**Formation Réseau Installation Serveur – Windows 2022-2016 – 2012R2 Server  
 - SR 22 - Cours**

Michel Cabaré / www.cabare.net / michel@cabare.net

Windows Serveur 2022-2019-2016-2012   
 - SR 22 - Cours V2-2 - décembre 2021

|  |  |  |
| --- | --- | --- |
| https://WWW.CABARE.NET © |  |  |

|  |  |
| --- | --- |
|  |  |

La formation a pour but de vous initier avec les logiciels Microsoft Windows 2022- 2016 voire 2012 R2 Serveur sur environnement P.C.

Ce Support a pour but de vous fournir un certain nombre d'éléments concernant soit des manipulations, soit des notions théoriques concernant la gestion de réseaux locaux

Il ne peut en aucun cas se substituer à la participation à la formation, ni à tout ou partie de la documentation fournie avec le logiciel.

En effet, **et c'est là sa vocation première**, ce document doit **"servir de support à la prise de notes en formation, et sera donc avantageusement complété par vos soins"**. Son but est de permettre une présentation de vos notes plus structurée et donc plus facilement utilisable ensuite.

Bon Travail

Michel Cabaré

**table des matiÈres**

[Versions Windows Server 7](#_Toc98835072)

[Versions 2012 et 2012R2: 7](#_Toc98835073)

[Essential 7](#_Toc98835074)

[Foundation 7](#_Toc98835075)

[Standard 7](#_Toc98835076)

[Datacenter 7](#_Toc98835077)

[Nouveautés 2016: 8](#_Toc98835078)

[Nouveautés 2019: 8](#_Toc98835079)

[Versions de référence: 9](#_Toc98835080)

[Classification WSUS - Produits: 10](#_Toc98835081)

[Versions & options d'installation & MAJ 2016: 11](#_Toc98835082)

[Versions fonctionnelles 2022-2016: 11](#_Toc98835083)

[Essential 11](#_Toc98835084)

[Standard 11](#_Toc98835085)

[Datacenter 12](#_Toc98835086)

[2016 Licensing par cœur ou processeur: 13](#_Toc98835087)

[Licensing par coeur 14](#_Toc98835088)

[Socket, processeur, cœur, hyper-threading: 14](#_Toc98835089)

[Licensing server 2016 serveurs physiques: 16](#_Toc98835090)

[Licensing server 2016 serveurs virtuels: 16](#_Toc98835091)

[Licensing CAL server 2016: 17](#_Toc98835092)

[Les NOMS de poste Windows 18](#_Toc98835093)

[Nom d'hôte - nom netbios Windows : 18](#_Toc98835094)

[Rechercher un poste 20](#_Toc98835095)

[Pourquoi je ne vois pas tel ou tel poste ?: 20](#_Toc98835096)

[S’assurer alors qu’un poste est bien présent: 20](#_Toc98835097)

[Réglage profils réseaux: 21](#_Toc98835098)

[Jeux de Réglages: 22](#_Toc98835099)

[les Cartes réseau 23](#_Toc98835100)

[Carte réseau & Driver Certifié : 23](#_Toc98835101)

[Accès au Centre Réseau et partage : 24](#_Toc98835102)

[Désactivation Carte Excédentaire : 24](#_Toc98835103)

[Connexion Wifi sur Serveur : 25](#_Toc98835104)

[Autorisations de partage - Permissions d'accès (ntfs) 26](#_Toc98835105)

[Autorisation de Partage : 26](#_Toc98835106)

[Partage et Sécurité: 26](#_Toc98835107)

[En système FAT32: 26](#_Toc98835108)

[En système NTFS : 26](#_Toc98835109)

[Autorisations de Partage 27](#_Toc98835110)

[Assistant partage simplifiés 27](#_Toc98835111)

[Désactiver les partages simplifiés: 29](#_Toc98835112)

[Partage Avancé: 29](#_Toc98835113)

[Donner une Autorisation de Partage: 31](#_Toc98835114)

[Les 3 "faux types" et 2 "vraies" Autorisations de Partage 32](#_Toc98835115)

[Le refus de Partage 32](#_Toc98835116)

[Combinaison d'autorisations de partage : 32](#_Toc98835117)

[Planification des autorisations de partages: 33](#_Toc98835118)

[Exemple 1 : 33](#_Toc98835119)

[Exemple 2 : 33](#_Toc98835120)

[Gestion des partages 34](#_Toc98835121)

[Paramétrage des partages 35](#_Toc98835122)

[Spécificité Windows 10 - 7 et mot de passe vide : 35](#_Toc98835123)

[Net share : 36](#_Toc98835124)

[lecteurs réseaux Client Windows 38](#_Toc98835125)

[Connecter un lecteur réseau client Windows: 38](#_Toc98835126)

[Se Créer un raccourcis sur un lecteur / répertoire réseau : 39](#_Toc98835127)

[Net use : 40](#_Toc98835128)

[Worksgroup & domaines 42](#_Toc98835129)

[Worksgroup Groupe de travail: 42](#_Toc98835130)

[Appartenir à un Worksgroup avec 10 SEVEN: 42](#_Toc98835131)

[Réseau windows 10: 43](#_Toc98835132)

[Réseau Windows en Workgroup : 43](#_Toc98835133)

[Domaine : 44](#_Toc98835134)

[Gestion de Domaine sous Windows Server: 45](#_Toc98835135)

[Active directory 47](#_Toc98835136)

[Qu'est-ce un service d'annuaire ?: 47](#_Toc98835137)

[La structure Logique d’Active Directory dans un Domaine: 48](#_Toc98835138)

[Domaine 48](#_Toc98835139)

[Annuaire & Espace de noms 48](#_Toc98835140)

[Active Directory & DNS 48](#_Toc98835141)

[Contrôleur de schéma 48](#_Toc98835142)

[Nom 49](#_Toc98835143)

[Objet 49](#_Toc98835144)

[Conteneur UO 50](#_Toc98835145)

[La Structure Logique au sein de plusieurs Domaines: 50](#_Toc98835146)

[Arbres-arborescence de domaines 50](#_Toc98835147)

[Forêts 51](#_Toc98835148)

[Catalogue Global 52](#_Toc98835149)

[Relations d'approbation 52](#_Toc98835150)

[La structure Physique d’Active Directory: 52](#_Toc98835151)

[Sites 52](#_Toc98835152)

[Création Active Directory 53](#_Toc98835153)

[Rôles et Création de Domaine : 53](#_Toc98835154)

[Assistant Rôle AD DS Création de Domaine : 54](#_Toc98835155)

[Promouvoir ce serveur (ex Dcpromo)en Contrôleur de Domaine : 57](#_Toc98835156)

[Gestionnaire de Serveur 61](#_Toc98835157)

[Lancer la mmc Gestionnaire de Serveur: 61](#_Toc98835158)

[Rôles services et fonctionnalités 61](#_Toc98835159)

[Présence du DNS 63](#_Toc98835160)

[Lancer la mmc DNS: 63](#_Toc98835161)

[Vérifier la présence de AD et du serveur: 63](#_Toc98835162)

[Vérification paramètre IP serveur : 64](#_Toc98835163)

[Présence de AD 65](#_Toc98835164)

[Lancer la mmc AD: 65](#_Toc98835165)

[Modification du mot de passe compte Administrateur: 65](#_Toc98835166)

[Stratégies de Domaine 66](#_Toc98835167)

[Stratégie Mot de Passe sur Domaine: 66](#_Toc98835168)

[Adhesion à un DOmaine 68](#_Toc98835169)

[Appartenir à un Domaine depuis un client 10-SEVEN : 68](#_Toc98835170)

[1-m Création du compte ordinateur sur le serveur (manuelle) 68](#_Toc98835171)

[1-a Création du compte ordinateur (à la volée) 69](#_Toc98835172)

[2 –m Création de l'enregistrement hôte dans le DNS (manuelle) 70](#_Toc98835173)

[2 –a Création de l'enregistrement hôte dans le DNS (à la volée) 70](#_Toc98835174)

[3 Saisie dans les paramètres Tcp-ip et vérification du nom machine 71](#_Toc98835175)

[4 Demande d'adhésion au Domaine 71](#_Toc98835176)

[Ouverture de Session 73](#_Toc98835177)

[Dernier login utilisé : 73](#_Toc98835178)

[Ouverture de session Normalisée (depuis SEVEN) : 74](#_Toc98835179)

[Changement avec ouverture avec XP : 74](#_Toc98835180)

[Comptes utilisateurs de domaine 75](#_Toc98835181)

[Comptes Utilisateurs Prédéfinis : 75](#_Toc98835182)

[Créer un Compte Utilisateur sur le Domaine: 76](#_Toc98835183)

[Propriété Compte Utilisateur de Domaine: 77](#_Toc98835184)

[Compte Utilisateur onglet Général : 78](#_Toc98835185)

[Compte Utilisateur onglet Compte : 78](#_Toc98835186)

[Compte Utilisateur onglet Profil : 79](#_Toc98835187)

[Compte Utilisateur onglet Membre de : 80](#_Toc98835188)

[Groupes Locaux 81](#_Toc98835189)

[Privilèges - permissions : 81](#_Toc98835190)

[Groupes Locaux Prédéfinis : 81](#_Toc98835191)

[Groupe Local Administrateurs 82](#_Toc98835192)

[Groupe Local Utilisateurs 82](#_Toc98835193)

[Groupe Local Invités 82](#_Toc98835194)

[Opérateur de sauvegarde 82](#_Toc98835195)

[Opérateur de Serveur 82](#_Toc98835196)

[Groupe Local Utilisateurs Bureau à Distance 83](#_Toc98835197)

[Groupe Local Opérateurs de configuration réseau 83](#_Toc98835198)

[Groupe Local Utilisateurs avec Pouvoir (que sous SEVEN - XP) 83](#_Toc98835199)

[Groupes Spéciaux 83](#_Toc98835200)

[Utilisateur authentifiés 84](#_Toc98835201)

[Tout le monde 84](#_Toc98835202)

[Créateur propriétaire 84](#_Toc98835203)

[Anonymous Logon 84](#_Toc98835204)

[Réseau 84](#_Toc98835205)

[Interactifs 84](#_Toc98835206)

[Groupes Globaux-Universels 85](#_Toc98835207)

[Groupes locaux - globaux - universels: 85](#_Toc98835208)

[Groupes Globaux prédéfinis 86](#_Toc98835209)

[Admins du Domaine 86](#_Toc98835210)

[Utilisateurs du Domaine (Utilisa. du Domaine sous 2003) 86](#_Toc98835211)

[Invités du Domaine 86](#_Toc98835212)

[Inclusions entre groupes sous NT 87](#_Toc98835213)

[Quelques règles pour créer des groupes : 88](#_Toc98835214)

[Exemple : Utilisateur de Domaine - Utilisateur avec pouvoir 88](#_Toc98835215)

[Exemple accès ressources : 89](#_Toc98835216)

[Exemples : 89](#_Toc98835217)

[Exemple : Groupes Admins de Domaine & Administrateurs: 90](#_Toc98835218)

[Création – gestion de groupes 91](#_Toc98835219)

[Groupe local sur un poste: 91](#_Toc98835220)

[Groupe local – Global sur un Serveur CD: 91](#_Toc98835221)

[Membres d’un groupe: 92](#_Toc98835222)

[Gérer - Information sur les groupes - 93](#_Toc98835223)

[Suppression d'un groupe 93](#_Toc98835224)

[Répertoire de base 94](#_Toc98835225)

[Répertoire de base ou d'Accueil : 94](#_Toc98835226)

[Mise en Place : 94](#_Toc98835227)

[Avant la création des comptes 94](#_Toc98835228)

[Pendant la création d'un compte 95](#_Toc98835229)

[Résultat : 96](#_Toc98835230)

[Modifier le répertoire de base : 97](#_Toc98835231)

[Script d'ouverture de session 98](#_Toc98835232)

[Objectif : 98](#_Toc98835233)

[Indiquer un script d'ouverture de session : 98](#_Toc98835234)

[Ecriture de scripts : 99](#_Toc98835235)

[création de lecteur logique 99](#_Toc98835236)

[Commande NET 100](#_Toc98835237)

[Convention d'écriture : 100](#_Toc98835238)

[Commandes NET Utilisables : 100](#_Toc98835239)

[Net Use : 101](#_Toc98835240)

[Net User 102](#_Toc98835241)

[Net view: 104](#_Toc98835242)

[Sauvegarde Serveur 105](#_Toc98835243)

[Ajout du Rôle Sauvegarde : 105](#_Toc98835244)

[Effectuer une Sauvegarde: 107](#_Toc98835245)

[Restauration...: 110](#_Toc98835246)

[Restaurer Active Directory: 110](#_Toc98835247)

[Exécuter une restauration non forcée: 112](#_Toc98835248)

[Exécuter une restauration forcée totale : 112](#_Toc98835249)

[PB mot de passe Restauration : 112](#_Toc98835250)

# Versions Windows Server

## Versions 2012 et 2012R2:

**N.B**: **2012R2** dispose des mêmes fonctionnalités que **2012**, cela correspond simplement à ce que l'on nommait auparavant un **Service pack**.

4 versions existent nommées

**Essential – Foundation - Standard – Datacenter**

### Essential

* Limite à un processeur physique (illimité en cœurs)
* Limité à 15 connexions utilisateurs (pas de Cal requises)
* Impossibilité de faire de la virtualisation, ni TSE
* Utilisation en OEM seulement (ne peut pas être vendu séparément)

### Foundation

* Licence unique par serveur
* Possibilité d’avoir un serveur bi-processeur avec une seule licence
* Connexion de 25 utilisateurs max, sans licence TSE (CAL)
* Cette édition de Windows Server peut être virtualisée, mais ne peut pas servir d’hôte de virtualisation (Hyper-V)

### Standard

* Licence unique par serveur et pour deux processeurs uniques (nombre de cœurs processeur illimité)
* Possibilité de virtualiser cette édition de Windows Server et de le transformer en hôte de virtualisation (Hyper-V)
* Cette licence est « activable » dans deux VM Hyper-V du même serveur physique.
* Aucune bride / limite quant aux utilisateurs et licences d’accès TSE
* Aucune bride quant aux rôles de Windows Server

### Datacenter

* Même droits / caractéristiques que l’édition « Standard »
* Pas de restriction quant au nombre de VM créées dans l’hyperviseur Hyper-V

Retrogradation possible vers 2008R2

* Windows Server **2012 Datacenter** peut être rétrogradé en **2008 Datacenter, Enterprise ou Standard**.
* Windows Server **2012 Standard** peut être rétrogradé en **2008 Enterprise ou Standard**.  
  On a toujours de votre droit à 2 machines virtuelles dans Hyper-V.

## Nouveautés 2016:

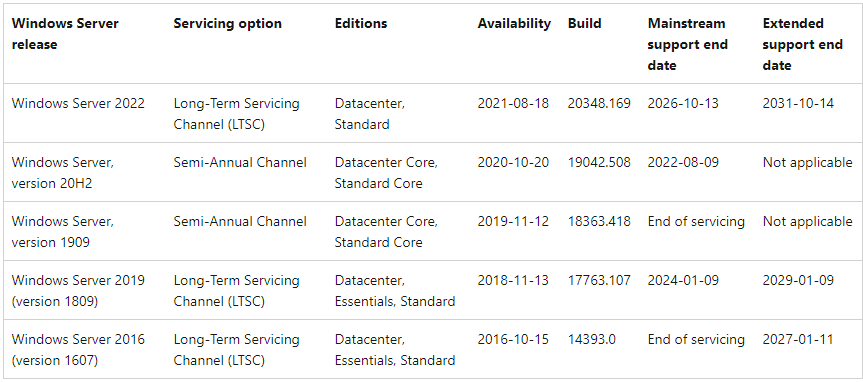
* **Nano Server** : Cette variante d'installation est nettement plus légère (20 fois) avec une fréquence de mise à jour et au nombre de patches requis plus réduits. **Nano Server** n'embarque que les composants essentiels tels que Hyper-V, les services réseaux, de cluster et de stockage. et pas d'interface graphique…Par exemple on à la possibilité d'installer un hôte Hyper-V tout en utilisant seulement 500 Mo de capacité de stockage.
* **Windows Defender pour Server** : une fonction intégrée qui protège le serveur directement après son installation.( Et une simple commande suffit pour retirer rapidement Windows Defender). Pour des raisons de sécurité, le recours à cette fonction peut constituer cependant la première démarche.
* **Storage Spaces Direct**: disponible en tant qu'extension des espaces de stockage existants. Le principe, à savoir l'utilisation de disques locaux dans un cluster de virtualisation permet d'avoir du stockage pour les machines virtuelles à moindre cout ( pour éviter la mise en place d'infrastructures SAN complexes.)
* **Hyper-V**: permet d'ajouter des cartes réseaux et de la mémoire à une machine virtuelle en cours de fonctionnement. Et la « Nested Virtualization » permet d'exploiter des services virtualisés dans un environnement virtuel déjà existant.
* **Container:** ce sont des systèmes isolés qui mettent des applications à disposition. Les conteneurs utilisent des ressources de l'hôte, telles que système d'exploitation, bibliothèques ou mémoire de travail et démarrent ainsi bien plus vite que les machines virtuelles classiques. Windows Server 2016 introduit la prise en charge des **containers Docker** qui peuvent être déployés et administrés sur un serveur Microsoft ou depuis le client Docker pour Windows ou par le biais de PowerShell. en parallèle la déclinaison de l'hyperviseur de Microsoft pour prendre en charge les containers **Hyper-V Containers**.
* **Azure Stack**: permet de créer un réel Cloud hybride avec les outils intégrés par Microsoft et de mettre à disposition des services IaaS et PaaS. Un environnement Azure-Stack tourne indépendamment du Cloud public Azure, mais peut échanger des données et à disposition des services communs dans un Cloud hybride.

## Nouveautés 2019:

* **Version LTSC** : Cette variante d'installation est nettement plus légère (20 fois) avec une fréquence de mise à jour et au nombre de patches requis plus réduits. **Nano Server** n'embarque que les composants essentiels tels que Hyper-V, les services réseaux, de cluster et de stockage. et pas d'interface graphique…

## Versions de référence:

[Windows Server release information | Microsoft Docs](https://docs.microsoft.com/en-us/windows/release-health/windows-server-release-info)



**N.B** : Les versions de référence correspondent à des versions **LTSC/LTSB**.

|  |  |  |
| --- | --- | --- |
| Version 1607 (build 14393) | **Windows Server 2016** | **LTSB - 2016** |
| Version 1809 (build 17763) | **Windows Server 2019** | **LTSC - 2019** |
| Version V1909 (build 18363) | **Windows Server 1909** |  |
| Version V20H2 (build 19042) | **Windows Server 20H2** |  |
| Version V21H2 (build 20348) | **Windows Server 2022** | **LTSC - 2021** |

**Ver publique Sortie Build (majeur) Build mineur**

LTSB

**Srv 2016** v1607 15/10/16 **14393** build initial **0**

**Srv 2019** v1809 13/11/18 **17763** build initial **107**

LTSC

**Srv 1909** v1909 12/11/19 **18363** build initial **418**

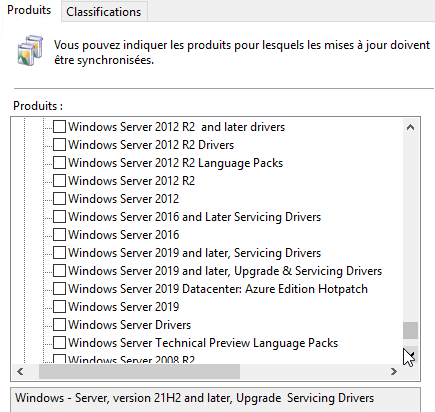
**Srv 20H2** v 2009 20/10/20 **19042** build initial **508**

**Srv 2022** v21H2 18/08/21 **20348** build initial **169**

LTSC

## Classification WSUS - Produits:

On retrouve en simplifié les catégories présentes pour Windows 10 ,



Avec quelques particularités notamment pour la version 2022

* **Windows – Server, version 21H2** correspond à **Windows Server 2022**



* Une possibilité por les Hotpatch de 2022 (21H2)



Alors que



* Correspond à 1 base commune à **Windows Serveur 2022** et le **Système Windows 10 21H2**

## Versions & options d'installation & MAJ 2016:

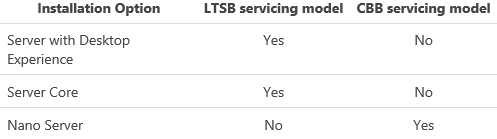
Il existe 3 Versions fonctionnelles principales

* **Essentials**: avec maximum 50 clients utilisateurs. Sans Hyper-V
* **Standard**: sans les fonctionnalités de , et avec 2 Vm maximum.
* **Datacenter**: toutes les fonctionnalités existantes, et autant de Vm que l'on souhaite

Pour les 2 versions majeures, c’est-à-dire et **Datacenter** et **Standard**, il y a 3 options d'installation :

* **Desktop experience** : avec une interface graphique
* **Core** : sans interface graphique.
* **Nano**: version allégée, sans interface graphique

En ce qui concerne les options de mises à jour possible, **LTSB ou CBB** , le tableau suivant détaille les possibilités**, LTSB** est indisponible sur **Nano Server**



## Versions fonctionnelles 2022-2016:

2 versions tarifées par Cœur**, standard et datacenter**, 1 par processeur, **Essential**

### Essential

* Limite à un processeur physique (illimité en cœurs)
* Limité à 50 connexions utilisateurs, pas de CAL requises
* Impossibilité de faire de la virtualisation, ni TSE
* Utilisation en OEM seulement (ne peut pas être vendu séparément)

### Standard

* Licence par coeur
* Possibilité de virtualiser cette édition de Windows Server et de le transformer en hôte de virtualisation (Hyper-V)
* Cette licence est « activable » dans deux VM Hyper-V du même serveur physique.
* Aucune bride / limite quant aux utilisateurs et licences d’accès TSE
* Aucune bride quant aux rôles de Windows Server, sauf storage server,

### Datacenter

* Licence par coeur
* Pas de restriction quant au nombre de VM créées dans l’hyperviseur Hyper-V
* Même droits / caractéristiques que l’édition « Standard » ,plus windows storage server

**Détail par Rôles classiques**



(1) Limited to the setting up of certification authorities - other features of the Active Directory Certificate Services (Network Device Enrollment Services, Online Responder Service)) are not available. More information can be found in the description of the AD CS role on TechNet.[[4]](https://www.thomas-krenn.com/en/wiki/Windows_Server_2016_Editions_comparison#cite_note-4)

(2) Must be the root of an ADDS domain structure and must own all operating master roles.

(3) Access requires an additional AD RMS CAL.

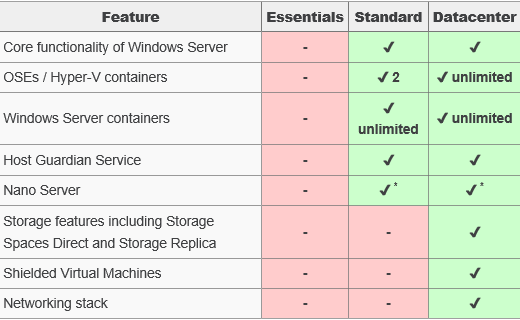
(4) Data deduplication is not available.

(5) Limited to 50 RRAS connections and 50 IAS connections; DirectAccess and VPN are supported.

(6) Access requires an additional RDS CAL (exception: using the Remote Web Access feature of the Essentials Edition).

(7) Only RD Gateway service is installed and configured, other remote services (including RD session host) are not supported.

**Détail par Nouveaux rôles 2016**



## 2016 Licensing par cœur ou processeur:

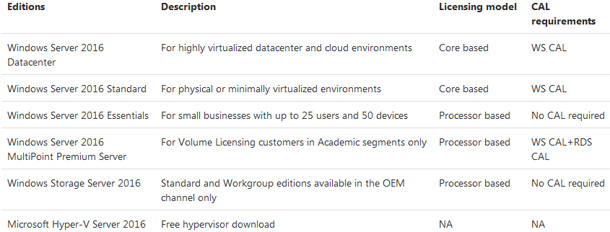
En termes de licence, Windows Server est désormais tarifié, pour ses éditions **Standard** et **Datacenter** en fonction du nombre de cœurs et plus du nombre de processeurs. L'objectif de Microsoft est d'uniformiser les modes de licence entre **Windows Server** et **Azure**, pour simplifier la situation en environnement de cloud hybride

Les 2 versions principales de Windows sont tarifées par Cœur,

* **Standard**
* **Datacenter**

Et 3 autres par processeurs

* **Essential**
* **Multipoint Server 2016 Premium**
* **Storage Server,**



# Licensing par coeur

## Socket, processeur, cœur, hyper-threading:

Un socket c'est l'emplacement physique sur la carte mère permettant de recevoir un processeur, les différents types de sockets définissent les types de processeurs que l'on peut y enchâsser

Les cartes mères peuvent recevoir de 1 (minimum évidemment) a 2-4-8 ou plus processeurs…

On fait souvent l'analogie suivante :

**1** processeur = **1** processeur physique (1 chipset)

Depuis 2005 les processeurs ont eu la capacité de recevoir plusieurs cœur, cela a provoqué la fin des "pentium"

Dans un processeur **multi core** se trouve plusieurs cœurs de calcul, ce qui revient à avoir plusieurs processeurs. Si un processeur possède deux cœurs, on parle de double cœur (**dual core** en anglais), s’il en possède quatre, on parle de **quadricœurs** (**quad core** en anglais)

**1** processeur **multi-core** = **X** x processeurs physiques (1 chipset)

Par exemple

**1** processeur **dual-core** = **2** processeurs physiques (1 chipset)

**1** processeur **quad-core** = **4** processeurs physiques (1 chipset)

**Hyper-Threading** est une technologie d’Intel et ne peut être présent que sur leurs processeurs. Un processeur avec la technologie **Hyper-Threading** permet de simuler virtuellement 2 processeurs (mais avec des performances moindres). **N.B**: Certains OS ne voient même pas la différence.

**L’Hyper-Threading** est compatible avec les processeurs **multicoeurs**. Ainsi, un processeur **quadricore** avec la technologie **Hyper-Threading** permet d’avoir au final 8 centres de calcul travaillant en parallèle

**1** proc **multi-core hyper-thread** = **2** x **X** x proc physique (1 chipset)

Par exemple

**1** **dual-core hyper-thread** = **2** proc physiques (1 chipset)

= **4** proc logiques

**1** **quad-core hyper-thread** = **4** proc physiques (1 chipset)

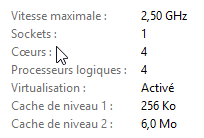
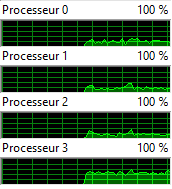
= **8** proc logiques

**EXEMPLE 1**

**Processeur 2 Cœurs et hyperthread 4 proc logiques**

Ici L'OS ne voit même pas la différence



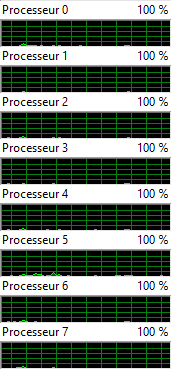
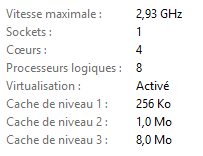
** **

**EXEMPLE 2**

**Processeur 4 Cœurs et hyperthread 8 proc logiques**

ici L'OS détecte l'hyperthread et comptabilise 4 cœurs et 8 proc logiques





## Licensing server 2016 serveurs physiques:

La licence est vendue par pack de 2 cœurs physiques (et non pas hyperthread) et donc plus par processeur physique.

