

# **Domaine Windows 20XX**

---

**Généralités**

**Les contrôleurs de domaine**

**DNS et AD**

**Les relations d'approbation**

**Les services (DHCP, impression, ...)**

**CLI et Serveur Core**

**Trousse de secours de l'administrateur**

# I. Généralités

---

Domaine Microsoft ??

- Gestion centralisée (consoles d'administration)
- Ressources partagées (impression, dossiers, annuaire, ...)
- Règles communes (GPO)
- Authentification (comptes machines, comptes utilisateurs)
- Travail collaboratif (Exchange, WebDav, ...)

Notion de services offerts (serveurs) et de clients

Organisation « Microsoft » : des domaines dans une forêt

Tous est organisé autour d'un annuaire LDAP (**AD**)

# I. Généralités

---

L'annuaire Microsoft (**A**ctive **D**irectory)

Annuaire employant le protocole LDAP

Il fournit un service centralisé d'authentification et d'identification (machines, utilisateurs)

Il centralise et publie la liste des ressources partagées (imprimantes, dossiers ...) disponibles dans l'ensemble de l'organisation

L'AD est hébergé sur les contrôleurs de domaine (**D**omain **C**ontroller)

## II. Les contrôleurs de domaine

---

Forêt = ensemble d'arbres

Forêt n'est pas un espace de noms contigus

Arbre = arborescence de domaines

Arbre = espace de noms contigus et hiérarchiques

Tous les arbres d'une forêt partagent le même schéma d'annuaire (cf cours LDAP)

NB : il est possible d'avoir une forêt avec un seul arbre

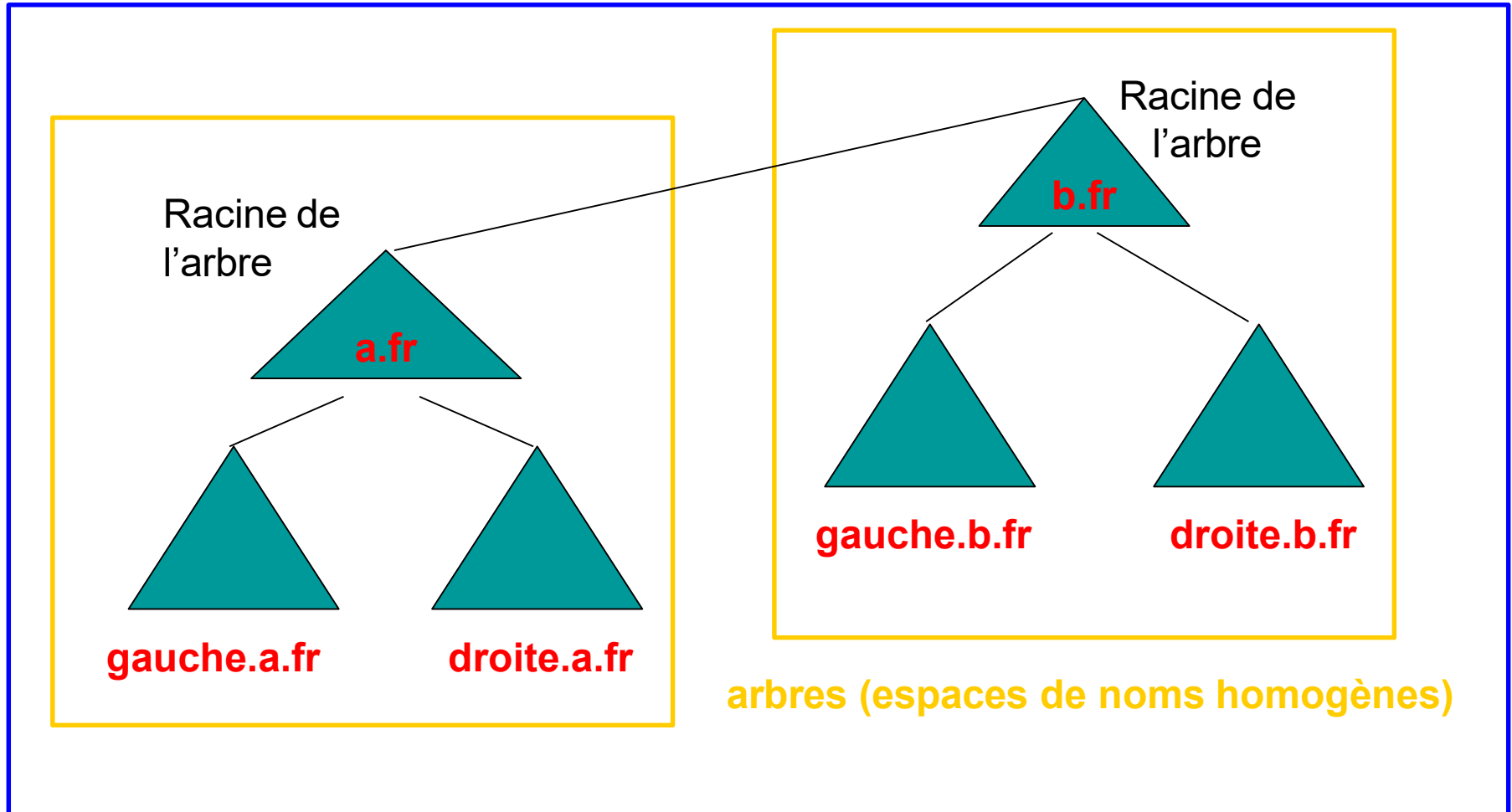
un arbre peut être constitué d'un seul domaine

