

WINDOWS SERVER ADMINISTRATION

Active Directory

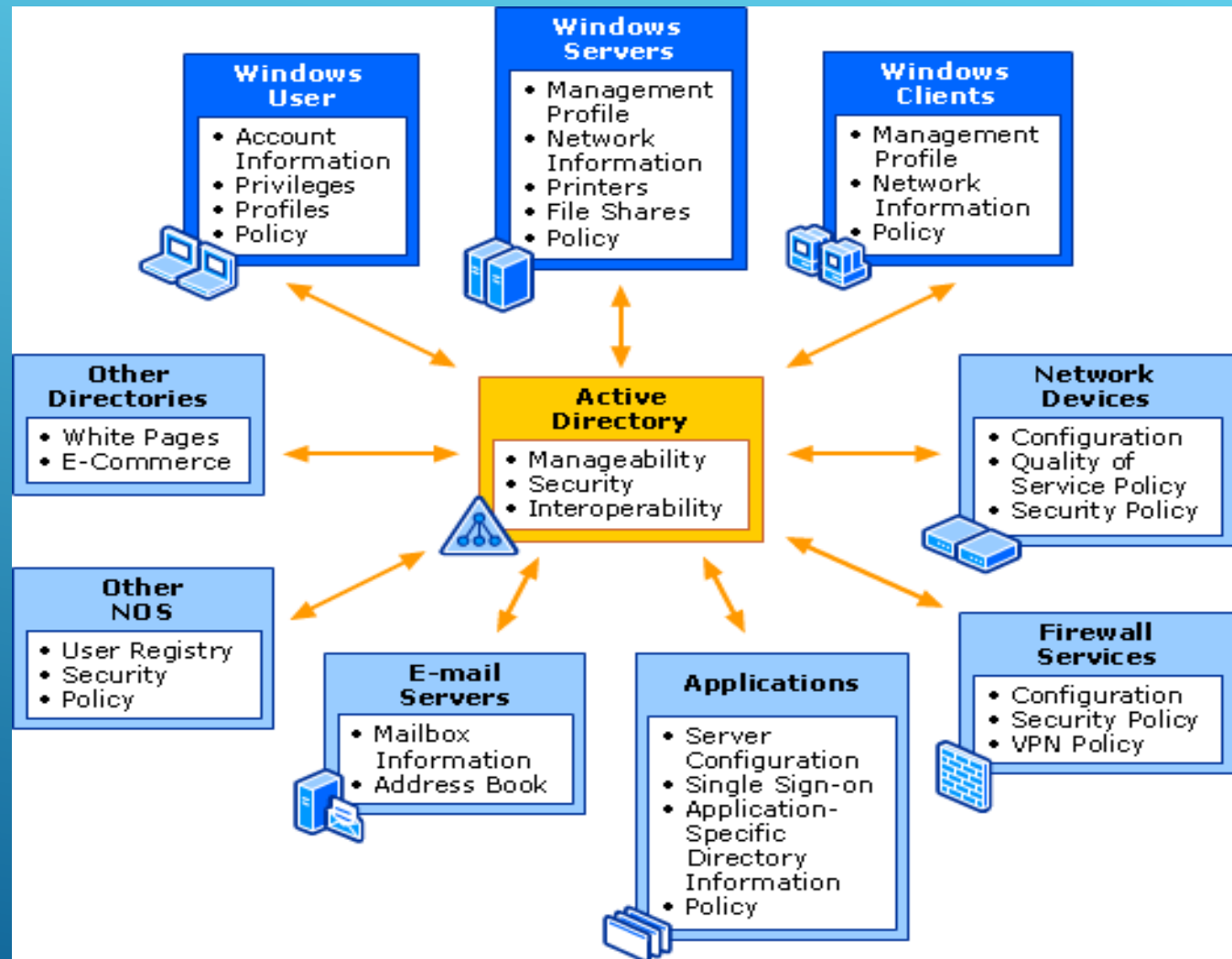
1ère Partie.

PLAN

- 1 • Concepts.
- 2 • Conception et Planification
- 3 • Espace de noms.
- 4 • Unités organisationnelles.
- 5 • Réseau d'agence.

CONCEPTS

PHILOSOPHIE



RÔLE D'ACTIVE DIRECTORY

Contrôle des
ressources
centralisé.

Gestion des
ressources
centralisée et
décentralisée

Stockage
sécurisé des
objets dans une
structure logique.

Optimisation du
trafic réseau.

L'ANNUAIRE

Constituer un « carnet d'adresses ».

Recenser des informations sur un parc matériel.

Authentifier des utilisateurs (grâce à un mot de passe).

Définir les droits de chaque utilisateur.

Interaction avec d'autres services d'annuaires.

PROTOCOLE LDAP

le rôle du protocole LDAP (Lightweight Directory Access Protocol), est de fournir un moyen unique (standard ouvert) d'effectuer des requêtes sur l'annuaire d'un réseau par l'intermédiaire de protocoles TCP/IP.

Active Directory est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.

DOMAINE

- ▶ Frontière de sécurité et de réplication.
- ▶ L'annuaire associé à chaque domaine est disponible sur 1 ou plusieurs serveurs du domaine.
- ▶ Il est possible de créer des arborescences de domaines.
- ▶ A chaque domaine est associé un nom DNS.
 - ▶ Ex : univ-montp2.fr

RÔLES DE MAITRE D'OPÉRATION

Rôles **F**lexible **S**ingle **M**aster **O**perations

Pour éviter les conflits lors de réplication.

- ▶ **Maître de schéma:**

Seul contrôleur de domaine autorisé à modifier le schéma. Gère aussi la réplication du schéma.

- ▶ **Maître d'attribution des noms de domaine:**

Gère l'ajout et la suppression de domaines dans la forêt.

- ▶ **Maître RID:**

Alloue les blocs d'identificateurs à chaque contrôleur de domaine.

RÔLES DE MAÎTRE D'OPÉRATION

► Maître d'infrastructure :

Mise à jour ou suppression d'objets fantômes.

