SUP MTI
École Supérieure de Management,
de Télécommunication et d'Informatique

بسم الله الرحمن الرحيم

Gestion des groupes

Présenté par :

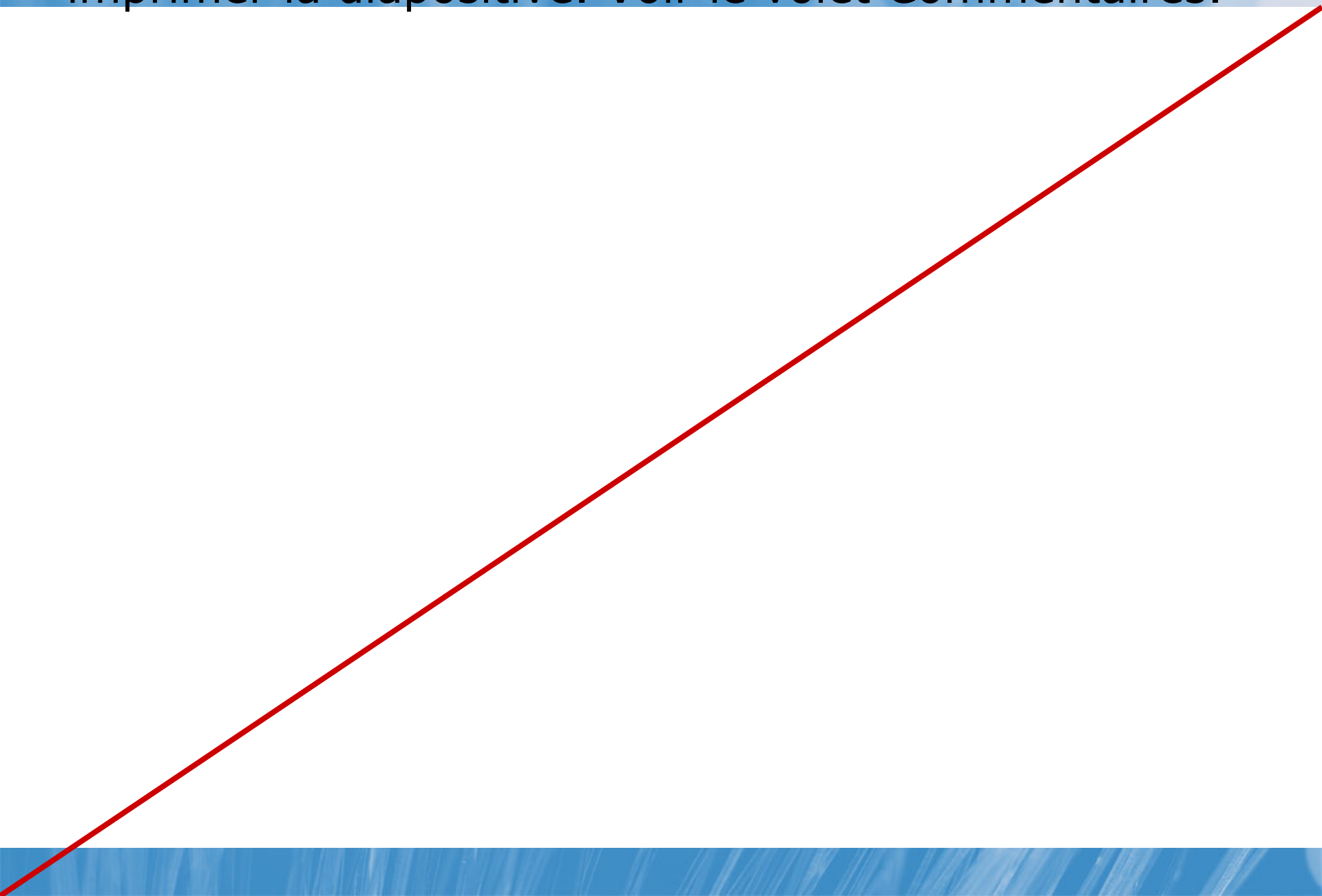
- **Pr. Nordine ZIDANE**

MICROSOFT OFFICIAL COURSE

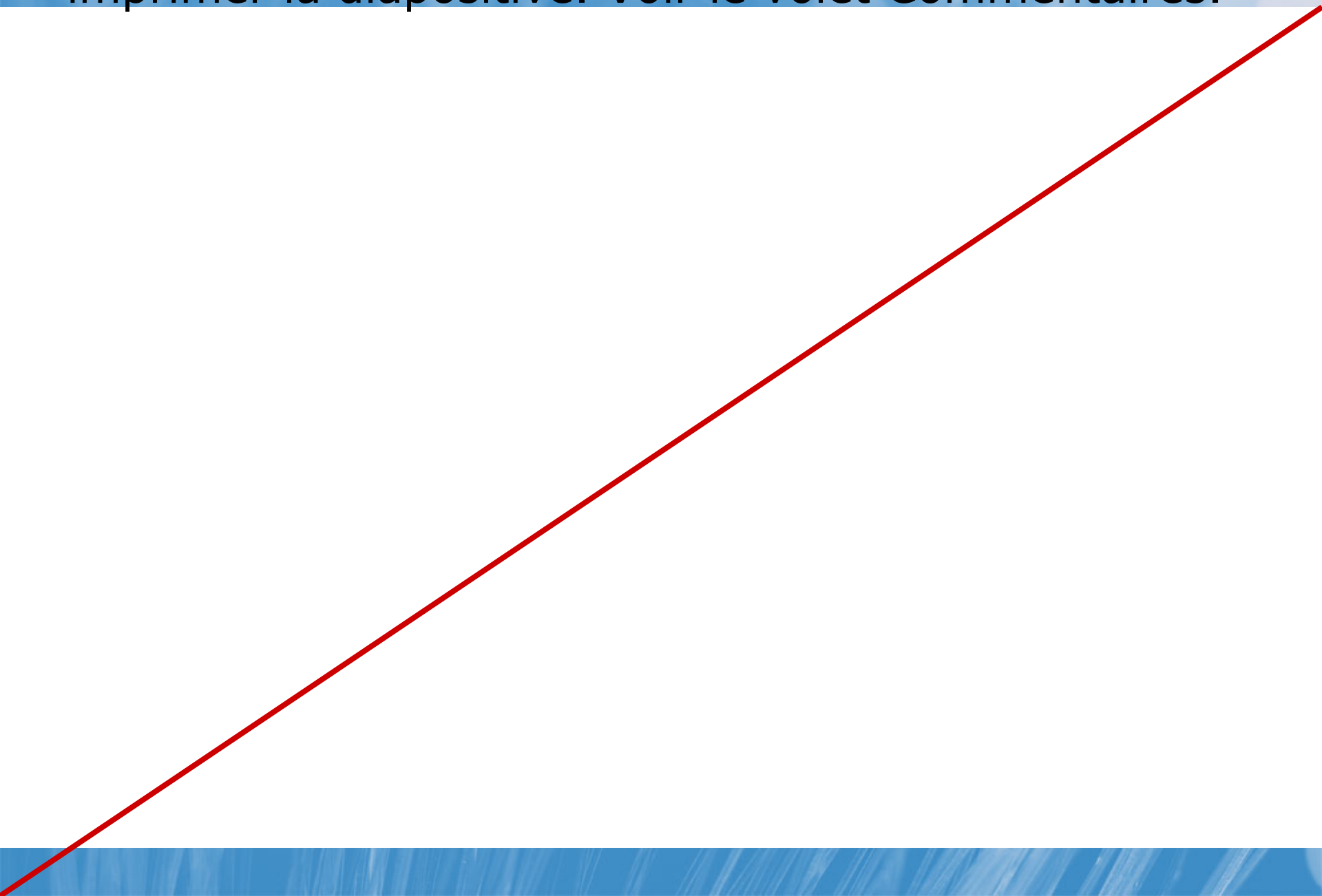
Module 4

Gestion des groupes

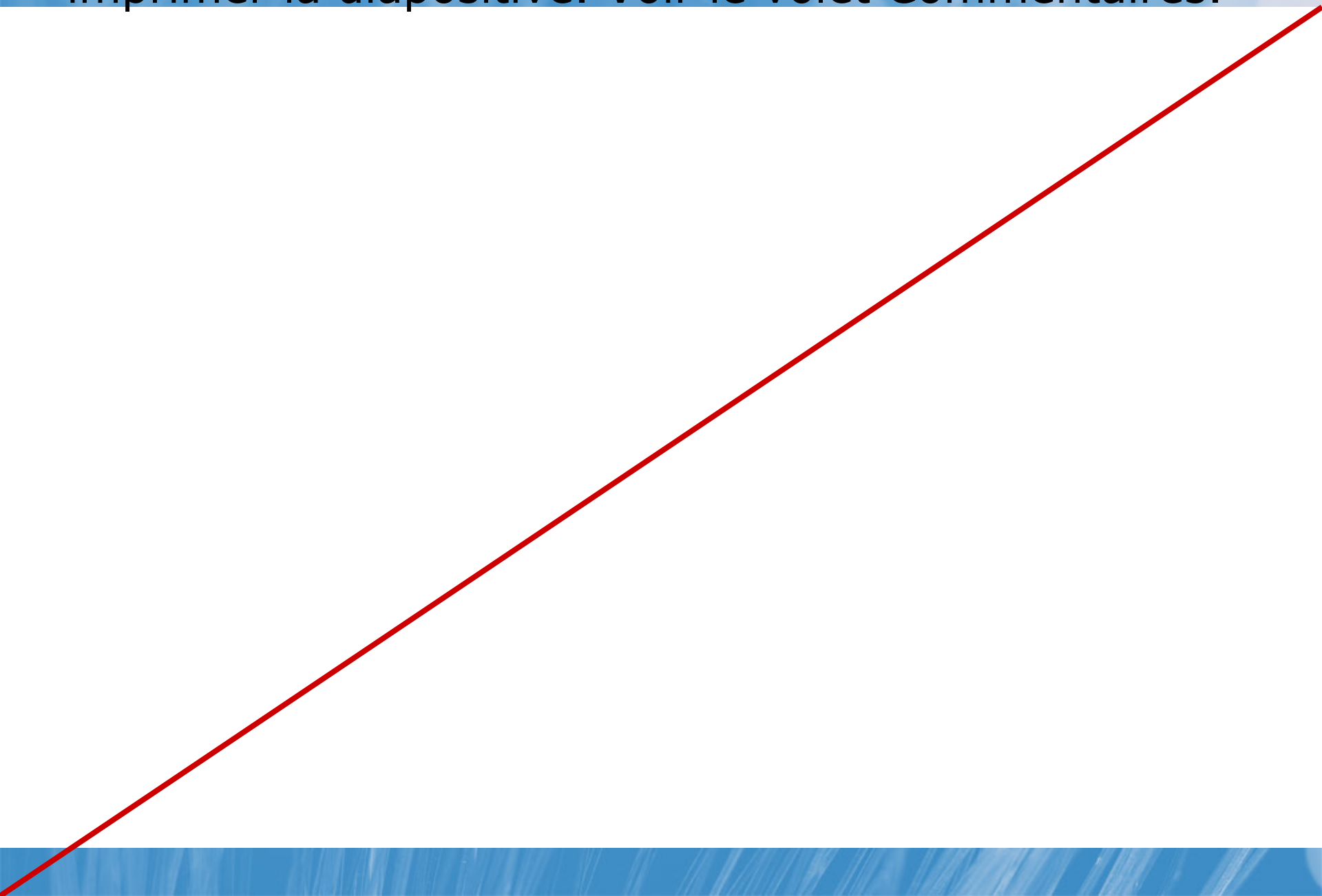
Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.



Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.



Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.



Vue d'ensemble du module

- Gestion d'une entreprise avec des groupes
- Administration des groupes
- Pratiques recommandées pour la gestion des groupes

