CÉGEP ÉDOUARD MONTPETIT

Services de domaines
Active Directory

420-2S5-EM Serveurs 1: Services intranet

Module 4 – Domaines Active Directory

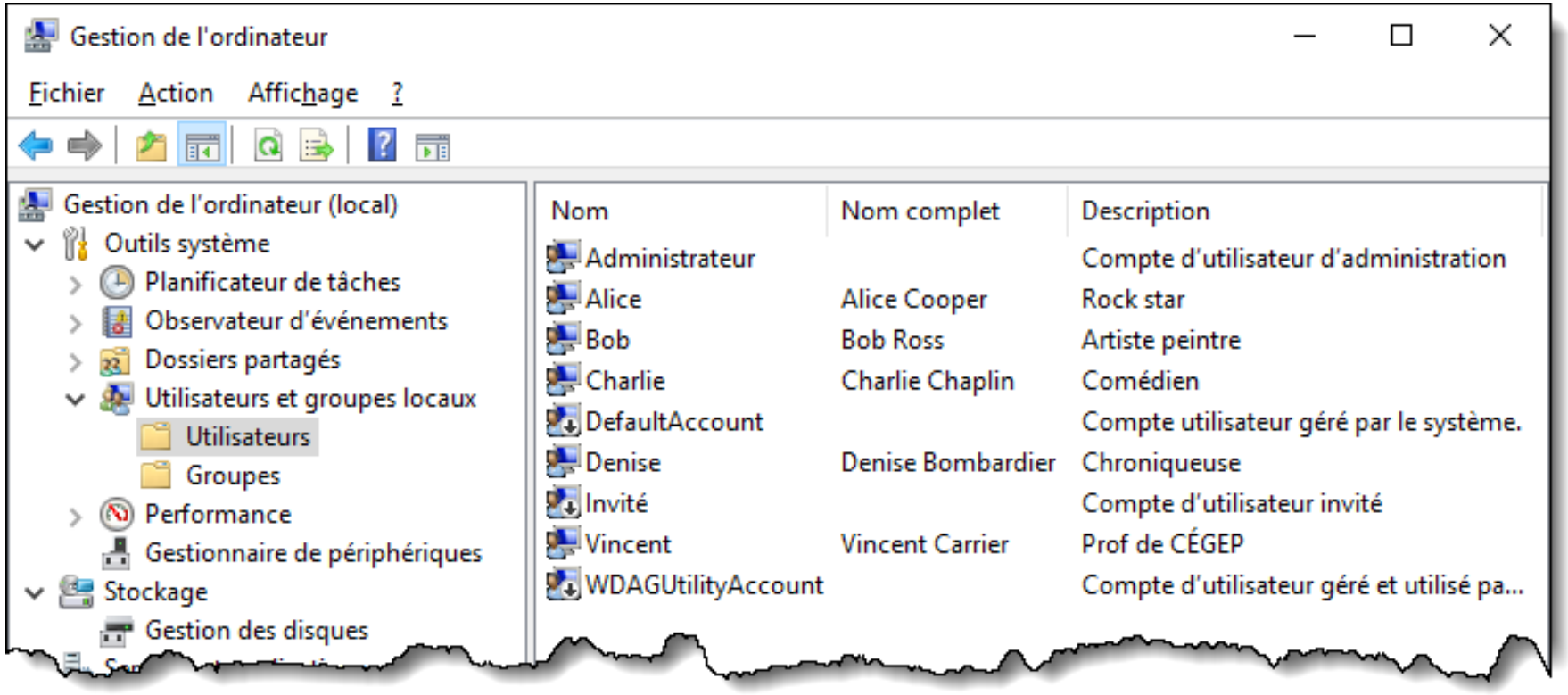
Prof.: Gabriel Gaudreault (Crédit: Vincent Carrier)

Rappel: Gestion des utilisateurs

- Windows est un système d'exploitation multi-utilisateurs
- Chaque utilisateur possède:
  - Un compte (nom d'utilisateur, mot de passe…)
  - Un profil pour stocker des fichiers personnels et sauvegarder des paramètres
  - Des privilèges sur le système d'exploitation (utilisateur régulier, administrateur, etc.)
  - Des permissions d'accès à des ressources, telles que des répertoires et des fichiers

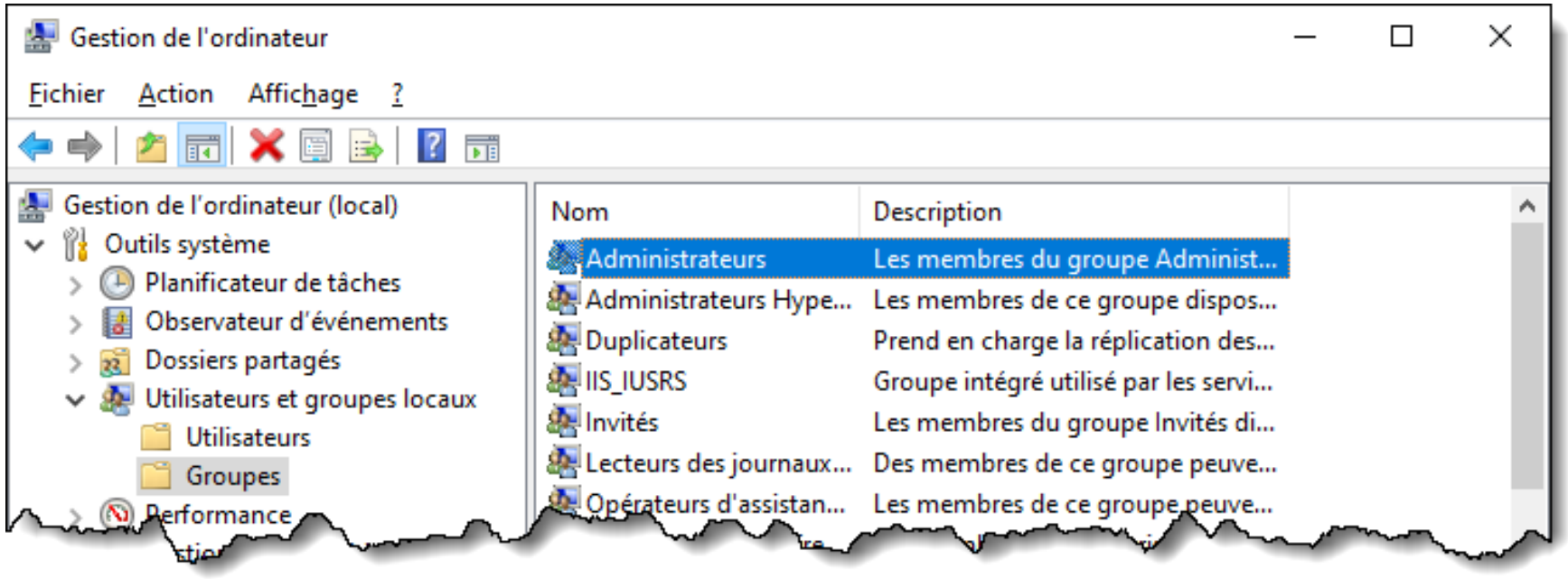
Comptes utilisateurs (local)

Les comptes utilisateurs sont configurés **localement** sur l'ordinateur.



Groupes d'utilisateurs (local)

Les groupes sont définis aussi localement sur l'ordinateur, et permettent l'attribution de permissions et de privilèges aux utilisateurs du système.



Problématique

Gérer les utilisateurs ainsi est très difficile à faire efficacement et de manière sécuritaire dans les grands parcs informatiques.

- Gestion des mots de passe
- Changements: embauche et départ d'un employé
- Un compte sur une machine est différent d'un compte du même nom sur une autre machine. Ce n'est pas la même identité.