► Emulateur PDC (CPD) :

Primary Domain Controller/Contrôleur de Domaine Primaire.

fonctions

- Assure la compatibilité avec les domaines de type Windows NT.
- Verrouillage des comptes utilisateurs et changements des mots de passe.
- Synchronisation du temps.
- Modifications des stratégies de groupe du domaine.

LE SCHÉMA

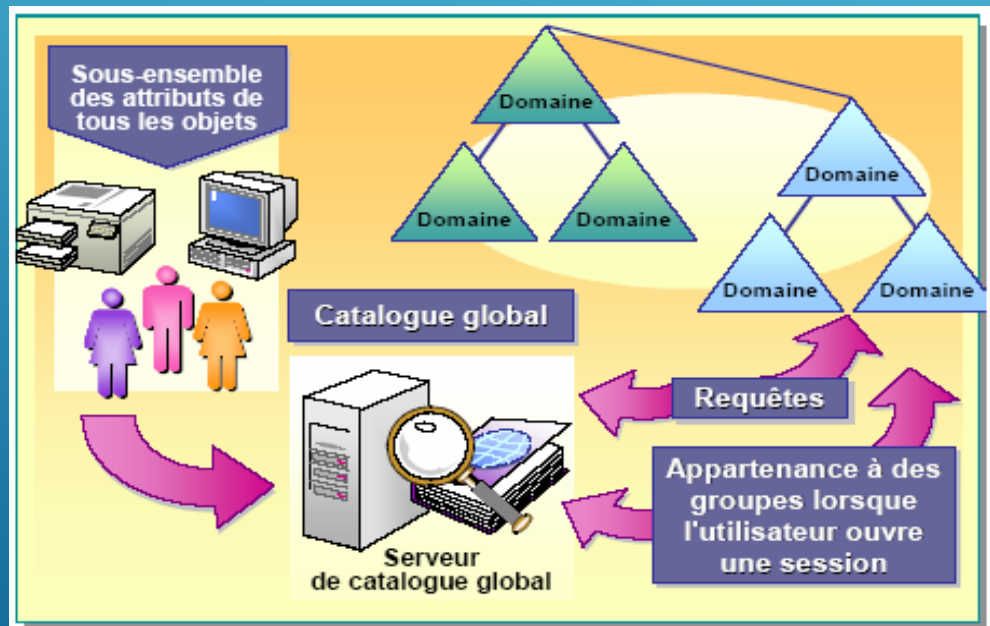
- ▶ Tout élément de l'AD est un objet défini par une classe qui est dotée d'attributs.
 - ▶ Ex : la classe 'user' a un attribut 'mail'
- ▶ Les définitions des classes et des attributs sont accessibles via le Schéma.
- ▶ Utilisation :
 - ▶ Extensibilité (ajouts de classe ou d'attribut)
 - ▶ Interopérabilité.

CATALOGUE GLOBAL

Il contient une réplique partielle (nb réduit d'attributs) des objets de l'annuaire.

Un catalogue global est présent dans chaque domaine.

Permet de localiser rapidement n'importe quel objet sans connaître son emplacement dans l'arborescence.



NOMMAGE D'OBJET

Nom unique relatif identifie l'objet de façon unique dans son conteneur parent.

CN=mon_ordinateur

Nom Unique LDAP: identifie le domaine et le chemin d'accès à un objet.

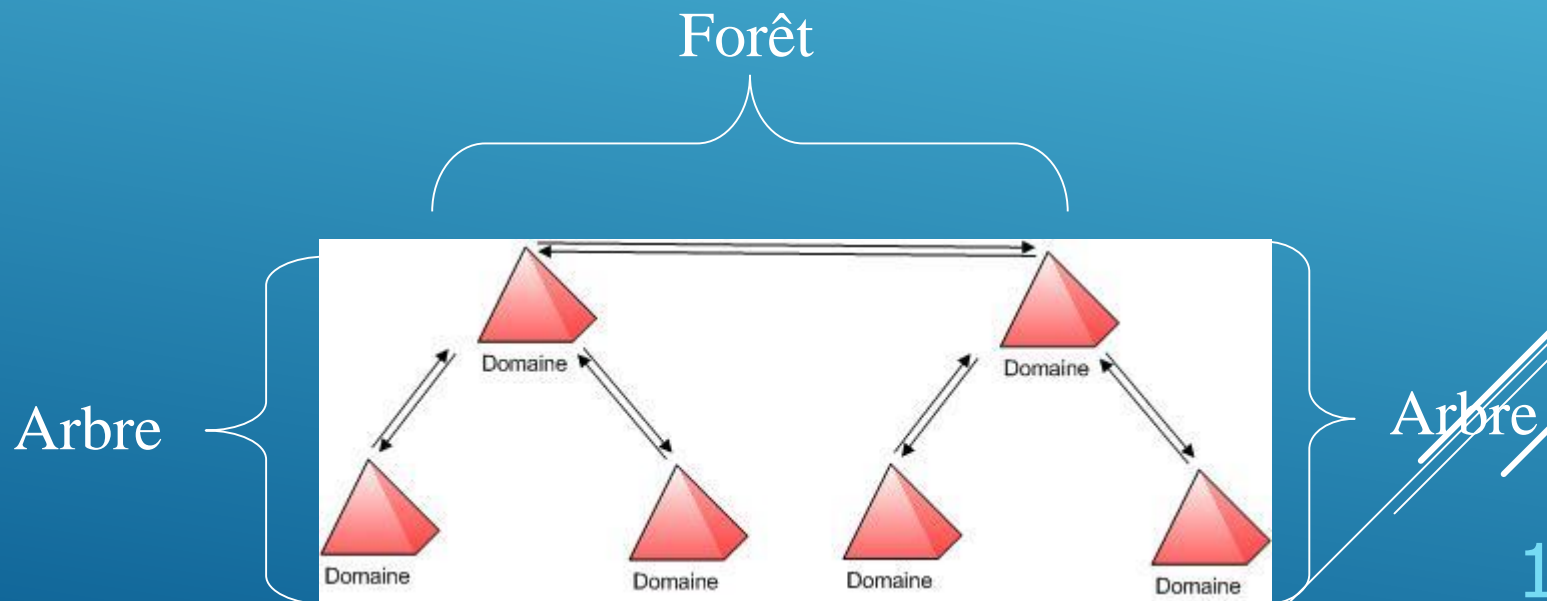
CN=mon_ordinateur, OU=Mon_Unité_Organisation, DC=microsoft, DC=com.