Leçon 1 : Gestion d'une entreprise avec des groupes

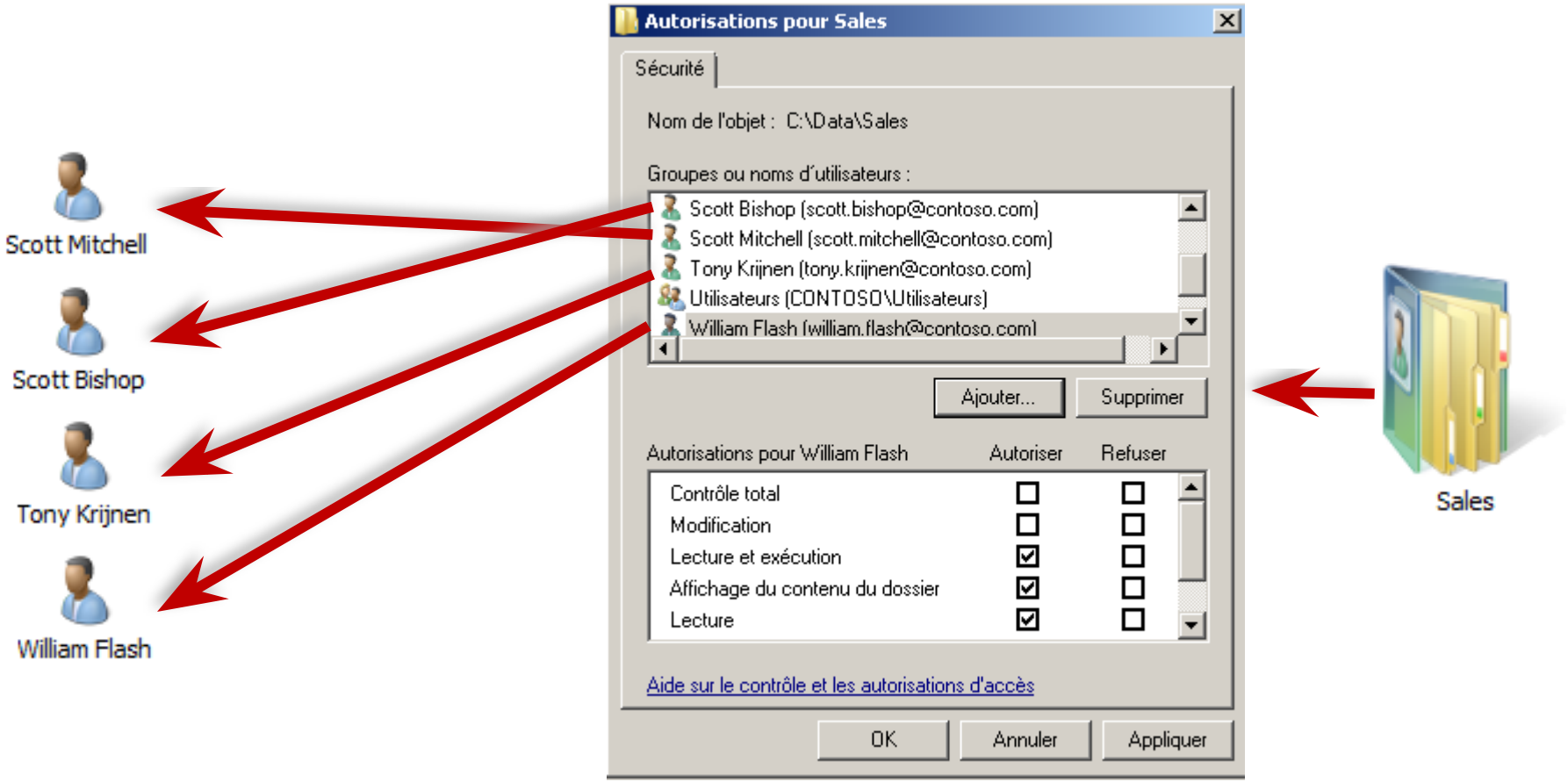
- Démonstration : Création d'un objet groupe
- Gestion des accès sans utiliser des groupes
- Simplification de la gestion par l'utilisation de groupes
- Évolutivité de l'utilisation des groupes
- Un seul type de groupe ne suffit pas
- Gestion à base de rôles : Groupes de rôles et groupes de règles
- Définition des conventions d'appellation pour les groupes
- Type de groupe
- Étendue d'un groupe
- Groupes locaux
- Groupes globaux
- Groupes universels
- Récapitulatif des possibilités de l'étendue des groupes
- Gestion des membres des groupes
- Développement d'une stratégie de gestion des groupes (IGDLA)
- Gestion à base de rôles et stratégie de gestion des groupes Windows

Démonstration : Création d'un objet groupe

Objectifs de cette démonstration :

