Université des Frères Mentouri Constantine
Faculté des Sciences de la Technologie
Département d'Electronique

Administration des services réseau

Master 1 : Réseau et Télécommunication
2021-2022

DR. GUELTOUM BENDIAB
EMAIL: BENDIAB.KELTHOUM@UMC.EDU.DZ

Prérequis

- Les bases des réseaux informatiques
- Les Protocoles de communication
- Modèle OSI
- Modèle TCP/IP
- Les éléments d’un réseau.

Objectifs du cours

Acquérir les connaissances et les compétences nécessaires pour **l'exploitation**, **l'administration**, **la maintenance** et **la surveillance des réseaux informatiques**. L'étudiant se familiarisera avec des fonctions et des protocoles qui doivent lui permettre de gérer entre autres les:

- les droits d'accès,
- le trafic des données circulant sur le réseau,
- la sauvegarde des données,
- le bon fonctionnement des services notamment les services annuaires,
- les services de messagerie électronique et les services d'applications, etc.

Contenu de la matière

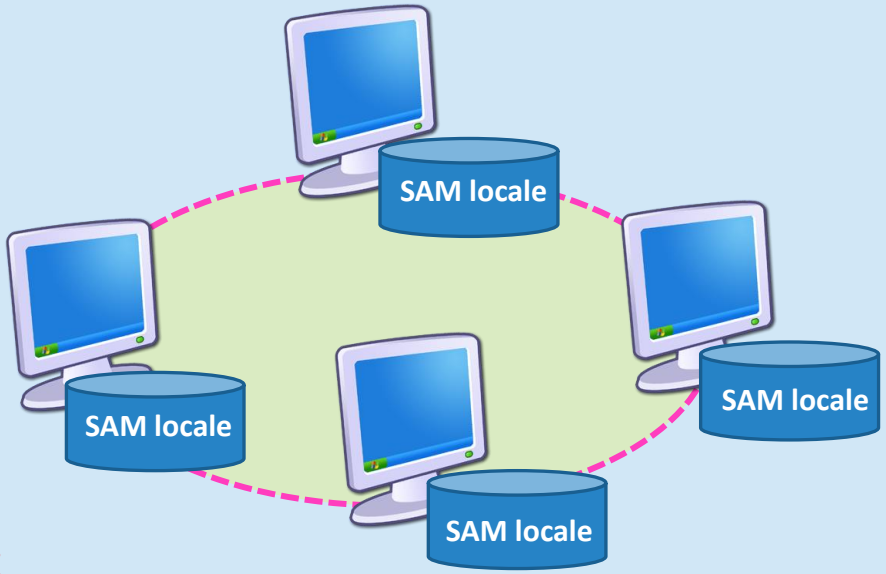
- **Chapitre 1**. Présentation de l'administration réseau,
- **Chapitre 2**. Le service SNMP (Simple Network Management Protocol)
- **Chapitre 3**. Les services annuaires
- **Chapitre 4**. Gestion des utilisateurs et service NFS
- **Chapitre 5**. Service de messagerie et services d'application
- **Chapitre 6**. Contrôleur de domaine

Chapitre 6. Contrôleur du domaine

- Introduction
- Présentation
- Architecture
  - Domaines
  - Arborescence,
  - Forêts
- Gestion des utilisateurs, des groupes et permissions
- Sécurité
- Gestion du domaine
- Notions d'approbations entre domaines
- Exemple d'un contrôleur de domaine (active directory AD)

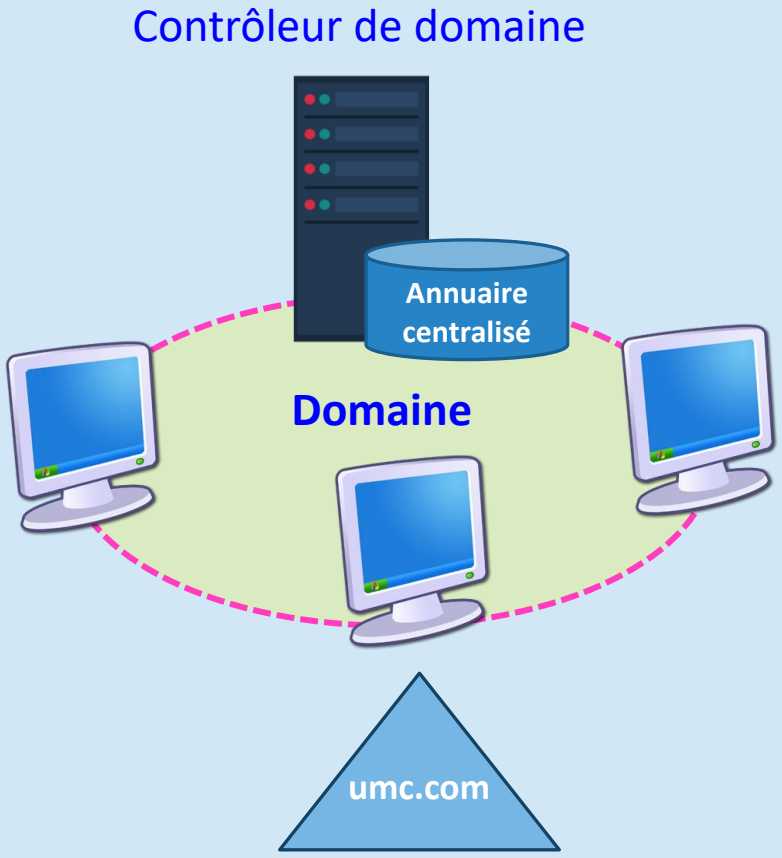
Groupe de travail vs Domaine

- **Groupe de travail** : toutes les machines sous Windows sont par défaut dans un groupe de travail nommé « **WORKGROUP** ».
- Il n'y a pas de notions **d'annuaire**, ni de **centralisation**
- **SAM**: chaque machine contient sa propre base d'utilisateurs indépendante les unes des autres, nommée SAM (Security Account Manager) ou gestionnaire des comptes de sécurité.
- **Avantage**: simple a mettre en œuvre, notamment pour le partage de fichiers entre quelques machines.
- **Problème**: ce modèle devient très vite inadapté dès que le nombre de postes et d'utilisateurs augmente, car cela devient lourd en administration.
- **Solution**: passage au modèle « **Domaine** ».



