



Schéma Active Directory

Damien SIMONET
damien@mysimonet.fr



Pourquoi faire un cours sur le schéma ?

- ▶ Le schéma, c'est le cœur de votre Active Directory.
- ▶ Il est très rarement modifié, mais il est intéressant de comprendre comment il fonctionne.
- ▶ En effet, lorsque vous allez créer un objet (un compte utilisateur, un ordinateur...), celui-ci va être validé ou non selon les informations que vous lui affectez avant d'être écrit dans la base Active Directory.

Définition du Schéma

- ▶ Le schéma contient des définitions formelles de chaque **classe** d'objets (OU, computer, ...) de la forêt AD.
- ▶ Il contient aussi des définitions formelles de chaque **attribut** (givenname, mail...).

- ▶ Exemple :
 - La **classe** « **User** » est le modèle qui permet la création d'un compte utilisateur.
 - Un compte utilisateurs a des **attributs** qui le caractérise :
 - **givenname**
 - **Mail**
 - **UPN (=login de connexion)**
 - ...
- ▶ On peut faire le parallèle avec la POO (Programmation Orientée Objet)

Outil de gestion du schéma

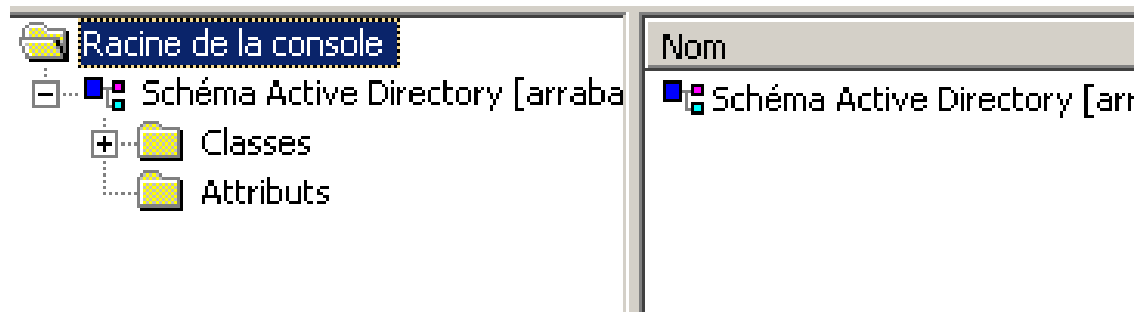
- ▶ L'outil de gestion du schéma est un composant logiciel qui permet de gérer le schéma Active Directory
- ▶ Pour utiliser l'outil, il faut :
 - Exécuter la commande windows « regsvr32 schmmgmt.dll »
 - Ouvrir la « MMC »
 - Ajoute le composant logiciel enfichable « Schéma active Directory »
- ▶ Attention aux erreurs de modifications !
 - Microsoft demande d'être vigilant et de bien comprendre les effets de la modification.
 - Cela peut entraîner des pertes ou une altération des données
- ▶ Seuls les membres du groupe « *administrateur du schéma* » peuvent faire ces modifications.

(Information) Les étapes ajout d'un attribut pour les comptes utilisateurs

- ▶ Seul l'administrateur du schéma peut exécuter ces actions
- ▶ Création du nouvel attribut avec l'outil de gestion du schéma
- ▶ Dans les propriétés de la classe « user », ajout de l'attribut facultatif
- ▶ Ouvrir « Utilisateurs et ordinateurs Active Directory »
- ▶ Afficher les fonctionnalités avancées
- ▶ Ouvrir les propriétés du compte utilisateur
- ▶ Dans l'onglet « Editeur d'attributs », le nouvel attribut est présent

Classes et attributs

- Dans le gestionnaire du schéma on retrouve 2 dossiers :
 - Classes
 - Attributs



Classes

- Quelques exemples de classes visibles depuis l'outil de gestion du schéma :

- categoryRegistration
- certificationAuthority
- classRegistration
- classSchema
- classStore
- comConnectionPoint
- computer**
- configuration
- connectionPoint
- contact
- container
- controlAccessRight
- country
- cRLDistributionPoint
- crossRef

