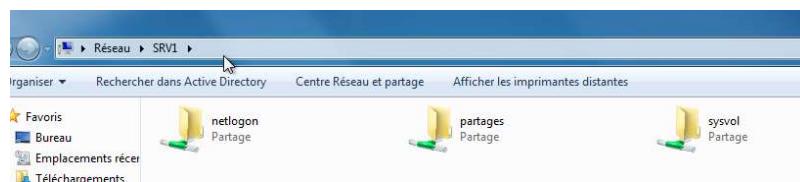
Cliquer sur **OK**.



Appuyez sur **Windows** et la touche **R** simultanément. La fenêtre exécuter s'ouvre. Entrer l'adresse suivante.

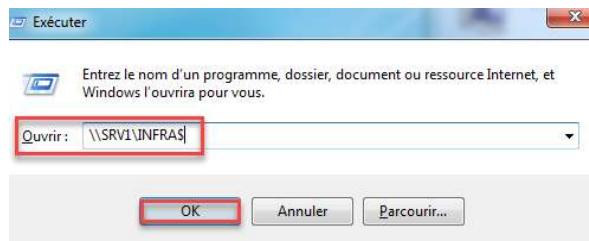


Voilà les accès que vous devez avoir.

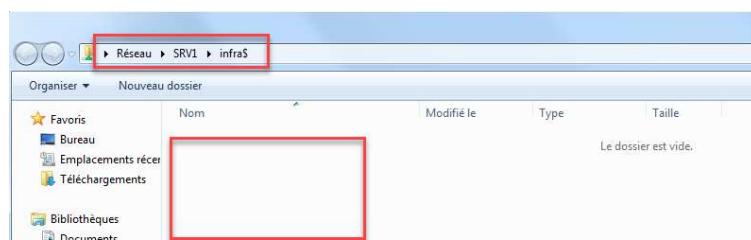


On ne voit pas le dossier **INFRA\$** vu qu'il est caché.

Pour le faire apparaître entrer le chemin suivant et cliquer sur **OK**.



Nous y avons maintenant accès, même s'il est vide pour le moment.



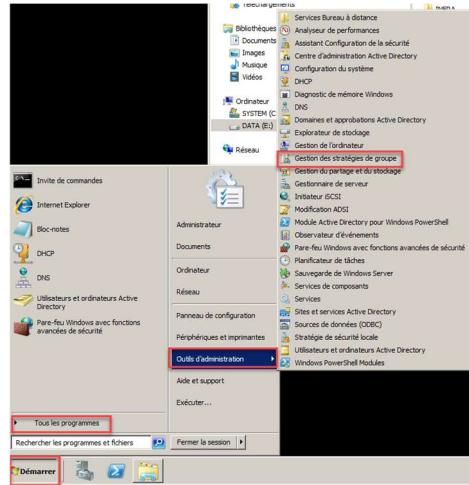
GPO [GROUP POLICY OBJECT]

Les Group Policy Object appelé GPO est un ensemble de stratégie de sécurité permissive ou restrictive pouvant être appliquée à un utilisateur ou un groupe d'utilisateur ou aux ordinateurs. Les GPO sont appelé **Gestion de stratégie de groupe**. Elles assurent la gestion des utilisateurs, des groupes et des unités d'organisationnelles. Nous pouvons aussi bien effectuer des restrictions d'accès à des modules sur le poste de l'utilisateur que d'installer ou mettre à jour des applications sur son ordinateur.

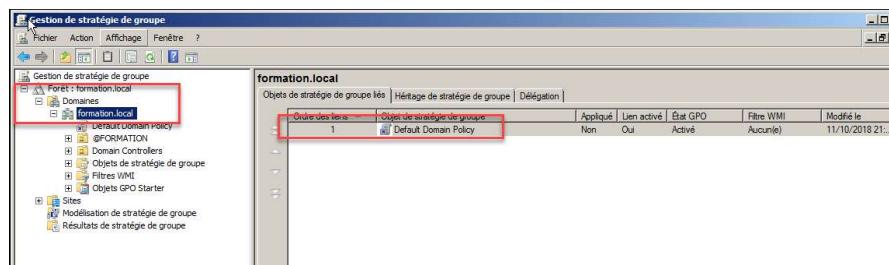
Exemples de GPO

Stratégie par défaut

Aller dans Démarrer -> Tous les programmes -> Outils d'administration -> Gestion des stratégies de groupe.



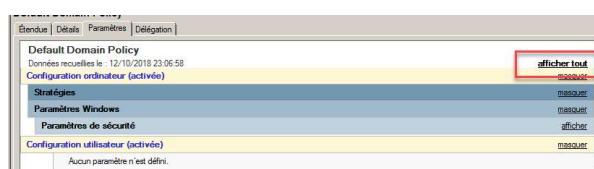
Dérouler la forêt : **formation.local** puis **Domaines** et ensuite **formation.local**. On peut voir qu'il existe déjà une GPO par défaut.



Double clic sur **Default Domain Policy**. Cliquer sur **OK**. Cliquer sur l'onglet **Paramètres**, puis **Ajouter** et encore **Ajouter** et Fermer.



Cliquer sur **afficher tout**.

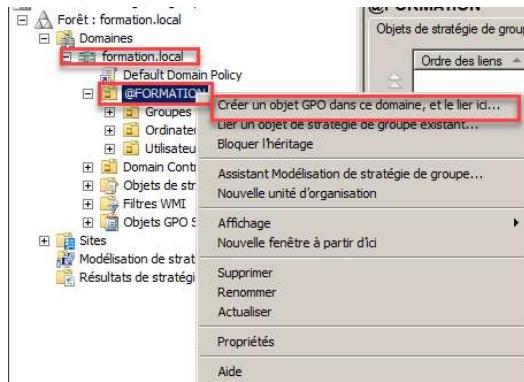


Voici la stratégie par défaut pour la gestion des comptes et mot de passe.

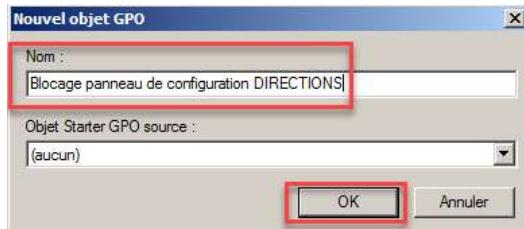
Blocage d'accès au panneau de configuration

Maintenant nous allons mettre en place une **GPO** permettant de **bloquer l'accès au panneau de configuration pour le groupe GDL_Directions**.

Dans le menu de gauche dérouler **@FORMATION**, faites un clic droit et cliquer sur **Créer un objet GPO dans ce domaine et le lier ici...**



Nommer l'objet **GPO** comme sur la capture d'écran ci-dessous et cliquer sur **OK**.



Faites un clic droit sur la **GPO**, et cliquer sur **Modifier**. La **GPO** doit s'appliquer à l'utilisateur et non à l'ordinateur vu qu'elle cible un groupe spécifique d'utilisateurs.

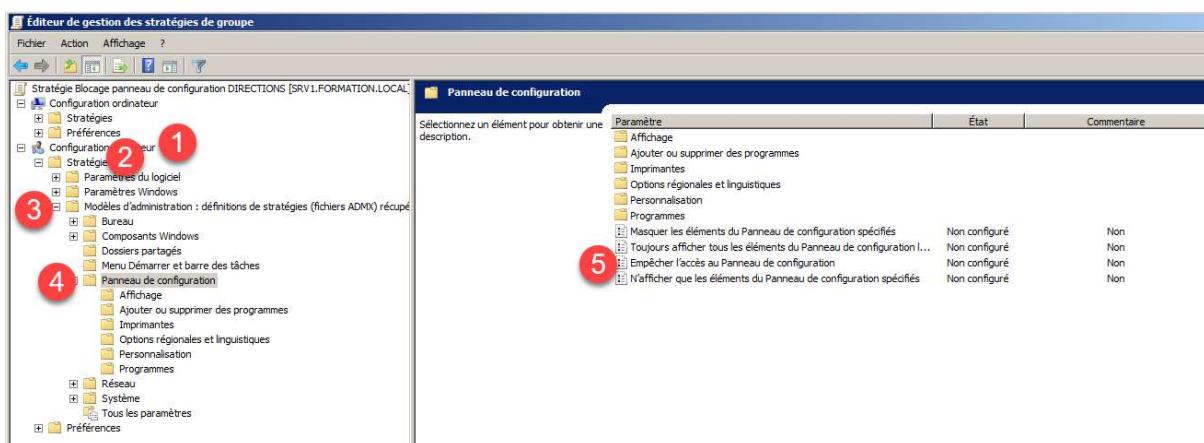
1 – dérouler **configuration utilisateur**

2 – dérouler **stratégies**

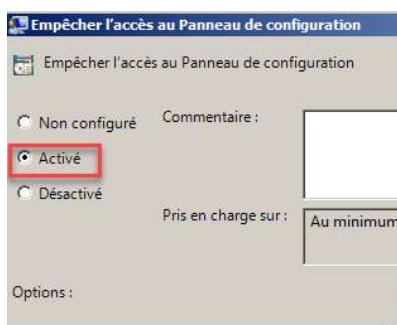
3 - dérouler **Modèles d'administration : définition de stratégies**

4- cliquer sur **panneau de configuration**

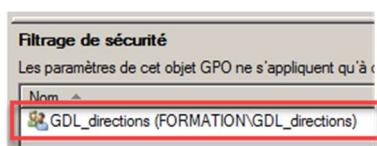
5- double clic sur Empêcher l'accès au panneau de configuration.



Cocher Activer et cliquer sur OK. Vous pouvez fermer la fenêtre d'éditions des stratégies de groupe.



Nous devons modifier les utilisateurs ciblés. Par défaut, c'est tous les **utilisateurs authentifiés** de l'unité organisationnelle qui sont ciblées. Dans l'onglet **Etendue** puis dans le panneau **filtrage de sécurité**, supprimer les **Utilisateurs authentifiés** et ajouter le groupe de domaine local **Directions** comme ci-dessous.



Mise à jour de la GPO sur le poste client

Par défaut les mises à jour se font à l'ouverture de session ou au redémarrage de l'ordinateur. Il existe une commande qui permet de forcer la mise à jour des stratégies de groupes.

Dans l'invite de commande taper la commande **GPUPDATE /FORCE**.