- Comment créer un groupe
- Comment configurer les propriétés d'un objet groupe

Gestion des accès sans utiliser des groupes

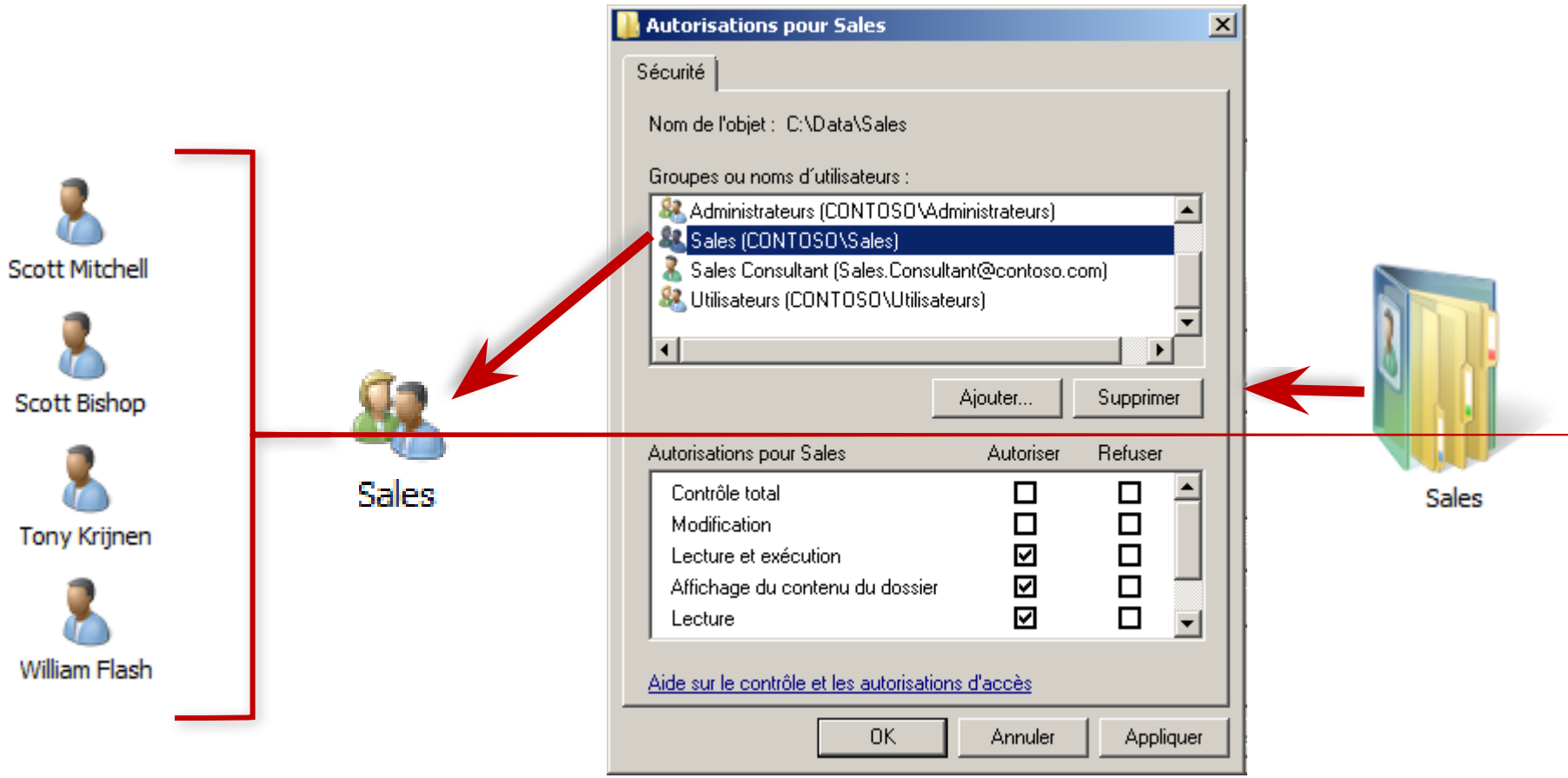


Identité

Gestion des accès

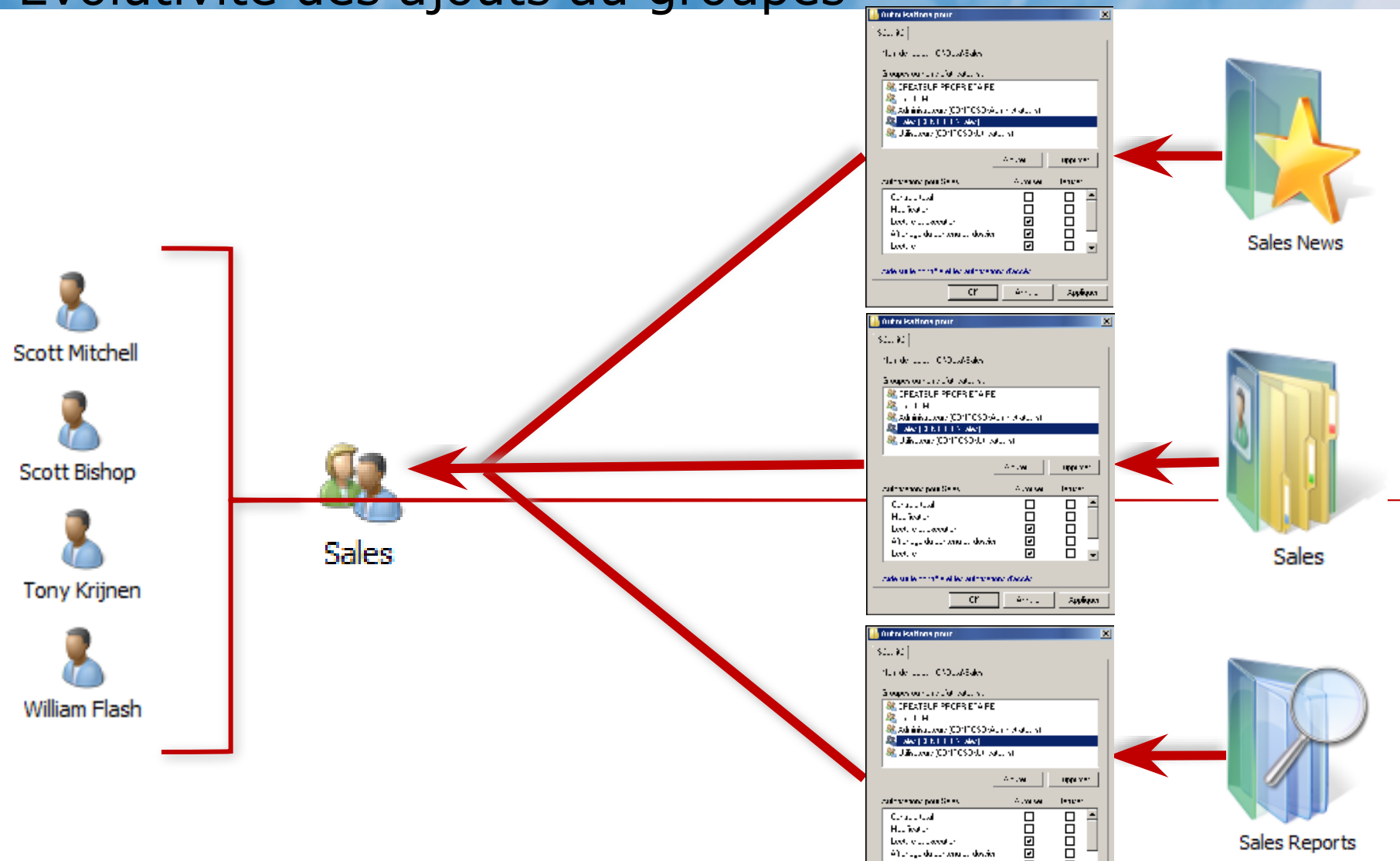
Ressource

Gestion des ajouts aux groupes

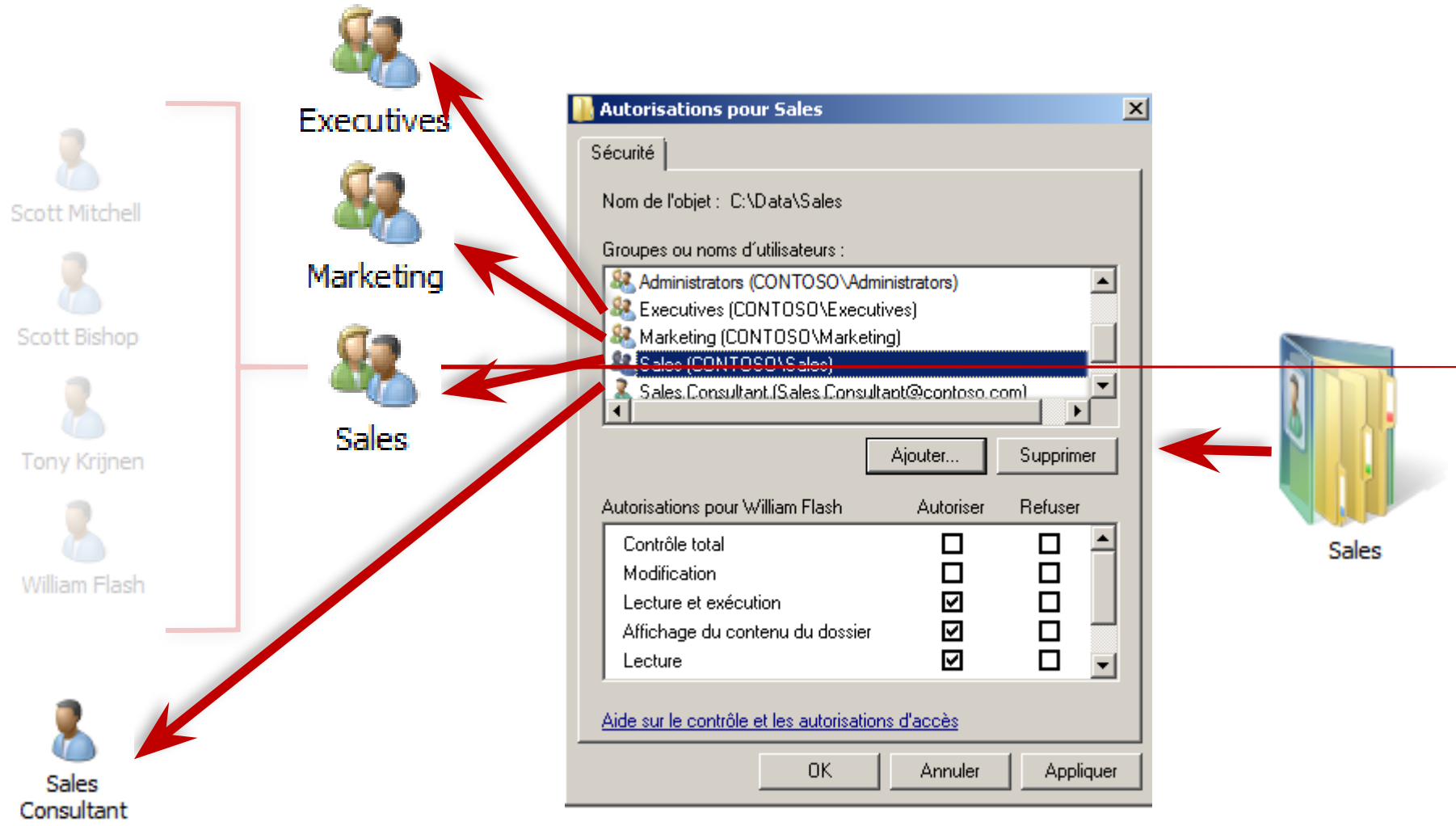


Identité **Groupe** **Gestion des accès** **Ressource**

Évolutivité des ajouts au groupes

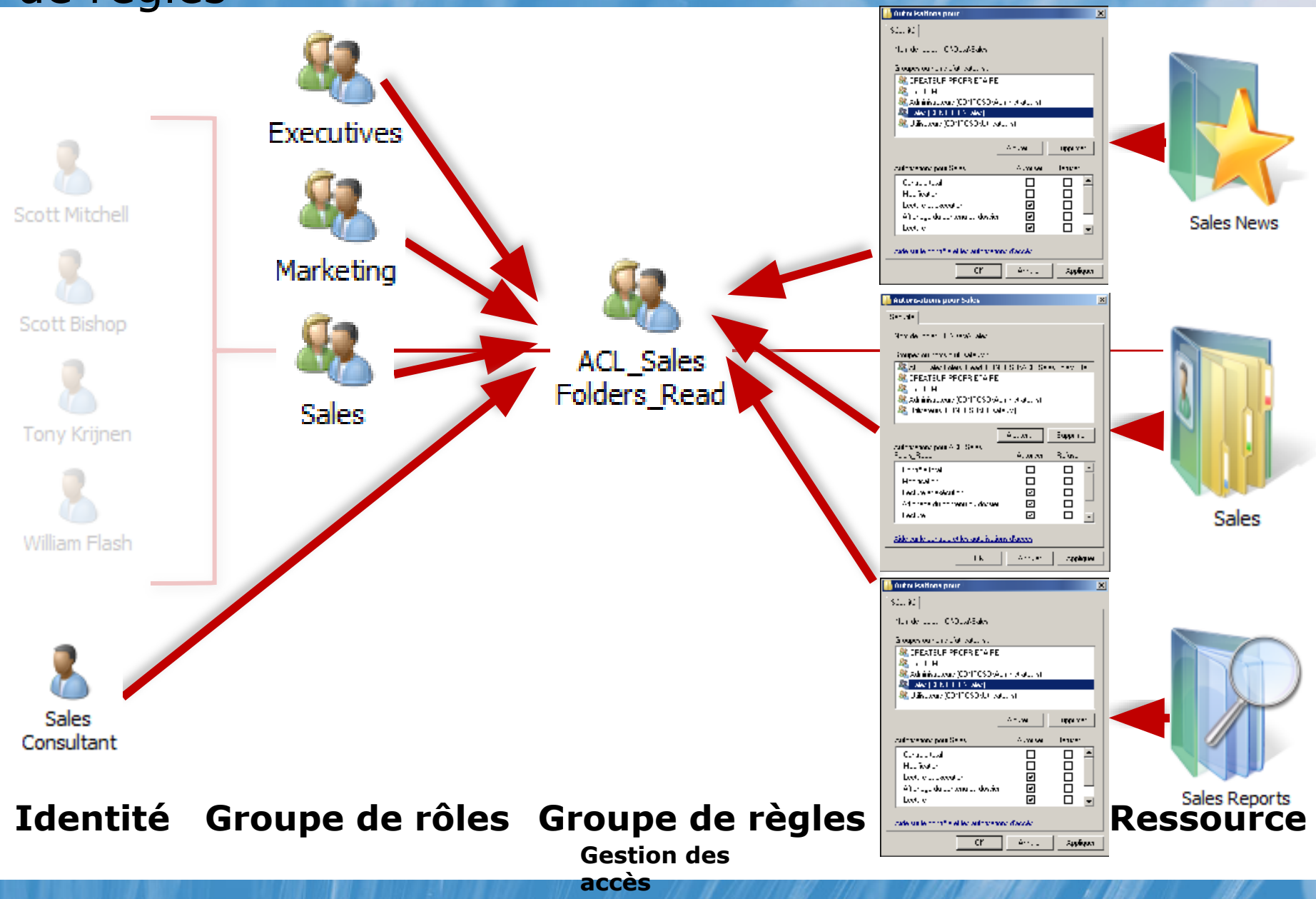


Un seul type de groupe ne suffit pas

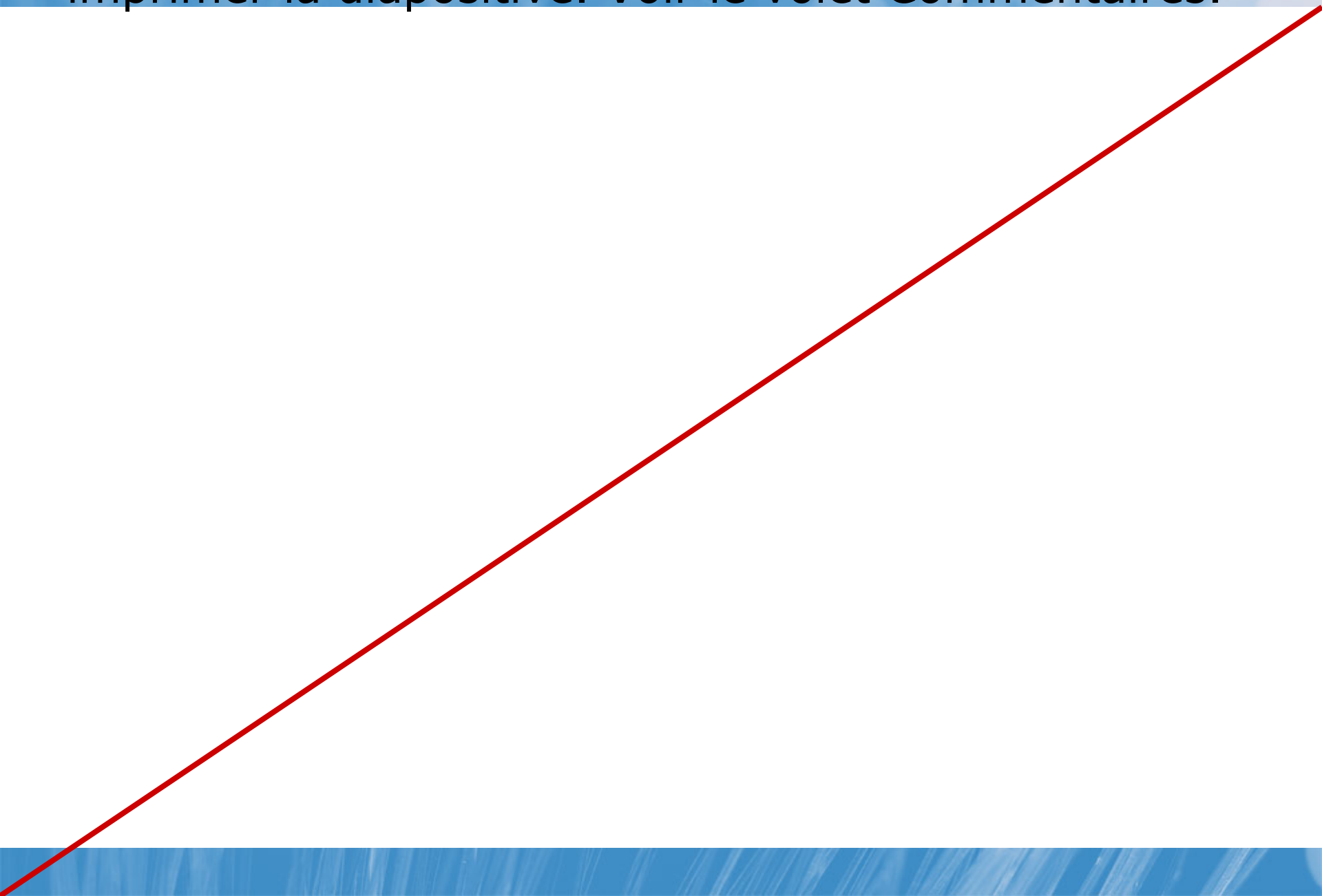


Identité **Groupe** **Gestion des accès** **Ressource**

Gestion à base de rôles : Groupes de rôles et groupes de règles



Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires.



Définition des conventions d'appellation pour les groupes

- Propriétés liées au nom
  - **Nom de groupe.** cn et nom de groupe -- unique dans l'UO
  - **Nom de groupe (avant Windows 2000).** sAMAccountName du groupe - unique dans le domaine
  - Utiliser le même nom (unique dans le domaine) pour les *deux* propriétés
