

# WINDOWS SERVER ADMINISTRATION

Active Directory

2ème Partie.

# PLAN

1

- Compte Utilisateur.

2

- Compte d'ordinateur.

3

- Groupes.

4

- Recherches.

# COMPTE UTILISATEUR.

# CRÉATIONS MODIFICATIONS

- ▶ Utilisation de lignes de commande pour créer des objets :

- ▶ dsadd user -> crée un compte utilisateur
- ▶ dsadd group -> crée un groupe
- ▶ dsmod group -> ajoute des membres à un groupes
- ▶ Dsquery -> recherche d'objet dans l'AD

- ▶ Possibilité de créer des fichiers de commandes

```
dsadd computer "cn=smithPC,ou=cso,dc=contoso,dc=msft "
```

```
dsadd user "cn=John Smith,ou=CSO,dc=contoso,dc=msft" -samid  
smithj -upn smithj@contoso.msft -fn John -ln Smith -display "John  
Smith" -pwd P@ssw0rd -disabled yes
```

Voir les exemples :

<http://www.microsoft.com/technet/scriptcenter/scripts/default.mspx>

et dsxxx/? évidemment !!

## Comptes d'utilisateurs locaux.

- Locaux a la machines.
- Droits et attributions locales.

## Comptes d'utilisateurs du domaine.

- Stokes dans Active Directory.
- Droits et attributions valable sur toutes les machines du domaine.

## 2 TYPES DE COMPTES.

# OUVERTURE DE SESSION

Locale

- Login.
- Mot de passe.
- Session locale.

Domaine

- Login: compte du domaine.
- Mot de passe.
- Domaine d'ouverture de session.

# CRÉATION GESTION DE COMPTES D'UTILISATEURS.

## Comptes locaux

- Ne pas activer pas le compte Invité
- Limiter le nombre de comptes.
- Gérer les privilèges.

## Comptes Domaine.

- Date de fin.
- Désactiver les comptes inutilisés.
- Gérer les plages d'ouvertures de session.
- Imposer les changements de mots de passes.

# GESTION DE COMPTES D'UTILISATEURS

Utilisateurs et ordinateurs Active Directory [chene.isim.intra]			
Requêtes sauvegardées			
isim.intra			
Builtin			
Comptes			
Comptes de services			
Etudiants			
Partis récemment			
Permanents			
utilisation provisoire			
Comptes à vérifier			
Computers			
defaultMigrationContainer30			
Domain Controllers			
ForeignSecurityPrincipals			
Groupes			
Groupes d'ordinateurs			
LostAndFound			
Managed Service Accounts			
Ordinateurs			
Prestataires			
Program Data			
Serveurs			
System			
test			
Users			
NTDS Quotas			
Nom	Type	Description	
athys	Utilisateur	voir Cres si encore besoin	
concours	Utilisateur		
congres	Utilisateur		
exterieur	Utilisateur	Compte générique	
formation	Utilisateur	Compte pour la Formation	
gillou	Utilisateur		
notes	Utilisateur	compte pour notes	
stage05	Utilisateur		
symposium	Utilisateur		



# COMPTE UTILISATEUR

## Ensemble des attributs d'un objet user.

- Nom, prénom, initiales, adresse, e-mail ...

## Profil.

- Local, itinérant, bloqué.

## Dossier de base.

## Groupes auxquels il appartient.

## UO ou hiérarchie d'UO.

## Mot de passe.

# ATTRIBUTS DU COMPTE


Propriétés de \_etud\_meca3

Sécurité Environnement Sessions Contrôle à distance

Profil de services Terminal Server COM+ Éditeur d'attributs Attributs UNIX

Certificats publiés Membre de Réplication de mot de passe Appel entrant Objet

Général Adresse Compte Profil Téléphones Organisation

 \_etud\_meca3

Prénom :  Initiales :

Nom :

Nom complet :

Description :

Bureau :

Numéro de téléphone :  Autre...

Adresse de messagerie :

Page Web :  Autre...

OK Annuler Appliquer Aide

Propriétés de \_etud\_meca3

Sécurité Environnement Sessions Contrôle à distance

Certificats publiés Membre de Réplication de mot de passe Appel entrant Objet

Général Adresse Compte Profil Téléphones Organisation

Profil de services Terminal Server COM+ Éditeur d'attributs Attributs UNIX

Attributs :

Attribut	Valeur
accountExpires	(jamais)
badPasswordTime	(jamais)
badPwdCount	0
cn	_etud_meca3
codePage	0
countryCode	0
description	cree le 20100924 - a completer
displayName	test _etud_meca3
distinguishedName	CN=_etud_meca3,OU=MECA3,OU=MECA,C
dSCorePropagationD...	0x0 = ( )
gecos	_ETUD_MECA3 Test
gidNumber	120
givenName	.
homeDirectory	\\buis.isim.intra\_etud_meca3\$

Modifier Filtrer

OK Annuler Appliquer Aide

# LE PROFIL

Décrit l'environnement de travail de l'utilisateur

Bureau, Mes Documents, données des applicatifs (IE, ...)

## Local

- Stocké sur la station locale.
- Différent sur chaque station.

## Itinérant

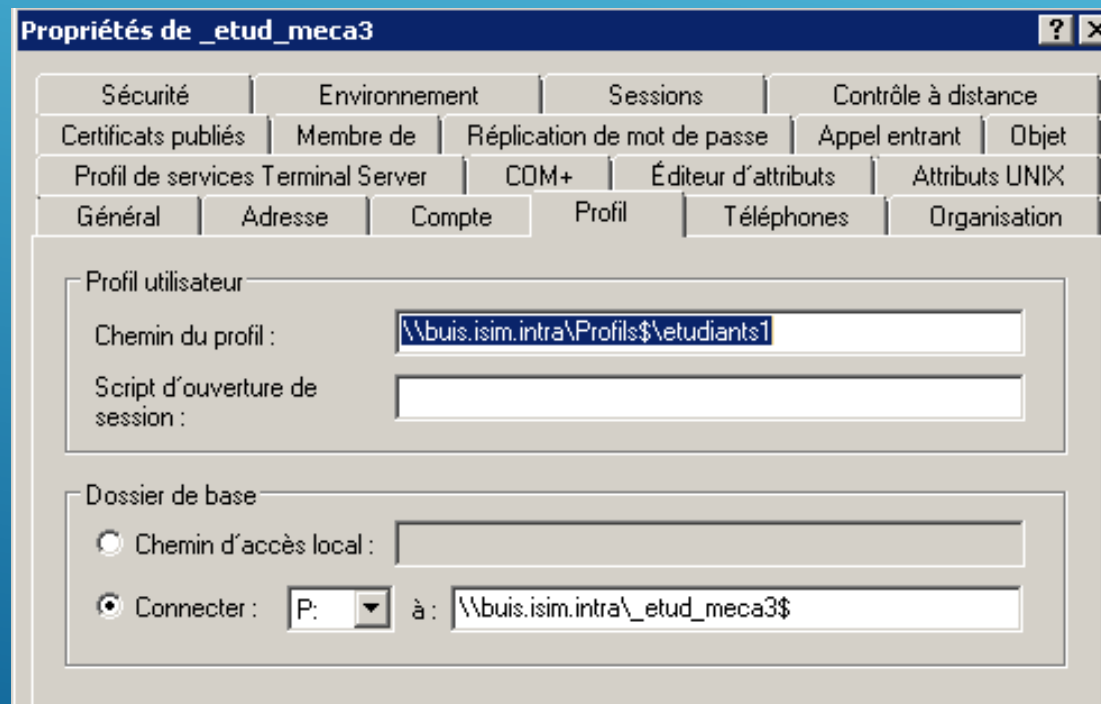
- stocké sur un serveur de fichiers.
- Est téléchargé sur toute station ou l'utilisateur se connecte => même environnement