Microsoft annonce que Le prix d'un "pack 2-cœurs" ou **Core Pack** correspond à 1/8 du prix d'une licence 2-socket pour Windows Server 2012 avec les 2 règles minima suivantes :

* Chaque processeur physique (socket) doit être couvert à minima par 8 licences (soit 4 Core Pack).
* Chaque serveur physique doit être couvert à minima par 16 licences (soit 8 Core Pack).

**Exemple**

Processeur : **1** Intel® Xeon® E3-1220 v5 avec 4 cœurs

Soit 4 cœurs à couvrir par des licences

Comme au minimum il faut "huit cœurs pour un processeur physique", et "16 cœurs pour un serveur" il nous faudra 8 licences 2 cœurs (dont 12 inutilisées…)

**Exemple**

Processeur : **2** Intel® Xeon® E5-4610 v3 avec 10 cœurs chacun.

Soit 2 processeurs X 10 cœurs = 20 cœurs à couvrir par des licences.

il nous faudra10 licences 2 cœurs

## Licensing server 2016 serveurs virtuels:

La règle est exactement la même si vous positionnez des licences pour chaque machine virtuelle, ce qui serait une erreur de déploiement de vos licences.

En effet pour chaque VM il faudrait se plier à la règle des minimas, c’est-à-dire minimun 8 cours par processeurs, et 16 cœurs par serveur physique sur lequel la VM tournerais..

Tout comme pour Windows Server 2012 il faut donc plutôt prendre en compte la capacité de virtualisation des systèmes d’exploitation Microsoft des deux éditions.

* **Standard** : Deux Système d’exploitation virtuels si tous les cœurs physiques du serveur hôte sont couverts par des licences.
* **Datacenter** : autant de Système d’exploitation virtuels que l'on souhaite si tous les cœurs physiques du serveur hôte sont couverts par des licences.   
  Au delà de 6 Vm formule quasiment obligatoire.

## Licensing CAL server 2016:

Les Licences d’Accès Client (CAL) ne changent pas :

* + **CAL par « User »** : chaque utilisateur qui accède à l’infrastructure peut être couvert par une CAL « User » et peut utiliser jusqu’à 5 périphériques (DEVICE).
  + **CAL par « DEVICE »** : chaque dispositif Windows qui accède à l’infrastructure peut être couvert par une CAL « DEVICE ».

Déjà, on ne prend plus jamais des licences clients en mode "Par serveur" !!! Cela revient à devoir acheter une CAL pour chaque connexion/user et pour chaque serveur.

Le mode dit "par site/siège" permet d'utiliser la même licence client pour tous les serveurs...

Donc Si l'on a beaucoup d'utilisateurs, mais peu de périphériques. Par exemple 60 ordinateurs partagés par 500 personnes, on peut se limiter à 60 licences liées aux machines.

En revanche, si chaque utilisateur a son propre ordinateur, voire un mobile, une tablette, etc.... il faut éviter le mode par périphériques!!! Et choisir le mode "par utilisateur" (tendance actuelle)

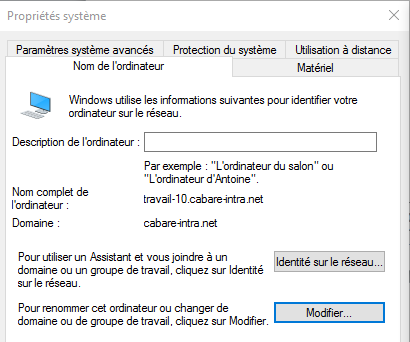
# Les NOMS de poste Windows

## Nom d'hôte - nom netbios Windows :

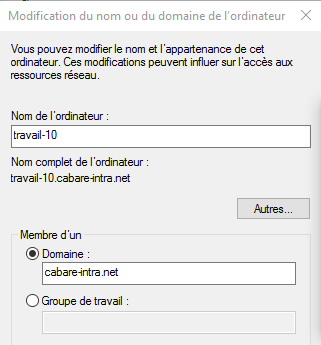
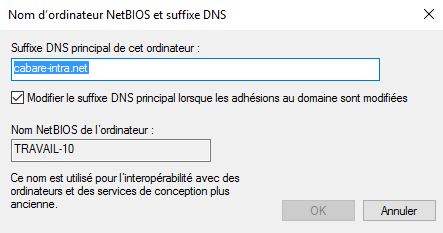
A noter qu'un nom d'hôte et un nom d'ordinateur (nom netbios 15 caractères maxi, lettre chiffre tiret pas de différence à la casse) sont deux choses différentes, même si par défaut, dans un réseau microsoft, ce sont les mêmes. En toute rigueur, ils se définissent ainsi :

**10-SEVEN: Nom netbios** = **Nom d'hôte** par défaut, (traduction automatique) : mais on peut en spécifier un différent, NON CONSEILLE !

via **Modifier**

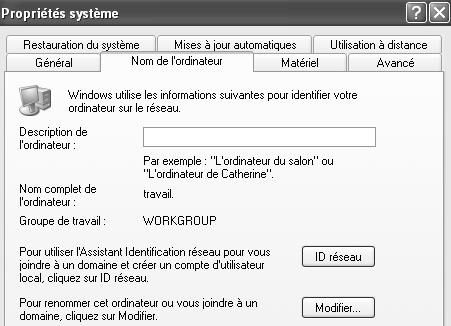
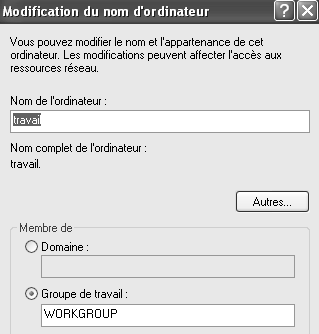


Puis **Autres**



Particularité :

**depuis windows XP:**



Apparition d'une zone   
"**Description de l'ordinateur**"

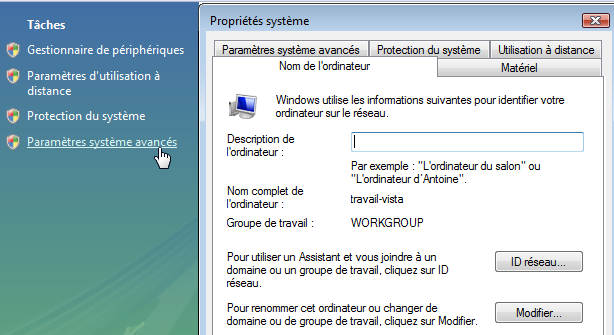
A ne pas confondre avec le nom de l'ordinateur

Accessible par **Modifier…**

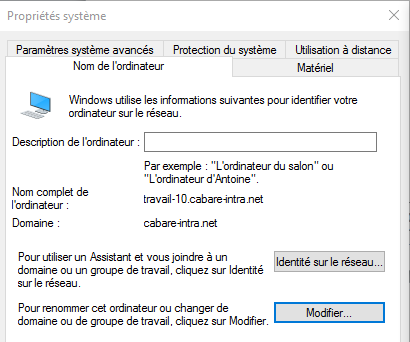
**N.B:** ne jamais rentrer une **Description de l'ordinateur** différente du **Nom de l'ordinateur**

**N.B:** ne jamais suivre l'exemple, mais utiliser les règles classiques (- de 15 caractères… etc…)

**idem windows SEVEN :**



**idem windows 10 :**



# Rechercher un poste

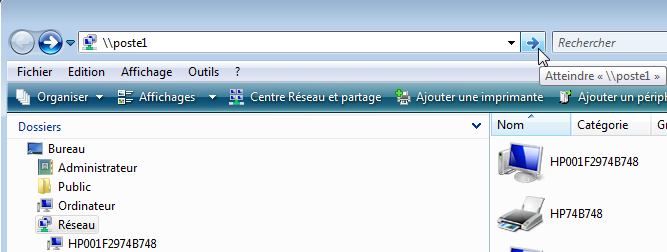
## Pourquoi je ne vois pas tel ou tel poste ?:

Souvent, un poste est long à apparaître, puis il apparaît comme par « magie » au bout d’un délai qui semble interminable. Il faut bien penser que les postes font autre chose de temps en temps que d’envoyer des trames sur le réseau dans le seul but de mettre à jour l’affichage !

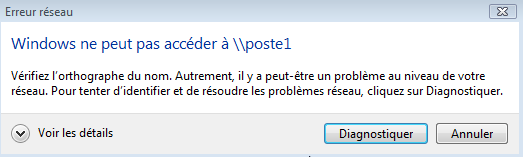
### S’assurer alors qu’un poste est bien présent:

On peut lorsque l’on demande de voir le réseau, demander alors d'atteindre une machine particulière

il suffit de taper le nom netbios UNC, sous la forme **\\nom-machine** dans la barre de titre

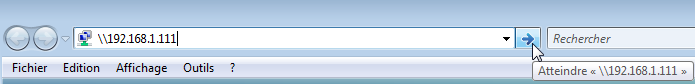


Si le nom n'existe pas (ou ne peut être trouvé) alors on obtient un message



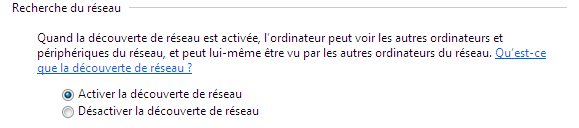
si le nom est correct, le poste s'affiche…

**N.B**: on peut aussi taper une adresse ip

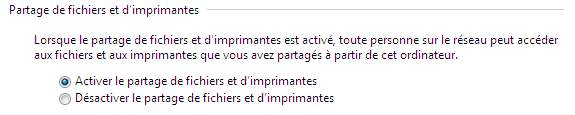


## Réglage profils réseaux:

Les réglages suivants existent selon les profils réseaux… Surtout



Pour voir les postes dans les favoris réseaux…



Mais pour que cela soit possible, il faut absolument que les 4 services suivants soient démarrés sur le poste  (ce qui n’est pas toujours le cas):

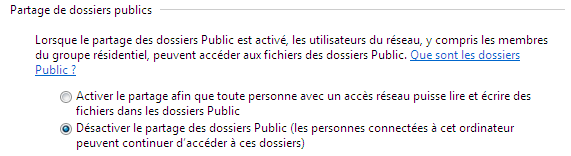
**Client DNS** **Publication des ressources…**

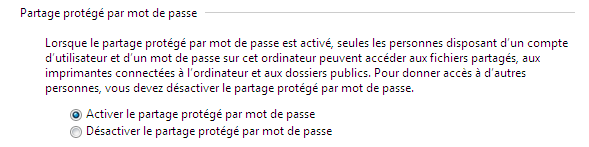


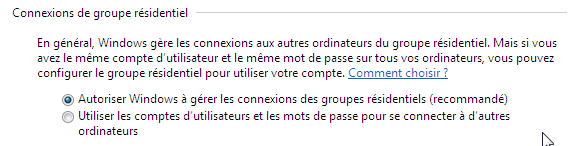
**Découverte SSDP Hôte de périphérique**

**Dossiers publics** et **groupe résidentiels** ne devraient pas être activés sur des machines professionnelles…



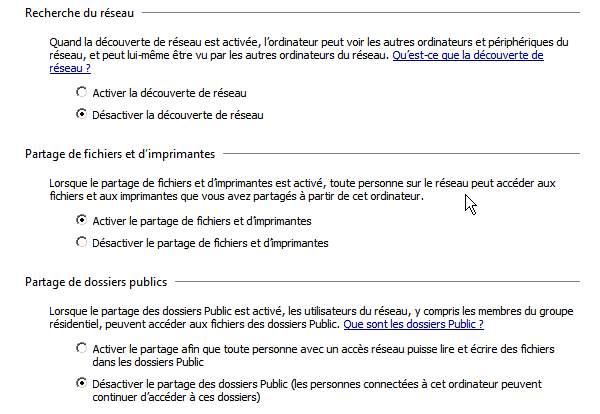




## Jeux de Réglages:

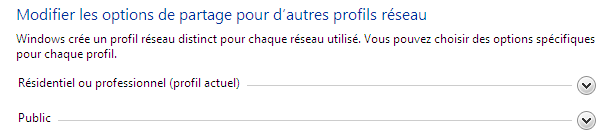
Le jeu des réglages est quasiment le même dans tous les profils...

à chaque emplacement correspond un "jeu de réglage" pré-réglé



Sur une machine en workgroup deux profils type existent

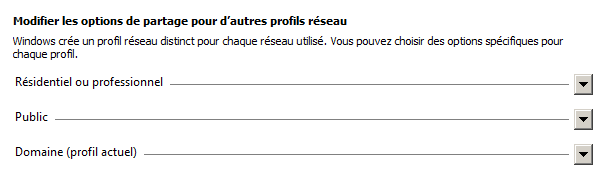
* un répondant au label "**privé**"



* un répondant au label "**public**"

Sur une machine appartenant à un domaine un troisième profil apparaît (et on ne peut pas en choisir un autre)

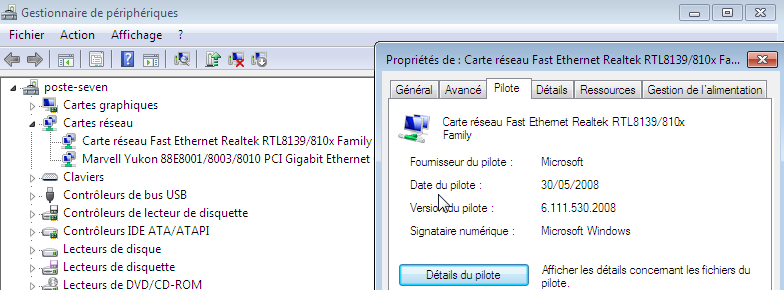
* répondant au label "**domaine**"



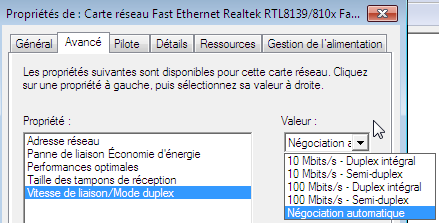
# les Cartes réseau

## Carte réseau & Driver Certifié :

Si aucune carte réseau n'est détectée, il faut installer un driver certifié …

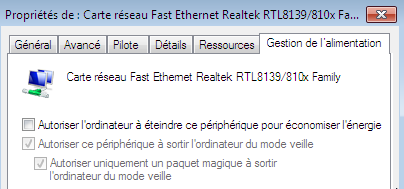


En cas de problème "physiques", on peut vérifier que le driver gère correctement nos flux Ethernet selon notre connectique



**N.B**: ces réglages sont parfois difficiles à trouver, ils dépendent des drivers …

On peut aussi éviter pour des raisons ACPI d'éteindre la carte réseau…

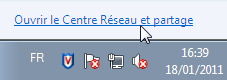


## Accès au Centre Réseau et partage :

Si une carte réseau (minimum) est installée correctement, une icône "réseau" devrait apparaître en bas à droite… 

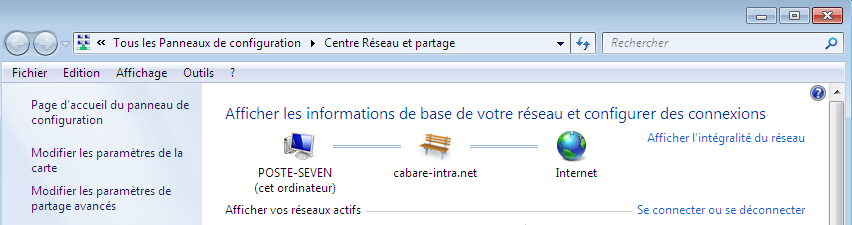
Quel que soit sont aspect…    

Un clic dessus puis "**Ouvrir le Centre Réseau et partage**"



On peut aller aussi aux réglages du pare-feu

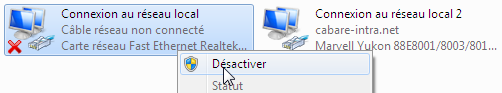
## Désactivation Carte Excédentaire :



**Modifier les paramètres de la carte** donne accès en fait à toutes les cartes physiques… Si plusieurs cartes réseaux sont présentes, il est plus judicieux de désactiver celle que l'on n'utilise pas.



Clic droit **Désactiver**

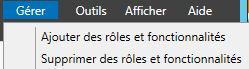


## Connexion Wifi sur Serveur :

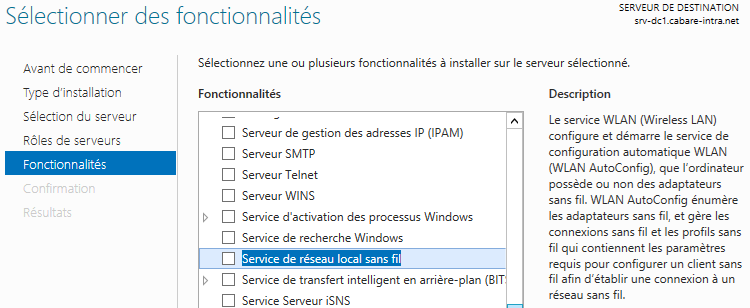
Bien évidement cela ne peut être qu'une connexion de secours ou temporaire. On privilégiera toujours du Filaires ou de la Fibre

A ce propos, une carte Wifi présente sur un serveur, même avec son driver certifié installée ne sera pas opérationnelle tant que l'on n'aura pas ajouter une fonctionnalité précise, et activer le service correspondant.

**Fonctionnalité** à Ajouter

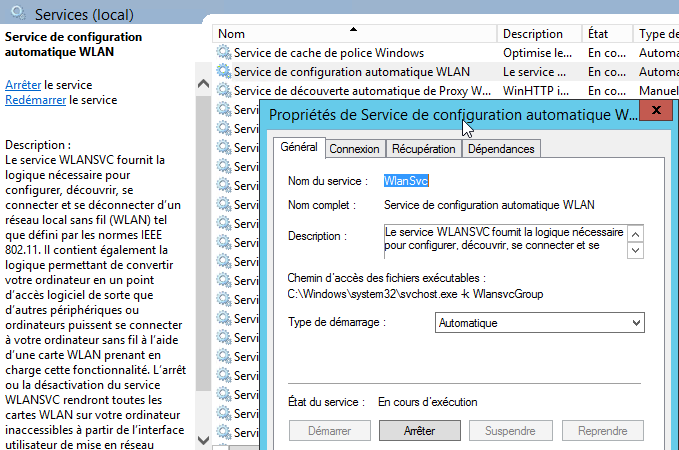


**Service de réseau local sans fil**



**Service de configuration automatique WLAN**

Qu'il faut démarrer bien sûr



# Autorisations de partage - Permissions d'accès (ntfs)

## Autorisation de Partage :

Toute personne connectée sur le réseau est un utilisateur qui peut accéder à des ressources qui ont été au préalable partagée.

Que le disque soit en FAT, FAT32 ou NTFS on doit forcément le partager pour pouvoir y accéder depuis le réseau

Les autorisations de partages s'appliquent également sur des ressources qui ne sont pas des espaces de stockage, comme des imprimantes ou des lecteurs de CDROM....

## Partage et Sécurité:

C'est à ce niveau-là qu'il va y avoir une différence entre des systèmes disques montés en FAT32, ou des systèmes disques montés en NTFS....

### En système FAT32:

* La seule sécurité possible sur une partition FAT32 est celle apportée par les mécanismes de partage de répertoire
* Par conséquent rien n'est prévu pour limiter les accès depuis une session locale

### En système NTFS :

* Les mécanismes de partage de répertoire existent sur un système NTFS pour réguler les tentatives d'accès depuis le réseau
* Mais les fichiers et les dossiers sur une partition NTFS peuvent se voir attribuer des permissions d'accès **indépendamment de leurs partages**, par conséquent NTFS est prévu pour limiter les accès aussi depuis une session locale

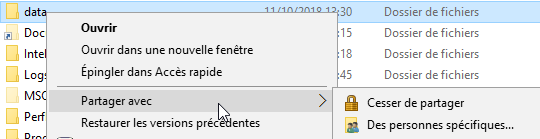
**N.B**: Sans refaire un chapitre en NTFS, il est clair que si la sécurité NTFS est disponible, alors au niveau des partages on laissera systématiquement **Tout le Monde** en **Contrôle Total** (ou en Lecture seule à la limite)

Et le chapitre suivant est … inutile !

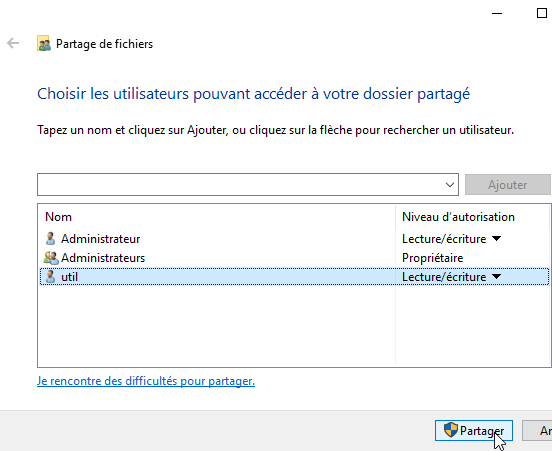
# Autorisations de Partage

## Assistant partage simplifiés

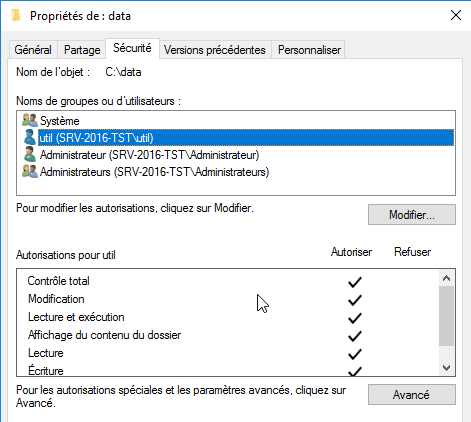
Disponible soit avec les propriétés du dossier, soit avec un clic droit sur le dossier à partager



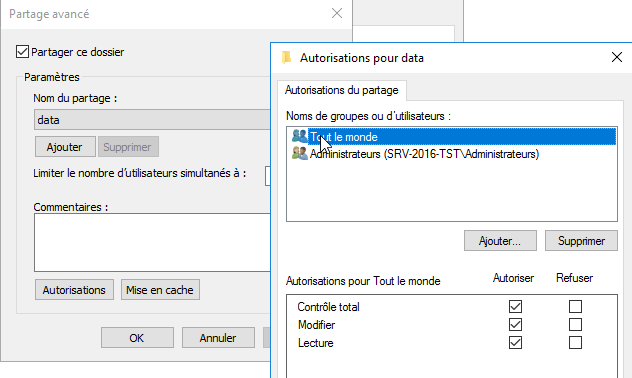
Lorsque l’on ajoute un utilisateur, par exemple ici ***Util***



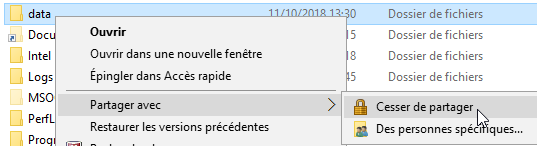
Cela a posé de la **sécurité NTFS** sur le dossier pour Util



Mais pas une **autorisation de partage** (visible dans partage avancé)



Pour supprimer le partage, il faut alors demander sur le dossier, via un clic droit **Cesser de partager**

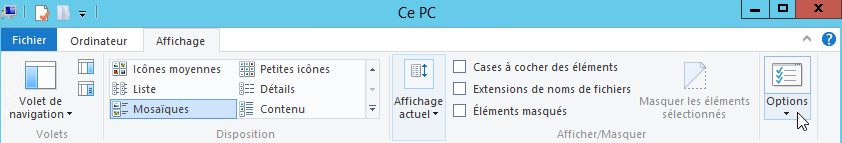


**N.B** : cela modifie la sécurité NTFS concernant les éventuels utilisateurs associés !!!!!

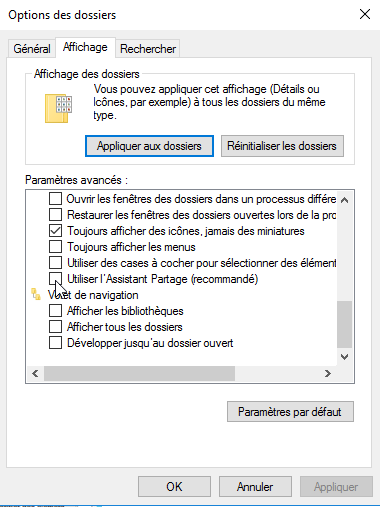
## Désactiver les partages simplifiés:

Afin de pouvoir travailler correctement, il faut désactiver la gestion simplifiée des partages, pour ne plus risquer d'avoir accès à l'assistant…

Dans le **Gestionnaire de fichier**, on demande dans l'onglet **Affichage**, **Options / modifier les options des dossiers et de recherche**

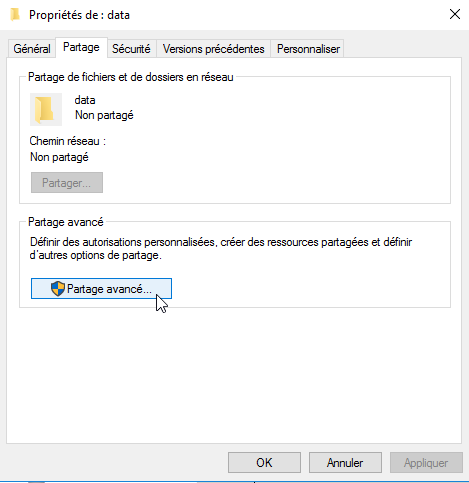


Et on décoche **Utiliser l'Assistant de Partage (recommandé)**



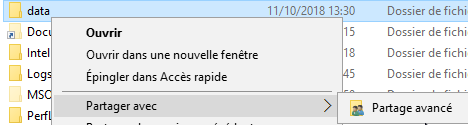
## Partage Avancé:

Toujours disponible via les propriétés du dossier, Il suffit de se placer sur la ressource à partager, puis de demander le menu contextuel **Propriétés**, onglet **Partage…**



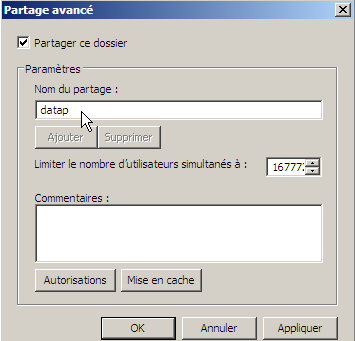
l'assistant est dévalidé, cela tombe bien, il ne faut pas s'en servir !

Ou clic droit sur le dossier à partager **/ partage avancé**



on demande **Partage avancé**…

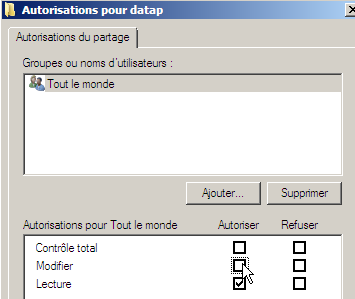
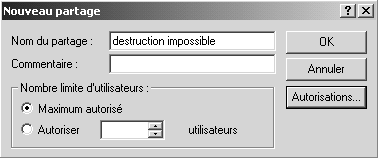
On obtient



Si on veut en réserver l'accès à certains comptes utilisateurs ou à certains groupes, il va falloir travailler sur les autorisations de partage en cliquant sur **Autorisations** ...

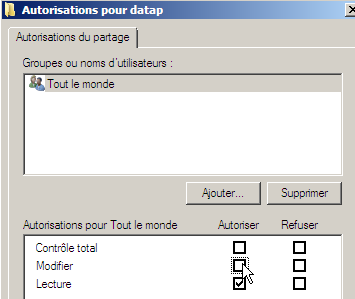
Attention : une ressource peut être partagée plusieurs fois par **Nouveau partage** sous des noms différents avec des autorisations différentes…

**Dans un premier temps partagez une ressource que sous un seul nom !**



## Donner une Autorisation de Partage:

Ce sont les **Autorisations** que l’on doit donner pour filtrer qui peut accéder à cette ressource depuis le réseau



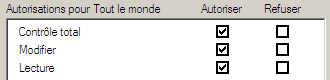
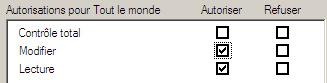
On peut Ajouter d’autres Groupes ou Utilisateurs par le bouton **Ajouter**

Sur lequel on appliquerait ensuite des Autorisations

(ou des Refus !)

