

Administration Windows Server 2016

Hainaut Patrick 2017

But de cette présentation

- Microsoft est un acteur incontournable dans le domaine des OS réseaux
- Nous nous intéressons ici à la version 2016 de Windows Server
- Dans cette présentation est regroupé la mise en place des services de base tel que serveur DHCP, DNS, NAT, Web, Contrôleur de domaine, ...

Introduction

Historique

- En 1993, Microsoft sort Windows NT 3.1 disponible en version Workstation et Server
- NT 4.0 sort en 1996 et est une version très populaire
- Windows 2000 Server sort en 2000 et introduit l'active directory
- Windows 2003 Server sort en 2003 et améliore l'Active Directory
- Ensuite viennent Windows Server 2008, 2012, et enfin 2016

Nouveautés: 1 Hyper-V

- Windows Server 2016 met plus que jamais l'accent sur la virtualisation en incorporant une nouvelle version d'Hyper-V, son hyperviseur maison, livré en standard.
 - Protection des ressources: une limitation d'utilisation des ressources peut être activée pour éviter qu'une machine virtuelle utilise trop de ressources et dégrade les performances de la machine hôte et des autres VM
 - Nested Virtualization (virtualisation imbriquée): permet d'utiliser Hyper-V dans une machine virtuelle exécutant Windows server 2016 et créer ainsi des machines virtuelles dans la machine virtuelle
 - Priorité de redémarrage des VM: permet de redémarrer les VM les plus importantes en premier
 - Storage QOS: possibilité d'appliquer des règles QOS sur les disques virtuels
 - Ajout/suppression de cartes réseau et mémoire à chaud: évite d'interrompre les services

©Hainaut P. 2017 - www.coursonline.be

5

Nouveautés: 2 Windows defender

- Windows Defender pour serveur est installé par défaut et protège le serveur directement après son installation
- Il est bien sûr possible de remplacer cette protection par un autre produit

©Hainaut P. 2017 - www.coursonline.be

6

Nouveautés: 3 nano server

- En installation standard, Windows 2016 consomme pas mal de ressources
- Cette option d'installation permet d'installer un serveur basique (serveur DNS, serveur WEB, hôte Hyper-V, ...) sur 500Mb de disque dur et avec des mises à jour moins fréquentes

Nouveautés: 4 Containers

- Microsoft ne pouvait pas passer à coté de la technologie des conteneurs qui constitue une nouveauté essentielle de 2016
- Il est possible d'utiliser des conteneurs compatibles docker ou Hyper-V
- Le déploiement d'environnement de test, de développement ou même de production se fait plus facilement et rapidement

Nouveautés: 5 Azure stack

- Azure, c'est le service cloud Microsoft
- Azure stack permet d'installer un cloud Azure au sein de son datacenter
- C'est un système de cloud hybride qui travaille indépendamment du cloud public Azure et du cloud privé sur le réseau local mais qui peut échanger des données avec les deux

©Hainaut P. 2017 - www.coursonline.be

9

Versions

- Standard, Datacenter et Essentials
- La version Essentials est réservée aux petites entreprises de maximum 25 personnes et 50 machines

fonctionnalité	Standard	Datacenter
Fonctionnalités principales de Windows Server	*	*
Environnements de syst. d'exploitation / conteneurs Hyper-V	2	illimité
Conteneurs Windows Server	illimité	illimité
Service Guardian hôte	*	*
Nano Server	*	*
Fcts de stockage (Storage Spaces Direct, Storage Replica, ...)		*
Machines virtuelles protégées		*

Prix

- Le prix dépend du nombre de cœurs présents dans le serveur
- A titre indicatif:
 - une licence Essentials coute 501\$
 - une licence Standard coute 882\$
 - une licence Datacenter coute 6155\$
- A cela, il faut ajouter les licences d'accès client (cal), à raison de 47€ par poste client (pour les versions Standard et Datacenter)

Planification

Choix d'une version

- Pour un serveur physique, on choisira la version standard sauf pour de très petites structures, où l'on prendra la version Essentials
- Si on virtualise beaucoup et si l'on recherche un serveur hautement disponible et performant, ayant des éléments de tolérances de panne supplémentaires, la version datacenter s'impose

Versions 32 ou 64 bits

- La question n'est plus à se poser avec Windows 2016 Server !
- Il n'existe qu'en 64 bits ...

Types d'installations

- Choix entre une installation sans GUI (Core server) et une installation avec GUI (Desktop experience)
- Au niveau de la version Core server, la configuration et la maintenance sont effectuées au travers de l'interface de ligne de commande Windows, ou en se connectant à distance en utilisant une console de gestion Microsoft (*Microsoft Management Console*).
- Une machine Core Serveur peut être configurée pour plusieurs rôles de base : Contrôleur de Domaine / *Active Directory Domain Services*, serveur DHCP, serveur DNS, serveur de fichiers, serveur d'impression, serveur web IIS 7, serveur virtuel *Windows Server Virtualization*, ...
- Le reste de notre propos fait référence à la version avec GUI

Virtualisation

- Windows server 2016 peut être installé en tant que serveur virtuel ou en tant que serveur hôte, soit en utilisant les outils de virtualisation classiques, soit en utilisant le nouveau moteur de virtualisation Hyper-V
- La virtualisation est un choix d'entreprise, mais la tendance est de virtualiser un maximum

Avantages et inconvénients de la virtualisation

- La virtualisation permet de réunir sur un serveur physique, des serveurs virtuels dont les rôles respectifs exigent qu'ils soient placés sur des serveurs différents
- En outre, il est possible de déplacer facilement un serveur virtuel d'un serveur physique à un autre
- L'inconvénient est que si le serveur physique est arrêté, tous les serveurs virtuels sont le sont aussi mais généralement, un serveur physique de secours est configuré pour prendre la place du serveur défectueux

©Hainaut P. 2017 - www.coursonline.be

17

Configuration minimale requise

Processeur	x64
Nombre de processeurs minimal	1
Puissance minimale théorique	1,4 Ghz
Puissance minimale conseillée	2 Ghz
Mémoire minimale théorique	512 Mb
Mémoire minimale conseillée	2 Gb
Espace disque minimal théorique	32 Gb
Espace disque minimal conseillé	60 Gb

©Hainaut P. 2017 - www.coursonline.be

18

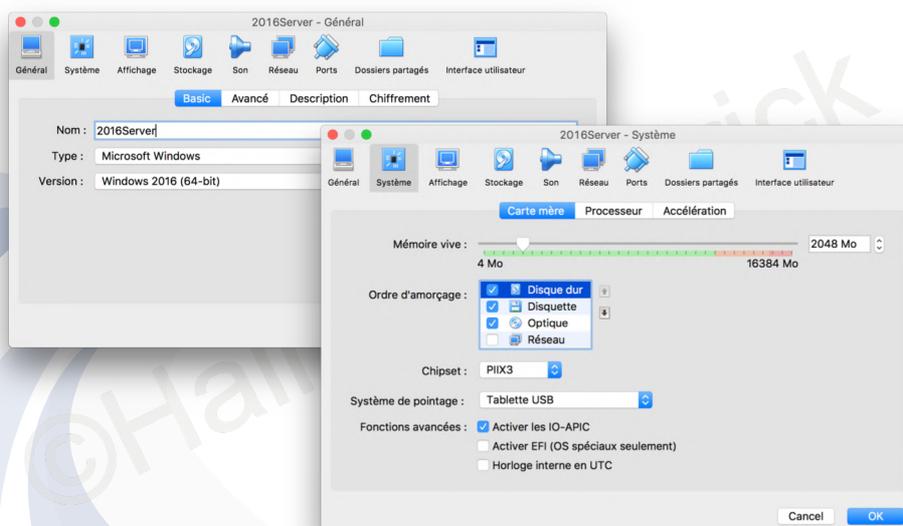
Bac à sable

- Sous VirtualBox, créez deux machines virtuelles Windows 2016 Server (AD1, AD2) avec:
 - 2 Gb de mémoire (1 Gb minimum)
 - 60 Gb de disque dur de taille variable
 - Une carte réseau en accès par pont
 - Une carte réseau en réseau interne
- Créez une machine virtuelle Windows 10 (CL10) avec:
 - 40 Gb de disque dur de taille variable
 - Une carte réseau en réseau interne

©Hainaut P. 2017 - www.coursonline.be

19

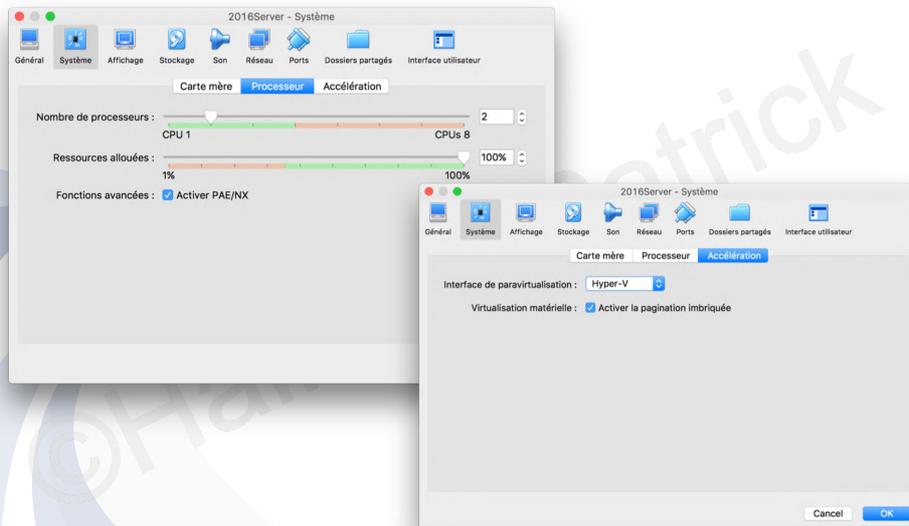
Bac à sable



©Hainaut P. 2017 - www.coursonline.be

20

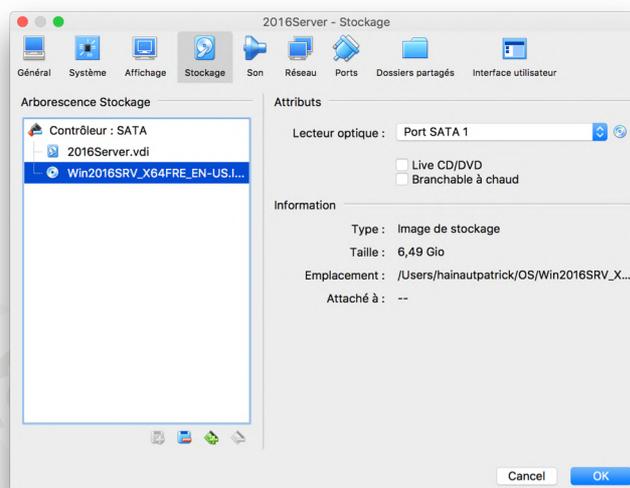
Bac à sable



©Hainaut P. 2017 - www.coursonline.be

21

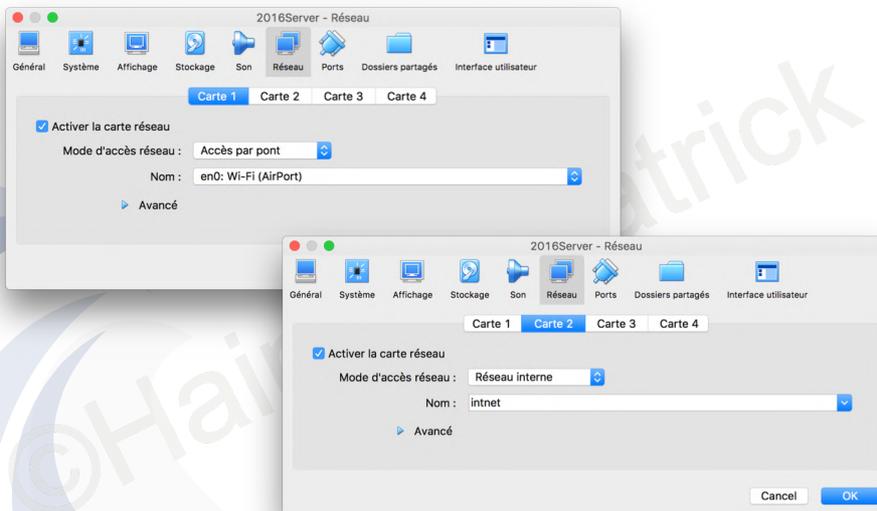
Bac à sable



©Hainaut P. 2017 - www.coursonline.be

22

Bac à sable

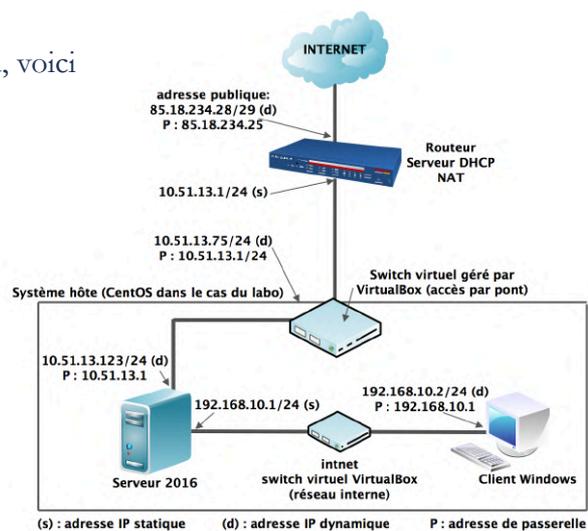


©Hainaut P. 2017 - www.coursonline.be

23

Bac à sable

- Au niveau du réseau, voici le scénario adopté:



©Hainaut P. 2017 - www.coursonline.be

24

Installation avec interface graphique

- 1. Sélection de la langue et du clavier

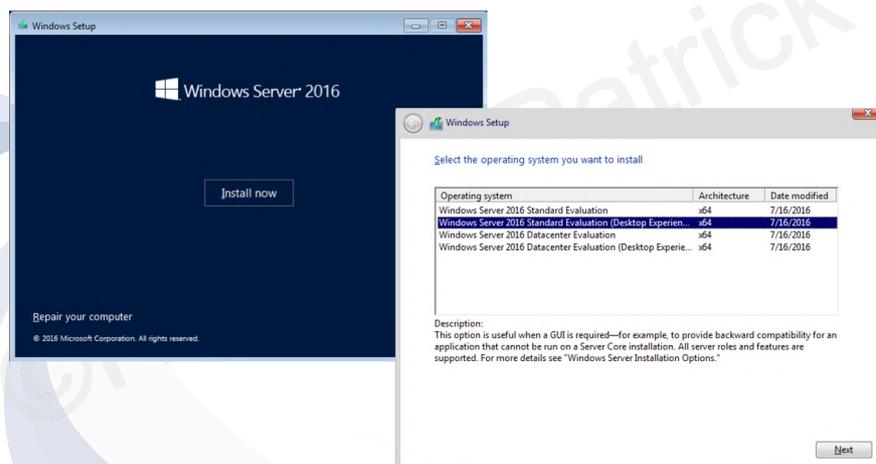


©Hainaut P. 2017 - www.coursonline.be

25

Installation avec interface graphique

- 2. Choix du type d'installation (Standard, Desktop Experience)

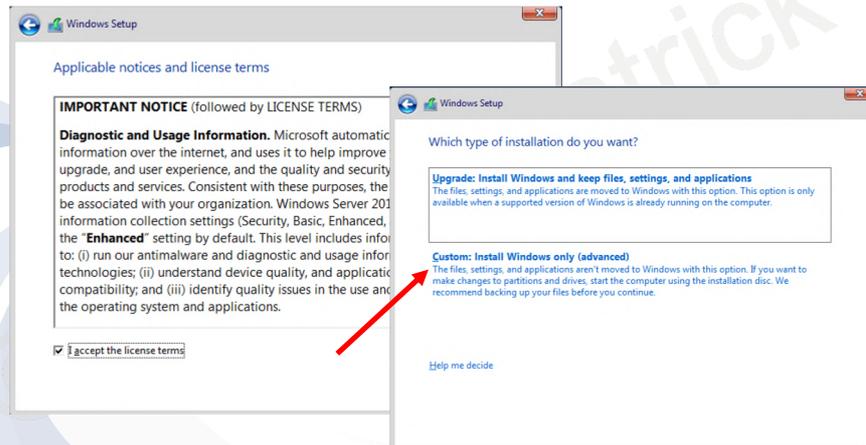


©Hainaut P. 2017 - www.coursonline.be

26

Installation avec interface graphique

- 3. Acceptation du contrat de licence et installation personnalisée

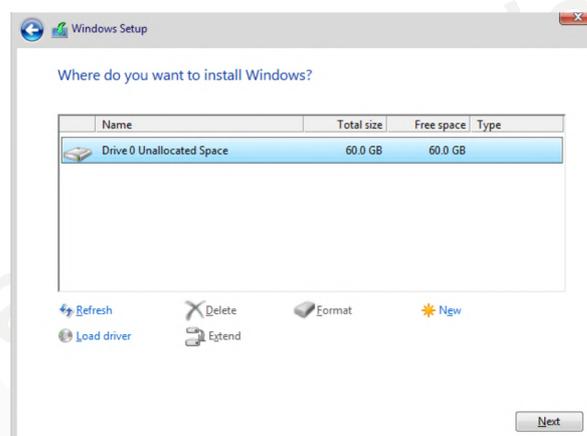


©Hainaut P. 2017 - www.coursonline.be

27

Installation avec interface graphique

- 4. Choix du disque, de la partition, ...



©Hainaut P. 2017 - www.coursonline.be

28

Installation avec interface graphique

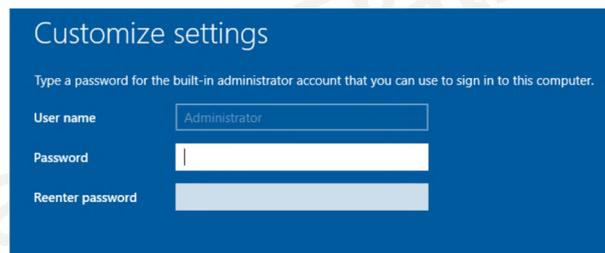
- 5. Copie des fichiers et installation de l'OS



1. Configuration initiale

Configuration initiale

- Attribution d'un mot de passe valide pour l'administrateur c'est à dire contenant des caractères appartenant à trois de ces quatre groupes (minuscules, majuscules, chiffres, caractères spéciaux) et d'une longueur d'au moins 6 caractères



Customize settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

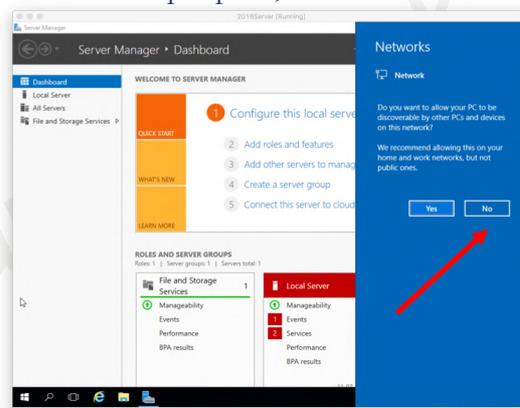
Password: []

Reenter password: []

- N'oubliez pas votre mot de passe d'un cours à l'autre

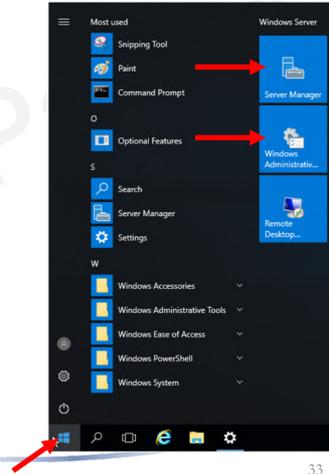
Configuration initiale

- La première carte réseau étant en accès par pont, Windows 2016 Server à accès à Internet automatiquement
- Il propose de découvrir les autres machines présentes sur le réseau
- Comme notre but est de créer un contrôleur de domaine et pas un réseau poste à poste, vous pouvez répondre "non"



Configuration initiale – nom du serveur

- La première chose à faire est de changer le nom de la machine attribué par défaut lors de l'installation
- Pour cela, allez dans le menu Windows, puis dans le *gestionnaire de serveur* (en passant par les *outils d'administration Windows* si celui-ci n'apparaît pas directement)

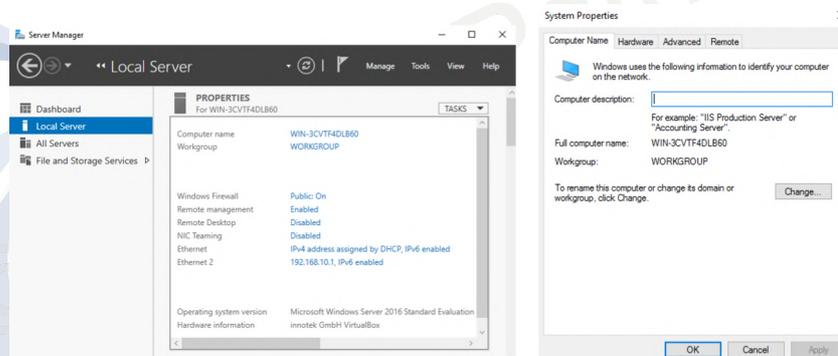


©Hainaut P. 2017 - www.coursonline.be

33

Configuration initiale – nom du serveur

- Cliquez sur l'onglet *Local Server*, puis sur le nom de l'ordinateur
- Dans la fenêtre qui s'ouvre, cliquez sur *Change ...*

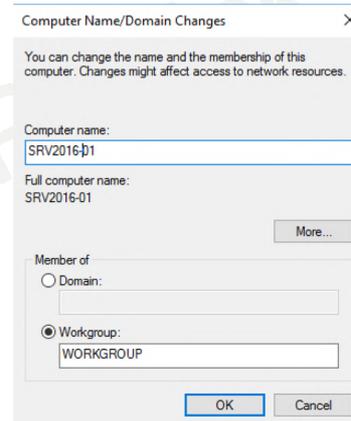


©Hainaut P. 2017 - www.coursonline.be

34

Configuration initiale – nom du serveur

- Dans la fenêtre qui s'ouvre, changez le nom de l'ordinateur
- Cliquez sur OK et puis redémarrer l'ordinateur pour prendre en compte les changements
- Remarque: on ne peut pas changer le nom de l'ordinateur et le groupe en même temps ...

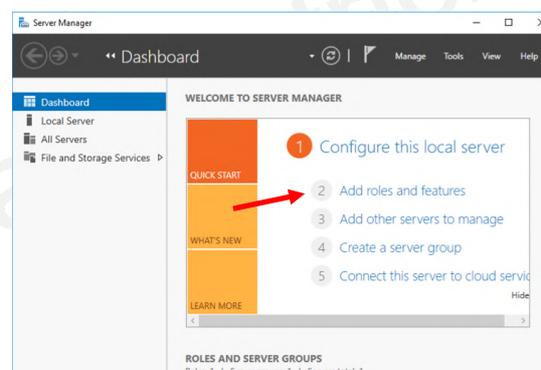


©Hainaut P. 2017 - www.coursonline.be

35

Configuration initiale – ajout de rôles

- Dans les manipulations qui vont suivre, vous devrez ajouter des rôles à votre serveur
- Pour cela, allez dans *le gestionnaire de serveur*, puis cliquez sur *ajouter des rôles*

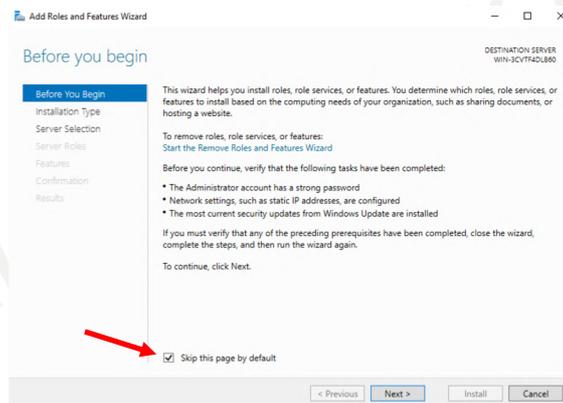


©Hainaut P. 2017 - www.coursonline.be

36

Configuration initiale – ajout de rôles

- Lisez l'avertissement et cliquez sur *suivant*

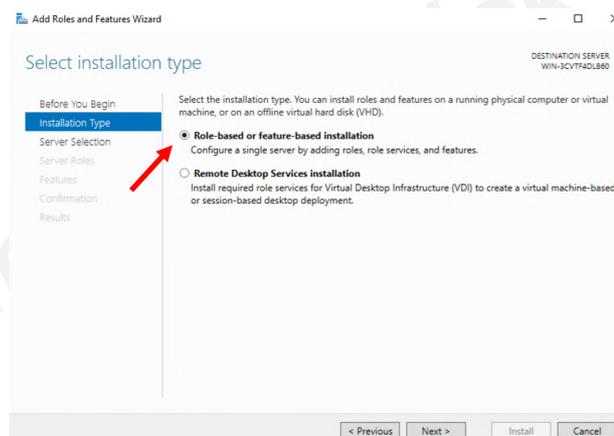


©Hainaut P. 2017 - www.coursonline.be

37

Configuration initiale – ajout de rôles

- Au niveau du type d'installation, comme on configure un serveur traditionnel, on choisit la première option

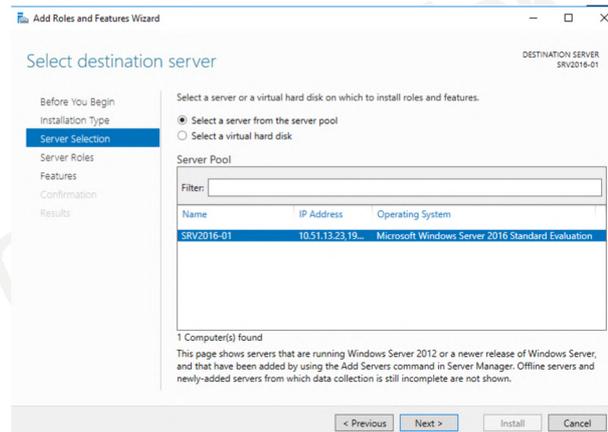


©Hainaut P. 2017 - www.coursonline.be

38

Configuration initiale – ajout de rôles

- On choisit notre serveur comme destination

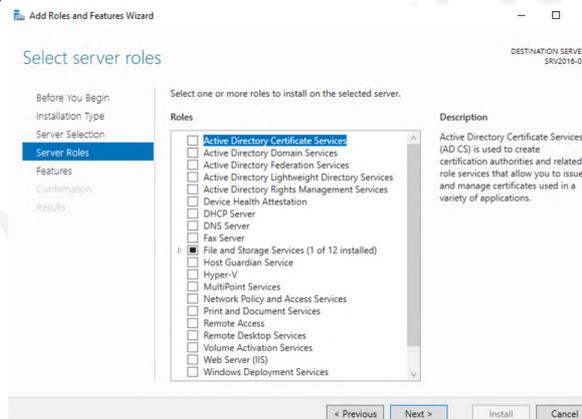


©Hainaut P. 2017 - www.coursonline.be

39

Configuration initiale – ajout de rôles

- On peut ensuite installer le ou les rôles désirés (voir plus loin dans la présentation)



©Hainaut P. 2017 - www.coursonline.be

40

2. Configuration de base des services réseau

Configuration de la carte réseau

- Examinons la configuration des cartes réseau après installation
- Cliquez sur *Rechercher* et tapez *cmd* pour accéder à l'invite de commande
- Entrez la commande *ipconfig*

```
Administrator: Command Prompt  
C:\Users\Administrator>ipconfig
```



Configuration de la carte réseau

- Les seules cartes qui nous intéressent sont les cartes *Ethernet* et *Ethernet 2*
- La carte *Ethernet* doit recevoir ses paramètres du DHCP comme c'est la cas sur la capture d'écran
- La carte *Ethernet 2* reçoit des paramètres d'auto-configuration qui ne nous conviennent pas
- C'est elle que nous allons configurer

```
Windows IP Configuration

Ethernet adapter Ethernet:

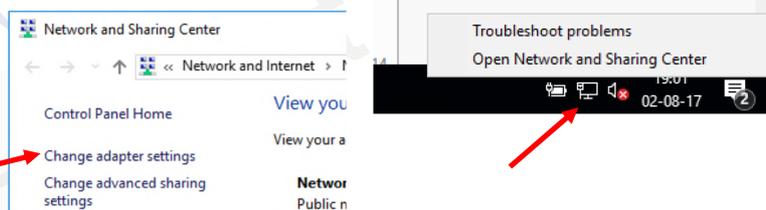
Connection-specific DNS Suffix . . . : 
Link-local IPv6 Address . . . . . : fe80::b40d:5301:c4f0:fc60%4
IPv4 Address. . . . . : 10.51.13.23
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.51.13.1

Ethernet adapter Ethernet 2:

Connection-specific DNS Suffix . . . : 
Link-local IPv6 Address . . . . . : fe80::414d:ba51:e256:26bb%2
Autoconfiguration IPv4 Address. . . : 169.254.38.187
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

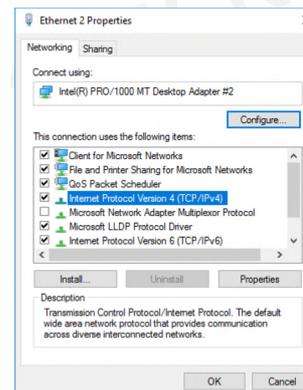
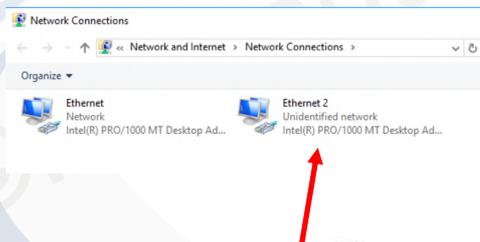
Configuration de la carte réseau

- Cette carte doit être configurée avec des paramètres statiques, elle constituera la passerelle pour les hôtes du réseau local
- Passez par le *Centre réseau et partage* puis cliquez sur *Gérer les connexions réseaux*



Configuration de la carte réseau

- Cliquez avec le bouton droit sur *Ethernet 2* pour accéder au menu contextuel et cliquez sur *Propriétés*
- Cliquez sur *Internet Protocol Version 4*



©Hainaut P. 2017 - www.coursonline.be

45

Configuration de la carte réseau

- Renseignez des paramètres statiques et validez
- Attention ! Pas de passerelle !
- Il y a une seule passerelle par équipement et elle est sur l'autre carte

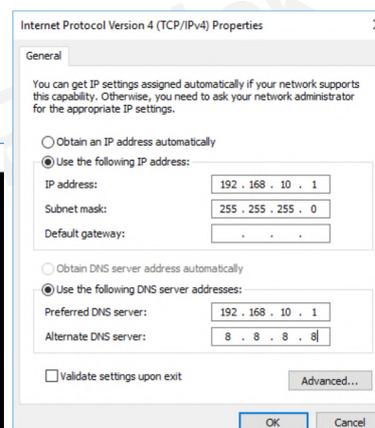
```
Administrator: Command Prompt
Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::b40d:5301:c4f0:fc60%4
    IPv4 Address. . . . . : 10.51.13.23
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.51.13.1