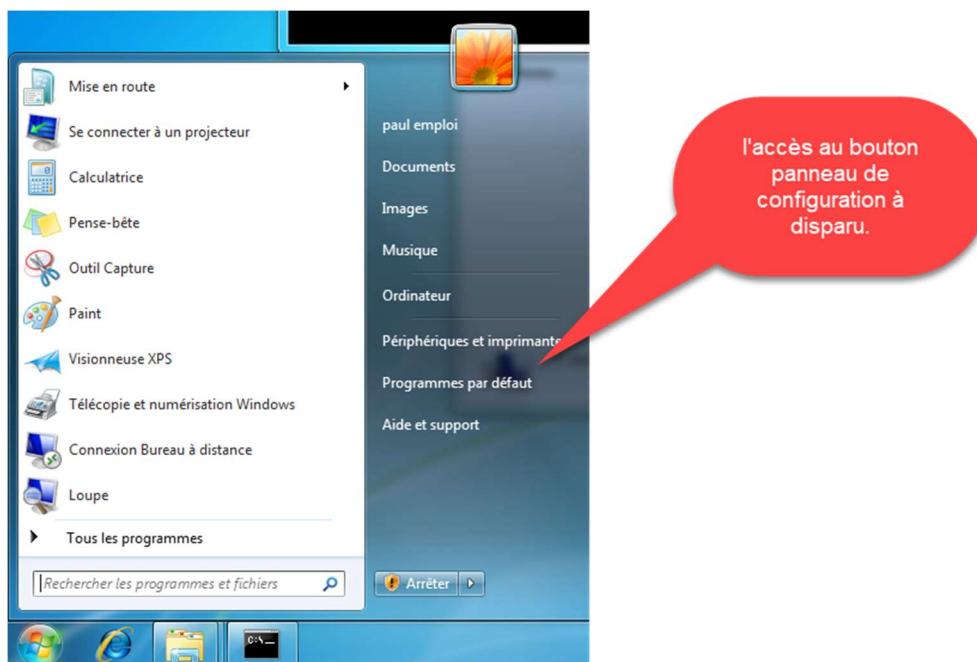
```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Tous droits réservés.

C:\Users\p.emploi>GPUPDATE /FORCE
```

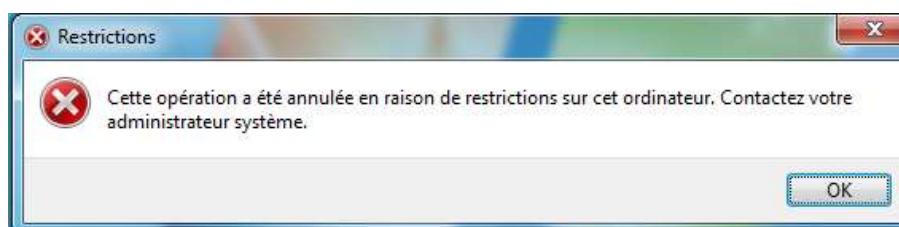
La GPO est appliquée. Selon les GPOs, il faut parfois se déconnecter pour valider sa prise en compte. Dans notre cas, aucune déconnection n'est nécessaire.

```
C:\>GPUPDATE /FORCE  
Mise à jour de la stratégie...  
La mise à jour de la stratégie utilisateur s'est terminée sans erreur.  
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.  
C:\>
```

Vérification de l'application de la GPO.



Essai avec un raccourci clavier **Windows + Pause**.



L'accès est interdit en raison d'une stratégie de groupe. Tous les modules de gestion présents dans le panneau de configuration sont maintenant bloqués.

Lancement des lecteurs réseaux à l'ouverture de session des utilisateurs

Cette GPO permettra aux utilisateurs d'avoir leur lecteur réseau qui se connectent à l'ouverture de session de leur système. En cas de déconnecter ou suppression accidentelle, cette GPO permettra de résoudre ce dysfonctionnement en relançant la session de l'utilisateur.

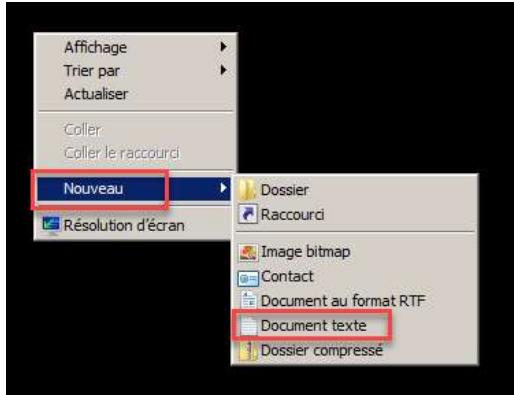
Elle peut être faite de deux façons :

- Avec un script d'ouverture de session
- Avec le mappage de lecteur

Script d'ouverture de session

Création du script sur le serveur avec un éditeur de texte.

Sur le **bureau** faites un clic droit sur le bureau puis cliquer sur **Nouveau**, puis clic simple sur **Document texte**.



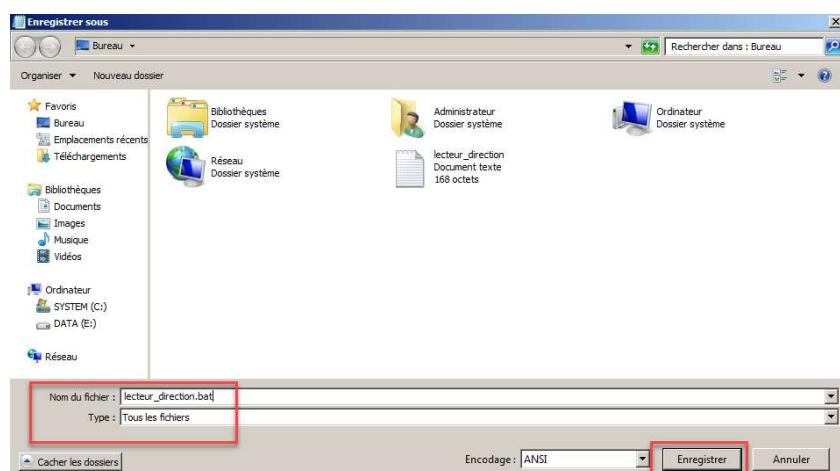
Entrer le nom du script par exemple lecteur_direction.

```

@ECHO OFF
NET USE DEL * /delete /y
NET USE Z: \\SRV1\PARTAGES\COMMUNS
NET USE Y: \\SRV1\PARTAGES\DIRECTORIE\COMMUNS
NET USE X: \\SRV1\PARTAGES\DIRECTORIE\%username%

```

Ensuite cliquer sur **Enregister sous** pour sauvegarder le fichier. Cliquer sur le type, sélectionner **Tous les fichiers**. Rajouter l'extension .bat à la fin du nom du fichier. Cliquer sur **Enregister**.



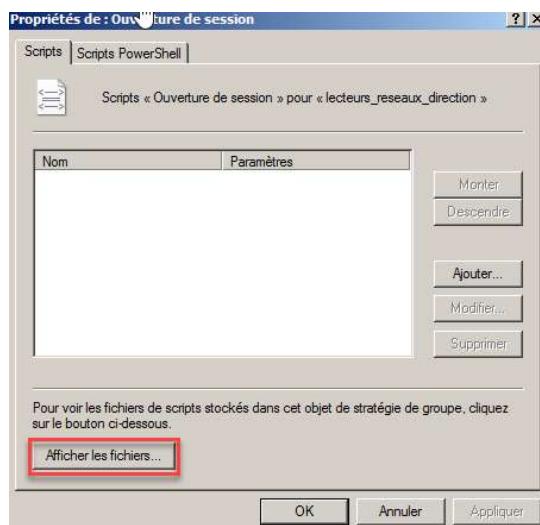
Ensuite ouvrir la console de gestion des stratégies de groupe. Créez un nouvelle GPO sur l'OU **@FORMATION**. Nommez cette GPO : **lecteurs_reseaux_direction** et cliquer sur **OK**.



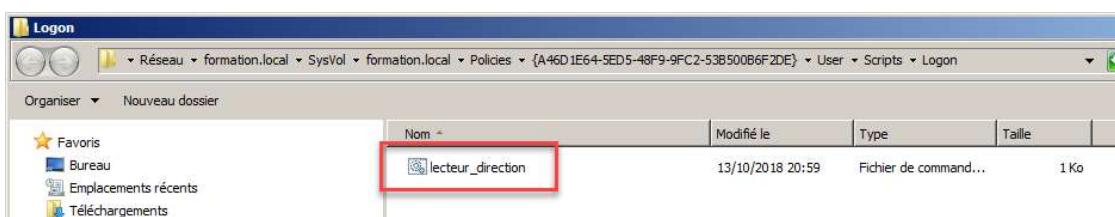
Editez cette GPO. Dérrouler ensuite configuration utilisateur, puis Stratégies, Paramètres Windows, Scripts (ouverture / fermeture de session), et sur la droite double clic sur Ouverture de session.



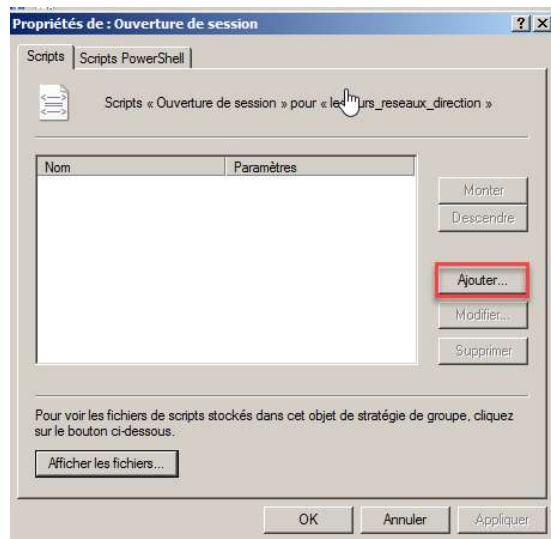
Cliquer ensuite sur Afficher les fichiers.



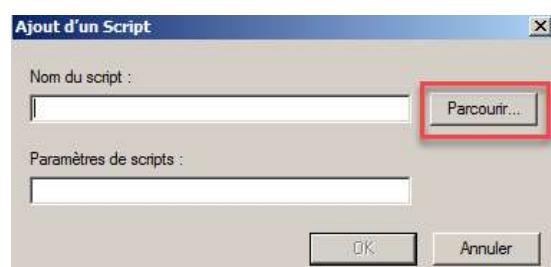
Une fenêtre de l'explorateur Windows se lance, le chemin d'accès est spécifique à cette GPO, dans la barre de navigation le numéro de cette GPO est visible. Couper votre script dans ce répertoire vide.



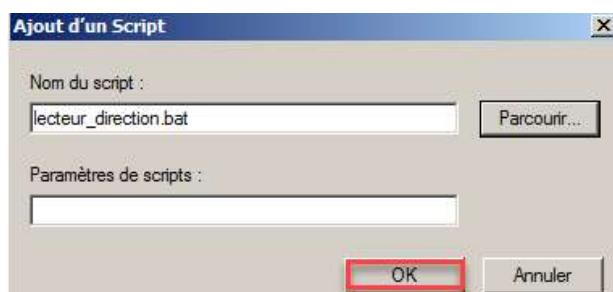
Fermer l'explorateur. Puis cliquer sur Ajouter.



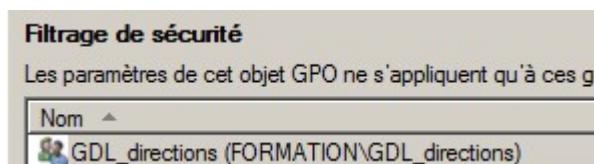
Cliquer sur **Parcourir**.



Sélectionner le script et cliquer sur **Ouvrir**. Cliquer sur **OK**. Puis **OK**. Supprimer les **utilisateurs authentifiés** dans le **filtrage de sécurité** et ajouter le groupe **Directions**. Fermer l'éditeur de GPO et lancer la mise à jour sur le poste client.



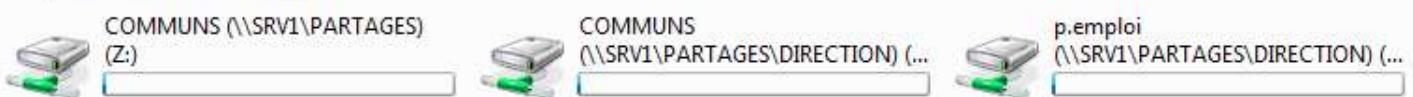
Cliquer sur **OK**.



Lancer la commande **GPUPDATE /FORCE**.