Le **Groupe Spécial Tout le Monde** est inclus par défaut ...en **Lecture**

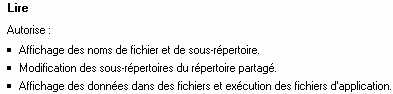
Mais on peut aussi donner

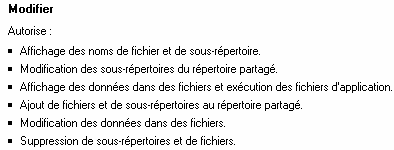
ou 

Attention aux valeurs des partages par défaut:

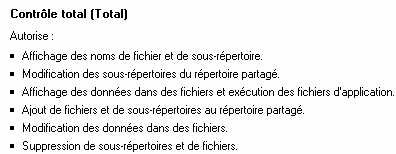
* Sous 2012 et 02016 Serveur un partage par défaut sera de type **Tout le Monde** en **Lecture Seule**

### Les 3 "faux types" et 2 "vraies" Autorisations de Partage





**Modifier** et **Contrôle Total** sont équivalent en partage…



### Le refus de Partage

Le refus de partage « passe avant toute autre autorisation ».

Par exemple si un individu isolé dans un groupe ne doit pas faire une action, on lui appliquera un refus de partage juste à lui…, le fait que son groupe ait l’autorisation n’est pas gênant.

## Combinaison d'autorisations de partage :

deux règles régissent les combinaisons de permission

1. la permission effective de l'utilisateur est la permission la moins restrictive obtenue par la combinaison des différentes permissions
2. si une permission "refuser » est donnée, cette dernière masque toutes les autres permissions, et la permissions effective résultantes est donc "aucun accès"

**Donc si l'utilisateur est membre de plusieurs groupes, il hérite de toutes les permissions définies à travers chacun des groupes, sauf si la permission "refuser" est spécifiée pour au moins un groupe !**

## Planification des autorisations de partages:

Il est capital que au niveau de l'arborescence, les dossiers nécessitant d'un **niveau de sécurité identique**, soit **créés à un niveau identique.** Le dossier partagé apparaît en tant que "racine", et si on peut voir la totalité de ce dossier, et de ses éventuels sous-dossiers, on ne peut pas en "sortir". **donc, on peut accéder au contenu d'un dossier partagé (et donc à la totalité des sous-dossiers) , mais on ne peut pas accéder aux dossiers situés à un niveau plus élevé, ni aux dossiers de même niveau**

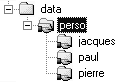
**N.B:** Il ne faut donc jamais partager tous les dossiers individuellement, mais seulement le point d'entrée de la hiérarchie.

**N.B:** Dans le cas on l'on ne dispose pas de volume NTFS on peut alors partager tous les dossiers individuellement, afin de construire une ébauche de sécurité…. MAIS CELA RESTE INCOMPLET ET PENIBLE.

### Exemple 1 :

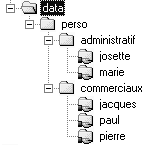
pierre, paul et jacques doivent avoir chacun un dossier personnel, sur lesquels l'administrateur à un droit de visite.

on commence par créer les dossiers personnels et les partages pour chacun

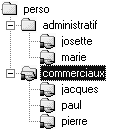
puis on partage au niveau supérieur (ici perso) pour l'administrateur : il verra toute la hierarchie et y aura accès !

### Exemple 2 :

pierre, paul, jacques marie et josette doivent avoir chacun un dossier personnel . Pierre, paul et jacques commerciaux, doivent avoir chacun un dossier personnel, sur lesquels les administratifs marie et josette ont un droit de regard. l'administrateur à un droit total sur tout le monde, ….



on commence par créer les dossiers personnels et les partages pour chacun

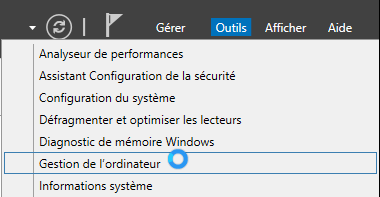


Puis on partage au niveau intermédiaire (ici commerciaux) pour le groupe des administratifs (marie + josette)

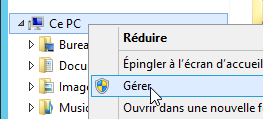
et enfin au niveau supérieur pour l'administrateur

## Gestion des partages

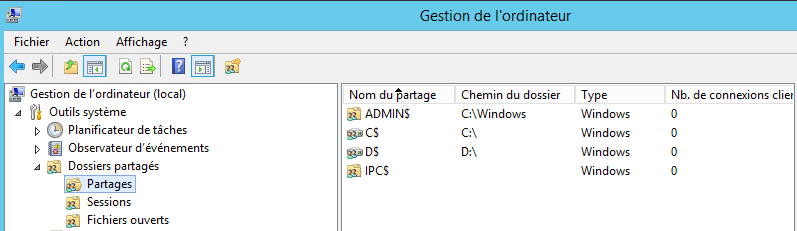
Soit par l'icône de la barre des tâches  **gestionnaire de Serveur / outils / gestion de l'ordinateur**



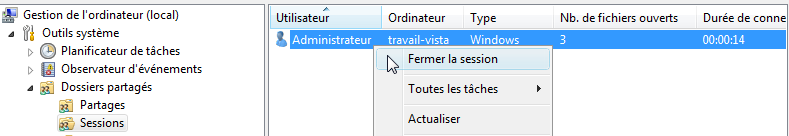
Soit **clic droit** / **gérer** du **poste de travail**, puis **outils / gestion de l'ordinateur**



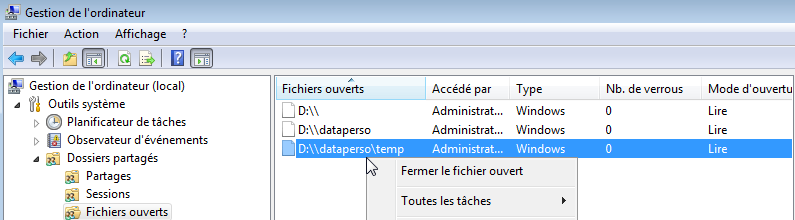
On obtient dans **Gestionnaire de l'ordinateur** / **dossiers partagés**



Onglet **Sessions**



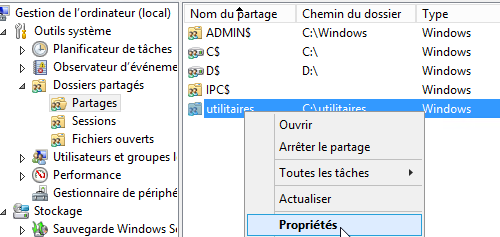
Onglet **Fichiers ouverts**



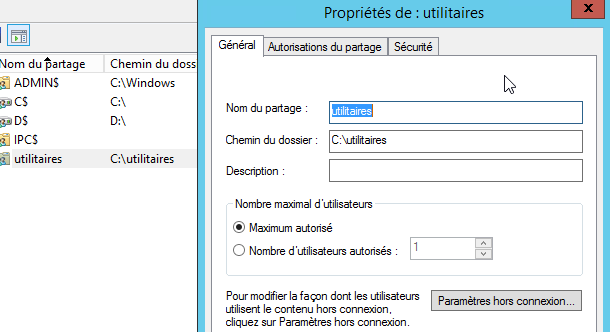
**N.B**: Sur Windows **10-SEVEN** il existe **10** sessions possibles simultanées maxi …

### Paramétrage des partages

on peut ensuite revenir sur un partage réalisé et demander les **propriétés** ...



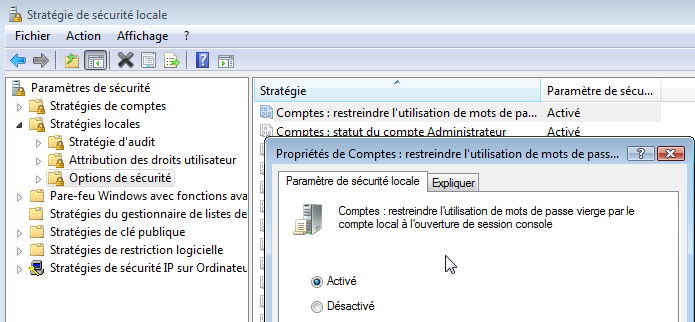
Et on retrouve alors directement



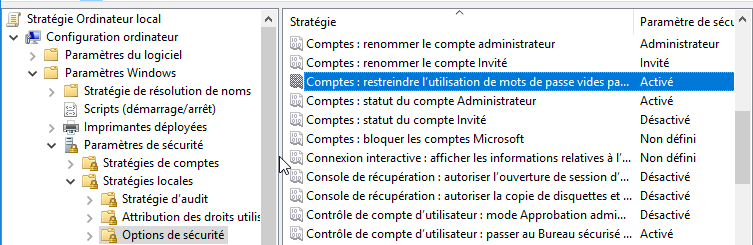
## Spécificité Windows 10 - 7 et mot de passe vide :

Les utilisateurs distants ne peuvent pas s'authentifier en utilisant un compte avec un mot de passe vide. Cette sécurité de l'authentification est configurée dans une **stratégie de sécurité locale**…

**Paramètres de Sécurité / Stratégies locales / Options de sécurité / Comptes:**

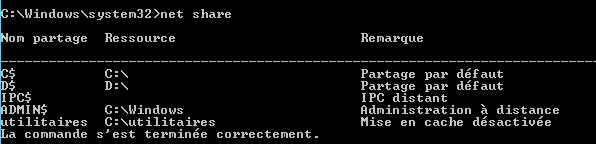


Cela est réglable dans une **GPO**



## Net share :

La commande **Net share** permet de visualiser les partages (aide en ligne possible via **net share /?**)

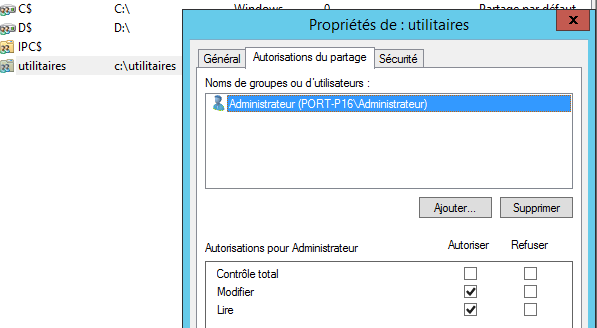


On peut supprimer un partage,



On peut créer un partage pour un utilisateur ou un groupe donné



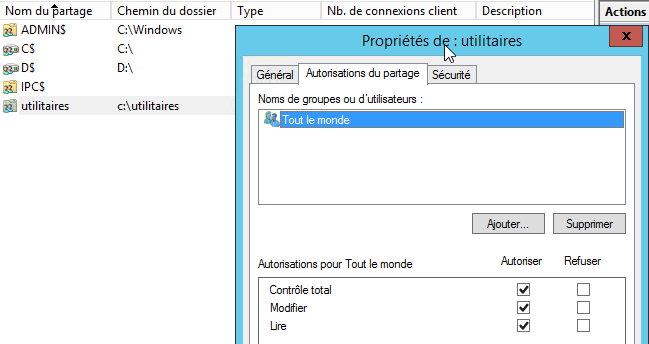


On peut créer un partage avec un groupe prédéfini (attention au nom avec " si besoin)



Voire

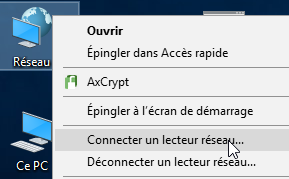




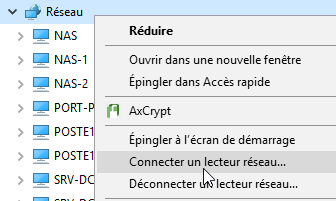
**N.B**: Par contre la situation au niveau NTFS est non modifiée !

# lecteurs réseaux Client Windows

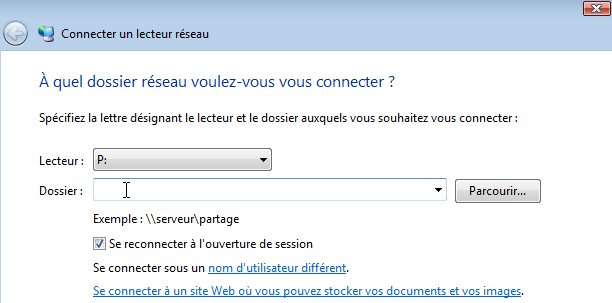
## Connecter un lecteur réseau client Windows:

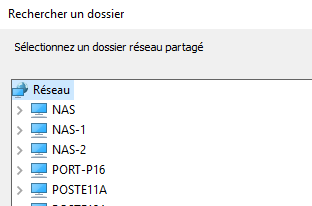
**N.B**: il faut bien sûr qu'un partage soit disponible coté "poste serveur", et que l'on ait les droits d'accès (partage + sécurité NTFS)

On accède à l’assistant connections de lecteur réseau en demandant

* le menu contextuel **Propriété** de l’icône **Favoris réseau** du bureau
* on peut aussi se placer directement sur la ressource à connecter… ou sur le début de l'arborescence réseau,

ou demander le menu **Outils / Connecter un lecteur Réseau**) pour obtenir cette boite de dialogue



on peut demander **Parcourir…**

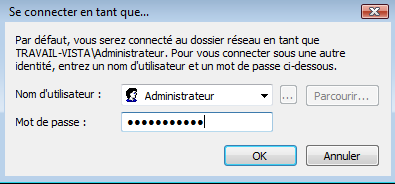
Mais on peut aussi sans attendre l'interface graphique entrer directement dans **Dossier** une invite du genre

 ou



\\nomserveur\nompartage \\adresse-ip\nompartage

On peut demander une autre authentification …

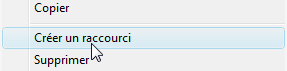


## Se Créer un raccourcis sur un lecteur / répertoire réseau :

Il faut bien sûr que le partage ait été fait sur le serveur

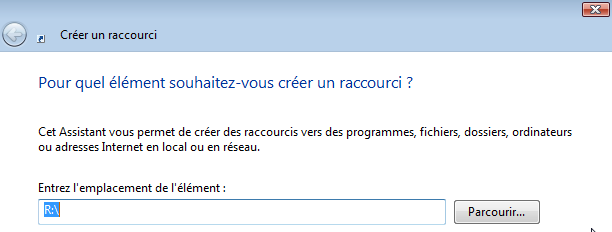
* Pour pouvoir créer un raccourci sur un répertoire partagé,

il suffit de lancer l'explorateur puis de visualiser la ressource à atteindre, un clic droit de la souris amène le menu contextuel:

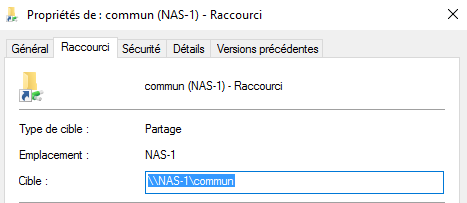


On demande **Créer un raccourci** Il suffit de placer ensuite le raccourci sur le bureau (voire le déplacer ailleurs…)

* Pour pouvoir créer un raccourci sur un lecteur réseau, on demande avec le clic droit de créer un raccourci, et on complète



on peut aussi indiquer un chemin réseau directement sous la forme **\\poste\partage**...on obtient alors

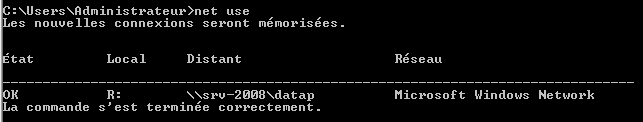
 

**N.B** : l'icône peut être différente, selon que vous ayez saisit le nom UNC, taper la lettre d'un lecteur réseau pré-existant, ou demandé parcourir le réseau…

**N.B** : lors d’une session ultérieure, si c’est un autre utilisateur qui se connecte sur le poste Windows, il ne verra rien des raccourcis crées par son collègue, car ses modifications sont stockées dans les profils

## Net use :

Il s'agit de lister les lecteurs réseau utilisés (montés) à un moment donné, on peut passer la commande suivante **net use (a**vec une aide en ligne disponible via **net use /?)**



Si on veut monter un lecteur réseau



Si on veut monter un lecteur réseau persistant (incorporé dans la session)



Si on veut supprimer un lecteur réseau



Si on veut monter un lecteur réseau en tant que un autre utilisateur que celui loggué en cours



Cela peut vite prendre des proportions…. Mauvaises, du genre, à éviter absolument, mieux faire un script de connexion.

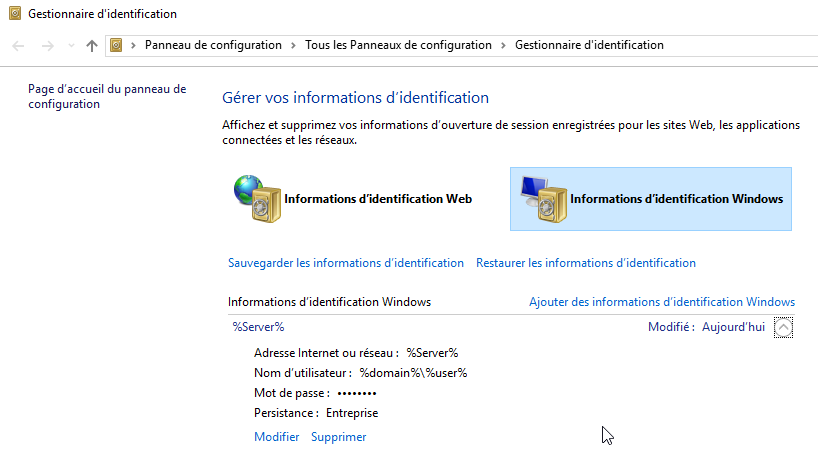
Avec la commande **cmdkey** Comme par exemple dans

**cmdkey /add:%Server% /User:%domain%\%user% /Pass:%PWD%**

**net use P: \\%Server%\share /SAVECRED /persistent:yes**

avec vérification possible via

**Executer** puis **control keymgr.dll**



**N.B** : pour l’**UAC** on peut utiliser l’utilitaire ***elevate***

**N.B** : pour les scripts, il faut désormais les passer par **GPO** ou **Préférence**

# Worksgroup & domaines

## Worksgroup Groupe de travail:

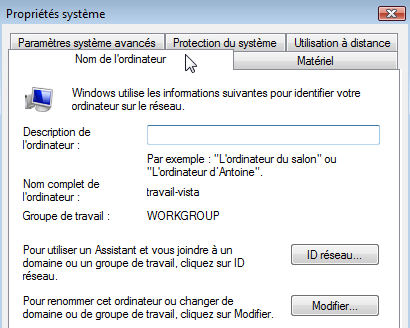
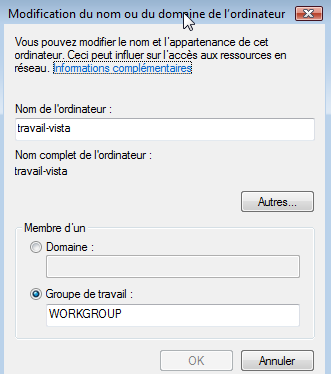
Cette notion est sensiblement la même depuis Windows Worksgroup 3.11 ou Windows 95-98 ! Un **groupe de travail**est un ensemble d'ordinateurs qui apparaît, pour des raisons pratiques, sous le même nom lorsque vous consultez les ressources réseau. Lorsque vous parcourez le réseau, les noms de tous les ordinateurs appartenant à votre groupe de travail s'affichent en premier dans le répertoire parcouru.

N'importe quel ordinateur peut devenir membre de n'importe quel groupe de travail unique.

## Appartenir à un Worksgroup avec 10 SEVEN:

Sous 10- SEVEN, la définition du groupe de travail se fait soit

*  en demandant dans **le panneau de configuration** l’icône **système** puis on demande **Paramètres système avancés** / onglet **Nom de l'ordinateur**
* en faisant un clic droit sur l’icône **ordinateur** du bureau, et demander **propriété** puis l’onglet **Nom de l'ordinateur**



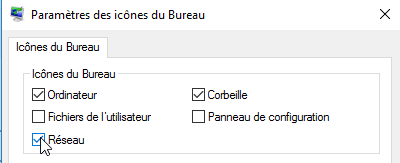
On peut changer le **Nom** du poste

(il faut redémarrer impérativement)

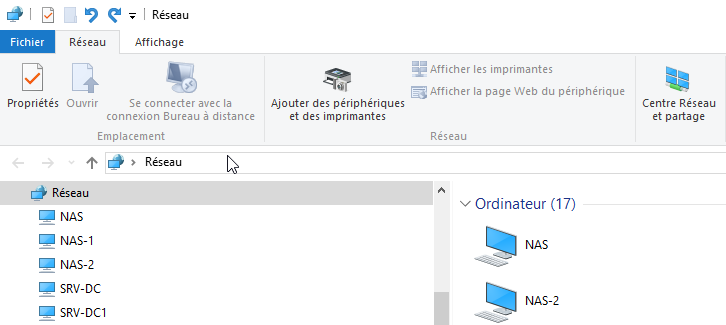
Et changer l’appartenance au un **Groupe de travail**.

## Réseau windows 10:

Sur un poste Windows 10 installé, si on demande d'afficher explicitement l'icône **Réseau**

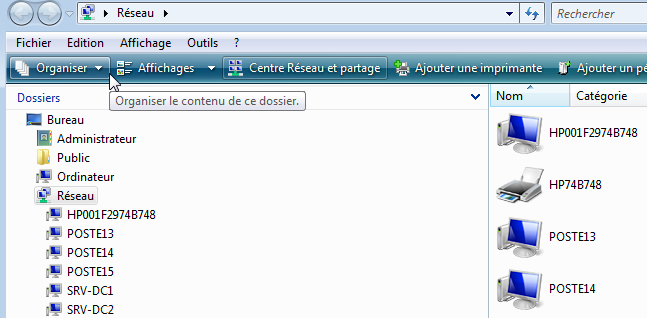


On obtient l'équivallent du placement sur réseau de l'explorateur de fichier



## Réseau Windows en Workgroup :

Si on est sur un poste Windows 10 SEVEN installé correctement, au niveau de l'icône **Réseau** on devrait voir



Dans la partie haute, une liste déroulante est disponible



Et on peut bien sur taper les noms UNC des postes que l'on souhaite atteindre…

## Domaine :

Cette notion existe depuis Windows NT 4

Un **domaine** est un ensemble "logique" d'ordinateurs défini par l'administrateur d'un réseau Windows NT Server.

Un domaine permet en outre d'accéder aux comptes d'utilisateur et comptes de groupes centralisés gérés par l'administrateur de domaine de manière centralisée.

Ses paramètres ne sont plus sont stockés au sein de fichiers, tels que la base de donnée **SAM** **Security Account Manager** contenant l'ensemble des données des comptes utilisateur, mais hébergé dans une base de donnée stockée sur le serveur **Contrôleur de Domaine** et répliqués le cas échéant sur un ou plusieurs autres contrôleurs, dit « **contrôleurs homologues** ». Un domaine est donc :

* l'unité de base de réplication et de sécurité d'un réseau Windows
* Un domaine partage une base de données d'annuaire centralisée nommée **Active Directory**

Contrairement à un groupe de travail, **un domaine doit déjà exister pour que vous puissiez en devenir membre**. Pour se joindre à un domaine au cours de l'installation, il est nécessaire d'avoir un **compte d'ordinateur** dans le domaine.

On peut imaginer que plusieurs domaines existent lors de la construction de grands réseaux, avec toute une gestion des relations entre eux, ce que l'on appelle les "approbations"

Pour des raisons de simplicité évidentes, nous nous limiterons à la gestion d'un seul domaine, définissant tous les comptes utilisateurs, tous les groupes et toutes les ressources

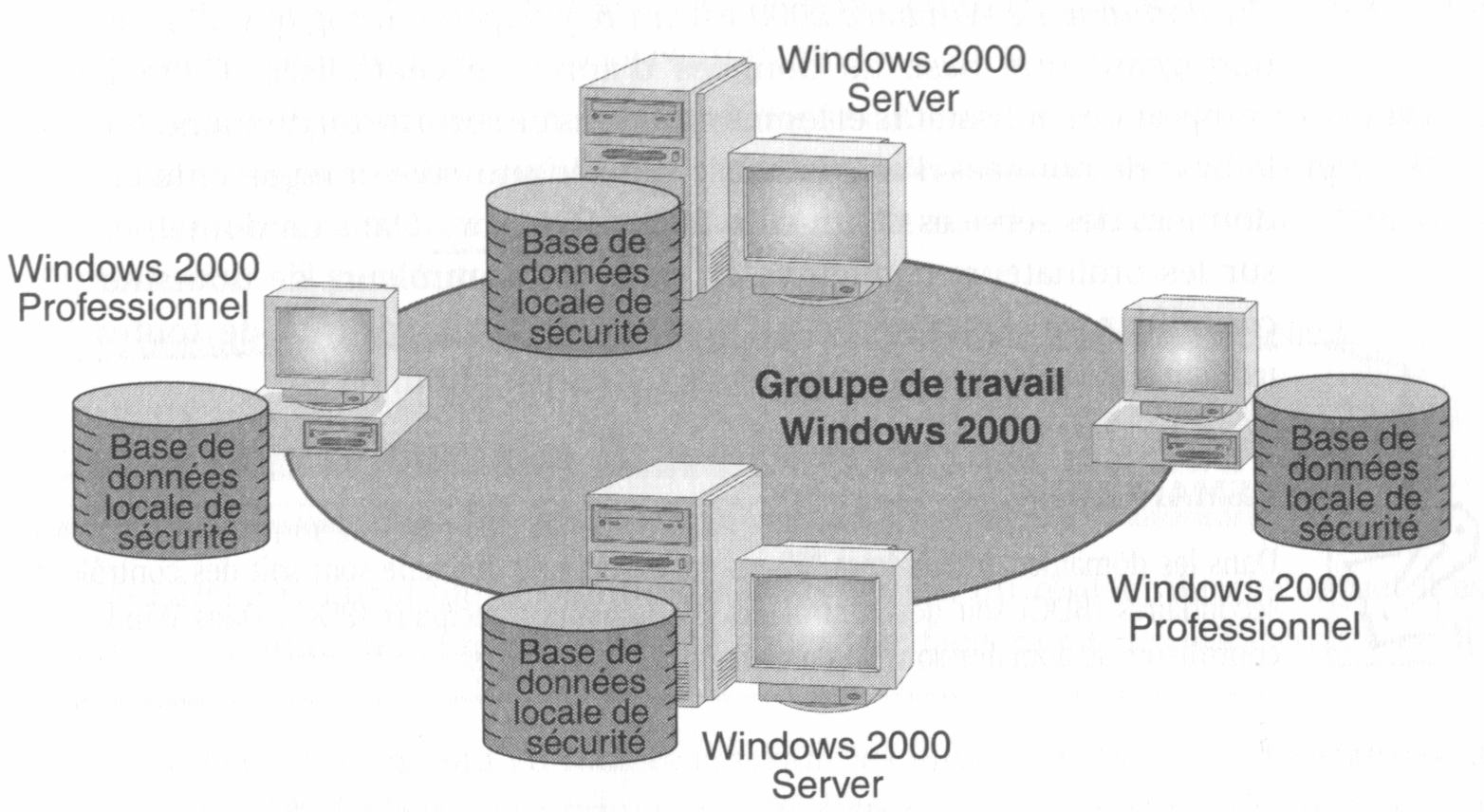
De même, un seul domaine ne veut pas forcément dire un seul contrôleur :

* Une organisation de petite taille qui utilise un réseau local unique peut nécessiter un seul domaine avec deux contrôleurs de domaine afin de garantir une disponibilité élevée et une tolérance de panne.
* Une organisation de grande taille avec plusieurs emplacements réseau nécessitera un ou plusieurs contrôleurs de domaine sur chaque emplacement afin de garantir une disponibilité élevée et une tolérance de panne.