Groupe de travail vs Domaine

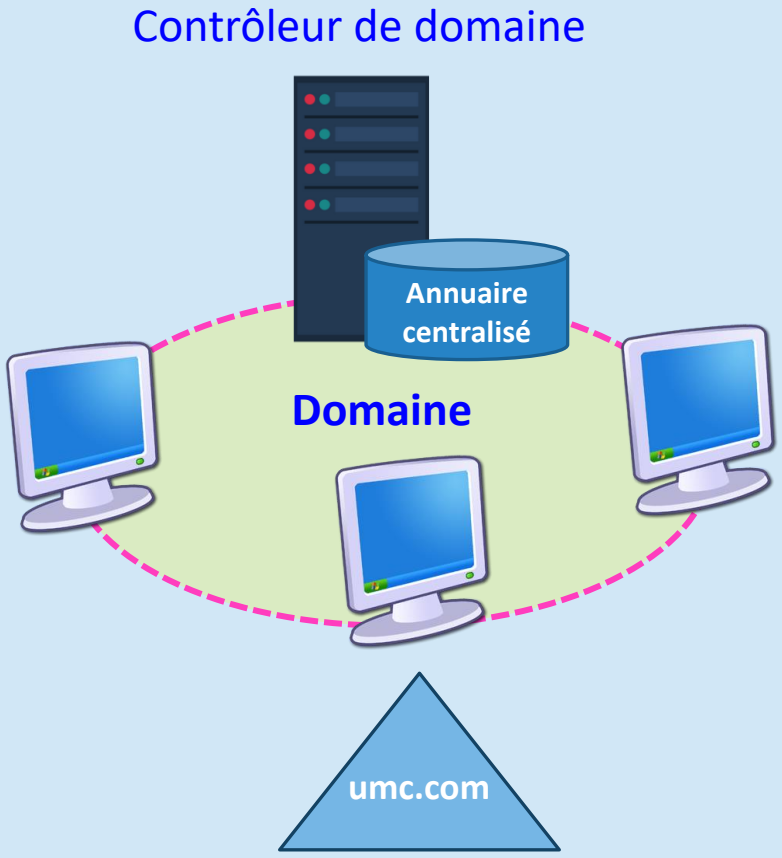
- **Domaine**: se réfère à un regroupement logique de serveurs et de machines clientes dans un réseau local.
- Base d'utilisateurs, de groupes et d'ordinateurs centralisée
- Ouverture de session unique par utilisateur
- Administration est gestion de sécurité centralisée
- Synchronisation de la base de données entre tous les contrôleurs de domaines
- Les domaines sont principalement utilisés dans le cadre des **entreprises**, pour gérer de **manière centralisée** les ressources du réseau (e.g., les utilisateurs, les machines, les imprimantes, les données, etc.



Symbolisation d'un domaine

Groupe de travail vs Domaine

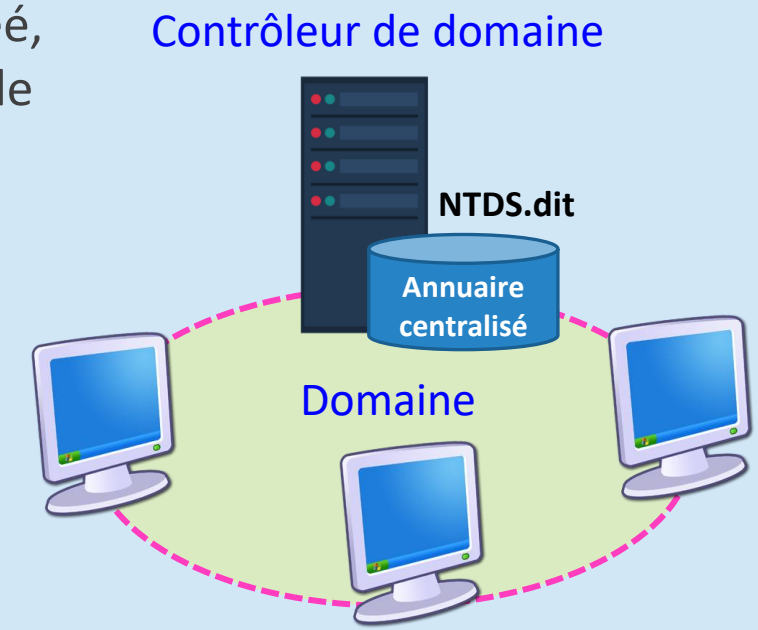
- **Contrôleur de domaine**: un domain est géré par un serveur appelé contrôleur de domaine, qui est chargé d'autoriser les machines à rejoindre le domaine et d'autoriser les utilisateurs à accéder aux ressources de l'ensemble du domaine.
- **Avantages**: Il permet à l'administrateur système de gérer plus efficacement les utilisateurs des stations déployées au sein de l'entreprise, car toutes ces informations sont centralisées dans une même base de données (**annuaire**) stockée dans un contrôleur de domaine.