Gestion centralisée de l'identité

- Les comptes sont définis centralement
- Les sessions des utilisateurs sont établies en authentifiant l'utilisateur via ce service centralisé
- Un utilisateur n'a qu'un compte, et celui-ci lui procure des privilèges et des permissions sur d'autres systèmes qui composent le réseau
- Plus sécuritaire, car l'utilisation d'un tel compte est traçable lors d'audits de sécurité

Active Directory

Active Directory **Domain Services** (ADDS)

Active Directory **Certificate Services** (ADCS)

Active Directory **Federation Services** (ADFS)

Active Directory **Lightweight Directory Services** (ADLDS)

Azure Active Directory (AAD)

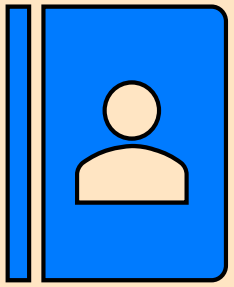
Active Directory Domain Services (AD DS)

- Offre un service centralisé de gestion d'identité, d'autorisation et d'authentification dans un réseau
- Répertorie, dans un annuaire, divers éléments composant le réseau, afin d'en faciliter la recherche:
  - Ordinateurs (serveurs et stations de travail)
  - Utilisateurs et groupes d'utilisateurs
  - Imprimantes
  - Dossiers partagés sur le réseau
- Stocke ces informations dans une base de données distribuée et répliquée, nativement redondante

Historique de Active Directory DS

- Lancé pour la première fois sous Windows 2000
- Son prédécesseur, NTDS, était disponible sous Windows NT, mais était beaucoup plus rudimentaire
- Avant Active Directory, le leader du marché était Novell Directory Service (NDS), beaucoup plus avancé et robuste que NTDS
- L'intégration d'AD au système d'exploitation Windows a provoqué l'obsolescence de NDS
- Plus de 90% des organisations utilisent Active Directory pour l'authentification et l'identification

Principaux services

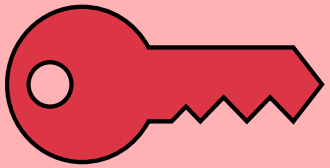


LDAP

Organisation et interrogation des objets (utilisateurs, ordinateurs, groupes, etc.) et leurs attributs dans une base de données de type annuaire.

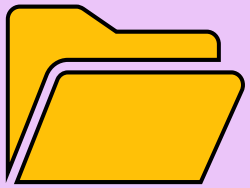
DNS

Résolution de noms des ordinateurs du réseau. Essentiel pour localiser les contrôleurs de domaine et autres serveurs.



Kerberos

Authentification centralisée pour gérer l'accès aux ressources du domaine.



DFS

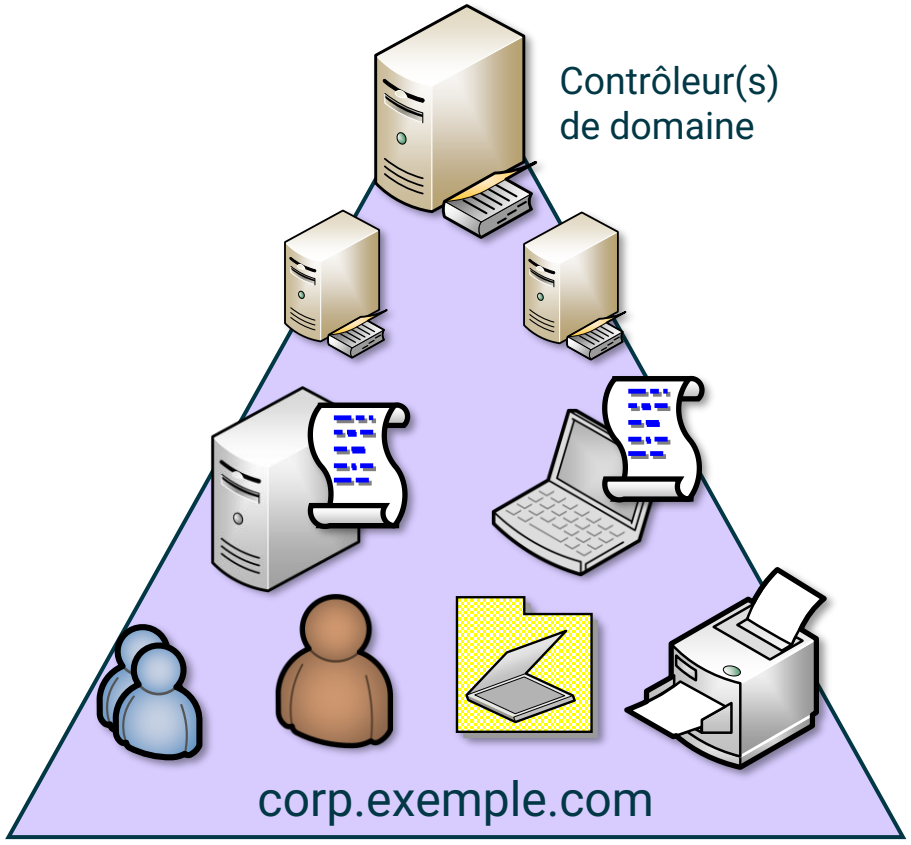
Partage de fichiers distribués et répliqués entre plusieurs serveurs mais disposant d'un lien commun.

NTP

Synchronisation des horloges système de tous les hôtes du réseau.

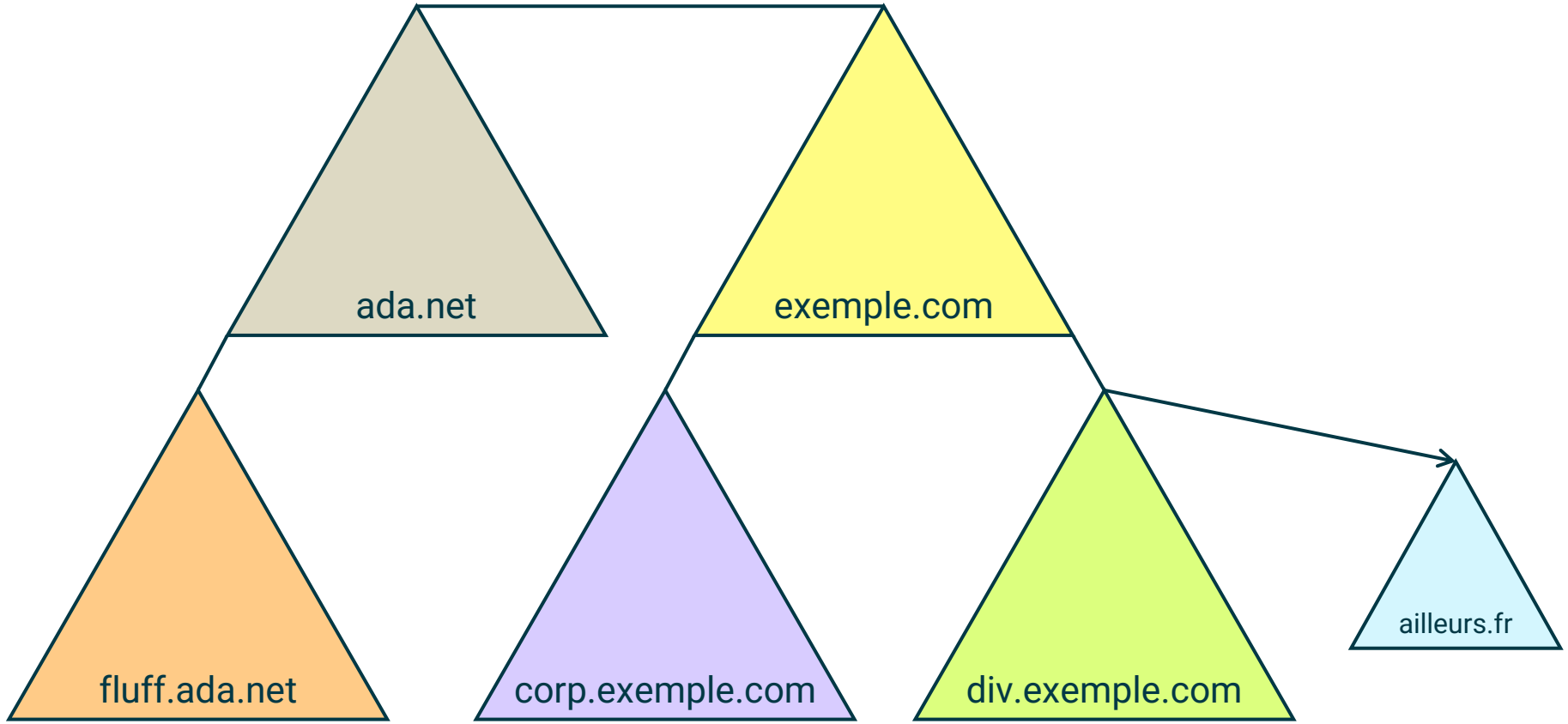
Qu’est-ce qu’un domaine AD?