le premier domaine déployé dans un AD est appelé domaine racine de la forêt : c'est le domaine hiérarchiquement le plus élevé.

## II. Les contrôleurs de domaine

---

**Forêt** = Organisation hiérarchique d'un ou plusieurs domaines



## II. Les contrôleurs de domaine

---

Installer l'OS serveur

Joindre le serveur à un groupe de travail au cours de l'installation

S'assurer de l'existence d'un serveur DNS (sinon, le créer)

Promouvoir le serveur en Contrôleur de Domaine (DC)

Deux cas: le domaine existe ou pas

Il existe: récupération de l'annuaire AD par réplication

Il n'existe pas: création de l'annuaire AD lors de la promotion

## II. Les contrôleurs de domaine

---

Tous les DC ont le droit d'écrire dans l'AD

Certains DC détiennent un rôle FSMO (Flexible Single Master Operation)

Ils sont dit maîtres d'opérations et sont autorisés à réaliser une action particulière sur l'AD

Rôle : Minimiser des risques de conflit lors des modifications de l'AD

Plusieurs rôles FSMO peuvent appartenir à un seul maître d'opération

Un rôle FSMO ne PEUT PAS appartenir à plusieurs maîtres d'opération

Il y a 5 rôles FSMO dans une forêt



## II. Les contrôleurs de domaine

---

### **Maître de schéma:**

Utilisé pour les mises à jour manuelles de schéma

Ex.: les mises à jour ajoutées par d'autres applications - Microsoft Exchange

Doit être en ligne lorsque les mises à jour de schéma sont effectuées



## II. Les contrôleurs de domaine

---

### Maître d'attribution des noms de domaine

- Unique au sein d'une forêt
- Attribue les noms de domaine

### Contrôleur de schéma

- Unique au sein d'une forêt
- Gère la structure du schéma

### Maître RID

- Unique au sein d'un domaine
- Attribue des blocs de RID aux contrôleurs de domaine pour assurer que les SID des objets soient unique

## II. Les contrôleurs de domaine

---

### Maître d'infrastructure

- Unique au sein d'un domaine
- Doit gérer les références d'objets au sein du domaine

### Émulateur PDC

- Unique au sein d'un domaine
- Assure diverses missions liées à la sécurité (MDP, Verrouillage, Stratégies de groupe)
- Par défaut, joue le rôle de serveur de temps pour l'ensemble du domaine

## II. Les contrôleurs de domaine

---

Catalogue global = ensemble de tous les objets d'une forêt

Lors de la création d'une forêt, le catalogue global est créé sur le premier DC

Un serveur de catalogue global dispose :