Symbolisation d'un domaine

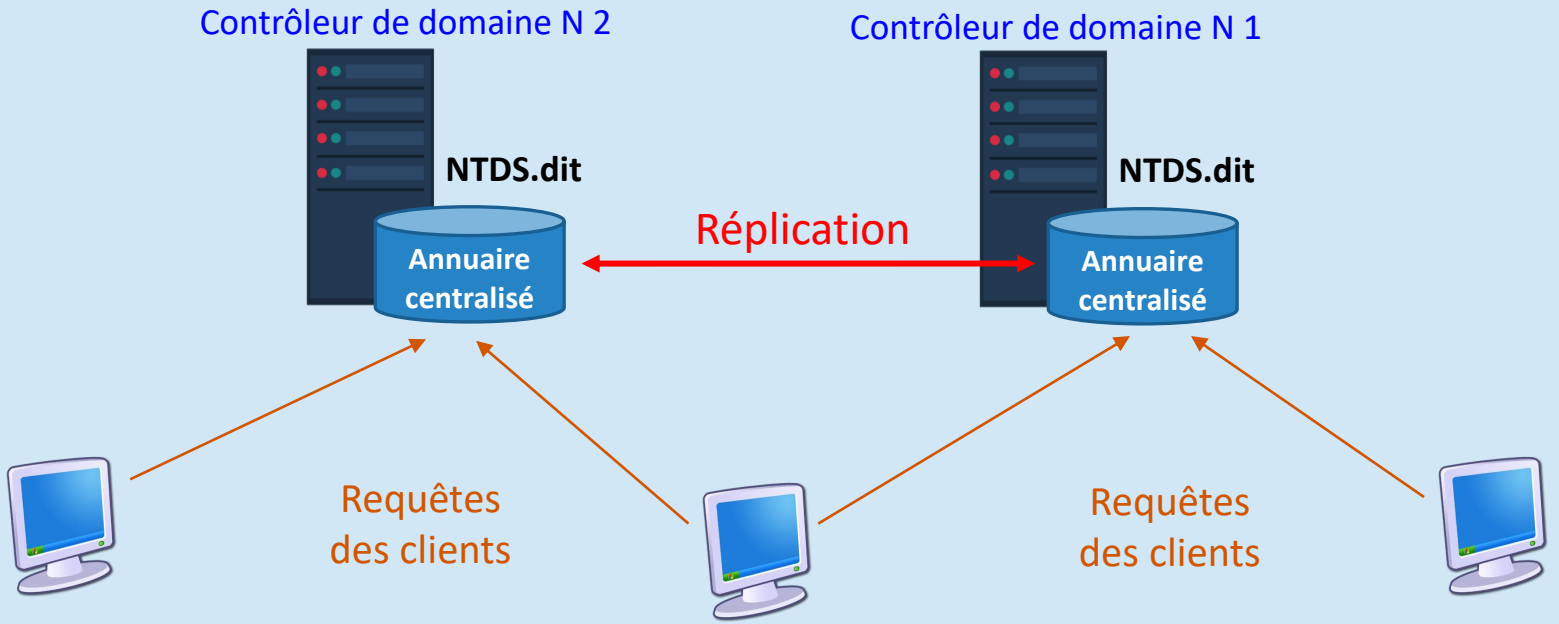
Contrôleur de domaine

- **Contrôleur de domaine :** est le serveur depuis lequel on effectue la création d'un domaine. Il devient contrôleur du domaine créé, ce qui implique qu'il sera au cœur des requêtes à destination de ce domaine.
- Il permet de:
  - Traiter les demandes d'authentification,
  - Veiller à l'application des stratégies de groupe,
  - Stocker une copie de l'annuaire Active Directory.
  - Vérifier les identifications des objets (utilisateurs, ordinateurs, groupes, etc.),
- Sur chaque contrôleur de domaine, on trouve une copie de la base de données de l'annuaire. Cette copie est symbolisée par un fichier « **NTDS.dit** » qui contient l'ensemble des données de l'annuaire.



Contrôleur de domaine

- **Recommandation**: au minimum deux contrôleurs de domaine (primaire
- La réplication entre les contrôleurs de domaines s'effectue via le protocole **DFSR** (Distributed File System Replication).
- Avant Windows server 2008, c' était le mécanisme **FRS** (File Replication Service)



Active Directory

- **Active Directory (AD):** est un service d'annuaire LDAP développé par Microsoft en **1996** et destiné à être installé sur les serveurs Windows (2000, 2003, 2008, 2012, etc.).
- **Objets**: AD contient différents objets, de différents types (e.g., utilisateurs, ordinateurs, imprimantes, serveurs, groupes, des unités d'organisation, etc.),
- **Classes d'objets**: les objets correspondent à des classes d'objets, c'est-à-dire des objets disposant des mêmes attributs.
- **Objectif:** centraliser deux fonctionnalités essentielles : l'identification et l'authentification au sein d'un système d'information

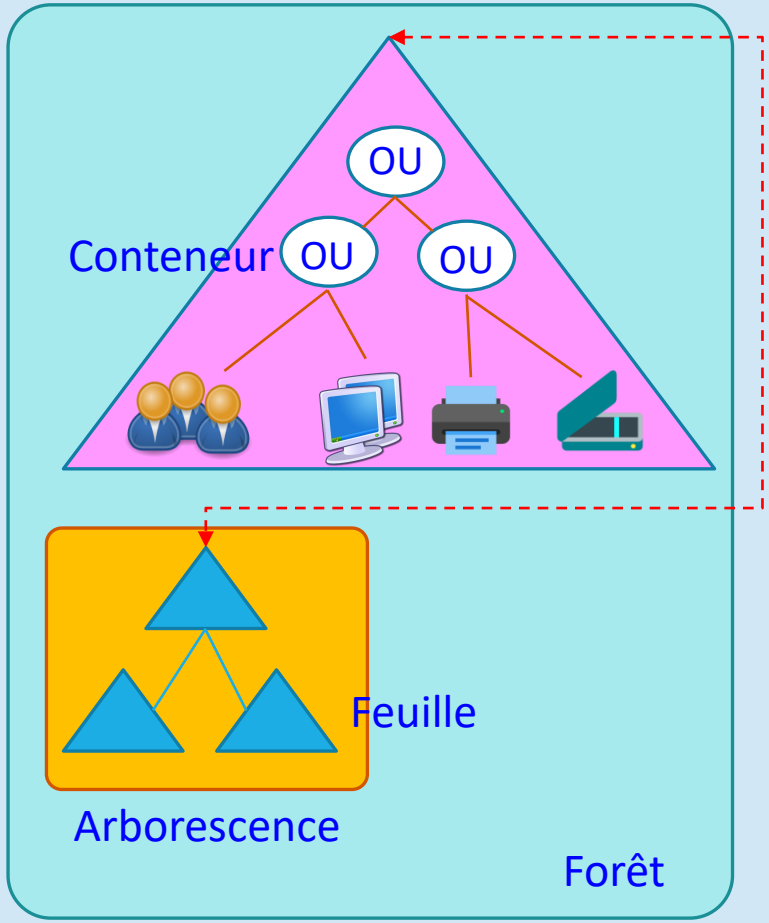
Fonctionnalités de l'AD

- Gestion centralisée des ressources du réseau.
- Accès aux informations concernant les ressources du réseau.
- Transparence des protocoles et de la topologie physique du réseau: gestion des ressources sans liens avec la disposition réelle où les protocoles réseaux employés.
- Assurer l'évolutivité du réseau.
- Possibilité d'exécution en tant qu'un service indépendant du système d'exploitation: plusieurs instances AD peuvent s'exécuter simultanément sur un serveur unique, chaque instance étant configurable de manière indépendante.