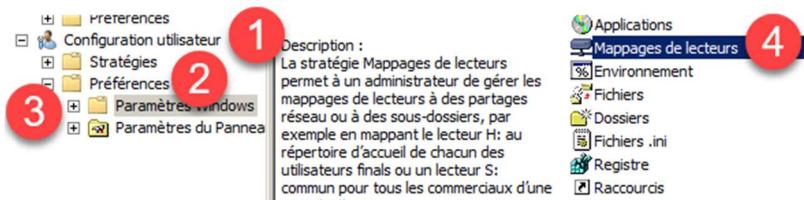
Redémarrer la session ou le l'ordinateur et voici les lecteurs

Emplacement réseau (3)

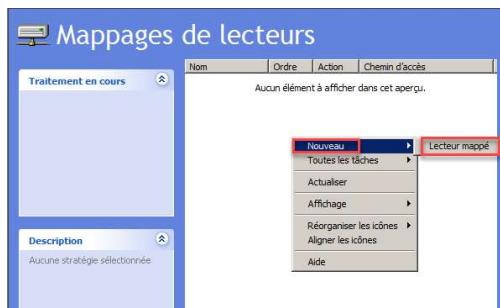


Mappage de lecteur

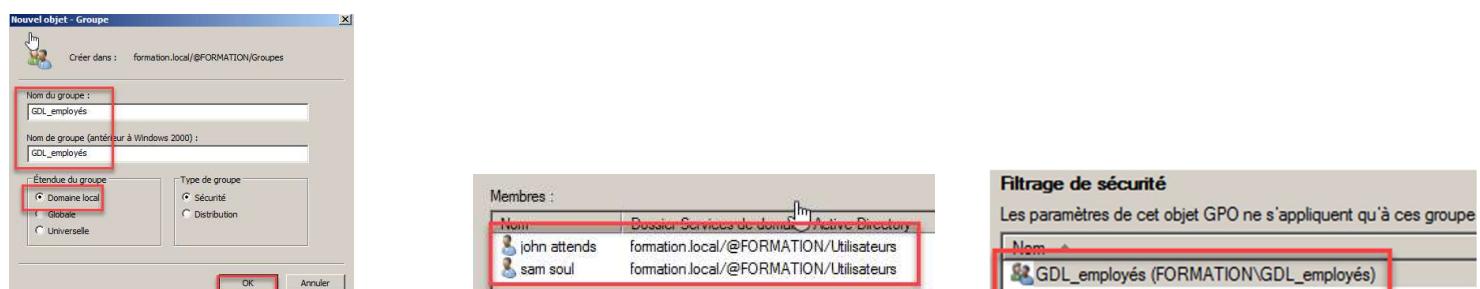
Crée une nouvelle GPO avec le nom **lecteur_reseaux_users**. Editez là. Dérouler **configuration utilisateur**, **Préférences**, **Paramètres Windows**, puis double cliquer sur **Mappage de lecteurs**.



Faites un clic droit **Nouveau** puis **Lecteur Mappé**.



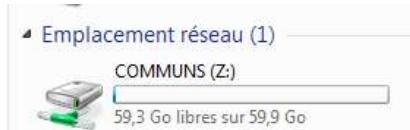
Dans **Action**, sélectionner **Créer**. Entrer le chemin suivant dans **Emplacement** : <\\SRV1\\PARTAGES\\COMMUNS>
Cocher **se reconnecter**. Entrer le libellé en tant que **COMMUNS**. Cliquer sur **Utiliser** la lettre **Z** : . Cliquer sur **OK**. Créer un groupe **GDL_employés** et rajouter les tous les autres utilisateurs.



Fermer l'éditeur de GPO et lancer la mise à jour sur le poste client ou connecter avec un compte qui ne soit pas dans le groupe **Directions** et qui n'a jamais été utilisé. Utilisons le compte **s.soul**.



Vérification de la remontée du lecteur.

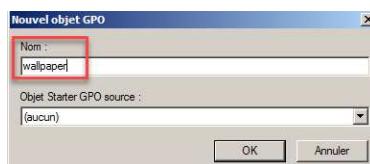


Attribution d'un fond d'écran à l'ensemble des utilisateurs.

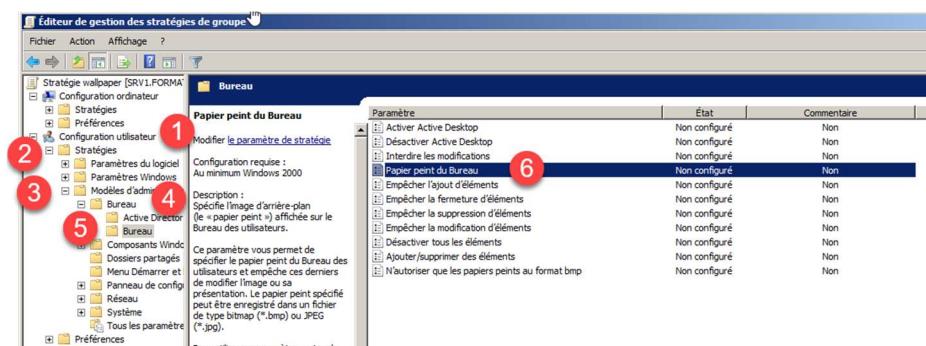
Avant tout chose, chercher un fond d'écran ayant l'extension .jpg avec la résolution 1024x768. Je choisi un fond d'écran. Copier ce fichier dans **INFRA**, puis créer un dossier **WALLPAPER** et copier le fichier dans ce dossier.



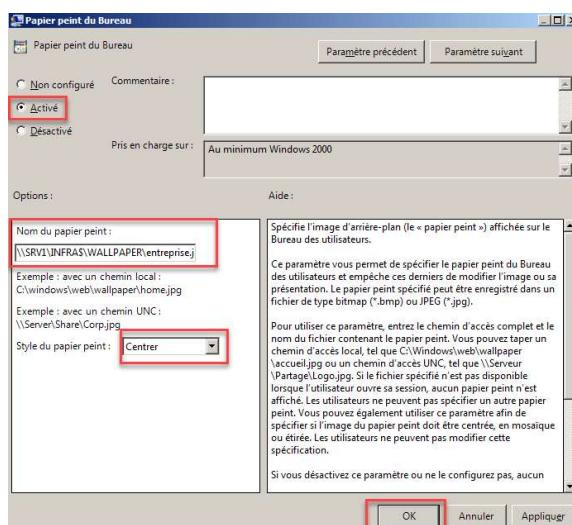
Ensuite ouvrir la console de gestion des stratégies de groupe. Créez une nouvelle **GPO** sur l'**OU @FORMATION**. Nommez cette GPO : **wallpaper** et cliquez sur **OK**.



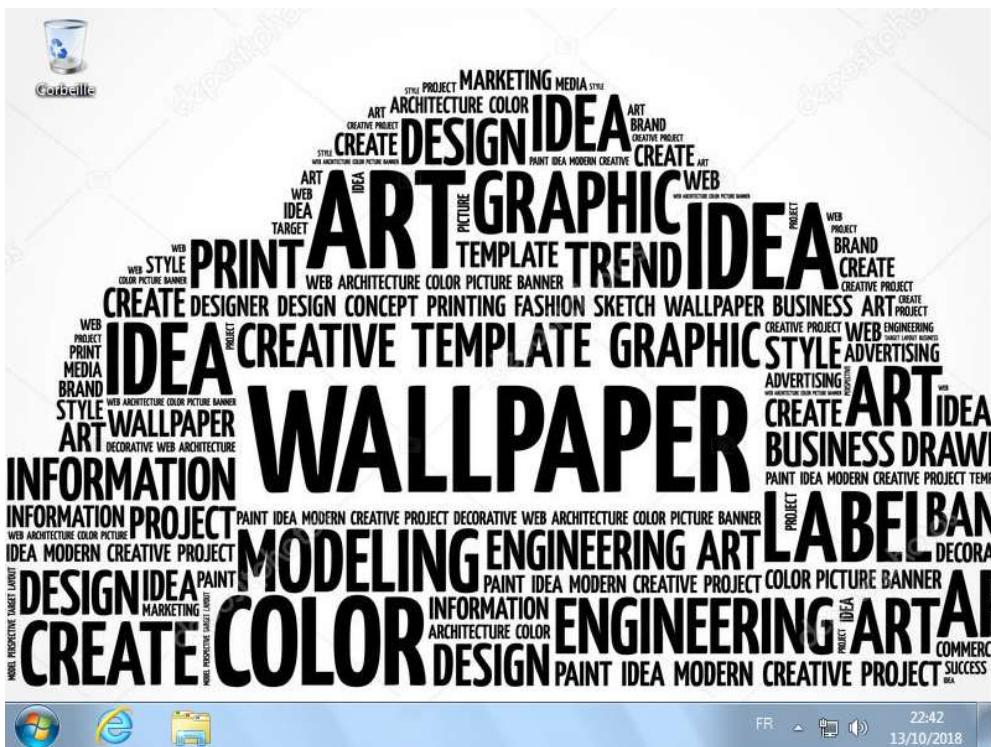
Editez là. Déroulez **configuration utilisateur, stratégies, modèles d'administration, bureau, bureau**. Double clic sur **Papier peint du Bureau**.



Cliquez sur **Activé**, spécifiez le nom du fichier papier peint : [\\SRV1\INFRA\\$\WALLPAPER\entreprise.jpg](\\SRV1\INFRA$\WALLPAPER\entreprise.jpg), pour **VMWare** choisissez le style de papier peint : **Centrer**. Cliquez sur **OK**.



Fermer l'éditeur de GPO et lancer la mise à jour sur le poste client ou connecter avec un compte qui ne soit pas dans encore tester. Utilisons le compte **j.attends**.



Le fond d'écran est appliqué avec la GPO permettant le blocage du panneau de configuration un utilisateur ne pourra donc pas le changer.

WINDOWS DEPLOYMENT SERVICES (WDS):

WDS sur Windows Server 2008

Un service WDS permet de déployer des images via le réseau en PXE. Le PXE est une méthode démarrage via une carte Ethernet afin de récupérer le CD d'installation de la version du système d'exploitation que vous voulez installer sur la machine. À votre convenance sur votre serveur. C'est une évolution du RIS de Windows Serveur 2003. l'intérêt de celui-ci réside dans la possibilité de pouvoir délivrer des installations en multicast sous condition que vos switches le gèrent. Par le biais de ce système, déployer une image de Windows Vista prend environ 5 minutes pour un poste et 7 minutes pour une 50aine de postes.

Les CD de Windows Vista, Seven ainsi que ceux de Windows Serveur 2008 contiennent des images VIM pour leurs installations. Ces images VIM sont des formats d'images orientés fichiers, qui, contrairement aux fichiers ISO qui eux sont orientés secteurs. Ces fichiers VIM ont l'avantage de pouvoir d'être déployé de façon native par le WDS.

Cependant il est possible de déployer tous les systèmes par le WDS, mais cela nécessite quelques étapes supplémentaires afin de créer ces fichiers VIM.

Prérequis :

- Windows Server 2008 configuré
- Un serveur DHCP, DNS et Active Directory dans notre cas
- Un CD de Windows à déployer

Dans les outils d'administration, lancez l'outil **Gestionnaire de Serveur**.

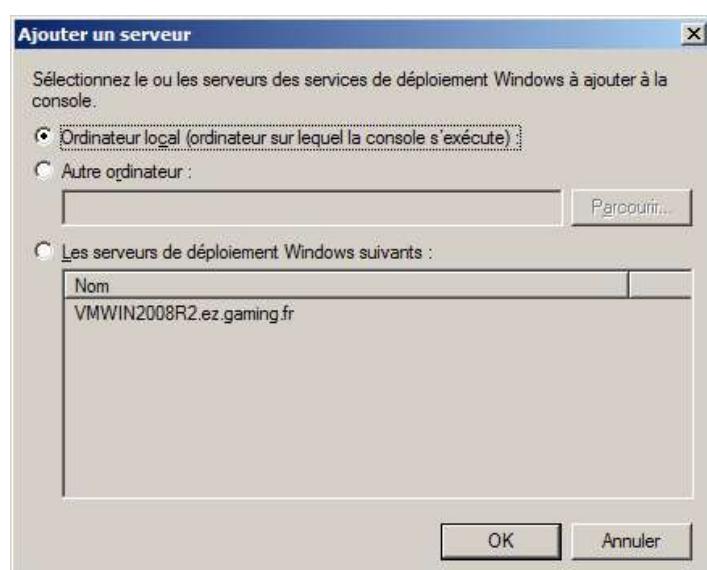
Cliquez sur **Rôles** dans l'arborescence à gauche puis sur **Ajout de Rôles** dans les liens à droite.