## bloqué

- L'utilisateur ne peut pas sauvegarder les modifications apportées au profil.
- Permet de fournir un profil identique à une population.

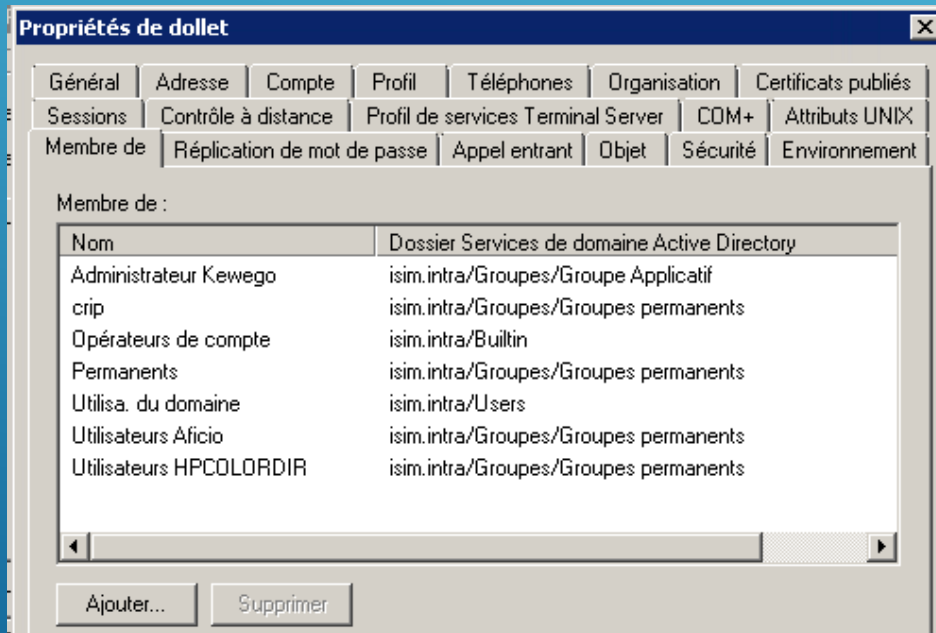
# LE DOSSIER DE BASE

Conteneur des données de l'utilisateur.  
Local ou sur un serveur de fichier.



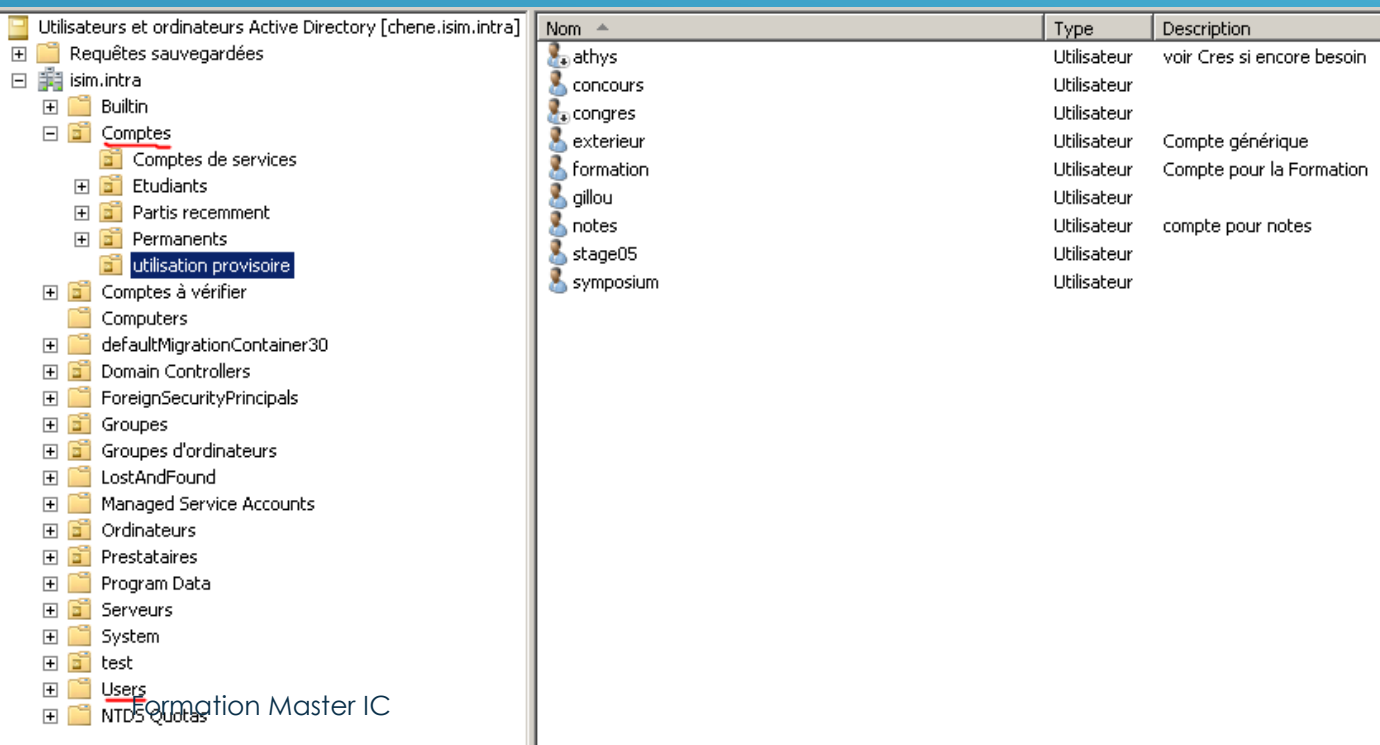
# GROUPE

Dans les propriétés, les différents groupes auxquels appartient le compte et les possibilités d'en ajouter d'autres.