Ethernet adapter Ethernet 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::414d:ba51:e256:26bb%2
    IPv4 Address. . . . . : 192.168.10.1
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :
```



©Hainaut P. 2017 - www.coursonline.be

46

Configuration de la carte réseau

Remarques

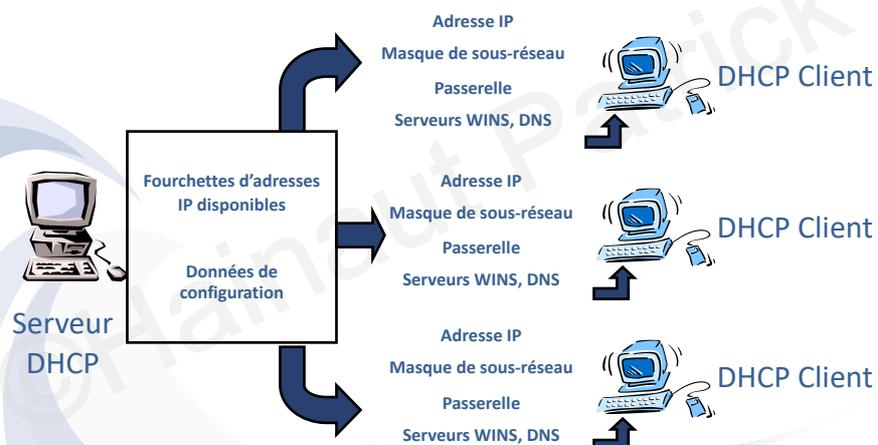
- L'adresse choisie sera la passerelle des PC clients et déterminera la plage dans laquelle travaillera le serveur DHCP de 2016
Ex: 192.168.10.1/24
- On évitera la plage 169.254, réservée traditionnellement aux clients DHCP n'ayant pas obtenu d'adresse IP
- On se placera dans un réseau différent de celui configuré sur la carte *Ethernet*

3. Installation et configuration d'un serveur DHCP

Introduction

- DHCP est un protocole client/serveur qui permet de centraliser et d'automatiser la configuration des données TCP/IP et d'affecter dynamiquement les adresses IP
- En plus de l'adresse IP, il est possible de télécharger sur le client DHCP plus de 50 paramètres supplémentaires, en particulier:
 - Le masque de sous-réseau
 - La passerelle par défaut
 - Les serveurs DNS

Introduction



Introduction

- On parle d'adresse dynamique pour un client DHCP et d'adresse statique pour une configuration manuelle. Les deux peuvent coexister
- Les avantages du DHCP sont:
 - Le gain de productivité par l'absence de configuration manuelle
 - Une modification éventuelle du système d'adresse est grandement simplifiée
 - Les erreurs de configuration sont impossibles en production
 - Il est possible de réserver une adresse pour un client afin qu'il utilise toujours la même

Processus d'acquisition d'une adresse IPv4

- Lorsque l'hôte se connecte sur un réseau, il envoie un message de diffusion appelé DHCPDISCOVER du port UDP 68 vers le port UDP 67 pour demander une IP
- Tout serveur DHCP recevant le message DHCPDISCOVER doit traiter cette requête
- Le serveur propose une adresse au client via un message de diffusion DHCPOFFER depuis le port UDP 67 vers le port UDP 68

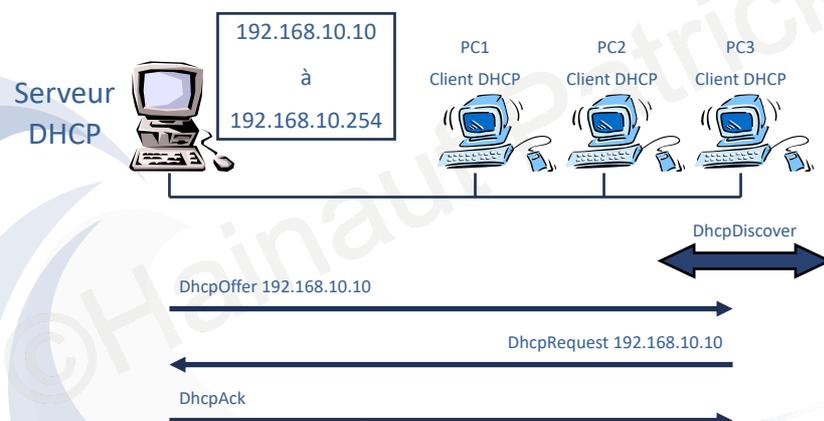
Processus d'acquisition d'une adresse IPv4

- Le client retourne un message de diffusion DHCPREQUEST afin de lui dire qu'il veut utiliser cette adresse
- Le serveur répond par un message DHCPACK, ce qui permet au client d'utiliser l'adresse IP pendant la durée du bail

©Hainaut P. 2017 - www.coursonline.be

53

Processus d'acquisition d'une adresse IPv4



©Hainaut P. 2017 - www.coursonline.be

54

Processus d'acquisition d'une adresse IPv4

- Le bail définit la durée d'utilisation de l'adresse IP par l'ordinateur client
 - La valeur par défaut est de 3 jours
- A 50% de la durée du bail, le client DHCP essaie automatiquement de renouveler le bail
 - Par un paquet DhcpRequest
- Si ce n'est pas possible, il réessaie à 87,5% de la durée du bail, et si cela ne fonctionne pas l'adresse IP est libérée à l'expiration et le client DHCP doit recommencer le processus complet
- Le renouvellement du bail (DHCPREQUEST et DHCPACK) se fait par messages unicast

©Hainaut P. 2017 - www.coursonline.be

55

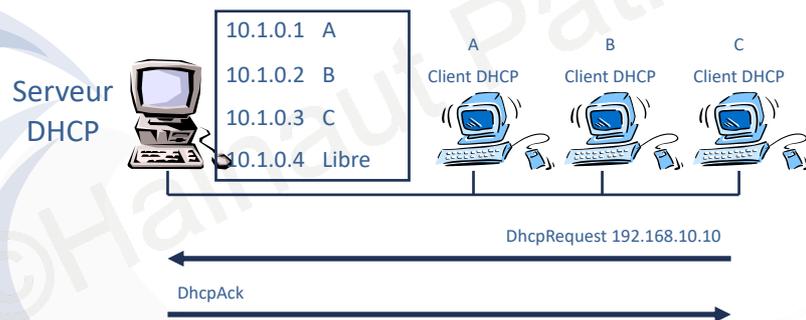
Processus d'acquisition d'une adresse IPv4

- Lors d'un redémarrage, le client envoie directement un message DHCPREQUEST
- Si l'adresse est toujours disponible, le serveur DHCP répond par un message DHCPACK
- Si pas, il répond par un message DHCPNACK et le client doit recommencer entièrement le processus d'acquisition

©Hainaut P. 2017 - www.coursonline.be

56

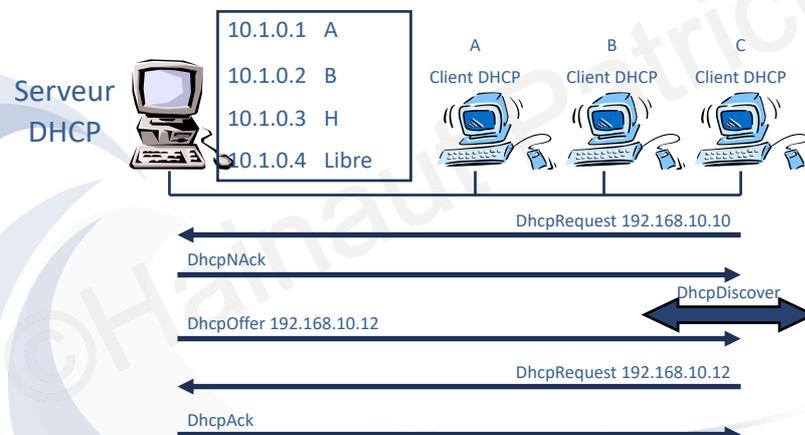
Processus d'acquisition d'une adresse IPv4



©Hainaut P. 2017 - www.coursonline.be

57

Processus d'acquisition d'une adresse IPv4



©Hainaut P. 2017 - www.coursonline.be

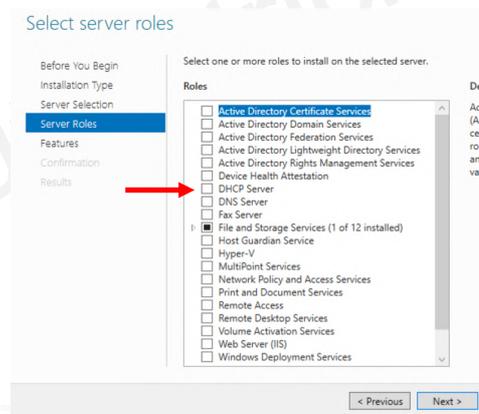
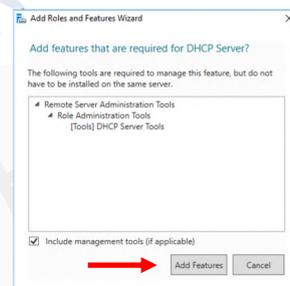
58

Pré-requis pour l'installation

- Le serveur doit disposer d'une adresse IP
- Cette adresse devrait être statique sinon les clients ne sauront pas renouveler leur bail

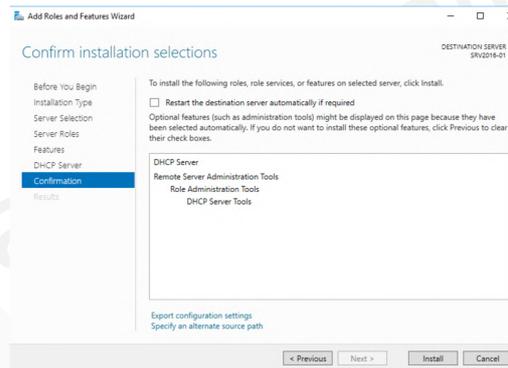
Installation du serveur DHCP

- Connectez-vous en tant qu'administrateur
- Dans le Gestionnaire de serveur, ajoutez le rôle de serveur DHCP
- Ajouter les fonctionnalités requises



Installation du serveur DHCP

- Vous pouvez cliquer sur Next au niveau des deux fenêtres suivantes
- Dans la fenêtre affichée, il vous reste à cliquer sur Install

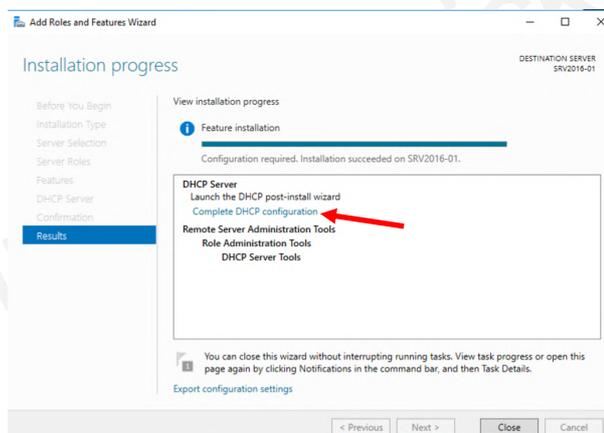


©Hainaut P. 2017 - www.coursonline.be

61

Installation du serveur DHCP

- Une fois l'installation terminée, cliquez sur la configuration complète DHCP

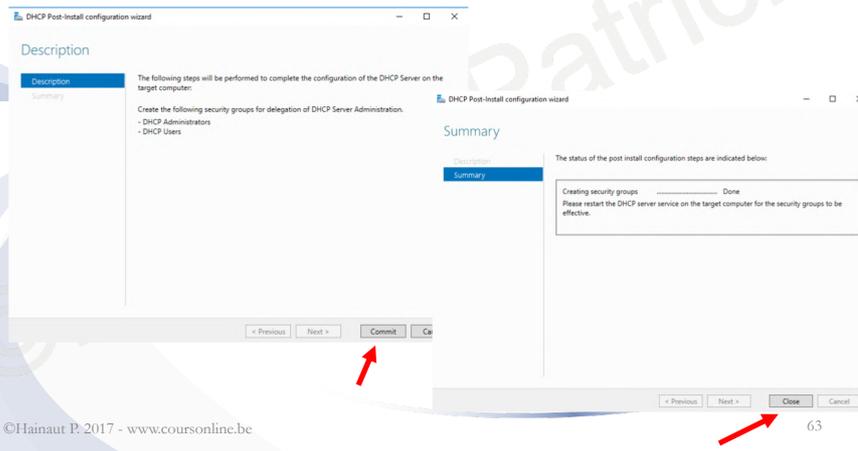


©Hainaut P. 2017 - www.coursonline.be

62

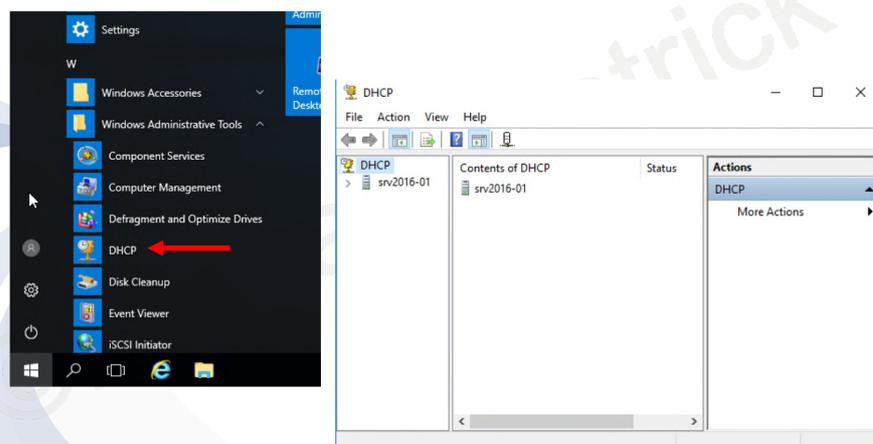
Installation du serveur DHCP

- Le système doit créer deux groupes de sécurité
- Validez et fermez la fenêtre



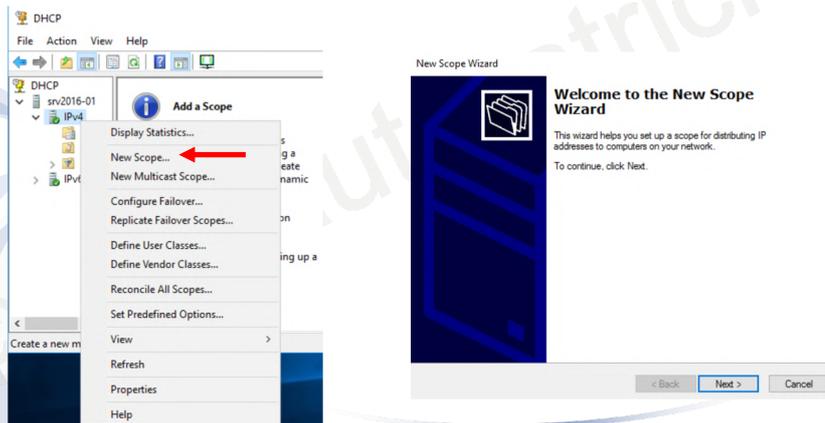
Installation du serveur DHCP

- Dans les outils d'administration, cliquez sur DHCP



Installation du serveur DHCP

- Cliquez avec le bouton droit sur IPv4 et sélectionner Nouvelle étendue ...

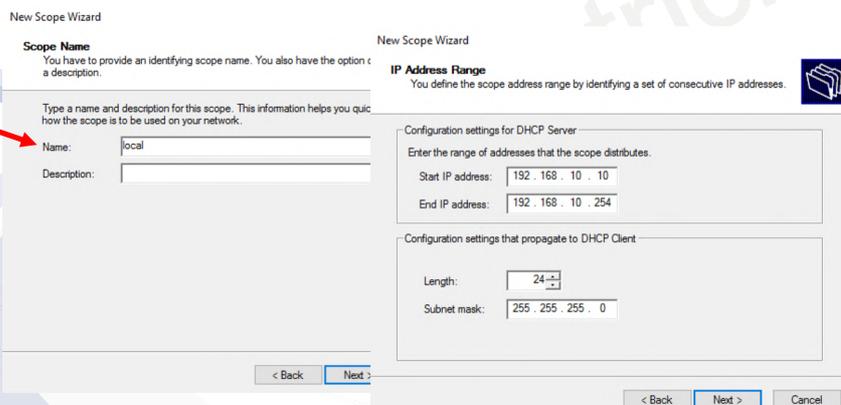


©Hainaut P. 2017 - www.coursonline.be

65

Installation du serveur DHCP

- Donnez un nom à l'étendue (peu importe) et définissez une étendue en accord avec l'adresse IP de la carte Ethernet 2



©Hainaut P. 2017 - www.coursonline.be

66

Installation du serveur DHCP

- Vous pouvez définir éventuellement une plage d'exclusion (plage d'adresses IP à l'intérieur de la plage DHCP mais qui ne seront pas distribuées par le serveur)

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address:

Excluded address range:

Subnet delay in milli second:

< Back

©Hainaut P. 2017 - www.coursonline.be

67

Installation du serveur DHCP

- Le bail par défaut pour un réseau local est de 8 jours
- Vous pouvez laisser la valeur par défaut

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back

©Hainaut P. 2017 - www.coursonline.be

68

Installation du serveur DHCP

- Il est important de configurer les options suivantes du serveur DHCP: - adresse de passerelle pour les clients
- adresse du serveur DNS pour les clients

New Scope Wizard

Configure DHCP Options
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

Yes, I want to configure these options now

No, I will configure these options later

< Back Next > Cancel

New Scope Wizard

Router (Default Gateway)
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.

IP address:
192.168.10.1 Add

Remove

Up

Down

< Back Next > Cancel

©Hainaut P. 2017 - www.coursonline.be

69

Installation du serveur DHCP

- Au niveau DNS, indiquez déjà le nom du domaine qui sera configuré et vérifiez que l'adresse IP de la carte Ethernet 2 fait bien partie des adresses de serveurs DNS

New Scope Wizard

Domain Name and DNS Servers
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain: atc.lan

To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

Server name: IP address:

Resolve

109.88.203.3
62.197.111.140
192.168.10.1
8.8.8.8

Add

Remove

Up

Down

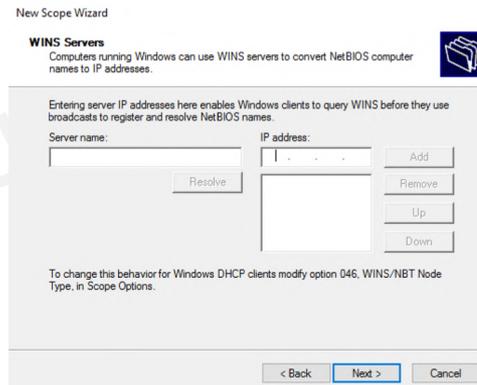
< Back Next > Cancel

©Hainaut P. 2017 - www.coursonline.be

70

Installation du serveur DHCP

- Le serveur WINS est un serveur de nom NetBIOS qui est remplacé avantageusement par le serveur DNS (sauf si vous utilisez des applications qui travaillent avec NetBIOS)
- On ne configurera pas de serveur WINS, vous pouvez donc cliquer directement sur Suivant

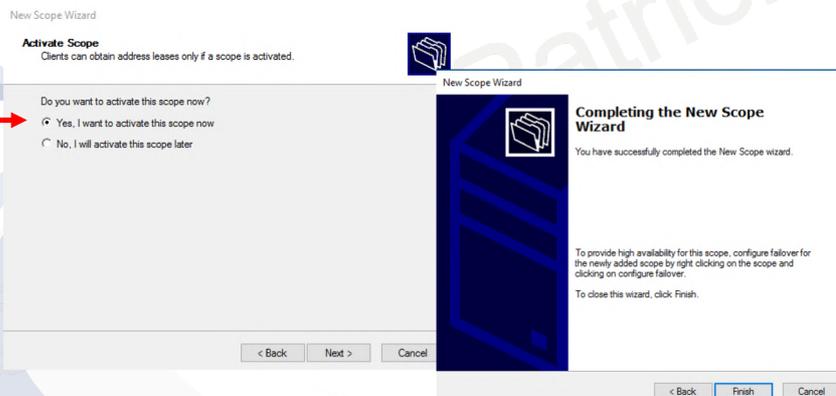


©Hainaut P. 2017 - www.coursonline.be

71

Installation du serveur DHCP

- On active l'étendue immédiatement et on clôture la configuration du serveur DHCP



©Hainaut P. 2017 - www.coursonline.be

72

Test sur le PC Client

- Le PC client connecté à votre serveur 2016 devrait maintenant recevoir ses paramètres IP du serveur ...
- Un **ipconfig/release** suivi d'un **ipconfig/renew** est sans doute nécessaire ...
- Faites un **ipconfig/all** pour vérifier que serveur DNS et passerelle sont bien présents -> sinon, retournez au niveau du serveur DHCP, pour activer les **options de serveur** nécessaires (serveur de noms et routeur)
- Attention, le PC client n'a pas encore d'accès Internet

©Hainaut P. 2017 - www.coursonline.be

73

Test sur le PC Client

- Le résultat en image

```
C:\Windows\system32\cmd.exe
Ethernet adapter Local Area Connection:

Connection-specific DNS Suffix . . . : atc.lan
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-59-2F-E8
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::7d9e:ch4f:f9d:a096%10(Preferred)
IPv4 Address. . . . . : 192.168.10.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : jeudi 3 août 2017 07:59:19
Lease Expires . . . . . : vendredi 11 août 2017 07:59:19
Default Gateway . . . . . : 192.168.10.1
DHCP Server . . . . . : 192.168.10.1
DHCPv6 IAID . . . . . : 235405351
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-09-FC-9D-08-00-27-59-2F-E8