Dans l'assistant, sélectionnez le rôle **Windows Deployment Services**, cliquez deux fois sur **Suivant**.

Vérifiez que **Deployment Server** et **Transport Server** sont bien cochés puis cliquez sur **Suivant** deux fois et sur **Install**.

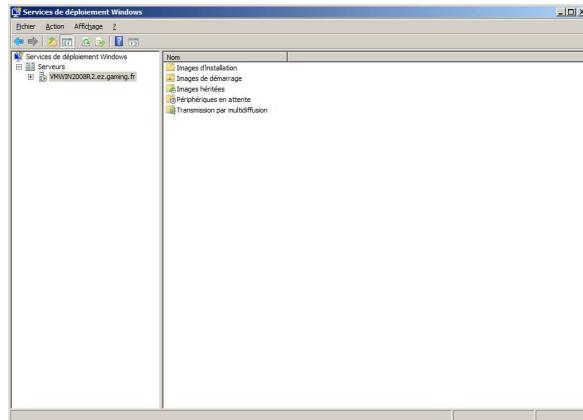


Clic droit sur Serveurs , Ajouter un serveur



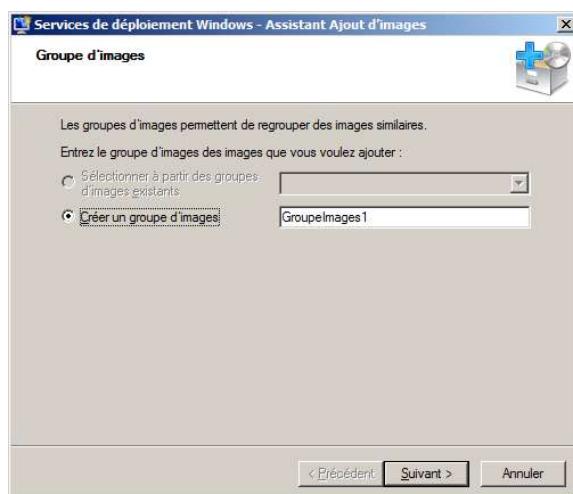
Cliquez sur OK

Voici ce qui apparait



Nous allons spécifiez quel type d'installation nous voulons diffuser sur le réseau.

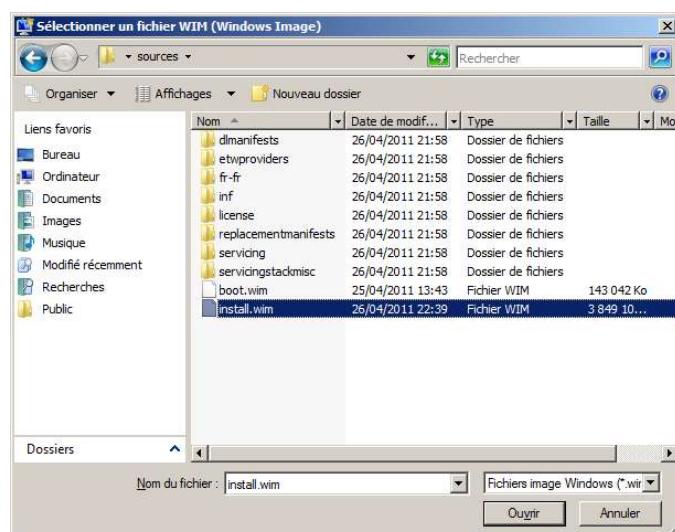
Clic Droit sur images d'installation / **ajouter une image d'installation**



Donnez un nom au groupe d'images pour la diffusion

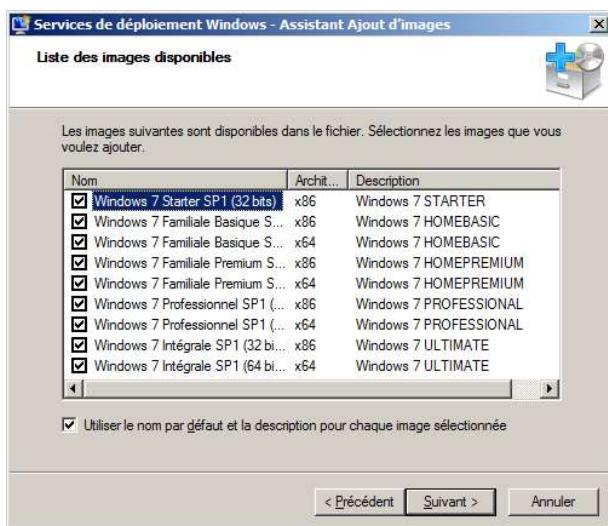
Maintenant il faut renseigner le dossier contenant les fichiers images. WIM. Vous pouvez les récupérez du disque d'installation Windows (Windows Seven par exemple)

D:/sources/**install.vim**

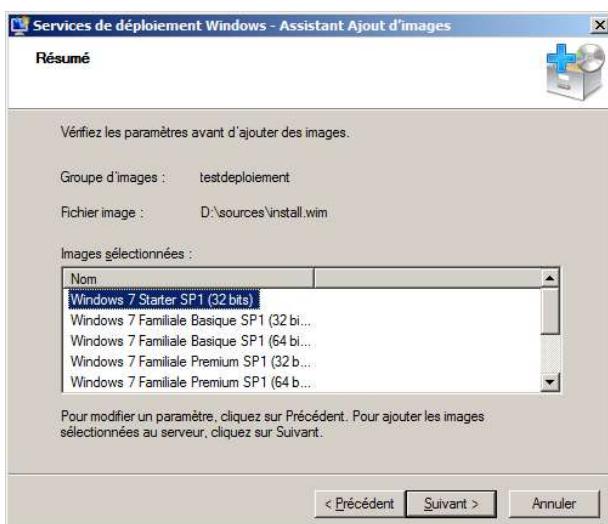


Cliquez sur Ouvrir, puis suivant

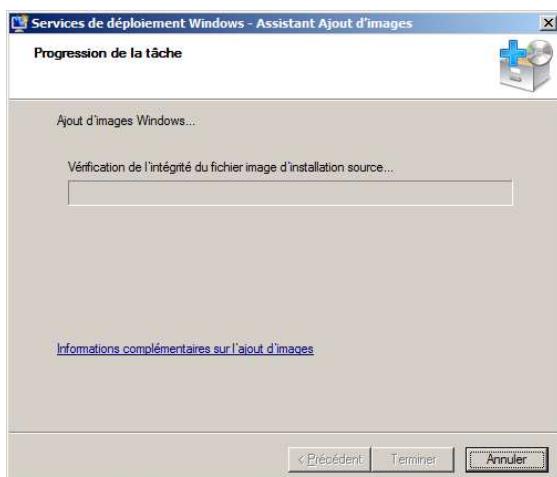
Lors de l'écran suivant (voir prochaine capture d'écran) choisissez la version que vous voulez déployer (32 bits ou 64 bits, familiale, premium, etc...) Si vous gardez les choix comme dans l'exemple lors de l'installation vous aurez le choix durant l'installation de Windows.



Cliquez sur suivant.

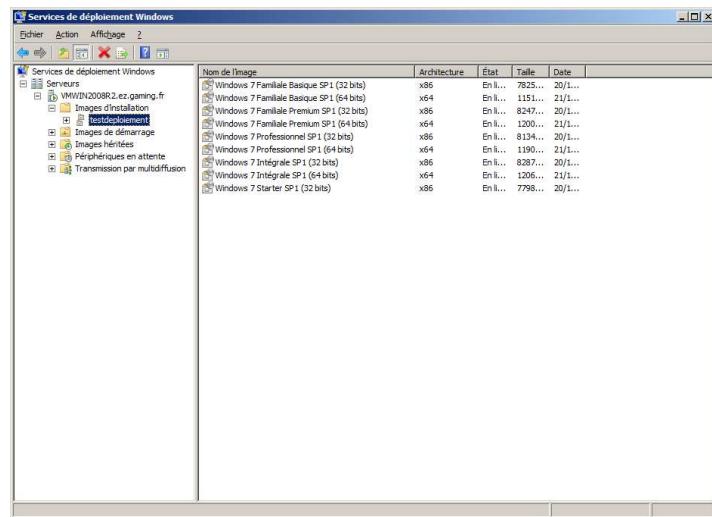


Vérifiez que vos choix précédent sont les bons et cliquer sur suivant quand vous êtes prêt.



Le service WDS vérifie et vous ajoute vos images en vue d'un déploiement prochain.

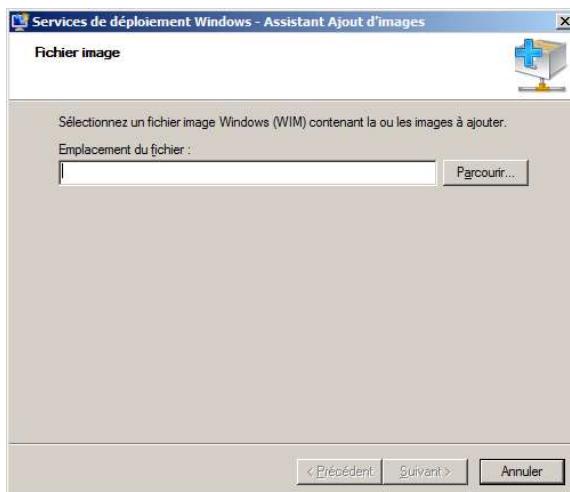
Cela peut prendre quelques minutes. Une fois l'opération terminée Cliquez sur Terminer.



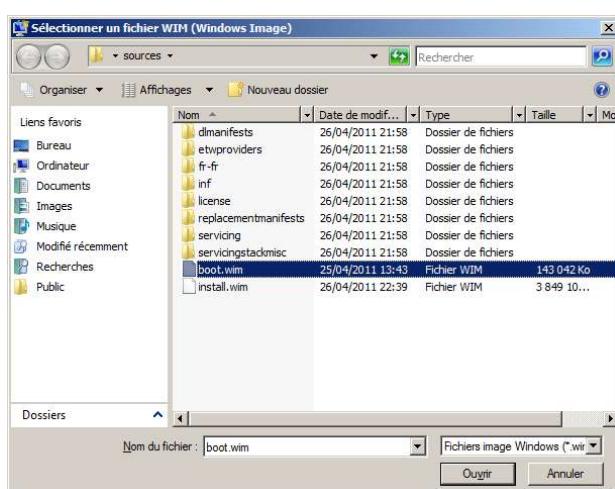
Le service a donc bien pris les versions que nous avions sélectionnez.

L'image du système est une chose importante mais sans l'image de démarrage rien ne permettra de lancer l'installation via le réseau.