Microsoft
Active Directory

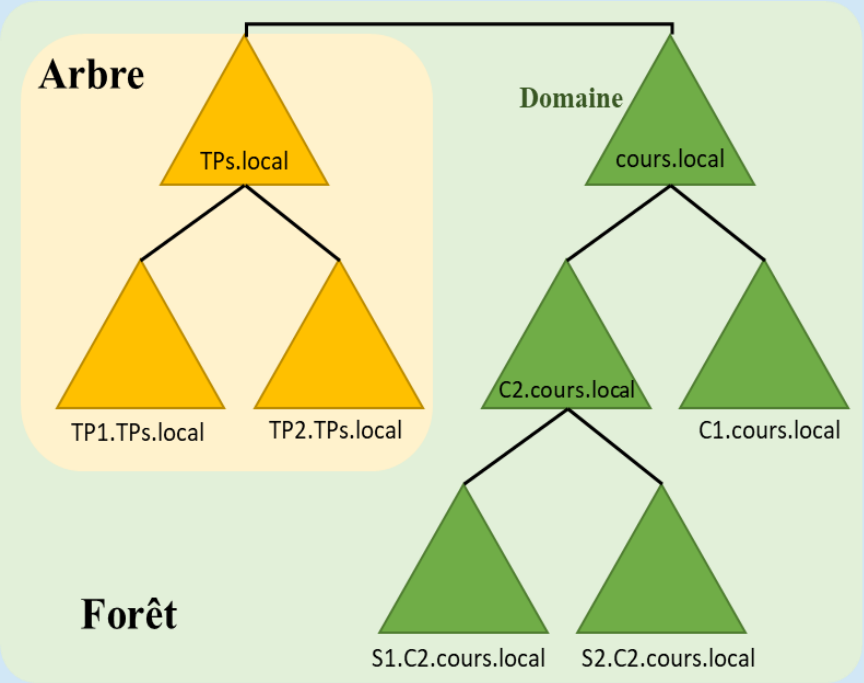
Structure logique de l'AD

- Par défaut, l'annuaire AD contient des instances d'objets de différents types.
- Chaque objet possède une identification unique et un certain nombre d'attributs regroupant diverses informations permettant par exemple d'effectuer des recherches précises dans l'annuaire.
- Les objets de l'AD sont tous organisés de manière hiérarchique.
- **Unités organisationnelles (OU)** : sont des objets conteneur et peuvent être imbriquées dans d'autres unités d'organisation ou conteneurs
- **Feuille**: si l'objet est au plus bas niveau de la hiérarchie, il est appelé « Feuille ».
- Les objets de l'AD sont classes en trois catégories
  - **Les ressources réseaux** : ordinateurs, serveurs, imprimantes, scanners, dossiers partagés, etc.
  - **Les utilisateurs** : les individuels et groupes d'utilisateurs, c'est-à-dire des listes d'utilisateurs avec leurs droits et leurs services.
  - **Les services réseau** : tels que les courriers électroniques, les espaces de stockage, etc.



Structure logique de l'AD

- **Arbre** : un arbre est un regroupement hiérarchique de plusieurs domaines.
- **Forêt** : une forêt est un regroupement d'une ou plusieurs arborescences de domaine, autrement dit d'un ou plusieurs arbres.
- Les arborescences de domaine sont indépendantes et distinctes bien qu'elles soient dans la même forêt.
- Les domaines d'une forêt fonctionnent de façon indépendante, mais la forêt facilite les communications entre les domaines dans toute l'architecture.
- **De manière générale, une forêt est un ensemble d'arbres, qu'un arbre est constitué d'une racine et potentiellement de branches qui sont représentées par des domaines et des sous-domaines.**



Structure physique de l'AD

- **Contrôleur de domaine:** est un ordinateur exécutant Windows Server qui stocke une copie de l'annuaire. Il assure la propagation des modifications faites sur l'annuaire, assure l'authentification et l'ouverture des sessions des utilisateurs, ainsi que les recherches dans l'annuaire.
- **Les sites** : sont des ensembles de plusieurs sous-réseaux IP reliés entre eux par des liaisons à haut débit.