- Un domaine (zone DNS)
- Un ou plusieurs contrôleurs de domaine
- Des objets de divers types:
  - Utilisateurs
  - Ordinateurs
  - Groupes
  - Stratégies de groupe (GPO)
  - Unités d’organisation (OU)
  - Autres (imprimantes, partages de fichiers…)



Architecture multi-domaines

- Domaine
- Arbre
- Forêt
- Approbations externes…



Création d'un domaine Active Directory

- Sélectionner le serveur qui agira à titre de contrôleur de domaine, (*Domain Controller*, ou DC) qui typiquement hébergera les services AD (DNS, LDAP, Kerberos, etc.)
- Installer le rôle Active Directory Domain Services à partir du Server Manager
- Effectuer la promotion du serveur au rang de contrôleur de domaine (DCPromo)
- Il n'est pas recommandé qu'un DC serve à autre chose qu'à l'hébergement des services de base de AD

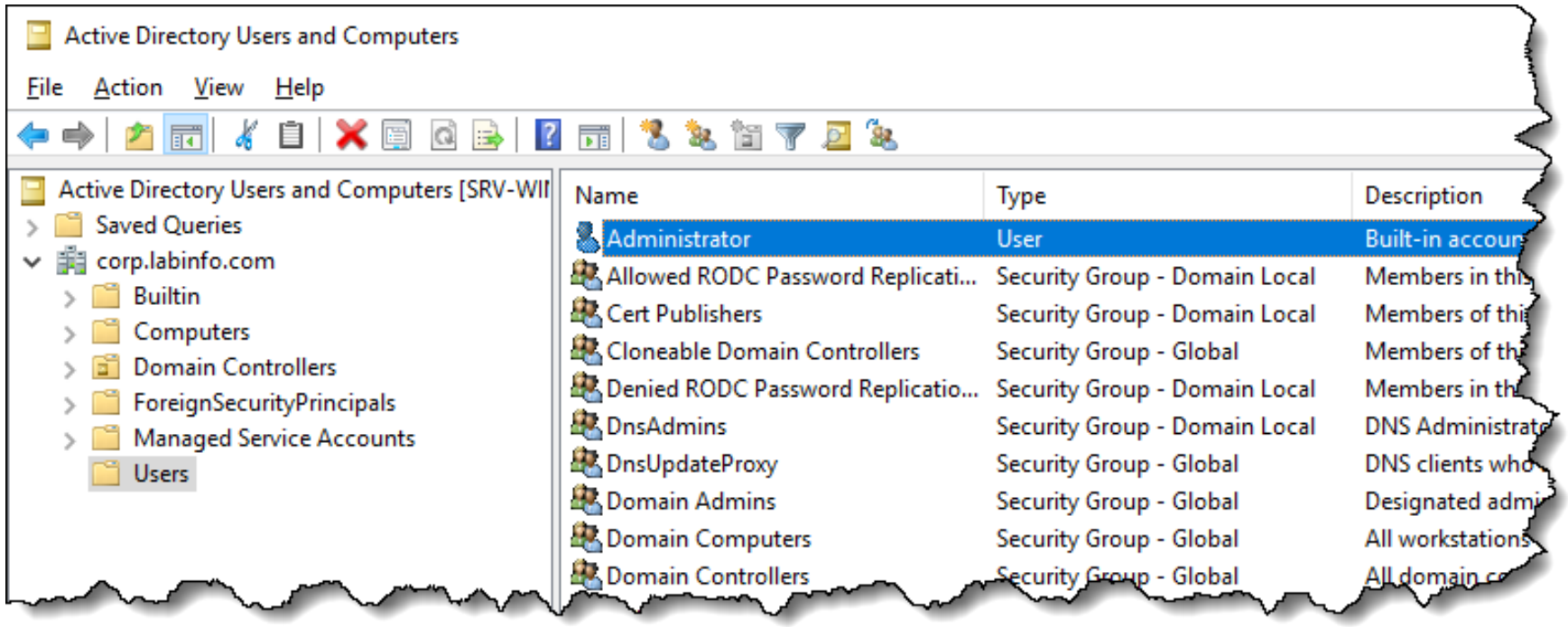
Nom du domaine

Un domaine Active Directory a deux noms:

- Nom NETBIOS:
  - Maximum 15 caractères
  - Typiquement en majuscules
  - Sert principalement à assurer une rétrocompatibilité
  - Exemple: ***LABORATOIRE***
- Nom DNS:
  - Zone DNS dédiée au domaine Active Directory
  - Typiquement un sous-domaine de la zone principale
  - Maximum de 253 caractères
  - Exemple: ***laboratoire.collegeem.qc.ca***

Utilisateurs et groupes AD

Le domaine possède sa propre liste d'utilisateurs et de groupes. Ils peuvent être utilisés sur toutes les machines du domaine.



Noms d'utilisateurs

Un utilisateur dans Active Directory a aussi plusieurs noms:

- Nom SAM (aussi appelé *sAMAccountName*, ou *Pre-Win2000*):
  - Maximum 19 caractères
  - Souvent préfixé avec le nom NETBIOS du domaine
  - Exemple: LABORATOIRE***1234567***
- Nom UPN (aussi appelé UserPrincipalName):
  - Maximum de 1024 caractères
  - Porte en suffixe le nom DNS du domaine (ou un de ses alias)
  - Souvent semblable à l'adresse courriel de l'utilisateur
  - Exemple: ***1234567***@cegepmontpetit.ca
- Nom LDAP
  - Seulement le nom de l'objet dans l'arborescence