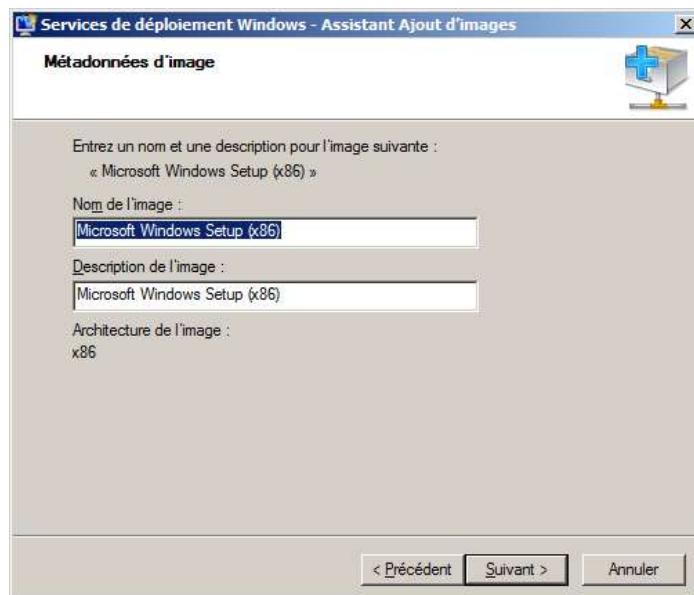
Clic droit sur images de démarrage **Ajouter une image de démarrage**



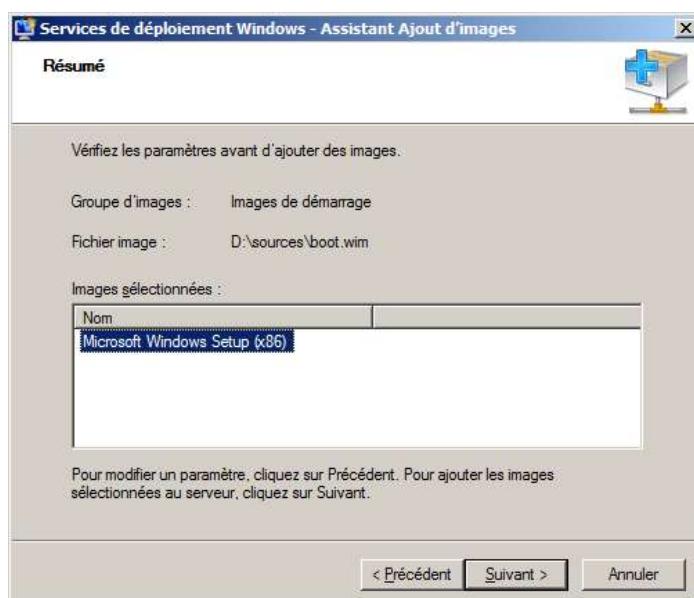
Pareil que pour l'image d'installation on parcourt le disque d'installation. Cette fois-ci on sélectionne **boot.wim**



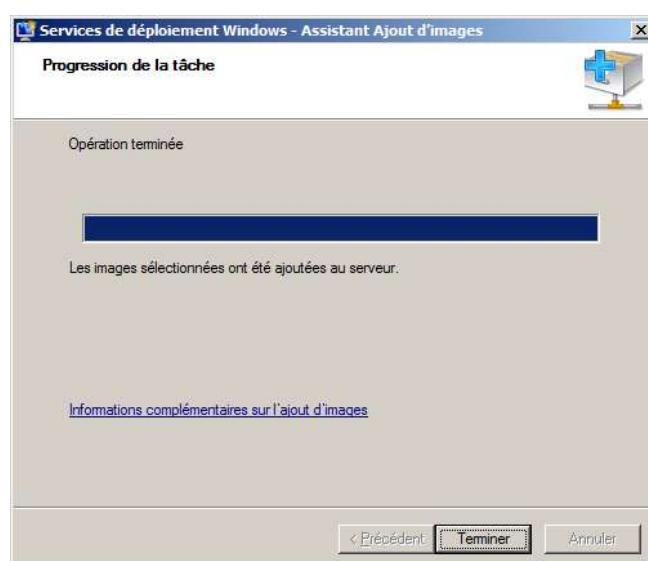
Cliquez sur suivant.



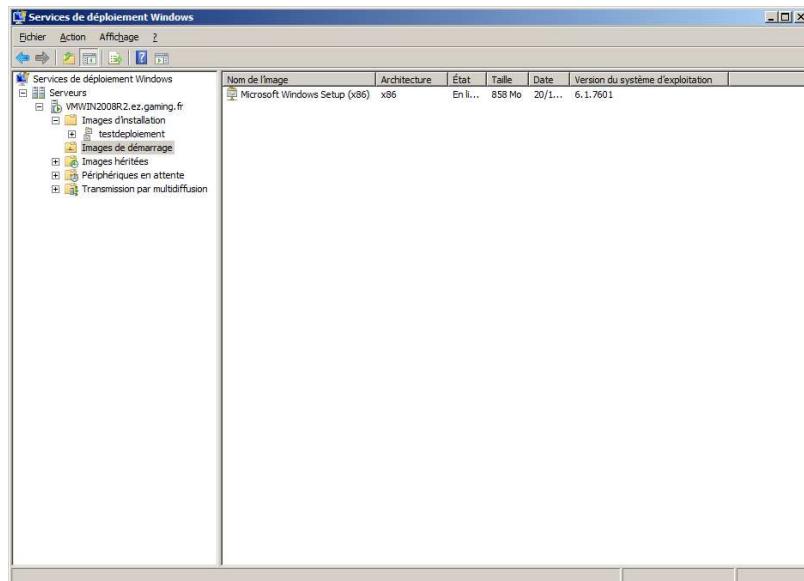
WDS applique la version 32 bits par défaut mais il gère quand même le 64bits vu qu'on lui a spécifié des images d'installations 64 bits. Cliquez sur Suivant



Récapitulatif avant d'appliquer la prise en compte. Cliquez sur suivant.



Cliquez sur Terminer une fois l'opération terminée.

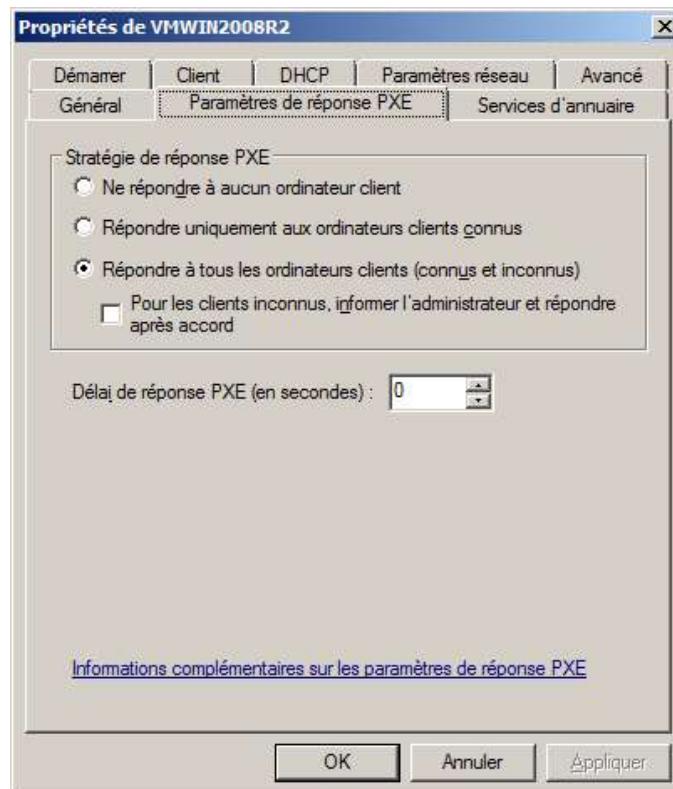


L'image de démarrage apparaît bien.

Vérifions les paramètres sur serveur de déploiement.

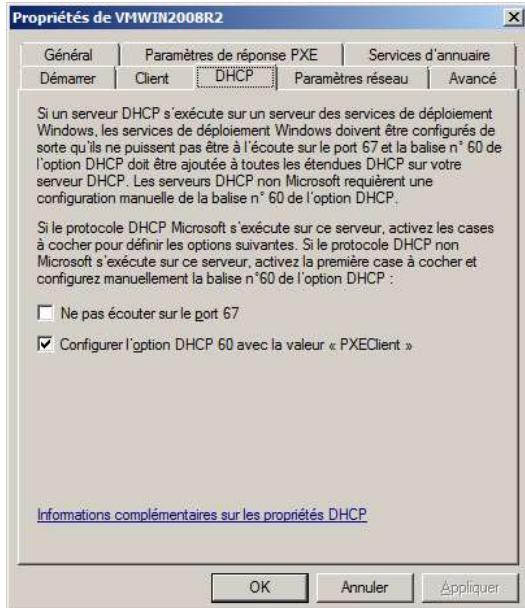
Dans mon cas Clic droit sur VMWIN2008R2.ez.gaming.fr puis propriété.

L'onglet paramètres de réponse PXE nous intéresse.

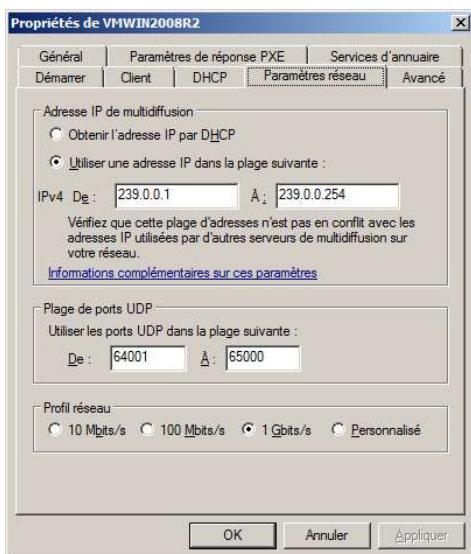


Cochez répondre à tous les ordinateurs clients (connus et inconnus)

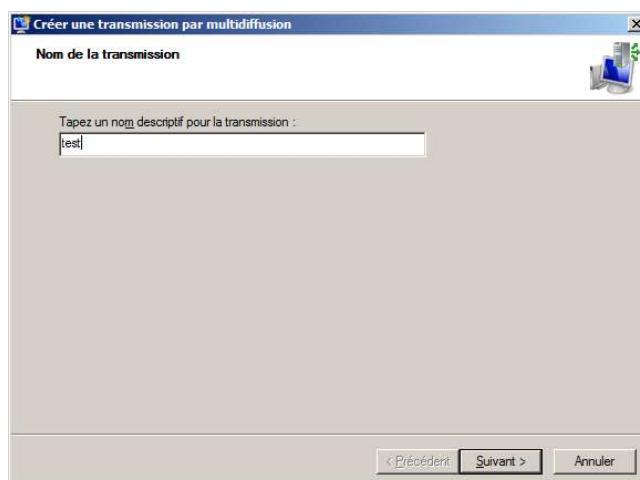
Aller dans l'onglet DHCP est vérifié bien le statut



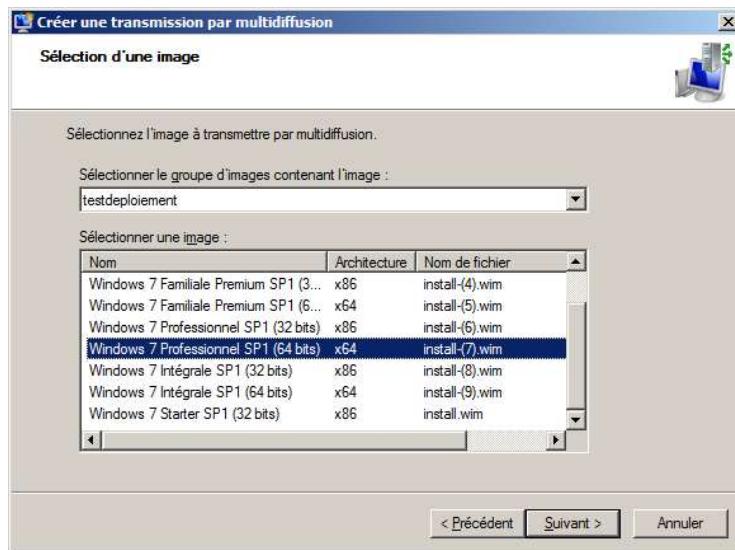
L'onglet paramètres réseau permet de régler la bande passante.