- Conventions d'appellation
  - **Groupes de rôles.** Nom simple unique, tel que Sales ou Consultants
  - **Groupes de gestion.** Par exemple, ACL_Sales Folders_Read
    - **Préfixe.** Fonction de gestion du groupe, par exemple liste ACL
    - **Identificateur de ressource.** Élément à gérer, tel que Sales Folders
    - **Suffixe.** Niveau d'accès, tel que Lecture
    - **Délimiteur.** Séparateur des éléments du nom, tel que le trait de soulignement (_)

Type de groupe

Groupes de distribution

- Utilisés uniquement avec les applications de messagerie
- Pas de sécurité activée (pas de SID) ; impossible d'accorder des autorisations

Groupes de sécurité

- Entité de sécurité avec un SID ; des autorisations peuvent être accordées
- Peuvent prendre en charge la messagerie

Étendue du groupe

- Un groupe peut avoir 4 étendues
  - Locale
  - Globale
  - Locale de domaine
  - Universelle
- Caractéristiques de chaque étendue
  - **Réplication**. Où sont stockés le groupe et sa liste de membres ?
  - **Membres**. Quels types d'objets, provenant de quels domaines, peuvent être membres d'un groupe ?
  - **Disponibilité (étendue)**. Où le groupe peut-il être utilisé ? Dans quelles étendues le groupe peut-il *se trouver* ? Le groupe peut-il être ajouté à une liste ACL ?

Groupes locaux

- Réplication
  - Définition dans le Gestionnaire de comptes de sécurité (SAM) d'un membre de domaine ou d'un ordinateur de groupe de travail
  - Aucune réplication de l'appartenance
- Membres : Un groupe local peut inclure :
  - tout type d'entité de sécurité du domaine : utilisateurs (U), ordinateurs (O), groupes globaux (GG) ou groupes locaux de domaine (GLD)
  - U, O, GG de tout domaine de la forêt
  - U, O, GG de tout domaine approuvé
  - groupes universels (GU) définis dans un domaine de la forêt
- Disponibilité / étendue
  - Limitée à l'ordinateur dans lequel le groupe est défini. Peut-être utilisé pour les listes ACL sur l'ordinateur local uniquement
  - Ne peut pas appartenir à un autre groupe