- d'une copie complète de l'AD pour son domaine hôte (arbre)
- d'une copie partielle (de tous les objets mais pas de toutes les informations concernant chacun d'entre-eux) en lecture des objets des autres domaine de la forêt

### III. DNS et AD

---

Il faut obligatoirement un serveur DNS dans un domaine AD

Ce serveur DNS sera de préférence dynamique

Possibilité d'utiliser un DNS externe mais très peu utilisé

Possibilité d'intégrer les zones DNS à l'Active Directory


Informations + enregistrements des zones = objet de l'AD    Objet =  
Implémentation d'un objet de la classe dnsZone (cf ADSIEdit)

Il est recommandé d'ajouter un serveur DHCP pour l'attribution des adresses IP

### III. DNS et AD

---

Intérêts :

DNS classique  Mise à jour (écriture, suppression) à partir du serveur hébergeant la zone principale

DNS intégré à l'AD  Maj depuis n'importe quel DC hébergeant le DNS

Nouveau DC dans l'AD  Zones automatiquement répliquées puis synchronisées

Synchronisation de l'AD plus optimisée que la synchro. de zone DNS

### III. DNS et AD

---

Application possible de droits pour l'enregistrement de ressources de zone



Mises à jour dynamiques autorisées uniquement pour un ordinateur client spécifique ou un groupe sécurisé ( groupe d'administrateurs de domaine)

Modèle de réplication multimaîtres de l'AD + intégration de toutes les zones DNS dans l'AD



Disparition de la notion de zones secondaires (toutes les zones sont " primaires ")

## IV. Les relations d'approbation

---

Une société en achète une autre – les deux disposent de domaines Microsoft

Monter un domaine commun : investissement en temps, en argent,  
interruption de service



Solution : mise en place d'une relation d'approbation entre les deux domaines

## IV. Les relations d'approbation

---



Les utilisateurs du domaine X pourront accéder aux ressources du domaine Y (et vice versa)

Un utilisateur du domaine X pourra se connecter avec son compte de domaine sur une machine du domaine Y (et vice versa)



## IV. Les relations d'approbation

---

Différentes relations d'approbation:

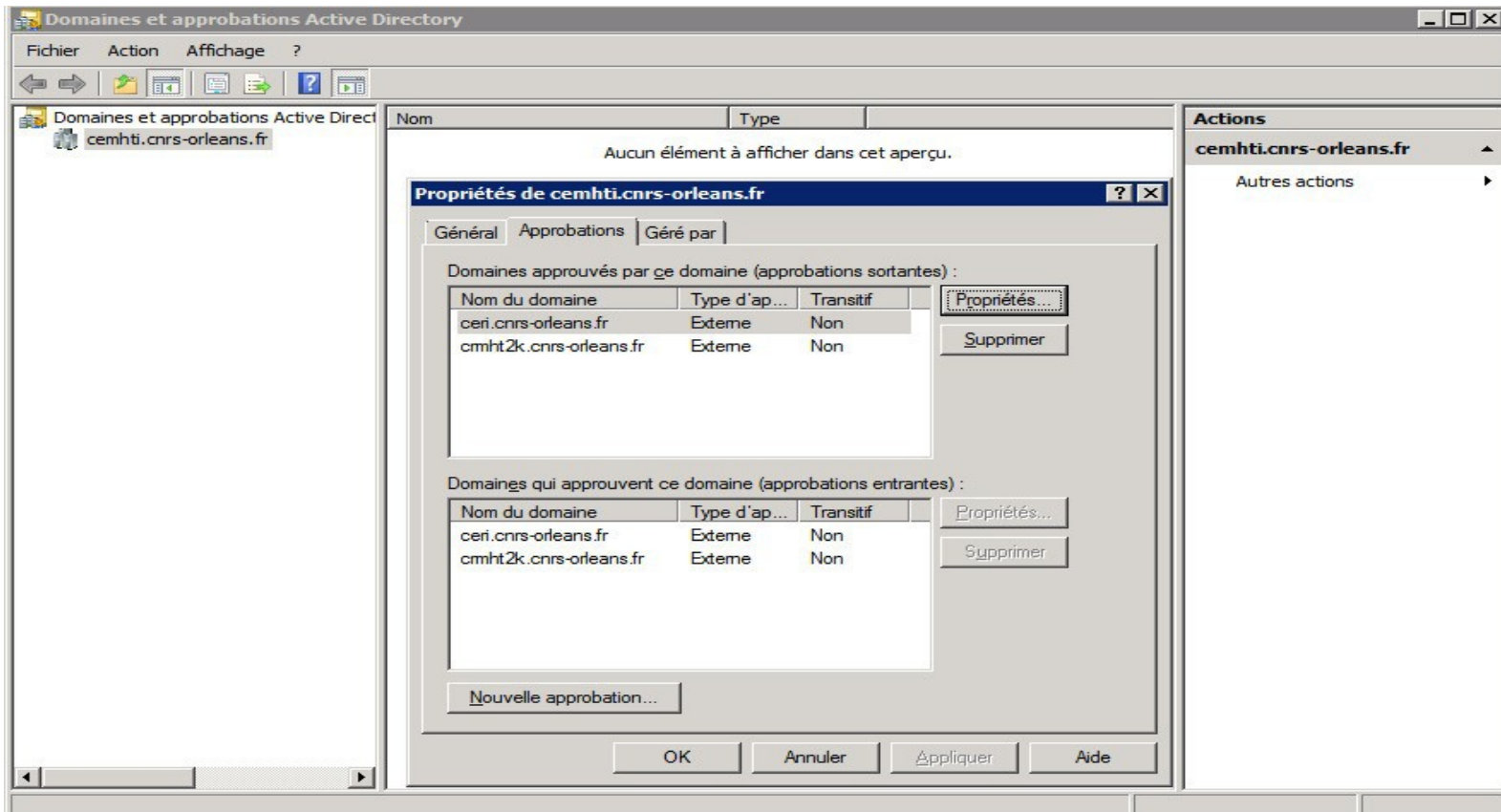
relation d'approbation **externe**: entre deux domaines de forêts distinctes

relation d'approbation **de forêt**: entre deux forêts distinctes

NB: les domaines d'une même forêt ont par défaut des relations d'approbation bidirectionnelles transitives avec l'ensemble des domaines de cette forêt

## IV. Les relations d'approbation

Gestion avec la console Domaines et approbations Active Directory



## IV. Les relations d'approbation

---

Pour créer une relation d'approbation :

- fournir le nom du domaine, de la forêt visé
- le type de relation d'approbation (externe, ...)
- le sens (bidirectionnelle, en entrée, en sortie)
- un mot de passe d'approbation (demandé dans les deux domaines / forêts)