DNS Servers . . . . . : 109.88.203.3
                       62.197.111.140
                       192.168.10.1
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter isatan.atc.lan:
```

©Hainaut P. 2017 - www.coursonline.be

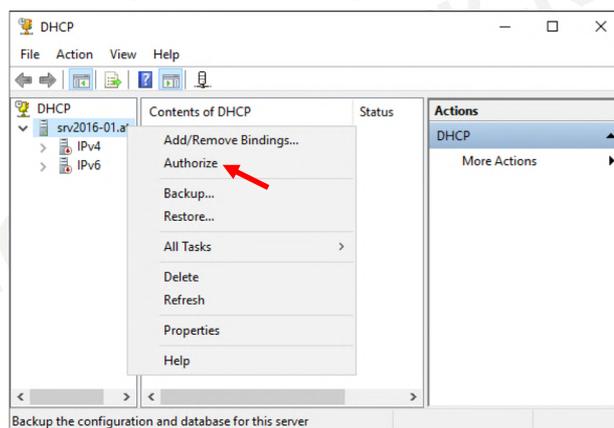
74

Autorisation du serveur DHCP

- La première fois qu'on redémarre le 2016, il faut généralement autoriser le serveur DHCP qui ne fonctionne plus

- Retournez dans la gestion du DHCP, cliquez avec le bouton droit de la souris pour accéder au menu

- Cliquez sur *Autoriser*



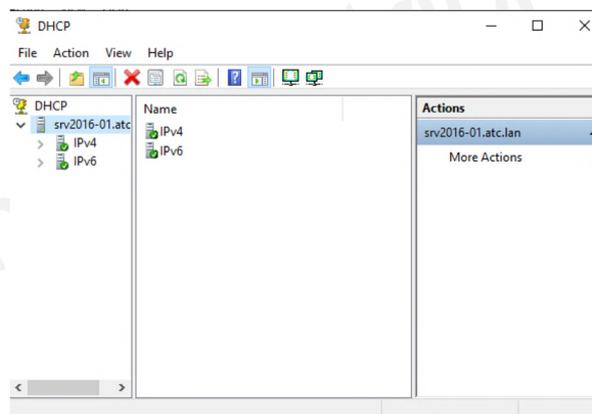
©Hainaut P. 2017 - www.coursonline.be

75

Autorisation du serveur DHCP

- Les indicateurs sont passés au vert, tout est ok

- L'opération est à faire une seule fois



©Hainaut P. 2017 - www.coursonline.be

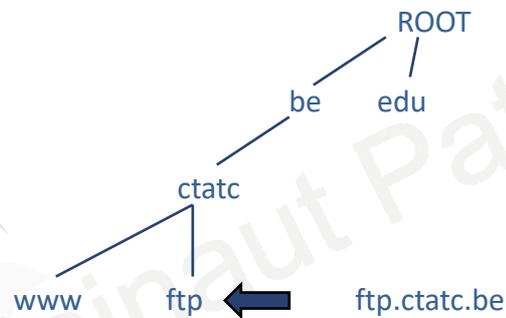
76

4. Installation et configuration d'un serveur DNS

Introduction

- Le système DNS (Domain Name System) utilise un espace de noms
- La racine internet de cet espace de noms est root, représentée par un point, sous laquelle on trouve les domaines de premier niveau comme be, com, net, ...
- Un serveur DNS peut être utilisé pour effectuer la résolution des noms
 - Un serveur DNS contient des mappages nom de domaine à adresse IP

Introduction



©Hainaut P. 2017 - www.coursonline.be

79

Introduction

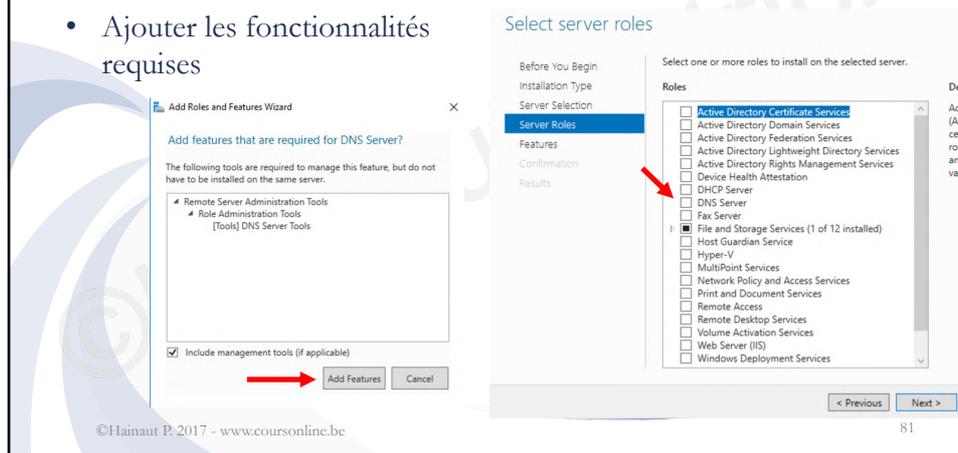
- On appelle FQDN (Fully Qualified Domain Name) un nom complet identifiant la ressource puis ses parents jusqu'à la racine
- Chaque point est un niveau de séparation hiérarchique
- Exemple: www.ctatc.be
 - . représente la racine (non visible)
 - be représente le nom de domaine de 1^{er} niveau
 - ctatc celui de 2^{ème} niveau
 - www représente un type d'enregistrement dans la zone

©Hainaut P. 2017 - www.coursonline.be

80

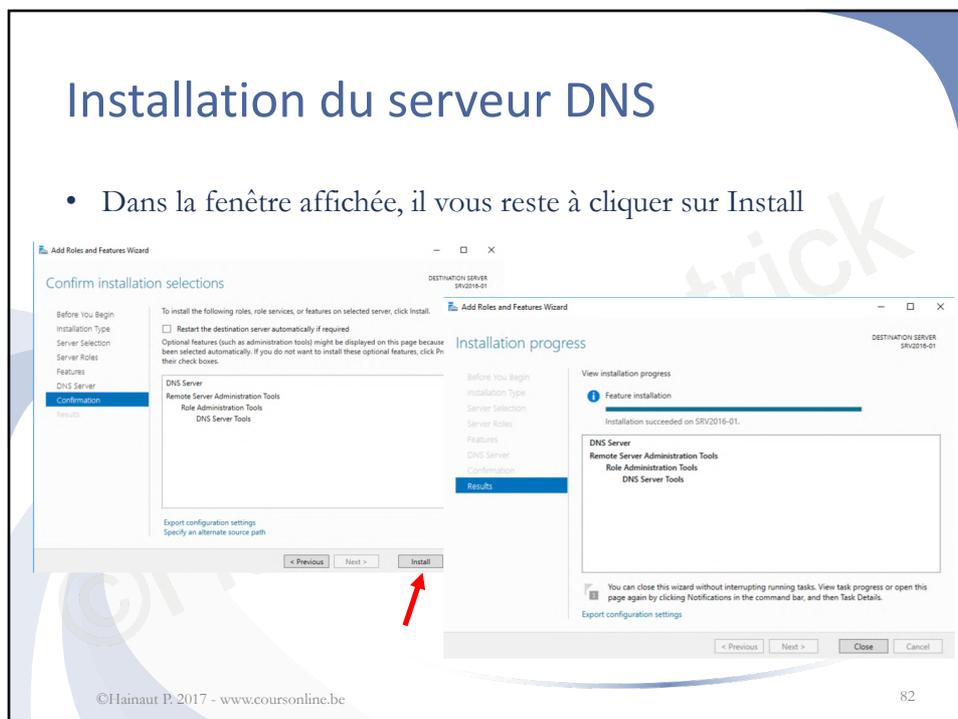
Installation du serveur DNS

- Connectez-vous en tant qu'administrateur
- Dans le Gestionnaire de serveur, ajoutez le rôle de serveur DNS
- Ajouter les fonctionnalités requises



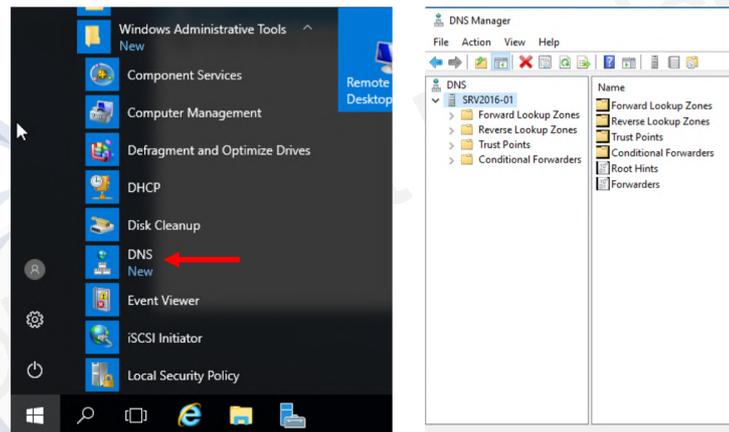
Installation du serveur DNS

- Dans la fenêtre affichée, il vous reste à cliquer sur Install



Installation du serveur DNS

- Dans les outils d'administration, cliquez sur DNS

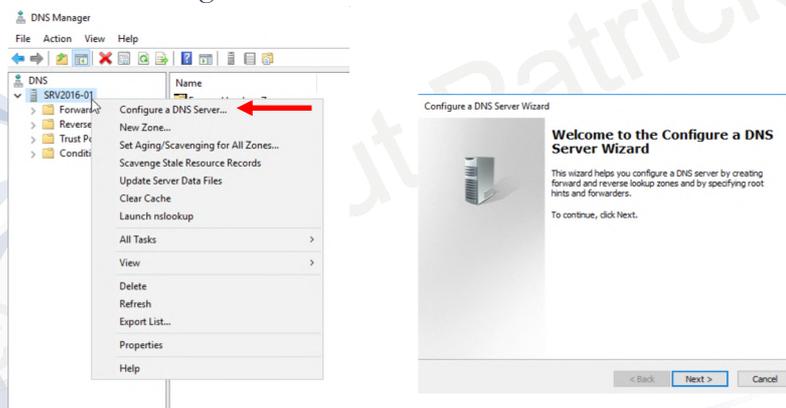


©Hainaut P. 2017 - www.coursonline.be

83

Installation du serveur DNS

- Cliquez avec le bouton droit sur le nom du serveur DNS et choisissez "Configurer un serveur DNS"

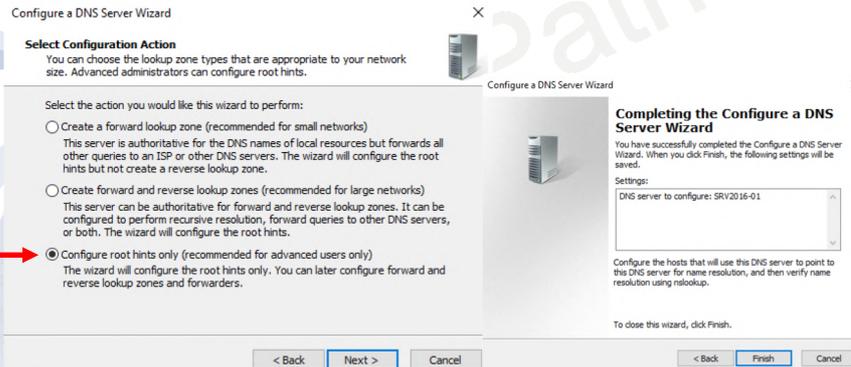


©Hainaut P. 2017 - www.coursonline.be

84

Installation du serveur DNS

- Sur la page Sélectionnez une action de configuration, sélectionnez Configurer les indications de racine uniquement, Suivant et puis Terminer

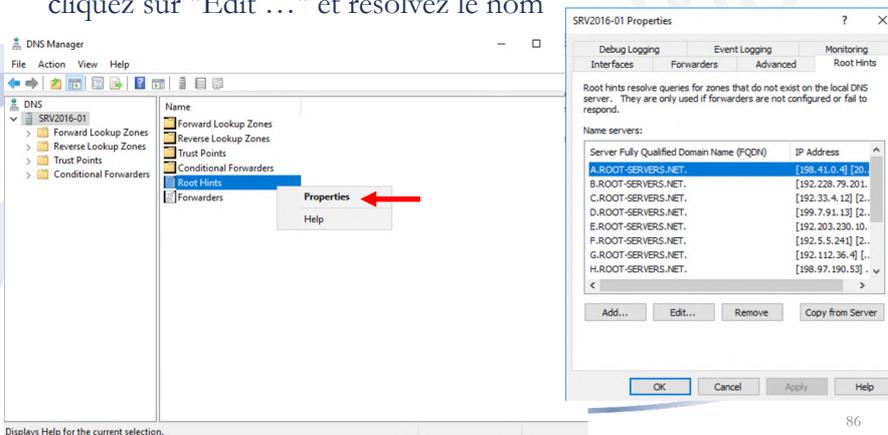


©Hainaut P. 2017 - www.coursonline.be

85

Installation du serveur DNS

- Cliquez avec le bouton droit sur "Serveurs racines", puis "Propriétés" et vérifiez que certains serveurs ont une adresse IP associée, sinon, cliquez sur "Edit ..." et résolvez le nom



86

Installation du serveur DNS

- Cette configuration basique permettra aux postes clients de résoudre les noms de domaines internet
- Nous verrons une configuration avancée du serveur DNS lorsque nous configurerons un serveur WEB

5. Installation et configuration du NAT

Routage et accès distant

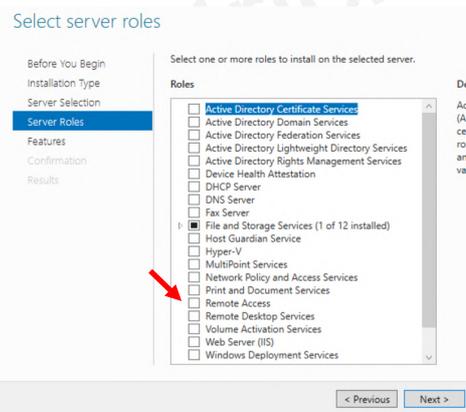
- Les rôles Serveur DHCP et DNS étant installé, il faut permettre à nos clients d'accéder à Internet automatiquement
- Nous allons pour cela ajouter le service de routage et d'accès distant

©Hainaut P. 2017 - www.coursonline.be

89

Installation du service d'accès distant

- Connectez-vous en tant qu'administrateur
- Dans le Gestionnaire de serveur, ajoutez le rôle Accès distant

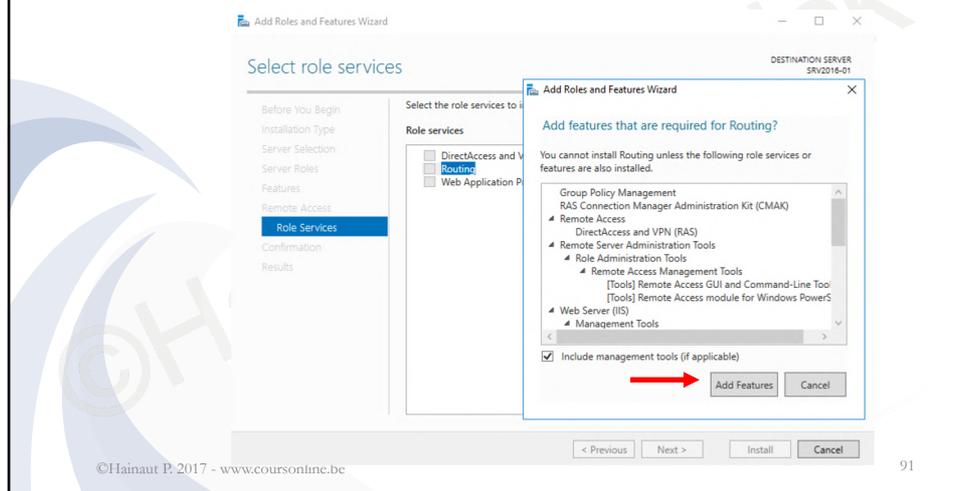


©Hainaut P. 2017 - www.coursonline.be

90

Installation du service d'accès distant

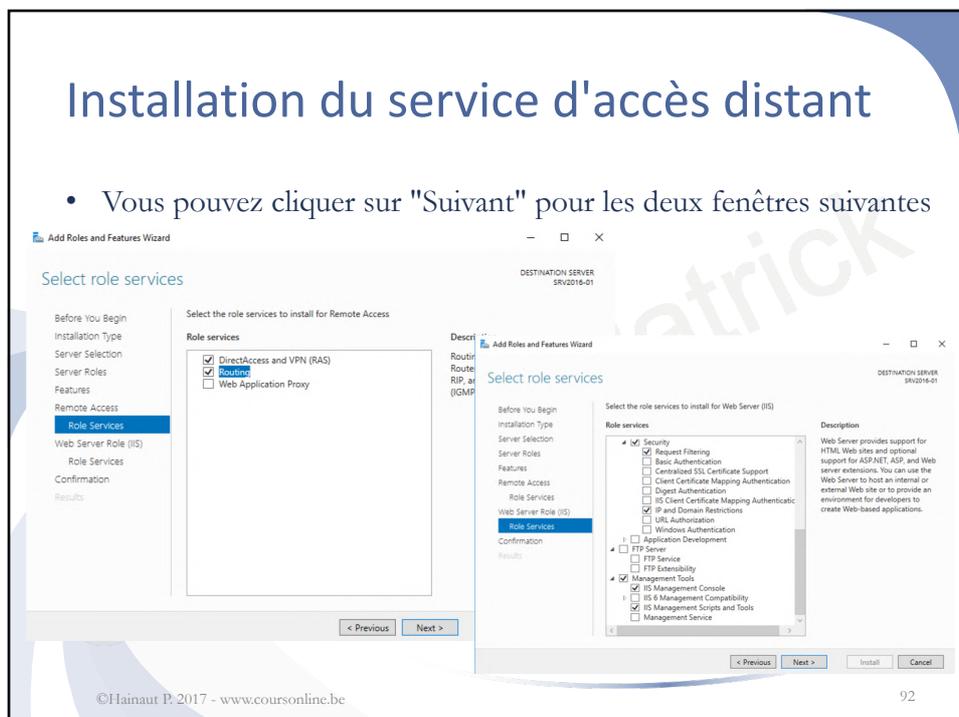
- Ajouter les fonctionnalités requises



91

Installation du service d'accès distant

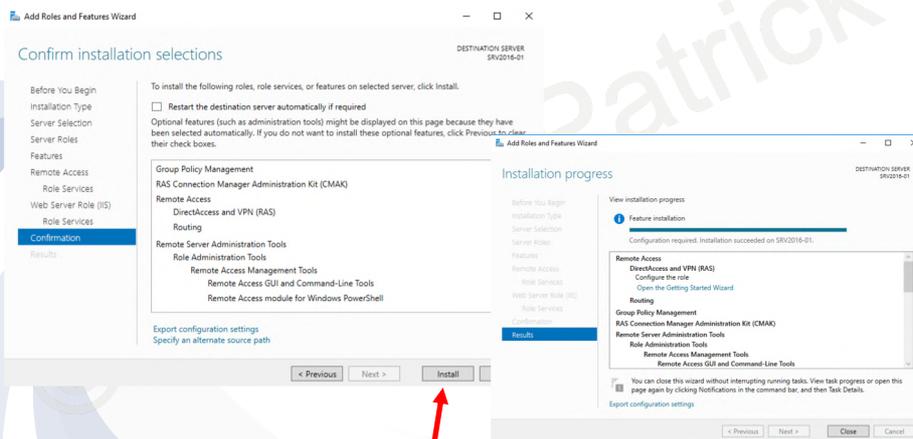
- Vous pouvez cliquer sur "Suivant" pour les deux fenêtres suivantes



92

Installation du service d'accès distant

- Et finalement, cliquer sur "Install" puis "Close"

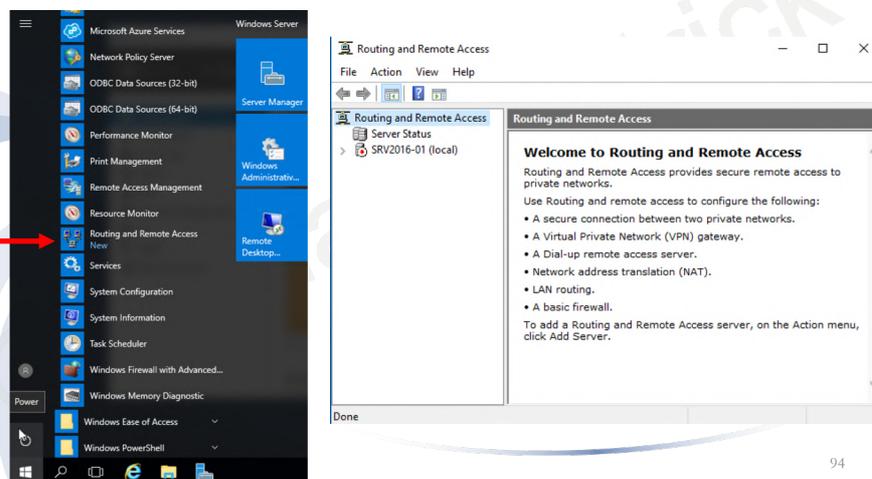


©Hainaut P. 2017 - www.coursonline.be

93

Installation du service d'accès distant

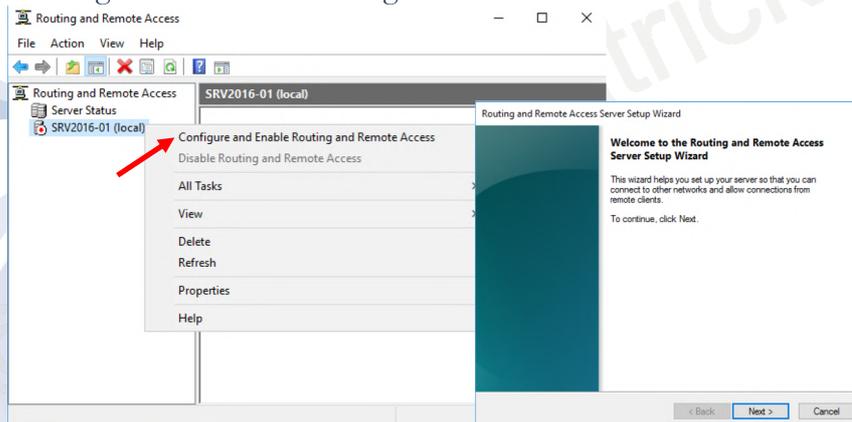
- Dans les outils d'administration, cliquez sur Routage et accès distant



94

Installation du service d'accès distant

- Cliquez avec le bouton droit sur le nom du serveur et choisissez "Configurer et activer le routage et l'accès distant"

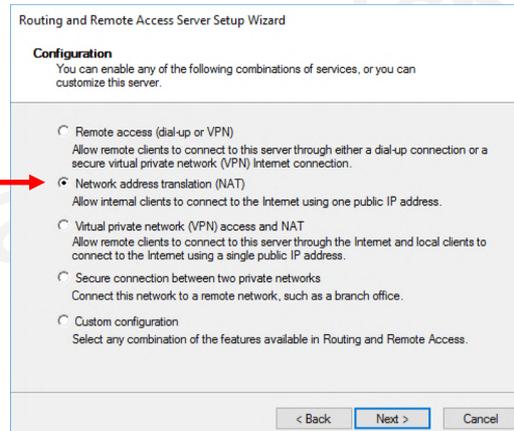


©Hainaut P. 2017 - www.coursonline.be

95

Installation du service d'accès distant

- Dans la fenêtre suivante, choisissez la fonctionnalité NAT



©Hainaut P. 2017 - www.coursonline.be

96

Installation du service d'accès distant

- Il faut sélectionner la carte réseau en accès par pont, si celle-ci est indisponible, cliquez sur Back et rafraichissez la liste

Routing and Remote Access Server Setup Wizard

NAT Internet Connection

You can select an existing interface or create a new demand-dial interface for client computers to connect to the Internet.

Use this public interface to connect to the Internet:

Network Interfaces:

Create a new demand-dial interface to the Internet

A demand-dial interface is activated when a client uses the Internet. Select option if this server connects with a modem or by using the Point-to-Point Protocol over Ethernet. The Demand-Dial Interface Wizard will start at the end of the wizard.

< Back Next >

Routing and Remote Access Server Status

Server Name	Server type	State
SRV2016-01	Windows Server 2016 Standard Evaluat...	Stopped

Refresh

©Hainaut P. 2017 - www.coursonline.be

97

Installation du service d'accès distant

- Choisissez la connexion vers Internet (Ethernet dans ce cas-ci)

Routing and Remote Access Server Setup Wizard

NAT Internet Connection

You can select an existing interface or create a new demand-dial interface for client computers to connect to the Internet.

Use this public interface to connect to the Internet:

Name	Description	IP Address
Ethernet	Intel(R) PRO/1000 MT...	10.51.13.23 (D...
Ethernet 2	Intel(R) PRO/1000 MT...	192.168.10.1

Create a new demand-dial interface to the Internet

A demand-dial interface is activated when a client uses the Internet. Select option if this server connects with a modem or by using the Point-to-Point Protocol over Ethernet. The Demand-Dial Interface Wizard will start at the end of the wizard.

< Back Next >

Completing the Routing and Remote Access Server Setup Wizard

You have successfully completed the Routing and Remote Access Server Setup wizard.

Summary:

Configured NAT for the following Internet interface Ethernet

NAT relies on external DNS and DHCP servers. Confirm that these services are configured properly.

Network Address Translation (NAT) cannot start when

To enable servers to respond to Internet requests, configure port mappings and update your firewall.

To close this wizard, click Finish.

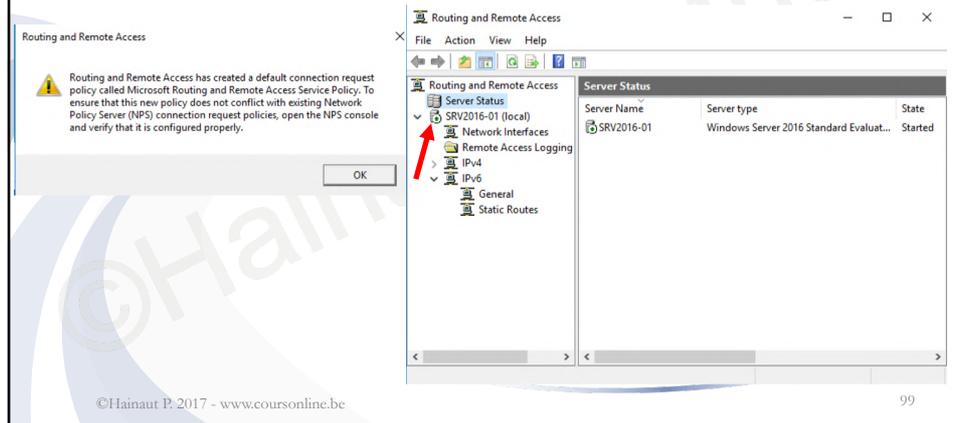
< Back Finish Cancel

©Hainaut P. 2017 - www.coursonline.be

98

Installation du service d'accès distant

- Cliquez sur "OK" au niveau du message d'avertissement et vérifiez que le service NAT fonctionne (macaron vert)



Installation du service d'accès distant

- Vérifiez sur le PC client que celui-ci à bien accès à Internet
- Si le ping vers 8.8.8.8 fonctionne, le NAT est bien installé
- Si le ping vers www.google.be fonctionne, c'est que le serveur DNS (qui sert ici de relais) est bien installé