# LES UNITÉS D'ORGANISATION

- L'utilisateur est placé dans une hiérarchie d'UO en fonction des droits qu'on voudra pouvoir lui donner.



The screenshot shows the Active Directory console for the domain 'chene.isim.intra'. The left pane displays the hierarchy of organizational units (OUs) under 'Comptes', with 'Utilisation provisoire' highlighted. The right pane displays a list of users with their names, types, and descriptions.

Nom	Type	Description
athys	Utilisateur	voir Cres si encore besoin
concours	Utilisateur	
congres	Utilisateur	
exterieur	Utilisateur	Compte générique
formation	Utilisateur	Compte pour la Formation
gillou	Utilisateur	
notes	Utilisateur	compte pour notes
stage05	Utilisateur	
symposium	Utilisateur	

Formation Master IC

# UNITÉ D'ORGANISATION

The screenshot displays the Active Directory console with the following structure:

- Utilisateurs et ordinateurs Active Directory [chene.isim.inte...]
  - Requêtes sauvegardées
  - isim.intra
    - Builtin
    - Comptes
      - Comptes de services
      - Etudiants
        - ENR
        - ERII
        - Etudiants hors ISIM
        - GASTE
        - INFO
        - MAT
        - MECA
          - EC
          - ECa
          - MECA3
            - MECA3a
            - MECA4
            - MECA4a
            - MECA5
            - MECA6
            - MECA7
          - MI
          - PEIP
          - STE
          - STIA

The 'Rechercher Utilisateurs, contacts et groupes' window is open, showing the following search results:

Nom	Type	Description
_etud_meca3	Utilisateur	creé le 20100924 - à compléter
antoine.ambar	Utilisateur	creé le 20101020 - à compléter

The search criteria are: Rechercher : Utilisateurs, contacts et groupes; Dans : MECA3. The search results table shows the following details for the first result:

Nom	Nom unique	Type
_etud_meca3	CN=_etud_meca3,OU=MECA3,OU=MECA,OU=Etudiants,OU=Comptes,DC=isim,DC=intra	Utilisateur

# STRATÉGIE LOCALE DE MOTS DE PASSE.

L'utilisateur doit  
changer le mot  
de passe à la  
prochaine ouverture  
de session

L'utilisateur ne peut  
pas changer de  
mot de passe

Le compte est  
désactivé

Le mot de passe  
n'expire jamais



# UTILISATION DES STRATÉGIES

- ▶ **L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**
- ▶ Création des comptes de domaine.
- ▶ Réinitialisation des mots de passe.
- ▶ **L'utilisateur ne peut pas changer de mot de passe**
- ▶ Création des comptes de services locaux et de domaine.
- ▶ Comptes locaux qui n'ouvrent pas de session.

# QUALITÉ DES MOTS DE PASSE.

Conservation  
Historique.

Durée de vie  
maxi et mini du  
mot de passe.

Longueur du  
mot de passe.

Exigences de  
complexité.

# DÉSACTIVATION / VERROUILLAGE

Un compte peut être désactivé et donc momentanément inaccessible.

Un seuil de tentative d'ouverture de session est fixé au delà le compte se verrouille.

Si elle est connue indiquer la date d'expiration du compte.

Protection

# SID, UPN, CN...

**Le SID (Security Identifier):** numéro composé de caractères alphanumériques qui permet d'identifier un ordinateur, un utilisateur ou un groupe d'utilisateurs.

- S-1-5-21-1098612359-567957490-142223018-18315

**DN ( distinguished name):** moyen d'identifier de façon unique un objet dans la hiérarchie

- CN=benezet,OU=CRIP,OU=Permanents,OU=Comptes,DC=isim,DC=intra

**UPN ( User Principal Name):** Nom de l'utilisateur au format d'adresse mail.

- benezet@isim.intra

**SAM-Account-Name**

Utilisé pour s'authentifier sur les systèmes antérieurs à W2000.

- benezet

**CN (comon name):** nom de la personne, utilisé pour effectuer des recherches.

- benezet

# MODÈLE DE COMPTE

## Pourquoi ?

Un modèle contient les propriétés qui s'appliquent aux utilisateurs courants .

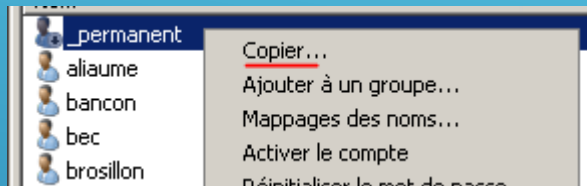
Rationalisation de la création de comptes d'utilisateur avec des configurations standard.

## Comment

Créer un compte modèle qui sera ensuite désactivé et identifié.

Toutes les informations utiles seront copiées les infos personnelles seront à remplir.

# CRÉATION PAR COPIE DE COMPTE

A screenshot of the 'Copier l'objet - Utilisateur' dialog box. The title bar says 'Copier l'objet - Utilisateur'. Below the title bar, there is a user icon and the text 'Créer dans : isim.intra/Comptes/Permanents/STE'. The dialog contains several input fields: 'Prénom :', 'Initiales :', 'Nom :', 'Nom complet :', 'Nom d'ouverture de session de l'utilisateur :', and 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :'. The 'Nom d'ouverture de session de l'utilisateur' field has a dropdown menu showing '@isim.intra'. The 'Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000)' field has a text input showing 'ISIM\_NT\'. At the bottom, there are three buttons: '< Précédent', 'Suivant >', and 'Annuler'.A screenshot of the 'Copier l'objet - Utilisateur' dialog box, showing the preview section. The title bar says 'Copier l'objet - Utilisateur'. Below the title bar, there is a user icon and the text 'Créer dans : isim.intra/Comptes/Permanents/STE'. The dialog contains a text area with the following text: 'Quand vous cliquerez sur Terminer, l'objet suivant sera créé :', 'Copier à partir de : \_permanent', 'Nom complet : test Agnes', 'Nom de connexion de l'utilisateur : testagnes@isim.intra', and 'Le compte est désactivé.' At the bottom, there are three buttons: '< Précédent', 'Terminer', and 'Annuler'.