Liste des classes

Nom	Type	Système	Description
volumeCount	Facultatif	Oui	Volume-Co
siteGUID	Facultatif	Oui	Site-GUID
rIDSetReferences	Facultatif	Oui	RID-Set-R
policyReplicationFlags	Facultatif	Oui	Policy-Repl
physicalLocationObject	Facultatif	Oui	Physical-Lc
operatingSystemVersion	Facultatif	Oui	Operating-
operatingSystemService...	Facultatif	Oui	Operating-
operatingSystemHotfix	Facultatif	Oui	Operating-
operatingSystem	Facultatif	Oui	Operating-
networkAddress	Facultatif	Oui	Network-A
netbootSIFFile	Facultatif	Oui	Netboot-SI
netbootMirrorDataFile	Facultatif	Oui	Netboot-M
netbootMachineFilePath	Facultatif	Oui	Netboot-M

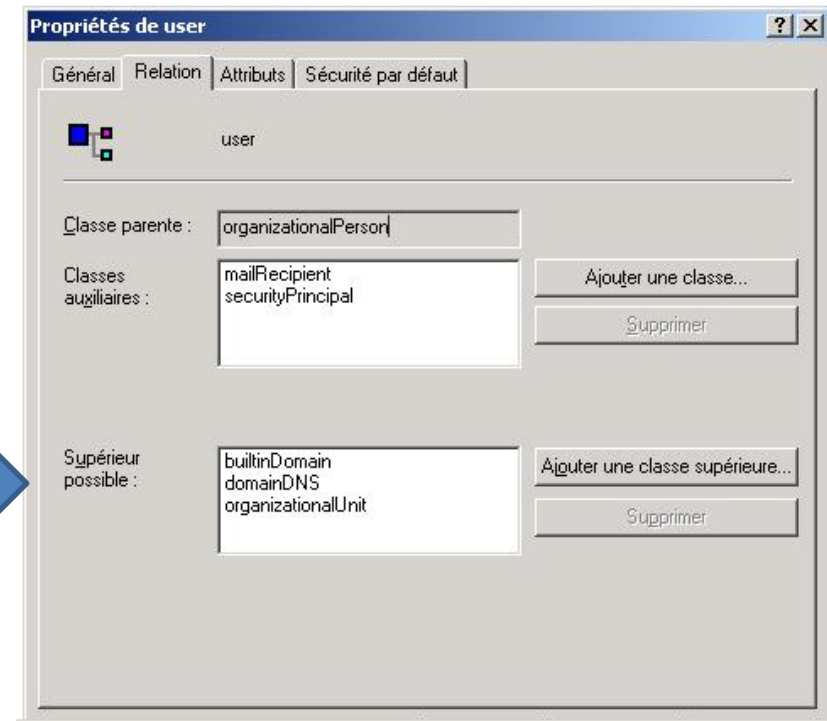
Liste des attributs
correspondant à la classe
sélectionnée

Classes

- C'est le schéma Active Directory qui définit la structure logique des objets.

Un compte utilisateur peut être stocké sous 3 types d'objets :

- Sous un dossier Builtin
- Sous un nom de domaine
- Sous une unité d'organisation



Classes

- Une classe contient une liste d'attributs. Ils peuvent être :
 - Obligatoires
 - Facultatifs

Un compte utilisateur a des attributs obligatoires. Ils ne sont pas visibles ici, car ils découlent de 2 classes auxiliaires.

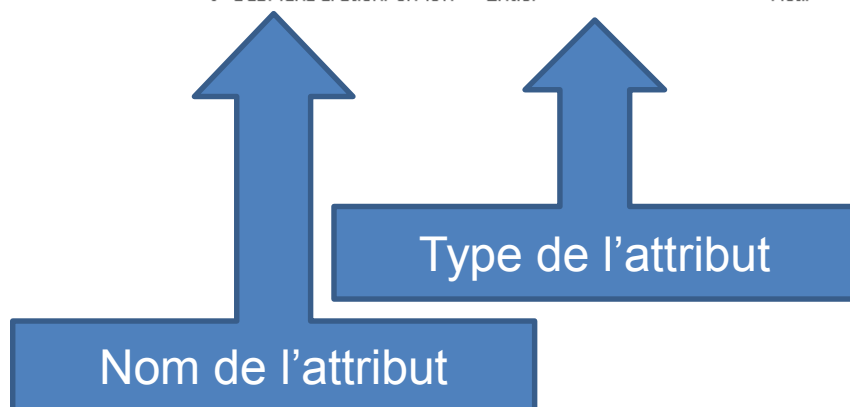
Un compte utilisateur a beaucoup d'attributs obligatoires.