```
C:\Windows\system32\cmd.exe
C:\Users\Admin>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=138ms TTL=42
Reply from 8.8.8.8: bytes=32 time=35ms TTL=42
Reply from 8.8.8.8: bytes=32 time=50ms TTL=42
Reply from 8.8.8.8: bytes=32 time=57ms TTL=42
Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 35ms, Maximum = 138ms, Average = 72ms
C:\Users\Admin>ping www.google.be
Pinging www.google.be [216.58.212.195] with 32 bytes of data:
Reply from 216.58.212.195: bytes=32 time=65ms TTL=51
Reply from 216.58.212.195: bytes=32 time=91ms TTL=51
Reply from 216.58.212.195: bytes=32 time=96ms TTL=51
Reply from 216.58.212.195: bytes=32 time=107ms TTL=51
Ping statistics for 216.58.212.195:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 65ms, Maximum = 107ms, Average = 89ms
C:\Users\Admin>
```

6. L'Active Directory

Présentation des services de l'AD

- L'active directory est un annuaire centralisé contenant des informations sur les utilisateurs, les ordinateurs, ...
- L'AD s'occupe également d'authentifier et d'autoriser l'accès aux ordinateurs et aux ressources d'un réseau Windows.

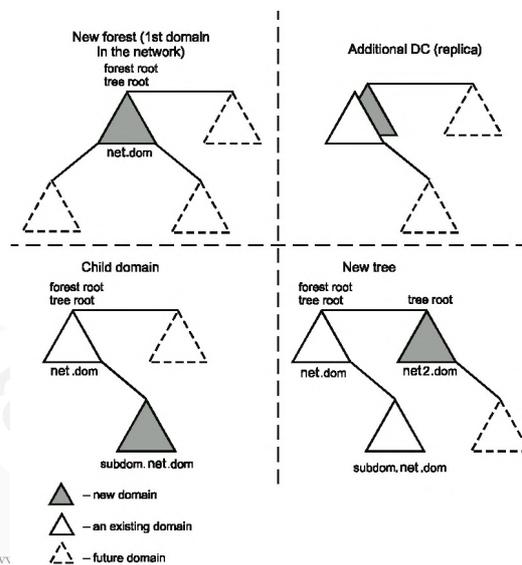
Présentation des services de l'AD

- L'AD implémente les protocoles suivants
 - LDAP(Lightweight Directory Access Protocol) pour les services d'annuaire
 - Kerberos v5 pour l'authentification
 - TCP/IP et DNS pour les services réseau

Organisation de l'AD

- La forêt
 - La forêt représente la frontière extérieure de l'AD de l'entreprise
 - Une forêt est composée d'une ou plusieurs arborescences ne partageant pas un même espace de noms.
- L'arborescence
 - C'est une organisation hiérarchique de domaines. Au départ, il y a un domaine parent et tous les nouveaux domaines seront des domaines enfants. Il partage un même espace de nom contigu.
- La relation d'approbation
 - Les relations d'approbations entre domaines sont créées automatiquement de façon transitive et bidirectionnelle.

Organisation de l'AD



105

Organisation d'un domaine

- Un domaine contient au moins un contrôleur de domaine, appelé DC
- Au moins deux DC par domaine sont recommandés
- A l'intérieur d'un domaine, il est possible de créer des unités d'organisation (OU), artifice permettant d'organiser hiérarchiquement l'AD afin de la rapprocher de la structure de l'entreprise

©Hainaut P. 2017 - www.coursonline.be

106

Organisation d'une OU

- Une OU est un objet conteneur Active Directory utilisé à l'intérieur des domaines

Les OU sont des conteneurs logiques dans lesquels vous pouvez placer des utilisateurs, des groupes, des ordinateurs et d'autres unités d'organisation (jusqu'à 32 sous-niveaux). Elles ne peuvent contenir que des objets de leur domaine parent

L'unité d'organisation est la plus petite étendue à laquelle un objet de stratégie de groupe peut être lié, ou sur laquelle une autorité administrative peut être déléguée

Principaux objets de l'AD

- Utilisateur: représente un utilisateur physique à qui on associe des droits et des permissions pour l'accès aux ressources
- Contact: utilisateur qui ne peut se connecter au réseau mais à qui on peut envoyer des e-mails
- Groupe: gère la sécurité des droits ou permissions. Contient des utilisateurs, des contacts ou des groupes
- InetOrgPerson: objet de classe utilisateur compatible LDAP

Principaux objets de l'AD

- OU: container permettant une organisation hiérarchique dans un domaine. On peut lui appliquer des stratégies de groupe
- Imprimante: peut être publié dans l'AD, ce qui simplifie sa recherche
- Dossier partagé: idem
- Container: container système, on ne peut pas lui appliquer des stratégies de groupe

Organisation physique de l'AD

- Sous-réseau IP: domaine de diffusion
- Site AD: composé d'un ou plusieurs sous-réseaux IP. Espace de réplication sans restriction de l'AD. Par défaut, un seul site par défaut dans la forêt
- Transport intersite: définit la méthode utilisée pour la réplication de l'AD entre deux sites
- Liens du site: réplication intersite de l'AD entre deux sites AD contigus
- Pont entre liens de sites: idem pour deux sites AD disjoints

Partitions de l'AD

- Schéma: contient la définition des attributs et des classes permettant de créer un objet dans l'AD
- Configuration: contient la topologie physique et de réplication de l'AD
- Domaine: Contient tous les objets d'un domaine spécifique
- DNS: Contient la base de données DNS
- Autre: l'admin peut créer une partition spécifique dans l'AD

Les maîtres d'opérations FSMO

- Si l'on se place dans une structure informatique d'entreprise, il est conseillé d'avoir plusieurs DC dans l'environnement AD
- Certains rôles au sein de l'AD sont plus délicats que d'autres et il serait dangereux d'autoriser la modification de certaines données sur deux DC différents, en même temps
- Microsoft a donc créé les rôles FSMO (Flexible Single Master Operation) qui seront gérés par des maîtres d'opérations FSMO (des DC ayant un ou plusieurs rôles FSMO particulier en plus du reste)

Les maîtres d'opérations FSMO

- Sur de petites structures, tous les rôles FSMO peuvent être concentrés sur un seul DC (non recommandé)

Rôle FSMO	Portée
Maître de schéma	1 par forêt
Maître de dénomination de dom.	1 par forêt
Maître RID	1 par domaine
Maître d'infrastructure	1 par domaine
Maître émulateur PDC	1 par domaine

Le maître de schéma

- Définit le serveur DC sur lequel il est possible de modifier le schéma (les autres DC ont une copie en lecture seule)
- Le schéma peut être étendu pour ajouter de nouveaux attributs, de nouvelles applications, ...
- Si on modifie le schéma, il faut tenir compte de la latence de réplication entre le maître de schéma et les DC où l'on installe l'application

Le maître de dénomination de domaine

- Le maître de dénomination de domaine garantit la cohérence des noms de domaines lors de l'ajout et la suppression de domaine ou la modification du nom de domaine

Le maître RID

- Dès qu'un contrôleur de domaine crée une entité de sécurité (un objet tel qu'un utilisateur, un groupe, un ordinateur), il attribue à cet objet un **identificateur de sécurité unique**, le SID (Security IDentifier). ce SID est composé de deux blocs : un **SID de domaine** (identique pour tous les objets du domaine), et un **identifiant relatif** (RID), qui est unique pour chaque SID d'objet créé dans le domaine.
- Le maître RID se charge d'allouer **des blocs d'identificateurs relatifs** à chaque DC du domaine. Chaque DC possède donc un pool de RID unique à attribuer aux nouveaux objets créés.
- Si le maître RID **ne peut être joint**, la création d'un objet est **impossible** sur un contrôleur de domaine dont la réserve d'identificateurs relatifs est épuisée.
- L'utilitaire **dcdiag** situé dans le dossier \Support\Tools du cd-rom de Windows 2016 server permet d'afficher la réserve d'identifiants relatifs du contrôleur de domaine.

Identification des objets

- C'est le SID qui permet d'identifier les différents utilisateurs et objets, et donc par conséquent de leur appliquer les permissions NTFS, ce qui explique que deux utilisateurs peuvent avoir le même nom d'utilisateur sans qu'il y ait de conflits. Un SID étant unique, il est alors impossible de recréer un compte utilisateur supprimé en le nommant par le même nom que le compte précédant car les permissions NTFS se basent sur le SID et non pas le nom affiché
- Attention, il ne faut pas confondre le SID et le GUID (Global Unique Identifier)
- Ils sont tout deux uniques au sein de la forêt, mais contrairement au SID, le GUID ne changera jamais.

©Hainaut P. 2017 - www.coursonline.be

117

Identification des objets

- En effet, un objet peut être identifié de plusieurs façons :
 - Son DN (Distinguish name) : cn=Loïc, OU=Labo-WS2008, dc=isat, dc=lan
 - Son SID
 - Son GUID
- Le DN peut **changer très fréquemment**, lors du déplacement de l'objet ou lors du renommage d'une OU ou d'un domaine
- Le SID est **passible de changements** également lors du déplacement de l'objet d'un domaine à un autre
- Il peut donc être utile de disposer de moyens de retrouver les objets d'une autre manière que par leurs SID ou DN

©Hainaut P. 2017 - www.coursonline.be

118

Identification des objets

- Lors de la création d'un objet, celui-ci se voit attribuer un GUID, un **nombre codé sur 128 bits** enregistré dans l'attribut **objectGUID**.
- Cet attribut est obligatoire pour chaque objet, il ne peut être ni modifié, ni supprimé.
- Ce nombre **unique dans la forêt** est généré par un algorithme qui garantit son unicité, et il est assigné à **chaque objet** lors de sa création. Cet algorithme utilise **l'heure de création** de l'objet ainsi que d'autres informations aléatoires afin de créer un GUID unique.
- Le GUID est utilisé par les applications afin de pouvoir accéder à ces objets, quelque soit leurs DN ou SID.
- Par exemple, pour enregistrer une référence à un objet Active directory dans une base de donnée, c'est l'attribut **objectGUID** qui doit être utilisé car il ne sera **jamais modifié**.

Le serveur catalogue global

- Serveur DC qui contient une partition en lecture seule appelée catalogue global qui est une copie partielle des objets et des attributs de la partition de domaine de chaque domaine de la forêt
- Certaines applications sont conçues pour rechercher des infos uniquement dans le catalogue global et non dans la partition du domaine
- Le catalogue global est tjs interrogé lors de l'authentification de l'utilisateur
- Il est recommandé de placer au moins un serveur catalogue global par site Active Directory

Le maître d'infrastructure

- Contrôle la cohérence et l'intégrité du domaine comme lors du déplacement d'un objet, par exemple
- Il est recommandé que le maître d'infrastructure ne soit pas catalogue global

Le maître émulateur PDC

- A l'origine pour la migration en douceur de NT4 à 2000
- Très peu probable de trouver un NT4 dans un réseau 2016
- Mais le PDC emulator gère aussi la synchronisation de l'horloge pour tous les ordinateurs du domaine
- Et il prend en charge la réplication urgente

Le maître émulateur PDC

- Soit un utilisateur situé sur le site AD A, appelant une personne ressource situé sur le site AD B, car il a oublié son mot de passe
- La personne ressource lui réinitialise son mot de passe et lui transmet directement par téléphone
- La réplication intersite n'étant pas immédiate, le mot de passe n'est pas encore reconnu sur le site A.
- Avant de refuser la demande de login, le système va interroger le PDC emulator, qui va permettre d'authentifier l'utilisateur

Configuration des FSMO

- Les rôles FSMO doivent être configurés sur le domaine racine de la forêt
- Par défaut, les services de domaine Active Directory affectent tous les rôles de maître d'opérations au premier DC dans le domaine racine de la forêt

Configuration des FSMO

- Si votre conception spécifie que tous les contrôleurs du domaine racine de la forêt constituent des serveurs de catalogue global, conservez les cinq rôles de maître d'opérations sur le premier contrôleur de domaine et définissez le second contrôleur de domaine comme maître d'opérations de secours
- Si votre conception spécifie un domaine enfant, transférez le rôle de maître d'infrastructure à un contrôleur de domaine qui n'est pas un serveur de catalogue global

La réplication

- En informatique, la **réplication** est un processus de partage d'informations pour assurer la cohérence de données entre plusieurs sources de données redondantes, pour améliorer la fiabilité, la tolérance aux pannes, ou l'accessibilité
- On parle de *réplication de données* si les mêmes données sont dupliquées sur plusieurs périphériques
- La réplication n'est pas à confondre avec une sauvegarde : les données sauvegardées ne changent pas dans le temps, reflétant un état fixe des données, tandis que les données répliquées évoluent sans cesse à mesure que les données sources changent

La réplication intrasite

- Le serveur DC sur lequel une modification a été effectuée notifie les serveurs DC se trouvant sur le même site
- La latence est très faible dans une infrastructure normale pour arriver à la convergence
- Les modifications urgentes sont immédiatement répliquées vers le PDC emulator

La réplication intersite

- Intervient selon une planification qui peut définir des intervalles de plusieurs heures entre chaque réplication
- La réplication concerne:
 - Le schéma au niveau tous les DC de la forêt
 - Le cat. global vers tous cat. globaux de la forêt
 - La réplication de l'attribut de domaine vers le cat. global du domaine
 - Les modif. des objets vers tous les DC du même domaine
 - La configuration vers tous les DC de la forêt
 - Les partitions spécifiques comme le DNS vers les serveurs visés

7. Mise en œuvre de l'AD

Installation du rôle services de domaine Active Directory (AD DS)

Prérequis

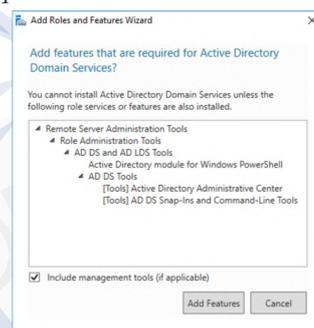
- Système de fichier NTFS
- Nom de serveur conforme aux spécifications DNS: 15 caractères max. (chiffes, lettres maj. et min. et tiret) ->Changez-le maintenant, si ce n'est déjà fait
- Paramètres IP corrects
- Nom de domaine correct
- Serveur DNS: pas obligatoire si on installe le rôle AD DS en même que les services AD DS (sur le même serveur). Sinon, le serveur doit être client d'un serveur DNS

©Hainaut P. 2017 - www.coursonline.be

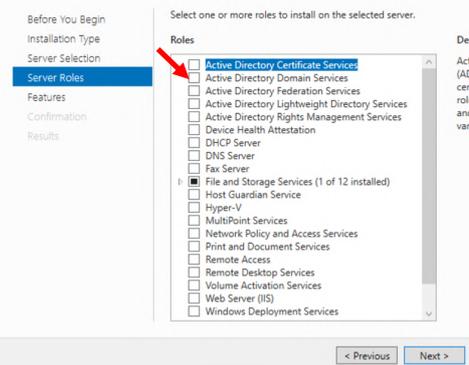
130

Installation du ctrl de domaine AD

- Connectez-vous en tant qu'administrateur
- Dans le Gestionnaire de serveur, ajoutez le rôle de serveur ADS
- Ajouter les fonctionnalités requises



Select server roles

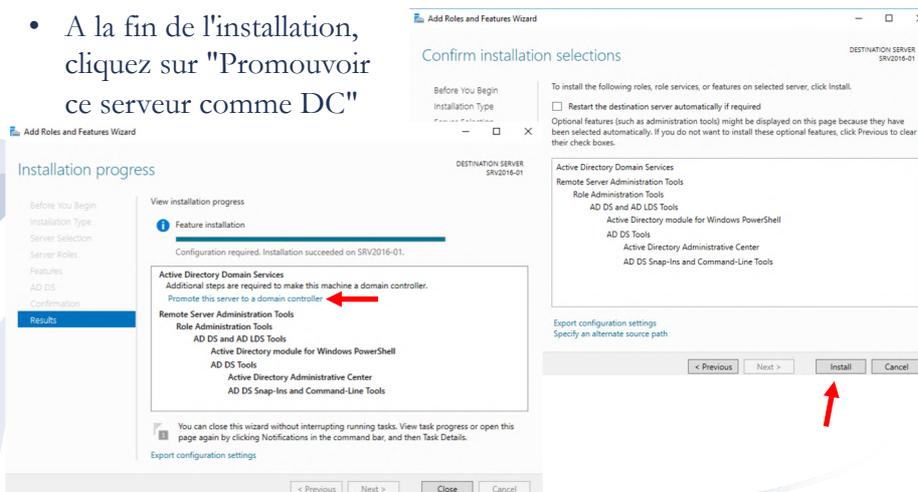


©Hainaut P. 2017 - www.coursonline.be

131

Installation du ctrl de domaine AD

- A la fin de l'installation, cliquez sur "Promouvoir ce serveur comme DC"

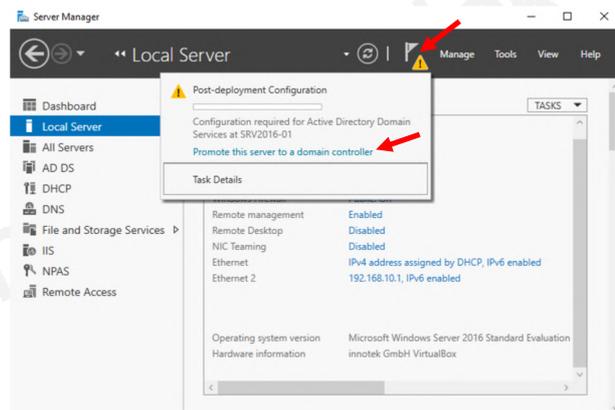


©Hainaut P. 2017 - www.coursonline.be

132

Installation du ctrl de domaine AD

- Si vous avez terminé l'installation sans le faire, dans les outils d'administration, cliquez sur le gestionnaire de serveur, puis sur le drapeau, et finalement sur "Promouvoir ce serveur comme DC"

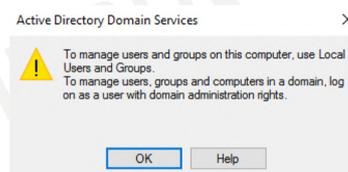


©Hainaut P. 2017 - www.coursonline.be

133

Installation du ctrl de domaine AD