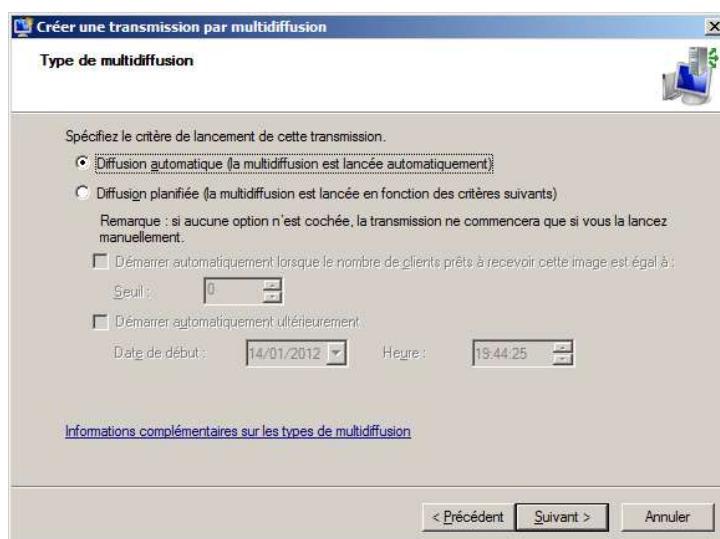
Pour créer une tâche de multidiffusion clic droit sur Transmission par multidiffusion / Créez une transmission par multidiffusion.



Sélectionnez l'image à transmettre.

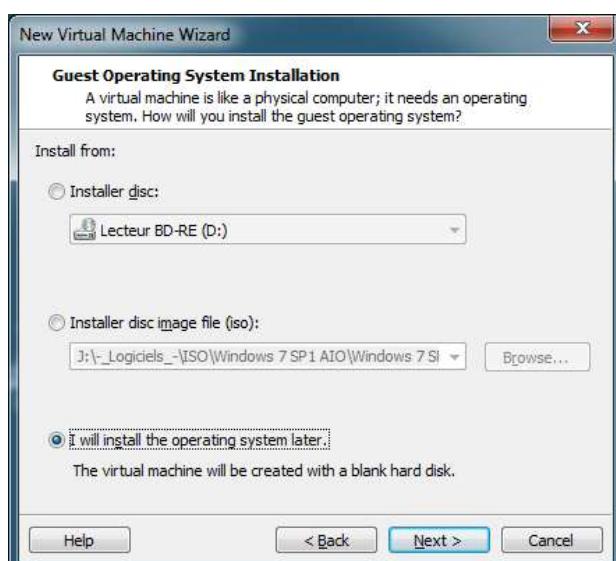


Cliquez sur suivant. Spécifiez le mode de diffusion. Automatique ou planifiée. Dans notre cas nous choisissons automatique.

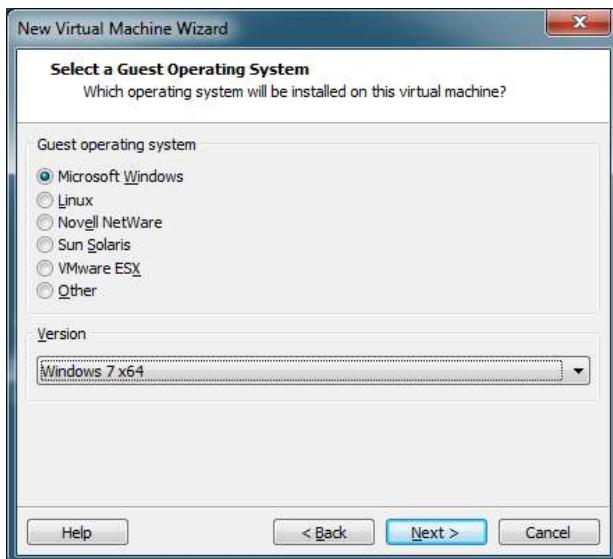


Et cliquez sur Terminer

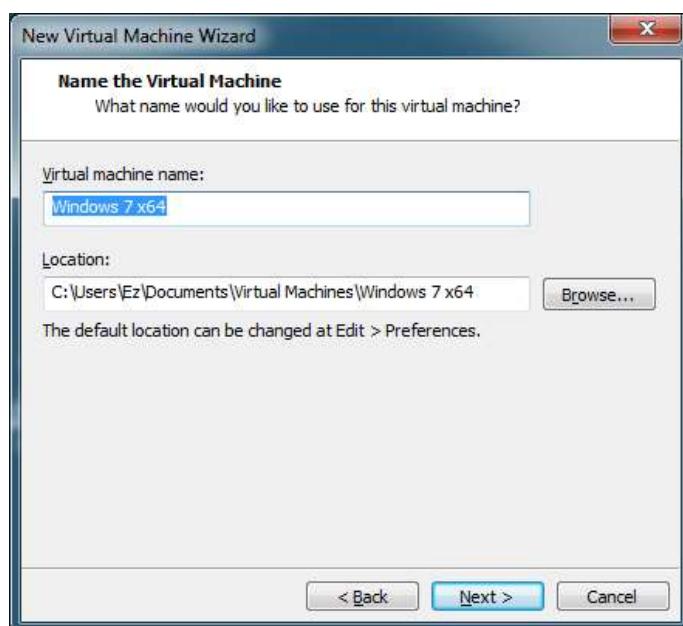
Vérifier bien que vous avez bien réglé votre carte réseau sur VNNET2 sur votre serveur ainsi que sur la VM ou l'on va essayer le déploiement.



Cliquez sur Next



Sélectionner le système correspondant à l'image que vous voulez déployer. Cliquez sur Next.

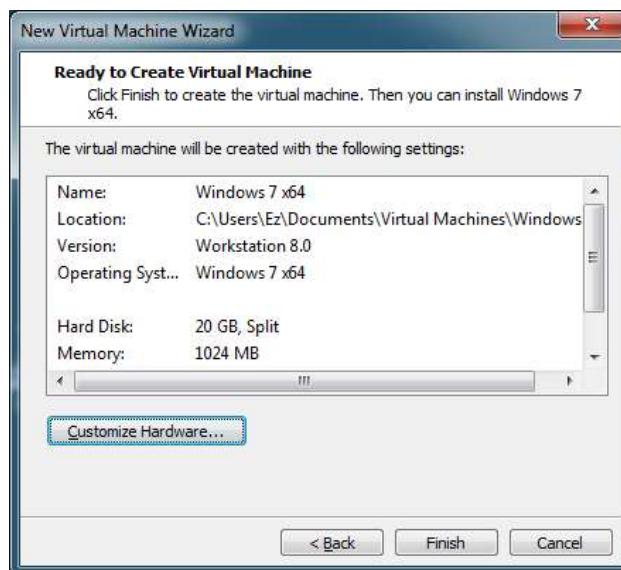
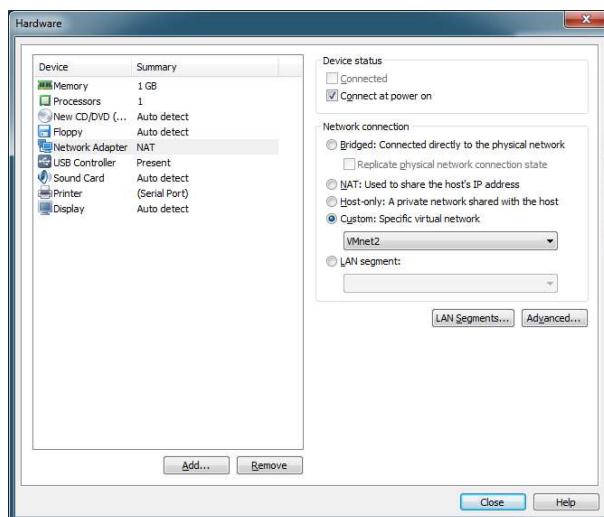


Spécifiez un nom et un emplacement à la Virtual machine de test.

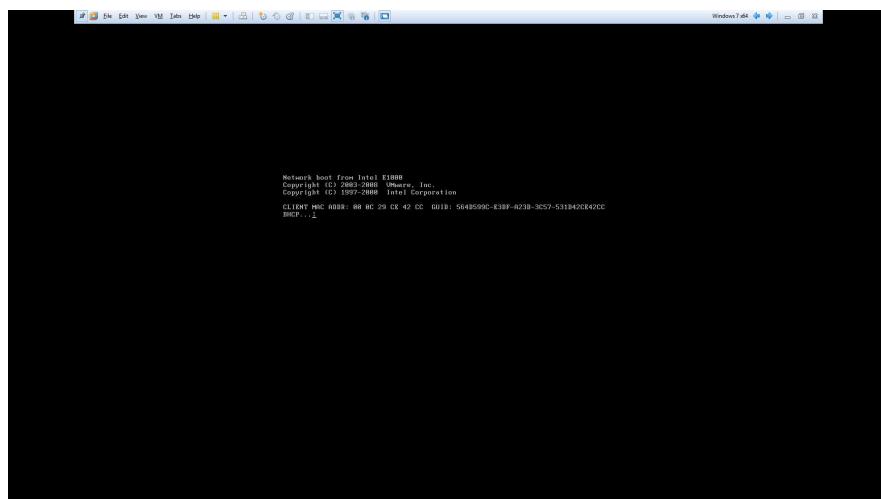


Cliquez sur Next

Dans customise, Régler bien la carte réseau sur le bon VNNET « 2 ». La quantité de ram et le nombre de processeur alloué à la VM.



Cliquez sur Finish et démarrez votre VM.



Appuyez sur F12 lorsque le commentaire vous le demande.

La suite est décrite dans une vidéo. (Serveur de déploiement Movie003).

WSUS

Définition WSUS

Windows Server Update Services (WSUS) est un service permettant de distribuer les mises à jour de Windows et d'autres applications Microsoft sur les différentes machines Windows d'un parc informatique. WSUS est un serveur de mises à jour local (ou proxy de mises à jour) qui se synchronise avec le site public [Microsoft Update](#) et permet de contrôler la diffusion des mises à jour dans le parc. Par défaut chaque machine Windows faisant ses propres mises à jour, va les chercher sur le site officiel, ce qui demande beaucoup de bande passante sur un parc avec de nombreuses machines.

Installation de WSUS (remplacer les noms de domaine par celui de l'exercice.)

Microsoft recommande comme configuration minimal pour le WSUS

1. Comment préparer l'installation de WSUS

1.1. Configuration minimale:

- Recommandation Microsoft pour 500 clients ou moins

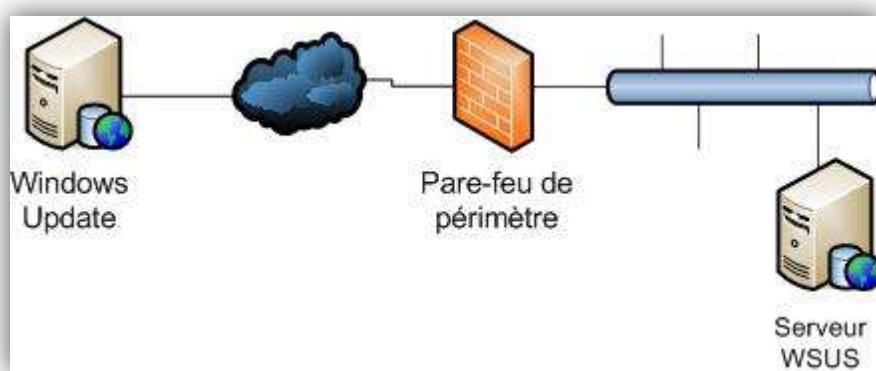
	Minimum	Recommandé:
CPU	750 MHz	1 GHz
RAM	512 MB	1 GB
Base de donnée	WMSDE/MSDE	WMSDE/MSDE
Disque dur	32 GB	32 GB

- Recommandation Microsoft pour 500 à 15.000 clients

	Minimum	Recommandé:
CPU	1 GHz	3 GHz biprocesseur
RAM	1 GB	1 GB
Base de donnée	SQL Server 2000 avec SP3a	SQL Server 2000 avec Service Pack 3a
Disque dur	32 GB	32 GB

J'ai choisi d'installer le rôle WSUS sur le même serveur que le WDS, la machine étant suffisamment puissante pour contenir les deux simultanément.