Mais ici encore, pour des raisons de simplicité, nous nous contenterons d'une situation avec un seul serveur dans notre domaine

## Gestion de Domaine sous Windows Server:

Dans un réseau sans domaine, c'est à dire constitué uniquement en **Workgroups**



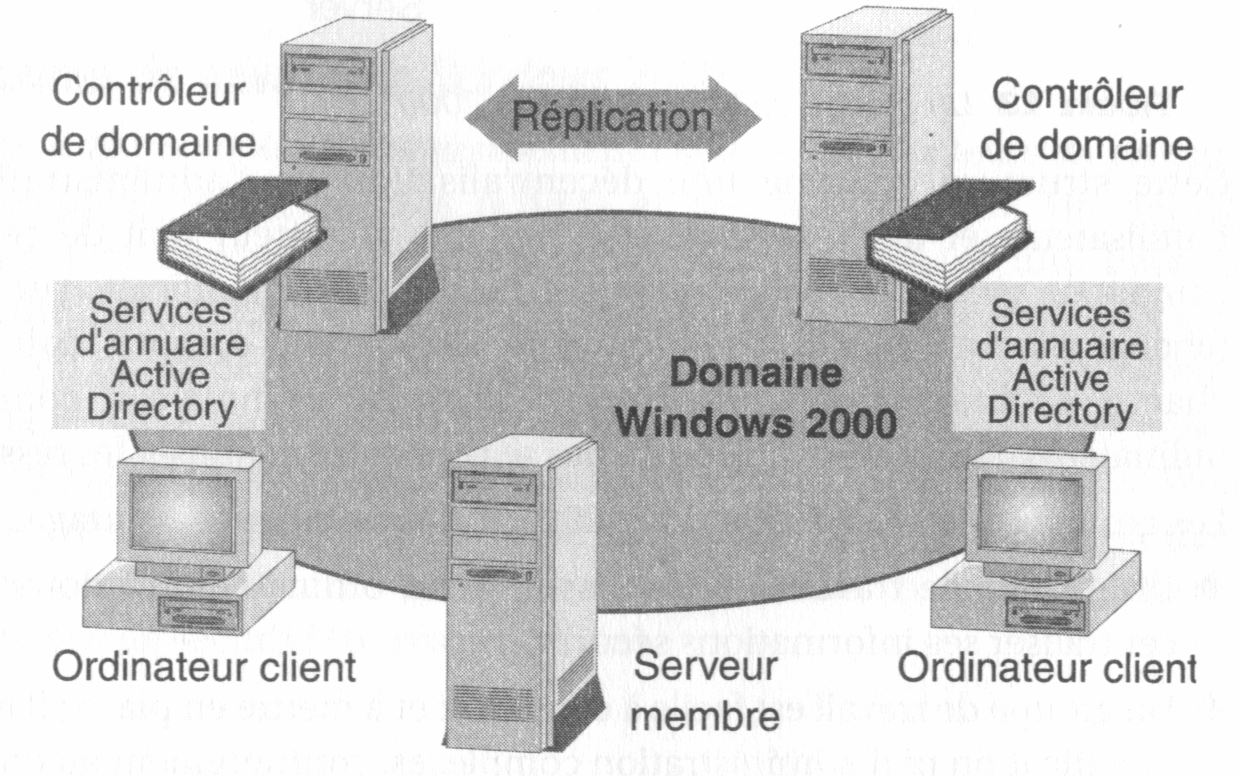
toutes versions

On peut trouver toute sorte de machine, (y compris des postes SEVEN, Windows XP, NT4.0 et windows95-98 non représentés)

**la sécurité est gérée localement sur chaque poste du réseau**

**N.B:** Dans le cas de machines Windows Server on parle alors de "**serveur autonome**"

Dans un réseau **avec domaine**, c'est à dire constitué avec un serveur 2016-2012 faisant office de contrôleur de domaine



2000-2003-2008-2012-2016-2019-2022…

On ne peut trouver que des machines "à partir" de NT4.0

**la sécurité est gérée sur le (les) contrôleurs du réseau uniquement**

**N.B:** A partir d'un Domaine 2012-2022 tous les "**contrôleurs de domaine**" de Active Directory sont **homologues**

Depuis Windows 2018, un **serveur** peut avoir l'un des trois rôles suivants vis-à-vis du domaine :

* **Les contrôleurs de domaine** contiennent les copies des comptes d'utilisateurs et d'autres données Active Directory pour un domaine donné :   
  N.B : **Il en faut au moins 1 pour parler de Domaine, il peut y en avoir plusieurs, ils sont alors tous homologues**
* Les **serveurs membres** appartiennent à un domaine, mais ne contiennent pas de copie des données Active Directory.
* Les **serveurs autonomes** appartiennent à un groupe de travail plutôt qu'à un domaine.

Il est conseillé de planifier le rôle de chacun de vos serveurs dans les domaines Windows avant d'exécuter le programme d'installation. Mais toutefois, vous pouvez modifier ces rôles après l'installation.

Avec Windows 10- SEVEN, un **client** peut avoir l'un des deux rôles suivants vis-à-vis du domaine :

* Poste appartenant à un domaine.
* Poste appartenant à un groupe de travail plutôt qu’à un domaine.

# Active directory

## Qu'est-ce un service d'annuaire ?:

Un service d'annuaire peut être comparé à un agenda téléphonique, celui-ci contient au départ des noms et des n° de téléphone, puis au fur et à mesure il peut s'enrichir d'autres éléments, comme des adresses postales ou Email...

On va définir un service d'annuaire tel que celui existant sous 2000-2016 et portant le nom d'**Active Directory** par ses fonctions :

* Un annuaire offre le moyen de **stocker des informations** sur les ressources du réseau afin de simplifier la recherche de ces informations. C’est un peu comme une base de registre globale à tout le réseau.
* Un annuaire offre le moyen de **gérer ces ressources** par l'intégration de tous les services nécessaires
* Un service d'annuaire agit comme un tableau de bords principal du système d'exploitation réseau, **il est distribué ou répliqué sur tous les ordinateurs** qui participent à la gestion du domaine de manière à en augmenter la fiabilité. Active directory n'utilise d'ailleurs que des contrôleurs de domaine homologues, les modifications effectuées par un administrateur sur un contrôleur sont immédiatement répercutées sur tous les autres contrôleurs
* Un annuaire étant amené à collecter/gérer des informations sur des machines différentes doit répondre à certaines normes. Les service **Actives Directory** utilisent le protocole **LDAP** (Lightweight Directory Acces protocol) normalisé . Active Directory localise les ressources grâce au protocole **DNS** (Domain Name System) et donc nécessite TCP/IP impérativement
* Active Directory est extensible, car on ne peut pas forcément tout prévoir dès le début !

Active Directory gère ses ressources de manière interne par un protocole particulier **X500** mais un peu "modifié" par Microsoft.

Ce qui fait que si AD est capable de trouver des ressources sur **tout système à la norme LDAP**, et si AD est interrogeable par tout **client LDAP**, on ne pourra **pas répliquer la structure AD de windows 2022-2019-2012-2008 sur un autre système que Windows 2022-2019-2016-2012-2008**.

## La structure Logique d’Active Directory dans un Domaine:

### Domaine

Un **Domaine** est défini par une **limite de sécurité** unique dans le cadre d'un réseau informatique tournant sous Windows.

Sur un poste de travail isolé, le domaine est l'ordinateur lui-même.

Un domaine constitue une **Unité de duplication**, dans le cas ou plusieurs contrôleurs de domaines sont présents. Dans ce cas, chaque contrôleur de domaine contient un réplica de l'annuaire Active Directory.

Dans un Domaine, tous les éléments qui en font partie ont une appellation commune, basée sur le **nom de Domaine**.

### Annuaire & Espace de noms

Active Directory est essentiellement un espace de noms, comme c'est le cas de tout service d'annuaire. La **résolution de nom** consiste à passer d'un nom à l'objet ou l'information que ce nom représente. Un annuaire téléphonique constitue un espace de noms dans lequel les noms des abonnés peuvent être résolus en numéros de téléphone.

Active Directory constitue un **espace de noms** dans lequel le nom d'un objet de l'annuaire peut être résolu pour obtenir l'objet lui-même.

### Active Directory & DNS

Puisqu'un annuaire c'est un espace de nom, Active Directory nécessite un serveur DNS par Domaine. Dans le cas ou on souhaite créer deux Domaines indépendant, il suffit d'avoir à disposition pour chaque domaine d'un serveur DNS gérant cet espace de nom...

**Domaine formation.edu**

**1CD+1DNS+1AD**

**Domaine commerce.com**

**1CD+1DNS+1AD**

**N.B**: Il ne faut pas confondre le problème de plusieurs domaines, avec la problématique de plusieurs Contrôleurs pour le même Domaine...

### Contrôleur de schéma

Puisque Active directory est un annuaire, la structure de la base de donnée contenant cet annuaire doit être physiquement gérée en un endroit, portant le nom de **contrôleur de schéma**. Ce contrôleur est le seul à pouvoir modifier la structure de la base de AD, Il en faut un, toujours un mais rien qu'un (jamais deux...)

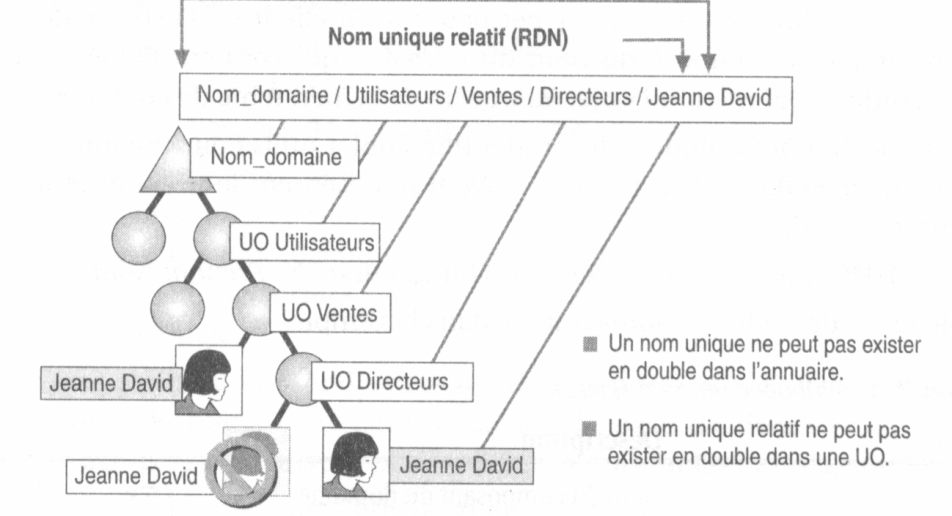
### Nom

Chaque objet dans Active Directory est identifié par un nom correspondant à un chemin LDAP. Il y a deux sortes de noms différents.

**Nom unique** (**DN – Distinguished Name**). Le nom unique identifie le domaine qui contient l'objet, ainsi que le chemin d'accès complet permettant d'accéder à l'objet à travers la hiérarchie des conteneurs. Voici un exemple typique de nom unique :

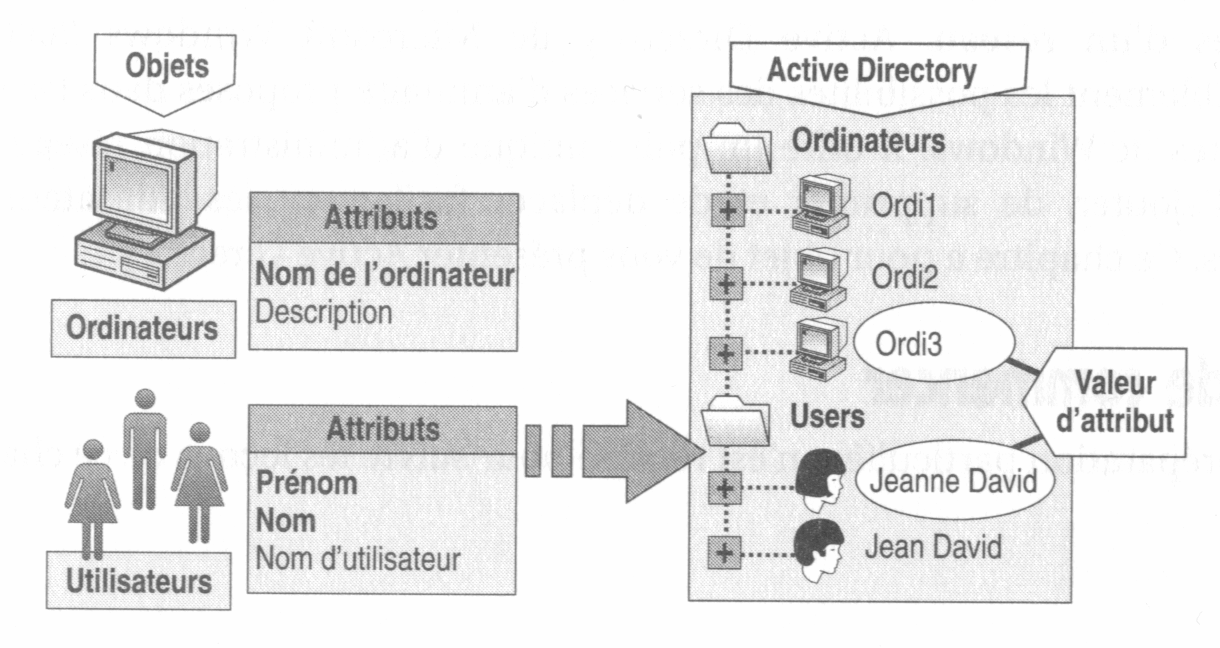
**DC**=Nom\_Domaine//**OU**=Utilisateurs /**OU**=Ventes/**CN**=Jeanne David

**Le nom relatif distinct** (**RDN – Relative Distinguished Name**) d'un objet est la partie du nom qui constitue un attribut de l'objet à proprement parler. Dans l'exemple précédent, le nom relatif distinct de l'objet utilisateur est **CN**=Jeanne David. Le nom relatif distinct de l'objet parent est **OU**=Ventes.



### Objet

Les **Objets** dans Active Directory peuvent être les données utilisateurs, les imprimantes, les serveurs, les bases de donnée, les groupes, les ordinateurs, les stratégies de sécurité. Un **Objet** est donc un ensemble d'attributs nommé et circonscrit qui représente un élément concret



Par rapport à la liste prévue initialement, il est possible de rajouter des objets supplémentaires. Certaines applications procèdent de cette manière lorsqu'elles s'installent…

### Conteneur UO

certains objets, contenant d’autres objets, sont appelés **Conteneurs** ou **UO Unité Organisationelle** dans le langage Active Directory . Un conteneur est semblable à un objet dans la mesure où il possède des attributs et fait partie de l'espace de noms de Active Directory. Toutefois, contrairement à un objet, il ne représente rien de concret. Ce n'est qu'un réceptacle pour un ensemble d'objets et/ou pour d'autres conteneurs.

On pourra définir qui en est le responsable en octroyant des permissions supplémentaires par rapport à celles définies par défaut, c'et ce que l'on appelle de la **délégation de permission**

Une **OU** est une unité d'administration sur laquelle on notamment pourra appliquer des **stratégies de groupe**

## La Structure Logique au sein de plusieurs Domaines:

### Arbres-arborescence de domaines

Un **domaine** seul, crée un **Arbre de domaine** (cet arbre est petit, sans branches, on peut dire que l'on a que la racine de l'arbre… mais …c'est un arbre quand même).

Autrement dit un domaine fait toujours partie d'un arbre, et si c'est le premier domaine que l'on crée, il sera défini comme le **domaine racine de la forêt**.

**Domaine racine formation.edu**

**1CD+1DNS+1AD**

Arbre a 1 domaine

Un arbre, ou arborescence de domaine, c'est un ensemble de domaine hierarchisés.

Si on ajoute un domaine à un arbre, le nouveau domaine est un **domaine enfant**, il a une relation d'approbation transitive bidirectionelle avec son parent. Son nom est hiérarchiquement lié au nom du domaine parent **enfant.parent.com** (le tronc se voit doté d'une branche…)

Arbre a 3 domaines

**Domaine racine parent formation.edu**

**1CD+1DNS+1AD**

**Domaine racine enfant informatique.formation.edu**

**1CD+1DNS+1AD**

**Domaine racine enfant langue.formation.edu**

**1CD+1DNS+1AD**

Une arborescence constitue un **espace de noms** hiérarchisé et continu. Les serveurs DNS du (des) domaines enfants reprends le nom du serveur DNS de plus haut niveau (du parent)

Les relations d'approbation sont bidirectionelles et transitives. Dans un **arbre de domaine** ils partagent un même **schéma**, et un même **catalogue global**.

### Forêts

Un **arbre** ne peut exister sans forêt, même s'il est seul. Donc un **arbre de domaine** seul crée une **forêt** ( même s'il y a un seule arborescence …)

Forêt d'1 Arbre a 1 domaine

**Domaine racine formation.edu**

**1CD+1DNS+1AD**

Forêt d'1 Arbre a 3 domaines

**Domaine racine parent formation.edu**

**1CD+1DNS+1AD**

**Domaine racine enfant langue.formation.edu**

**1CD+1DNS+1AD**

**Domaine racine enfant informatique.formation.edu**

**1CD+1DNS+1AD**

Forêt de 2 Arbres respectivement a 3 et 1 domaine

**Domaine racine parent formation.edu**

**1CD+1DNS+1AD**

**Domaine racine parent commerce.com**

**1CD+1DNS+1AD**

**Domaine racine enfant informatique.formation.edu**

**1CD+1DNS+1AD**

**Domaine racine enfant langue.formation.edu**

**1CD+1DNS+1AD**

Une forêt permet d'établir des communications entre les arbres. Une forêt ne constitue pas un **espace de noms** hiérarchisé et continu. Les serveurs DNS des arbres de la forêt sont indépendants

Les relations d'approbation sont bidirectionnelles et transitives Lorsque plusieurs arbres de domaines sont interconnectés pour former une forêt. les **arbres de domaine** de la forêt partagent un même **schéma**, et un même **catalogue global de AD**.

### Catalogue Global

Le **catalogue global** c'est une liste de définition de tous les noms existant dans l'annuaire d'un domaine, afin d'éviter l'attribution d'un nom en "doublons". Le **Catalogue Global** permet de trouver tout objet dans Active Directory, et ce au travers du domaine, de l'arbre ou de la forêt… selon l'importance. Sans **Catalogue Global** une recherche s’effectuerait sur chaque domaine de la forêt

Le premier serveur devenant Contrôleur de Domaine devient serveur de catalogue global. Ce catalogue global peut être répliqué sur tous les contrôleurs de Domaine…. En théorie toutes les modifications sont possibles à n'importe quel moment depuis tout CD, le "dernier qui cause à raison". Dans la pratique, cette théorie du dernier qui cause est gérée par un n° **USN** (**update Sequence Number**) qui est incrémenté automatiquement par le CD au moment de la modification. Le n° le plus élevé remporte….

### Relations d'approbation

Elles peuvent être **uni-directionelles**, c'est à dire que ce n'est pas parce que un domaine approuve un autre domaine, que la réciproque est vrai. (Si A approuve B, alors B n'approuve pas A)

Elles peuvent être **bi-directionelles** , c'est à dire que 2 chemins d'approbation vont dans les 2 direction entre 2 domaines (Si A approuve B, alors B approuve A)

Elles peuvent être **transitives** , c'est à dire que 2 chemins d'approbations permettent d'en définir un troisième (Si A approuve B, et B approuve C alors A approuve C…)

## La structure Physique d’Active Directory:

### Sites

Un **site** est un emplacement d'un réseau qui contient des serveurs Active Directory. Un site est défini comme un ou plusieurs sous-réseaux TCP/IP "bien connectés". (la connectivité du réseau doit être fiable et rapide vitesses de réseau local égales ou supérieures à 10 millions de bits par seconde).

Définir des sites permet de configurer l'accès à Active Directory et la manière dont la réplication va se faire entre les contrôleurs de domaine.

Un site contient au minimum un contrôleur de Domaine.

Lorsqu'un utilisateur ouvre une session, le client Active Directory recherche les serveurs Active Directory qui font **partie du même site que l'utilisateur**. La détermination du site local à l'ouverture de session se fait facilement parce que le poste de travail de l'utilisateur sait déjà à quel sous-réseau TCP/IP il appartient et que les adresses de sous-réseaux se traduisent directement en adresses de sites Active Directory.

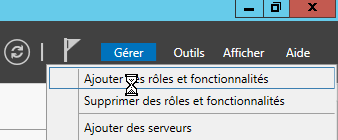
**N.B:** il est conseillé de penser son réseau en Domaine, et de gérer ensuite les problèmes de géographie physique par la notion de site, que de faire autant de domaines que de sites géographiques.   
Lorsque l'on fait plusieurs domaines, c'est plutôt que les modèles d'administration et de sécurité diffèrent entre les domaines…

# Création Active Directory

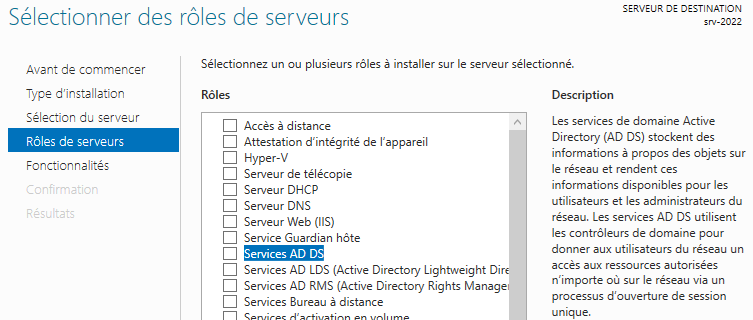
## Rôles et Création de Domaine :

Pour créer un domaine, il faut **promouvoir** au moins un ordinateurs exécutant **Windows Server** afin qu'ils devienne un (ou des) contrôleurs de domaine. Si les **services AD** sont effectivement nécessaires sur un **CD**, ils ne permettent pas la création d'un domaine à proprement parler (ils sont par exemples nécessaires pour réaliser un CD en lecture seule...)

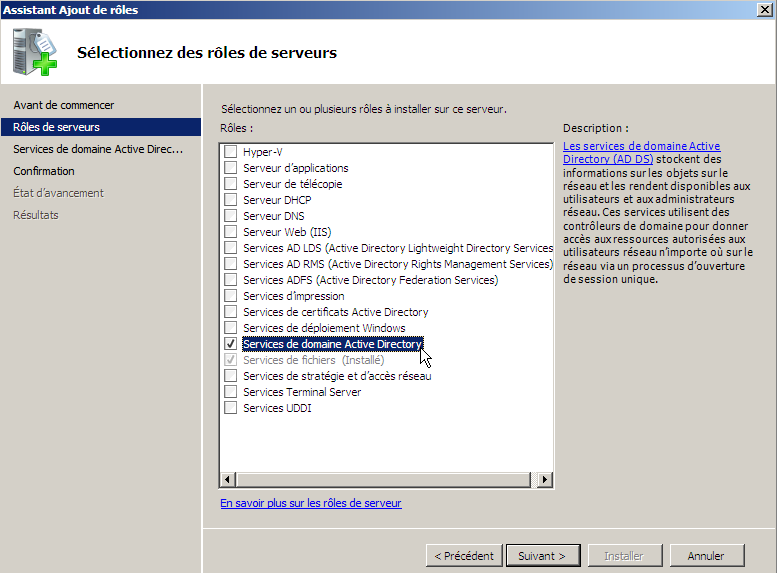
Cette création ne pourra se faire que via la console **gestionnaire de serveur.** On demande **Gérer / Ajouter des Rôles et fonctionnalités**

 Les 2 rôles voulus sont

* celui de **AD DS** c'est à dire (**Service de Domaine Active Directory**)
* et celui de **Serveur DNS**…



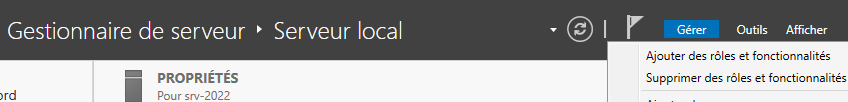
Ou anciennement

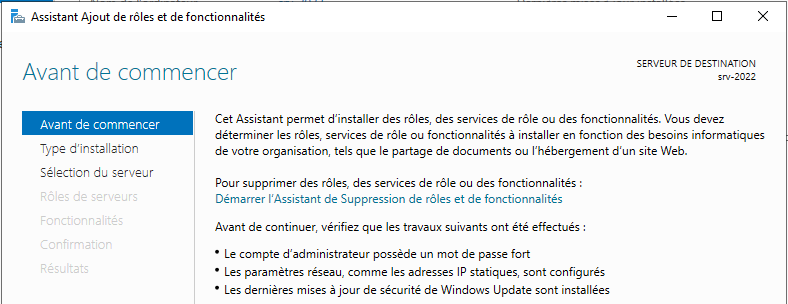


**N.B**: mais nous on veut créer le domaine… et pas juste ajouter les rôles !

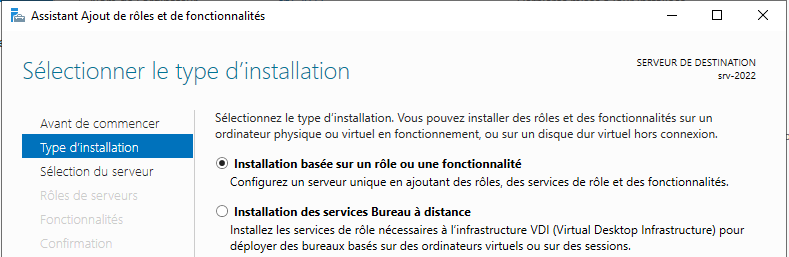
## Assistant Rôle AD DS Création de Domaine :