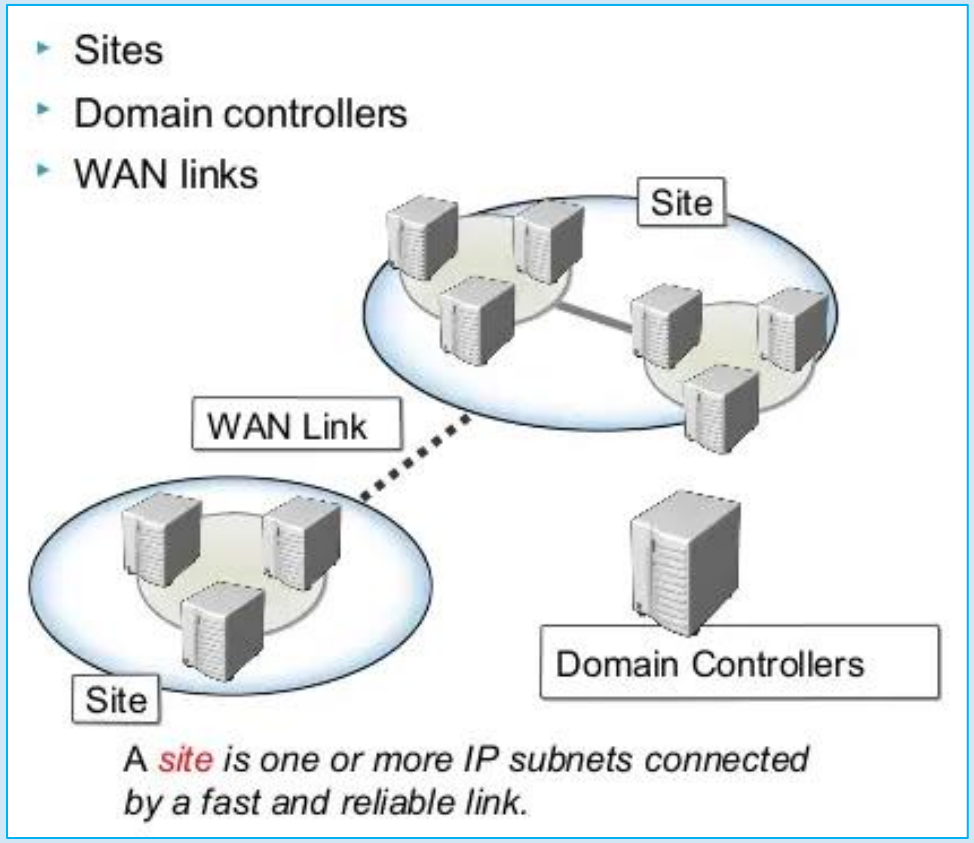


Schéma de l'AD

- **Le schéma AD** permet de stocker la définition formelle de tous les objets disponibles et autorisés au sein d'un annuaire AD.
- Il est unique au sein d'une forêt, ce qui permet une homogénéité de l'ensemble des domaines.
- Il possède deux types de définitions :
  - **Les classes d'objets**: décrit les objets de l'AD (e.g., utilisateur, ordinateur, imprimante, etc.). Chaque classe d'objets est un ensemble d'attributs
  - **Les attributs**: sont définies séparément des classes d'objets. Chaque attribut n'est défini qu'une seule fois et peut-être utilisé dans plusieurs classes d'objets. Par exemple, l'attribut « **Description** » est utilisé dans de nombreuses classes d'objets, mais il n'est défini qu'une seule fois dans le schéma afin de préserver la cohérence.
- Le schéma est par défaut protégé et seuls les membres du groupe « Administrateurs du schéma » peuvent effectuer des modification

Active Directory

Active Directory s'appuie donc sur une organisation des machines en domaines DNS, dont il assure la bonne intégration ; sur une centralisation des informations des membres du réseau (machines, utilisateurs, ….) dans un annuaire LDAP ; sur une sécurisation forte par le protocole d'authentification Kerberos ; sur des partages de ressources (dossiers, imprimantes, etc.) par le protocole SMB/CIFS.

Gestion des groupes

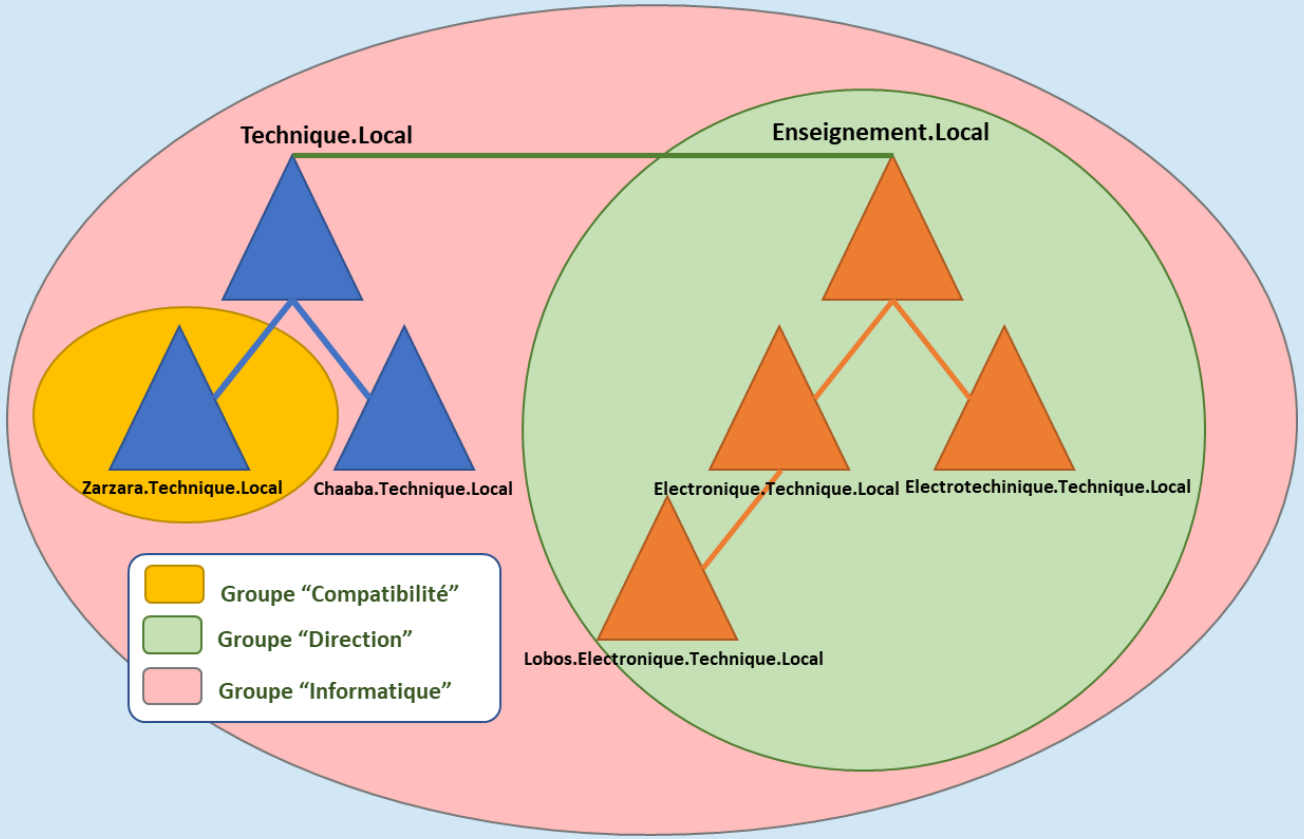
- **Classe d'objets « groupe »:** regroupe des objets au sein d'un groupe, notamment pour simplifier l'administration.
- **Exemple :** attribution de droits à un service « informatique » qui correspond à un groupe nommé « informatique ».
- Un groupe permet également de simplifier la gestion des droits d'accès aux fichiers partagés par les différents utilisateurs de domaine.
- **L'étendue du groupe** : corresponds à sa portée au niveau de l'arborescence AD. Il existe trois étendues différentes:
  - **Domaine local** : un groupe qui dispose d'une étendue « domaine local » peut être utilisé uniquement dans le domaine dans lequel il est créé.
  - **Domaine Globale** : un groupe ayant une étendue « globale » pourra être utilisé dans le domaine local, mais aussi dans tous les domaines approuvés par le domaine de base.
  - **Domaine Universelle** : un groupe disposant de l'étendue « universelle » à une portée maximale puisqu'il est accessible dans l'ensemble de la forêt, ce qui implique qu'il soit disponible sur tous les domaines de la forêt.