Nom canonique (*Canonical name*) Le nom canonique de l'ordinateur de l'exemple précédent est
Microsoft.com/Mon_Unité_Organisation/mon_ordinateur.

Identifiant global unique GUID, pour *Globally Unique Identifier*) qui est une chaîne de caractères de 128 bits unique et non modifiable.

ARCHITECTURE LOGIQUE

- ▶ Arbre : ensemble de domaines situé sous une racine unique formant un espace de noms contigus.
- ▶ Forêt : ensemble d'arbres ne formant pas un espace de noms contigus.



CARACTÉRISTIQUES D'UNE FORÊT

Dans une forêt les domaines partagent:

- Un même schéma.
- Une même partition de configuration.
- Un même catalogue global.

Dans une forêt, les domaines sont liés entre eux par des relations d'approbations :

- Transitives.
- Bidirectionnelles.

RELATION D'APPROBATION

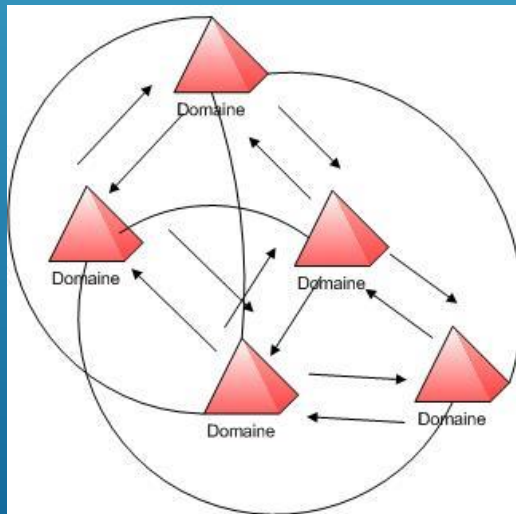
Mécanisme permettant
aux utilisateurs
authentifiés dans un
domaine de pouvoir
accéder aux ressources
d'un autre domaine.

RELATIONS D'APPROBATION

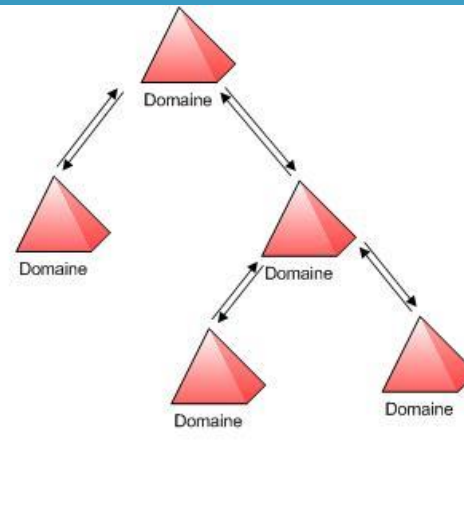
Les relations d'approbation entre domaines utilisent Kerberos et sont :

- Implicites, transitives et bidirectionnelles

NT 4.0

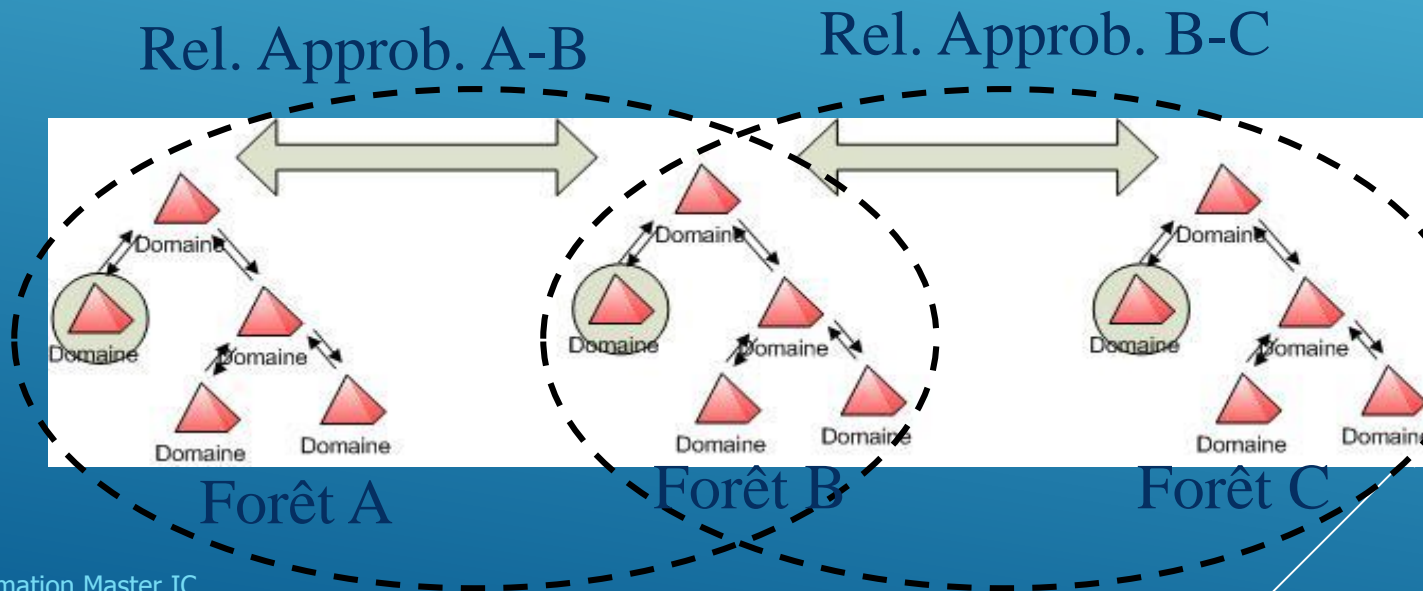


W2003/2008



RELATIONS D'APPROBATION

- A partir de WS2003 les relations d'approbation inter forêts réduisent la charge d'administration



PARTITIONS D'ANNUAIRE

partitions sont des conteneurs logiques dans lesquels sont conservés un type de données.