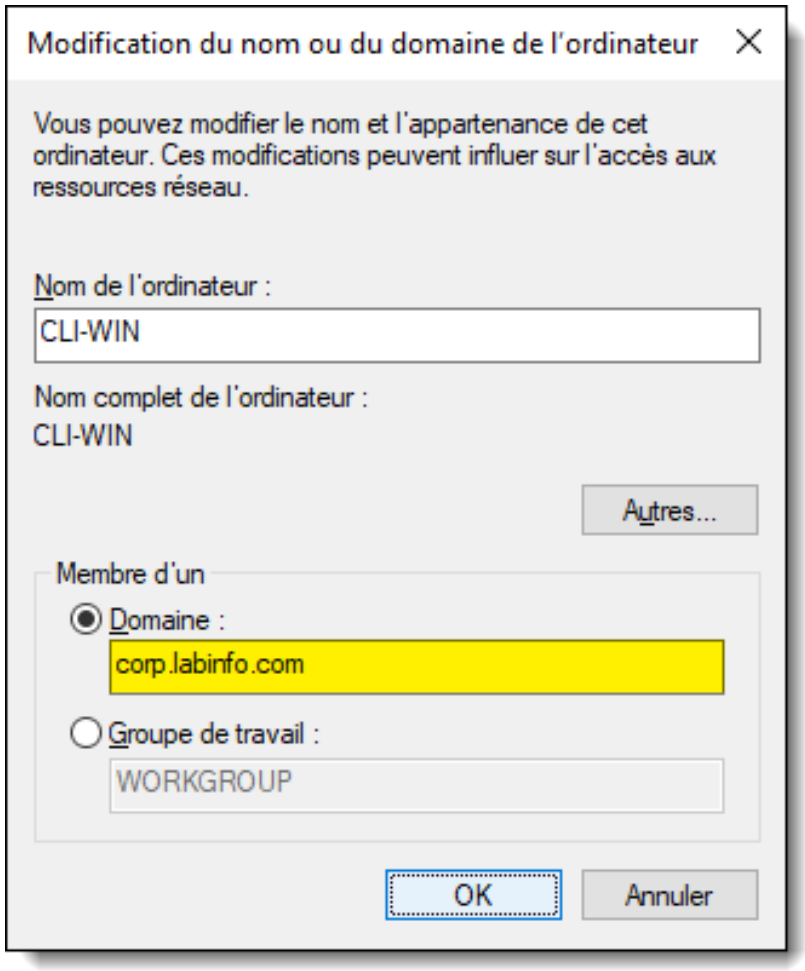
Jonction d'un ordinateur au domaine

Pour être pris en charge, on doit joindre les ordinateurs au domaine. On dit alors que ce sont des membres du domaine.

Les administrateurs du domaine ont ainsi une **autorité sur toutes les machines** du domaine.

Deux manières de joindre une machine:

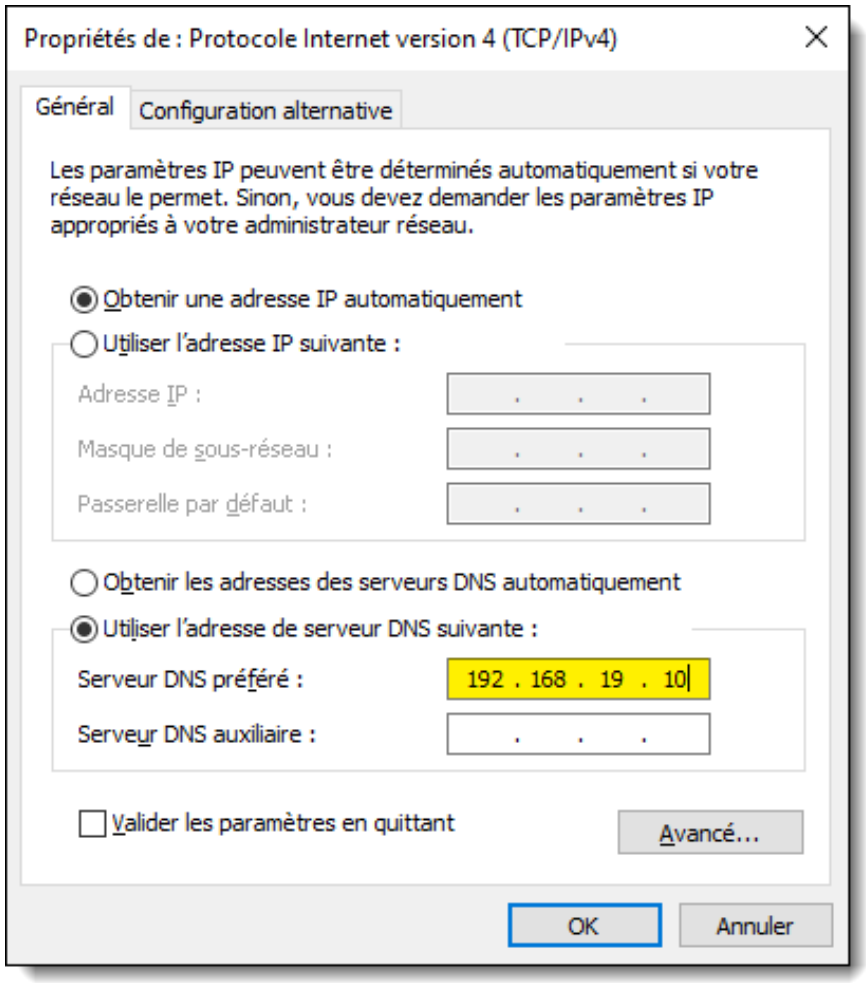
- Par le GUI: **sysdm.cpl**
- Avec PowerShell: **Add-Computer**



Configuration IP des membres AD

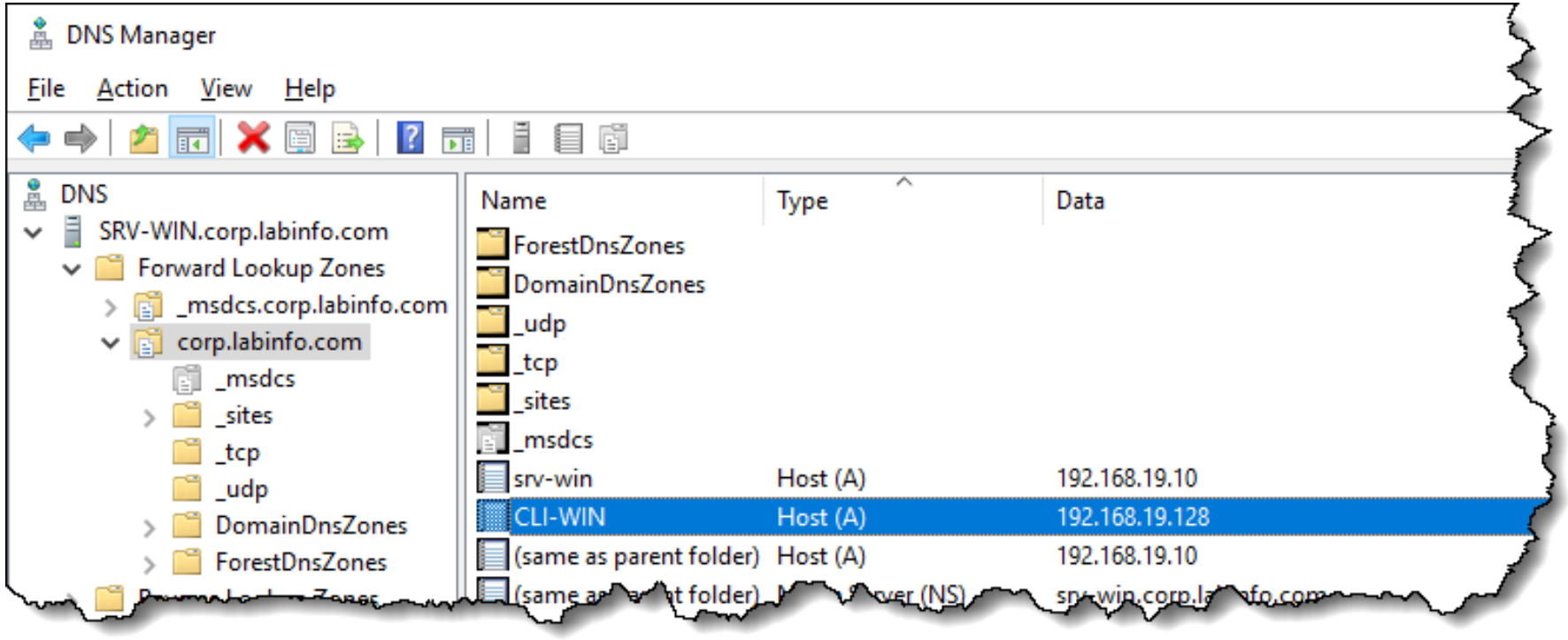
Pour joindre un domaine AD, il faut impérativement que les machines membres soient en mesure de résoudre le nom du domaine dans leur configuration DNS!!!