Gestion des groupes

Exemple : soit les trois groupes suivants et leurs étendues cohérentes :

- **Comptabilité :** étendue « domaine local » sur « Enseignement.Local ».
- **Direction :** étendue « globale » sur « Enseignement.Local» qui approuve tous les sous-domaines.
- **Informatique :** étendue « universelle » sur la forêt.

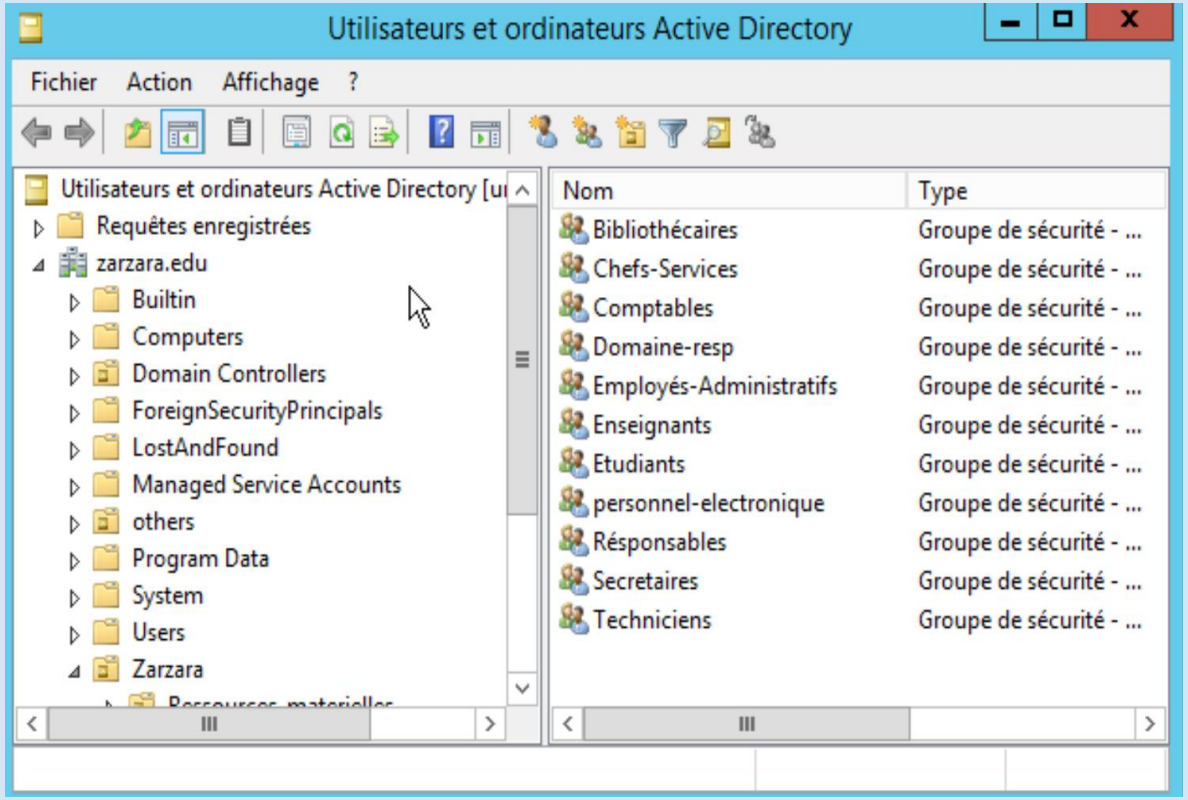
Ainsi, la portée de ces groupes pourra être schématisée comme ceci au sein de la forêt.



Gestion des groupes

Type du groupe : il existe deux types :

- **Sécurité** : ils permettent d'utiliser les groupes pour gérer les autorisations d'accès aux ressources.
- **Distribution** : l'objectif de ce type de groupe n'est pas de faire du contrôle d'accès, mais plutôt des listes de distribution. Par exemple, créer une liste de distribution d'adresses e-mail en ajoutant des contacts. Ces groupes sont utilisés principalement par des applications de messagerie, comme Microsoft Exchange.