- ▶ partition du domaine :
 - ▶ Objets du domaine commun à tous les serveurs.
- ▶ Partition de la configuration :
 - ▶ Information de configuration de la forêt, commun à tous les contrôleurs de la forêt
- ▶ Partition du schéma :
 - ▶ Schéma de l'AD, sur tous les contrôleurs
- ▶ Partition de l'application :
 - ▶ Peut être créée avec des objets de tout type sauf de sécurité (user, groupe, ordi) peut être répliquée sur n'importe quel ensemble de contrôleurs dans la forêt

CONCEPTION ET PLANIFICATION

Conception.

- Besoins de l'entreprise

Plan
d'implémentation.

- Aspects techniques de la conception
- Etablir les structures d'implémentation

mise en œuvre.

- Création de la structure

CONCEPTION

Taches de conception

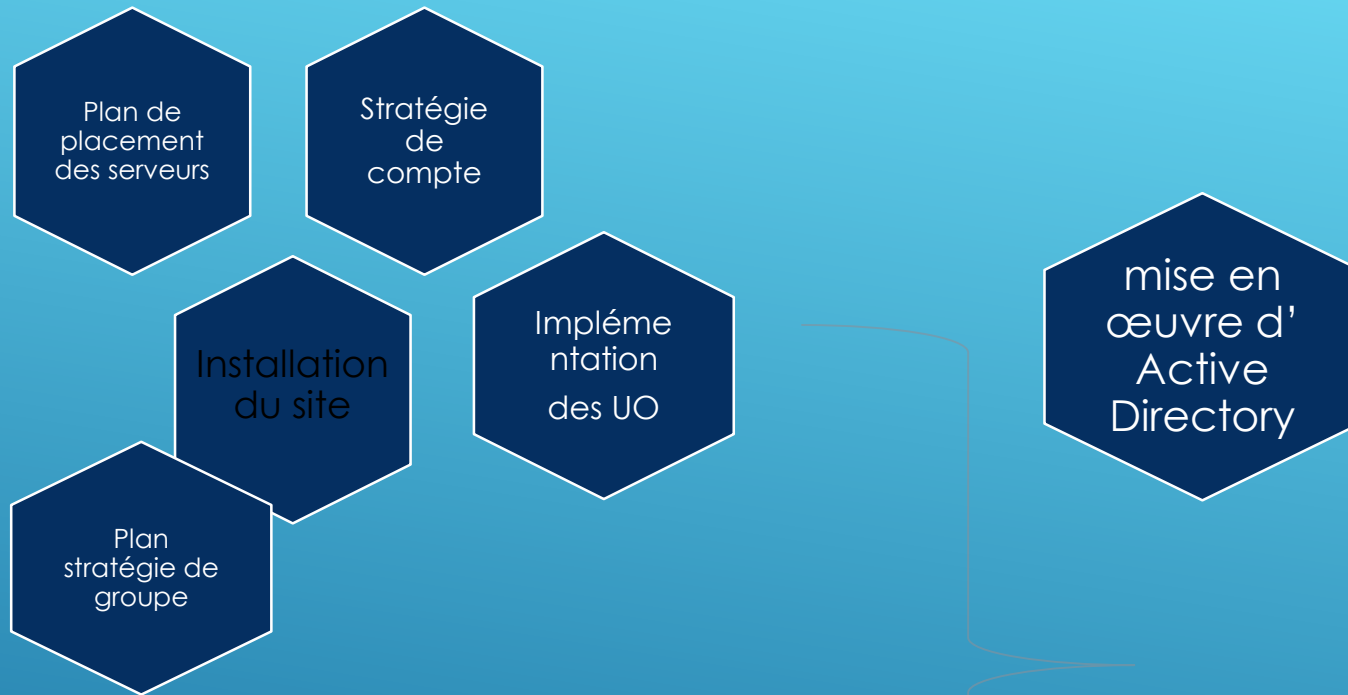
- Collecte d'information sur l'organisation.
- Analyse des informations.
- Analyse des options de conception.
- Sélection et affinage de la conception.

Résultats de la phase de conception.

- Conception du domaine et de la forêt.
- Conception des UO.
- Conception du site.



CONCEPTION



IMPLÉMENTATION

Implémenter la forêt le domaine les structures DNS	Créer UO & Groupes de sécurité. Comptes utilisateurs & ordinateurs. Stratégies de groupe	Mise en œuvre des sites