Via le **gestionnaire de Serveur** on demande d'ajouter un **rôle**

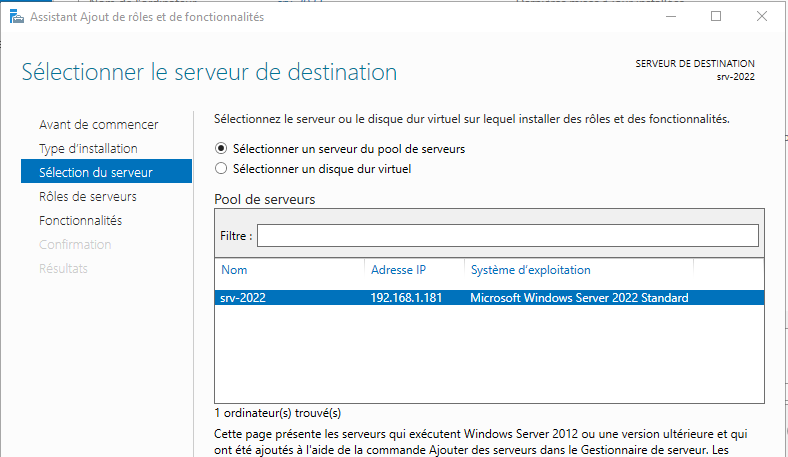




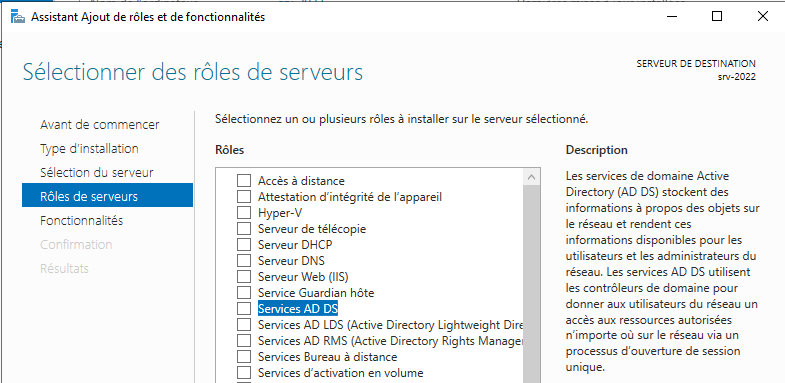
On veut **un rôle**

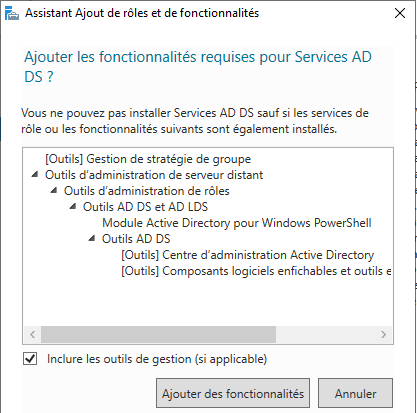


Pour notre serveur qui a le **bon nom** et une **adresse IP correcte**



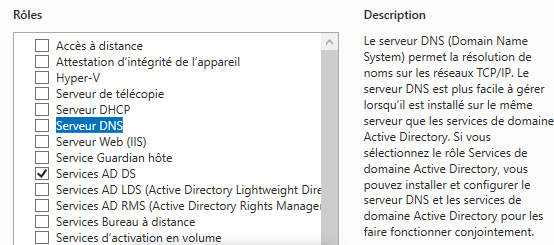
On veut les **services AD-DS** et les fonctions inclusent

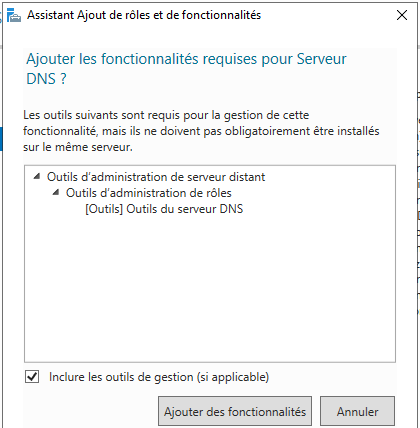




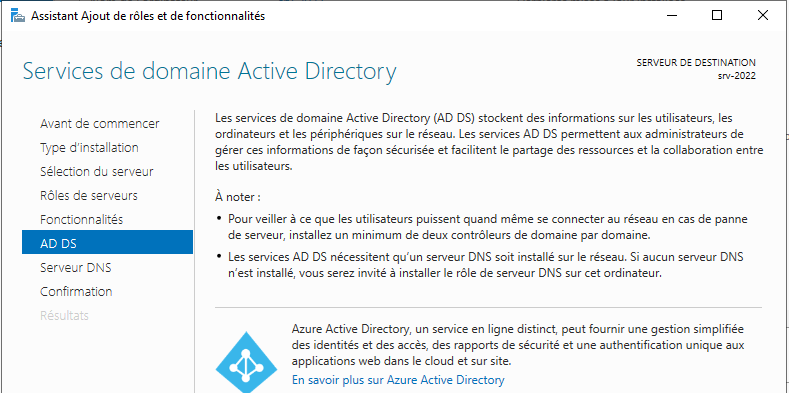
et **les fonctions incluses**

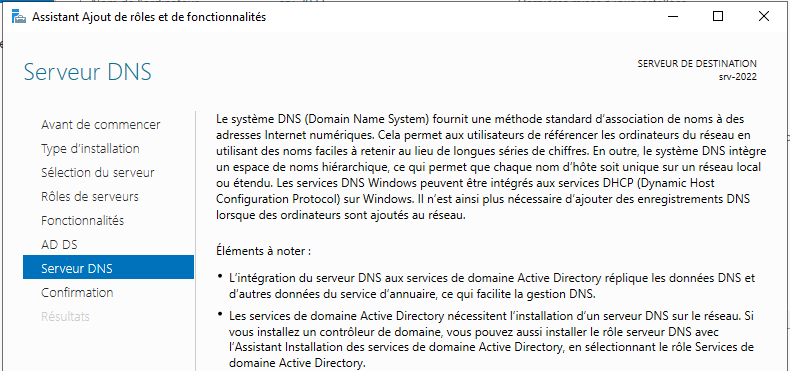
Et on veut le **service DNS** et les fonctions inclusent



et **les fonctions incluses**

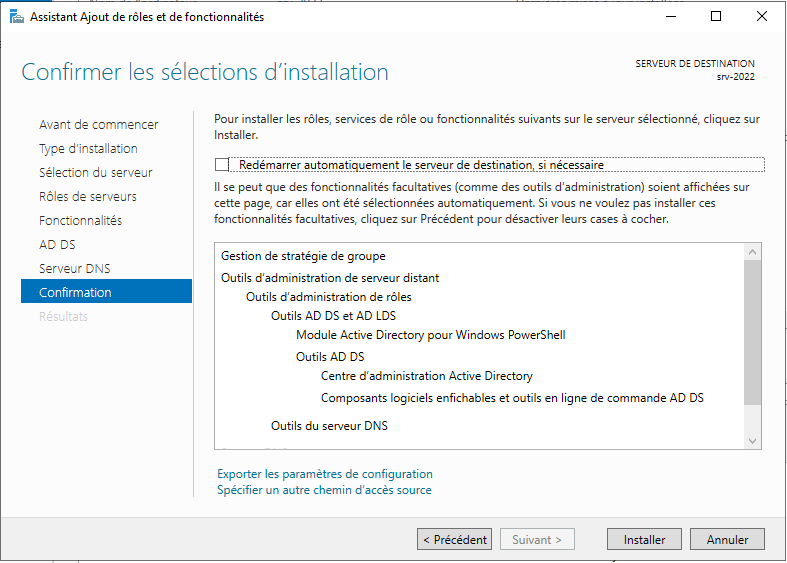
On ne veut pas d’autres rôles (**rien d'autres que AD DS et DNS**…) ni aucunes autres fonctionnalités que celles installée automatiquement par les 2 rôles précédents





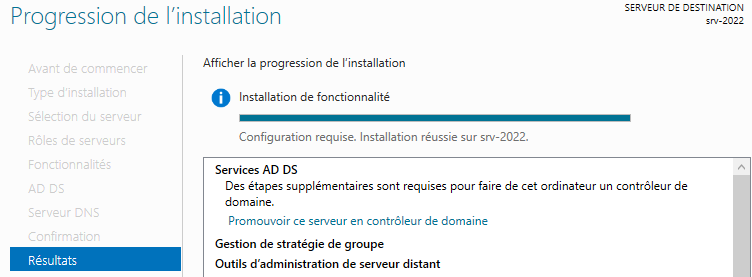
**N.B**: si on oublis le **DNS** (…) Le **service DNS** sera automatiquement proposé…

Et on demande **Installer**

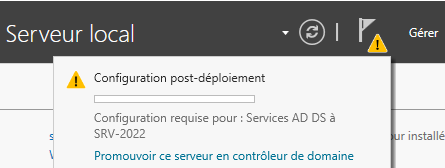


## Promouvoir ce serveur (ex Dcpromo)en Contrôleur de Domaine :

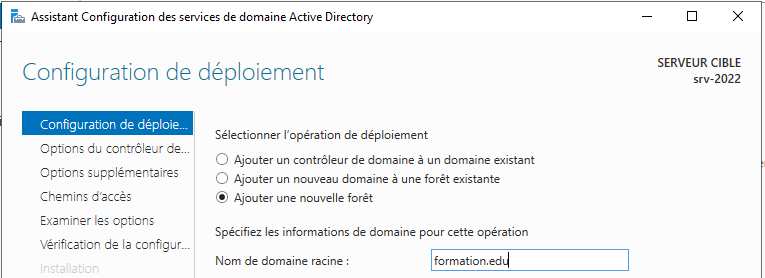
Une fois le rôle ajouté, il faut soit dans la boite de dialogue **Promouvoir ce serveur en Contrôlleur de domaine**



soit dans le **Gestionnaire de serveur** que ce serveur prenne le rôle de **DC**… (ex **DCpromo**)



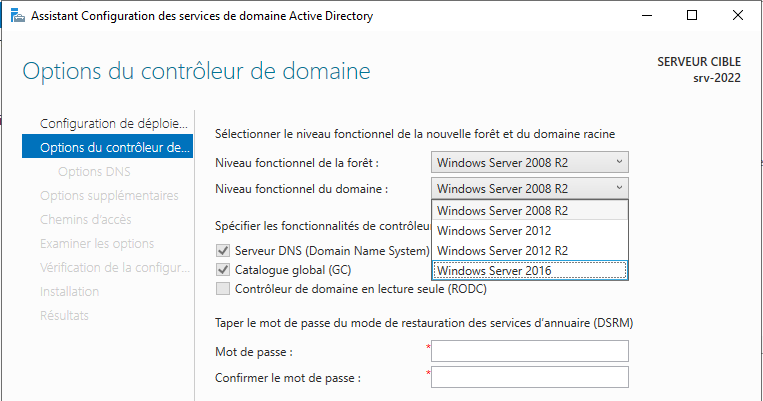
Le premier choix ici est capital ! On veut créer un nouveau « **Domaine dans une nouvelle forêt** », donc on **crée une forêt**, et on indique le **nom de domaine**



Un nom **Netbios** sera généré (15 premier caractères dans l’étendue des caractères autorisés par **netbios**).

Puis il faut choisir un **niveau fonctionnel de Forêt et de Domaine**…

[**https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels**](https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/active-directory-functional-levels)



6 niveaux de fait existent au niveau **forêt**

* 2016 pam utilisant mim
* 2012 / 2012R2 ras
* **2008R2** corbeille Active Directory powerschell
* 2008 / 2008R2 (permet d’avoir des domaines 2008 et 2012)

6 niveaux existent au niveau **domaine**

* 2016
* 2012 / 2012R2 (même fonctionnalités sans serveur 2008 – 2008r2)
* 2008 / **2008R2** DFS x Sysvol. (permet d’avoir des serveurs 2008 et 2008R2)
* 2003 FRS réplication à supprimer

**N.B**: on peut toujours augmenter d'un niveau, on ne peut jamais redescendre

**N.B**: on ne peut avoir un **niveau fonctionnel de Domaine** plus bas que le **niveau fonctionnel de fôret**

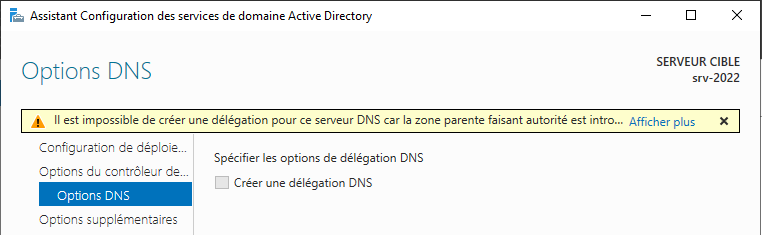
La question du **DNS** refait surface. Si on avait renseigné un adresse IP comme serveur **DNS**, alors la case à cocher **Serveur DNS** est optionnelle... (si on n'a pas d'adresse **IP** de renseignée comme **DNS**, on doit installer un **DNS**)

On peut prévoir ensuite un mot de passe ici différent de celui d’administration courant. En effet lors d’une restauration des services d’annuaire, Un **Serveur Windows** démarre sans charger **Active Directory**, et donc le mot de passe doit être stocké « en dehors » de **AD**.

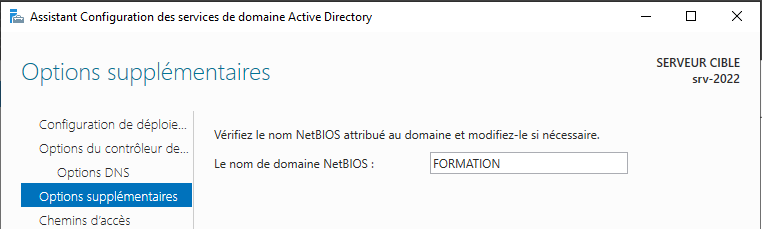
**N.B** : depuis 2008 il existe un utilitaire **NTDSUTIL.exe** permettant de modifier ce mot de passe par une commande genre **Set DSRM Password** puis **reset password on server null   
 (**ou **reset password on server nomhotedistant)   
**

**N.B**: cet utilitaire n'est présent que sur les **Contrôleurs de Domaine**

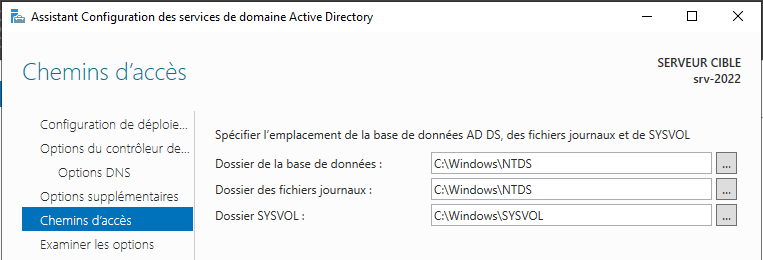
Une mise en garde apparaît, on répond de continuer…



Le nom **netbios** est vérifié… **N.B:** Il est déconseillé de donner un nom **netbios** différent de celui construit par défaut à partir du nom de Domaine.



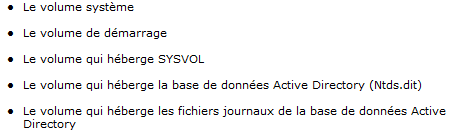
ensuite on demande l'emplacement des fichiers système



Active directory et fichiers miroirs de l’Active Directory  destinés à la lecture et réplication (on doit les mettre sur un volume NTFS)

On peut garder les valeurs par défaut

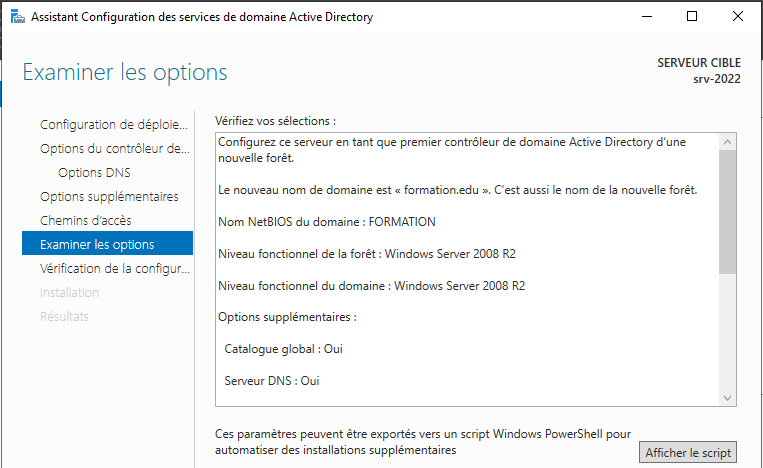
Si on veut affiner, il faut savoir que 5 "composants" existent

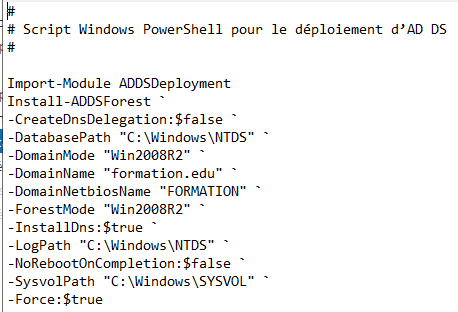


et si plusieurs volumes (partitions) sont disponibles : mettre sur le 1° disque les 3 premiers volumes (système-démarrage-sysvol), et sur le 2° disque les 2 derniers volumes (base AD et les fichiers journaux AD)

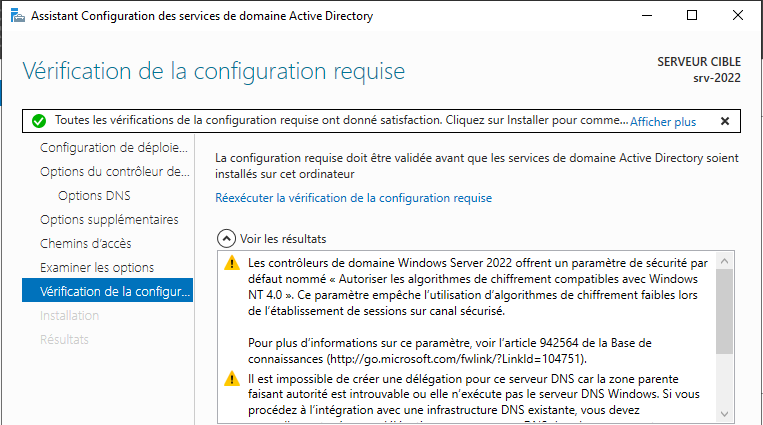
**N.B:** Si on veut prévoir une sauvegarde stockée localement, il faut un volume distinct pour son stockage

Après l’affichage d’un bref résumé

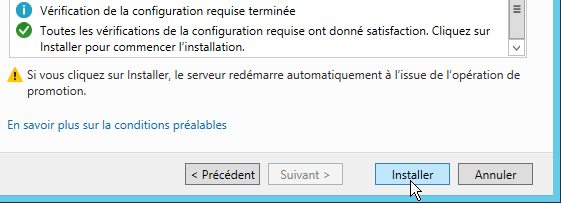




Une vérification est effectuée



Et si on est d’accord, on demande l’installation



Un redémarrage du serveur sera nécessaire.

# Gestionnaire de Serveur

## Lancer la mmc Gestionnaire de Serveur:

Depuis la barre des tâches 

ou depuis icone **Gestionnaire de Serveur** de l’écran d’accueil

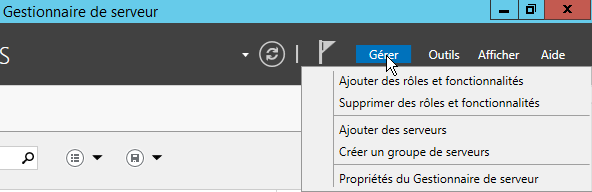


on accède à



en cliquant coté gauche, sur le noeuds, on obtient le détail, coté droit...

## Rôles services et fonctionnalités



Un **rôle de serveur** est un ensemble de programmes logiciels qui, une fois installés et correctement configurés, permettent à un ordinateur de remplir une fonction spécifique

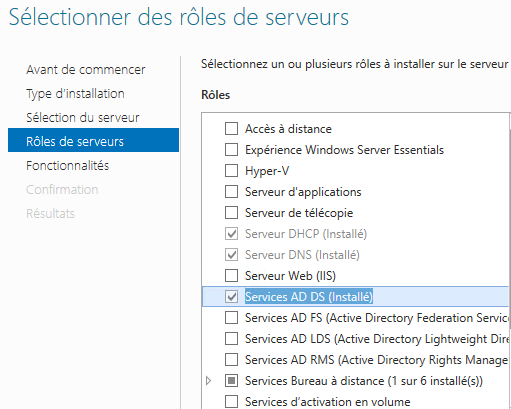
Une fois correctement installés et configurés, les rôles ont été conçus de manière à fonctionner automatiquement

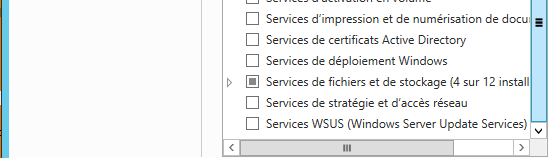
Les **services de rôle** sont des programmes logiciels qui fournissent la fonctionnalité d’un rôle.

Certains rôles, tels que Serveur DNS, possèdent une seule fonction et ne disposent donc pas de services de rôle disponibles, mais en général Vous pouvez considérer un rôle en tant qu’un groupement de services de rôle étroitement associés et complémentaires

Les **fonctionnalités** sont des programmes logiciels qui, bien qu’elles ne fassent pas directement partie des rôles, peuvent prendre en charge ou augmenter la fonctionnalité d’un ou de plusieurs rôles, ou encore améliorer la fonctionnalité de la totalité du serveur, quels que soient les rôles installés

A l'origine (2012) 17 rôles existaient, mais depuis certains développements sont apparus (comme Wsus , activation en Volume...)





en **Core Mode** seuls 9 **rôles** sont possibles

* Hyper-V
* Serveur DHCP
* Serveur DNS
* Serveur WEB (sans ASP)
* Services AD LDS
* Services d'impression
* Services de domaine Active Directory
* Services de fichier

# Présence du DNS

## Lancer la mmc DNS:

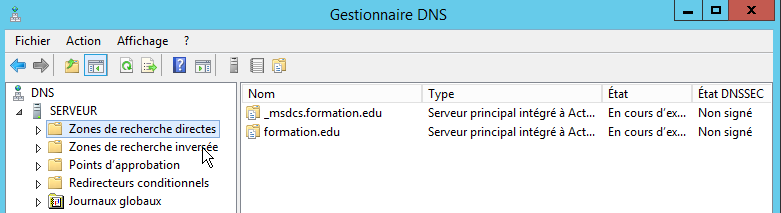
On peut accéder au DNS soit par le biais du **Gestionnaire de serveur**

via **Outils / DNS**

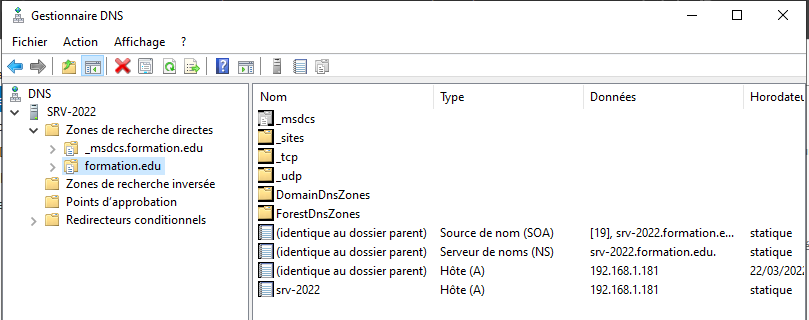


Soit depuis les outils d’administration

**Panneau de configuration / outils d’Administration / DNS**



## Vérifier la présence de AD et du serveur:



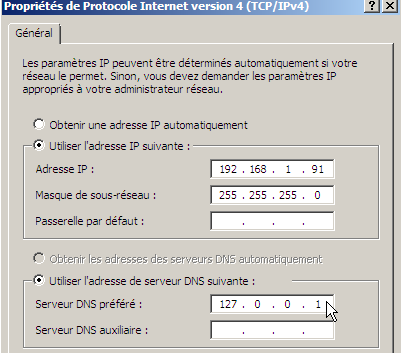
La présence de

* Un structure d’enregistrements de type **SRV**
* L’enregistrement de notre serveur

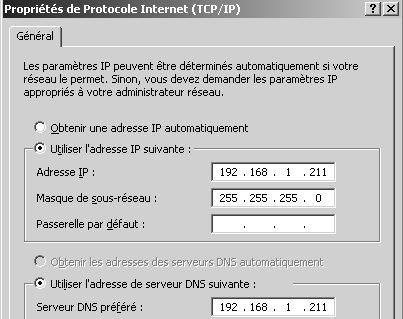
Devrait suffire pour l’instant pour valider notre serveur **DNS**

## Vérification paramètre IP serveur :

Selon les versions, cette opération peut êst effectuée automatiquement avec comme adresse de serveur DNS **127.0.0.1 (lui-même)**



il peut donc être nécessaire de modifier le paramétrage **IP** en indiquant qu’il est son propre serveur **DNS (indépendamment de la valeur)**



# Présence de AD

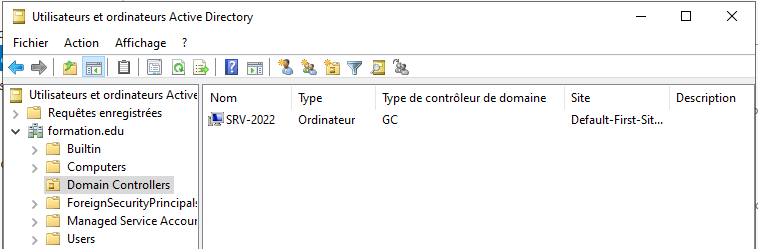
## Lancer la mmc AD:

On peut accéder à la gestion de AD soit par le biais du **Gestionnaire de serveur** via **Outils / Utilisateurs et Ordinateurs Active directory**



Soit on visualise **Active Directory** par les outils d’administration

**Panneau de configuration / outils d’Administration / Utilisateurs et Ordinateurs Active Directory**

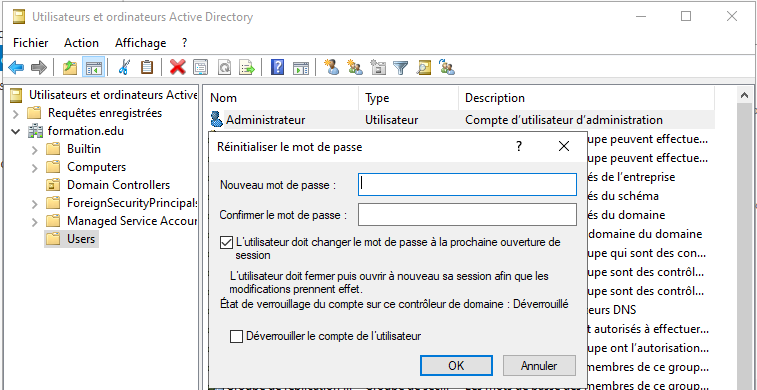


Les éléments suivant confirment la création de notre domaine :

* de notre Serveur (ici SERVEUR) dans l’Unité Organisationnelle **UO** **Domain Controllers**
* du nom de Domaine dans l’arborescence
* Du compte Administrateur dans l’Unité Organisationnelle **Users**

## Modification du mot de passe compte Administrateur:

Dans l’UO **Users**, on a le compte **Administrateur**, il faut lui changer son mot de passe, c’est un compte **Administrateur de Domaine**…



**N.B**: Attention aux stratégies de domaine par défaut…

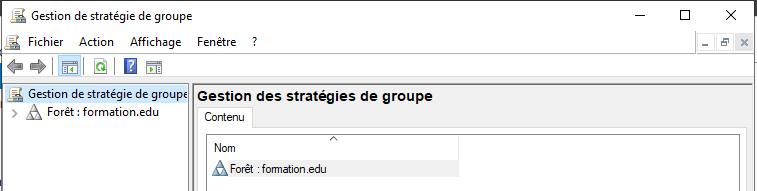
# Stratégies de Domaine

## Stratégie Mot de Passe sur Domaine:

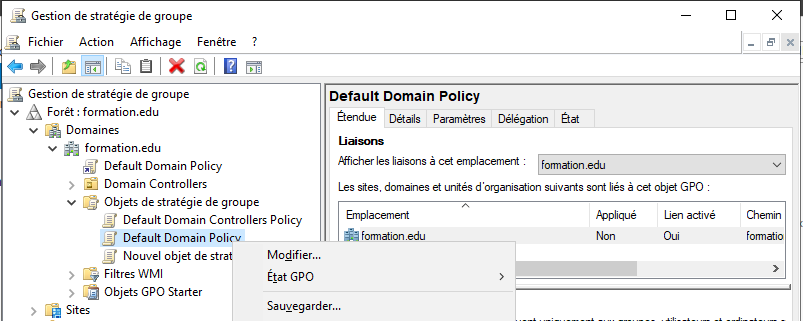
On peut accéder à la gestion des stratégies soit par le biais du **Gestionnaire de serveur** via **Outils / Gestion des stratégies de groupe**



soit depuis le **panneau de configuration**, **outils d'administration**, **Gestion de stratégie de groupe**