Ça peut aussi se configurer avec DHCP! ☺



Enregistrement DNS dynamique

Lorsqu'une machine devient membre d'un domaine AD, un enregistrement A est créé dans sa zone DNS.



Contrôleurs de domaine

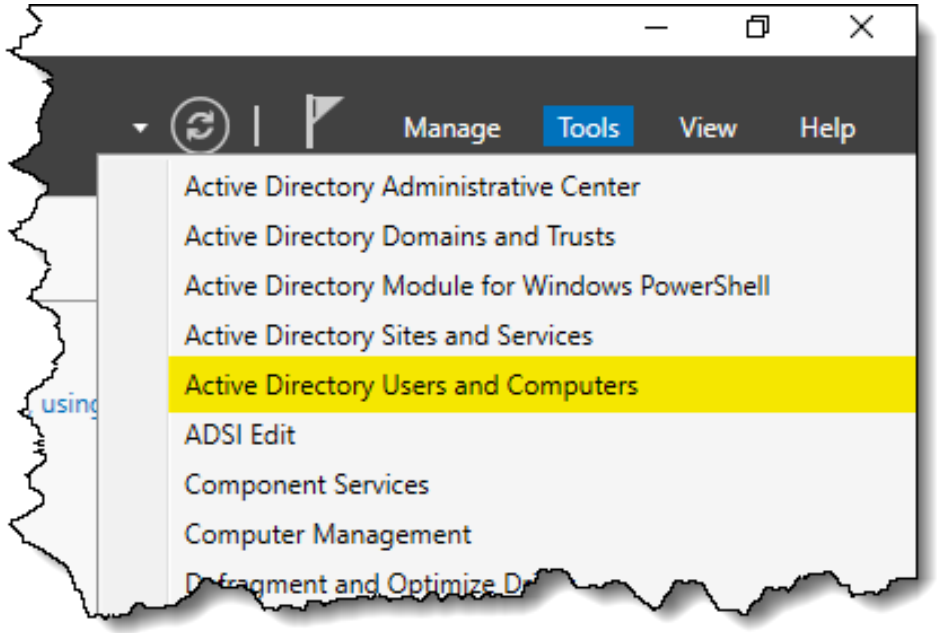
Le contrôleur de domaine est un point central d'Active Directory. Il est l'autorité de gestion du domaine.

- Conserve une copie de tout le contenu de la base de données et permet d'y accéder avec LDAP
- Traite les authentifications
- Réplique les informations avec les autres contrôleurs de domaine
- Doit être protégé! S'il est compromis, l'attaquant a tout pouvoir sur les systèmes de l'entreprise!!!

Outils de gestion du domaine

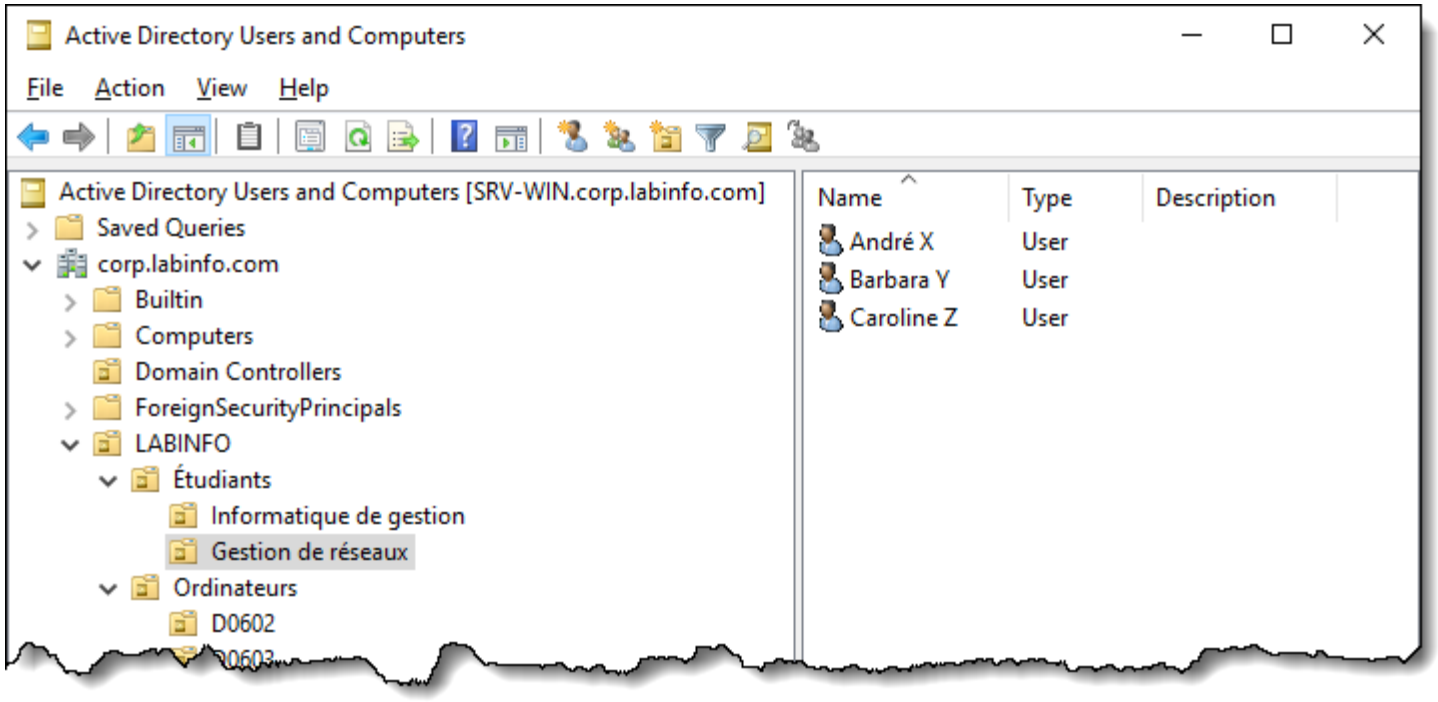
Plusieurs outils sont accessibles à partir du gestionnaire de serveur sur un contrôleur de domaine, mais peuvent être installés sur n'importe quelle machine Windows.