DÉFINIR LE PLAN D'ACTION

CONCEPTION DE L'ESPACE DE NOMS

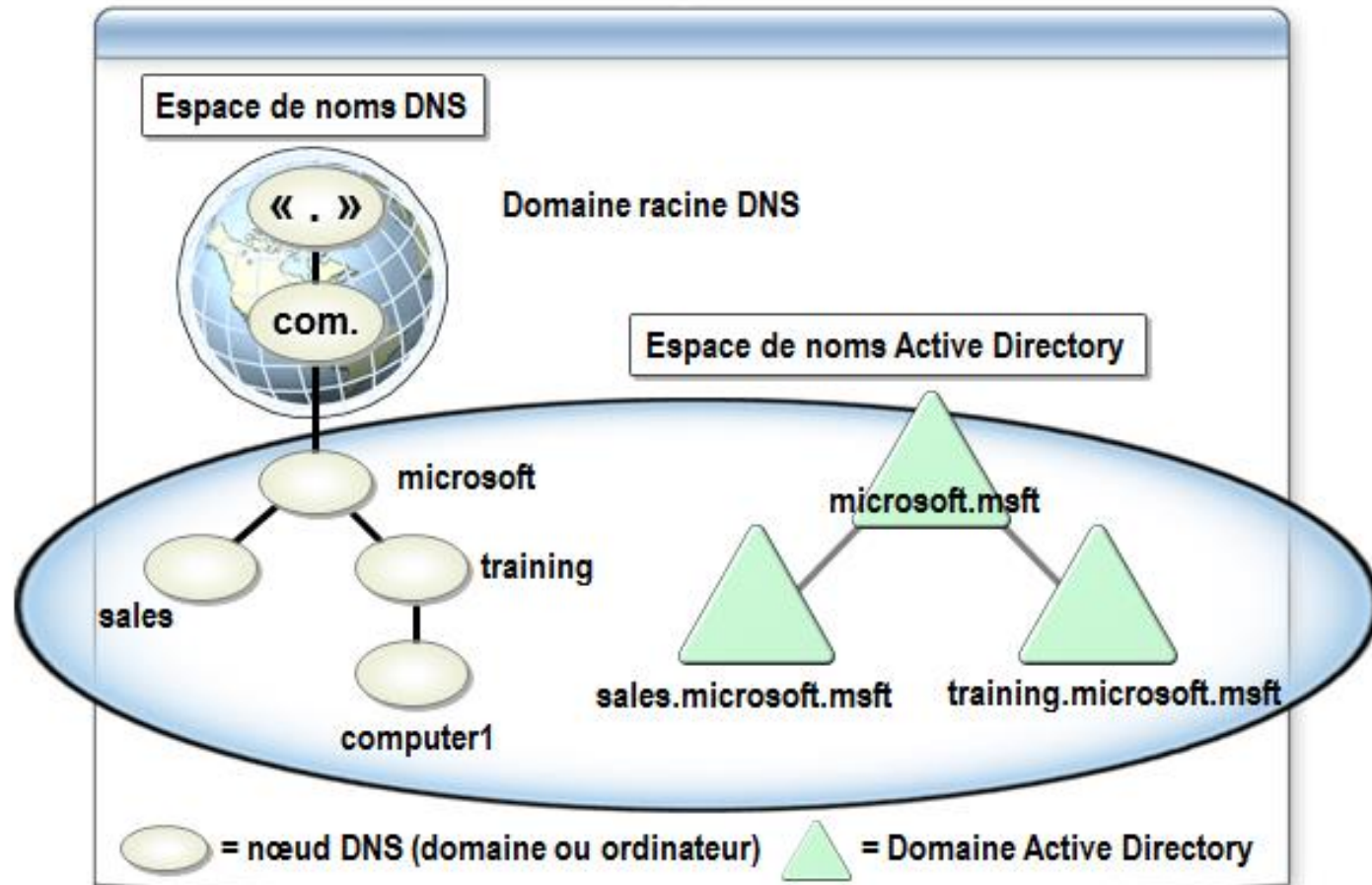
DÉFINITION DE L'ESPACE DE NOMS

Doit se rapprocher des topologies

Doit déboucher sur un découpage utile :

- Espace de noms des domaines et DNS.
- Topologies d'UO.
- Topologies de sites.

DÉFINITION DE L'ESPACE DE NOMS



DÉFINITION DE LA RACINE DE LA FORÊT

- ▶ Le 1^{er} domaine créé est la racine de la forêt
- ▶ Il donne son nom à la forêt
- ▶ Il héberge 2 groupes sensibles :
 - ▶ Admins de l'Entreprise
 - ▶ Admins du Schéma
- ▶ Choix du domaine Racine :
 - ▶ A choisir parmi les domaines déjà définis
 - ▶ Ou à créer pour les besoins

COMBIEN DE FORÊTS ?

- ▶ Au départ une forêt !
- ▶ Pour créer une forêt de + il faut des arguments :
 - ▶ Nécessité de préserver des schémas distincts
 - ▶ Refus de dévoiler une topologie de domaines
 - ▶ Désaccord sur la composition des groupes sensibles
 - Administrateur de Schéma
 - Administrateur de l'Entreprise
 - ▶ Souhait de conserver le contrôle des approbations

CONTRAINTES DU NOMBRE DE FORÊTS

- ▶ Un domaine ne peut pas changer de forêt.
- ▶ Déplacement d'objet :
 - ▶ On sait migrer des objets d'un domaine à un autre
 - ▶ Mais ce n'est pas anodin !
- ▶ On ne sait pas interroger le Catalogue Global d'une autre forêt ...
- ▶ ... à moins de passer par un Méta Annuaire!!