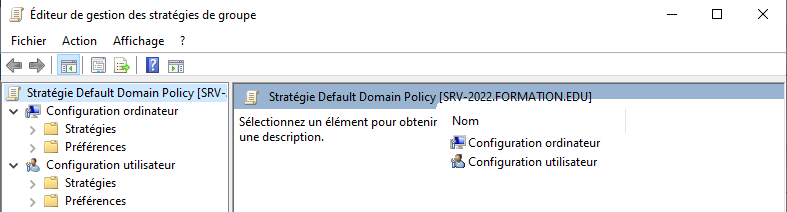


il faut se placer dans les **objets de stratégie de groupe**, sur **default domain policy**

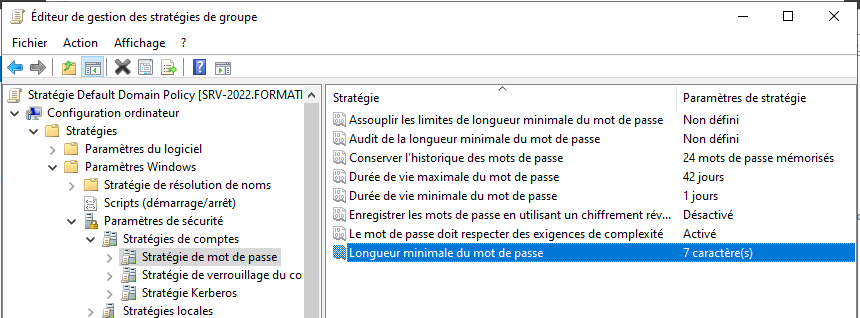


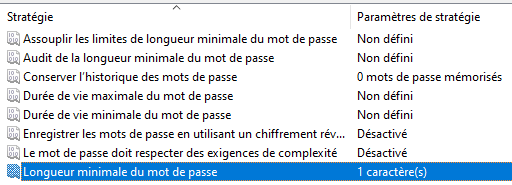
puis on demande clic droit / **modifier**

alors l'éditeur de stratégies apparait

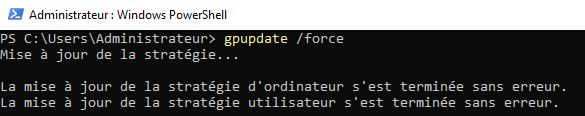


dans lequel on va chercher

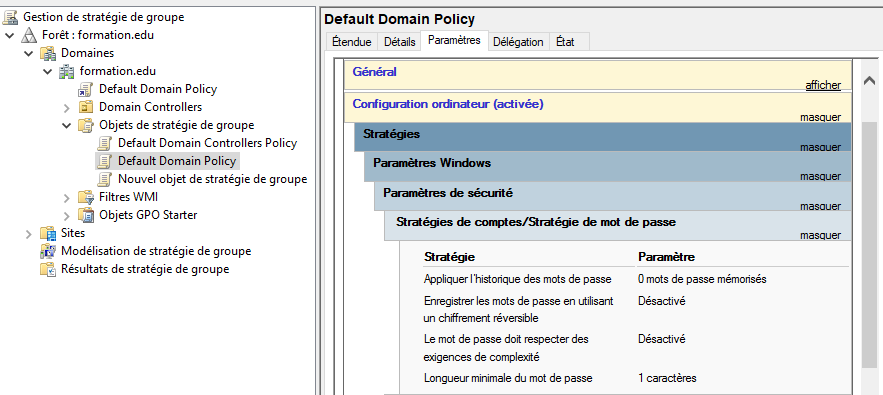
et on indique



après éventuelle propagation via **gpupdate/force**



on peut vérifier



# Adhesion à un DOmaine

## Appartenir à un Domaine depuis un client 10-SEVEN :

Pour qu’un client Windows 10-SEVEN puisse faire partie d’un Domaine, il faut plusieurs conditions, réalisées (certaines peuvent se faire de manière plus ou moins automatique

Mais détaillons de plus près:

1. Serveur : Dans A.D. un compte ordinateur ayant le même nom que le nom d'hôte du poste doit exister
2. Serveur : Dans la zone DNS de votre domaine, un enregistrement hôte correspondant a votre poste avec son adresse IP doit être saisit.
3. Client : l'adresse du serveur DNS doit être correctement renseignée, le nom machine doit correspondre a celui du compte d'’ordinateur.
4. Client : une demande à se rattacher au domaine doit être faite.

Ces étapes peuvent se faire manuellement, ou peuvent être automatisées de certaines manières…

### 1-m Création du compte ordinateur sur le serveur (manuelle)

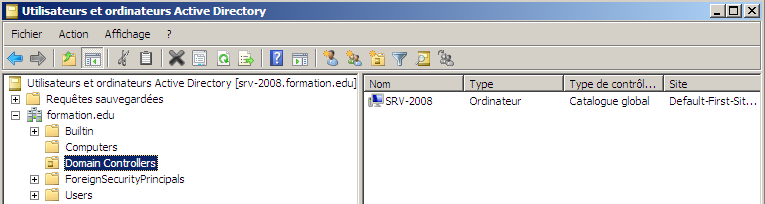
Les membres du groupe **Opérateurs de compte**, **Admins du domaine** peuvent créer des comptes ordinateurs

Par défaut, les utilisateurs authentifiés dans un domaine reçoivent le **droit d’utilisateur Ajouter des stations de travail au domaine** et ils peuvent créer jusqu’à 10 comptes d’ordinateurs dans le domaine

**N.B:** on peut aussi dans une unité d’organisation, attribuer à l’utilisateur ou au groupe l’autorisation **Créer des objets d’ordinateur**

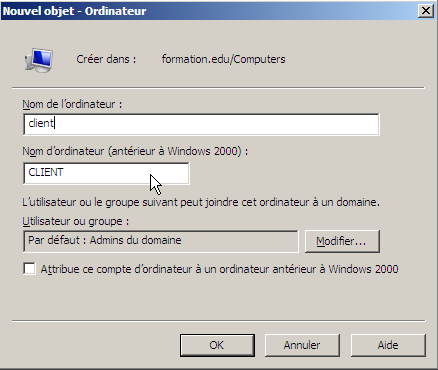
Pour créer un compte ordinateur, il faut lancer la console

Outils d’Administration / Utilisateurs et ordinateurs Active Directory



Se placer dans L'UO voulue (par exemple **Computers**) puis demander dans le menu

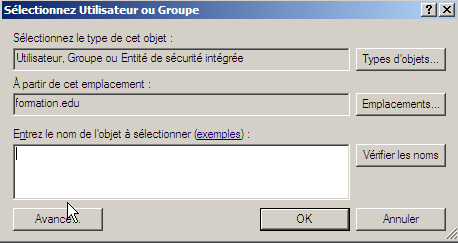
Action / Nouveau / Ordinateur un assistant se déclenche alors



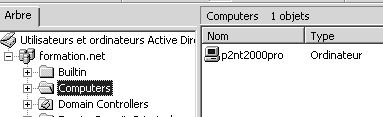
Et rentrer ici le nom machine du poste SEVEN XP qui va faire sa demande d’accès au Domaine

Ainsi que les comptes de domaines autorisés à ajouter ce PC au domaine : par défaut le groupe des

**Admins du domaine**…



Et le compte ordinateur se crée !



### 1-a Création du compte ordinateur (à la volée)

Windows 2012 accorde par défaut le droit d'ajouter des stations de travail à un domaine au groupe Utilisateurs authentifiés

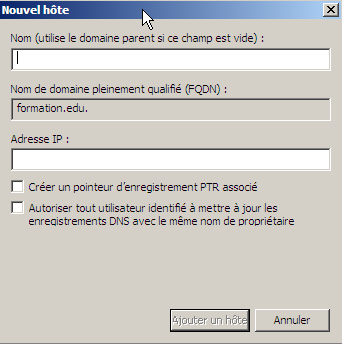
Un utilisateur authentifié peut joindre par défaut dix comptes d'ordinateur au maximum

Un administrateur de Domaine aussi, évidemment, et sans limitation de nombre.

Lorsqu’un utilisateur authentifié crée à la volée un compte ordinateur, celui-ci est stocké dans l'**UO** par défaut **Computers**.

### 2 –m Création de l'enregistrement hôte dans le DNS (manuelle)

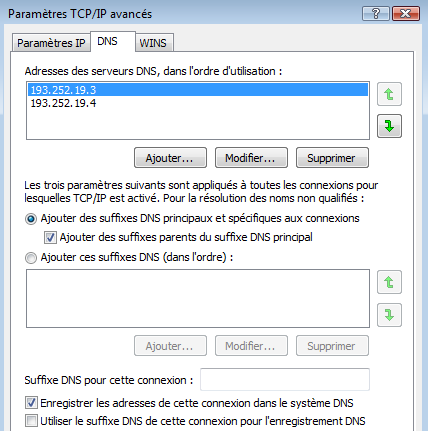
Dans le DNS on ajoute un hôte



### 2 –a Création de l'enregistrement hôte dans le DNS (à la volée)

Dans le cas d'un machine 10, SEVEN, et d'un serveur DDNS acceptant les mises à jours…,

et si dans les paramètres avancés tcp-ip, onglet **DNS**



on a demandé

**Enregistrer les adresses… dans le système DNS**

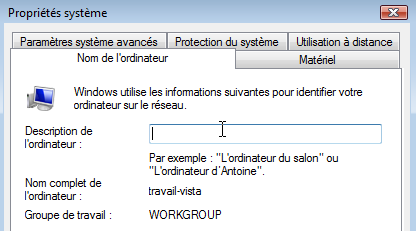
Alors l'enregistrement hôte peut de faire tout seul automatiquement.

### 3 Saisie dans les paramètres Tcp-ip et vérification du nom machine

il faut saisir l'adresse du serveur DNS dont le client va dépendre



et vérifier le nom machine



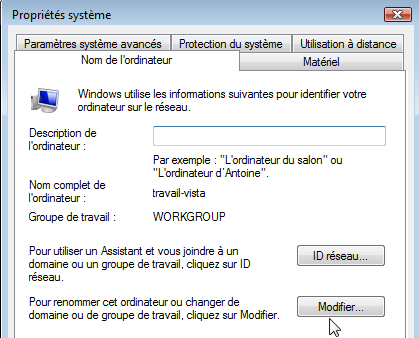
**N.B**: attention pour les postes SEVEN et XP, ne pas confondre le nom d'hôte (nom complet) utilisé et le nom indiqué en "description" dans les propriétés du poste de travail. ou système…

**N.B**: Si un changement de nom est nécessaire, il faut absolument rebooter le PC avant de faire la demande d'adhésion.

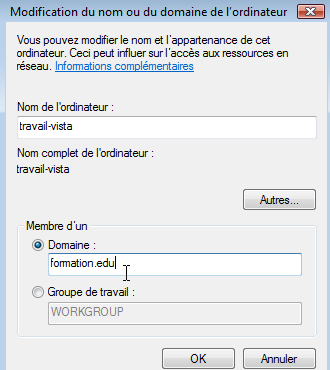
### 4 Demande d'adhésion au Domaine

Sous 10 SEVEN l'appartenance au domaine se fait

*  en demandant dans le panneau de configuration l’icône **système** puis l’onglet **identification réseau**
* en faisant un clic droit sur l’icône **ordinateur** du bureau, et demander **propriété** puis l’onglet **Nom de l'ordinateur**



on demande **Modifier…**

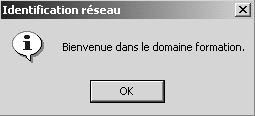


il faut rentrer un nom DNS !

Après authentification obligatoire, on pourra alors finir la procédure

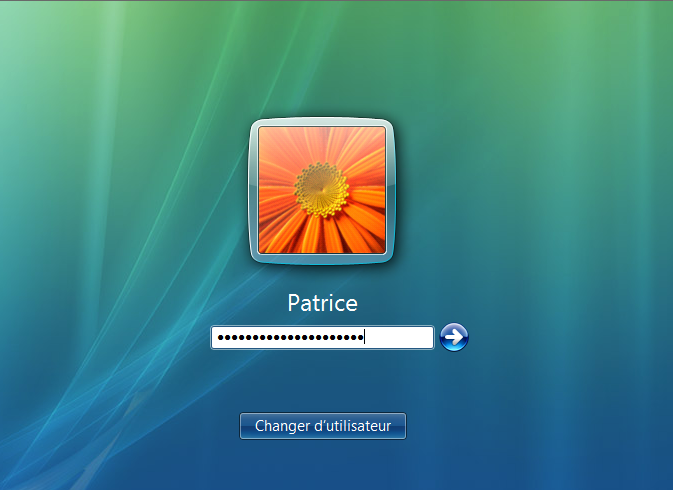
Et changer l’appartenance ou non à un Domaine

et si tout se passe bien on a



# Ouverture de Session

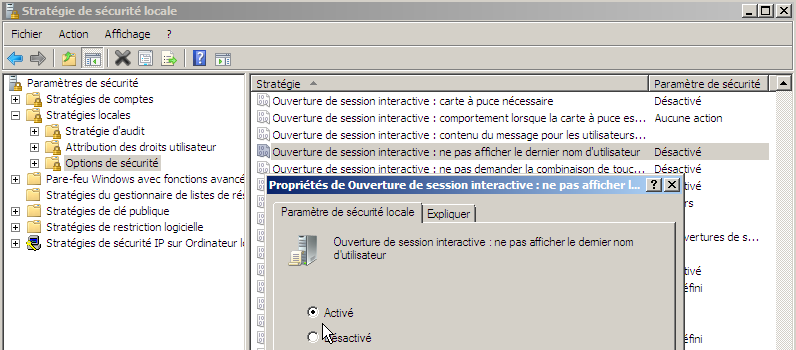
## Dernier login utilisé :

Par défaut, 10 et SEVEN re-proposent de visualiser le dernier utilisateur ayant ouvert une session.

Par sécurité, ou simplement par commodité (pour changer de login sous SEVEN il faut demander expressément **autre utilisateur** dans la fenêtre de login…)

il est possible de désactiver cette fonction via les stratégies de locales de sécurité

**Panneau de configuration / outils d’administration / stratégies de sécurité locale**



**N.B :** par ailleurs il est fortement déconseillé de garder la possibilité d’ouvrir des sessions multiples sur un poste en domaine, cela ne peut qu'amener des perturbations…

## Ouverture de session Normalisée (depuis SEVEN) :

Une fois le poste Windows 10 – (SEVEN) raccordé au domaine…

Si le poste client se nomme « **client-10 »**

Et le domaine se nomme« **formation.edu »** nom netbios « **formation »**

On peut taper un nom de la forme : **NOM\LOGIN**

**client-10\administrateur**  admin local du poste

**formation.edu\administrateur**  admin domaine,

**formation\administrateur**  admin domaine (nom NETBIOS)

On peut taper un nom de la forme : **LOGIN@NOM** (domaine uniquement)

**administrateur@formation.edu**  admin domaine

**administrateur@formation**  admin domaine (nom NETBIOS)

**administrateur@client-10**  ne marche pas

## Changement avec ouverture avec XP :

Une fois le poste XP raccordé au domaine…



Si ce n’est pas le cas, on demande le choix du domaine via **Options>>**



Dans **Se connecter à**: 2 choix existent :

* **Domaine**
* **Cet Ordinateur**

Il faudra alors choisir si on demande de s’authentifier sur le domaine ou sur le poste localement à travers cette liste déroulante.

# Comptes utilisateurs de domaine

## Comptes Utilisateurs Prédéfinis :

Sous **Windows Serveur** Il existe 2 Comptes Utilisateurs prédéfinis





Le **Compte Administrateur** :

C'est la personne qui aura le pouvoir maximal sur la station de travail, et pourra gérer la configuration du système

Ce compte ne peut être supprimé, mais peut être renommé

Le **Compte Invité** :

Sert pour des utilisateurs occasionnels ayant un minimum de droits sur le système

Ce compte par défaut est inactivé

Sous Windows 2003 Serveur un nouveaux compte etait crée, il n’existe plus sous à partir de Windows 2008 Serveur

Le **Compte Support** :

Ce compte par défaut est inactivé

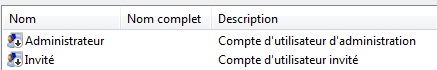


**N.B**  Sur un **Serveur CD**, les comptes sont représentés par une icône , car ce sont forcément des **Comptes de Domaine**





**N.B** : sur un client Windows 10 SEVEN ou XP, un compte utilisateur est représenté avec une icône devant une machine, car il s’agit forcement d’un **Compte local**

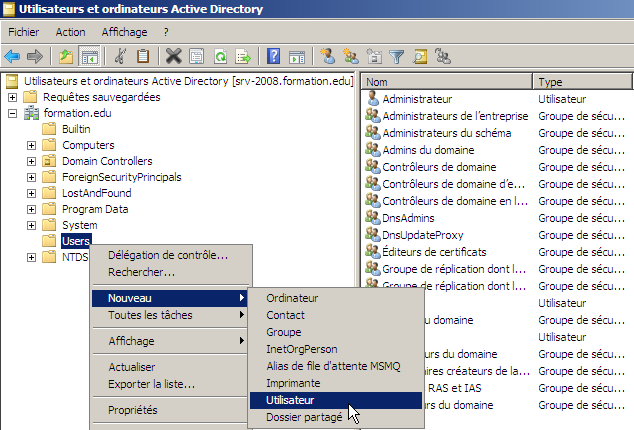


## Créer un Compte Utilisateur sur le Domaine:

Dans **Utilisateur et Ordinateurs Active Directory**

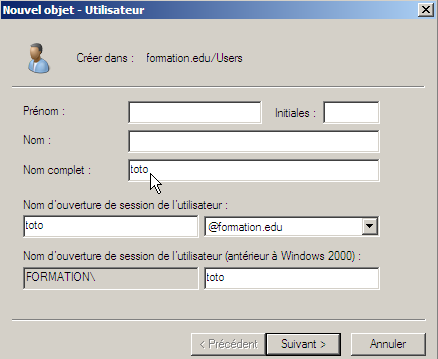
On se place dans l’unité organisationnelle voulue, par exemple **Users** et on demande ensuite

Clic droit , **Nouveau / Utilisateur**



Un assistant se déclenche alors

Les 3 renseignements requis au minimum sont

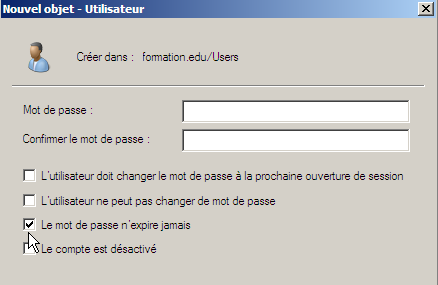


**Nom complet**

**Nom d’ouverture de session de l’utilisateur**

**Nom d’ouverture de session de l’utilisateur (antérieur à Windows 2000)**

Et le mot de passe



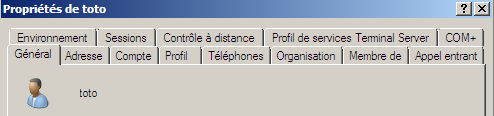
On peut choisir ses réglages…

il vaut mieux éviter de demander de changer le mot de passe à la première ouverture de session, surtout en formation…

durée par défaut :45j

## Propriété Compte Utilisateur de Domaine:

Il faut se placer sur le compte utilisateur voulu et demander le menu contextuel **propriété…**



Parmi les onglets existants, certains sont indispensables au quotidien,

**Général**

**Compte**

**Profil**

**Membre de**

d’autres correspondent à des fonctionnalités plus spécifiques

**Environnement**

**Sessions**

**Contrôle à distance**

**Profil de services Terminal Server**

**Com+**

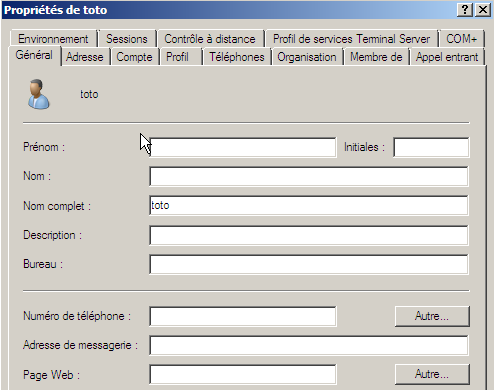
**Adresse**

**Téléphones**

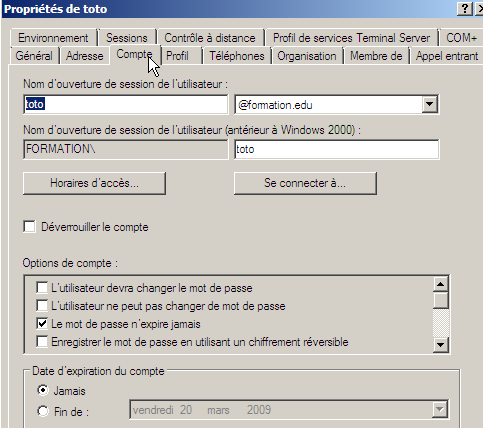
**Organisation**

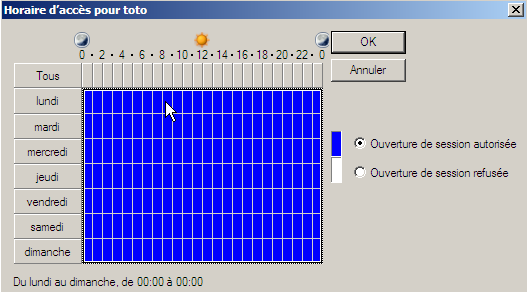
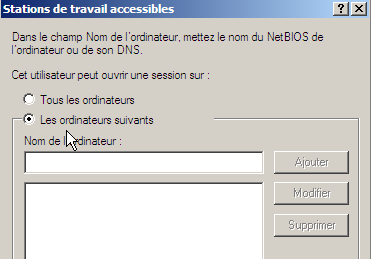
**Appel entrant**

### Compte Utilisateur onglet Général :



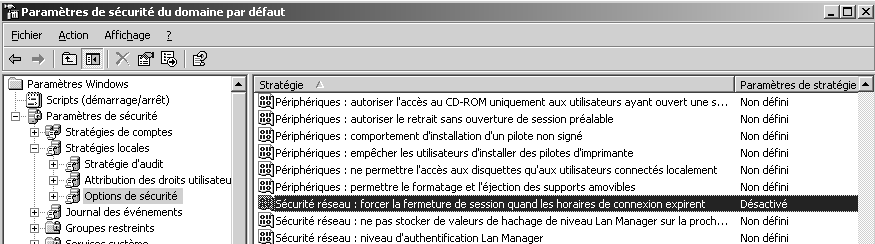
### Compte Utilisateur onglet Compte :





**Horaire d’accès**

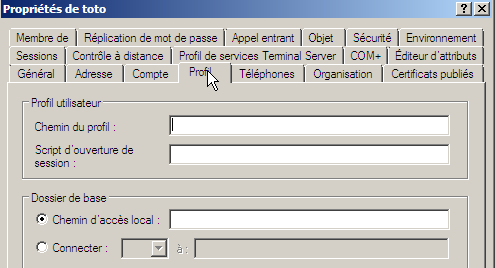
Si jamais un utilisateur reste en session après les horaires convenus, par défaut il ne sera pas déconnecté. Cela est modifiable par une **stratégie de Domaine**



**Se connecter à**

Si le nom **Netbios** est utilisé, donc cela s’applique aussi à des postes Windows 9.x, même si dans ce cas on ne pourra pas garantir le poste (comme avec Windows 10, SEVEN ou XP…)

### Compte Utilisateur onglet Profil :



**Profil utilisateur**

Il est possible de définir des profils errants, et des profils obligatoires non modifiables

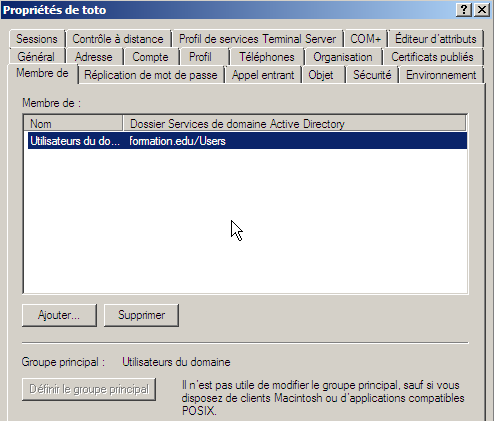
**Script d’ouverture de session**

On peut développer des scripts se déclenchant au moment de l’ouverture de session de cet utilisateur sur le client (cf chapitre script page 98)

**Dossier de base**

Une facilité de création de répertoire sécurisé pour cet utilisateur peut être mise en place (cf chapitre répertoire de base page 94)

### Compte Utilisateur onglet Membre de :



**Ajouter / Supprimer** : Il est possible de visualiser / modifier l’appartenance de l’utilisateur à un groupe local – global – universel…

# Groupes Locaux

## Privilèges - permissions :

Il ne faut pas confondre "**privilèges**", qui est un paramètre pérenne, affecté à une "classe" d'utilisateurs

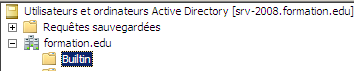
Avec "**permissions**", qui est un paramètre ponctuel, affecté à une "instance" d'utilisateur

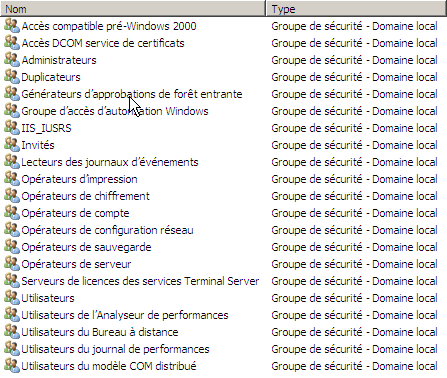
## Groupes Locaux Prédéfinis :

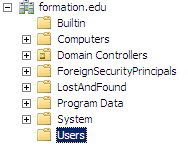
Les droits d'un utilisateur sont souvent déterminés par le groupe auquel il appartient, un **groupe** étant un ensemble d'utilisateur ayant les mêmes droits, ou mieux, un ensemble de droits et de permissions bien définis, dont on bénéficiera lorsque l'on en fait partie.