- Administrative Center
- Users and computers
- Sites and services
- Domains and trusts
- ADSI Edit



Organisation des objets

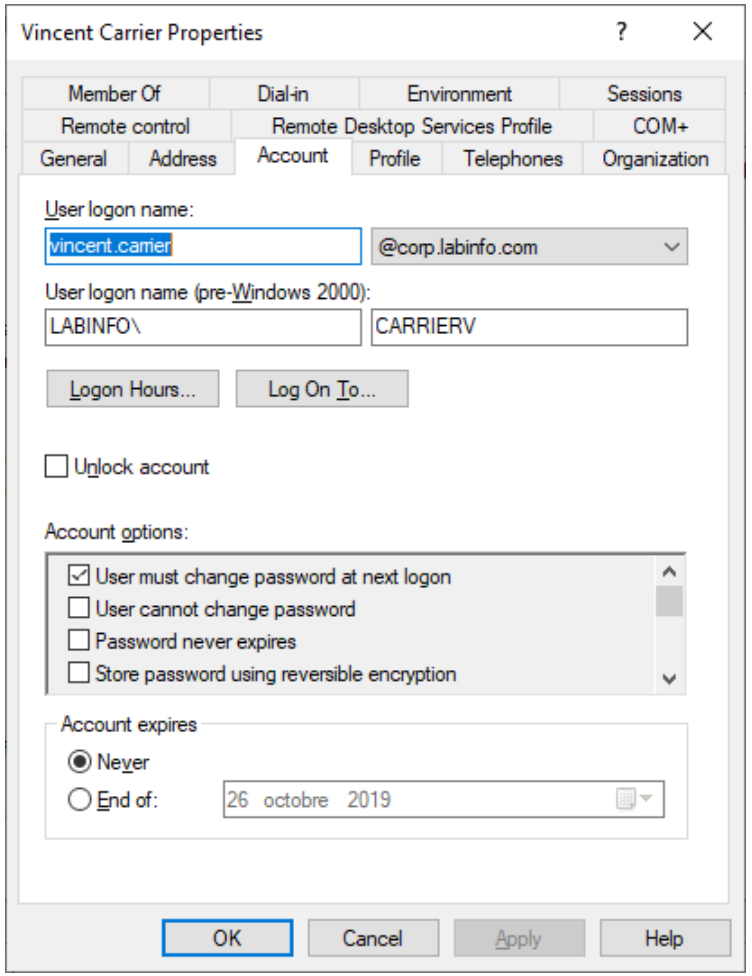
Les objets AD sont organisés dans une arborescence similaire à un système de fichiers, composée de conteneurs et d'unités organisationnelles (OU)



Objets utilisateurs

Permet d'authentifier un utilisateur et lui autoriser l'accès à une ressource.

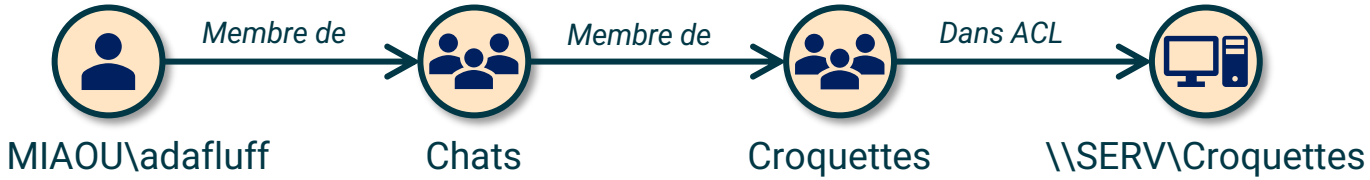
- Possède un mot de passe qu'il peut devoir changer au prochain démarrage
- Peut être membre de groupes
- Plusieurs autres options…

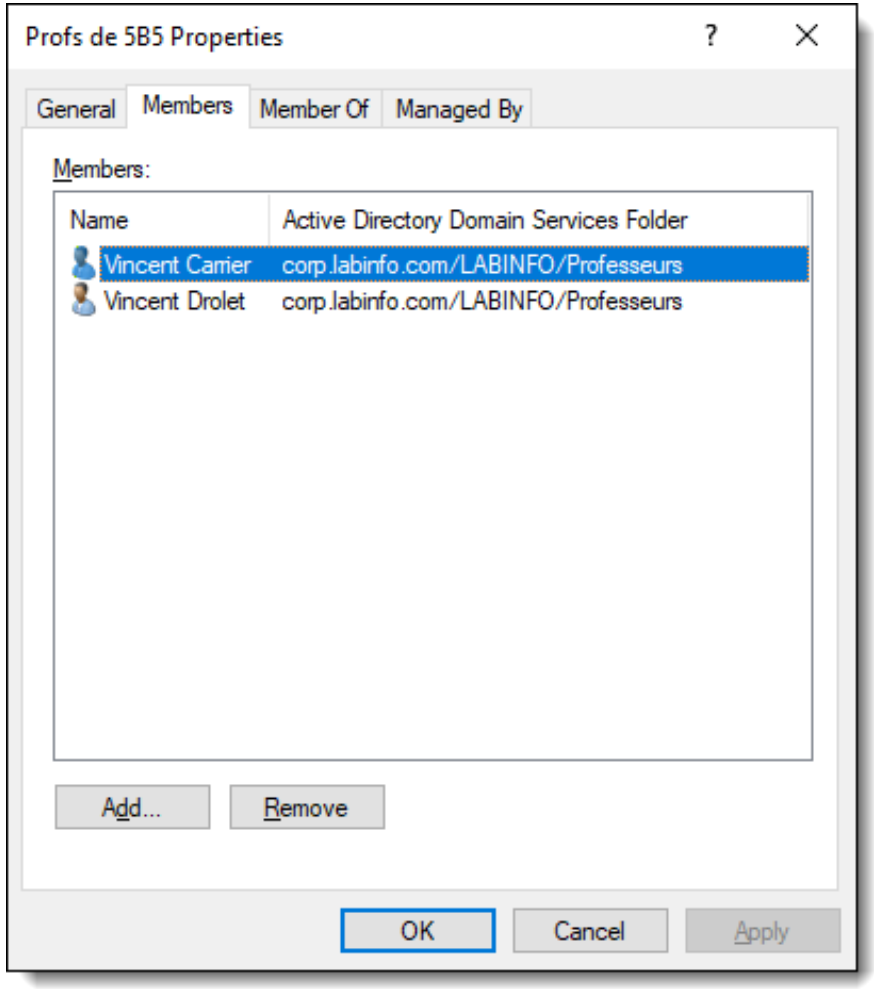


Objets groupes

Contient des utilisateurs

- On peut attribuer un accès à une ressource à un groupe pour donner accès à tous ses membres
- Un groupe peut contenir d'autres groupes (nesting)