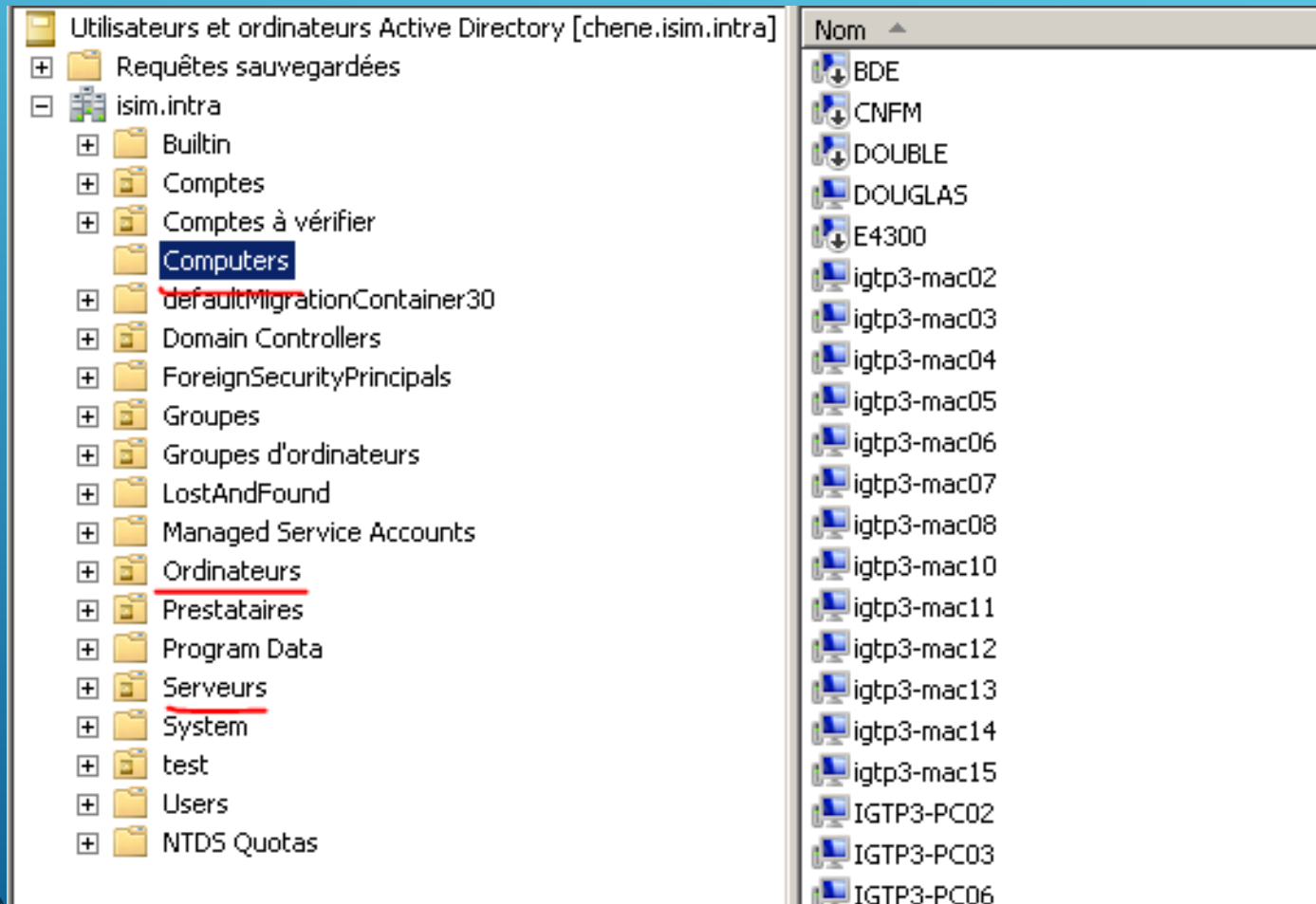
# COMPTE ORDINATEUR

# COMPTE D'ORDINATEUR

- ▶ Active l'authentification et l'audit de l'accès d'un ordinateur aux ressources du domaine.
- ▶ Permet de lui attribuer des stratégies de groupe ou de sécurité.
- ▶ Permet l'administration via Active Directory.  
(déploiement logiciels, inventaire du parc...gestion MAJ)



# CRÉATION DES COMPTES D'ORDINATEURS DANS UN DOMAINE



# OPTIONS DES COMPTES D'ORDINATEURS

### Propriétés de STXA04

Emplacement

Géré par

Objet

Sécurité

Appel entrant

Éditeur d'attributs

Attributs


Général

Système d'exploitation

Membre de

Délégation

Réplication de mot de p

 STXA04

Nom d'ordinateur (antérieur à Windows 2000):

Nom DNS :

Type de contrôleur de domaine :

Site :

Description :

OK

Annuler

Appliquer

Aide

### Propriétés de STXA04

Général

Système d'exploitation

Membre de

Délégation

Réplication de mot de passe

Emplacement

Géré par

Objet

Sécurité

Appel entrant

Éditeur d'attributs

Attributs UNIX

Attributs :

Attribut	Valeur
instanceType	0x4 = ( WRITE )
isCriticalSystemObject	FALSE
lastLogoff	(jamais)
lastLogon	27/06/2011 13:50:04 Paris, Madrid
lastLogonTimestamp	27/06/2011 13:10:11 Paris, Madrid
localPolicyFlags	0
logonCount	2
name	STXA04
objectCategory	CN=Computer,CN=Schema,CN=Configuration
objectClass	top; person; organizationalPerson; user; com
objectGUID	d0c64ebd-ec2d-4fc3-b16f-b11b4b8654ad
objectSid	S-1-5-21-1098612359-567957490-14222301
operatingSystem	Windows XP Professional
operatingSystemServi...	Service Pack 3

Modifier

Filtrer

OK

Annuler

Appliquer

Aide

Formation Master IC

AD – Objets.