A noter : Chaque entité doit accepter la relation d'approbation

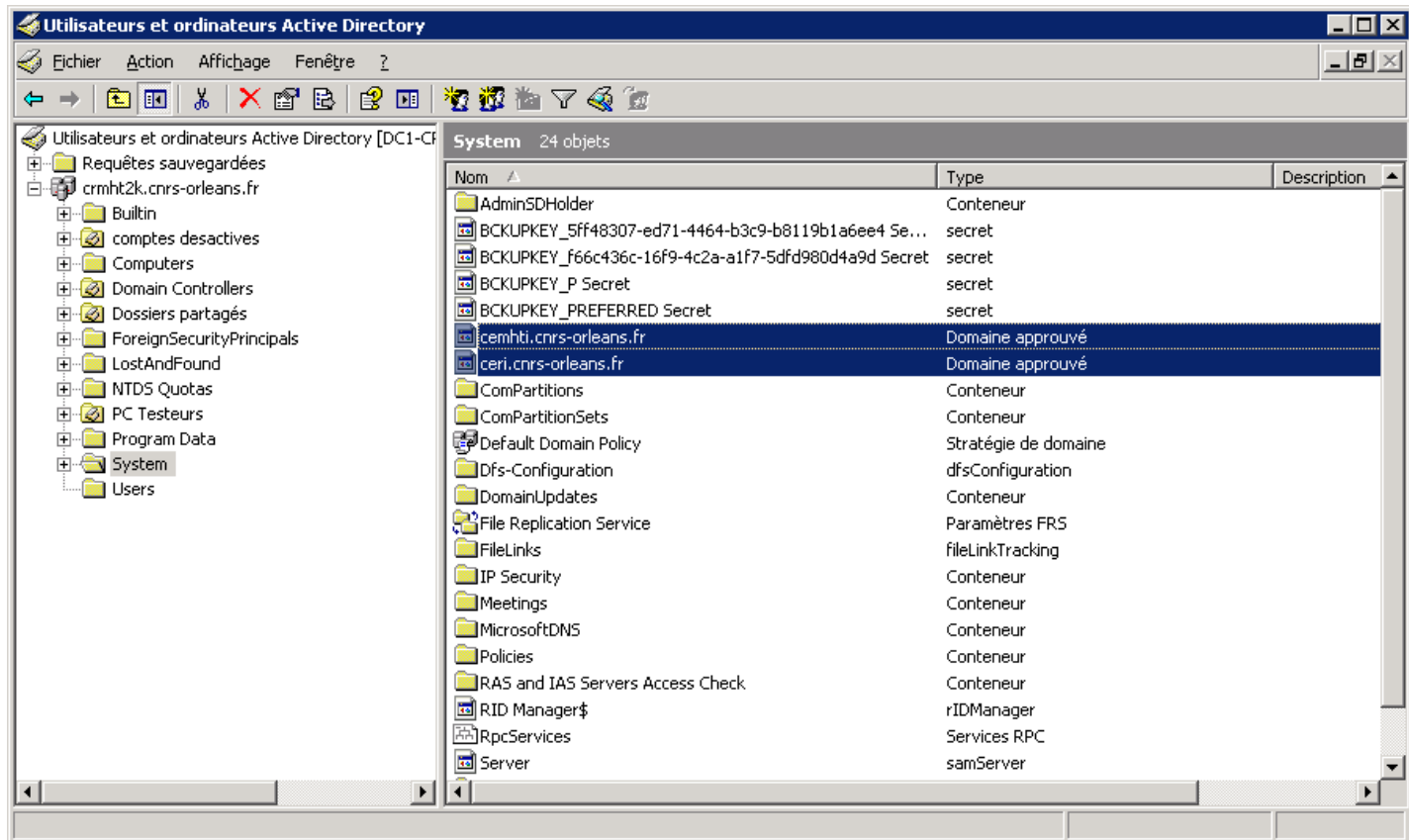
➔ Il faut intervenir sur un DC dans chaque domaine / forêt