COMBIEN DE DOMAINES

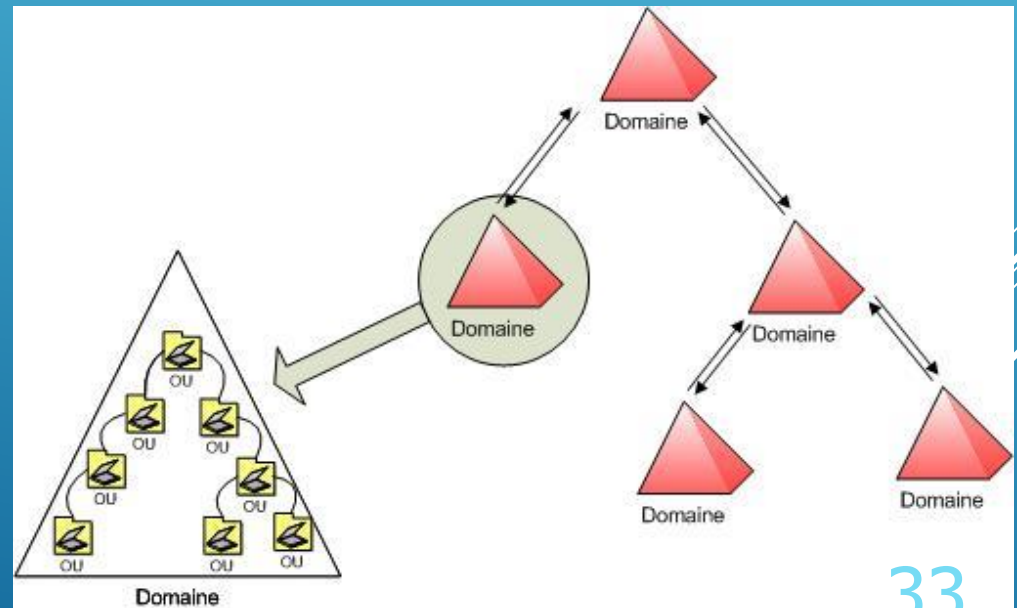
- ▶ Au départ un domaine.
- ▶ Un domaine de plus, il faut argumenter:
 - ▶ Délégation ne suffit pas
 - ▶ Nécessité de mettre en place des stratégies spécifiques dans un domaine WS2003 :
 - ▶ Gestion des mots de passe.
 - ▶ Verrouillage des comptes.
 - ▶ Gestion des tickets Kerberos.
 - ▶ Soucis d'optimisation de la réplication.
 - ▶ Restructuration prévue, mais + tard.

UNITÉS ORGANISATIONNELLES

UNITÉS ORGANISATIONNELLES

- ▶ Conteneurs d'objets de type utilisateurs, groupes, ordinateurs .
- ▶ Définies dans un domaine.
- ▶ Utilisation :

- ✓ Organisations des données.
- ✓ Délégation des droits pour l'administration.
- ✓ Application des stratégies de sécurité.



RÔLES DES UNITÉS ORGANISATIONNELLES

- ▶ Les OU peuvent servir à :
 - ▶ Organiser des objets.
 - ▶ Définir des périmètres de délégation.
 - ▶ Ne pas tout montrer à tout le monde.
 - ▶ Définir des périmètres d'applications pour les GPO.
- ▶ Une OU contient des objets et pas des références à des objets.
- ▶ A une OU correspond des sécurités.

PROCESSUS DE PLANIFICATION D'UO

1

- Documenter la structure existante.

2

- Identification des modifications à apporter.



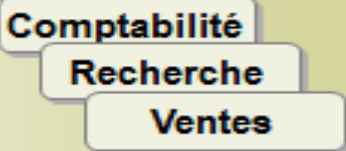

3

- Niveaux d'administration.

4

- Identifiez chaque administrateur et compte d'utilisateur ainsi que les ressources qu'ils administrent.

PLANIFICATION

Modèle d'administration basé sur	Structure OU conçue sur :
L'emplacement géographique 	L'emplacement
L'organisation 	La structure de l'organisation
La fonction business 	Les fonctions dans l'organisation
Modèle hybride 	<ul style="list-style-type: none"> ■ Emplacement d'unités d'organisation ou de domaines de niveau supérieur ■ Structure organisationnelle d'unités d'organisation ou de domaines de niveau inférieur

CRÉATION DES UNITÉS ORGANISATIONNELLES

Interface
graphique.

Langage de script

Ligne de
commande Ldifde.

Par les outils de
service d'annuaire:

DsAdd
DsMod...

PowerShell.