The screenshot shows a Windows-style dialog box titled 'Propriétés de : user'. It has four tabs: 'Général', 'Relation', 'Attributs', and 'Sécurité par défaut'. The 'Attributs' tab is selected. Inside the dialog, there is a tree view on the left showing a folder icon and the name 'user'. Below the tree view, there are two sections: 'Obligatoire :' and 'Facultatif :'. The 'Obligatoire :' section is empty. The 'Facultatif :' section contains a list box with the following attributes: 'accountExpires', 'aCSPolicyName', 'adminCount', 'audio', 'badPasswordTime', 'badPwdCount', 'businessCategory', 'carLicense', and 'codePage'. To the right of the list box are two buttons: 'Ajouter...' and 'Supprimer'. At the bottom of the dialog are four buttons: 'OK', 'Annuler', 'Appliquer', and 'Aide'.

Attributs

- Quelques exemples d'attributs visibles depuis l'outil de gestion du schéma :

◆ accountExpires	Entier long/Intervalle	Actif	Account-
◆ accountNameHistory	Chaîne Unicode	Actif	Account-
◆ aCSAggregateTokenRa...	Entier long/Intervalle	Actif	ACS-Agg
◆ aCSAllocableRSVPBand...	Entier long/Intervalle	Actif	ACS-Allo
◆ aSCacheTimeout	Entier	Actif	ACS-Cac
◆ aCSDirection	Entier	Actif	ACS-Dire
◆ aCSDSBMDeadTime	Entier	Actif	ACS-DSB
◆ aCSDSBMPriority	Entier	Actif	ACS-DSB
◆ aCSDSBMRefresh	Entier	Actif	ACS-DSB
◆ aCSEnableACSService	Booléen	Actif	ACS-Ena
◆ aCSEnableRSVPAccoun...	Booléen	Actif	ACS-Ena
◆ aCSEnableRSVPMessag...	Booléen	Actif	ACS-Ena
◆ aCSEventLogLevel	Entier	Actif	ACS-Eve
◆ aCSIIdentityName	Chaîne Unicode	Actif	ACS-Ider
◆ aCSMaxAggregatePeak...	Entier long/Intervalle	Actif	ACS-Max
◆ aCSMaxDurationPerFlow	Entier	Actif	ACS-Max



Attributs

Propriétés de mail

Général

mail

Description : E-mail-Addresses

Nom commun : E-mail-Addresses

ID d'objet X.500 : 0.9.2342.19200300.100.1.3

Syntaxe et étendue

Syntaxe : Chaîne Unicode

Minimum : 0

Maximum : 256

Cet attribut est à valeur simple.

☐ Autoriser cet attribut à apparaître dans le mode d'affichage détaillé

☒ L'attribut est actif

☒ Indexer cet attribut dans Active Directory

☐ Résolution de noms ANR (Ambiguous Name Resolution)