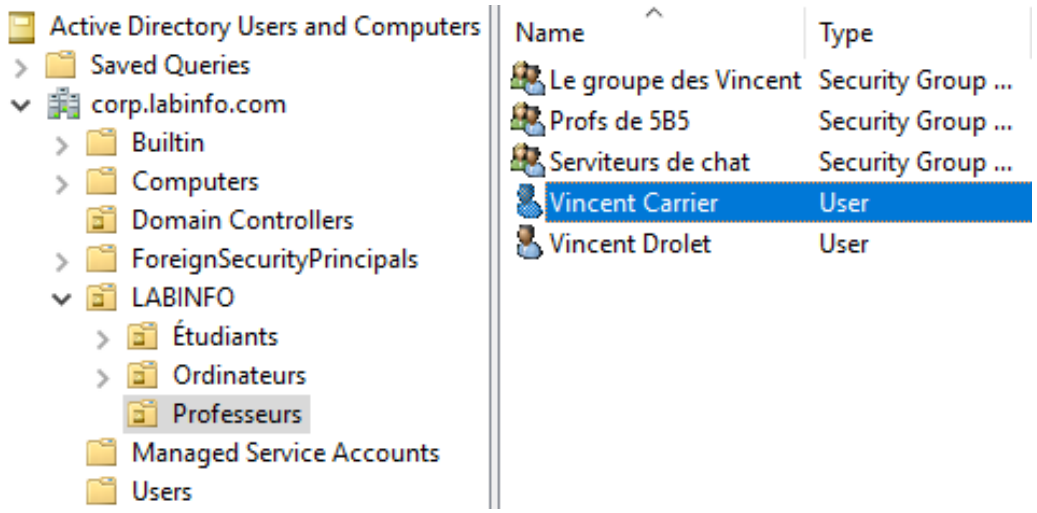
Objets ordinateurs

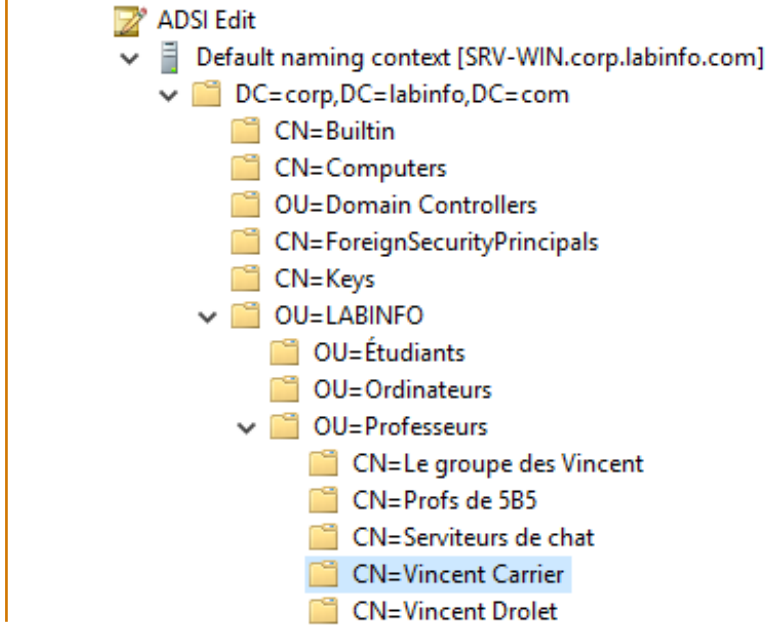
Comme un compte d'utilisateur pour un système

- La jonction au domaine crée un compte pour l'ordinateur membre
- Les mots de passe sont négociés régulièrement et automatiquement
- Peuvent aussi être membre d'un groupe
- On peut attribuer des permissions à des comptes d'ordinateurs, mais cela n'affecte pas l'utilisateur. Ce sont plutôt les services du système à qui on confère un accès.

Distinguished Name (DN)

Selon le protocole LDAP, les objets AD sont identifiés par un DN qui décrit sa position dans l'annuaire.

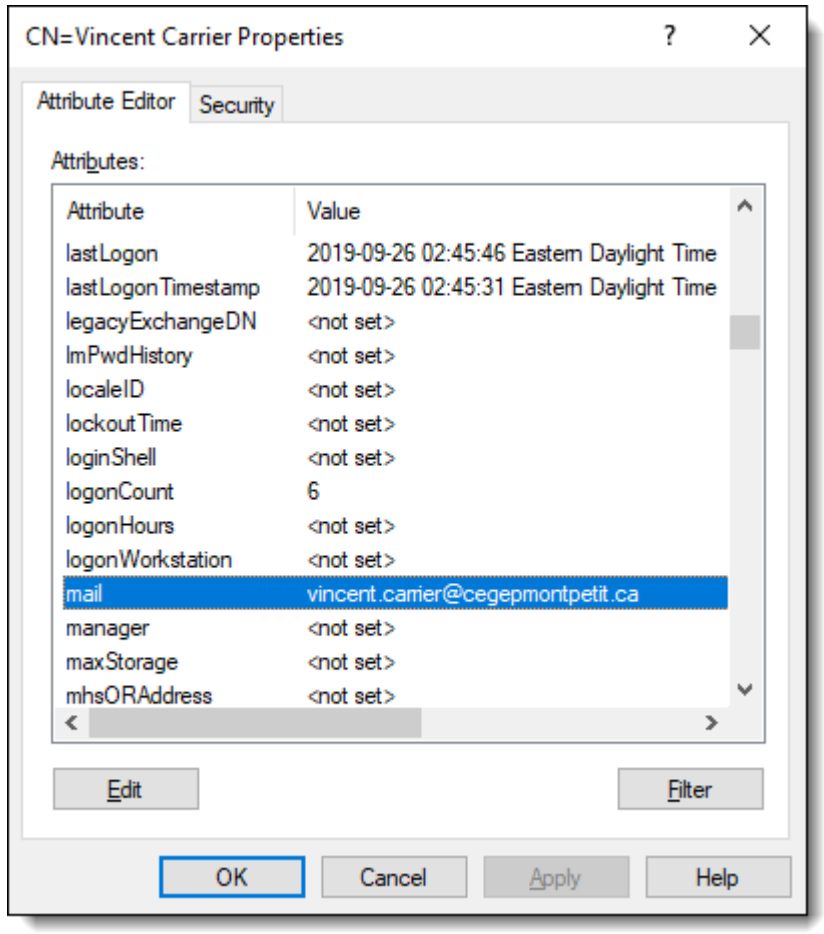




Distinguished Name:
CN=Vincent Carrier, OU=Professeurs, OU=LABINFO, DC=corp, DC=labinfo, DC=com

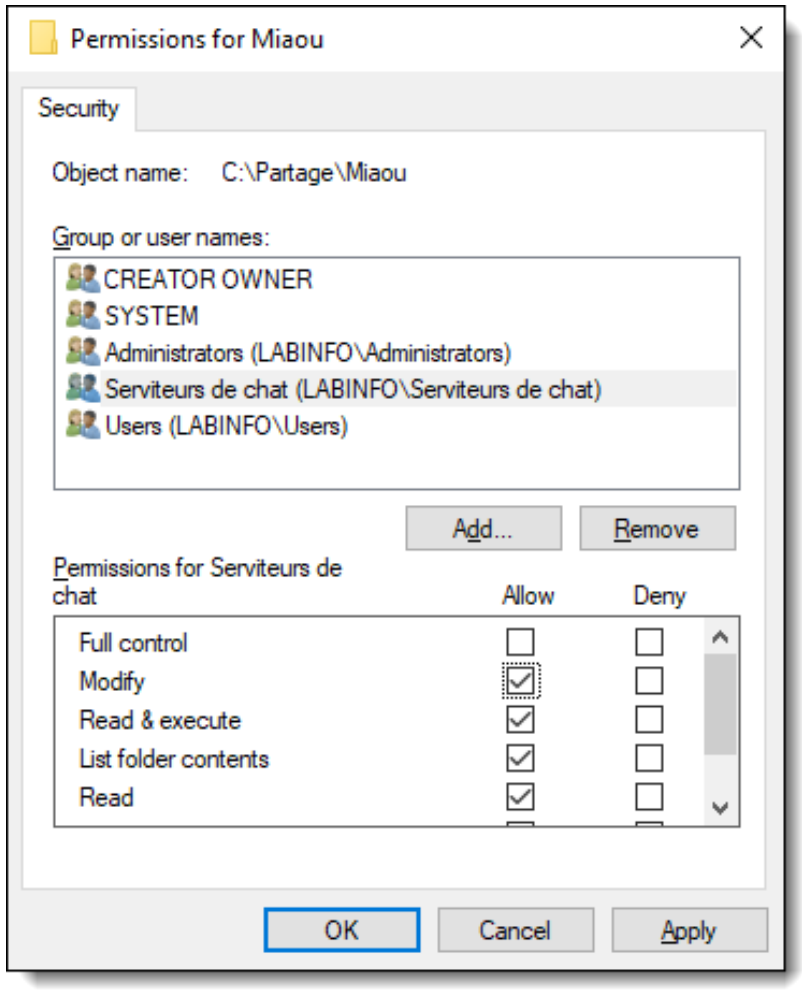
Attributs d'objets

- Les objets possèdent des attributs.
- Certains sont exposés dans les consoles graphiques, d'autres non.
- Ces attributs sont définis dans le schéma.
- *Vous en apprendrez plus à ce sujet en Serveurs 3!*