DÉLÉGATION D'ADMINISTRATION

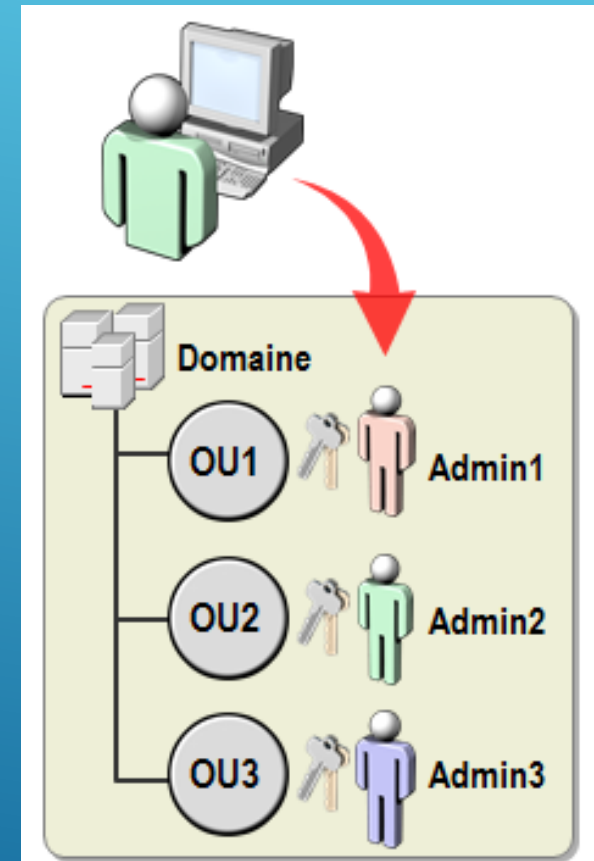
Décentralisation de la gestion



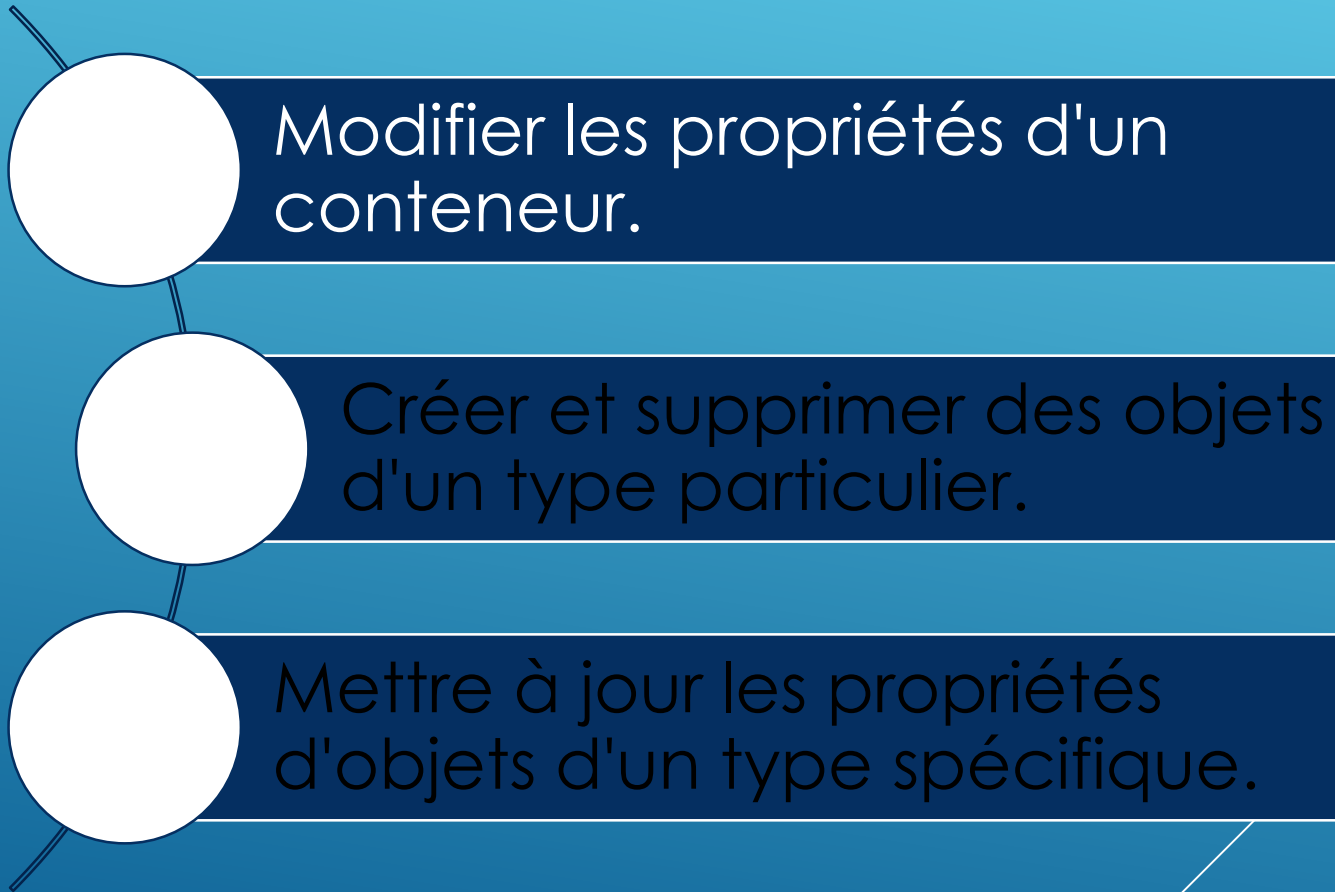
Isolation de la gestion des services ou des données.



Autonomie administrative



TACHES D'ADMINISTRATION.



RÉSEAU D'AGENCES

► Qu'est ce qu'un site ?

- Ensemble machines « bien communicantes».
- Défini comme un agrégat de sous réseaux IP.
- Suppose un subnetting géographique.

Un site peut s'étendre sur plusieurs domaines, un domaine sur plusieurs sites.

Les sites ne font pas partie de l'espace de noms du domaine.

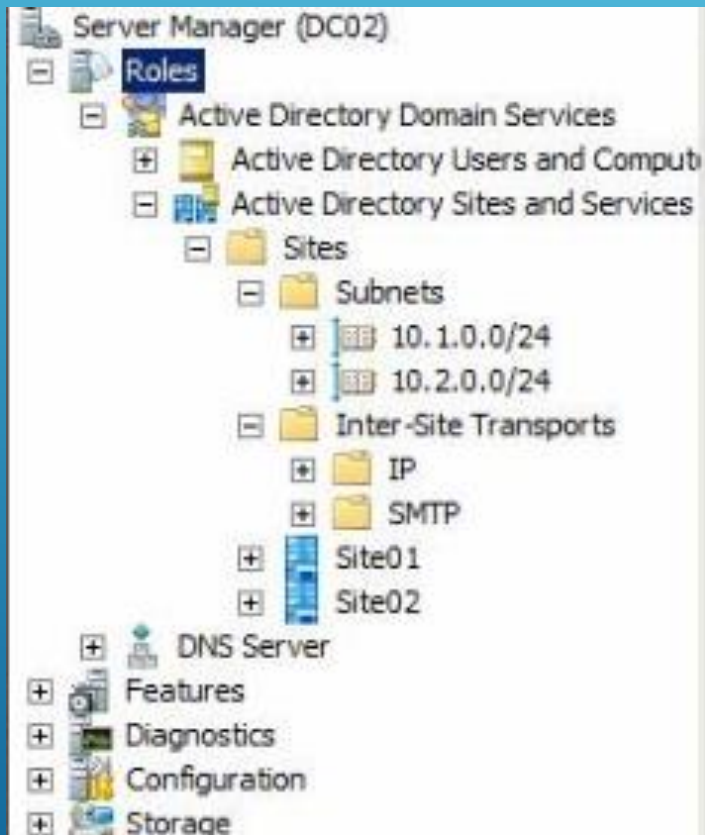
NOTION DE SITE ACTIVE DIRECTORY

► Qui utilise les sites ?

- Les stations pour localiser un DC proche.
- KCC (Konsistency Coherence Checker) pour limiter le trafic de réplication sur liaisons lentes.
- Client DFS (Distributed File System) pour localiser un répliqua proche.
- Utilisateur pour localiser une imprimante proche.

NOTION DE SITE ACTIVE DIRECTORY

CONSOLE SITES ET SERVICES



Affichage des sites valides d'une entreprise.