- ADS va permettre de créer des comptes utilisateurs, groupes et ordinateurs valables sur tout le domaine en centralisant la gestion de ces comptes sur le DC
- Cliquez sur OK au niveau de l'avertissement

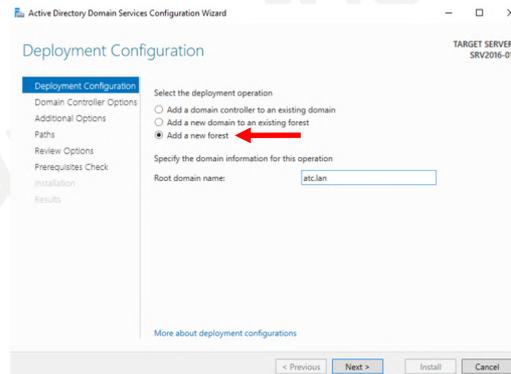


©Hainaut P. 2017 - www.coursonline.be

134

Installation du ctrl de domaine AD

- Au niveau de l'organisation de l'AD, on pourra choisir entre:
 - Créer une nouvelle forêt
 - Créer un nouveau domaine dans la forêt
 - Créer un DC dans le domaine
- Ici, nous allons créer une nouvelle forêt (et simultanément le premier DC dans le premier domaine)

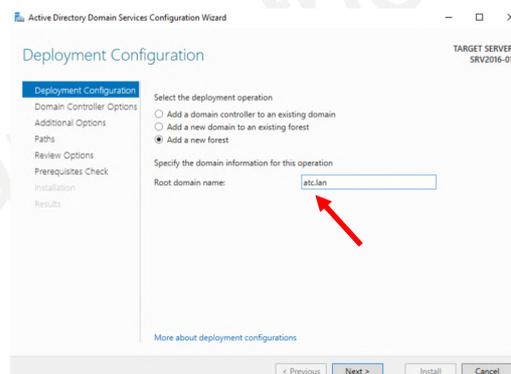


©Hainaut P. 2017 - www.coursonline.be

135

Installation du ctrl de domaine AD

- Le nom de domaine principal sera celui qu'on a renseigné lors de la configuration du serveur DNS



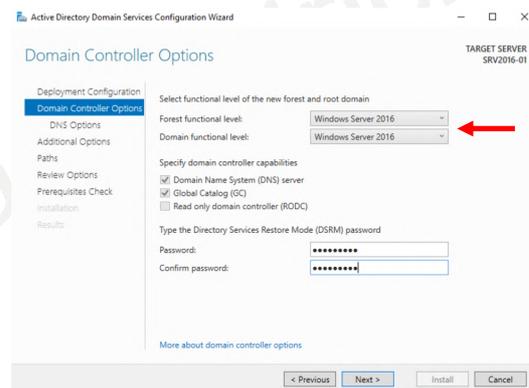
©Hainaut P. 2017 - www.coursonline.be

136

Installation du ctrl de domaine AD

- Pour le niveau fonctionnel de la forêt, si vous n'avez pas de DC d'une génération précédente (2008 ou antérieur), choisissez "Windows Server 2016"

- Notre DC sera:
 - serveur DNS
 - catalogue global
 - mais pas en lecture seule



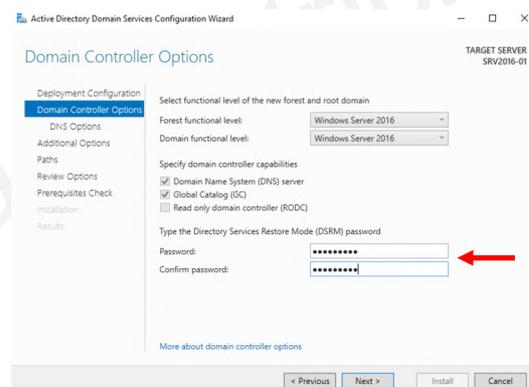
©Hainaut P. 2017 - www.coursonline.be

137

Installation du ctrl de domaine AD

- Remarque: il est parfois intéressant de déployer des DC en lecture seule, pour équiper des sites distants dont la sécurité physique ne peut être garantie (magasins par exemple)

- Choisissez un mot de passe de restauration, qui permettra à l'administrateur de réparer ou restaurer la base de données AD

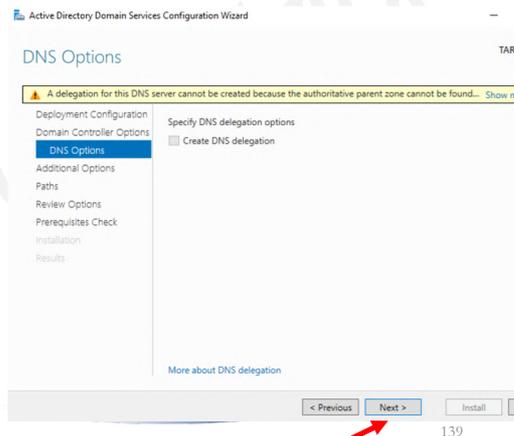


©Hainaut P. 2017 - www.coursonline.be

138

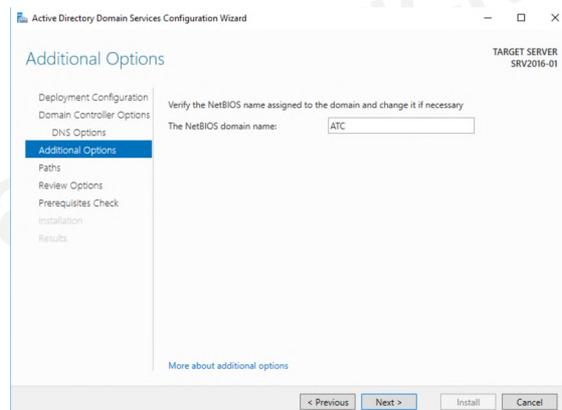
Installation du ctrl de domaine AD

- La délégation de zone DNS permet de diviser l'espace DNS de l'entreprise en plusieurs zones afin de répartir la charge
- Comme nous avons créé un .lan inexistant dans les extensions DNS officielles (c'est pour cela qu'on l'a pris), le système renvoie un warning mais qui est sans importance dans le cadre de notre manipulation



Installation du ctrl de domaine AD

- Le nom de domaine NETBIOS est le nom de domaine sans l'extension DNS

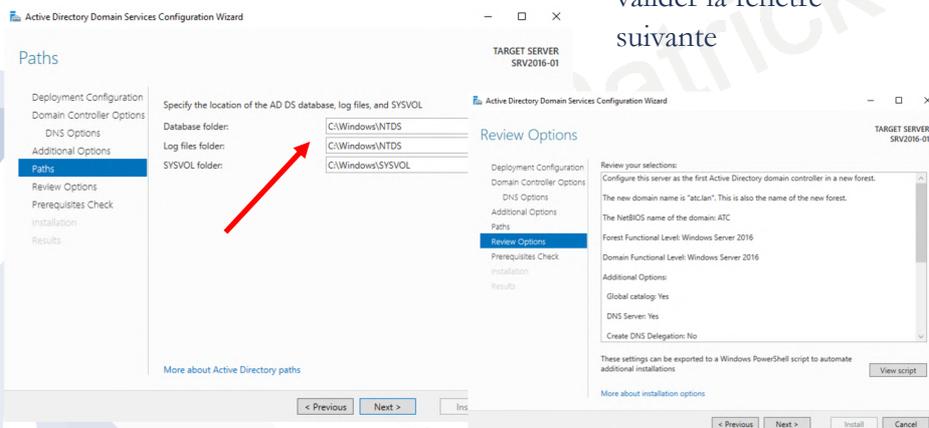


Installation du ctrl de domaine AD

- NETBIOS est le système de nommage des machines et domaines antérieur au DNS
- Cela permettait de créer des réseaux à l'aide des noms de machines (voisinage réseau)
- NETBIOS utilise la diffusion (broadcast) et ne passe donc pas à travers les routeurs
- On peut utiliser un serveur WINS pour palier à cet inconvénient
- NETBIOS est remplacé avantagement par DNS bien qu'il soit toujours utilisé au niveau local

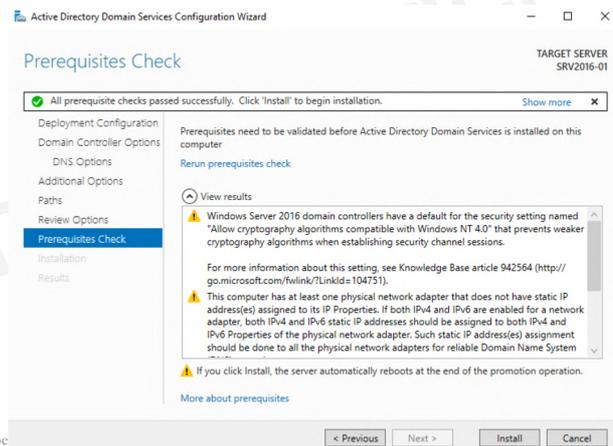
Installation du ctrl de domaine AD

- Les chemins par défaut peuvent être conservés et vous pouvez valider la fenêtre suivante



Installation du ctrl de domaine AD

- Quelques mises en garde avant installation concernant l'algorithme de cryptographie et le fait qu'on utilise une adresse dynamique
- L'adresse est ici dynamique parce que c'est un cas d'école, dans l'entreprise, elle sera statique



©Hainaut P. 2017 - www.coursonline.be

Installation du ctrl de domaine AD

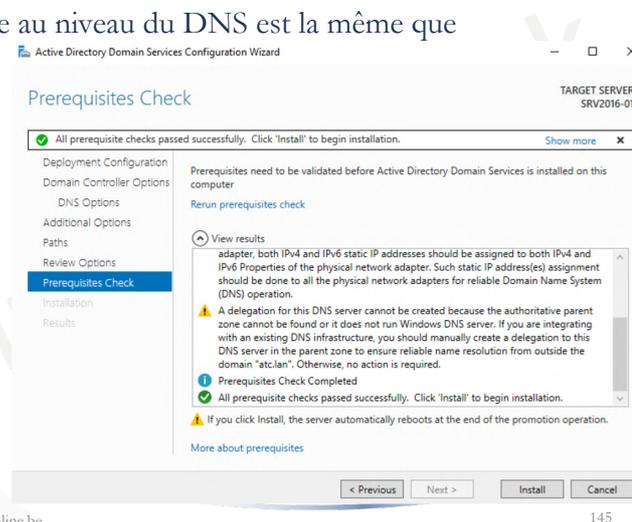
- Au niveau de la compatibilité de l'algorithme avec NT4.0, cela peut être réglé en exécutant gpmmc.msc
- Dans l'arborescence, choisissez Domains -> *Nom du domaine* -> Group Policy Objects -> bouton droit sur Default Domain Controllers Policy -> Edit
- Dans la nouvelle fenêtre: Computer Configuration -> Politiques -> Administrative Templates -> System -> Net Logon et finalement Allow Cryptography ... à activer ou pas

©Hainaut P. 2017 - www.coursonline.be

144

Installation du ctrl de domaine AD

- La mise en garde au niveau du DNS est la même que précédemment et concerne le fait que l'extention .lan n'est pas valable dans l'espace DNS public



©Hainaut P. 2017 - www.coursonline.be

145

8. Gestion des utilisateurs

Objectifs

- Dans un réseau, il est nécessaire de gérer efficacement les utilisateurs de manière centralisée
- Active Directory répond à ce besoin en offrant un moyen simple et centralisé et authentifier l'utilisateur et l'autoriser à accéder à des ressources se trouvant sur le réseau de l'entreprise grâce au compte utilisateur

Le compte utilisateur

- Celui-ci peut être local ou de domaine
- Il se compose d'un nom d'utilisateur et d'un mot de passe
- Il est possible d'ajouter d'autres informations comme le téléphone de l'utilisateur, ses droits d'accès distant, ...
- On distingue le compte d'utilisateur local dont les informations de compte résident dans la sam locale de l'ordinateur du compte d'utilisateur de domaine qui est stocké dans l'AD
- Sur un contrôleur de domaine, la sam est désactivée

Le compte utilisateur

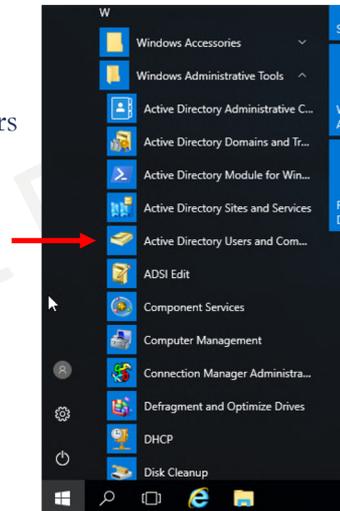
- Un compte d'utilisateur de domaine peut se connecter sur n'importe quel ordinateur et accéder à toutes les ressources du domaine, alors qu'un compte d'utilisateur local ne peut le faire que sur l'ordinateur considéré
- Dans une entreprise, la gestion des comptes d'utilisateur se fera par domaine

Le compte utilisateur

- Le système contient des comptes prédéfinis dont:
 - Administrateur: compte qui a accès à tout l'ordinateur (local) ou à la forêt ou au domaine (AD)
Ne peut être détruit ou désactivé mais peut être renommé
 - Invité: compte disposant de droits limités. Par défaut, il est désactivé et sans mot de passe
Il est conseillé de s'assurer qu'il reste désactivé et lui attribuer un mot de passe

Création des utilisateurs du domaine

- Une fois l'installation de l'AD terminée, nous retrouvons l'utilitaire AD Users and Computers disponible dans les outils d'administration

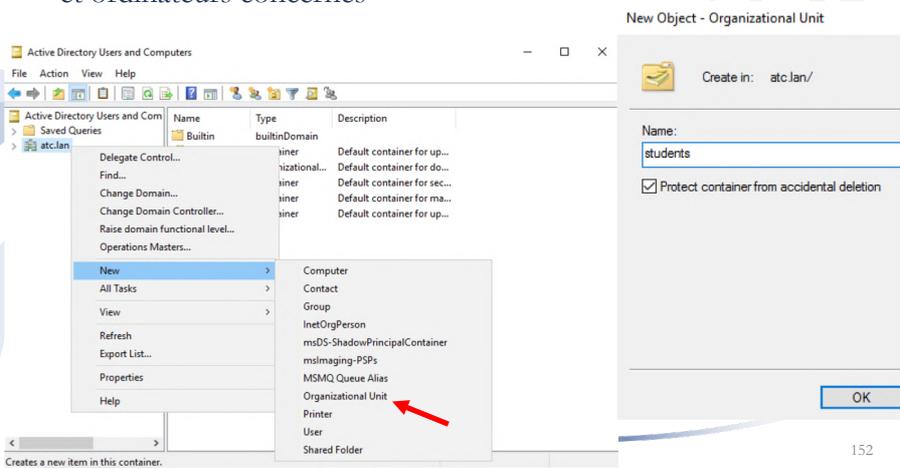


©Hainaut P. 2017 - www.coursonline.be

151

Création des utilisateurs du domaine

- On va premièrement créer une OU pour y mettre les utilisateurs et ordinateurs concernés



152

Création des utilisateurs du domaine

- On crée, dans cette OU, un compte utilisateur

New Object - User

Create in: atc.lan/students

First name: Bart Initials:

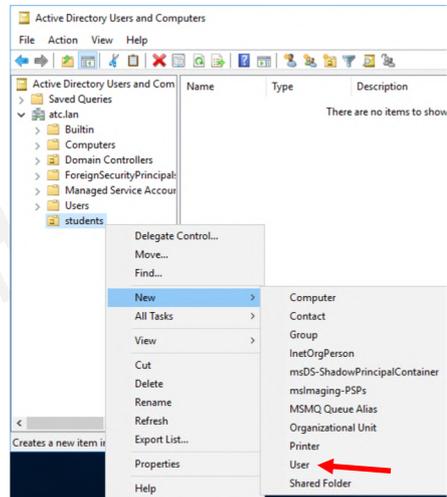
Last name: Simpson

Full name: Bart Simpson

User logon name: bart.simpson @atc.lan

User logon name (pre-Windows 2000): ATC\bart.simpson

< Back Next > Cancel



©Hainaut P. 2017 - www.coursonline.be

153

Création des utilisateurs du domaine

- Pour le nom d'ouverture de session, généralement on utilise l'UPN (User Principal Name)
- Les noms UPN se composent de trois parties : le préfixe UPN (nom d'ouverture de session de l'utilisateur), le caractère @ et le suffixe UPN
- Le suffixe UPN par défaut est le nom DNS de la forêt, qui correspond au nom DNS du premier domaine dans le premier arbre de la forêt

©Hainaut P. 2017 - www.coursonline.be

154

Création des utilisateurs du domaine

- On indique un mot de passe sécurisé pour l'utilisateur et on spécifie la politique de mots de passe

New Object - User

Create in: atc.lan/students

Password: [masked]

Confirm password: [masked]

User must change password at next logon

User cannot change password

Password never expires

Account is disabled

< Back Next > Cancel

< Back Finish Cancel

©Hainaut P. 2017 - www.coursonline.be

155

Création des utilisateurs du domaine

- On crée un compte ordinateur, soit dans l'OU, soit directement dans le domaine, suivant la portée de ce compte

New Object - Computer

Create in: atc.lan/students

Computer name: PC01

Computer name (pre-Windows 2000): PC01

The following user or group can join this computer to a domain.

User or group: Default: Domain Admins Change...

Assign this computer account as a pre-Windows 2000 computer

OK Cancel Help

Active Directory Users and Computers

File Action View Help

Active Directory Users and Com

Name Type Description

There are no items to show

atc.lan

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipal

Managed Service Account

Users

students

Delegate Control...

Move...

Find...

New > Computer

All Tasks >

Contact

Group

InetOrgPerson

msDS-ShadowPrincipalContainer

msImaging-PSPs

MSMQ Queue Alias

Organizational Unit

Printer

User

Shared Folder

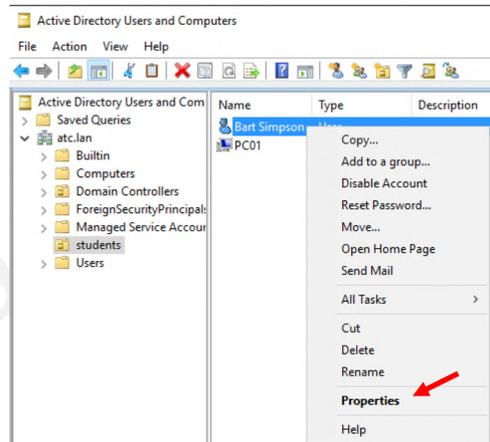
Creates a new item in

©Hainaut P. 2017 - www.coursonline.be

156

Création des utilisateurs du domaine

- Au niveau du compte utilisateur, on va définir l'emplacement du répertoire utilisateur, du répertoire de profil, et le nom du script d'ouverture de session

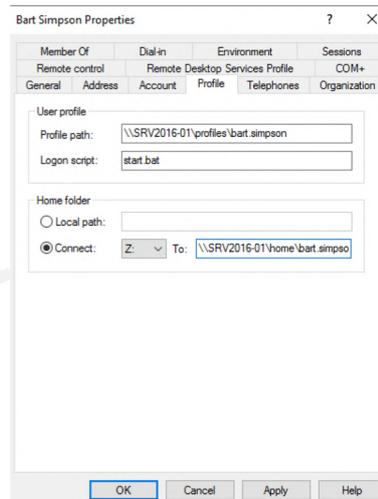


©Hainaut P. 2017 - www.coursonline.be

157

Création des utilisateurs du domaine

- C'est le client Windows 7 qui va utiliser ces informations, on spécifie donc un chemin réseau
- Pour le script, seul le nom est nécessaire, le chemin est connu du système

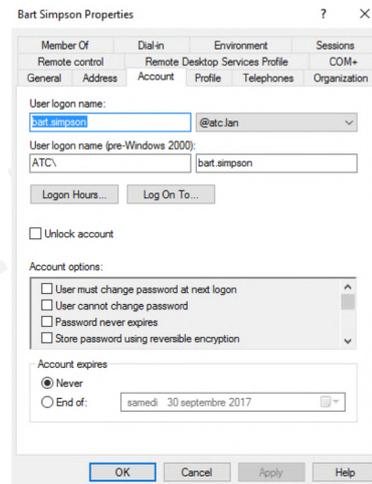


©Hainaut P. 2017 - www.coursonline.be

158

Création des utilisateurs du domaine

- Sur la page Account, on peut modifier la politique de mots de passe, débloquer un compte (parce qu'on a essayé de se loguer trop de fois sans succès), ou mettre une date d'expiration pour un compte (pour un stagiaire qui vient pour une durée déterminée dans l'entreprise par exemple)

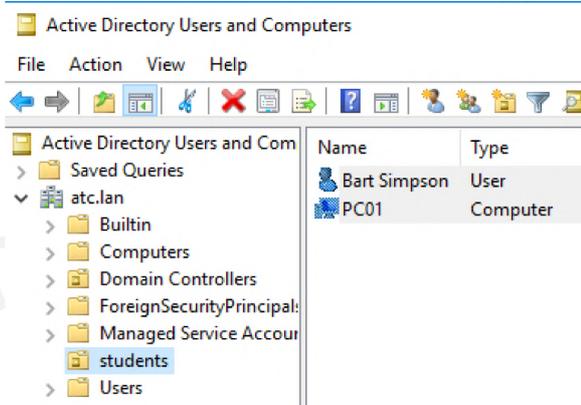


©Hainaut P. 2017 - www.coursonline.be

159

Création des utilisateurs du domaine

- Nous avons donc deux items dans notre OU students
- On peut en créer beaucoup plus, évidemment



©Hainaut P. 2017 - www.coursonline.be

160

Profil d'un utilisateur

- Dès qu'un utilisateur se connecte sur un ordinateur, son profil est chargé du serveur en local puis le profil local est utilisé durant la session
- Il se trouve dans le dossier Users sur Windows 7
- A la fin de la session, le profil éventuellement modifié est sauvé sur le serveur

Profil d'un utilisateur

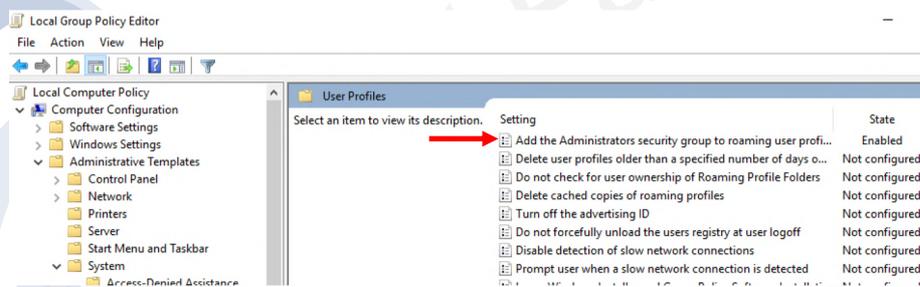
- S'il s'agit d'un profil itinérant obligatoire, les modifications de celui-ci ne sont pas sauvegardées en fin de session
- Pour créer un profil obligatoire, il faut renommer le fichier nuser.dat se trouvant dans le répertoire de profil (sur le serveur) en nuser.man

Profil d'un utilisateur

- Pour pouvoir gérer les profils itinérants correctement, on doit rajouter le groupe des administrateurs pour la gestion de ceux-ci
- Sinon, il sera impossible de configurer un profil itinérant en profil mandataire (profil en lecture seule)
- Pour cela, il faut exécuter **gpedit.msc** qui ouvre l'éditeur de stratégie de groupe

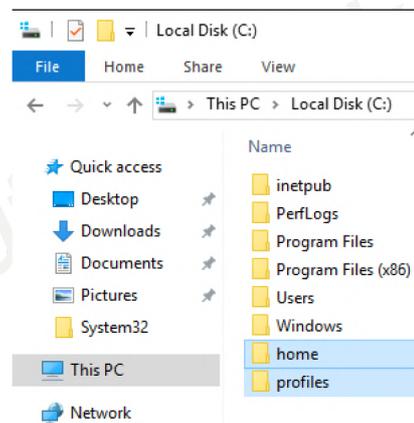
Profil d'un utilisateur

- On va dans Configuration de l'ordinateur -> Modèles d'administration -> Système -> Profils utilisateurs -> ajouter le groupe de sécurité des administrateurs aux profils utilisateur itinérants -> cliquez dessus pour activer cet item



Création des utilisateurs du domaine

- Il faut maintenant créer les répertoires spécifiés dans l'onglet profil du compte utilisateur

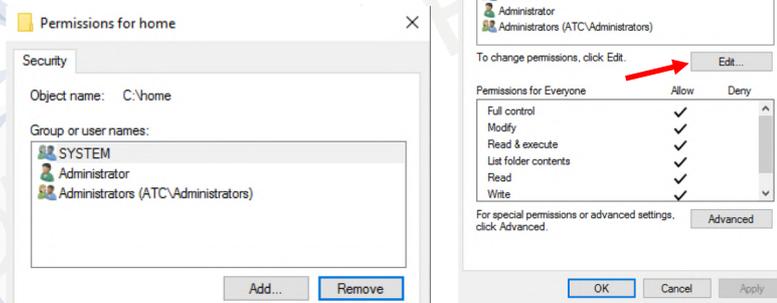


©Hainaut P. 2017 - www.coursonline.be

165

Création des utilisateurs du domaine

- Par défaut, tout le monde a accès aux répertoires créés
- On va éditer les permissions pour supprimer "Tout le monde"

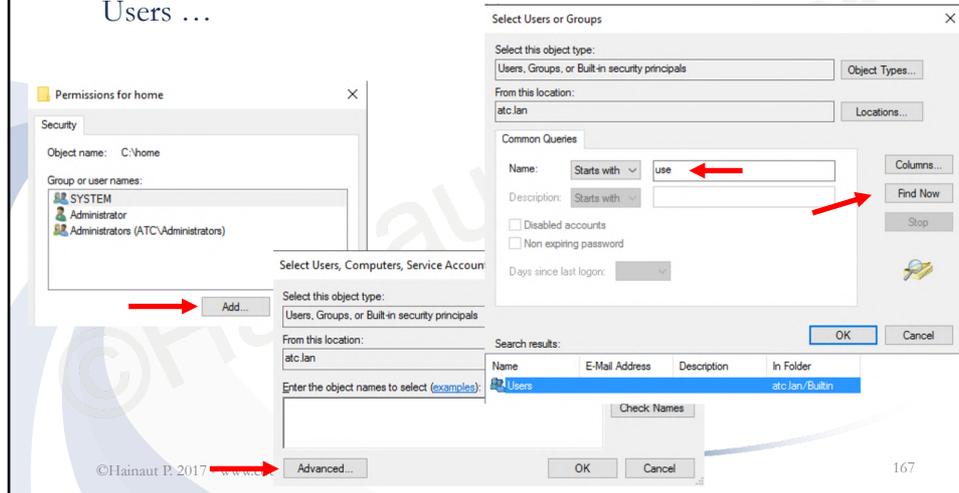


©Hainaut P. 2017 - www.coursonline.be

166

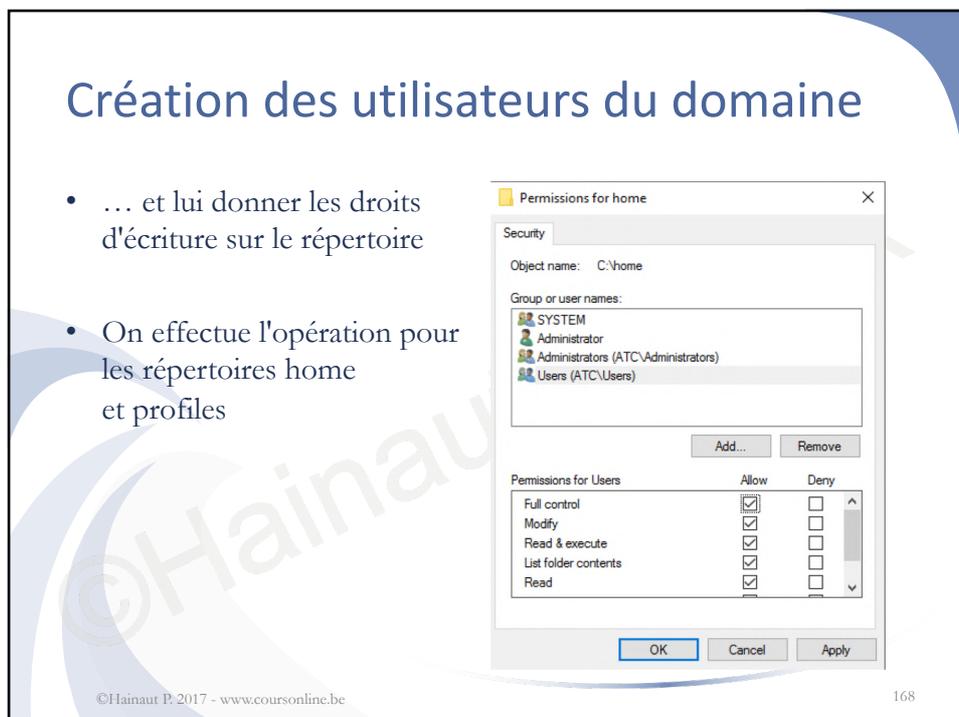
Création des utilisateurs du domaine

- Il faut ensuite ajouter le groupe Users ...



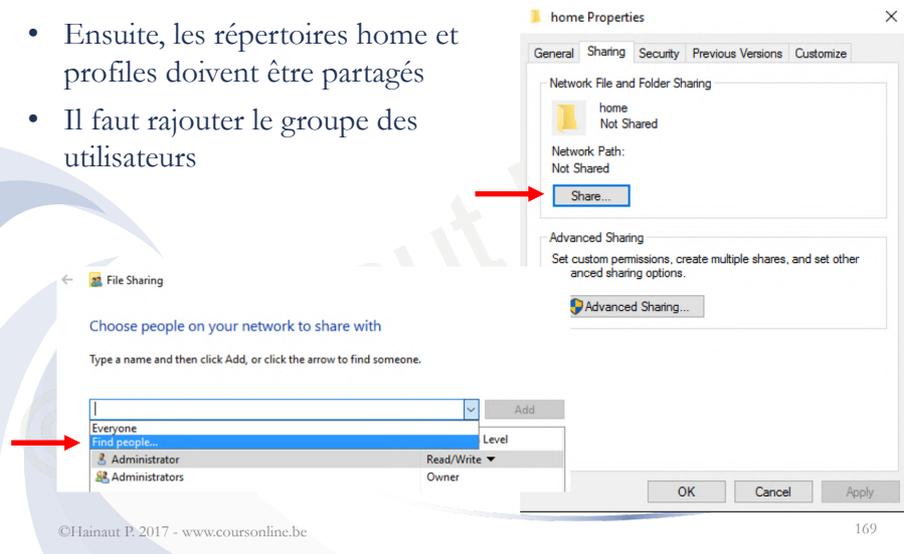
Création des utilisateurs du domaine

- ... et lui donner les droits d'écriture sur le répertoire
- On effectue l'opération pour les répertoires home et profiles

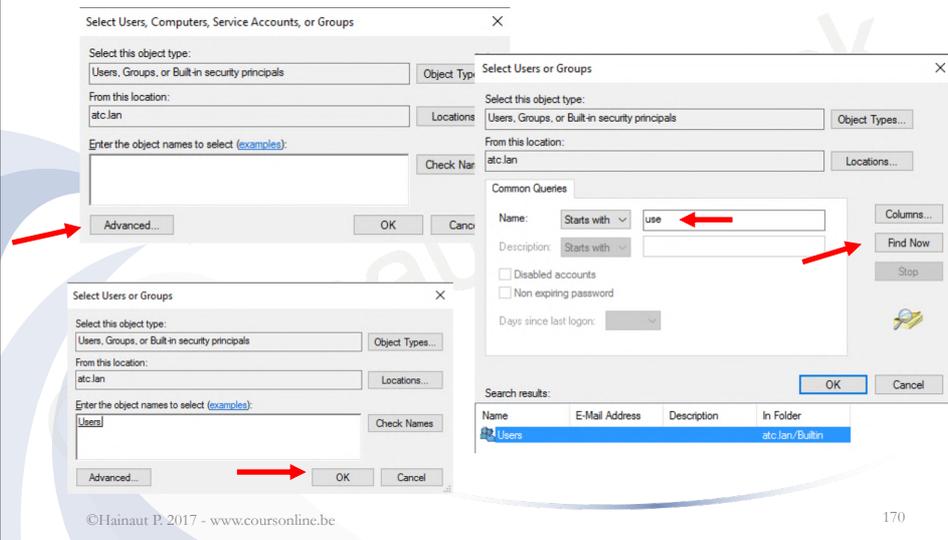


Création des utilisateurs du domaine

- Ensuite, les répertoires home et profils doivent être partagés
- Il faut rajouter le groupe des utilisateurs

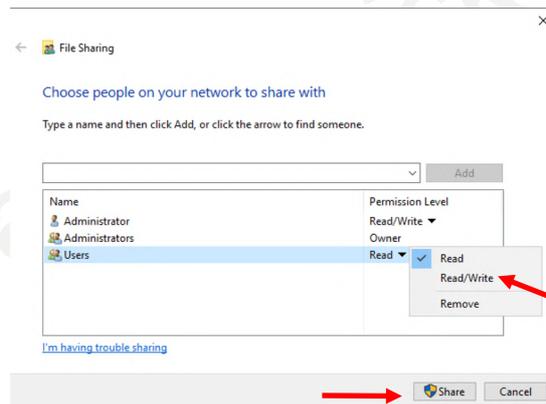


Création des utilisateurs du domaine



Création des utilisateurs du domaine

- Il faut lui donner un accès en écriture
- L'opération est à effectuer pour les répertoires home et profiles

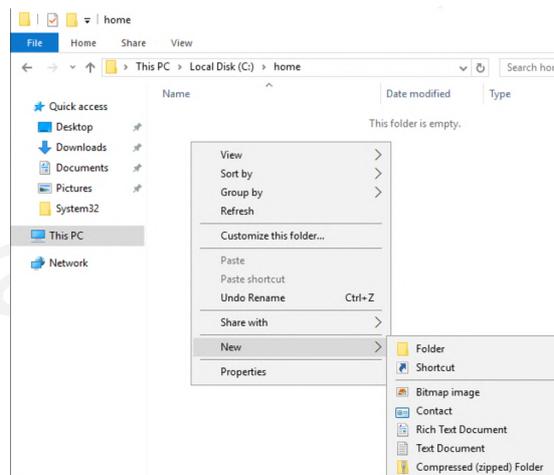


©Hainaut P. 2017 - www.coursonline.be

171

Création des utilisateurs du domaine

- On crée ensuite, dans le répertoire home, un répertoire au nom de chaque compte utilisateur créé

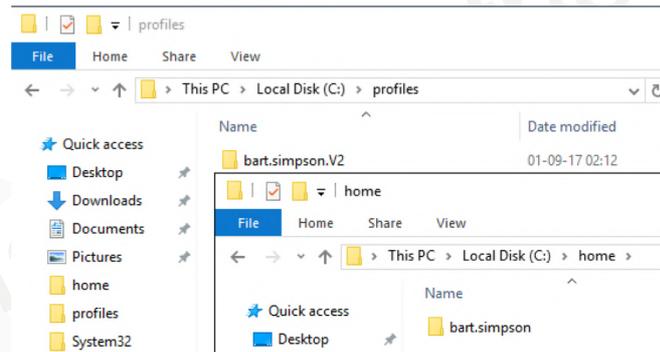


©Hainaut P. 2017 - www.coursonline.be

172

Création des utilisateurs du domaine

- Idem pour le répertoire profiles, mais on rajoute un .V2 au nom du répertoire créé (car client Windows 7)

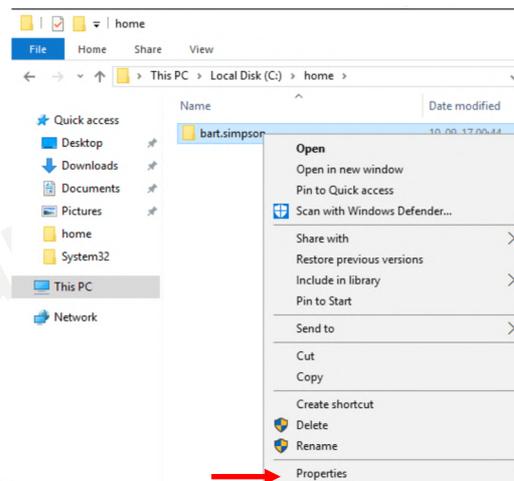


©Hainaut P. 2017 - www.coursonline.be

173

Création des utilisateurs du domaine

- Il faut ensuite éditer les permissions sur les dossiers nouvellement créés

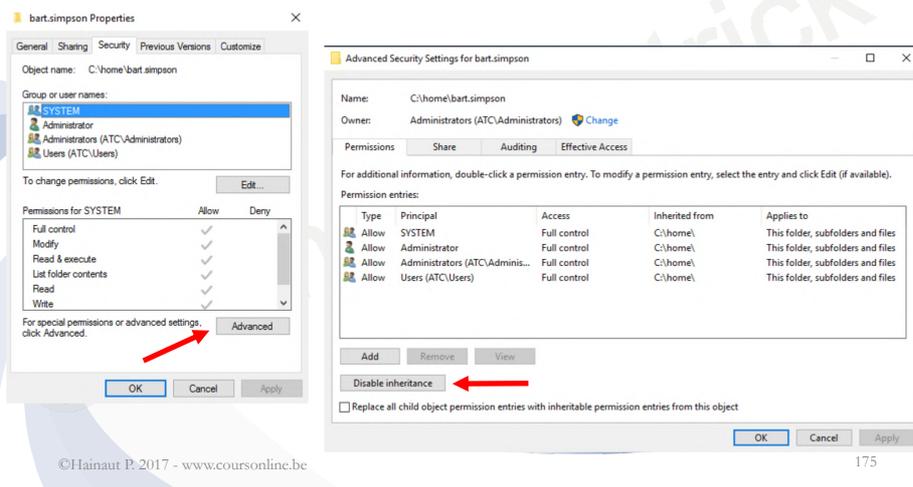


©Hainaut P. 2017 - www.coursonline.be

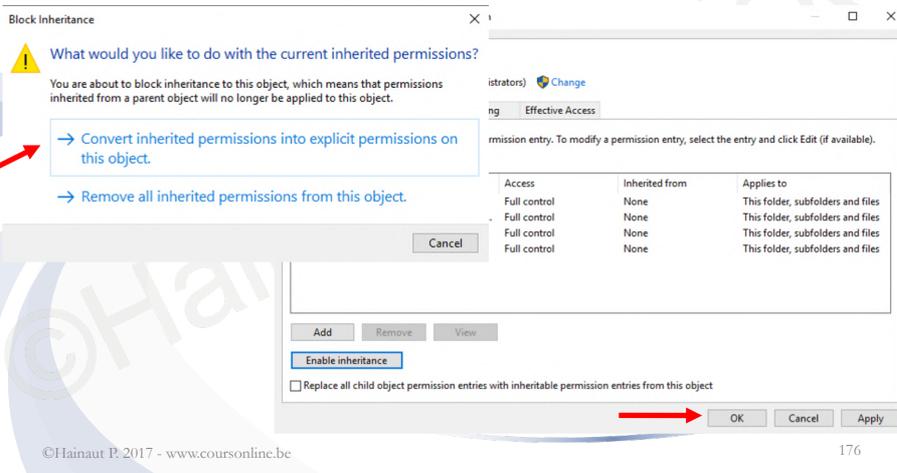
174

Création des utilisateurs du domaine

- Il faut, premièrement, désactiver l'héritage des permissions

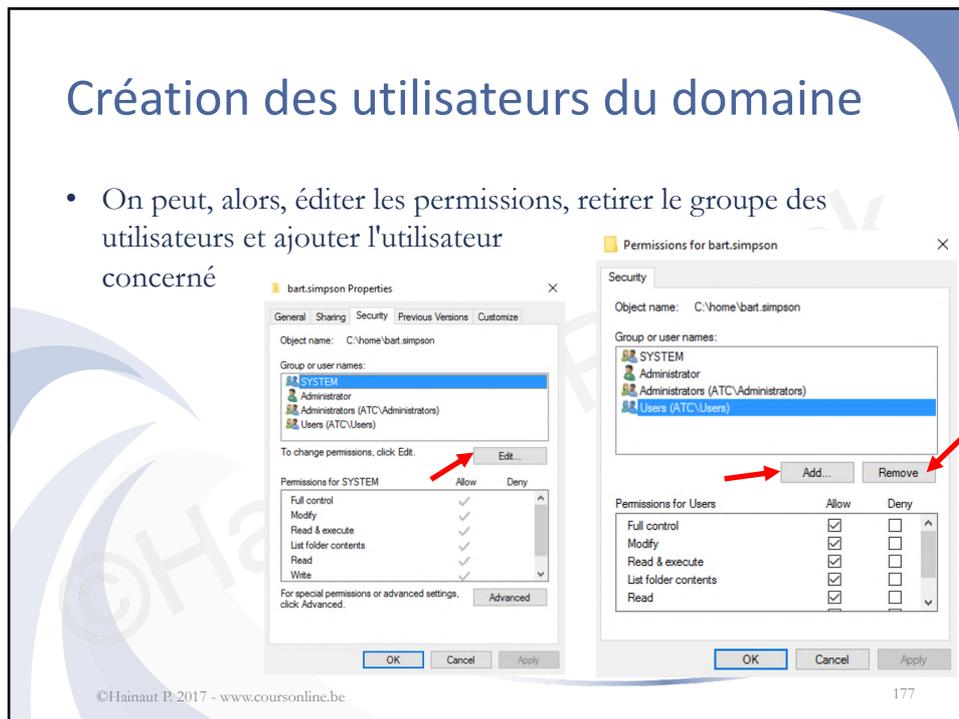


Création des utilisateurs du domaine

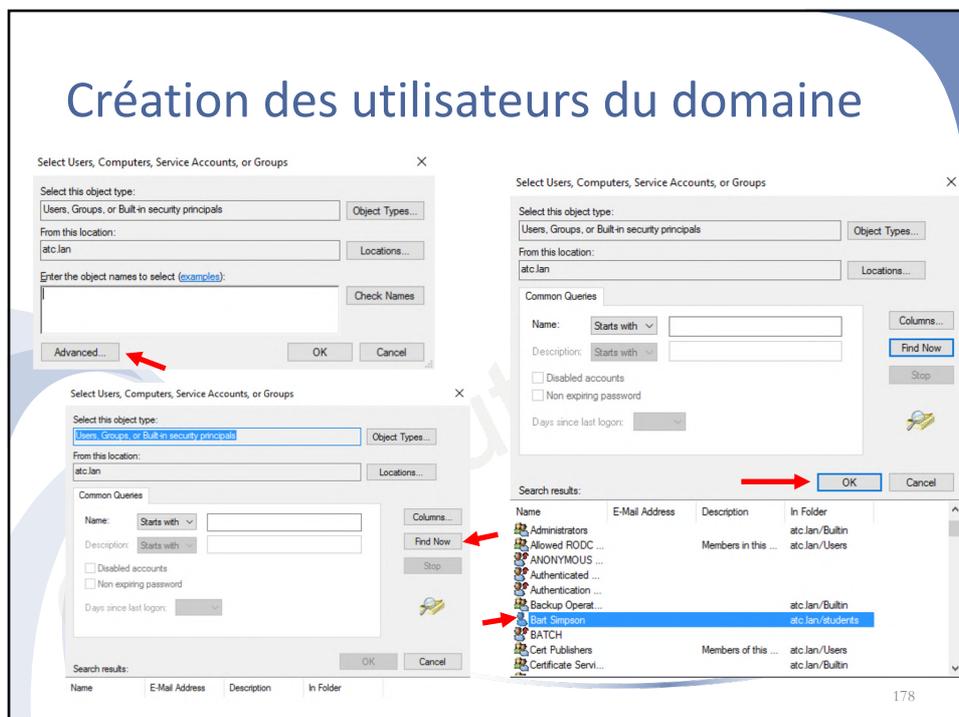


Création des utilisateurs du domaine

- On peut, alors, éditer les permissions, retirer le groupe des utilisateurs et ajouter l'utilisateur concerné

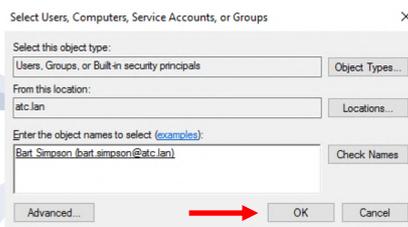


Création des utilisateurs du domaine

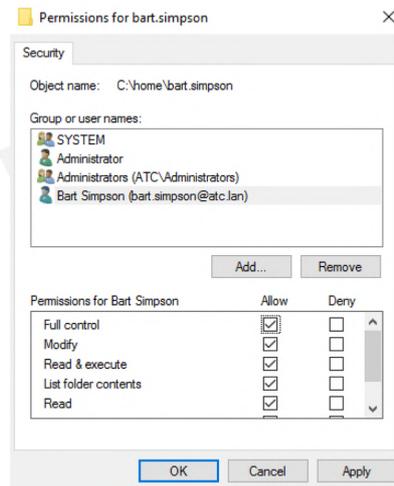


Création des utilisateurs du domaine

- On donne tous les droits sur le dossier à l'utilisateur concerné



- L'opération est à répéter pour le répertoire de profil de l'utilisateur

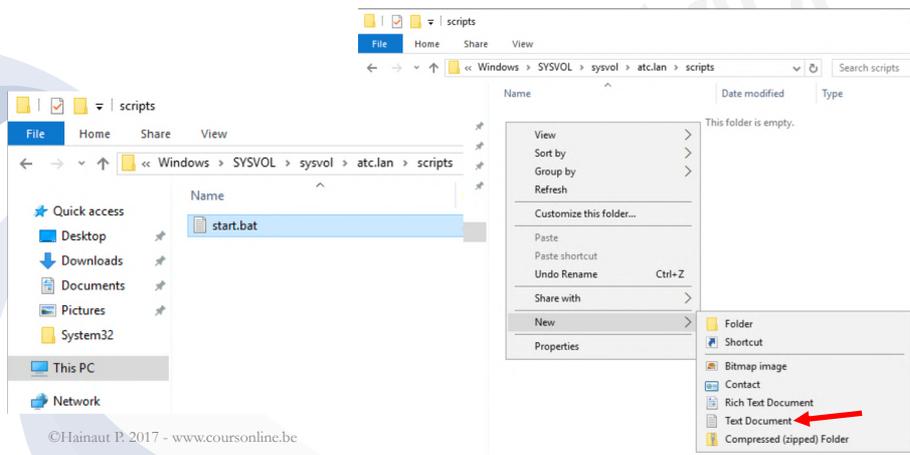


©Hainaut P. 2017 - www.coursonline.be

179

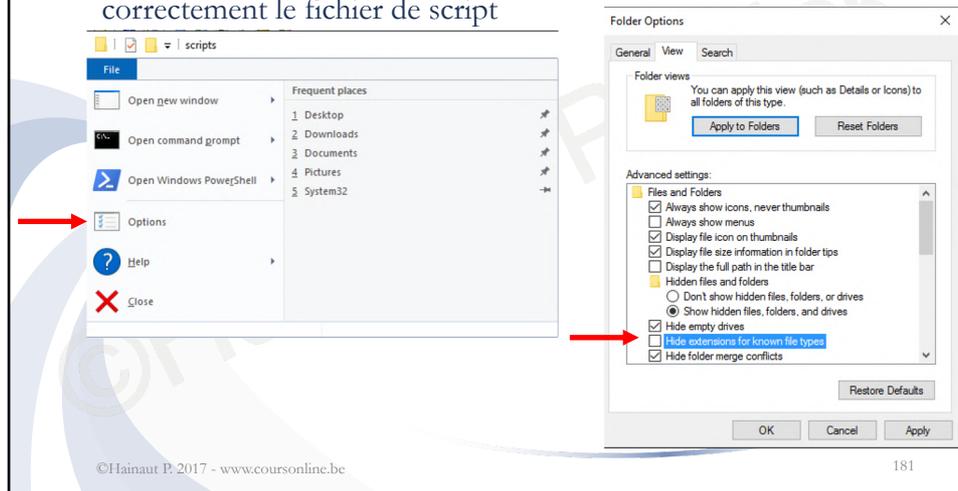
Création des utilisateurs du domaine

- Il reste à créer le script d'ouverture de session qui doit se trouver dans: C:\Windows\SYSTEM\sysvol\sysvol*nomDuDomaine*\scripts



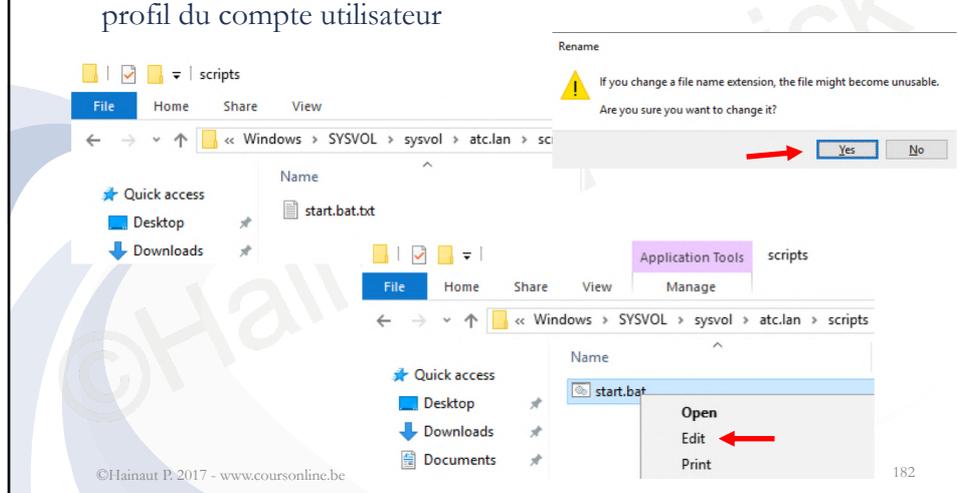
Création des utilisateurs du domaine

- Il faut afficher les extensions de fichiers pour pouvoir nommer correctement le fichier de script



Création des utilisateurs du domaine

- Le fichier de script doit porter le nom spécifié dans l'onglet profil du compte utilisateur



Création des utilisateurs du domaine

- Le script contiendra la commande net use permettant d'affecter une lettre de lecteur à un disque réseau
- On peut ainsi déclarer plusieurs partages