## IV. Les relations d'approbation

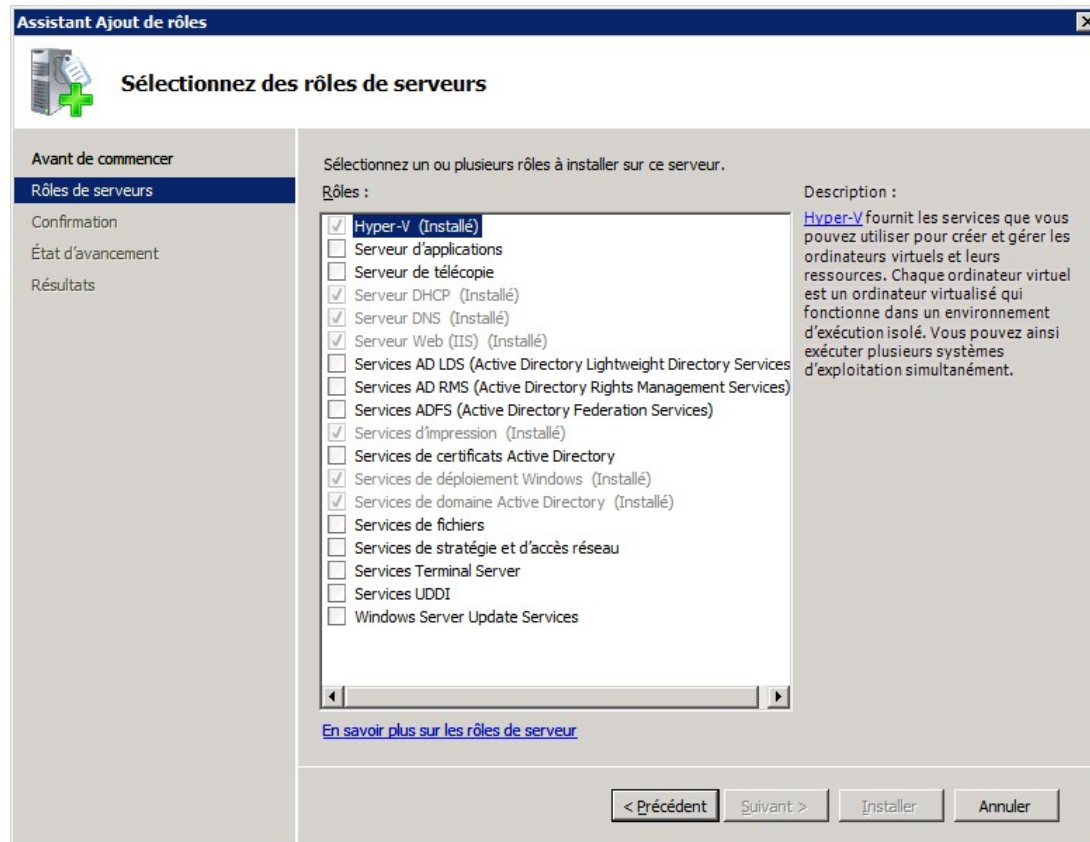
Chaque relation d'approbation



Création d'un objet de la classe Trust Domain Object dans l'AD (container System)



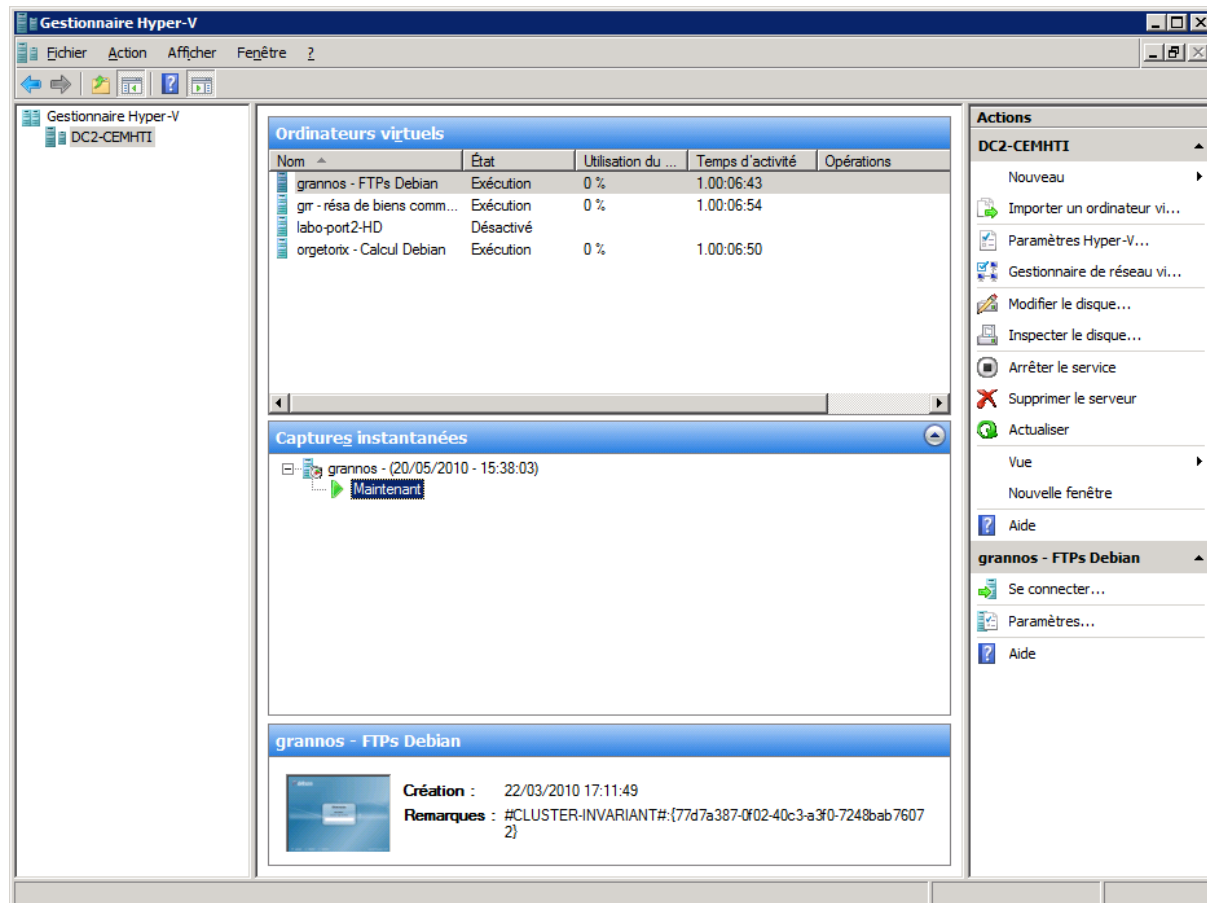
# V. Les services (Rôles et fonctionnalités)