Affichage des sous-réseaux.

Affichage des transports et des liens entre sites.

Affichage des applications qui exploitent les connaissances du site.

Affichage des serveurs qui font partie d'un site..

DÉFINITION D'UNE TOPOLOGIE DE RÉPLICATION

- ▶ Qui réplique avec qui (en inter sites) ?
 - ▶ Tout automatique : le KCC fait tout
 - ▶ Semi-automatique :
 - ▶ Fournir qques indices au KCC :
 - ▶ Créer manuellement qques connexions
 - ▶ Ajouter des liens de sites
 - ▶ Designer des têtes de pont
 - ▶ Tout manuel :
 - ▶ Créer toutes les connexions manuellement
 - ▶ Inhiber le KCC

OPTIMISATION DE LA RÉPLICATION

Le KCC Fonctionne sur tous les contrôleurs de domaine, et génère la topologie de réplication de la forêt.

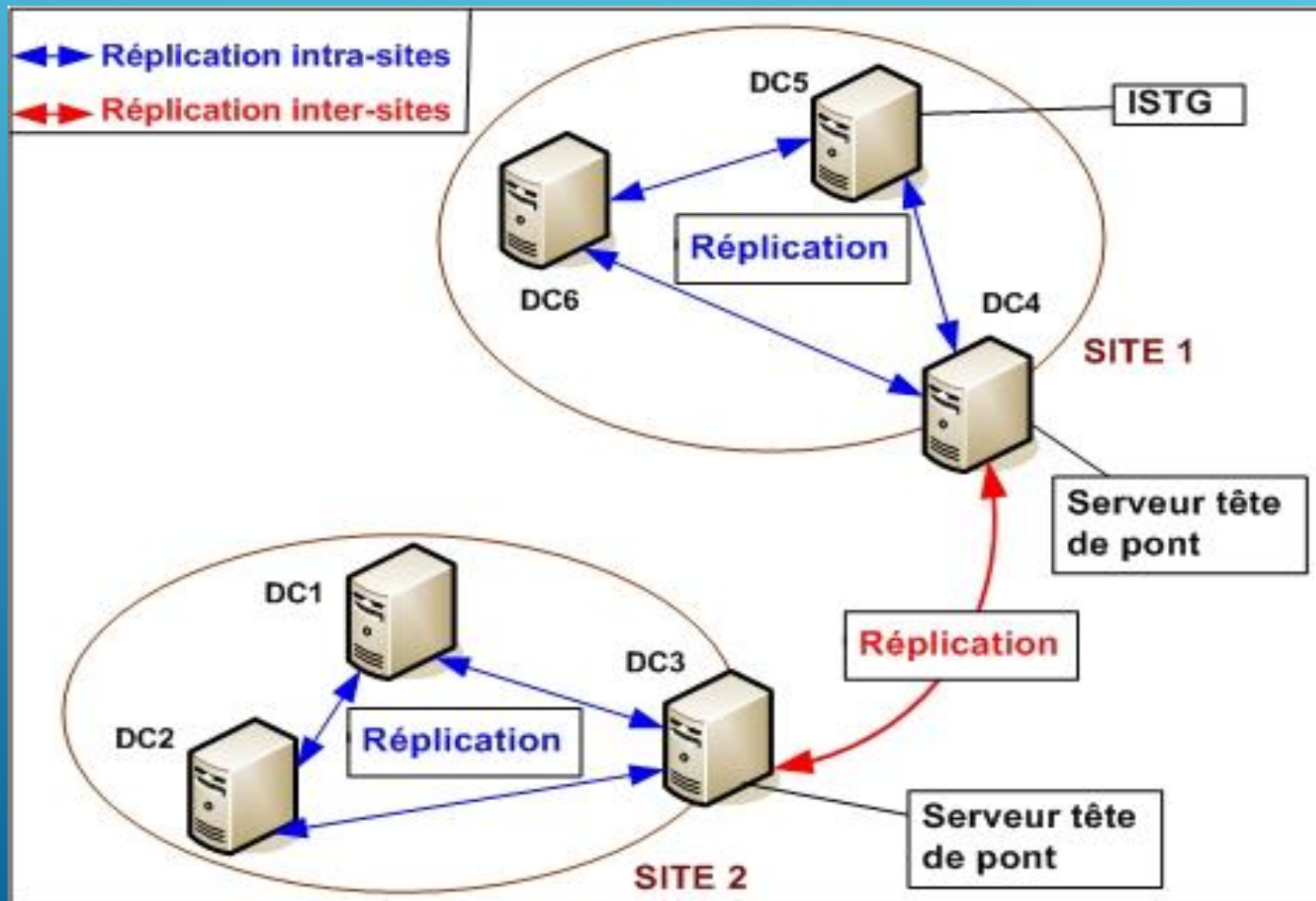
- Assure le Load balancing des connexions intra sites en passant par des « Bridgehead Servers »
- En interne Le KCC crée des chemins de réplication unidirectionnels entre les « partenaires de réplication »

SERVEUR TÊTE DE PONT

Envoie et reçoit
des données
répliquées

Est désigné
pour chaque
partition du site

OPTIMISATION DE LA RÉPLICATION



OPTIMISATION DE LA RÉPLICATION

Depuis WS2003 : réplication unitaire des modifications

- Suppression de la limite max des 5000 utilisateurs par groupe, réconciliation en cas de mises à jour concurrentes.
- Seuls les attributs ajoutés sont répliqués.

Tous les contrôleurs doivent être en WS2003 minimum.

PLANIFICATION DES SITES

Conception de la topologie de site

Nombre de sites et emplacements.

Liens pour relier les différents sites.

Exigences de disponibilité des sites.

Stratégies de sécurité de site.

Nombre d'utilisateurs.

Planification de la topologie de site

Planification et durée d'une liaison de site.

Ponts entre liens de sites.

Serveurs de tête de pont.

Objets de sous-réseau.

Contrôleurs de domaine Disponibles.