```
start.bat - Notepad
File Edit Format View Help
net use w: \\SRV2016-01\home\share
```

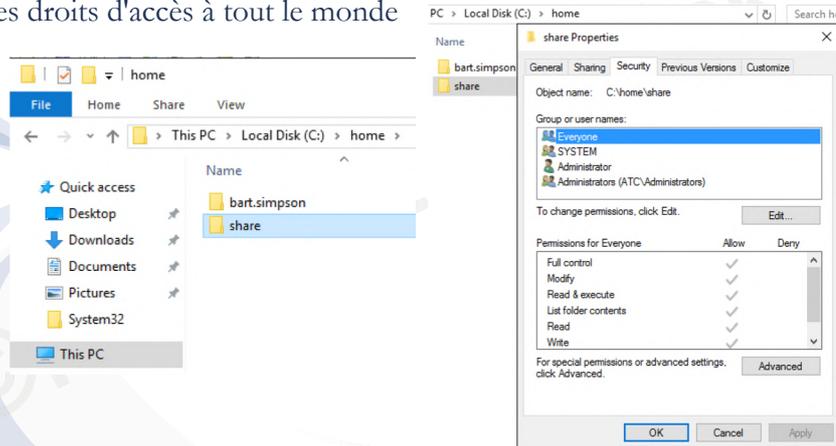
- Le chemin réseau universel est:
\\NomDuServeur\NomDeLaRessourcePartagée\NomDuSous-répertoire

Création des utilisateurs du domaine

- Le répertoire scripts du serveur en accès local par
C:\Windows\SYSTEM32\sysvol*nomDuDomaine*\scripts
est un répertoire partagé nommé netlogon, accessible en écriture
par les administrateurs et en lecture par les autres

Création des utilisateurs du domaine

- On crée, ensuite, le répertoire spécifié dans le script en donnant les droits d'accès à tout le monde

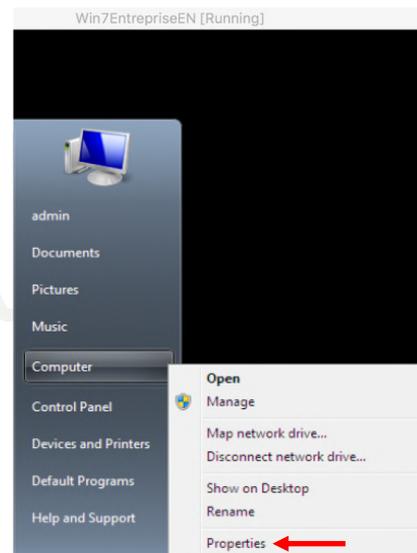


©Hainaut P. 2017 - www.coursonline.be

185

Installation du ctrl de domaine AD

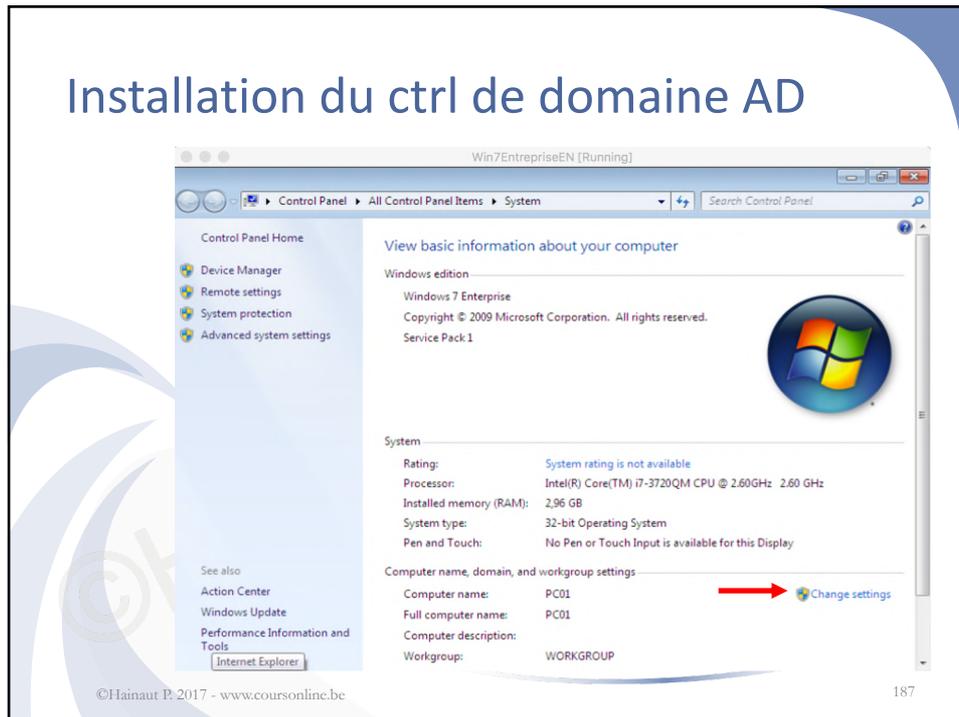
- La configuration sur le serveur étant terminée, il faut maintenant faire passer le client Windows 7 dans le domaine fraîchement créé



©Hainaut P. 2017 - www.coursonline.be

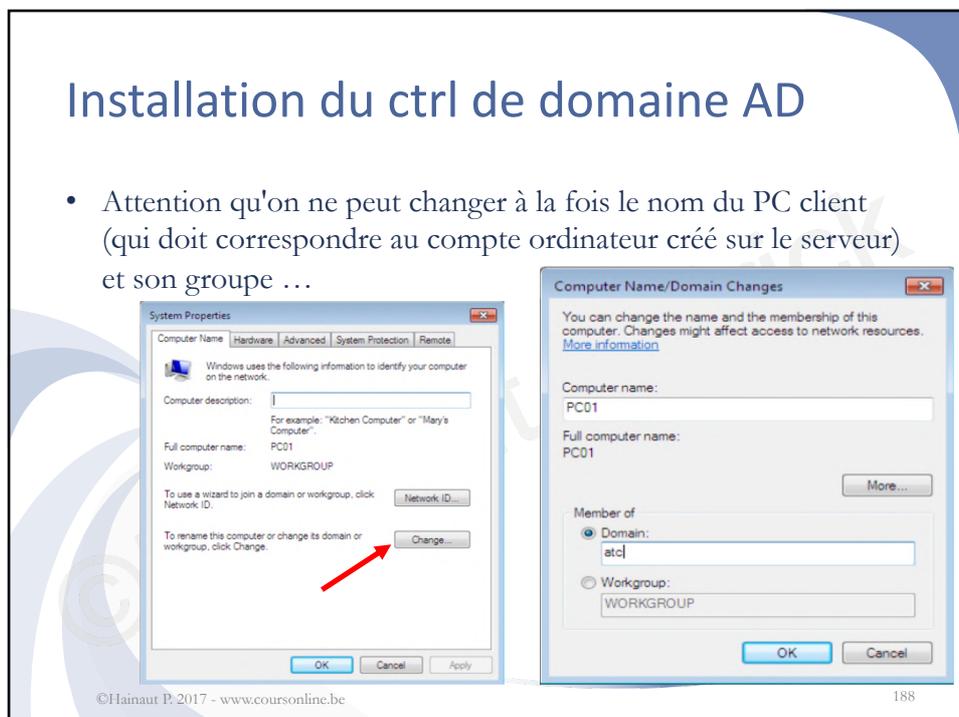
186

Installation du ctrl de domaine AD



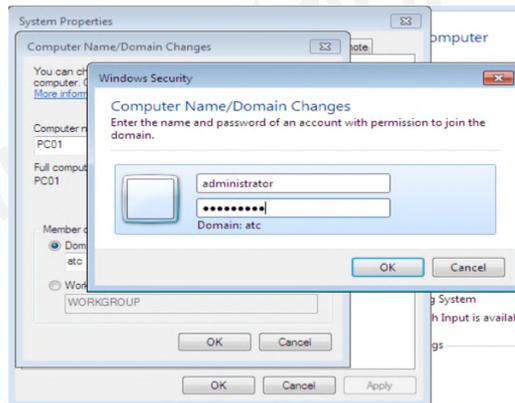
Installation du ctrl de domaine AD

- Attention qu'on ne peut changer à la fois le nom du PC client (qui doit correspondre au compte ordinateur créé sur le serveur) et son groupe ...



Installation du ctrl de domaine AD

- Le nom de domaine correspond au nom de domaine créé sur le serveur mais sans l'extension DNS
- Pour rejoindre le domaine, il faut bien sur en avoir le droit, et il faut valider la demande avec le compte administrateur du domaine

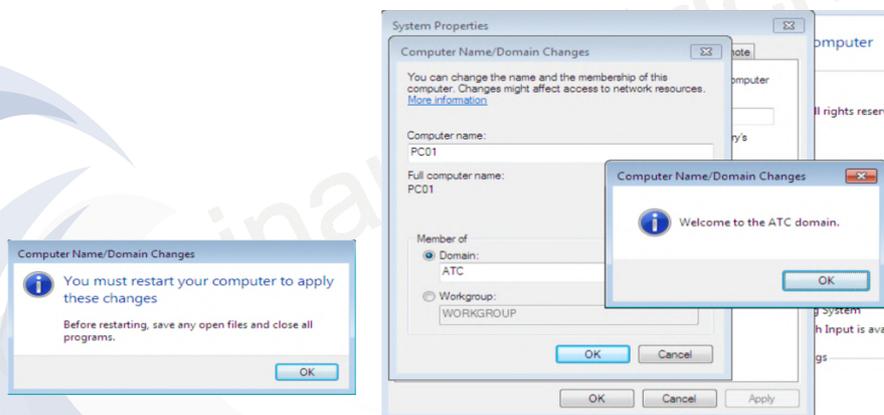


©Hainaut P. 2017 - www.coursonline.be

189

Installation du ctrl de domaine AD

- Une fois l'ordinateur client accepté dans le domaine, il faut redémarrer celui-ci

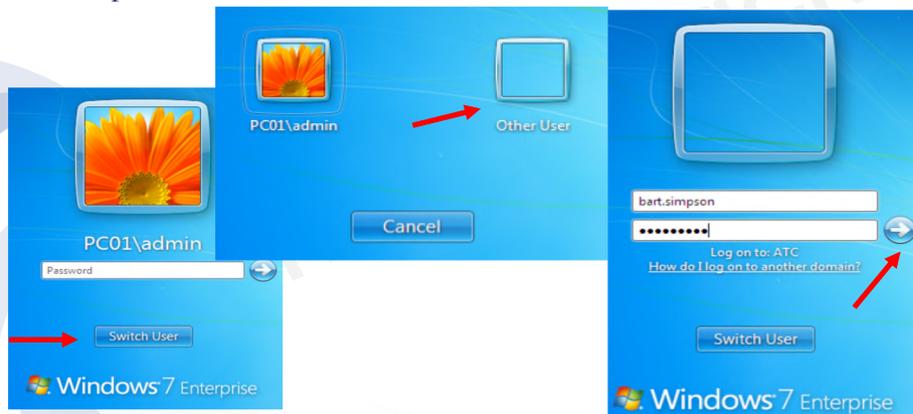


©Hainaut P. 2017 - www.coursonline.be

190

Installation du ctrl de domaine AD

- Une fois le PC client redémarré, on peut se loguer avec un des comptes utilisateur du domaine, créés sur le serveur



©Hainaut P. 2017 - www.coursonline.be

191

Installation du ctrl de domaine AD

- On retrouve dans le poste de travail de l'utilisateur, son répertoire personnel sur le serveur plus le répertoire d'échange

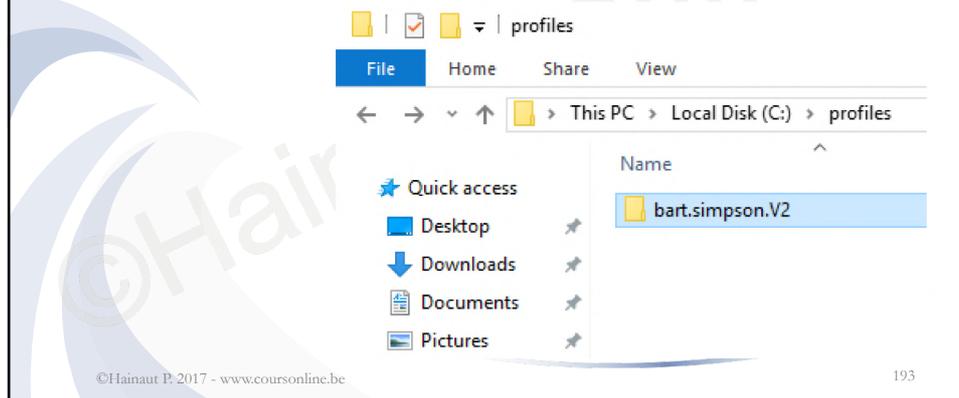


©Hainaut P. 2017 - www.coursonline.be

192

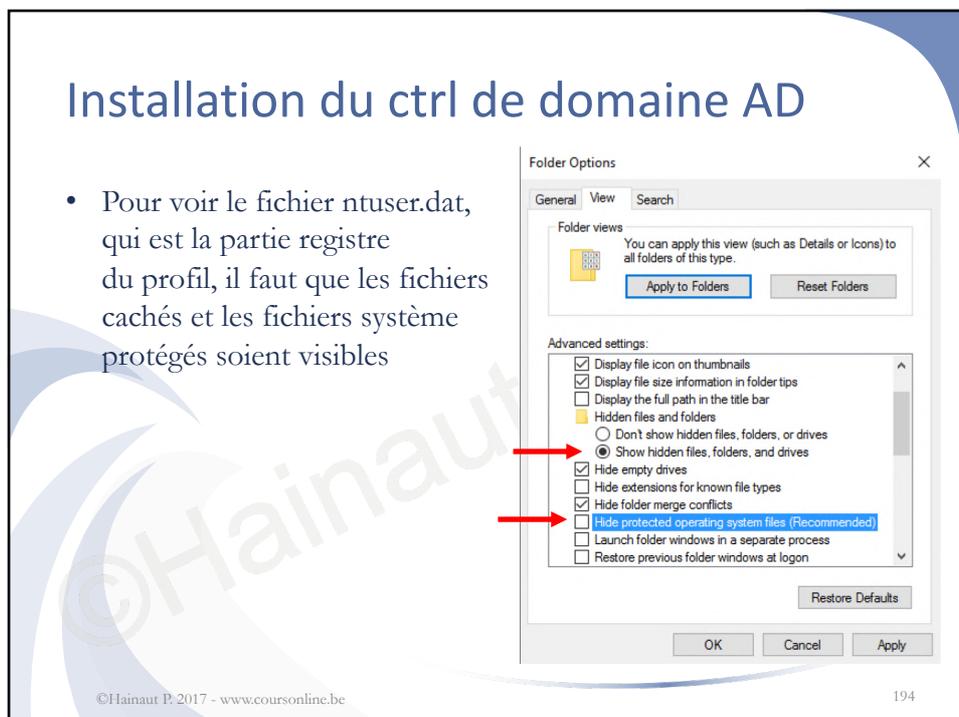
Installation du ctrl de domaine AD

- Si on se délogue, le profil de l'utilisateur sera sauvegardé sur le serveur dans le répertoire spécifié dans l'onglet profils du compte utilisateur (avec l'extension V2 pour les clients Windows 7)



Installation du ctrl de domaine AD

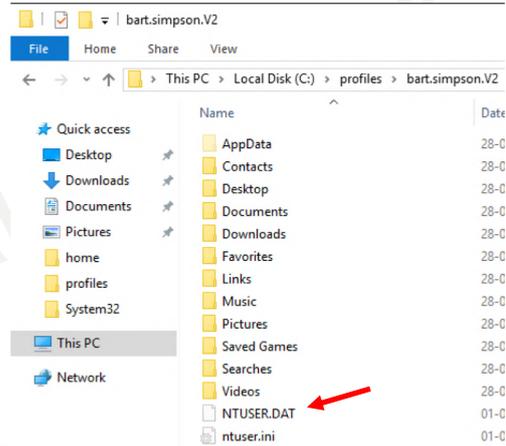
- Pour voir le fichier ntuser.dat, qui est la partie registre du profil, il faut que les fichiers cachés et les fichiers système protégés soient visibles



Installation du ctrl de domaine AD

- On peut alors modifier le ntuser.dat en ntuser.man si on veut transformer le profil itinérant en profil mandataire (profil figé)

- Cela veut dire que toute modification du bureau, tout dossier ou fichier créé sur le bureau ou dans Mes Documents, sera perdu ...



©Hainaut P. 2017 - www.coursonline.be

195

Installation du ctrl de domaine AD

- Cela permet plusieurs choses:
 - Uniformisation des fond d'écran
 - Profils légers à charger (pas de risque d'avoir une image blue-ray de 16Gb à sauvegarder sur le serveur à chaque fermeture de session et à rapatrier sur le client à chaque ouverture de session)
 - Obligation pour les utilisateurs d'utiliser les répertoires réseau mis à leur disposition pour sauvegarder les données (et faciliter ainsi le backup des données de l'entreprise puisqu'il suffit de faire un backup du disque serveur)

©Hainaut P. 2017 - www.coursonline.be

196

En cas de problème ...

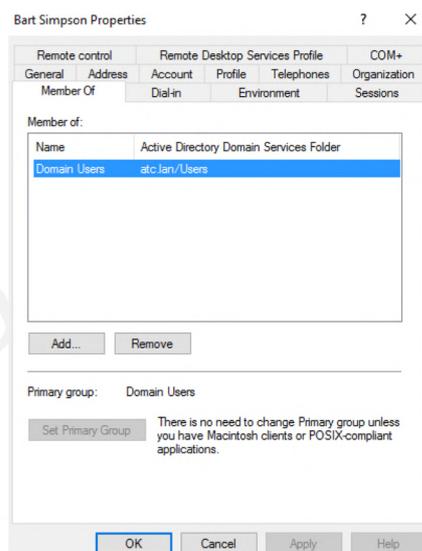
- Si le système ne veut pas charger le profil:
 - Vérifiez avec une commande net use... sur le PC client, que celui a bien accès au serveur
 - Si vous obtenez une erreur 67, remplacer le nom netbios du DC par son adresse IP (à répercuter sur la config du profil de l'utilisateur)
 - Effacez le profil copié en local sur le client
 - Créez un autre utilisateur ...

©Hainaut P. 2017 - www.coursonline.be

197

Groupe(s) d'un utilisateur

- L'onglet Membre permet de définir le ou les groupes auquel(s) appartient l'utilisateur



©Hainaut P. 2017 - www.coursonline.be

198

Groupe(s) d'un utilisateur

- Le groupe permet de réunir les utilisateurs et n'avoir à gérer qu'une seule entité au lieu de plusieurs
- L'utilisateur hérite des droits et des permissions accordés au groupe
- Si certains droits ou permissions sont en conflit, généralement c'est la permission la plus restrictive qui est accordée

Groupe(s) d'un utilisateur

- Microsoft a intégré un certains nombres de groupes prédéfinis comme Administrateurs du domaine ou Utilisateurs du domaine
- Il est bien sur possible de créer de nouveaux groupes et de les placer dans une OU par exemple
- Deux types de groupes sont définis:
 - De sécurité: prévu pour gérer des éléments de sécurité comme les permissions
 - De distribution: pour réunir des personnes, pour envoyer des mails par exemple

Stratégies d'utilisation des utilisateurs et des groupes

- Dans la philosophie Microsoft, dans le cas d'un domaine, il y a deux sortes de groupes;
 - Les groupes globaux: qui contiennent les utilisateurs
 - Les groupes locaux: sur lesquels les permissions sont appliquées
- Pour obtenir des permissions, les groupes globaux doivent être mis dans des groupes locaux

©Hainaut P. 2017 - www.coursonline.be

201

Portée des différents groupes

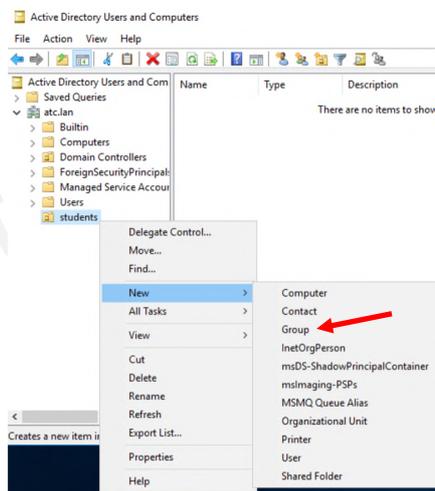
Groupe	Type	Portée	Stocké sur	Utilisé pour gérer des
Local	Sécurité	Ordinateur local	Ordinateur local SAM	Utilisat. et des perm. dans des workgroup ou des perm. dans une AD
Local de domaine	Sécurité ou distribution	Domaine AD	Partition de domaine AD	Ressources AD
Global	Sécurité ou distribution	Forêt AD	Partition de domaine AD	Utilisateurs de dom. AD
Universel	Sécurité ou distribution	Forêt AD	Catalogue global AD	Utilisat. ou des grp globaux dans une forêt AD
Identité intégré de sécurité	Sécurité	Ordinateur local	Ordinateur local SAM	Droits et des permissions

©Hainaut P. 2017 - www.coursonline.be

202

Gestion des groupes

- Création d'un groupe:
 - Dans les outils d'administration -> Utilisateurs et ordinateurs AD
 - Ouvrez ou créez une OU
 - Cliquez avec le bouton droit sur ce conteneur et choisissez Nouveau puis Groupe

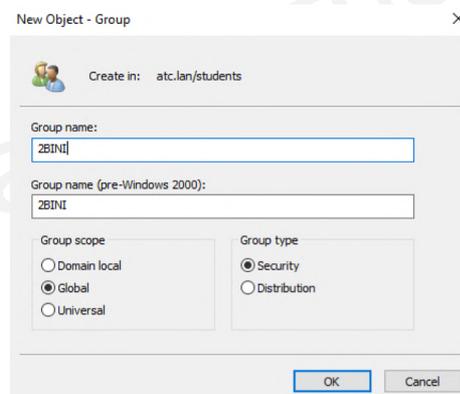


©Hainaut P. 2017 - www.coursonline.be

203

Gestion des groupes

- Création d'un groupe:
 - Tapez le nom du groupe et modifiez éventuellement le type et l'étendue du groupe



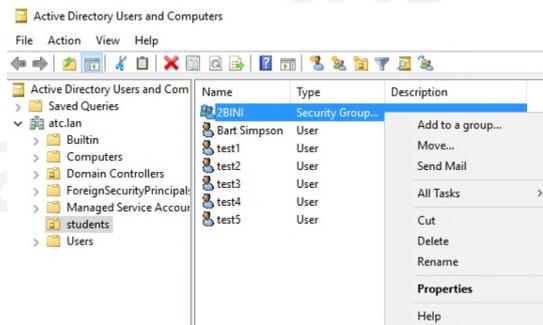
©Hainaut P. 2017 - www.coursonline.be

204

Gestion des groupes

- Modification d'un groupe:
 - Dans les outils d'administration -> Utilisateurs et ordinateurs AD

– Dans l'arborescence du domaine, cliquez avec le bouton droit sur votre groupe puis sur Propriétés

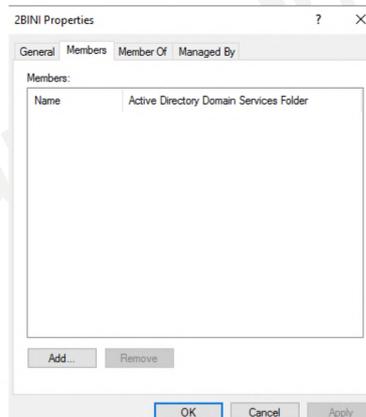


©Hainaut P. 2017 - www.coursonline.be

205

Gestion des groupes

- Modification d'un groupe:
 - Sur la page Membres, on peut ajouter ou enlever des utilisateurs ou d'autres groupes



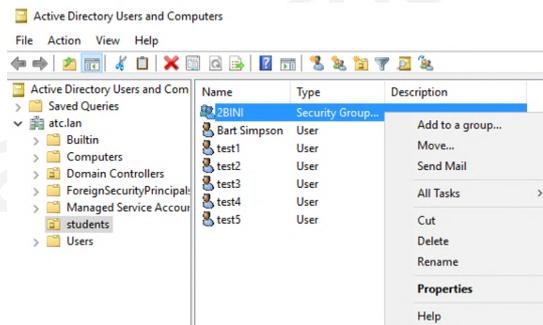
©Hainaut P. 2017 - www.coursonline.be

206

Gestion des groupes

- Suppression d'un groupe:
 - Dans les outils d'administration -> Utilisateurs et ordinateurs AD

– Dans l'arborescence du domaine, cliquez avec le bouton droit sur votre groupe puis sur Effacer



©Hainaut P. 2017 - www.coursonline.be

207

Actions possibles sur un utilisateur

- A partir de la console Utilisateurs et ordinateurs AD, vous pouvez:
 - Activer ou désactiver un compte utilisateur
 - Réinitialiser son mot de passe
 - Déplacer ou supprimer un utilisateur
 - Ouvrir la page de démarrage de l'utilisateur
 - Envoyer un message si une adresse de messagerie a été définie
 - Ajouter un compte utilisateur à un groupe
- Etudiez ces différentes possibilités

©Hainaut P. 2017 - www.coursonline.be

208

9. Serveur Intranet

Introduction

- IIS10 (Internet Information Services) est la dernière version du serveur Web de Microsoft
- IIS10 permet d'héberger et de gérer la plupart des langages utilisés sur le Web, allant de l'ASP.net au PHP
- Il est rétro compatible avec les anciennes versions

Nouvelle architecture

- Les fonctionnalités d'IIS10 ont été découpées en modules chargeables selon les besoins
- Pour la partie Serveur Web:
 - Fonctionnalités HTTP communes (contenu statique, documents par défaut, ...)
 - Développement d'applications (ASP, CGI, ...)
 - Intégrité et diagnostics (journalisation, suivi, ...)
 - Sécurité (authentification, autorisations, ...)
 - Performances (compression de contenu)

Nouvelle architecture

- Pour la partie Outils de gestion:
 - Console de gestion IIS
 - Scripts et outils de gestion
 - Service de gestion
 - Gestion de la compatibilité avec IIS6
- Le service FTP (File Transfert Protocol) est séparé de la partie Serveur Web, c'est un rôle à part entière

Nouvelle administration

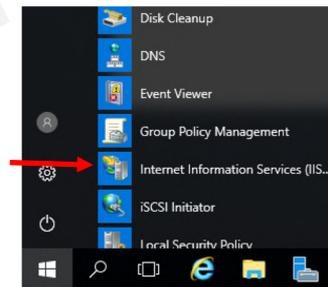
- La configuration est découpée en plusieurs XML:
 - applicationHost.config contient la config. Globale (liste des sites, paramètres par défaut, ...)
 - redirection.config contient les infos de redirection (site sur un autre serveur, maintenance, ...)
 - web.config contient la config globale ASP.net du serveur
 - machine.config contient les propriétés requises pour les fonctionnalités Framework

Installation du rôle Serveur Web IIS

- Le rôle a déjà été installé précédemment, si pas rendez vous dans le Gestionnaire de serveur, ajoutez le rôle de serveur Web (IIS)
- Ajouter les fonctionnalités requises
- Laissez les options d'installations par défaut et cliquez sur Installer
- Après installation, pour vérifier que IIS est bien opérationnel, ouvrez un navigateur et tapez: `http://localhost`

Création et configuration d'un site

- Les fichiers des sites web se trouvent par défaut dans `c:\inetpub\wwwroot`
- Nous allons créer ici un site statique basique répondant au nom de domaine `info.lan`
- Créez un répertoire `info.lan` dans le dossier `wwwroot`
- Dans les outils d'administration, cliquez sur le Gestionnaire de services Internet (IIS)

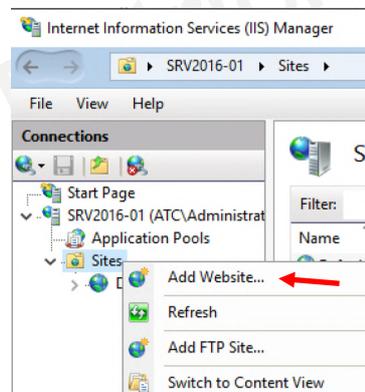


©Hainaut P. 2017 - www.coursonline.be

215

Création et configuration d'un site

- Déroulez l'arborescence et au niveau de l'onglet Sites, cliquez avec le bouton droit, puis ajoutez un site Web



©Hainaut P. 2017 - www.coursonline.be

216

Création et configuration d'un site

- Remplissez les champs puis validez:
 - Nom du site
 - Chemin d'accès
 - Nom de l'hôte

©Hainaut P. 2017 - www.coursonline.be 217

Création et configuration d'un site

- Il vous faut un document à afficher dans votre site
- Créez le document suivant (notepad):

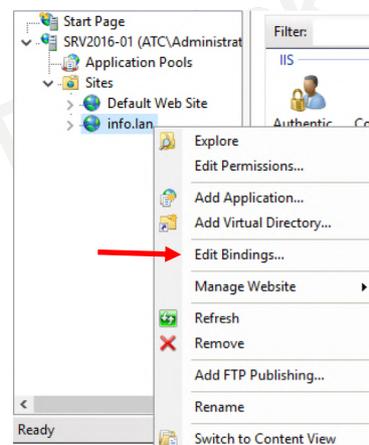
```
<HTML>
<head>
  <title>Site de la section Info</title>
</head>
<body>
  Ceci est mon premier site affiché par IIS10
</body>
</HTML>
```
- Enregistrez le dans c:\inetpub\wwwroot\info.lan\default.htm

Création et configuration d'un site

- Remarques:
 - Apache cherche par défaut le fichier index.html, ou index.php
 - IIS cherche par défaut le fichier default.htm d'où le choix du nom de fichier
 - Pour l'instant, notre site répond sur <http://info.lan>, on va modifier la configuration du site pour qu'il puisse répondre aussi sur <http://www.info.lan>

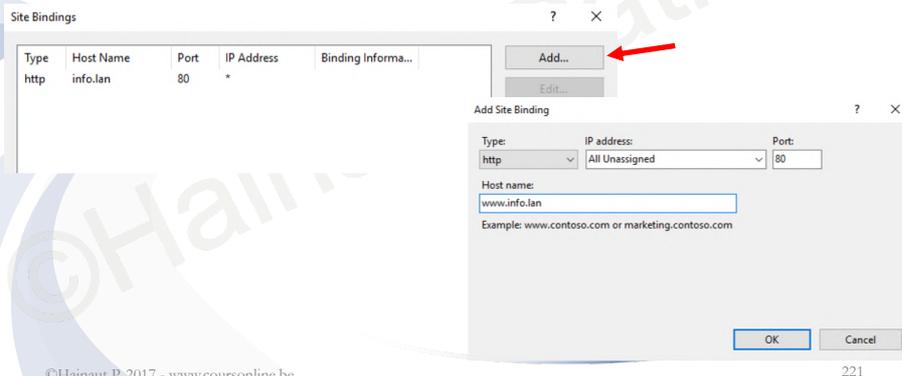
Création et configuration d'un site

- Allez dans la console Gestionnaire des services Internet (IIS)
- Développez l'arborescence Sites pour faire apparaître le site créé précédemment
- Cliquez avec le bouton droit sur le site puis cliquez sur Modifier les liaisons



Création et configuration d'un site

- Dans la fenêtre Liaisons de site, cliquez sur Ajouter
- Spécifiez comme nom d'hôte: info.lan et laissez le port 80

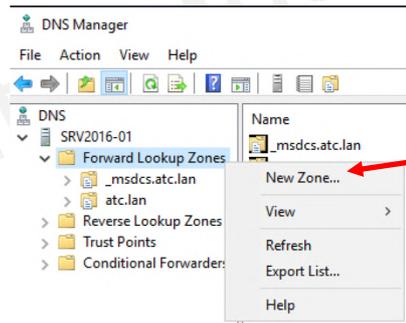


Mise à jour du domaine DNS

- Pour que notre site soit accessible du réseau local, il faut créer des zones dans notre serveur DNS, de façon à mettre en correspondance l'adresse IP locale du serveur (192.168.10.1) avec les noms de domaines
- Si on héberge plusieurs sites, ils auront tous la même IP et c'est le nom de domaine qui fera la différence et qui permettra d'afficher les bonnes pages
- Si on veut que le site soit accessible de l'extérieur, il faut réserver un nom de domaine valide (par exemple .be) et s'enregistrer auprès du service DNS correspondant (par exemple DNS Belgium)

Création d'une zone de recherche directe

- Dans les outils d'administration, cliquez sur DNS
- Dans le volet gauche, cliquez avec le bouton droit sur Zones de recherche directes, puis sur Nouvelle zone

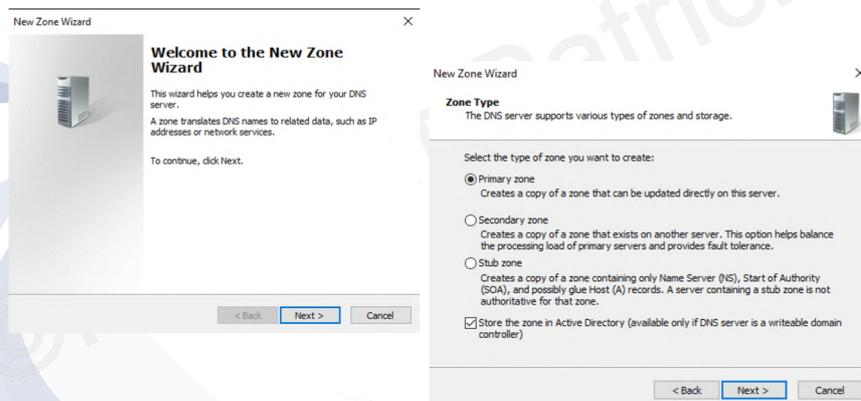


©Hainaut P. 2017 - www.coursonline.be

223

Création d'une zone de recherche directe

- Sur la page Type de zone, sélectionnez l'option Zone principale



©Hainaut P. 2017 - www.coursonline.be

224

Types de zone

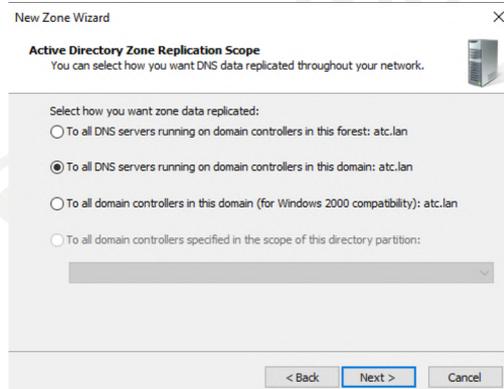
- Zone principale: permet de créer une zone DNS en lecture et écriture
- Zone secondaire: permet de créer une copie de la zone en lecture seule sur le serveur DNS
- Zone de stub: permet de créer une zone en lecture qui ne contient que les enregistrements SOA, NS et A correspondants aux enregistrements des serveurs DNS hébergeurs de la zone

©Hainaut P. 2017 - www.coursonline.be

225

Création d'une zone de recherche directe

- Sur la page Etendue de la zone de réplication AD, laissez les informations par défaut (la zone sera active sur tous les serveurs DNS du domaine)



©Hainaut P. 2017 - www.coursonline.be

226

Création d'une zone de recherche directe

- Sur la page Nom de la zone, tapez le nom DNS de la zone à créer, dans notre exemple, c'est info.lan

The screenshot shows the 'New Zone Wizard' dialog box with the 'Zone Name' step selected. The title bar reads 'New Zone Wizard'. The main heading is 'Zone Name' with the question 'What is the name of the new zone?'. Below this, there is explanatory text: 'The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.' A text input field contains 'info.lan'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

©Hainaut P. 2017 - www.coursonline.be

227

Création d'une zone de recherche directe

- Sur la page Mise à niveau dynamiques des enregistrements DNS, vous pouvez laisser par défaut, dans notre cas, ça n'a pas d'importance

- Le plus sûr est de ne pas accepter les mises à jour dynamiques

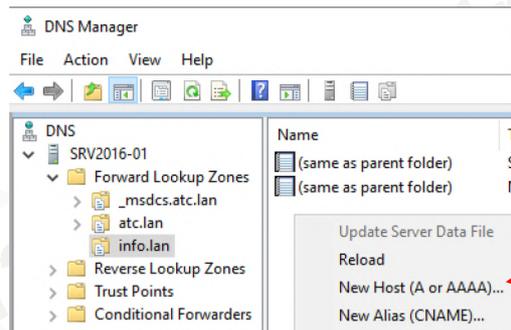
The screenshot shows the 'New Zone Wizard' dialog box with the 'Dynamic Update' step selected. The title bar reads 'New Zone Wizard'. The main heading is 'Dynamic Update' with the question 'You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.' Below this, there is explanatory text: 'Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur. Select the type of dynamic updates you want to allow:'. There are three radio button options: 1. 'Allow only secure dynamic updates (recommended for Active Directory) - This option is available only for Active Directory-integrated zones.' (selected). 2. 'Allow both nonsecure and secure dynamic updates - Dynamic updates of resource records are accepted from any client. This option is a significant security vulnerability because updates can be accepted from untrusted sources.' 3. 'Do not allow dynamic updates - Dynamic updates of resource records are not accepted by this zone. You must update these records manually.' At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. To the right, a smaller dialog box titled 'Completing the New Zone Wizard' is visible, showing the summary of settings: Name: info.lan, Type: Active Directory-Integrated Primary, Lookup type: Forward. It also includes a note: 'Note: You should now add records to the zone or ensure that records are updated dynamically. You can then verify name resolution using nslookup.' and a 'Finish' button.