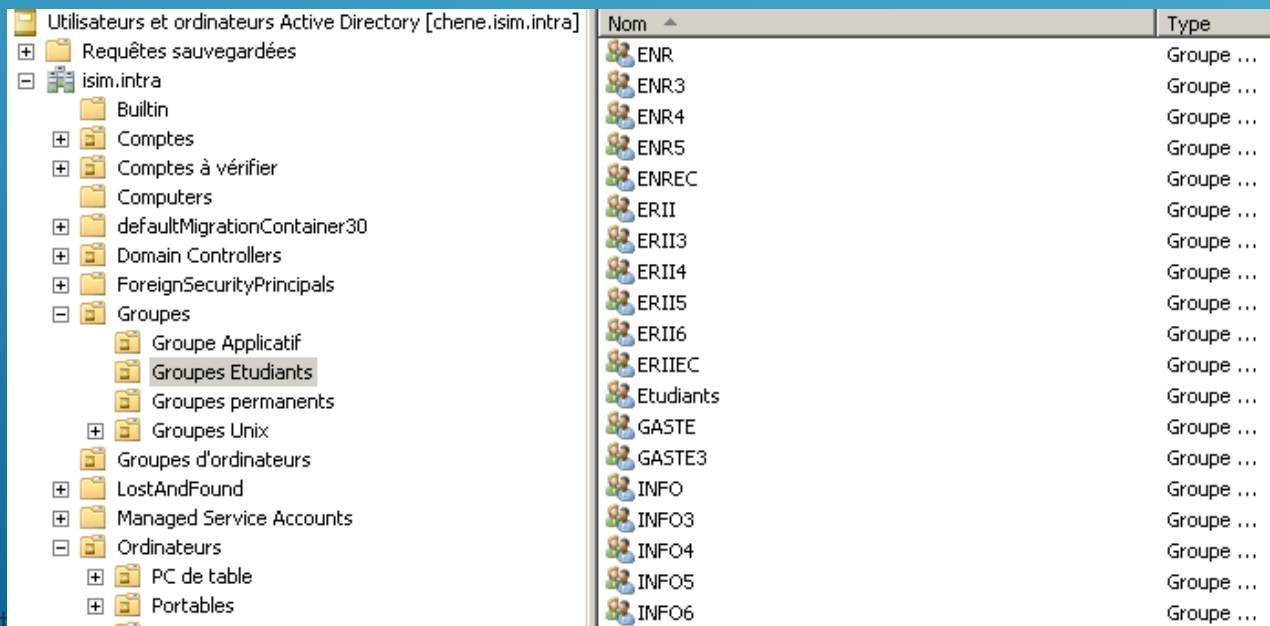
# GROUPES

# GROUPES

Les groupes simplifient l'administration par l'attribution

d'autorisations d'accès aux ressources

- Regrouper des utilisateurs par classe (étudiant, administratif, enseignant, ...)



Nom	Type
ENR	Groupe ...
ENR3	Groupe ...
ENR4	Groupe ...
ENR5	Groupe ...
ENREC	Groupe ...
ERII	Groupe ...
ERII3	Groupe ...
ERII4	Groupe ...
ERII5	Groupe ...
ERII6	Groupe ...
ERIIEC	Groupe ...
Etudiants	Groupe ...
GASTE	Groupe ...
GASTE3	Groupe ...
INFO	Groupe ...
INFO3	Groupe ...
INFO4	Groupe ...
INFO5	Groupe ...
INFO6	Groupe ...

# TYPES DE GROUPES

## **3 types de groupe (dans l'AD) :**

- ▶ Local au domaine
- ▶ Global au domaine
- ▶ Universel

L'étendue détermine si le groupe couvre plusieurs domaines ou s'il est limité à un seul domaine.

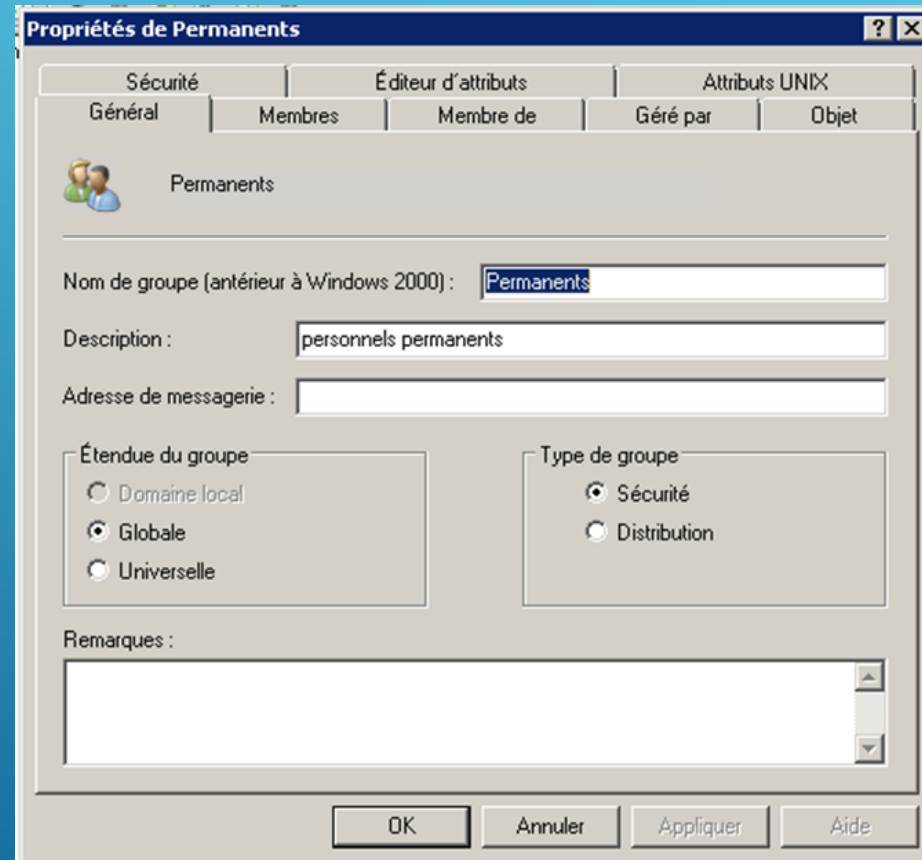
**+ les groupes locaux de la machine.**

# TYPES DE GROUPES

## 2 aspects :

- ▶ Sécurité: Pour attribuer des droits et des autorisations aux utilisateurs.
- ▶ Distribution: réservés aux applications de courrier électronique.

# TYPES DE GROUPES



## Membres

- Comptes d'utilisateurs.
- Comptes d'ordinateurs.
- Groupes globaux et groupes universels de n'importe quel domaine de la forêt.
- Groupes de domaine local (du même domaine)

## Etendue

- Uniquement dans son propre domaine

## Autorisations

- Domaine d'appartenance.

# GROUPES DE DOMAINE LOCAL.



## Membres

- Comptes d'utilisateurs.
- Comptes d'ordinateurs..
- Groupes globaux du même domaine.

## Etendue

- Tous les domaines de la forêt
- Tous les domaines qui approuvent.

## Autorisations

- Tous les domaines de la forêt.
- Tous les domaines qui approuvent.

# GROUPE GLOBAUX

# GROUPES UNIVERSELS

## Membres

- Comptes d'utilisateurs.
- Comptes d'ordinateurs.
- Groupes globaux et groupes universels de n'importe quel domaine de la forêt..