Le serveur sera situé sur le même réseau que les postes. Il possède deux cartes réseaux, une connecté sur le réseau local de formation et une autre directement connecté à Internet.



WSUS va permettre de diffuser les mises à jour Microsoft sur le réseau.

Les mises à jour sont déployées par le biais du client de mise à jour automatique.

L'installation de WSUS nous impose d'installer les services IIS (web) pour diffuser ses mises à jour.

Les clients iront récupérer les mises à jour sur le site web créé lors de l'installation de WSUS. Par défaut le port du site est le « 8530 ».

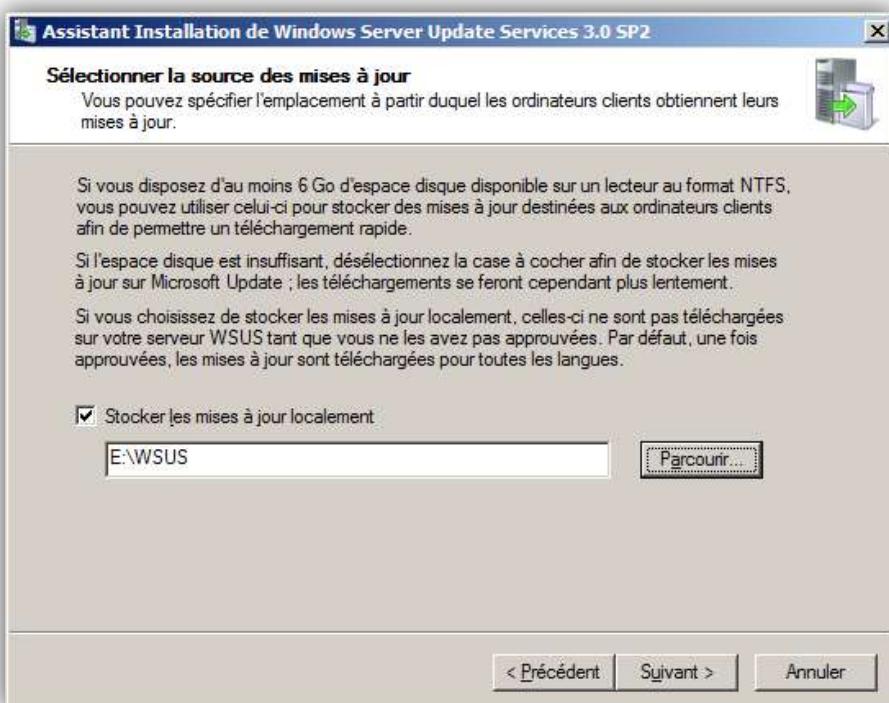
Installation du rôle WSUS



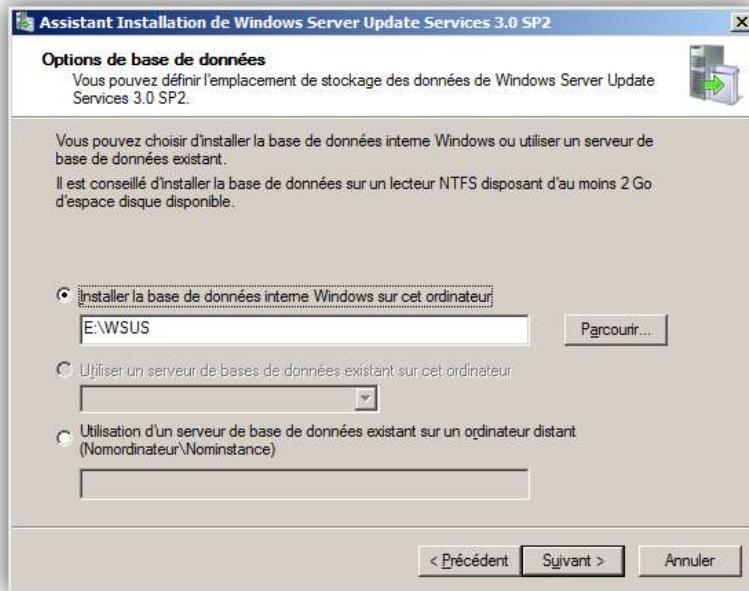
Microsoft recommande lors d'un réseau utilisant plusieurs serveurs WSUS, de n'effectuer les mises jour du WSUS que depuis un seul serveur, les autres se synchroniseront sur le premier.

Lors de l'installation du WSUS 3.0 SP2, l'assistant nous informe que « Microsoft Report Viewer 2008 Redistributable ne sera pas installé », ce qui signifie que nous n'aurons pas d'informations et statiques sur les journaux d'évènements interne au WSUS, il faudra l'installer après le WSUS. <http://www.microsoft.com/fr-fr/download/details.aspx?id=577>

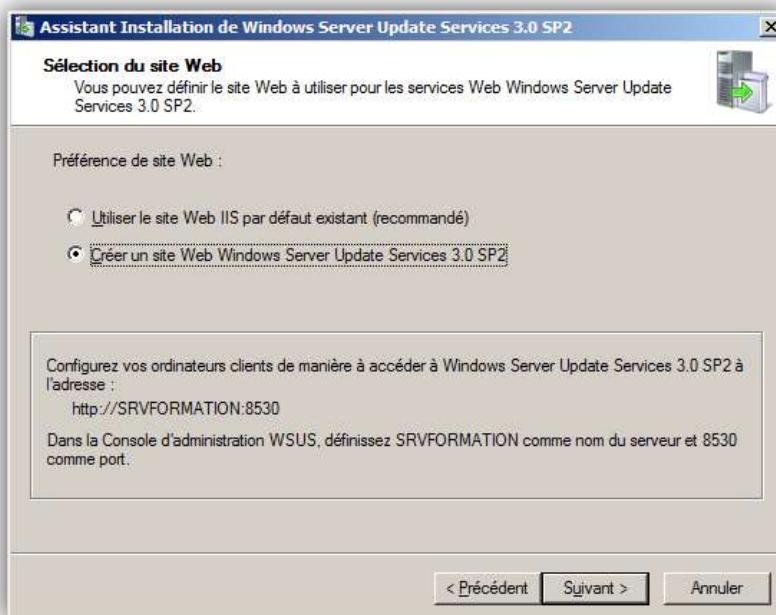
Comme pour le WDS, le fichier contenant les mises à jour ne doit pas être sur le disque système. J'ai choisi de le mettre sur le même disque que le WDS. Microsoft recommande au moins 6Go d'espace disque disponible sur un lecteur au format NTFS pour stocker les mises à jour pour les ordinateurs du parc.



Ne possédant pas de base de données sur le réseau disponible, j'ai choisi d'utiliser celle interne à Windows.



Comme expliquer précédemment, WSUS requiert un site web pour diffuser les mises à jour aux clients.



Configuration de WSUS :

Une fois l'installation terminée, nous devons paramétrter le rôle.

Je défini comme serveur principal WSUS, en lui spécifiant qu'il ira chercher directement les mises à jour en se synchronisant à Windows Update.

Une première connexion à Windows Update permet de télécharger les informations comprenant :

- ✓ Les types de mises à jour disponibles
- ✓ Les produits qui peuvent être mis à jour
- ✓ Les langues disponibles

Une fois ces informations récupérées du serveur Microsoft, nous pouvons dans un premier temps :

1. paramétrer la langue utilisée sur le système
2. Sélectionner les produits à maintenir à jour

Dans notre Cas, Microsoft Security Essentials, Windows Defender, Microsoft Office, 2010, 2013, Microsoft Windows XP, 7, 8, Microsoft Serveur 2008,2008 R2.

3. Ensuite les mises à jour sont classées par catégories et types :

- Service pack
- Mise à jour de la sécurité
- Mise à jour de définition
- Critiques
- Pilotes

J'ai choisi les Services pack, qui sont un ensemble de correctifs majeurs.

Les mises à jour de la sécurité permettent de combler les failles.

Les mises à jour critiques qui peuvent poser un problème au bon fonctionnement du produit Microsoft.

Les mises à jour de définitions qui maintiennent l'antivirus à jours.

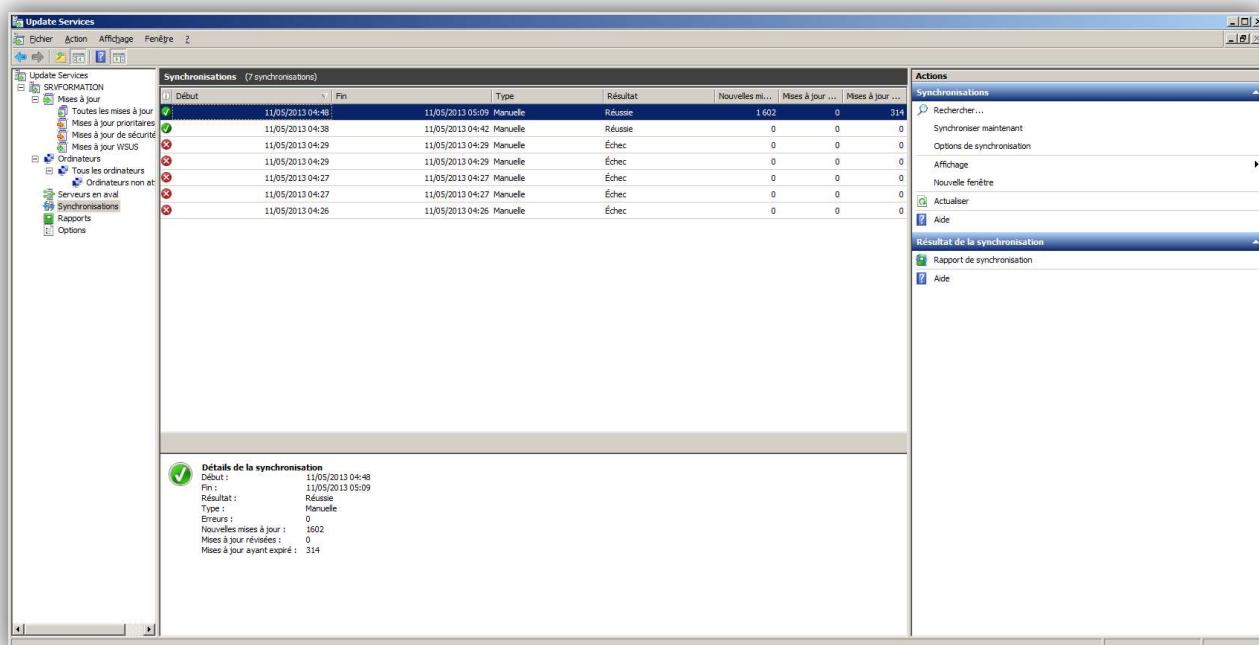
Pour finir la configuration « basique » il suffit de définir une plage horaire durant lesquels les mises à jour seront effectuées.

Il est recommandé de les effectuer le dernier jour de la semaine ouvrée afin d'éviter toutes gênes à l'utilisateur. Notamment lorsque la mise à jour requiert un redémarrage, où dans de cas très rare, ce qui peut provoquer un blocage de l'ordinateur. Cela permet au technicien d'intervenir sur le parc facilement quand celui-ci n'est plus occupé.