Groupes locaux de domaine

- Réplication
  - Définition dans le contexte d'appellation du domaine
  - Groupe et membres répliqués sur chaque CD du domaine
- Membres : un groupe local de domaine peut inclure :
  - tout type d'entité de sécurité du domaine : U, O, GG, GLD
  - U, O, GG de tout domaine de la forêt
  - U, O, GG de tout domaine approuvé
  - GU définis dans un domaine de la forêt
- Disponibilité / étendue
  - Peut être sur les listes ACL de toute ressource ou membre du domaine
  - Peut être membre des autres groupes locaux du domaine ou des groupes locaux de l'ordinateur
- Bien adapté à la définition de règles de gestion d'entreprise

Groupes globaux

- Réplication
  - Définition dans le contexte d'appellation du domaine
  - Groupe et membres répliqués sur chaque CD du domaine
- Membres : Un groupe global peut inclure :
  - *Uniquement* les entités de sécurité du même domaine : U, O, GG, GLD
- Disponibilité / étendue
  - Peut être utilisé par tous les membres d'un domaine, tous les autres domaines de la forêt et tous les domaines externes autorisés à approuver.
  - Peut être sur les listes ACL de toute ressource ou tout ordinateur de ces domaines
  - Peut être membre de tout GLD ou GU de la forêt, et de tout GLD d'un domaine externe autorisé à approuver
- Bien adapté à la définition de rôles

Groupes universels

- Réplication
  - Définis dans un seul domaine de la forêt
  - Répliqué sur le catalogue global (à l'échelle de la forêt)
- Membres : Un groupe universel peut inclure :
  - U, O, GG et GU de tout domaine de la forêt
- Disponibilité / étendue
  - Disponible pour chaque domaine et membre de domaine de la forêt
  - Peut être sur les listes ACL de toute ressource sur tout système de la forêt
  - Peut être membre des autres GU ou GLD n'importe où dans la forêt
- Utile dans les forêts multi-domaines
  - Définition de rôles incluant des membres de plusieurs domaines
  - Définition de règles de gestion d'entreprise pour gérer les ressources de plusieurs domaines de la forêt

Récapitulatif des possibilités de l'étendue des groupes

Étendue du groupe	Membres d'un même domaine	Membres d'un domaine de la même forêt	Membres d'un domaine externe approuvé	Attribution d'autorisations sur les ressources
Locale	U, O, GG, GLD, GU et utilisateurs locaux	U, O, GG, GU	U, O, GG	Dans l'ordinateur local uniquement
Locale de domaine	U, O, GG, GLD, GU	U, O, GG, GU	U, O, GG	N'importe où dans le domaine
Universelle	U, O, GG, GU	U, O, GG, GU	S/O	N'importe où dans la forêt
Globale	U, O, GG	S/O	S/O	N'importe où dans le domaine ou un domaine approuvé

U Utilisateur
O Ordinateur
GG Groupe global
GLD Groupe local de domaine
GU Groupe universel

Gestion des membres des groupes

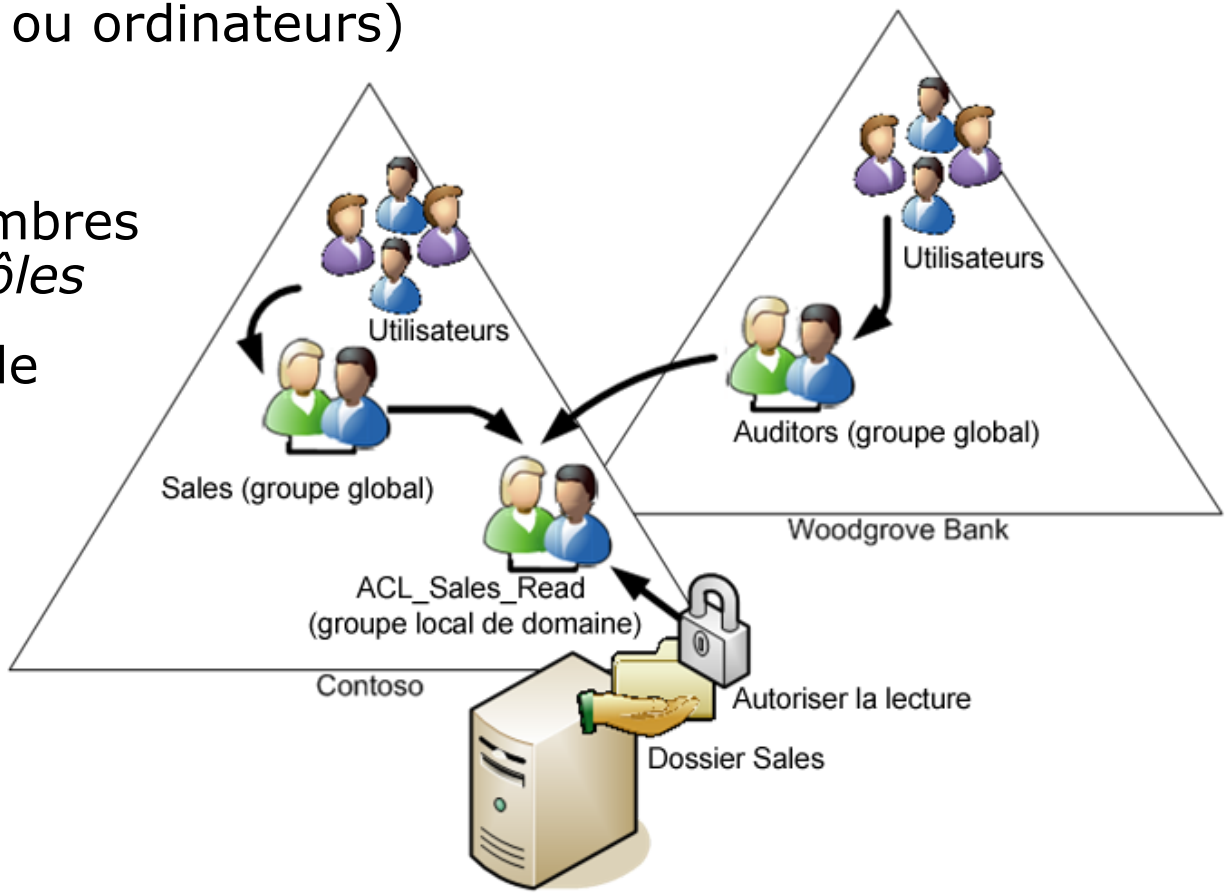
- Méthodes
  - Onglet "Membres" d'un groupe (Ajout/Suppression)
  - Onglet "Membre de" d'un membre (Ajout/Suppression)
  - Commande "Ajouter à un groupe" d'un membre (Ajout)
- Vous modifiez sans cesse l'attribut member
  - L'attribut memberOf est un attribut de lien précédent mis à jour par Active Directory
- Les modifications de la liste des membres ne sont pas appliquées immédiatement
  - L'ouverture de session (utilisateur) ou le démarrage (ordinateur) est nécessaire.
  - Jeton défini avec les SID des groupes de membre à ce moment là
  - Compte pour réplication de modification de la liste de membres sur le contrôleur de domaine de l'utilisateur ou l'ordinateur
  - Conseil : Modifiez les membres d'un groupe sur un CD du site de l'utilisateur