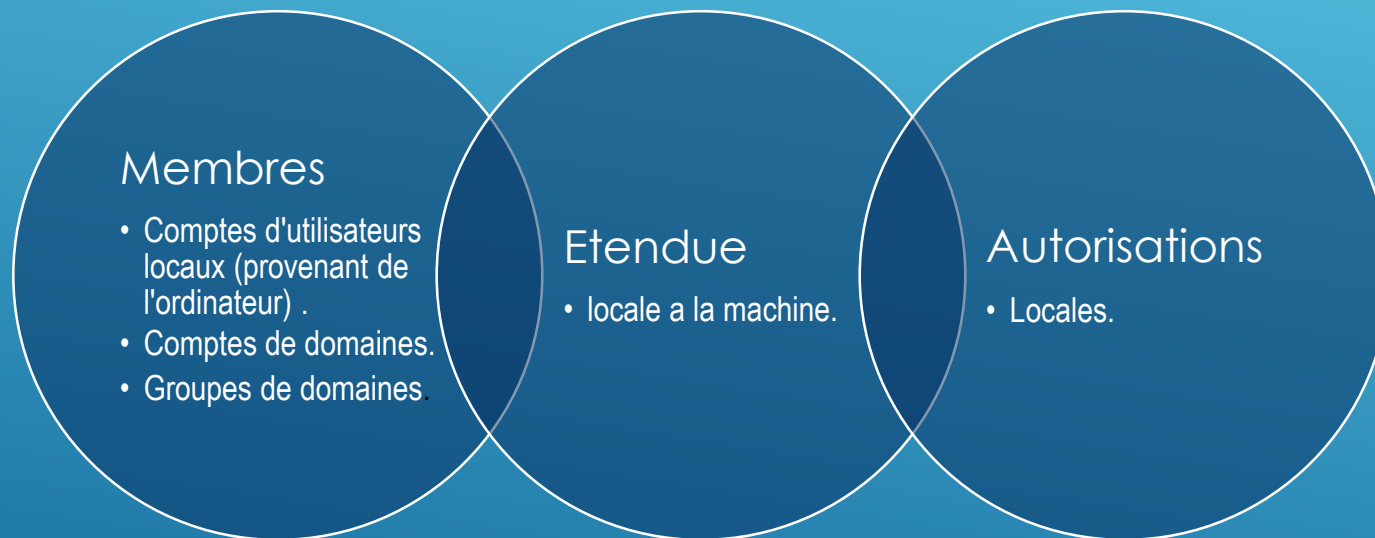
## Etendue

- Visible dans tous les domaines d'une forêt.
- Visible dans les domaines qui approuvent.

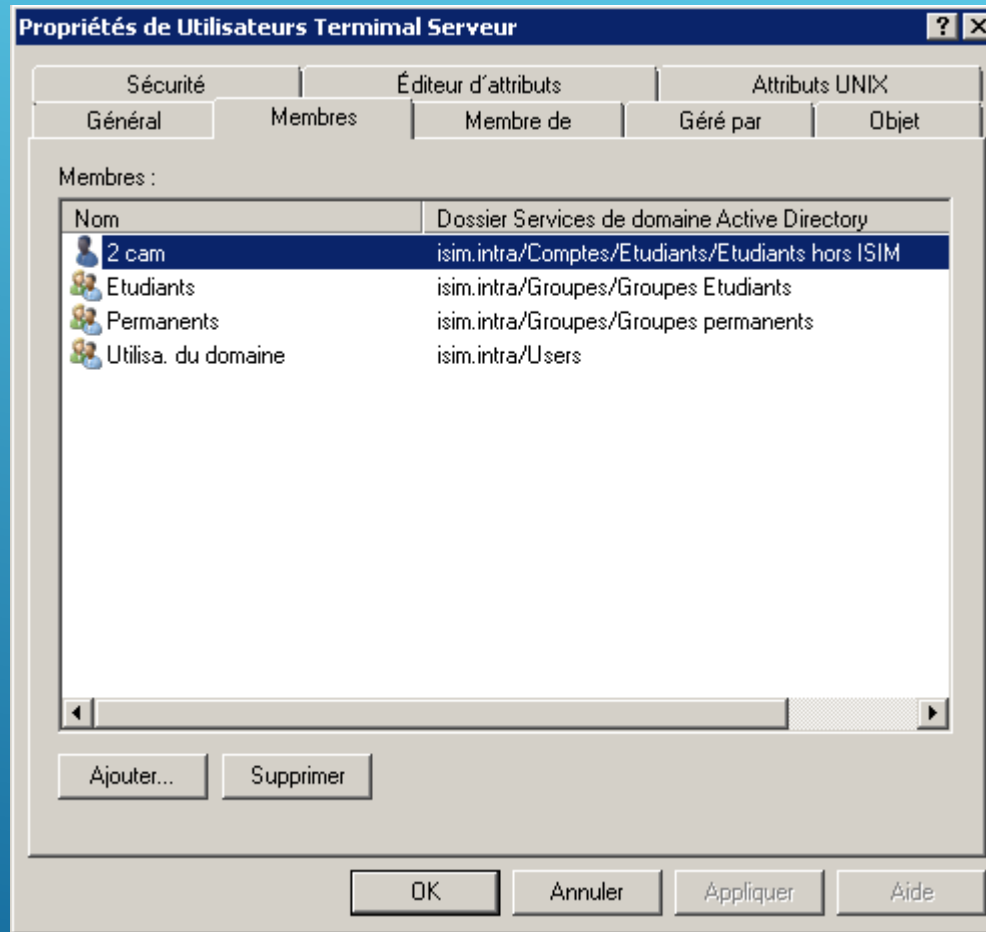
## Autorisations

- Tous les domaines de la forêt..

# GROUPES LOCAUX.



# MEMBRES DES GROUPES

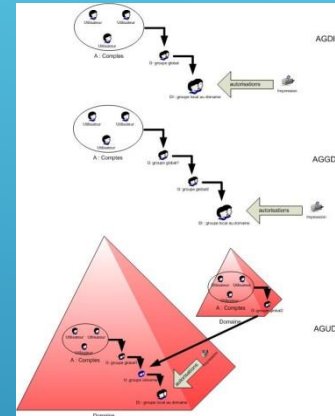


# STRATÉGIE D'UTILISATION DES GROUPES

Pour une efficacité + grande imbrication des groupes:

Methode AGDLP, AGGDLP, AGUDLP, AGGUDLP

- ▶ A : account,
- ▶ G : global,
- ▶ DL : local au domaine,
- ▶ U : universel,
- ▶ P : permission.