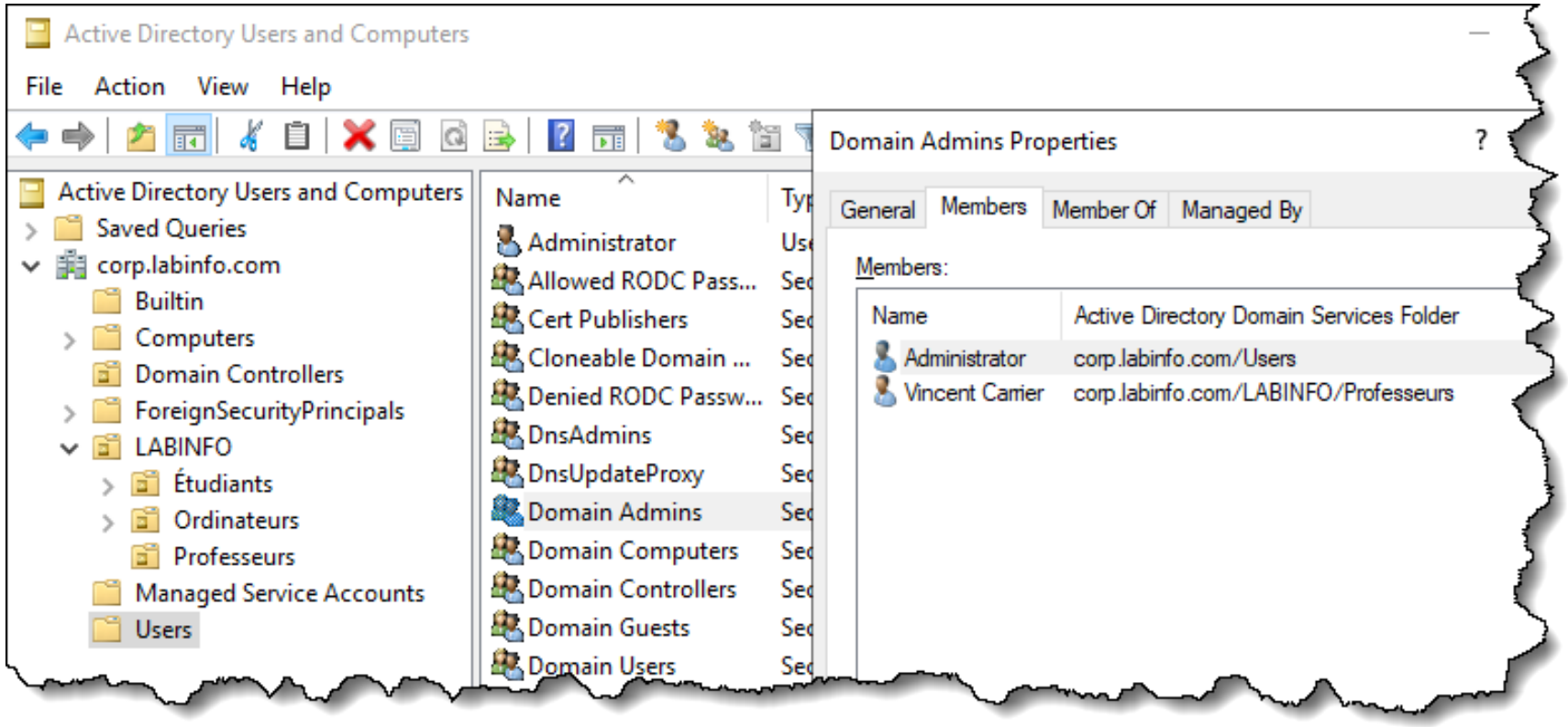
Gestion d'accès aux ressources

Une machine membre du domaine peut conférer des permissions pour accéder à ses ressources à des utilisateurs et des groupes du domaine, en plus des utilisateurs et groupes locaux.



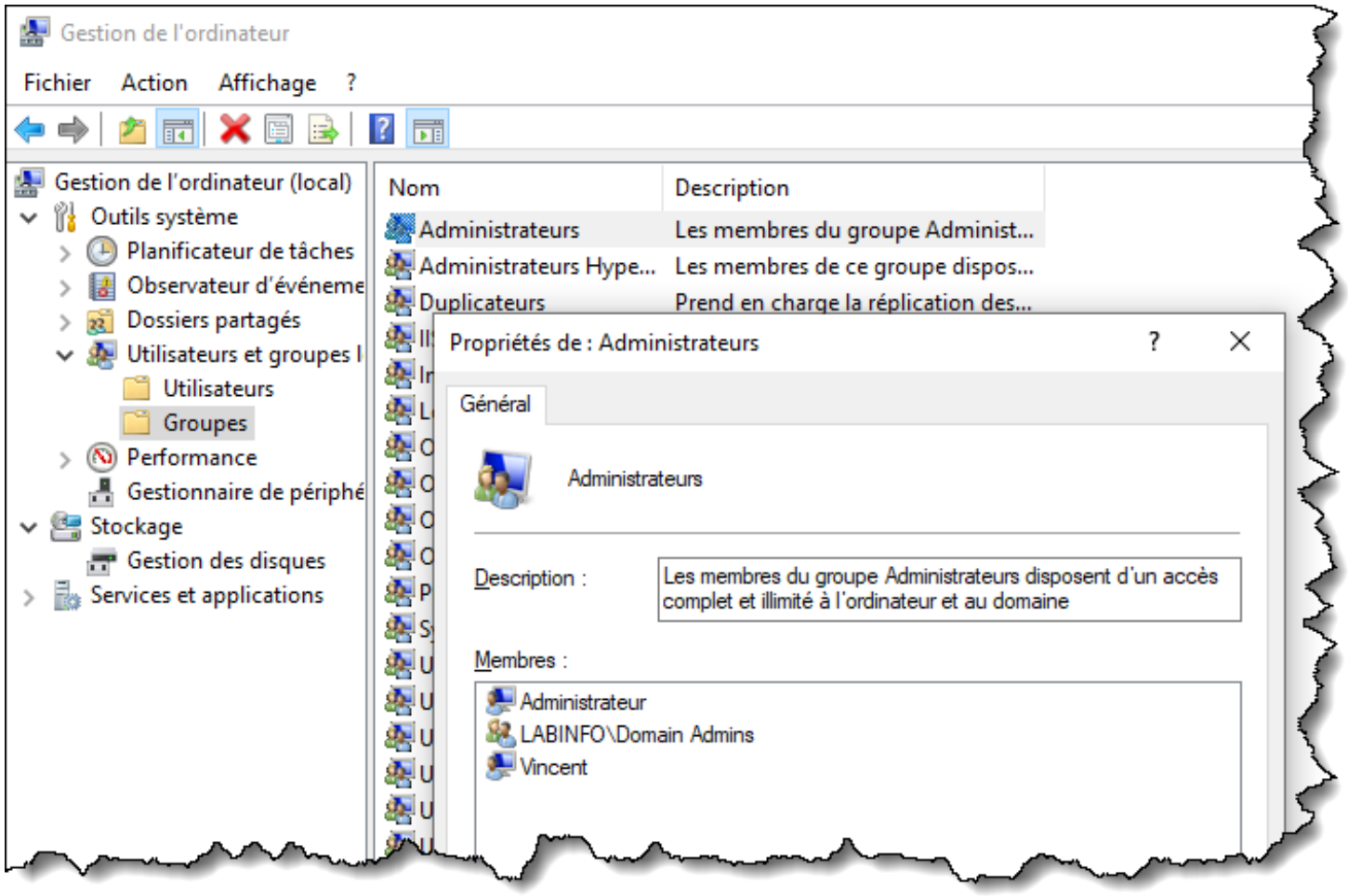
Admins du domaine

Le groupe des admins du domaine est le plus puissant du domaine, car il permet de contrôler tout l'AD.



Groupe administrateur local

Par défaut, dans Active Directory, tous les admins du domaine sont aussi admins locaux de tous les ordinateurs membres du domaine.



Questions?