Un groupe local à un symbole qui est sur un serveur 

Il existe un certain nombre de **groupes prédéfinis** dans Windows, depuis le groupe **Administrateurs** (disposant de tous les droits) jusqu'au groupe Invité (ayant les droits les plus faibles)

Sur les Serveurs les **groupes locaux** prédéfinis sont stockés essentiellement dans l’UO **Builtin**

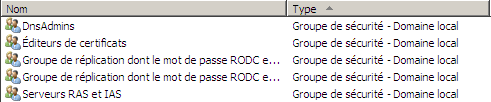
****



**N.B** : Les groupes prédéfinis suivant n’existent pas sous Windows 2003 Serveur

* IIsiusr
* Accès DCOM service de certificat
* Opérateurs de chiffrement
* Lecteurs des Journaux d’évènements

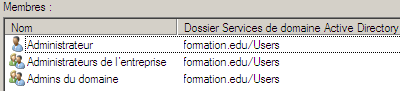
Certains groupes locaux prédéfinis sont aussi stockés dans l’UO **Users**



### Groupe Local Administrateurs

Contient : Compte **Administrateur** (de la machine locale)

+ Groupe Global **Admins du Domaine**

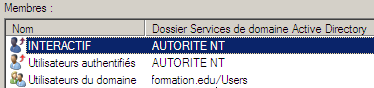


Utilisation : Tout faire sur la machine locale (si la machine est un contrôleur de domaine, on peut tout faire sur le domaine)

### Groupe Local Utilisateurs

Contient : Tous les comptes crées sur la machine

Groupe Global **Utilisateurs du Domaine**

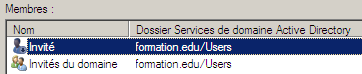


Utilisation : Faire ce que on leur a accordé et accéder aux ressources que on leur a partagé

### Groupe Local Invités

Contient : Compte **Invité**

+ Groupe Global **Invités du Domaine**



Utilisation : Faire ce que on leur a accordé et accéder aux ressources que on leur a partagé. Mais les membres de ce groupe ne peuvent pas modifier de manière permanente leur environnement

### Opérateur de sauvegarde

Contient : Vide

Utilisation : Sauvegarder et restaurer des fichiers sur la machine locale (via le gestionnaire de sauvegarde)

### Opérateur de Serveur

Contient : Vide

Utilisation : Les membres peuvent administrer les serveurs de domaine

### Groupe Local Utilisateurs Bureau à Distance

Contient : Vide

Utilisation : Utiliser le bureau à Distance

### Groupe Local Opérateurs de configuration réseau

Contient : Vide

Utilisation : Droits de configuration réseau (changement adresse IP)

### Groupe Local Utilisateurs avec Pouvoir (que sous SEVEN - XP)

Contient : Tous les comptes autorisés manuellement

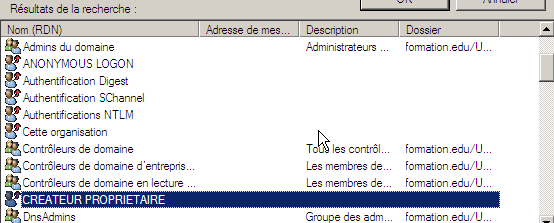
(+ Groupe Global **Utilisateurs du Domaine)**

Utilisation : Faire ce que on leur a accordé et accéder aux ressources que on leur a partagé

**N.B: En général beaucoup de groupes prédéfinis par rapport aux besoins de gestion d'un réseau local classique, et qu'il paraît souhaitable de n'utiliser que les groupes importants**

## Groupes Spéciaux

Ces **groupes Spéciaux** prédéfinis, l'administrateur lui-même ne peut les détruire ni les renommer, et **on les voit apparaître notamment lors du partage d’accès aux ressources**.



Autrement dit **ce n’est pas vous qui gérez les groupe spéciaux prédéfinis, mais vous pouvez vous en servir….**

En effet, selon ce qu'un utilisateur est en train de faire, il devient automatiquement membre (ou est supprimé) d'un groupe Spécial

[**https://docs.microsoft.com/fr-fr/windows/security/identity-protection/access-control/special-identities**](https://docs.microsoft.com/fr-fr/windows/security/identity-protection/access-control/special-identities)

Seuls deux de ces groupes présentent un intérêt dans un premier temps

### Utilisateur authentifiés

Contient : Tous les utilisateurs ayant ouvert une session vec un nom d'utilisateur et un mot de passe

Utilisation : Accorder des droits à tous les utilisateurs

### Tout le monde

Contient : Tous les utilisateurs travaillant sur une machine, y compris les invités. Contient les **utilisateurs Authentifiées** plus les I**nvités**, et le **Local Service**

Utilisation : Accorder des droits à tous les utilisateurs

### Créateur propriétaire

Contient : L'utilisateur ayant créé ou pris possession d'un ressource (en NTFS)

Utilisation : gérer les accès aux fichiers et aux dossiers sur des disques NTFS

### Anonymous Logon

Ouverture de session anonyme

Contient : Ce groupe représente les utilisateurs et les services qui accèdent à un ordinateur et à ses ressources par l’intermédiaire d’un réseau sans utiliser un nom de compte, un mot de passe ou un nom de domaine

Sur Windows NT et des versions antérieures, le groupe Ouverture de session anonyme est un membre par défaut du groupe Tout le monde.

Depuis Windows Server 2008 ou 2003, le groupe Ouverture de session anonyme n’est plus un membre par défaut du groupe Tout le monde.

### Réseau

Contient : utilisateurs qui accèdent à une ressource donnée sur le réseau, par opposition aux utilisateurs qui accèdent à une ressource en se connectant localement à l’ordinateur contenant la ressource. Chaque fois qu’un utilisateur accède à une ressource donnée sur le réseau, l’utilisateur est ajouté automatiquement au groupe Réseau

### Interactifs

Contient : Ce groupe représente tous les utilisateurs qui sont actuellement connectés à un ordinateur particulier et qui accèdent à une ressource donnée sur cet ordinateur, par opposition aux utilisateurs qui accèdent à la ressource sur le réseau

# Groupes Globaux-Universels

## Groupes locaux - globaux - universels:

En fait 2 catégories de groupes existent par défaut depuis les serveurs 2003:

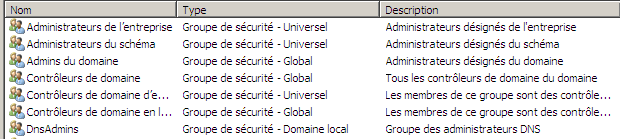
1. Les **Groupes Globaux :** contiennent les utilisateurs du domaine, c'est à dire définissent les groupes de personnes qui auront les même droits et permissions sur tout le Domaine
2. Les **Groupes Locaux :** sont généralement associés à une machine, et définissent les droits d'accès se rapportant à des ressources locales, c'est à dire sur une machine

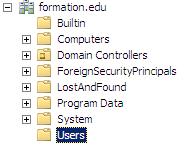
**N.B:** il existe des **Groupes Locaux de Domaine**, et des **Groupes Locaux hors Domaine**.   
En effet si un groupe local est défini sur un contrôleur de Domaine, il existera sur tous les contrôleurs de domaine, alors qu s'il est défini sur une machine autre, il n'existera que sur cette machine

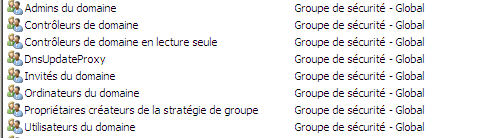
Et trois catégories depuis les serveurs 2008, car un nouveau type de groupe apparaît:

1. Les **Groupes Universels :** permettent de consolider les groupes qui s’étendent sur plusieurs domaines. Pour ce faire, ajoutez les comptes aux groupes à étendue globale et insérez ces groupes dans des groupes à étendue universelle

Un **groupe global** – **Universel** à un symbole différent  sur un serveur



Depuis 2008 SRV les **groupes globaux** et **Universels** prédéfinis sont stockés essentiellement dans l’UO **Users**



Sur un serveur 2003, les 2 groupes **Administrateur de l’entreprise**, **Administrateur du schéma**, peuvent exister en tant que **Groupe Global** si on choisit un niveau fonctionnel 2000…



Le groupe **Contrôleur de domaine d’entreprise en lecture seule**, **Administrateur**  ne peut exister que sur un serveur 2008 RODC



## Groupes Globaux prédéfinis

Sur tout poste NT Server 2012 2008 Contrôleur de Domaine

### Admins du Domaine

Contient : Compte **Administrateur**



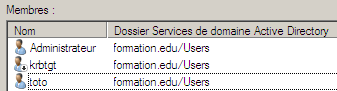
Inclus dans : Groupe Local **Administrateurs** de toute poste du domaine



Utilisation : Tout faire sur la machine locale et sur le domaine

### Utilisateurs du Domaine (Utilisa. du Domaine sous 2003)

Contient : Automatiquement tous les comptes crées sur le domaine , on ne peut les supprimer de leur groupe principal



Inclus dans : Groupe Local **Utilisateurs** de chaque machine du domaine, y compris serveurs



Utilisation : Faire ce que on leur à accordé et accéder aux ressources que on leur à partagé

### Invités du Domaine

Contient : Compte Invité



Inclus dans : Groupe Local **Invité** de chaque machine du domaine, y compris serveurs



Utilisation : Faire ce que on leur à accordé et accéder aux ressources que on leur a partagé. Mais les membres de ce groupe ne peuvent pas modifier de manière permanente leur environnement

## Inclusions entre groupes sous NT

Un intérêt majeur de la notion de groupe, réside dans l’idée de pouvoir inclure des groupes dans des groupes, ainsi que des utilisateurs dans des groupes.

Cela permet de structurer les accès aux ressources et les attributions de droits de manière plus fiable et rationnelle, plutôt que de travailler au niveau de l’individu.

**Sous Windows 2012-2008 (mixte-natif)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Type de Groupe | Peut contenir (**en Mixte-NT4)** | Peut contenir (***en natif)*** | Peut être membre de **(en Mixte-NT4)** | Peut être membre de **(*en natif)*** |
| **G-LOCAL** | **Utilisateur**  **G-Global** | **Utilisateur**  **G-Global**  ***G-Local***  ***G-Universel*** | **-** | ***G-Local*** |
| **G-GLOBAL** | **Utilisateur** | **Utilisateur**  ***G-Global*** | **G Local (mixte)** | **G Local**  ***G-Global***  ***G Universel*** |
| **G-UNIVERSEL** | - | ***Utilisateur***  ***G-Global***  ***G-Universel*** | **-** | ***G-Local***  ***G Universel*** |

En mode natif (exclusion de NT4) il est possible désormais de :

* Inclure des groupes Locaux dans des groupes Locaux
* Inclure des groupes Globaux dans des groupes Globaux
* Créer des groupes Universels
* Changer de Nom de Domaine (…)

## Quelques règles pour créer des groupes :

L'administration d'un réseau Windows repose sur une analyse en 3 étapes

1. Définir les diverses fonctions ou types d'utilisateurs intervenant sur le réseau, pour permettre la définition des droits et des permissions des Groupes Globaux
2. Définir les diverses fonctions et ressources utilisables localement sur un poste selon des besoins des différents types d'utilisateur pour créer les Groupes Locaux
3. Faire de ces Groupes Globaux des membres des Groupes Locaux

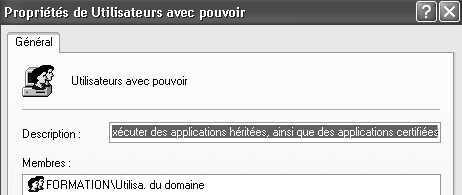
* Pour Créer des Groupes il faut faire partie d'un des groupes prédéfinis suivant : **Administrateurs**, **Opérateurs de Compte**
* Les noms de groupe doivent être uniques au sein du Domaine, être différents des noms des comptes utilisateurs ne pas dépasser 20 caractères ni contenir les caractères suivants :   
   **? \ \* " < > | / [ ] ; : + =**
* Regroupez logiquement tous les utilisateurs du domaine en fonction de leurs besoins commun:   
  Par exemple tous ceux devant utiliser une imprimante couleur, tous ceux devant accéder en lecture à tous les fichiers…
* Créez d'abords les Groupes Globaux logiques d'utilisateurs, puis ajoutez ensuite dans chaque groupe les comtes utilisateurs nécessaires
* Créez des Groupes Locaux en fonction des besoins d'accès aux ressources
* Affectez aux groupes locaux les permissions adéquates
* Incluez les Groupes Globaux dans les groupes locaux

## Exemple : Utilisateur de Domaine - Utilisateur avec pouvoir

On souhaite qu’un utilisateur, dès qu’il est créé, soit reconnu sur tous les postes du domaine avec des droits du niveau utilisateurs avec Pouvoir

Au niveau de chaque poste membre du domaine, il faut les configurer avec comme membre du groupe local des **Utilisateurs avec Pouvoir**

Le groupe des **Utilisateurs du domaine**



## Exemple accès ressources :

Si les chefs de service (regroupés dans un **Groupe Global** "***Chef de service***") doivent accéder à tous les fichiers

Et les commerciaux (regroupés dans un **Groupe Global** "***Commerciaux***" ) ne doivent que pouvoir les lire,

Alors il faut créer deux **Groupes Locaux** là où sont stockés les fichiers: un pour l'accès complet (nommé "***Accès complet***") , l'autre pour l'accès en lecture seule (nommé "***Accès lecture***").

Le **Groupe Global** ***"Chef de service***" sera inclus dans le **Groupe Local** "***Accès complet***",

le **Groupe Global** "***Commerciaux***" sera inclus dans le **Groupe Local** "***Accès lecture*** "

## Exemples :

On a besoin de créer au niveau des utilisateurs une fonction de Secrétariat une fonction de Commercial et une fonction de comptable. Les Logiciels installé sont des logiciels de bureautique ou de gestion de base de donnée.

trois groupes globaux "**Secretariat**",  
 "**Commercial**"  
 "**Comptable**" correspondant aux fonctions ,

ainsi que deux groupes locaux définissant le type de ressources que l'on peut avoir besoin d'utiliser, à savoir "**Bureautique**"  
 "**Base-de-Donnee**"

On intègrera chaque groupe global dans les groupes locaux dont il à l'usage, par exemple

**groupe global**  
Secretariat

**groupe global**  
comptable

**groupe global**  
commercial

Inclus dans ...

Inclus dans

Inclus dans

et dans





**Groupe Local**   
Base-de-Donnee

**Groupe Local**   
Bureautique

* Si un Commercial arrive, en le mettant dans le grpe Global "**Commercial**" il récupère tous les droits sur les logiciels qu'il peut avoir besoin d'utiliser...

## Exemple : Groupes Admins de Domaine & Administrateurs:

Dans un domaine, on a besoin de créer au niveau des utilisateurs une fonction d'Administrateur, il existe par conséquent un groupe global "**Admins du Domaine**" correspondant à la fonction d'administration sur tout le domaine en général

Au niveau des stations il existe un groupe local "**Administrateurs** " ayant tous les droits et les permissions possibles et imaginables mais limitées à la station

Le Groupe Global "**Admins du Domaine**" est intégré dans le groupe Local "**Administrateurs** " de façon à ce que les administrateurs du domaine soient également administrateur de la station

**groupe global**  
Aministrateur Domaine

compte utilisateur jean dupont

compte utilisateur albert maurice

Inclus dans

Inclus dans

Inclus dans







Client 3  
**Groupe Local**   
Administrateur Station

Client 2  
**Groupe Local**   
Administrateur Station

Client 1  
**Groupe Local**   
Administrateur Station

* Si on relie une nouvelle station, le groupe Global "**Admins du Domaine**" est placé dans le groupe Local "**Administrateurs** " et très simplement, les membres du groupe des administrateurs de domaine ont tous les droit sur la station
* Si un nouvel Administrateur est embauché, il suffit de le placer dans le groupe Global "**Admins du Domaine**" pour qu'il récupère automatiquement tous les droits sur toutes les stations...

**N.B :** Si on avait travaillé au niveau des comptes directement, il aurait fallu insérer le nouvel administrateur dans chaque station au lieu de simplement l'ajouter dans le groupe Global "**Admins de Domaine**"

# Création – gestion de groupes

## Groupe local sur un poste:

l'outil pour faire cela se trouve dans le menu

**Démarrer / Programme / Outils d'Administration/ gestion de l’ordinateur**



On demande le menu

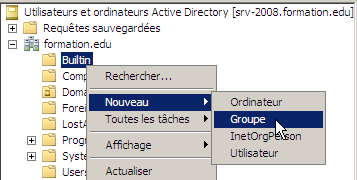
Action /Nouveau groupe …

## Groupe local – Global sur un Serveur CD:

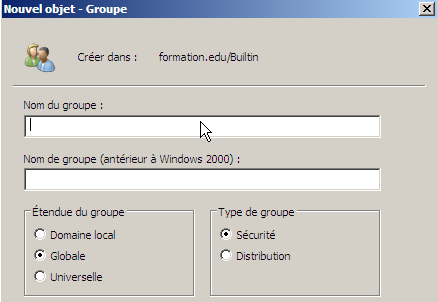
Sur le serveur contrôleur de domaine on demande

Utilisateurs et ordinateurs Active Directory

puis dans le gestionnaire MMC On se place par exemple sur l’UO **Builtin**



et on demande le menu **Action / Nouveau / Groupe** (ou clic droit, …)

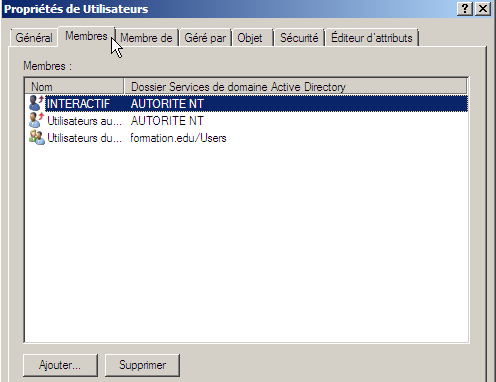


On demande un groupe dont la portée est **Local ou Globale**

puis OK

## Membres d’un groupe:

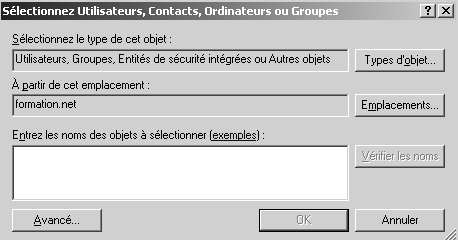
* Sur un poste **Serveur ou Windows** on fera un double clic sur le groupe que l’on souhaite gérer, deux onglets apparaissent, on choisit l’onglet **Membres** et on demandera **Ajouter**

****

et on demandera **Ajouter**

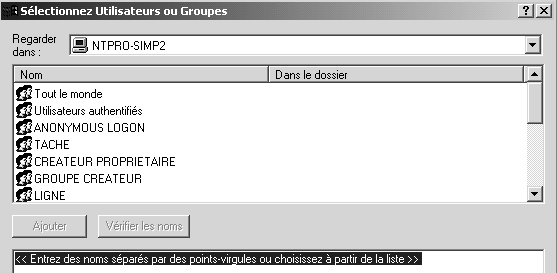
* Sur un poste client **Windows** on fera un double clic sur le groupe local que l’on souhaite gérer, onglet **Membres** et on demandera **Ajouter**

On obtiendra alors la boite de dialogue suivante :



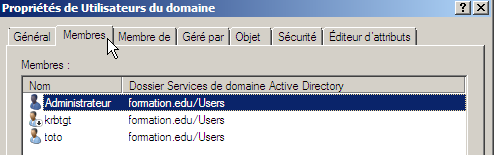
Proposant un certain nombre de Utilisateurs, **groupes locaux, globaux ou Universel**, selon le domaine dans lequel on effectue la recherche

Ou

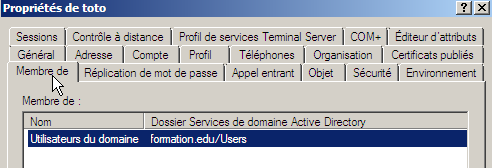


## Gérer - Information sur les groupes -

Si on peut savoir quels sont tous les utilisateurs membre d'un groupe, en double-cliquant sur le groupe et en demandant **Membres**



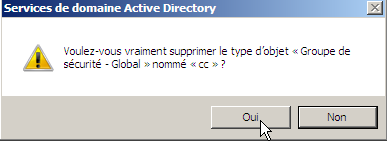
On peut aussi savoir quels sont tous les groupes dont un compte Utilisateur est membre en double-cliquant sur le compte Utilisateur, puis demander **Membres de,** on obtient alors



## Suppression d'un groupe

Il faut sélectionner le groupe que l'on veut supprimer et demander **Supprimer ...**

Un message de mise en garde apparaît informant du coté irréversible de la commande



Il faut parfois encore confirmer (sur AD un simple Confirmation est demandée)

# Répertoire de base

## Répertoire de base ou d'Accueil :

Il peut être intéressant de fournir pour chaque utilisateur, un répertoire par défaut dans lequel les commandes de type **Fichier / Ouvrir** ou bien de type **Fichier / Enregistrer sous** iraient correctement se placer.

Ce répertoire par défaut, nommé répertoire de base ou répertoire d'accueil, peut-être :

* placé sur la station locale où l'utilisateur ouvre sa session (on parle alors de « chemin local »)
* ou mieux, il peut être placé sur le serveur (on parle de « connecter »)

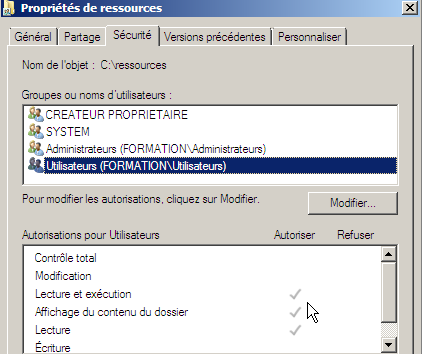
Si le client ouvre une session sur une machine de type SEVEN ou XP, un lecteur logique Réseau l'amenant directement sur son répertoire peut être automatiquement crée.

## Mise en Place :

Un certain nombre d'opérations doivent être effectuées, certaines avant la création des comptes utilisateurs, et d'autres pendant la création de ces comptes.

### Avant la création des comptes

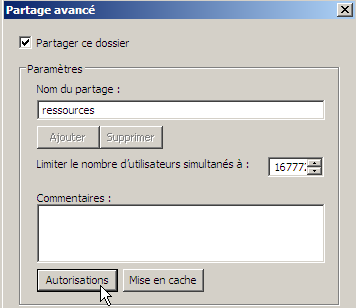
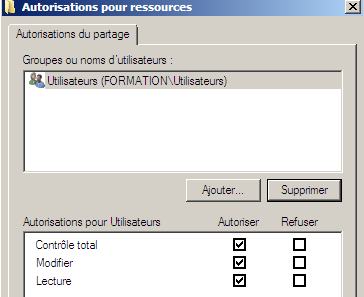
Il faut se créer la structure de rangement :

* Créer le dossier "racine" de la future arborescence pour les dossiers des utilisateurs, nommé par exemple **ressources (**mais il ne faut pas se créer soi-même les dossiers utilisateurs à l'intérieur ! **sauf si ce dossier est sur un volume FAT)**

Les permissions de sécurité NTFS sont les permissions par défaut

* Il faut ensuite partager ce dossier **Ressource** en donnant une permission de type **contrôle total** à tous les utilisateurs à même d'y venir par la suite

**N.B** : par sécurité il vaut mieux donner **contrôle total** au **groupe Utilisateurs** plutôt qu’au **groupe Tout le monde**…ainsi seuls les utilisateurs ayant des comptes de domaine peuvent accéder au dossier partagé !

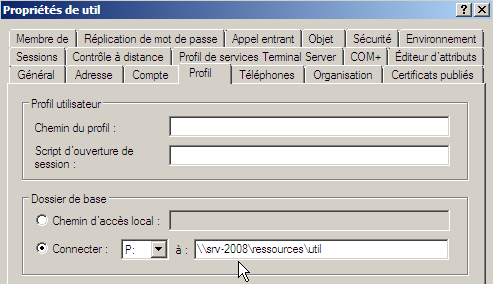


L’icône de partage apparaît

 ou 

### Pendant la création d'un compte

Lorsqu'ensuite l'on crée un compte Utilisateur, il faut demander les propriétés et demander l’onglet **Profil,**

****

Dans la boîte de dialogue il faut donner un nom et un emplacement au **dossier de base**, et choisir **Connecter**, puis choisir une lettre de lecteur logique associée à ce répertoire de base (ici **P:** par exemple)

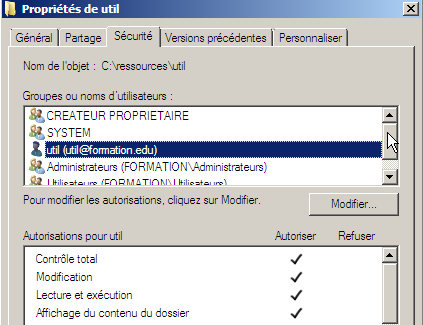


Après ouverture de session de **Util** sur un client, celui-ci devrait automatiquement voir apparaître

Sur le serveur un dossier perso pour util est crée…



La sécurité NTFS est posée par héritage, plus **util** en accès **contrôle total**



**N.B**: si on utilise la variable **%username%**, celle-ci sera automatiquement remplacée par le nom de l'utilisateur qui à ouvert une session, et créera automatiquement un dossier du même nom



Cela permet de créer un compte « modèle » utilisable ensuite par copier

Noter que dans l'écriture du type:

**\\serveur\ressource\%username%**

on à selon les conventions de nom les valeurs suivante :

**\\Serveur** nom d'identification du serveur sur lequel on crée les dossiers de stockage

**\ressource** nom du dossier "racine" des dossiers de chaque Utilisateur. C'est le seul que l'on crée !

**\%username%** Variable système prédéfinie

## Résultat :

Si on crée un répertoire de base pour les utilisateurs, la structure suivante (par exemple) va se créer automatiquement au fur et à mesure de la création des comptes :

**N .B** : si le dossier est dans un support NTFS, lors de la première connection de cet utilisateur, un dossier à son nom sera créé dans ressources avec des droits **pour cet utilisateur et l’administrateur** uniquement

**N .B**: si le dossier est dans un support FAT, lors de la première connection de cet utilisateur, le dossier à son nom ne sera pas crée (**il faut le faire au préalable**, pour chaque utilisateur…)

## Modifier le répertoire de base :

Il n'existe aucun moyen de modifier simplement de dossier de base pour plusieurs utilisateurs, si ce n'est de sélectionner tous les utilisateurs dont on veut modifier le dossier d'accueil, puis d'effectuer la modification

Rappels :

on peut trier les utilisateurs par leur nom, mais aussi par leur nom détaillé, (menu **Affichage /tri** dans le gestionnaire des utilisateurs…)

on peut en sélectionner plusieurs par la touche **CTRL**,

on peut en sélectionner tout un "paquet" en cliquant sur le 1°, en maintenant la touche **MAJ** appuyée, et en cliquant sur le dernier…

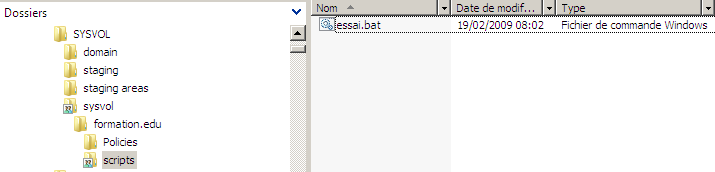
# Script d'ouverture de session

## Objectif :

Un script d'ouverture de session est un fichier qui est exécuté chaque fois qu'un utilisateur ouvre une session. Il peut s'agir d'un fichier de commandes (portant une extension de nom de fichier**.bat** ou **.cmd**) ou d'un programme exécutable (portant une extension de nom de fichier**.exe**).

Un script d'ouverture de session est un fichier qui est exécuté chaque fois qu'un utilisateur ouvre une session. Il peut s'agir d'un fichier de commandes (portant une extension de nom de fichier**.bat** ou **.cmd**).

Pour les ordinateurs clients, le chemin d'accès du script d'ouverture de session sur un serveur 2008-2003 est **Winnt\Sysvol\sysvol\domaine\scripts**.

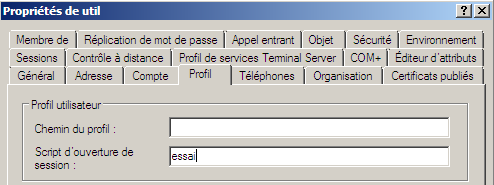


**N.B:** depuis 2012-2008, les clients Windows 10- SEVEN peuvent recevoir en plus à l'ouverture de session, une notion de stratégie.