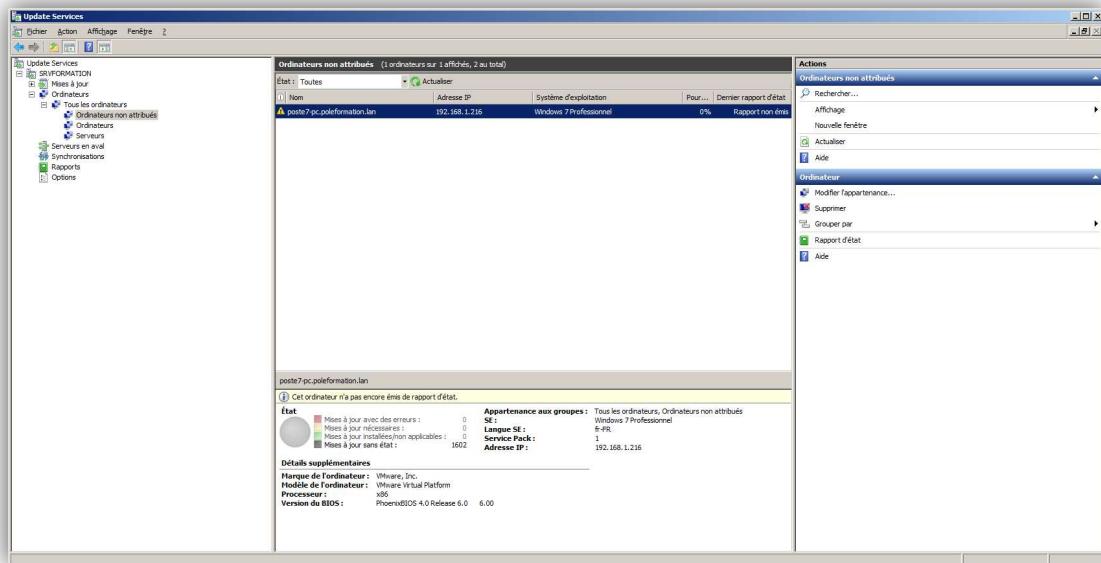
Le temps du téléchargement de toutes ses mises à jour a pris environ 11 heures.

La durée dépend de la connexion internet et du trafic sur le Microsoft Update.

Pendant ce temps nous pouvons continuer le paramétrage.



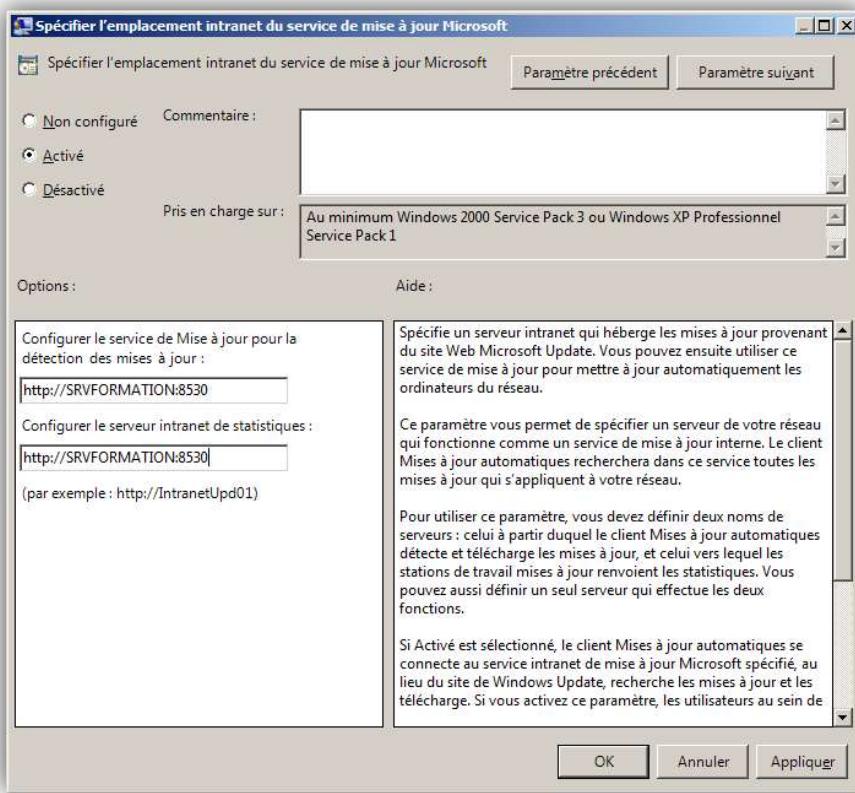
Afin de gérer au mieux son parc il est recommandé de créer des groupes



Une fois la structure faite, il faut obligatoirement mettre en place une GPO (Group Policy Object). Elles permettront d'indiquer aux postes et serveurs où chercher les mises à jour.

Elles se feront plus par le Microsoft Update mais par le WSUS en local.

La règle de la GPO suivante, permet d'indiquer aux postes clients où effectuer la mise à jour. Pour voir l'ensemble de la procédure des GPO qui doivent être mises en place voir annexe page n°66.



La suivante permet d'enlever le redémarrage automatique en cas de mise à jour nécessitant un redémarrage.

La troisième autorise l'installation immédiate des mises à jour. Elle évite de passer sur tous les postes pour lancer l'installation.

La quatrième définit la durée pendant laquelle Windows attendra pour vérifier la disponibilité des nouvelles mises à jour.

La cinquième définit la durée pendant laquelle les mises à jour automatiques doivent attendre avant de redemander confirmation en cas de redémarrage planifié.

La sixième indique le site qui diffusera les mises à jour recommandées et importantes.

La septième paramètre les mises à jour automatiques et la planifie l'installation sur le poste.

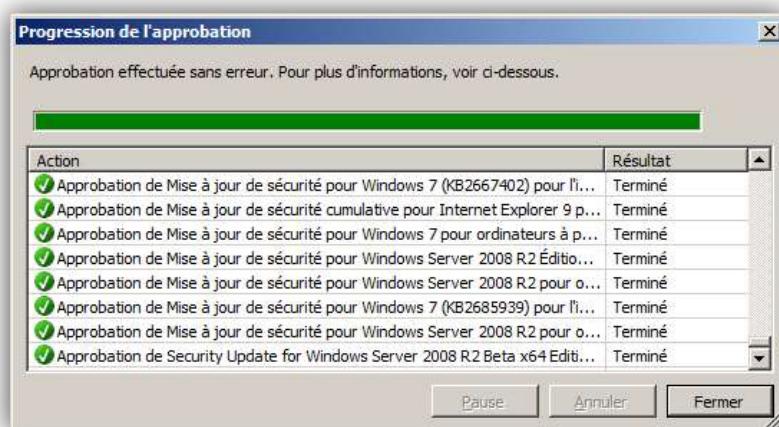
La huitième consiste à autoriser les non-administrateurs à recevoir les notifications de mises à jour. Une fois l'ensemble de ses règles paramétrées, il faut appliquer cette GPO. Il est conseillé de forcer la mise à jour de cette GPO. Ouvrez l'invite de commande sur le serveur et taper la commande suivante :

GPUPDATE /FORCE.

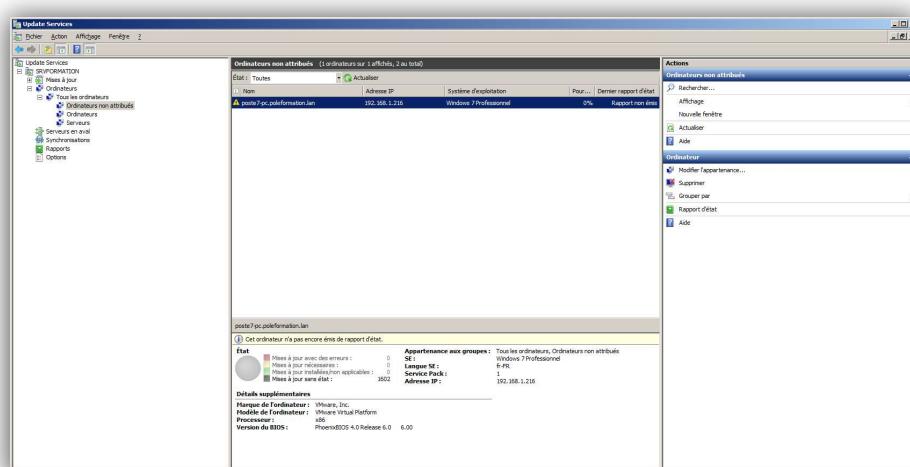


En tant qu'administrateur du WSUS il incombe la charge de donner son approbation à une mise à jour ou non. Il est conseillé de laisser un laps de temps entre la diffusion de la mise à jour par Microsoft et son utilisation sur son réseau.

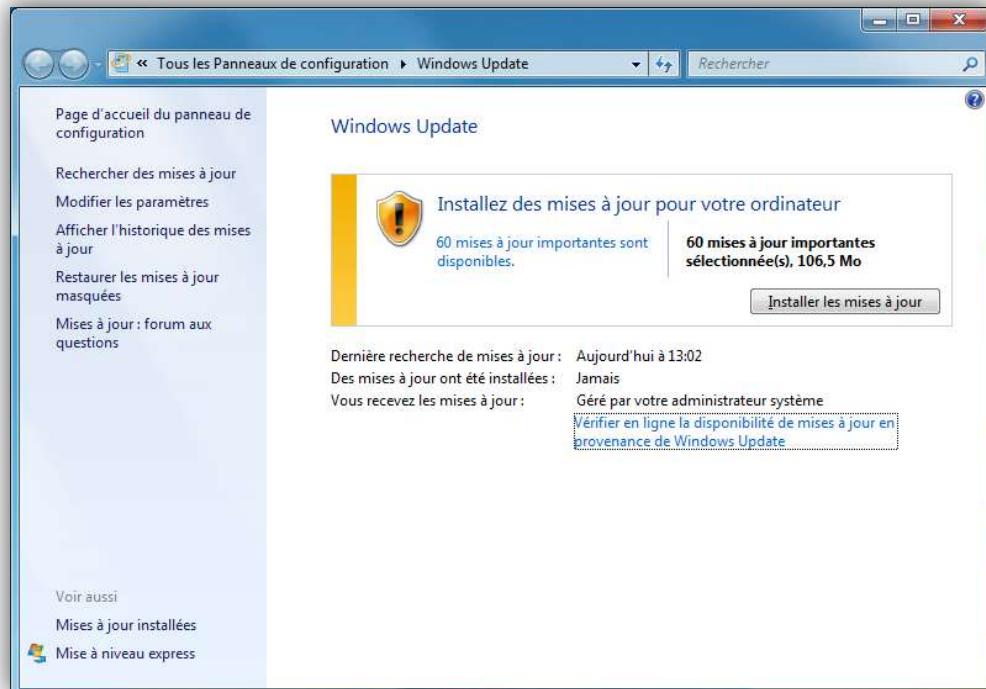
On peut choisir d'attribuer manuellement les mises à jour ou bien de définir des règles d'approbation automatique concernant le type de mise à jour et le produit ciblés.



Une fois le paramétrage mis en place, j'ai connecté un poste qui venait d'être déployé avec une image de base Windows 7 pro 64 bits, préalablement joint au domaine « poleformation.lan ». Après quelques minutes, le poste est remonté dans la console WSUS.



J'ai approuvé ce poste et je l'ai déplacé dans le groupe Ordinateurs de la console WSUS.
Une fois actualisé j'ai pu apercevoir une notification concernant des mises à jour Windows sur le poste Client.



Les mises à jour se sont téléchargées comme jamais auparavant.

Pour l'installation c'est autre chose.

Après quelques minutes le rapport d'installation s'est affiché.