# AGDLP

## Efficace dans un domaine restreint.

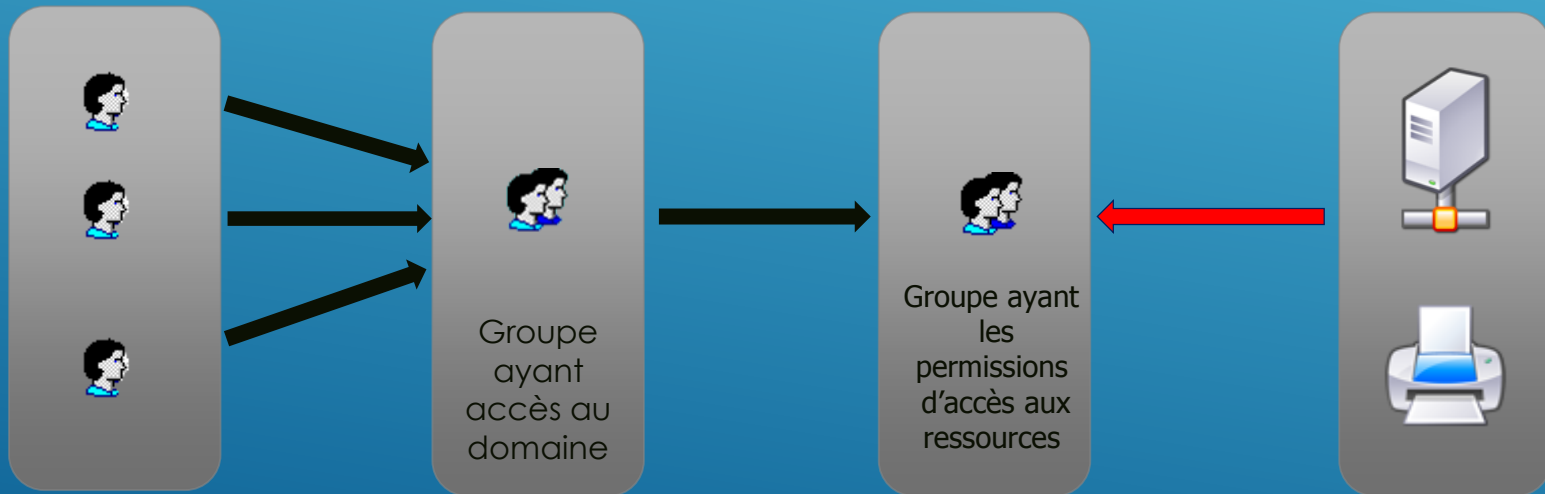
concentrer les permissions sur un seul groupe au niveau puis joindre a ce groupe les utilisateurs ou groupes autorisés..

Utilisateur

Groupe Global

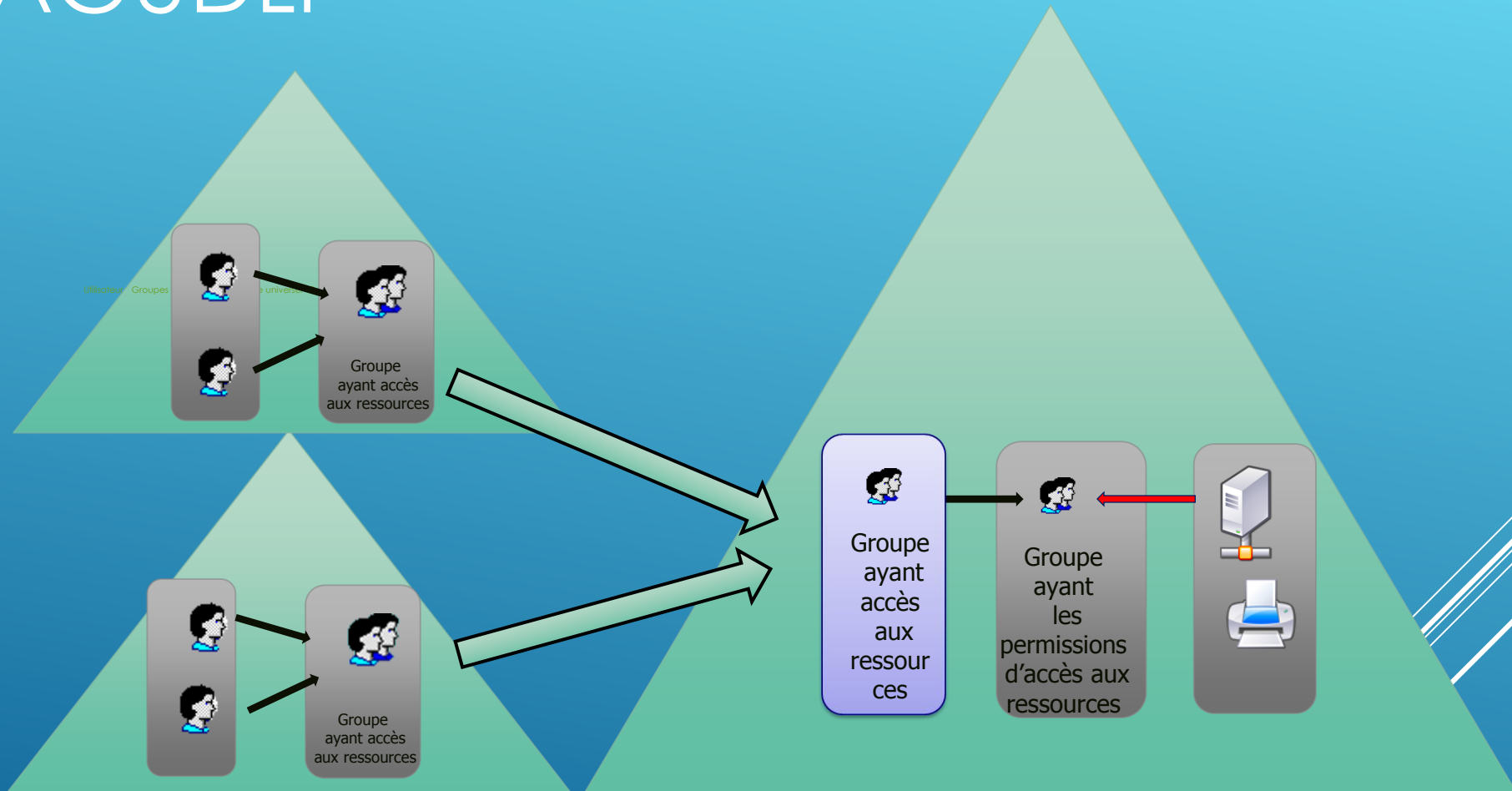
Groupe local

Ressource



# ACUDLP

A utiliser dans une forêt Active Directory



# GROUPES PRÉDÉFINIS

Crées à l'installation du système d'exploitation ou par des services ou applications ( AD, IIS...).

Possèdent des droits prédéfinis.

Permettent de contrôler l'accès aux ressources partagées , et la ddéléguer une administration spécifique à l'échelle d'un domaine.