©Hainaut P. 2017 - www.coursonline.be

228

Création d'un nouvel hôte dans la zone

- Cliquez avec le bouton droit dans la zone créée précédemment et cliquez sur Nouvel hôte

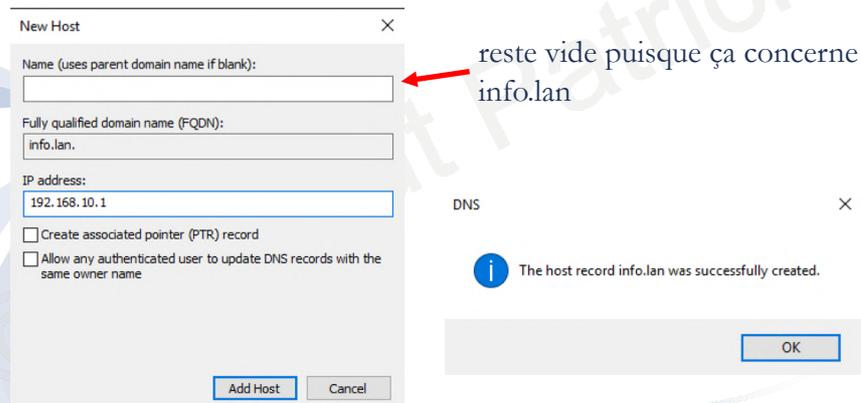


©Hainaut P. 2017 - www.coursonline.be

229

Création d'un nouvel hôte dans la zone

- On va lier le nom de domaine à l'adresse IP du serveur (du côté local, c'est pour cela qu'on parle d'intranet ...)



©Hainaut P. 2017 - www.coursonline.be

230

Création d'un nouvel hôte dans la zone

- On fait la même chose pour www (de cette façon, on pourra taper indifféremment <http://info.lan> ou <http://www.info.lan> dans un navigateur

The screenshot shows the Windows DNS Manager interface. A 'New Host' dialog box is open, allowing the user to add a new host record. The fields are filled with: Name (uses parent domain name if blank): www, Fully qualified domain name (FQDN): www.info.lan, and IP address: 192.168.10.1. There are checkboxes for 'Create associated pointer (PTR) record' and 'any authenticated user to update DNS records with the owner name'. The 'Add Host' button is highlighted. In the background, the DNS console shows the hierarchy: SRV2016-01 > Forward Lookup Zones > info.lan > www. The table below shows the existing records in the console:

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], srv2016-01.atc.lan, ho...
(same as parent folder)	Name Server (NS)	srv2016-01.atc.lan.
(same as parent folder)	Host (A)	192.168.10.1
www	Host (A)	192.168.10.1

©Hainaut P. 2017 - www.coursonline.be 231

Types d'enregistrement

- SOA: correspond à la source de l'autorité de la zone concernée. Toute modification incrémente un numéro de version associé
- NS: contient tous les serveurs de noms autorisés à répondre pour ce domaine
- A: définit l'adresse IP associée à un nom de machine
- CNAME: crée un alias dans une zone, qui pourra être associé à un enregistrement de type A
- PTR: est le pendant du type A. N'existe que dans les zones de recherche inversée
- MX: pointe sur un enregistrement de type A pour indiquer le serveur de messagerie

232

Test au moyen d'un navigateur

- Avant de tester, il faut actualiser les données du serveur DNS et du serveur Web
- Pour cela, dans les deux gestionnaires, cliquez avec le bouton droit sur le DC (DC01 dans notre exemple) puis sur Actualiser
- On peut dès lors tester notre site web au niveau d'un navigateur sur le serveur comme sur le PC client

Création d'une zone de recherche inversée (facultatif pour cette manip)

- Permet de résoudre des adresses IP en noms
- Dans les outils d'administration, cliquez sur DNS
- Dans le volet gauche, cliquez avec le bouton droit sur Zones de recherche inversée, puis sur Nouvelle zone
- Sur la page Type de zone, sélectionnez l'option Zone principale. Enregistrez la zone dans l'AD

Création d'une zone de recherche inversée

- Sur la page Etendue de la zone de réplication AD, laissez les informations par défaut
- Sur la page Nom de la zone, sélectionnez l'adressage IPv4 et tapez l'ID réseau
- Sur la page Mise à niveau dynamiques des enregistrements DNS, vous pouvez les interdire

Exercice d'application

- Soit à rendre notre serveur intranet, qui accepte des sites statiques, compatible avec les sites dynamiques
- Vous devez en fait, jouer le rôle d'un provider comme OVH qui vous propose un espace serveur gérant le PHP et MySQL, un outil de gestion de bases de données comme PHPmyAdmin, et un support FTP pour le transfert de vos fichiers

Exercice d'application

- Donc, du côté serveur, il faut installer:
 - Un serveur FTP pour que le client puisse "uploader ses fichiers", serveur FTP qui doit pointer vers le répertoire où vont se trouver les fichiers du site Web dynamique
 - Un serveur MySQL pour prendre en charge la base de données du site client
 - Un serveur PHP qui permettra d'interroger la base de données
 - PHPmyAdmin qui permettra de gérer la base de données client
- Pour cela, trouvez les outils nécessaires ... (Google)
Remarque: EasyPHP ou WAMP ne sont pas des outils adaptés ! (outils client ...)
- Et vous devrez désactiver la sécurité accrue du navigateur Web pour télécharger ce qu'il faut ... (gestionnaire de serveur)

Exercice d'application

- Du côté client, il faut:
 - "Uploader" les fichiers sur le serveur via un client FTP (Filezilla, FlashFXP, ...) qui se connectera à votre serveur FTP suivant la façon dont vous l'avez configuré ...
 - Vous rendre sur le site, à partir du PC client où vous devrez voir apparaître la page d'installation du site JOOMLA
 - Installer JOOMLA (voir présentation sur le sujet ou présentation sur LAMP)
 - Enlever via FTP le répertoire **Installation**
 - Vérifier avec PHPmyAdmin que la base de données est bien créée

Remarque

- Ce qui vient d'être vu pour un intranet, par facilité (adresses IP privées et noms de domaine fictifs), peut être adapté facilement à un serveur Web actif sur Internet
- Il suffit d'avoir une IP publique fixe sur ce serveur et de faire correspondre cette adresse IP à des noms de domaines loués et enregistrés auprès de providers

NOTIONS COMPLEMENTAIRES

10. Impression

Terminologie

- **Imprimante:** file d'attente (zone tampon), partie logique du périphérique d'impression
- **Périphérique d'impression:** imprimante physique, locale ou réseau
- **Impression locale:** impression à partir d'un poste client sur une imprimante directement raccordée à cette station (USB, //, série,...)
Disponibilité si le poste client est allumé
- **Impression réseau:** impression à partir d'un serveur d'impression dont l'imprimante peut être raccordée localement ou via le réseau
Disponibilité toujours assuré

Terminologie

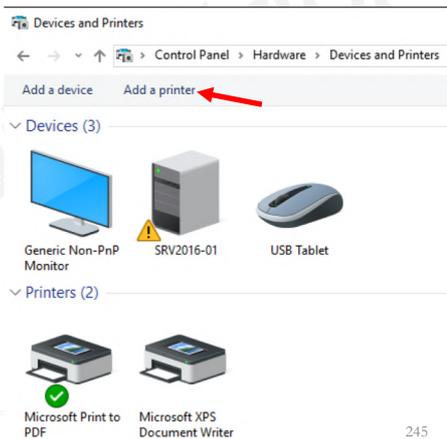
- **Serveur d'impression:** se compose d'un spouleur d'impression, d'imprimantes, de pilotes d'imprimantes et du processeur d'impression. Gère les imprimantes et les files d'attente
- **Pilote d'imprimante:** interface logicielle qui permet de gérer et d'imprimer sur un périphérique d'impression. Chez microsoft, les pilotes sont gérés et distribués par le serveur d'impression lorsqu'un ordinateur client se connecte

Terminologie

- **Spouleur d'impression:** zone du disque où sont stockés les fichiers prêts à être imprimés. Par défaut, c'est
`%systemroot%\system32\spool\printers`
- **Processeur d'impression:** gère la manière dont les documents sont envoyés à l'impression (ordre, ordre des pages,...)

Imprimante locale

- L'ajout d'une imprimante locale se fait de façon traditionnelle via le panneau de configuration/Matériel/Périphériques et Imprimante /Ajouter une imprimante

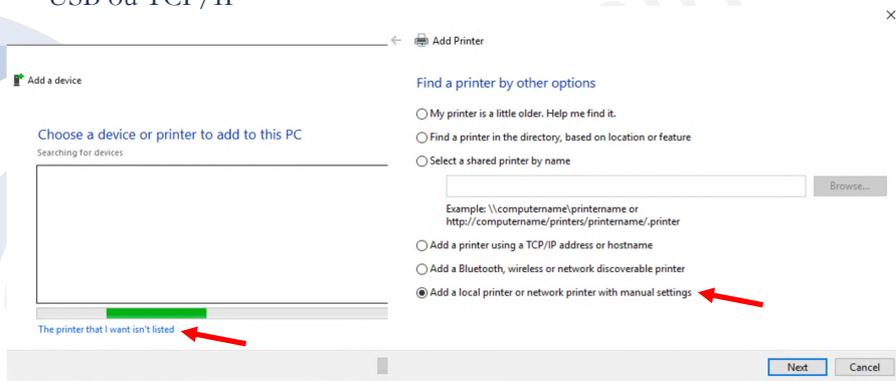


©Hainaut P. 2017 - www.coursonline.be

245

Imprimante locale

- Vous pouvez interrompre la recherche automatique en cliquant sur le lien en bas de fenêtre
- Vous pouvez prendre la dernière option qui convient à une imprimante USB ou TCP/IP



©Hainaut P. 2017 - www.coursonline.be

246

Imprimante locale

- Pour une imprimante USB, on choisira d'utiliser un port existant et on sélectionnera le port correspondant
- Pour une imprimante réseau, on créera un nouveau port, et comme type de port, on prendra un port TCP/IP standard

Choose a printer port

A printer port is a type of connection that allows your computer to exchange information with a printer.

Use an existing port: LPT1: (Printer Port)

Create a new port:

Type of port: Local Port, Local Port, Standard TCP/IP Port

Next Cancel

©Hainaut P. 2017 - www.coursonline.be

247

Imprimante locale

- Si c'est une imprimante réseau, une fenêtre permettant de renseigner l'adresse IP de l'imprimante apparaît
- On peut désactiver la recherche automatique de l'imprimante

Type a printer hostname or IP address

Device type: TCP/IP Device

Hostname or IP address: 192.168.10.5

Port name: 192.168.10.5

Query the printer and automatically select the driver to use

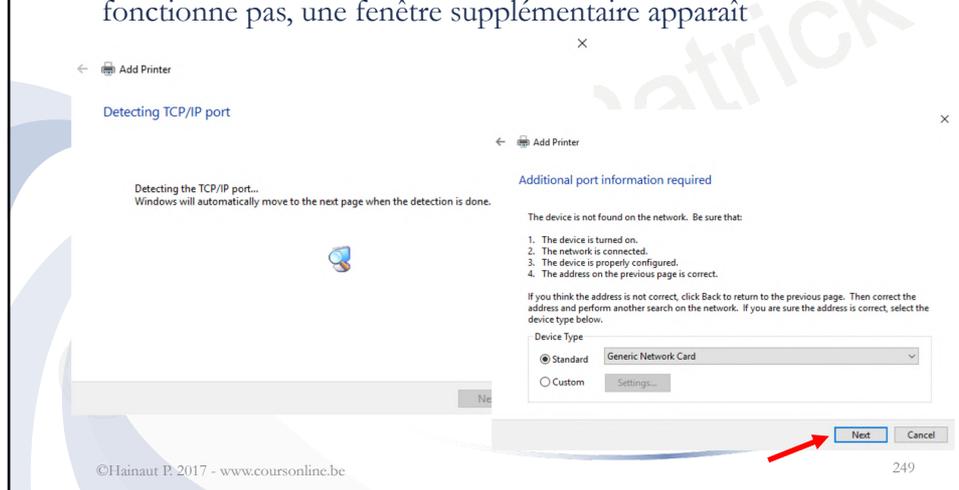
Next Cancel

©Hainaut P. 2017 - www.coursonline.be

248

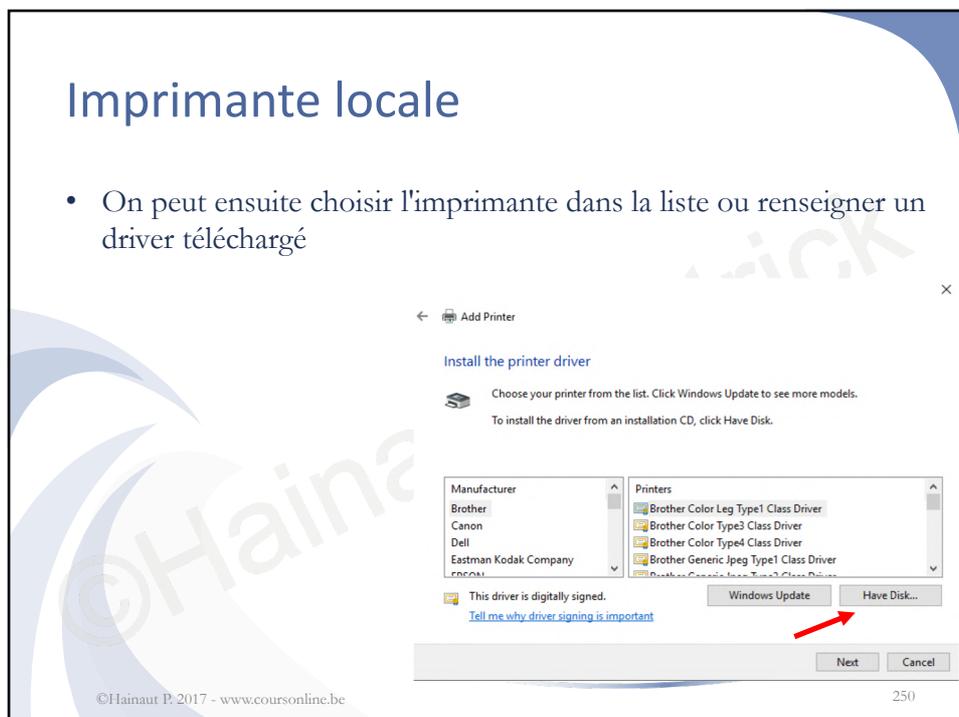
Imprimante locale

- Le système essaie de détecter le port de l'imprimante, et si ça ne fonctionne pas, une fenêtre supplémentaire apparaît



Imprimante locale

- On peut ensuite choisir l'imprimante dans la liste ou renseigner un driver téléchargé



Imprimante locale

- On peut décider ensuite si l'imprimante sera partagée ou non sur le réseau
- Si c'est une imprimante USB, ça peut être intéressant, mais pas dans le cas d'une imprimante TCP/IP

← Add Printer ×

Printer Sharing

If you want to share this printer, you must provide a share name. You can use the suggested name or type a new one. The share name will be visible to other network users.

Do not share this printer

Share this printer so that others on your network can find and use it

Share name:

Location:

Comment:

Next Cancel

©Hainaut P. 2017 - www.coursonline.be

251

Imprimante locale

- Il reste à indiquer si l'imprimante doit être utilisée par défaut et éventuellement imprimer une page de test

← Add Printer ×

You've successfully added HP Color LaserJet A3/11x17 PCL6 Class Driver

Set as the default printer

To check if your printer is working properly, or to see troubleshooting information for the printer, print a test page.

Print a test page

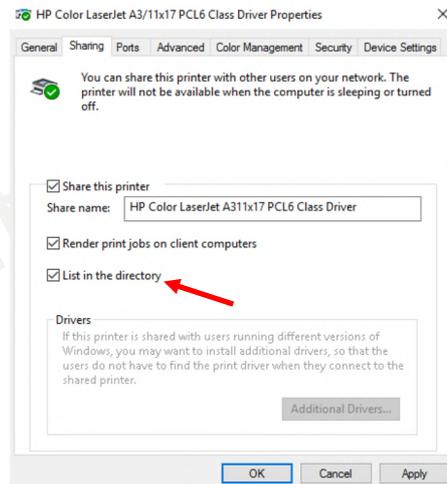
Finish Cancel

©Hainaut P. 2017 - www.coursonline.be

252

Publication d'une imprimante dans l'AD

- Dans les propriétés d'une imprimante donnée, on trouve dans l'onglet partage l'option Lister dans l'annuaire
- Si on l'active (facultatif), il est, dès lors, possible de rechercher cette imprimante dans l'AD



©Hainaut P. 2017 - www.coursonline.be

253

Configuration et gestion d'une imprimante

- Au niveau du panneau de configuration, section imprimantes, en cliquant avec le bouton droit au niveau d'une imprimante donnée, on accède aux propriétés de l'imprimante
- Onglet général:
 - Nom, emplacement et commentaire
 - Le bouton Options d'impression permet de modifier la façon dont le périphérique d'impression va travailler. Il vaut mieux créer plusieurs imprimantes disposant chacune de paramètres spécifiques comme couleur ou n&b
 - Le bouton Imprimer une page de test permet de tester le bon fonctionnement de l'imprimante

©Hainaut P. 2017 - www.coursonline.be

254

Configuration et gestion d'une imprimante

- Onglet partage:
 - La case à cocher Partager cette imprimante active le partage avec les paramètres par défaut
 - Evitez les espaces dans le nom de l'imp. Partagé
 - L'option Rendu des travaux d'impression sur les ordinateurs clients indique si une partie du travail de préparation se fait sur l'ordinateur client
 - Le bouton Pilotes supplémentaires permet d'ajouter des pilotes pour les autres OS Microsoft utilisés

©Hainaut P. 2017 - www.coursonline.be

255

Configuration et gestion d'une imprimante

- Onglet Ports:
 - Cet onglet affiche la liste des ports disponibles actuellement sur le serveur d'impression, leur description et s'ils sont rattachés à une imprimante
 - Le bouton Ajouter un port permet d'ajouter un port local, TCP/IP ou un autre type de port
 - Le bouton Supprimer un port permet de supprimer le port sélectionné sauf les ports par défaut
 - Le bouton configurer le port permet éventuellement de modifier les paramètres pour le port sélectionné
 - L'option Activer la gestion du mode bidirectionnel permet également au périphérique d'impression de communiquer avec l'imprimante
 - L'option Activer le pool d'imprimante permet de grouper plusieurs périphériques d'impression identiques

©Hainaut P. 2017 - www.coursonline.be

256

Configuration et gestion d'une imprimante

- Onglet Avancé:
 - Permet de définir des horaires d'impression, des priorités, des fonctionnalités avancées, ...
 - Expérimentez-les
- Onglet Gestion des couleurs
 - Permet de définir, pour chaque périphérique d'impression, des profils pour gérer les couleurs et donner le meilleur rendu possible

Configuration et gestion d'une imprimante

- Onglet Sécurité:
 - Permet de gérer les permissions applicables aux imprimantes
 - Le mieux est de restreindre au maximum les droits des utilisateurs
 - Par défaut, Tout le monde a la permission d'imprimer
 - Les administrateurs, les opérateurs de serveur et d'impression ont tous les droits sur le serveur d'impression
 - Expérimenter les différentes possibilités

Configuration et gestion d'une imprimante

- Onglet paramètres du périphérique:
 - Cet onglet est réservé pour configurer des paramètres propres à l'imprimante définis par le fabricant
 - Pour éviter que les utilisateurs ne modifient ces paramètres, il est conseillé de créer plusieurs imprimantes, chacune correspondant à une catégorie d'utilisateurs

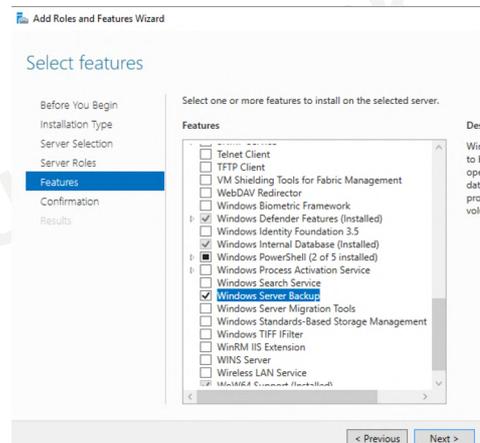
11. Sauvegarde et Restauration

Introduction

- Un fichier corrompu, un disque qui tombe en panne, sont des exemples de problèmes courants et pour se prémunir contre ce type de risque, il est nécessaire de copier les données sur un autre emplacement
- L'utilitaire dédié est Windows Server Backup
- Un utilitaire en ligne de commande existe: wbadmin
- Windows requiert un disque dédié à la sauvegarde
- Ce disque peut être un disque externe USB ou Firewire, un volume du disque, un média amovible

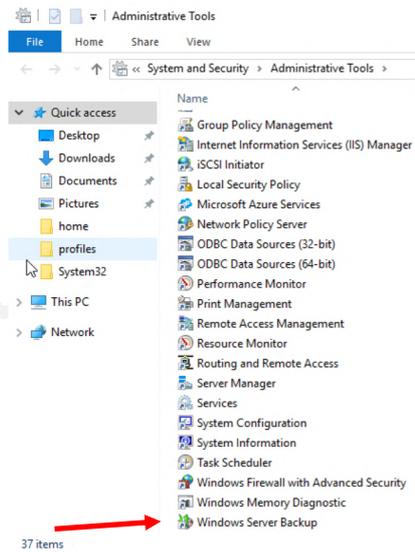
Mise en œuvre

- Installation de la fonctionnalité de sauvegarde:
 - A partir du Gestionnaire de serveur, installez la fonctionnalité Windows Server Backup



Mise en œuvre

- Un nouvel outil apparaît dans les outils d'administration

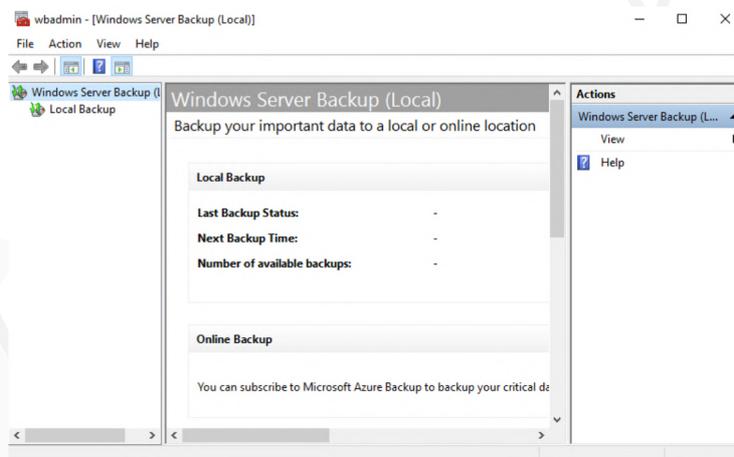


©Hainaut P. 2017 - www.coursonline.be

263

Mise en œuvre

- Interface:

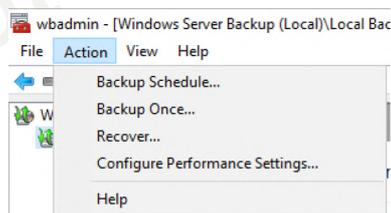


©Hainaut P. 2017 - www.coursonline.be

264

Mise en œuvre

- Les seules opérations possibles sont:
 - La planification de la sauvegarde
 - La sauvegarde manuelle unique
 - La configuration des paramètres de performances
 - La récupération

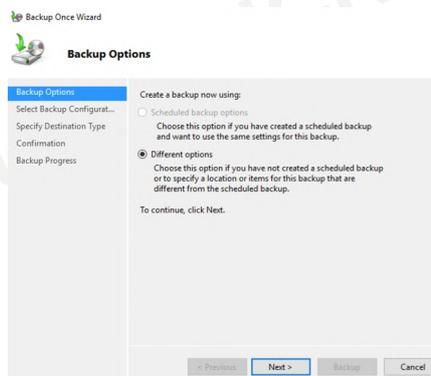


©Hainaut P. 2017 - www.coursonline.be

265

Création d'une sauvegarde

- Création d'une sauvegarde manuelle unique:
 - Dans le volet de droite (ou dans le menu Action), cliquez sur Sauvegarde unique
 - Parcourez les pages Options de sauvegarde, Sélectionner la configuration..., Spécifier le type de destination,
 - Spécifier une option avancée pour configurer votre sauvegarde
 - Sur la page Confirmation, relisez les infos et cliquez sur Sauvegarder



©Hainaut P. 2017 - www.coursonline.be

266

Création d'une sauvegarde

- Planification de sauvegarde:
 - Dans le volet de droite, cliquez sur Planification de sauvegarde
 - Parcourez les différentes pages afin de spécifier les différentes options dont l'heure et la fréquence de sauvegarde, ainsi que la destination
 - Sur la page Confirmation, relisez les infos et cliquez sur Terminer

Création d'une sauvegarde

- Configuration des paramètres de performances:
 - Dans le volet de droite, cliquez sur Configurer les paramètres de performance
 - Vous pouvez choisir entre la sauvegarde complète et les sauvegardes incrémentielles afin de réduire le temps de sauvegarde