☒ Répliquer cet attribut dans le catalogue global

☐ L'attribut est copié lors de la duplication de l'utilisateur

☐ Indexer cet attribut pour des recherches en conteneur dans Active Directory

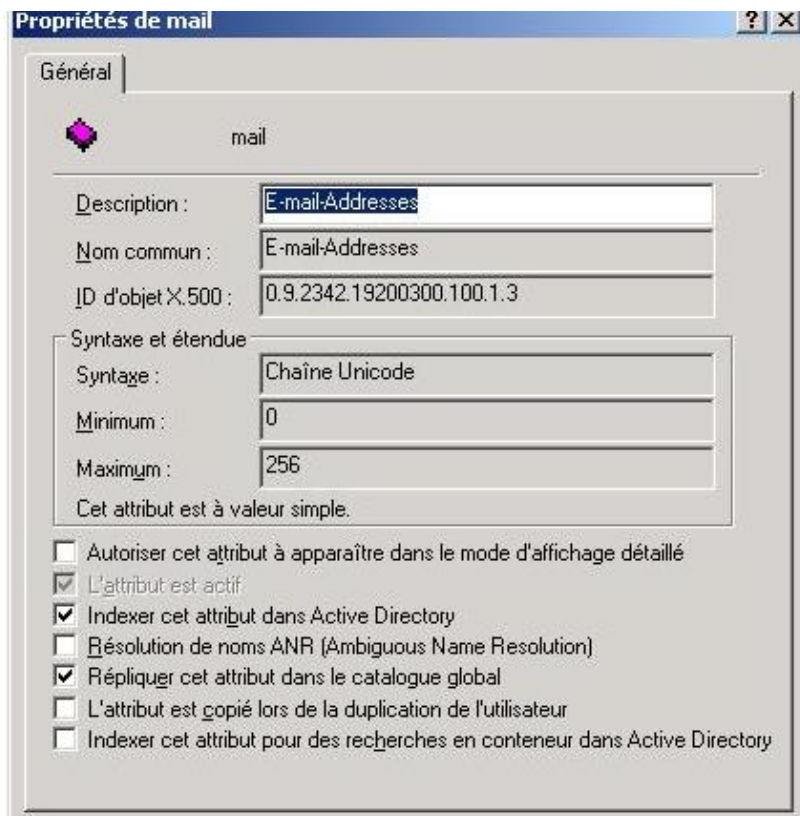
Décrire les fonctions de l'attribut

Nom utilisé pour la liaison attribut-classes

Assigné par l'ISO (obligatoire et unique dans le monde)

Type de l'attribut (booléen, entier...)

Attributs



Propriétés de mail

Général

mail

Description : E-mail-Addresses

Nom commun : E-mail-Addresses

ID d'objet X.500 : 0.9.2342.19200300.100.1.3

Syntaxe et étendue

Syntaxe : Chaîne Unicode

Minimum : 0

Maximum : 256

Cet attribut est à valeur simple.

☐ Autoriser cet attribut à apparaître dans le mode d'affichage détaillé

☒ L'attribut est actif

☒ Indexer cet attribut dans Active Directory

☐ Résolution de noms ANR (Ambiguous Name Resolution)

☒ Répliquer cet attribut dans le catalogue global

☐ L'attribut est copié lors de la duplication de l'utilisateur

☐ Indexer cet attribut pour des recherches en conteneur dans Active Directory

Autoriser cet attribut à apparaître dans le mode d'affichage détaillé :

Cette option est explicite et permet d'afficher l'attribut dans le cas où on a activé l'affichage détaillé.

L'attribut est actif : Cette option n'est disponible qu'en **niveau fonctionnel de forêt Windows Server 2003**. Par défaut, Active Directory ne permet pas de supprimer des attributs ou des classes. Par contre, on peut les désactiver via cette option. Si un attribut est désactivé, il ne plus être lié à des classes

Attributs

Indexer cet attribut dans Active Directory : Permet de rechercher plus rapidement et plus efficacement les objets possédant cet attribut.

Résolution de nom ANR (Ambiguous Name Resolution) : Cette option est utilisée dans les recherches. Par exemple, lorsqu'on va faire une recherche dans l'annuaire pour trouver l'utilisateur « Julien Martin » en donnant comme critère de recherche « Ju Ma » la résolution ANR va renvoyer une correspondance avec le compte utilisateur « Julien Martin ». (Pratique pour les homonymes.)

Attributs

Propriétés de mail

Général

mail

Description : E-mail-Addresses

Nom commun : E-mail-Addresses

ID d'objet X.500 : 0.9.2342.19200300.100.1.3

Syntaxe et étendue

Syntaxe : Chaîne Unicode

Minimum : 0

Maximum : 256

Cet attribut est à valeur simple.