# LES GROUPES PRÉDÉFINIS

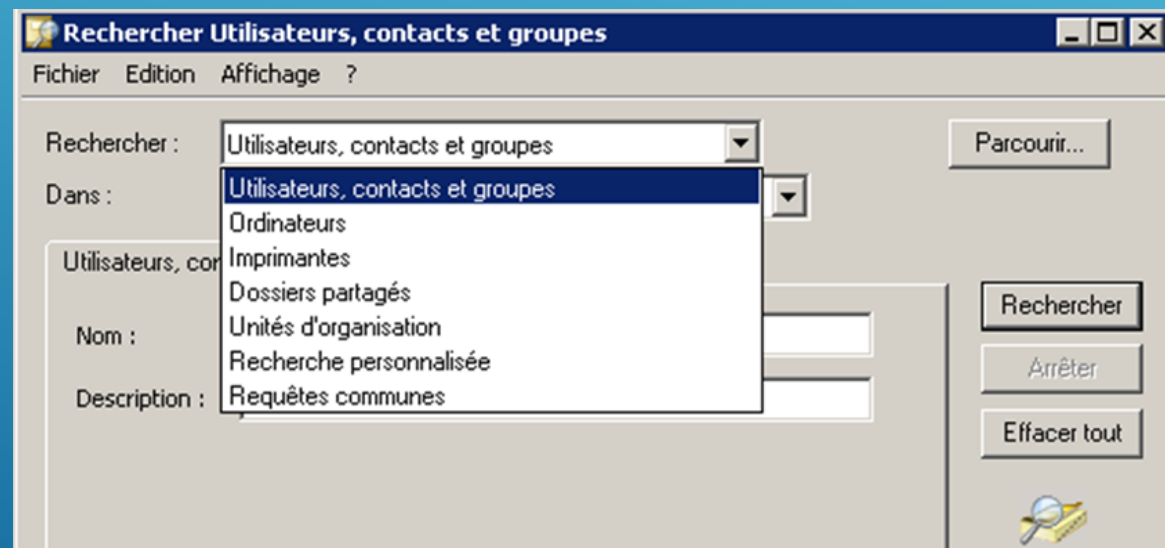
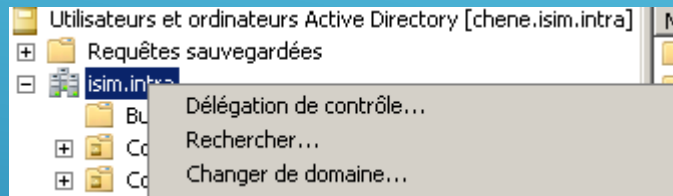
Utilisateurs et ordinateurs Active Directory [chene.isim.intra]		Nom	Type	Description
+ Requêtes sauvegardées		Accès compatible Pre-Windows 2000	Groupe de sécu...	Un groupe de compatibilit...
- isim.intra		Accès DCOM service de certificats	Groupe de sécu...	Les membres de ce group...
+ Builtin		Administrateurs	Groupe de sécu...	Les membres peuvent enti...
+ Comptes		Duplicateurs	Groupe de sécu...	Prend en charge la duplica...
+ Comptes à vérifier		Générateurs d'approbations de forêt entrante	Groupe de sécu...	Les membres de ce group...
+ Computers		Groupe d'accès d'autorisation Windows	Groupe de sécu...	Les membres de ce group...
+ defaultMigrationContainer30		IIS_IUSRS	Groupe de sécu...	Groupe intégré utilisé par l...
+ Domain Controllers		Invités	Groupe de sécu...	Utilisateurs ayant reçu le ...
+ ForeignSecurityPrincipals		Lecteurs des journaux d'événements	Groupe de sécu...	Des membres de ce group...
- Groupes		Opérateurs de chiffrement	Groupe de sécu...	Les membres sont autoris...
+ Groupe Applicatif		Opérateurs de compte	Groupe de sécu...	Les membres peuvent ad...
+ Groupes Etudiants		Opérateurs de configuration réseau	Groupe de sécu...	Les membres de ce group...
+ Groupes permanents		Opérateurs de sauvegarde	Groupe de sécu...	Les membres peuvent pas...
+ Groupes Unix		Opérateurs de serveur	Groupe de sécu...	Les membres peuvent ad...
+ Groupes d'ordinateurs		Opérateurs d'impression	Groupe de sécu...	Les membres peuvent ad...
+ LostAndFound		Serveurs de licences des services Terminal Server	Groupe de sécu...	Serveurs de licences des s...
+ Managed Service Accounts		Utilisateurs	Groupe de sécu...	Utilisateurs ordinaires
- Ordinateurs		Utilisateurs de l'Analyseur de performances	Groupe de sécu...	Les membres de ce group...
+ PC de table		Utilisateurs du Bureau à distance	Groupe de sécu...	Les membres de ce group...
+ Portables		Utilisateurs du journal de performances	Groupe de sécu...	Les membres de ce group...
+ services		Utilisateurs du modèle COM distribué	Groupe de sécu...	Les membres sont autoris...
+ Prestataires				
+ Program Data				
- Serveurs				

- ▶ Préférer le groupe Utilisateurs authentifiés groupe Tout le monde.
- ▶ Créer des groupes selon les besoins d'administration.
- ▶ Ajoutez les comptes d'utilisateurs au groupe le plus restrictif.
- ▶ Limitez le nombre d'utilisateurs du groupe Administrateurs.
- ▶ Plutôt que de créer un groupe, utilisez dans la mesure du possible le groupe intégré.

## RECOMMANDATIONS RELATIVES À L'ADMINISTRATION DES GROUPE

# RECHERCHES

# VOLET DE RECHERCHE.



# VOLET DE RECHERCHE.

**Rechercher Utilisateurs, contacts et groupes**

Fichier Edition Affichage ?

Rechercher : Utilisateurs, contacts et groupes Parcourir...

Dans : isim.intra

Utilisateurs, contacts et groupes Avancé

Nom : dollet

Description :

Rechercher Arrêter Effacer tout

Résultats de la recherche :

Nom	Nom unique
adollet	CN=adollet,OU=ENR,OU=Permanents,OU=Comptes,DC=isim,DC=intra
dollet	CN=dollet,OU=CRIP,OU=Permanents,OU=Comptes,DC=isim,DC=intra

2 élément(s) trouvé(s)

# CRITÈRES FONDAMENTAUX

- ▶ le type d'objet
- ▶ l'emplacement
- ▶ Les valeurs associées à l'objet, comme le nom, la description...

Rechercher Utilisateurs, contacts et groupes

Fichier Edition Affichage ?

Rechercher : Utilisateurs, contacts et groupes

Dans : isim.intra

Utilisateurs, contacts et groupes Avancé

Champ	Condition	Valeur

Liste des conditions : <Ajouter les critères ci-dessus à cette liste>

Parcourir...

Rechercher

Arrêter

Effacer tout

# ENREGISTREMENT DES REQUÊTES

- ▶ Gain de temps pour des tâches répétitives.
- ▶ Surveillance de comptes...

# REQUÊTE SAUVEGARDÉE