Impressions, Quotas, IIS,...

# V. Les services - HyperV

HyperV → hyperviseur de virtualisation Microsoft

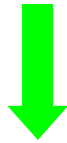


## V. Les services - WSUS

---

WSUS  Windows Server Update Services

Service de déploiement de mise à jour



Les clients ne vont plus chercher sur Internet les correctifs

Le serveur le fait pour eux

Les clients chargent à partir du serveur les maj validées par l'administrateur

## VI. CLI et serveur Core

---

Administration avancée en ligne de commande : PowerShell

Serveur Core : Serveur sans interface graphique

- Administration en ligne de commande locale ou distante (PowerShell)
- Ou avec les consoles d'administration à distance (RSAT)



## VI. Trousse de secours de l'administrateur

---

net view \\mamachine      liste des partages de mamachine

nbtstat -a @IP      liste des noms de la machine @IP

nbtstat -n      liste des noms de la machine locale

nbtstat -S      liste des sessions de la machine locale et donne les @IP distantes

## VI. Trousse de secours de l'administrateur

---

Commandes utilisant la couche TCP/IP

netstat pour Network Statistics

netstat -an	affichage numérique des connexions et ports d'écoute associés
-------------	---

netstat -r	affiche la table de routage
------------	-----------------------------

## VI. Trousse de secours de l'administrateur

---

nslookup

nslookup nomdhote

résolution de nomdhote par le DNS de la configuration réseau du poste client

nslookup @IP

résolution de @IP par le DNS de la configuration réseau du poste client

nslookup nomdhote @IP1

résolution de nomdhote par le serveur DNS ayant l'adresse @IP1

nslookup @IP @IP1

résolution de @IP par le serveur DNS ayant l'adresse @IP1

## VI. Trousse de secours de l'administrateur

---

arp  Résolution des macAddress à partir de @IP

arp -a = arp -g                      renvoie toutes les entrées du cache local

arp -s @IP macAddress              création d'une entrée statique dans le cache

arp -d @IP                              destruction de l'entrée correspondant à @IP  
dans le cache

## VI. Trousse de secours de l'administrateur

---

ipconfig

ipconfig	renvoie toutes les données IP du client
ipconfig /all	renvoie toutes les données IP détaillées du client
ipconfig /release	force la libération de @IP obtenue par DHCP
ipconfig /renew	force la demande d'actualisation du bail DHCP
ipconfig /flushdns	vide le cache local DNS du client