☐ Autoriser cet attribut à apparaître dans le mode d'affichage détaillé

☒ L'attribut est actif

☒ Indexer cet attribut dans Active Directory

☐ Résolution de noms ANR (Ambiguous Name Resolution)

☒ Répliquer cet attribut dans le catalogue global

☐ L'attribut est copié lors de la duplication de l'utilisateur

☐ Indexer cet attribut pour des recherches en conteneur dans Active Directory

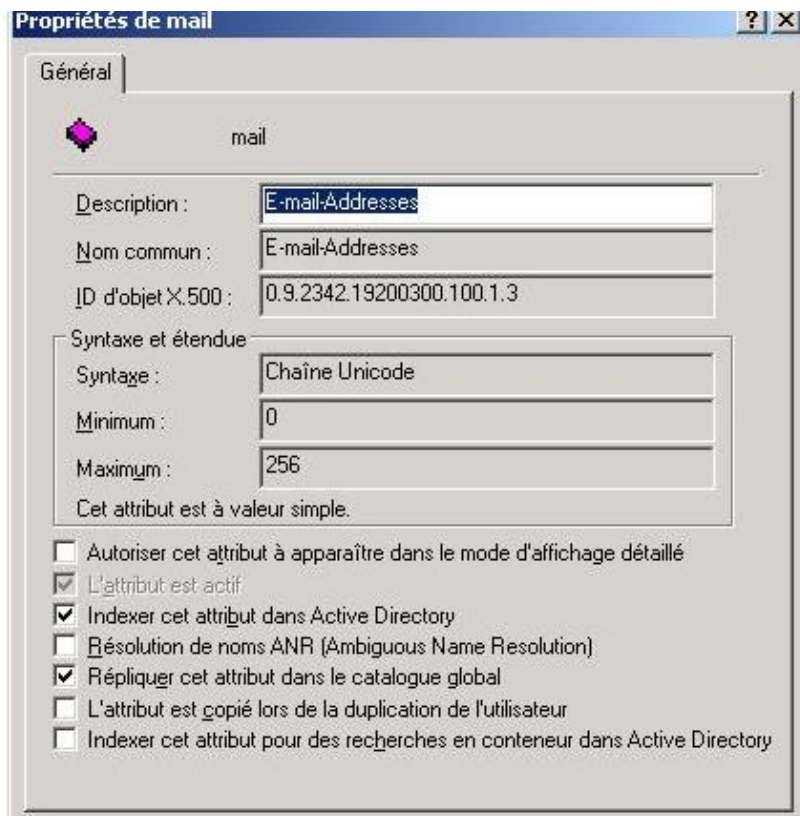
Répliquer cet attribut dans le catalogue global : le catalogue global est un rassemblement de certains attributs d'objets créés dans Active Directory. Cette option permet de placer l'attribut dans le catalogue global afin d'optimiser les recherches.

L'attribut est copié lors de la duplication de l'utilisateur : C'est une option uniquement utilisable sur les attributs qui sont liés à la classe utilisateur. L'option permet de conserver les valeurs de l'attribut lors d'une copie.

➔ Conseil :

Par défaut, utiliser des modèles de comptes d'utilisateurs permet de conserver l'appartenance aux groupes, les options de comptes, Dossier de base....

Attributs



Propriétés de mail

Général

mail

Description : E-mail-Addresses

Nom commun : E-mail-Addresses

ID d'objet X.500 : 0.9.2342.19200300.100.1.3

Syntaxe et étendue

Syntaxe : Chaîne Unicode

Minimum : 0

Maximum : 256

Cet attribut est à valeur simple.

☐ Autoriser cet attribut à apparaître dans le mode d'affichage détaillé

☒ L'attribut est actif

☒ Indexer cet attribut dans Active Directory

☐ Résolution de noms ANR (Ambiguous Name Resolution)

☒ Répliquer cet attribut dans le catalogue global

☐ L'attribut est copié lors de la duplication de l'utilisateur

☐ Indexer cet attribut pour des recherches en conteneur dans Active Directory

Indexer cet attribut pour les recherches en conteneur dans Active Directory : Cette option permet d'activer des recherches sur un attribut se trouvant dans un conteneur comme une unité d'organisation. Cela permet notamment de gagner du temps.