Restauration d'une sauvegarde

- Récupération des données:
 - Dans le volet de droite, cliquez sur Récupérer
 - Sur la page Démarrer, sélectionnez l'emplacement de la sauvegarde
 - Sur la page suivante, sélectionnez la date et l'heure de la sauvegarde à utiliser
 - Sur la page Sélectionnez le type de récupération, sélectionnez Fichiers et dossiers, Applications ou Volumes

Restauration d'une sauvegarde

- Récupération du système d'exploitation:
 - Vous pouvez récupérer l'OS (et les applications installées), ce qui suppose que la taille des disques est importante et au moins égale à la taille des disques de l'ancien système
 - Démarrer votre serveur à l'aide du DVD d'installation
 - Spécifiez les paramètres de langue et sélectionnez Réparer votre ordinateur
 - Sur la page Options de récupération système, sélectionnez l'OS
 - Sur la page Choisir un outil de récupération -> Restauration de l'ordinateur Windows -> sélectionnez la sauvegarde
 - Sur la page Choisissez comment restaurer..., choisissez les options de restauration

12. Accès aux fichiers

Introduction

- La gestion des fichiers et des dossiers est un des points les plus sensibles dans une entreprise
- Les données sont en effet primordiales et doivent être protégées contre la destruction et l'accès non-autorisé, accidentels ou pas
- Il faut de plus limiter l'espace à disposition des utilisateurs sous peine de se retrouver avec une masse impressionnante de données sur le serveur

12a. Permissions NTFS

Permissions NTFS

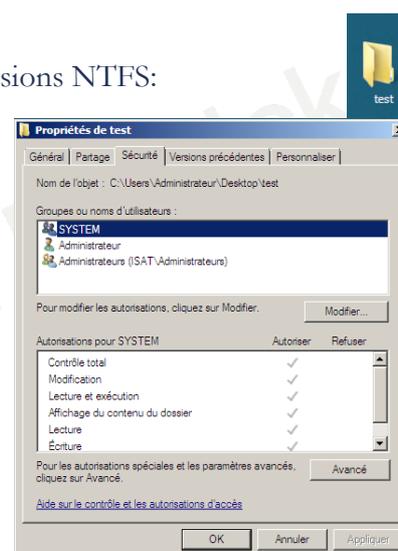
- Les permissions NTFS permettent de protéger les fichiers d'un système Windows contre des accès non-autorisés
- Windows utilise les permissions NTFS basées sur les DACLs (Discretionary Access Control List) pour protéger les dossiers et les fichiers
- A chaque objet est affectée une liste appelée ACL (Access Control List)

Permissions NTFS

- L'ACL se compose de descripteurs de sécurité ACE (Access Control Entry)
- Chaque ACE définit une décision pour un utilisateur ou un groupe; autorisation ou refus

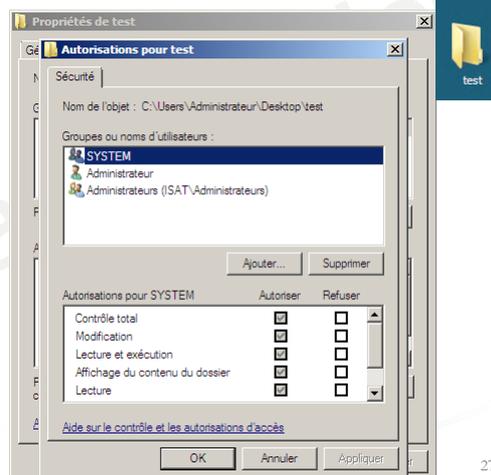
Permissions NTFS

- Pour afficher et modifier les permissions NTFS:
 - Connectez-vous en tant qu'administrateur
 - Ouvrez l'explorateur Windows et déplacez-vous jusqu'à l'objet dont vous voulez afficher les permissions
 - Cliquez avec le bouton droit sur l'objet, puis sur Propriétés
 - Cliquez sur l'onglet Sécurité



Permissions NTFS

- Si vous cliquez sur Modifier, vous pouvez changer les permissions actuelles

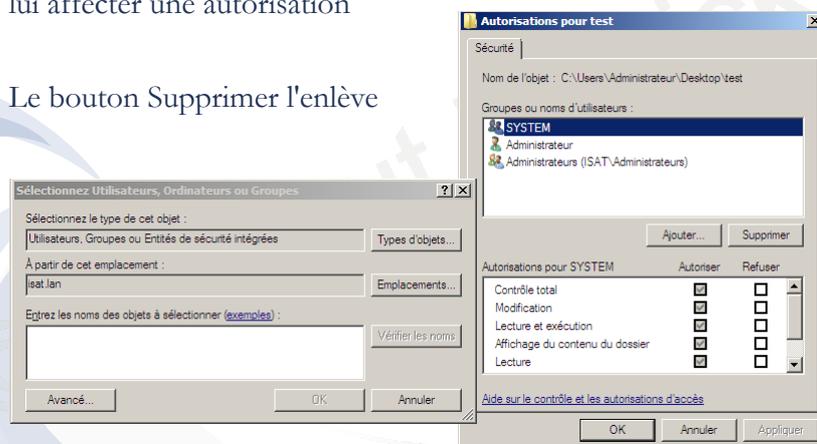


©Hainaut P. 2017 - www.coursonline.be

277

Permissions NTFS

- Le bouton Ajouter permet d'ajouter un groupe ou un utilisateur pour lui affecter une autorisation
- Le bouton Supprimer l'enlève

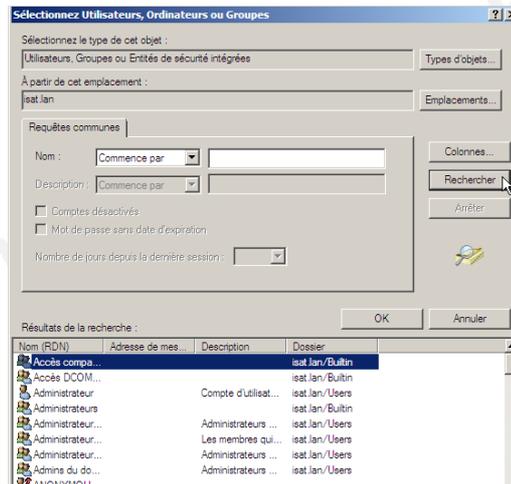


©Hainaut P. 2017 - www.coursonline.be

278

Permissions NTFS

- En cliquant sur **Avancé...** puis sur **Rechercher**, on peut récupérer la liste des utilisateurs de l'ordinateur

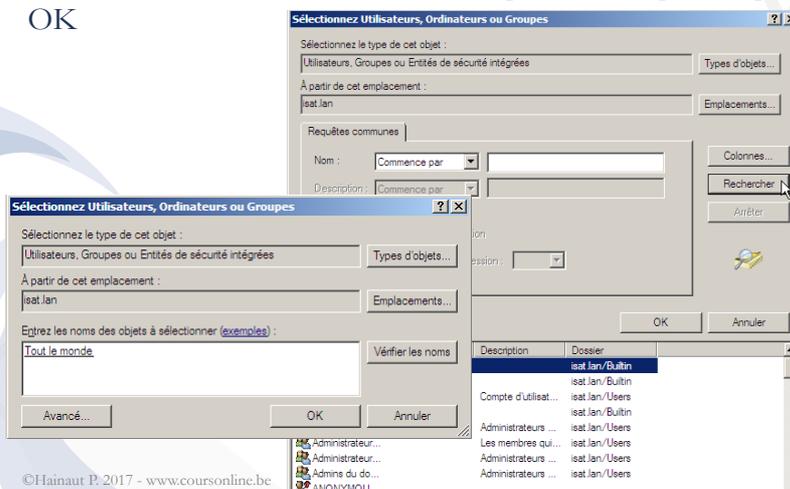


©Hainaut P. 2017 - www.coursonline.be

279

Permissions NTFS

- Une fois l'utilisateur choisi, double-cliquez dessus, puis cliquez sur **OK**

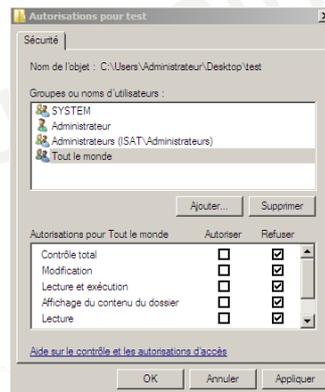


©Hainaut P. 2017 - www.coursonline.be

280

Permissions NTFS

- L'utilisateur est alors ajouté à la liste
- Attention, un refus explicite est prioritaire par rapport à une autorisation (ce qui n'est pas le cas du refus implicite)



©Hainaut P. 2017 - www.coursonline.be

281

Permissions NTFS

- Testez l'influence de ces permissions avec plusieurs comptes utilisateurs
- attention que, par défaut, seuls des utilisateurs appartenant au groupe des administrateurs peuvent ouvrir une session sur le contrôleur de domaine
Point de vue sécurité, il est normal qu'il en soit ainsi, le DC étant un élément critique du domaine
- Juste pour le test, comment pourriez-vous permettre aux utilisateurs du domaine d'ouvrir une session en local sur le DC ? (attention à ne pas mettre en production ...)

©Hainaut P. 2017 - www.coursonline.be

282

12b. Partage de fichiers

Les partages

- Un partage est un point d'entrée réseau pour accéder à des ressources de type fichier sur un serveur
- Un dossier peut correspondre à plusieurs points de partage nommés différemment et disposant de permissions différentes

Les partages

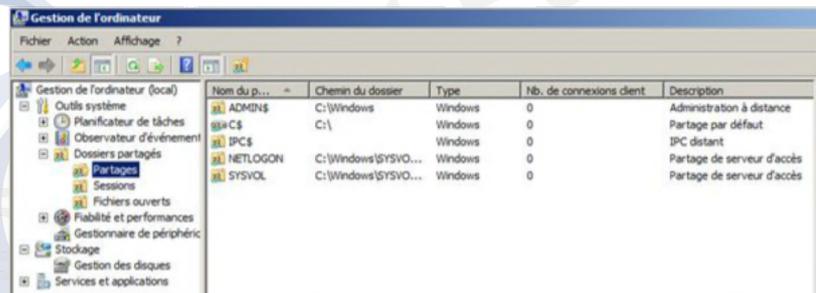
- L'accès au dossier partagé utilise un chemin UNC (Universal Convention Name) de syntaxe suivante:
\\NomDuServeur\NomDuPartage ou
\\NomDuServeur\DossierPartagé\Ressource
- Si on ajoute un caractère \$ à la fin du partage, celui-ci n'apparaîtra pas dans la liste des partages

Les partages

- Le déplacement d'un dossier partagé supprime le partage
- Il existe de multiples façon de créer un partage. Nous en développerons une ...

Les partages

- Création d'un partage via l'outil Gestion de l'ordinateur:
 - Connectez-vous en tant qu'administrateur
 - Démarrer -> Outils d'administration -> Gestion de l'ordinateur
 - Dans le volet gauche, cliquez sur le nœud Dossiers partagés



©Hainaut P. 2017 - www.coursonline.be

287

Les partages

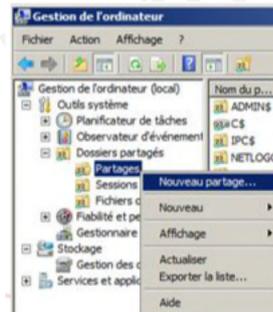
- Le nœud Partages affiche tous les partages de l'ordinateur
- Le nœud Sessions affiche les utilisateurs actuellement connectés sur les dossiers partagés
- Le nœud Fichiers ouverts affiche des informations sur les fichiers actuellement ouverts

©Hainaut P. 2017 - www.coursonline.be

288

Les partages

- Cliquez avec le bouton droit sur Partages puis cliquez sur Nouveau Partage
- Sur la page Assistant création d'un dossier partagé, lisez les infos puis cliquez sur Suivant

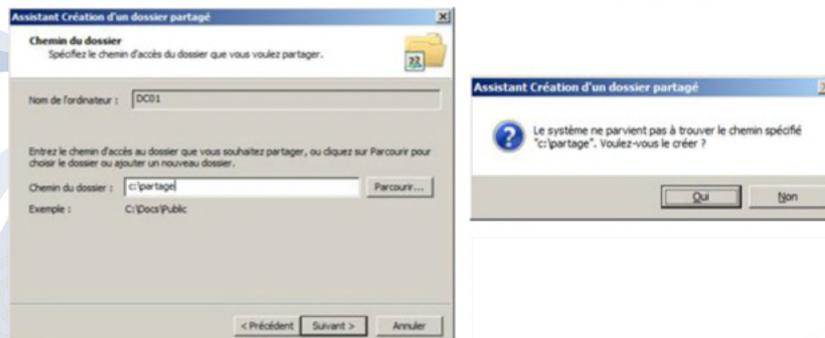


©Hainaut P. 2017 - www.coursonline.be

289

Les partages

- Sur la page Chemin du dossier, recherchez l'emplacement du dossier à partager
- S'il n'existe pas, le système proposera de le créer

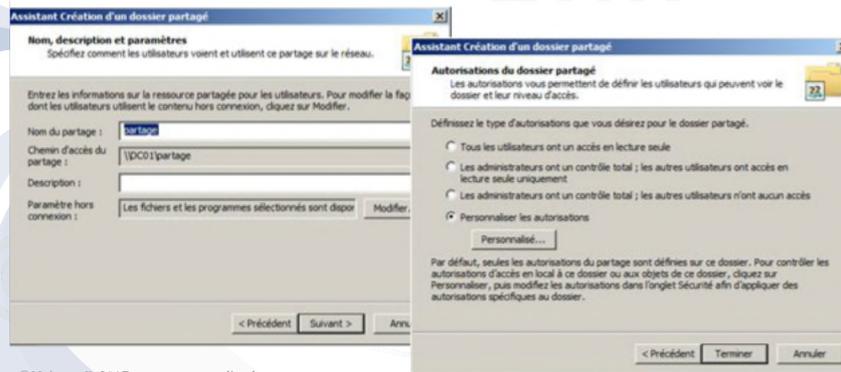


©Hainaut P. 2017 - www.coursonline.be

290

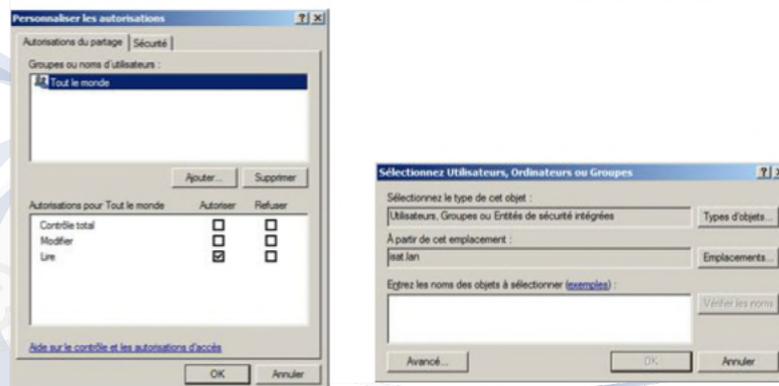
Les partages

- Le nom de partage peut être modifié et sur la page suivante, on peut choisir les autorisations d'accès
- ... le plus souplement, en cliquant sur Personnalisé ...



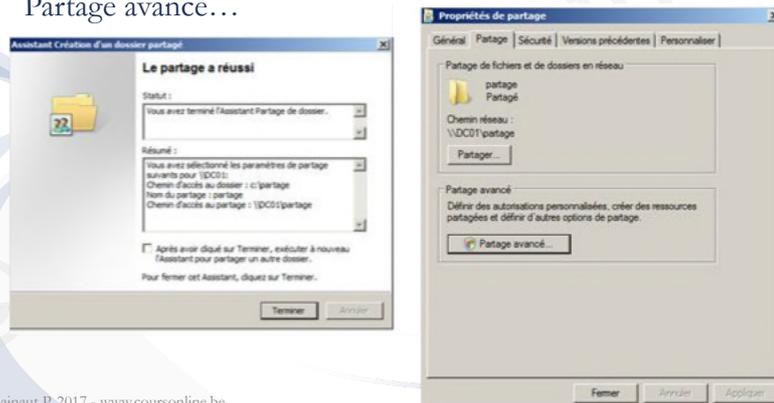
Les partages

- On peut modifier les permissions pour les utilisateurs existants ou en ajouter d'autres en cliquant sur Ajouter ...
- Ca se passe ensuite de manière similaire aux diapos 224 à 226



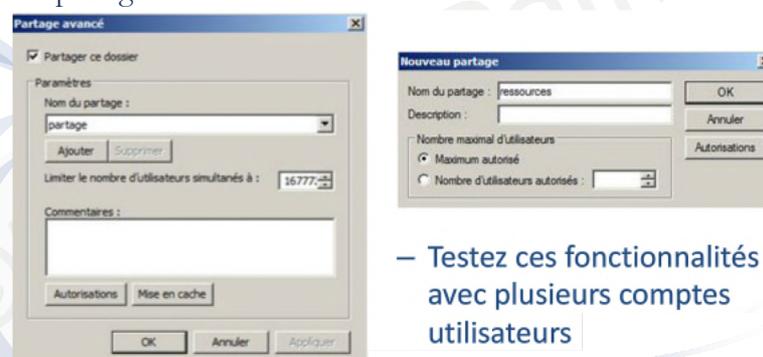
Les partages

- Une fois le partage effectué, on peut modifier celui-ci en cliquant avec le bouton droit de la souris sur le dossier partagé et en sélectionnant propriétés, puis l'onglet partage et finalement Partage avancé...



Les partages

- Vous pouvez modifier le nom de partage ou en ajouter un autre, sur lequel vous pourrez spécifier d'autres autorisations, différentes de celles précisées pour le premier nom de partage



12c. Gestion des quotas

Mise en œuvre des quotas

- Pour éviter que quelques utilisateurs occupent tout l'espace disponible, il est possible de restreindre l'espace disque par utilisateur à l'aide des quotas
- L'activation des quotas s'appliquent à tous les fichiers déjà créés de tous les utilisateurs, donc prudence...

Mise en œuvre des quotas

- Activation des quotas:
 - Connectez-vous en tant qu'administrateur
 - Ouvrez l'explorateur Windows et cliquez avec le bouton droit sur le disque sur lequel vous voulez activer les quotas -> Propriétés -> Quota -> activer la gestion de quota
 - La case à cocher Refuser de l'espace disque ... garantit que l'utilisateur ne peut pas dépasser l'espace qui lui est alloué

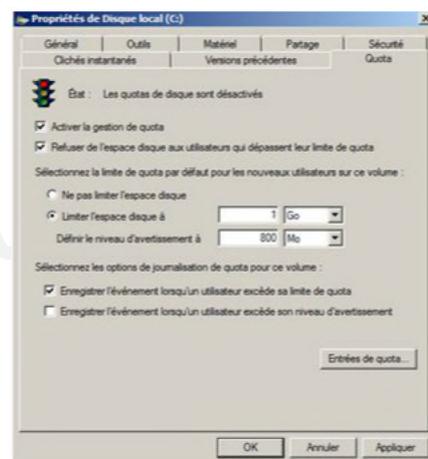


©Hainaut P. 2017 - www.coursonline.be

297

Mise en œuvre des quotas

- L'option de limite du quota par défaut définit un quota pour tous les utilisateurs, en spécifiant un niveau d'alerte et un niveau maximum
- Les cases à cocher Enregistrer l'événement... permettent d'ajouter un événement dans le journal des événements
- Le bouton Entrées de quota permet de définir un quota pour un utilisateur, différent du quota par défaut

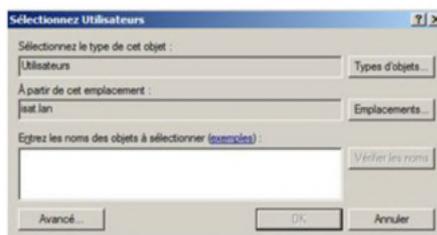
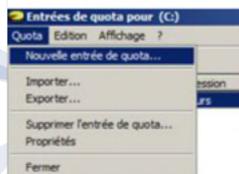


©Hainaut P. 2017 - www.coursonline.be

298

Mise en œuvre des quotas

- En cliquant sur Quota puis Nouvelle entrée de Quota..., on peut spécifier un utilisateur (voir dias 224 à 226)

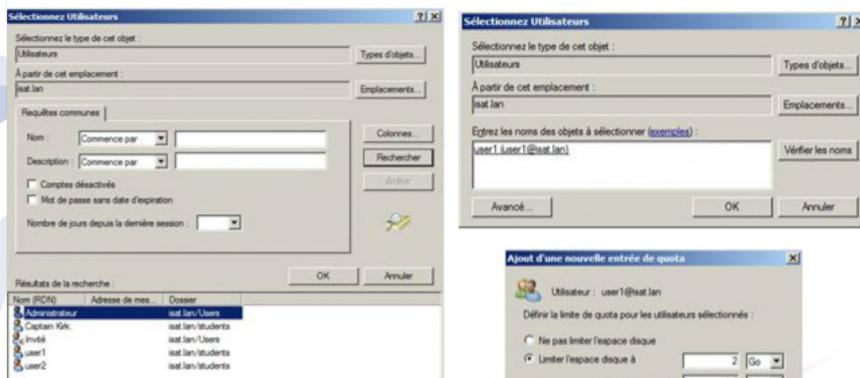


©Hainaut P. 2017 - www.coursonline.be

299

Mise en œuvre des quotas

- Une fois l'utilisateur choisi, on peut spécifier la limite d'espace personnalisée



©Hainaut P. 2017 - www.coursonline.be

300

13. Stratégies de Groupe

Introduction

- La stratégie de groupe ou GPO (Group Policy Object) est sûrement le meilleur compromis pour canaliser les besoins des utilisateurs
- Une stratégie de groupe est un ensemble de paramètres formant une règle s'appliquant automatiquement à des utilisateurs ou à des groupes placés à l'intérieur d'un objet conteneur

Introduction

- L'objet conteneur peut être un site Active Directory, un domaine ou une unité d'organisation
- Tous les objets à l'intérieur du conteneur subissent la stratégie définie
- L'objet subit toutes les stratégies de groupe appliquées au conteneur

Introduction

- Les stratégies sont traitées les unes après les autres, dans l'ordre suivants:
 - Stratégies de groupe locales
 - Stratégies de groupe liées au site
 - Stratégies de groupe liées au domaine
 - Stratégies de groupe liées aux OU
 - Stratégies de groupe liées aux OU enfant
- Si des paramètres entrent en conflit, par défaut, c'est le dernier paramètre lu qui s'applique

Introduction

- Technologie IntelliMirror:
 - Présente depuis Windows 2000, c'est un ensemble de fonctions puissantes destinées à augmenter l'efficacité des systèmes
 - Elle n'est utilisable que dans un environnement AD avec des serveurs et clients Windows à partir de Windows 2000 et n'est pas compatible Linux ou MacOS

Introduction

- Technologie IntelliMirror:
 - Elle permet une gestion des modifications et changements de configuration s'appuyant sur deux grands types de stratégies:
 - La stratégie locale: stockée localement sur la machine, est supplantée par une stratégie issue du domaine
 - La stratégie de groupe: est appliquée de manière centralisée et uniforme à des groupes d'utilisateurs et/ou d'ordinateurs

Stratégies de groupe (de domaine)

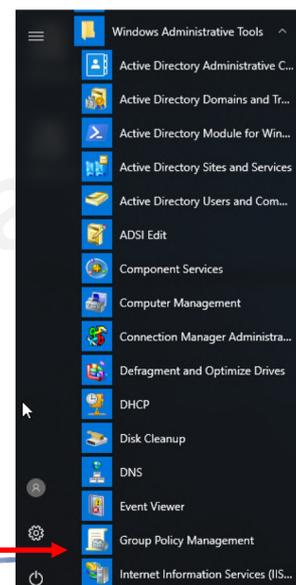
- Une stratégie de groupe se compose de paramètres que l'administrateur peut modifier, voire ajouter
- Ils peuvent s'appliquer soit à l'ordinateur, soit à l'utilisateur
- Comme paramètres, on trouve des stratégies et des préférences
- Les stratégies sont strictement appliquées, pas les préférences
- Un utilisateur peut modifier une préférence, pas une stratégie

©Hainaut P. 2017 - www.coursonline.be

307

Outil de gestion des stratégies de groupe (GPMC)

- Pour ouvrir l'outil GPMC:
 - Dans les outils d'administration -> Gestion des stratégies de groupe
 - S'il n'était pas installé, ajoutez la fonctionnalité: Gestion des stratégies de groupe



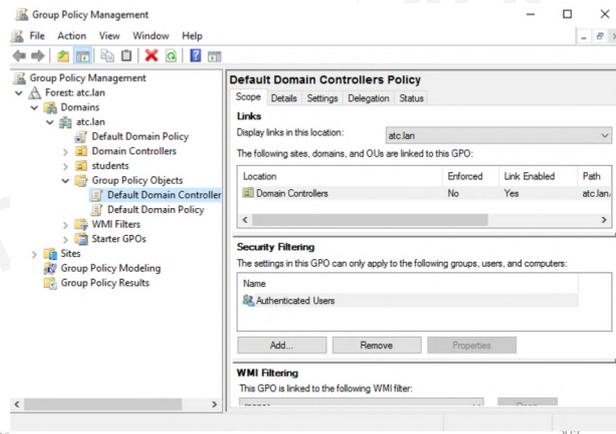
©Hainaut P. 2017 - www.coursonline.be

Outil de gestion des stratégies de groupe (GPMC)

- Un moyen efficace d'utiliser les GPO est d'utiliser les modèles de stratégie pour contrôleur de domaine

- Développez l'arborescence et cliquez avec le bouton droit sur Default DC Policy

- Sélectionnez Modifiez... pour accéder à l'éditeur



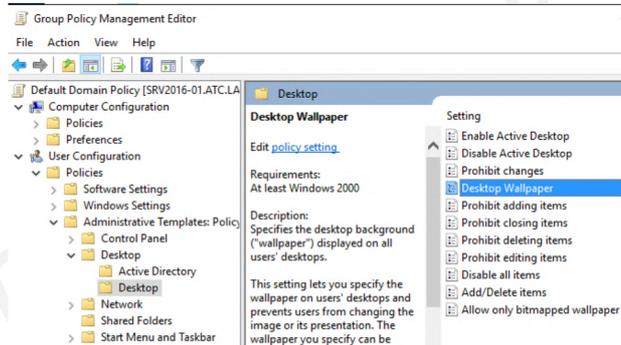
©Hainaut P. 2017 - www.coursonline.be

Outil de gestion des stratégies de groupe (GPMC)

- Les restrictions peuvent porter sur l'ordinateur ou l'utilisateur

- Les restrictions se placeront au niveau de l'onglet Stratégies

- Par exemple, apportons une restriction au niveau du bureau en spécifiant le papier peint

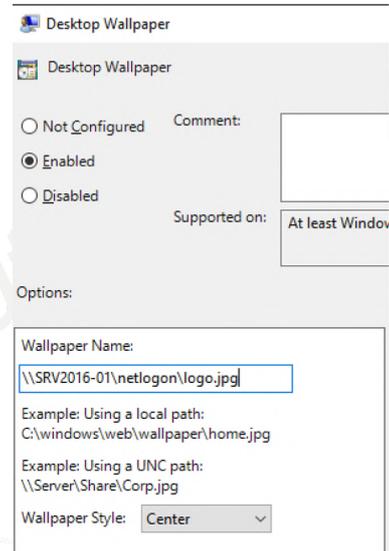


©Hainaut P. 2017 - www.coursonline.be

310

Outil de gestion des stratégies de groupe (GPMC)

- On spécifiera le fichier image à utiliser pour cela
- On peut placer ce fichier dans le répertoire partagé netlogon
- Le chemin indiqué sera un chemin UNC puisque ce sont les PC clients qui utilise cette info.

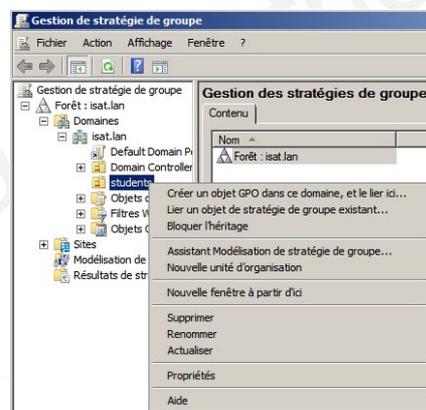


©Hainaut P. 2017 - www.coursonline.be

311

Outil de gestion des stratégies de groupe (GPMC)

- Pour répercuter cette stratégie sur notre OU, cliquez avec le bouton droit sur l'OU et puis cliquez sur Lier un objet de stratégie de groupe ...

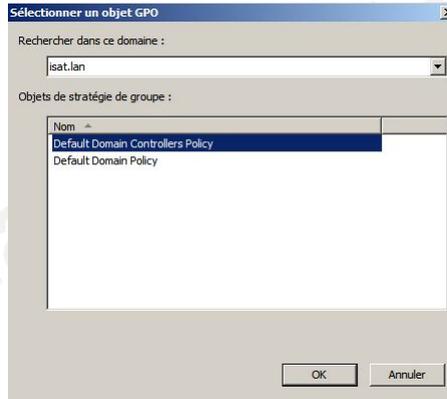


©Hainaut P. 2017 - www.coursonline.be

312

Outil de gestion des stratégies de groupe (GPMC)

- Dans la fenêtre suivante, on sélectionnera Default Domain Controllers Policy

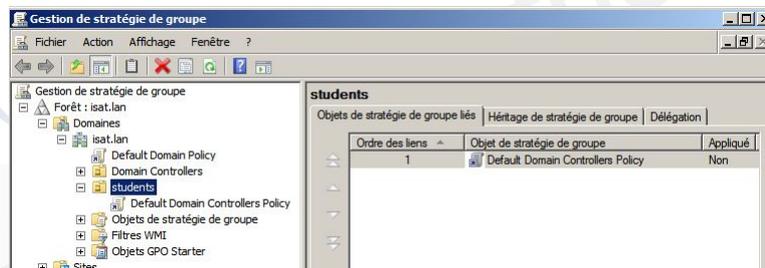


©Hainaut P. 2017 - www.coursonline.be

313

Outil de gestion des stratégies de groupe (GPMC)

- L'objet de stratégie de groupe est maintenant lié à notre unité d'organisation

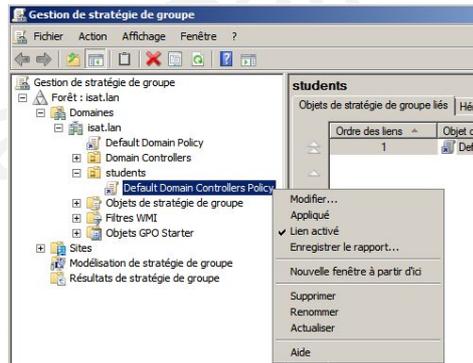


©Hainaut P. 2017 - www.coursonline.be

314

Outil de gestion des stratégies de groupe (GPMC)

- Il reste à activer les stratégies retenues
- Pour cela, on clique avec le bouton droit sur l'objet de stratégie et puis sur Appliqué



©Hainaut P. 2017 - www.coursonline.be

315

Outil de gestion des stratégies de groupe (GPMC)

- Maintenant que vous connaissez le principe des GPO, essayez d'appliquer d'autres stratégies ...

©Hainaut P. 2017 - www.coursonline.be

316

14. Gestion du support de stockage

Disque MBR et Disque GPT

- Le mécanisme GPT permet de:
 - S'affranchir des limitations imposées par le BIOS
 - Créer plus de 4 partitions
 - Gérer en théorie 2^{64} blocs logiques de 512 octets, soit 18 exa-octets, ce qui implique que la taille d'un cluster disque est fixe et ne change pas en fonction de la taille du disque

Un cluster disque ne peut contenir des informations que provenant d'un seul fichier

Si la taille d'un cluster est de 8k et la taille d'un fichier de 2k, 6k sont inutilisés

Disque MBR et Disque GPT

- Fonctionnalités des disques MBR et GPT

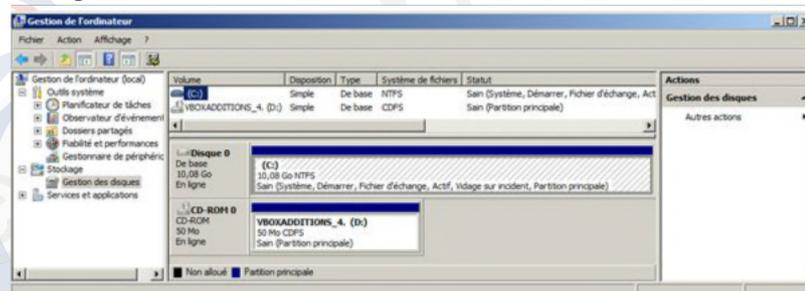
	MBR	GPT	Imp. GPT de Windows
Nbr de partitions	4	illimité	128
Taille du cluster	Variable	512 o	Variable
Syst. de fichier supporté	FAT NTFS	Divers	NTFS
Taille minimale recommandée	0 Mo	0 Mo	4 To
Taille maximale	2 To	18 Eo	256 To
Peut contenir des données	Oui	Oui	Oui
Démarrage Windows	Oui	Oui	Seulement sur des sys. Basés EFI

©Hainaut P. 2017 - www.coursonline.be

319

Initialisation d'un disque

- Initialiser un disque avec l'outil Gestion des disques:
 - Démarrer -> Outils d'administration -> Gestion de l'ordinateur -> Stockage de l'arborescence de la console -> Gestion des disques



©Hainaut P. 2017 - www.coursonline.be

320

Initialisation d'un disque

- Initialiser un disque avec l'outil Gestion des disques:
 - Sélectionnez le disque à initialiser puis le type de disque:
Secteur de démarrage principal pour MBR ou partition GPT

Conversion d'un disque

- Convertir un disque avec l'outil Gestion des disques:
 - Pour pouvoir convertir un disque, il ne faut pas qu'il soit partitionné
 - Démarrer -> Outils d'administration -> Gestion de l'ordinateur -> Stockage de l'arborescence de la console -> Gestion des disques
 - Cliquer avec le bouton droit sur le disque puis cliquez sur Convertir et choisissez GPT ou MBR suivant l'état du disque

Conclusion

- Vous savez maintenant comment configurer un serveur 2016 pour activer les services de base
- D'autres présentations viendront compléter celle-ci
- Merci de votre attention