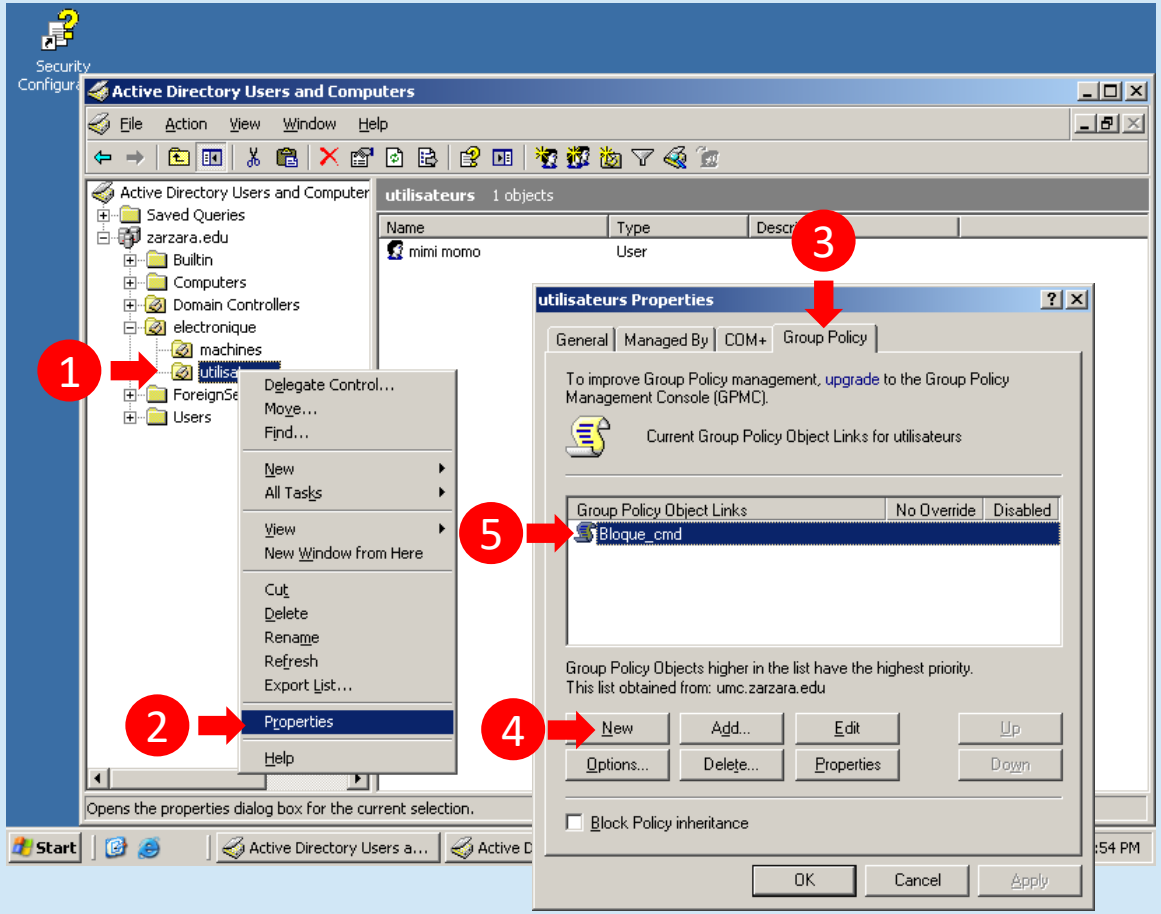


Sécurité: GPO

- À fin d'augmenter la capacité de sécurisation d'un réseau informatique, l'environnement AD offre des stratégies de groupe. Ces derniers peuvent être utilisés pour modifier la configuration et les droits d'accès aux postes de travail et des serveurs ainsi que des données du réseau.
- Par exemple, elles peuvent être utilisées pour contrôler des clés de registre, la sécurité NTFS, la politique de sécurité et d'audit, l'installation de logiciel, les scripts de connexion et de déconnexion, la redirection des dossiers, et les paramètres d'Internet Explorer.
- Plus particulièrement, les GPO peuvent être utilisées pour :
  - imposer un niveau de sécurité ;
  - créer des configurations communes ;
  - simplifier le processus d'installation des ordinateurs ;
  - limiter la distribution d'applications.

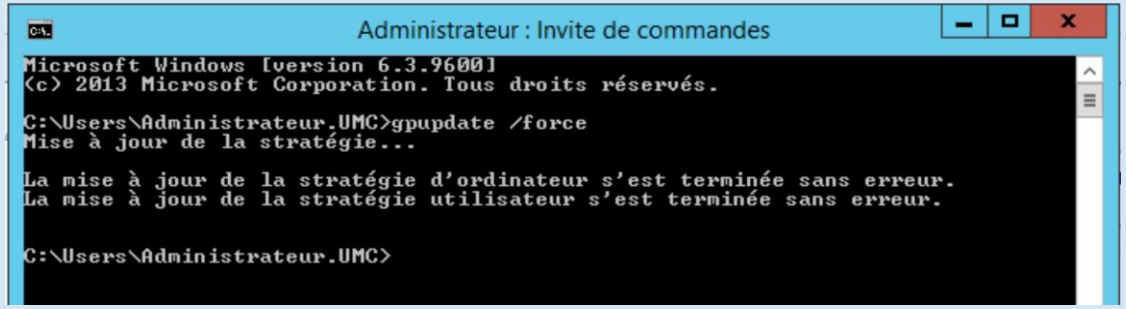
Exemple de GPO

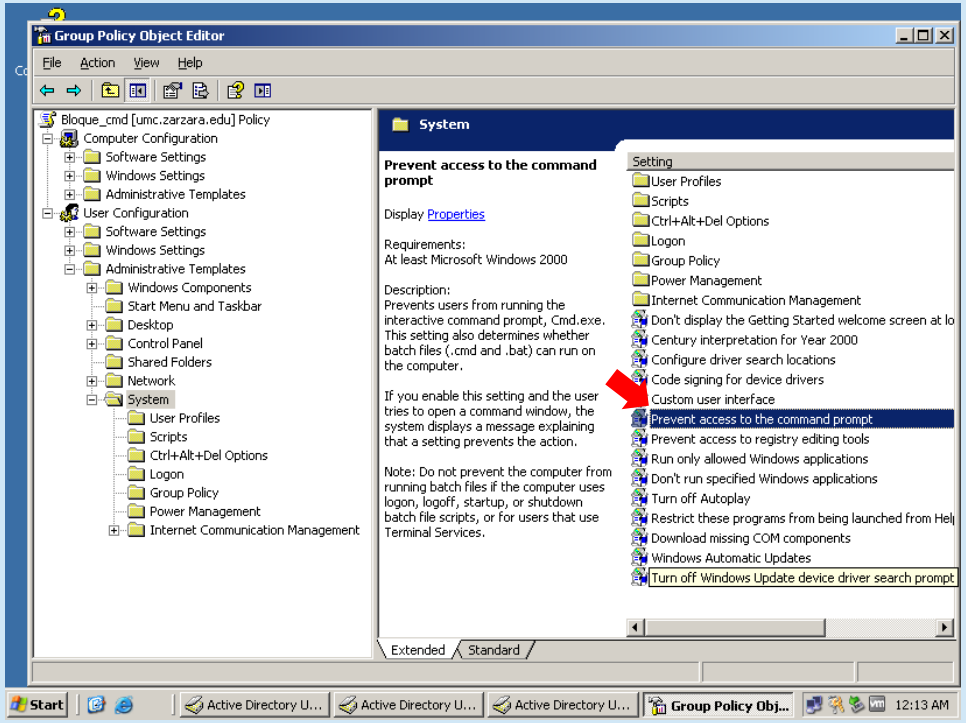
- **Exemple**: nous allons créé la stratégie « **Bloque_cmd** » pour bloquer l'accès au terminal de commandes (CMD) aux étudiants et personnel administratif.
- Ce dernier permet une communication directe entre l'utilisateur et le système d'exploitation, ainsi que d'exécuter divers programmes en ligne de commande. Ce qui donne aux utilisateurs malveillants la possibilité d'exécuter des commandes qui peuvent endommager le réseau de la faculté. Il est donc préférable de la désactiver pour les utilisateurs ordinaires.