Donc si un client est un poste Windows 10 ou SEVEN, alors celui-ci récupère lors de l'ouverture de session **les scripts et les stratégies**…

## Indiquer un script d'ouverture de session :

Pour chaque utilisateur, il est possible d'indiquer le nom d'un script d'ouverture de session, dans les propriétés des utilisateurs, en demandant onglet **Profil** tapez le nom de fichier à exécuter (sans **.bat**) dans la zone Nom du script d'ouverture de session :



**essai**

**N.B :** Si le script d'ouverture de session se trouve dans un sous-répertoire du chemin de ce script, indiquez son **chemin relatif** avant le nom du fichier, par exemple s'il se trouve dans un dossier nommé **actuels** alors il faut entrer **actuels\essai**

## Ecriture de scripts :

Il existe parfois de légère (et parfois importantes) différences de syntaxe entre l'implémentation des commandes sous environnement SEVEN, XP, 2000 …et la moindre erreur dans la syntaxe d'une commande fait que celle-ci ne s'exécute pas…

Par conséquent il est tout à fait conseillé de tester localement un script dans l'environnement de destination, pour vérifier son bon déroulement, avant de le mettre à disposition sur le serveur…

### création de lecteur logique

commande de base

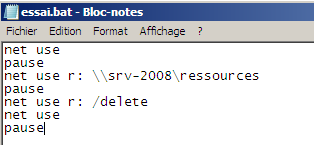
**net use x: /home**

ou

**net use x: \\nomposte\nompartage**

avec x correspondant à la lettre du lecteur que l'on désire connecter en tant que partage de base

voici un exemple de script permettant de visualiser, créer, et effacer un lecteur réseau



# Commande NET

## Convention d'écriture :

Pour utiliser les commandes en ligne; il est nécessaire par rapport à la syntaxe normale des fichier BATCH existant depuis ms-dos, de connaître quelques commandes spécifiques à NT, telles que NET ou AT

* Les mêmes conventions que pour NTBACKUP sont utilisées:

Ainsi, la ligne de syntaxe ci-dessous :

**NET COMMANDE [nom] {OPTION1 | OPTION2}**

signifie que vous devez taper NET COMMANDE et soit OPTION1, soit OPTION2. Par contre, vous n'êtes pas obligé de fournir un nom.

* Quand ils sont tapés à l'invite de commande, les noms de service comprenant deux mots ou plus doivent être entre guillemets anglo-saxons (**"**).

Par exemple, **NET START "Explorateur d'ordinateurs"** démarre le service d'exploration de l'ordinateur.

## Commandes NET Utilisables :

Les commandes utilisables avec la commande Net sont :

|  |  |
| --- | --- |
| **ACCOUNTS** |  |
| **COMPUTER** |  |
| **CONFIG** |  |
| **CONFIG SERVER** |  |
| **CONFIG WORKSTATION** |  |
| **CONTINUE** |  |
| **FILE** |  |
| **GROUP** |  |
| **HELP** |  |
| **HELPMSG** |  |
| **LOCALGROUP** |  |
| **NAME** |  |
| **PAUSE** |  |
| **PRINT** |  |
| **SEND** |  |
| **SESSION** |  |
| **SHARE** | Crée, supprime ou affiche des ressources partagées |
| **START** |  |
| **STATISTICS** |  |
| **STOP** |  |
| **TIME** | Synchronise l'horloge de l'ordinateur avec celle d'un autre ordinateur ou d'un domaine. |
| **USE** | Liste, établit ou rompt une connexion d'une station de travail à une ressource partagée |
| **USER** | Liste, ajoute, modifie ou supprime un utilisateur |
| **VIEW** | Affiche la liste des domaines, des ordinateurs ou des ressources partagées par l'ordinateur spécifié |

Pour plus de renseignement sur la syntaxe on peut taper

**NET xxx /?** voir **NET xxx /? |MORE**

exemple

**NET USE /?** voir **NET USE /? |MORE**

## Net Use :

**NET USE** établit ou rompt une connexion d'une station de travail à une ressource partagée. Employée sans argument, NET USE liste les connexions de la station de travail.

Les paramètres utilisables avec la commande Net USE sont :

**NET USE [nom de périph.|\*] [\\Ordinateur\Partage[volume] [mot de passe | \*]] [/USER:[nom de domaine\]nom d'utilisateur] [[/DELETE] | [/PERSISTENT:{YES | NO}]]**

ou

**NET USE [nom de périphérique | \*] [mot de passe | \*] [/HOME]**

ou

**NET USE [/PERSISTENT:{YES | NO}]**

|  |  |
| --- | --- |
| **nom de périphérique** | Spécifie le nom de périphérique affecté à la connexion à établir ou à rompre. Ce nom de périphérique désigne soit un lecteur de disque (de D: à Z:),soit une imprimante (de LPT1: à LPT3:). Mettez une astérisque pour affecter la première lettre disponible au périphérique. |
| [**\\Ordinateur**](file:///\\Ordinateur) | Est le nom du serveur qui gère la ressource partagée. Le nom d'ordinateur peut contenir de 1 à 15 caractères. |
| **\Partage** | Est le nom réseau de la ressource partagée. |
| **mot de passe** | Est le mot de passe nécessaire pour accéder à la ressource. |
| **\*** | Affiche un message demandant le mot de passe. Celui-ci n'est pas affiché lorsque vous le tapez. |
| **/USER** | Spécifie un nom d'utilisateur différent pour établir la connexion. |
| **nom de domaine** | Spécifie un autre domaine. Si cet argument est omis, le domaine où se déroule la session courante est utilisé. |
| **nom d'utilisateur** | Spécifie le nom d'utilisateur à employer pour la session. |
| **/HOME** | Connecte un utilisateur à son répertoire de base. |
| **/DELETE** | Rompt une connexion réseau et la supprime dans la liste des connexions persistantes. |
| **/PERSISTENT** | Permet de gérer les connexions réseau persistantes. La valeur par défaut est celle définie en dernier. |
| **YES** | Enregistre toutes les connexions à mesure que vous les établissez et les restaure à la session suivante. |
| **NO** | N'enregistre ni la connexion à établir, ni les suivantes ; les connexions existantes seront restaurées à la session suivante. Employez l'option /DELETE pour supprimer des connexions persistantes. |

## Net User

**NET USER** ajoute, modifie ou supprime un utilisateur. Employé sans argument, NET USER liste les paramètres de l'utilisateur

**net user** [*nom\_utilisateur* [*mot\_de\_passe* | **\***] [*options*]] [**/domain**]

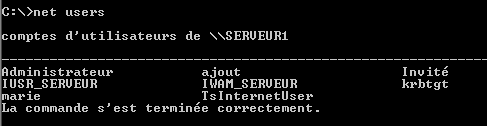
**net user** *nom\_utilisateur* {*mot\_de\_passe* | **\***} **/add** [*options*] [**/domain**]

**net user** *nom\_utilisateur* [**/delete**] [**/domain**]

**Paramètres**

Aucun

Utilisée sans paramètre, la commande **net user** affiche la liste des comptes d'utilisateurs sur l'ordinateur.



net users ou net user

*nom\_utilisateur*

Indique le nom du compte d'utilisateur à ajouter, supprimer, modifier ou afficher. Ce nom peut comporter jusqu'à 20 caractères.



net users compte ou

net user compte

*mot\_de\_passe*

Assigne ou modifie le mot de passe du compte d'utilisateur.

**\***

Produit une invite pour le mot de passe. Le mot de passe ne s'affiche pas quand vous le tapez à l'invite du mot de passe.

**/domain**

Exécute l'opération sur le contrôleur de domaine principal du domaine principal de l'ordinateur. Ce paramètre ne s'applique qu'aux ordinateurs Windows qui font partie du domaine Windows Server. Par défaut, les ordinateurs Windows Server exécutent les opérations sur le contrôleur de domaine principal.

Cette action est appliquée au contrôleur de domaine principal du domaine principal de l'ordinateur. Il peut ne pas s'agir du domaine de connexion.

**/add**

Ajoute un compte d'utilisateur à la base de données de comptes d'utilisateurs.

**/delete**

Supprime un compte d'utilisateur de la base de données de comptes d'utilisateurs.

## Net view:

**NET view** Affiche la liste des domaines, des ordinateurs ou des ressources partagées par l'ordinateur spécifié

**net view** [\\*nom\_ordinateur* | **/domain**[**:***nom\_domaine*]]

**net view** **/network:nw**[\\*nom\_ordinateur*]

**Paramètres**

Aucun

Utilisée sans paramètre, la commande **net view** affiche la liste des ordinateurs de votre domaine en cours.

\\*nom\_ordinateur*

Indique l'ordinateur pour lequel vous voulez afficher les ressources partagées.

**/domain**[**:***nom\_domaine*]

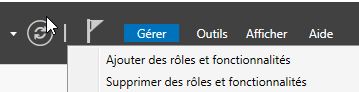
Désigne le domaine dont vous voulez afficher les ordinateurs disponibles. Si *nom\_domaine* est omis, tous les domaines du réseau sont affichés

# Sauvegarde Serveur

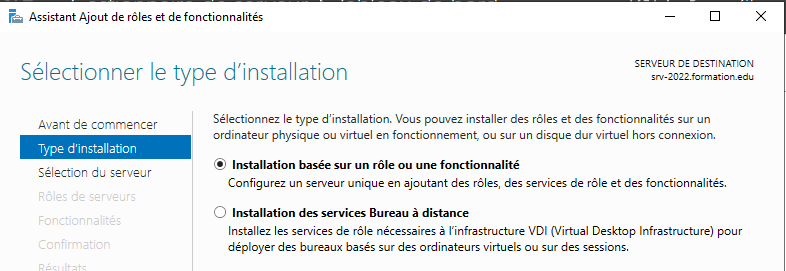
## Ajout du Rôle Sauvegarde :

La fonctionnalité n'est pas installée par défaut. Il est donc nécessaire de le faire dans le **gestionnaire de Serveur**, on demande

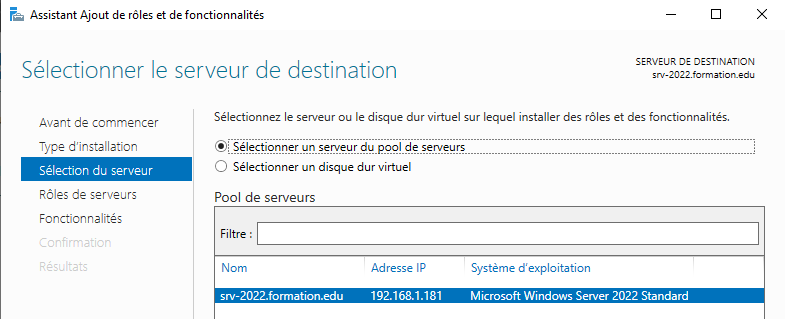
**Gérer / Ajouter des rôles et fonctionnalité**



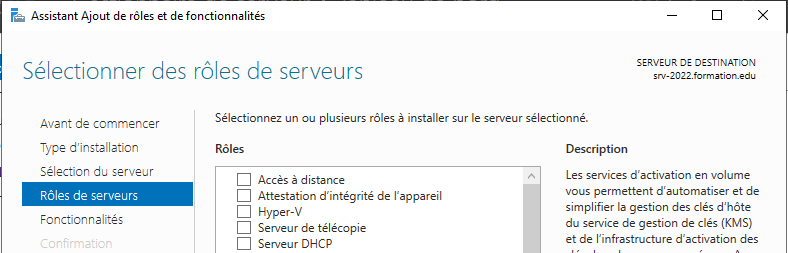
Puis



On choisit notre serveur

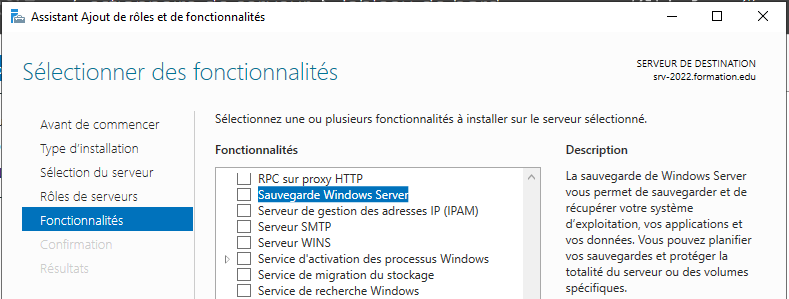


On coche aucun Rôle

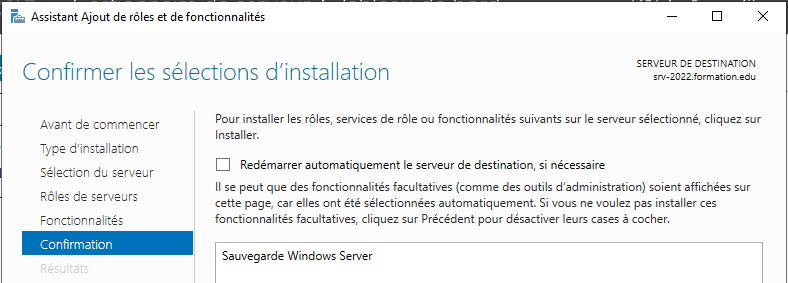


Par contre on demande la fontionnalité

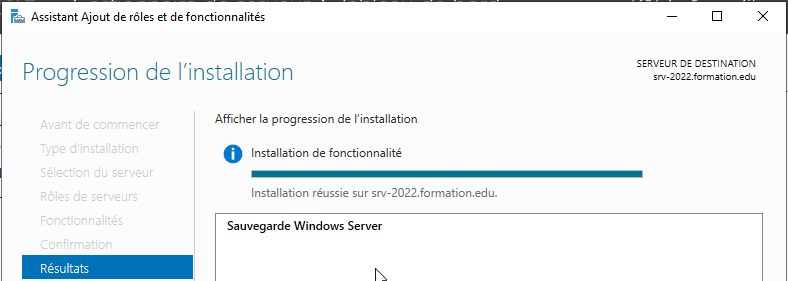
**Sauvegarde Windows Server**

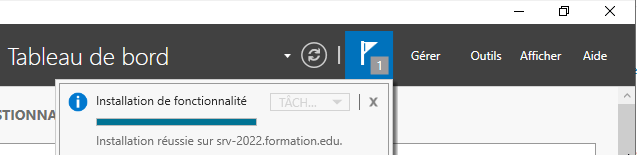


on confirme



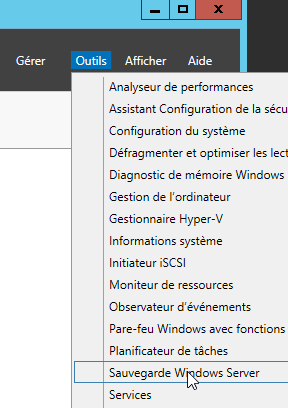
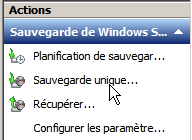
Et on a une validation



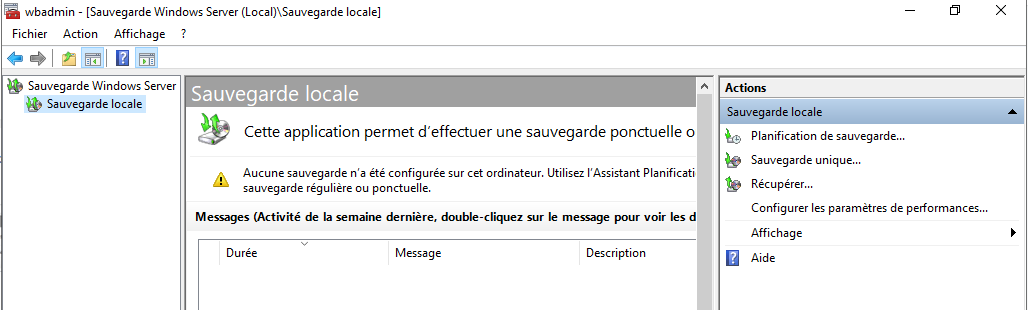


## Effectuer une Sauvegarde:

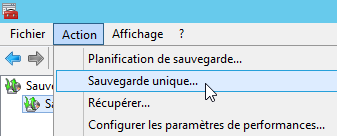
Depuis le **Gestionnaire de Serveur**, on demande **Outils / Sauvegarde Windows Server**



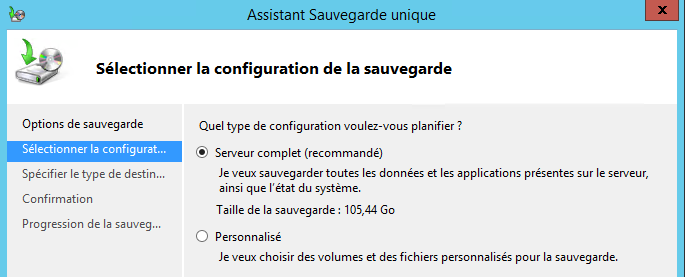
On arrive dans la console **wbadmin**, dans laquelle on va demander **Action / Sauvegarde Unique**



Il faut demander d'effectuer une **sauvegarde unique**

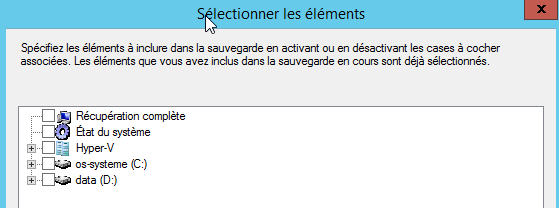


pour pouvoir ensuite la paramétrer..



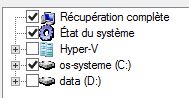
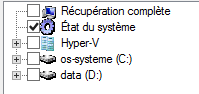
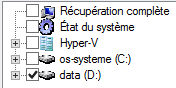
**N.B:** la granularité de l'outil de sauvegarde est le VOLUME, la restauration se fera ensuite par Volume, objectifs ou fichiers...

Si on demande **Personnalisé**, on obtient par exemple



dans laquelle on peut dire que les choix suivants correspondent à

**Serveur Entier** **Active Directory** **Data**

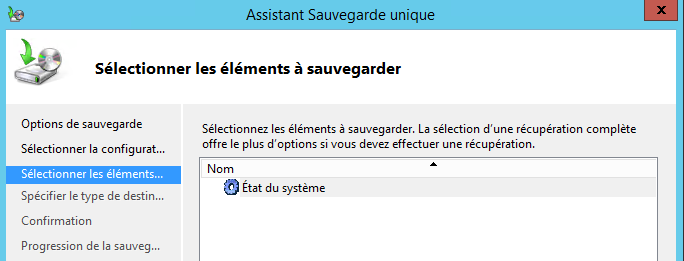
Si on souhaite sauvegarder **Active Directory**, on parle de sauvegarde de l'**état du système**… Si on souhaite sauvegarder le serveur complet, (on peut cocher récupération complète).Une sauvegarde de **l’état du système** avec un serveur Contrôleur de domaine comprends

* **Active Directory** : complète
* Volume partagé **SYSVOL** : contenant les modèles des stratégies de groupe, les stratégies, les scripts…
* Le **Registre** : tout la base de registre du système et des applications
* Fichiers de démarrage du système

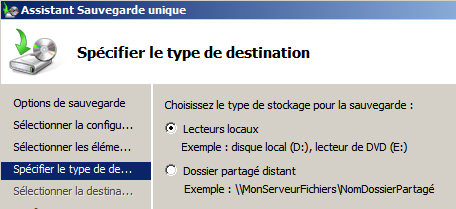
Un "**volume** est dit **"critique"** lorsqu'il contient l'un des éléments suivants

* Volume **système SYSVOL**:
* Volume de démarrage (celui ou windows est installé)
* Volume contenant **AD** (ntds.dit) et ses fichiers journaux

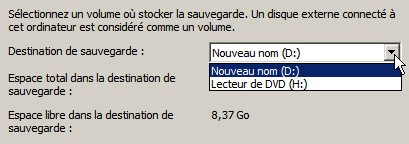
Pour sauvegarder que AD par exemple, on demanderait donc

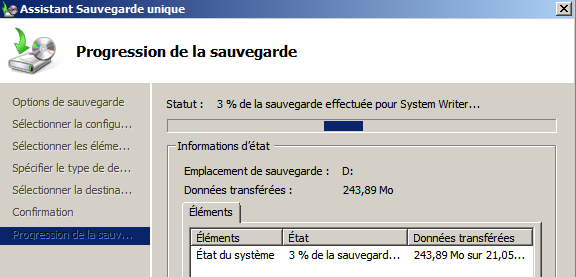


on peut choisir un emplacement

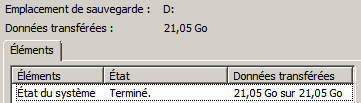


**NB**: on peut indiquer un chemin valable sur le réseau





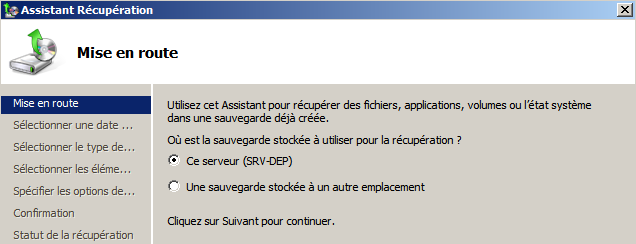
la taille peut être conséquente !!! (au minimum 6-10 Giga...)

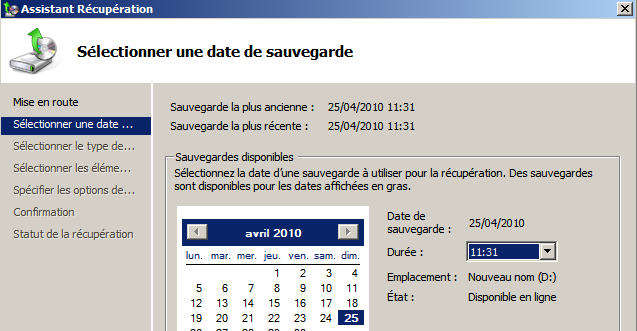


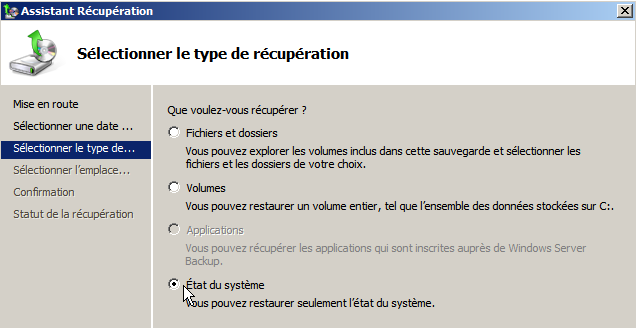
**N.B: Pour AD, cette sauvegarde ne doit pas être plus ancienne que 60 jours sous 2003 et 180 Jours sous 2008R2… car le CD ne garde des traces sur les objets supprimés que pendant cette durée !**

## Restauration...:

Il suffit de déclencher l’outil et de lancer l'assistant...







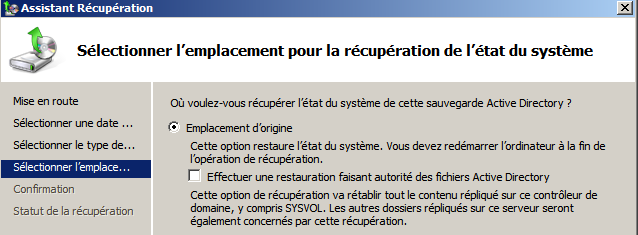
## Restaurer Active Directory:

Pour restaurer **Active Directory**, il s'agit de restaurer l'état du système



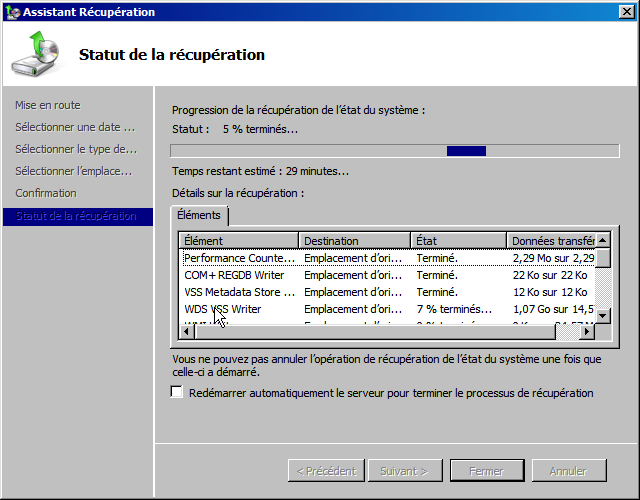
mais deux méthodes permettent de le faire :

* Méthode de restauration non forcée
* Méthode de restauration forcée (complète ou partielle)



**N.B** cette case à cocher est IMPORTANTE !

cela peut être long...



**N.B** ne pas redémarrer si on veut une restauration forcée partielle !

**Si on** **utilise la méthode non forcée**, après restauration, et s'il y a d'autres CD alors la réplication va rentrer en jeu, et les différences entre la restauration effectuées de AD et les copies de AD présentent sur les autres CD vont modifier à terme l'état de la restauration….

On **risque de ne pas avoir exactement** après re-synchronisation, **une restauration de AD** comportant exactement ce qu'il y avait dans la sauvegarde. Mais une résultante des données les plus récentes !

**Si on** **utilise la méthode forcée**, après restauration, et s'il y a d'autres CD alors la réplication va rentrer en jeu **Mais** les objet de la copie de AD que vous venez de restaure vont avoir un n° de version plus élevé que tous ceux présent dans les autres copies de AD.

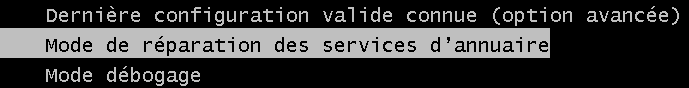
On **à exactement** après re-synchronisation, **une restauration de AD** comportant exactement ce qu'il y avait dans la sauvegarde, mais **PLUS** ce qui avait été nouvellement crée depuis cette sauvegarde !

## Exécuter une restauration non forcée:

Si on a un seul CD de domaine, c'est l'opération à faire…

Il faut suivre le mode opératoire suivant :

1. redémarrer l'ordinateur, **F8** (ou **MAJ+Arrêt**)et sélectionner l'option de démarrage **Mode de réparation des services d'annuaire**



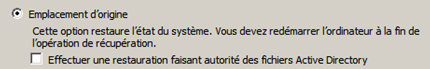
1. il faut s'identifier en utilisant le compte local de la SAM identifié comme **administrateur restauration service d'annuaire**   
   Ce compte est différent de celui de l’administrateur de Domaine, il a été saisie lors du DCPROMO qui a créer le serveur CD…
2. dans l'utilitaire de sauvegarde demander obligatoirement de **Restaurer l'état du système**
3. Redémarrer le serveur

## Exécuter une restauration forcée totale :

Si on a un plusieurs CD de domaine, c'est l'opération à faire pour être sur du contenu de AD après la sauvegarde.

**N.B:** La restauration forcée ne fonctionne pas pour les modifications qui aurait été faites sur le schéma d'annuaire. On ne peut donc pas annuler des modification sur le schéma par cette technique.

Il faut suivre le mode opératoire suivant :

1. redémarrer l'ordinateur, **F8** (ou **MAJ+Arrêt**) et sélectionner l'option de démarrage **Mode restauration des services d'annuaire**
2. il faut s'identifier en utilisant le compte local de la SAM identifié comme **administrateur restauration service d'annuaire**
3. dans l'utilitaire de sauvegarde demander obligatoirement de **Restaurer l'état du système et cocher Effectuer une restauration faisant autorité des fichiers Active Directory   
    **ne
4. Redémarrer le serveur

## PB mot de passe Restauration :

Il est possible de changer le mot de passe stocké en **SAM** pour la **restauration des Service d'Annuaire**. La commande à lancer est **ntdsutil**….

**ntdsutil**

**set dsrm password**

**reset password on server null**

…(entrer 2 fois le nouveau mot de passe)

**Q** …

suivit de **Q**