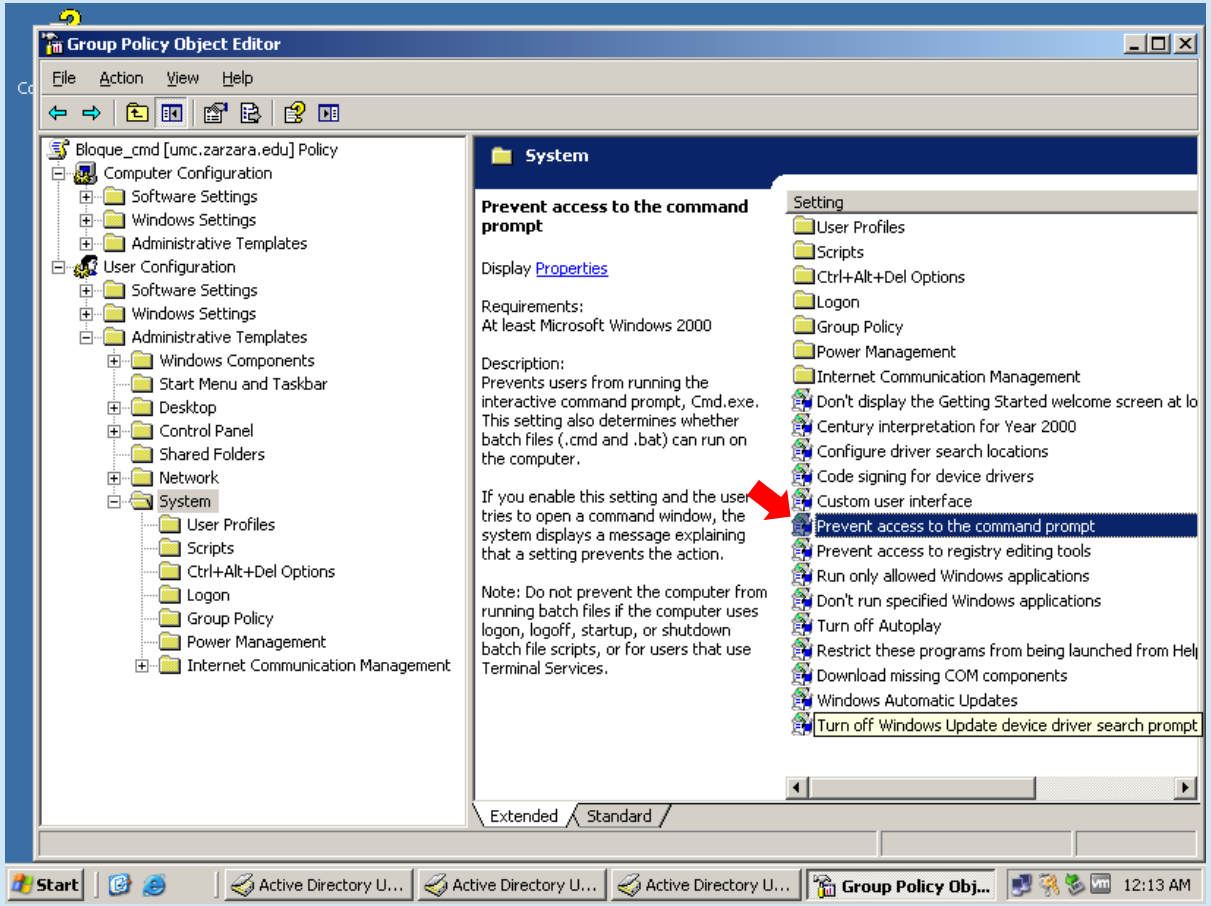
Exemple de GPO

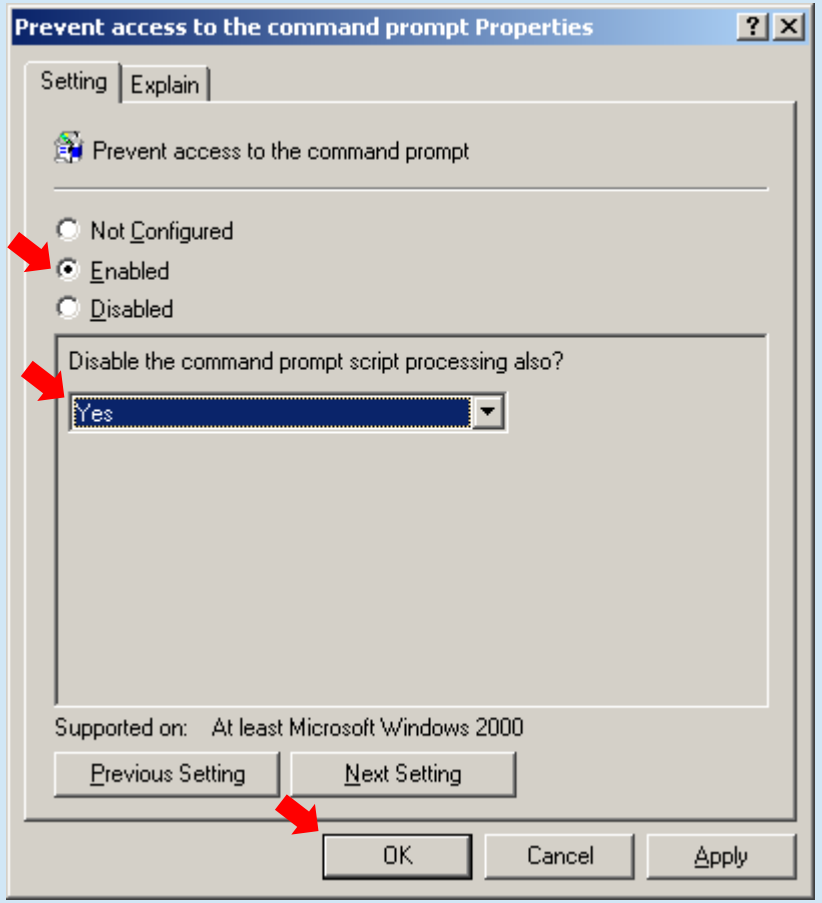
- Activé l'option « **désactiver l'accès à l'invite de commandes DOS** » à partir de l'arborescence « **Utilisateur/modèle d'administration/système » en suite tu trouva "Désactiver l'accés à l'invite de commande" que tu doit l'activer,**
- Afin que le serveur puisse prendre en compte plus rapidement ces GPO, nous avons exécuté la commande « **gpupdate** » dans le terminal.





Exemple de GPO





Exemple de GPO

La Figure montre la vérification de l'application de la stratégie « **Bloque_cmd** » depuis le compte étudiant « racha@zarzara.edu».
Le message « **l'invite de commandes a été désactiver par votre administrateur** » ci-dessous sera affiché lorsqu'un étudiant ou un personnel administratif tentera de le faire