Développer une stratégie de gestion de groupes (IGDLA)

- **I**dentités (utilisateurs ou ordinateurs) membres de
- Groupes **G**lobaux qui collectent des membres en fonction de *leurs rôles*

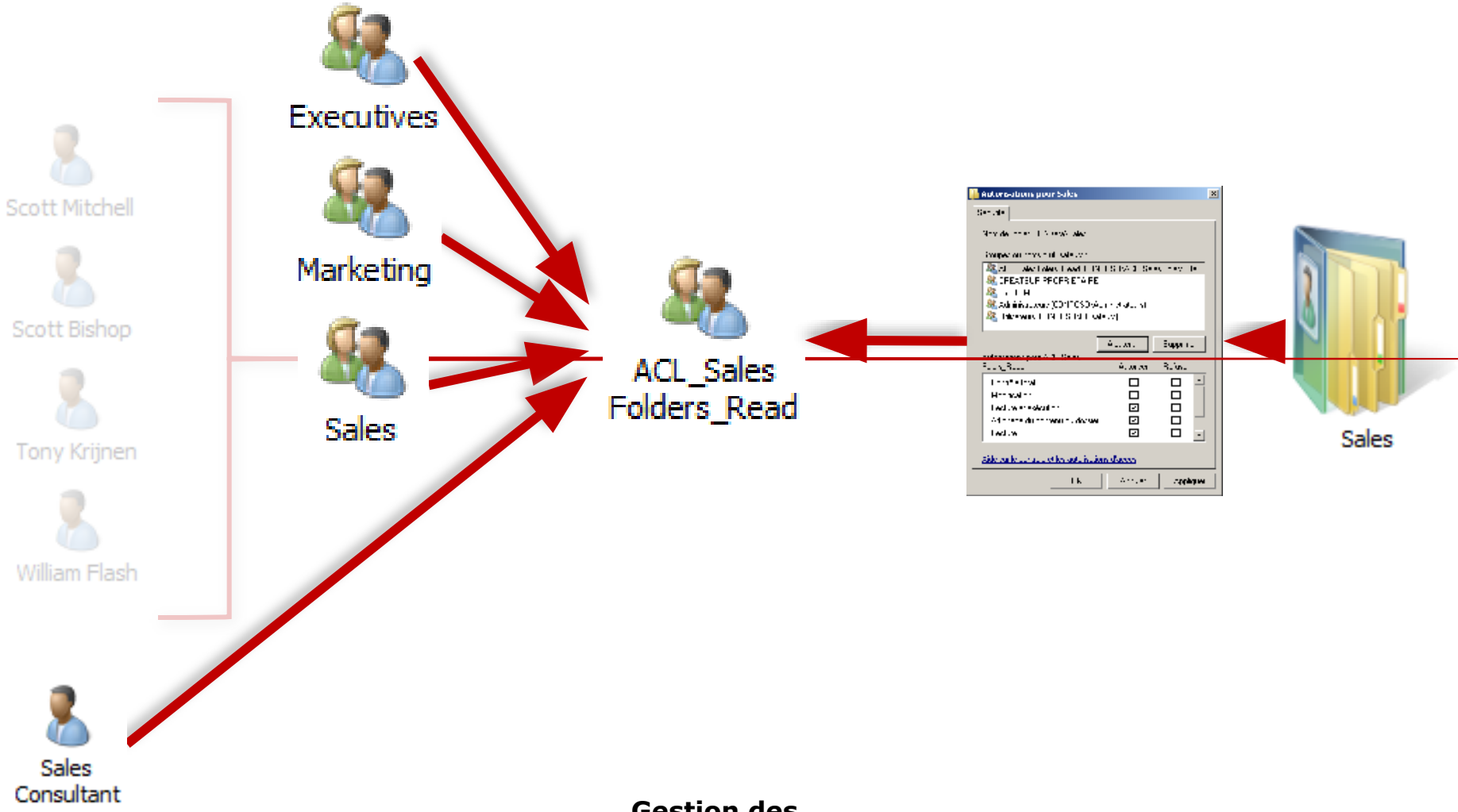
  qui sont membres de
- Groupes de **D**omaine **L**ocaux qui assurent des fonctions de *gestion*, telles que la gestion de l'accès aux ressources

  qui



- ont **A**ccès à une ressource (par exemple, sur une liste **A**CL)
- constituent une forêt multi-domaines : IG**U**DLA

Gestion à base de rôles et stratégie de gestion de groupes Windows



Identité	Groupe de rôles	Gestion des accès	Groupe de règles	Ressource
Identité	Globale		Locale de domaine	Accès

Leçon 2 : Administration des groupes

- Création de groupes avec DSAdd
- Importation de groupes avec CSVDE
- Importation de groupes avec LDIFDE
- Conversion de l'étendue et du type de groupe
- Modification des membres des groupes avec DSMod
- Modification des membres des groupes avec LDIFDE
- Extraction des membres des groupes avec DSGet
- Copie des membres des groupes
- Déplacement des groupes et changement de leurs noms
- Suppression de groupes

Création de groupes avec DSAdd

- dsadd group *DNGroupe* –secgrp {yes|no} –scope {g | l | u}
  - **DNGroupe.** Nom unique du groupe à créer
  - **-secgrp**. Security-enabled (yes=sécurité ; no=distribution)
  - **-scope**. étendue (**g**lobale, **l**ocale du domaine, **u**niverselle)
  - **-samid**. sAMAccountName (non nécessaire, par défaut cn)
  - **-desc Description**. attribut description
  - **-member MemberDN** …. Liste des membres (séparés par un espace) à ajouter lors de la création du groupe
  - **-memberof DNGroupe ...**. Liste des groupes (séparés par un espace) auxquels ajouter ce groupe

```
dsadd group "CN=Marketing,OU=Role,OU=Groups,
    DC=contoso,DC=com"
    –samid Marketing –secgrp yes –scope g
```

Importation de groupes avec CSVDE

- Fichier CSV (valeurs séparées par une virgule)

  Liste d'attributs séparés par une virgule
  Groupes à créer, un par ligne et tous les attributs répertoriés sur la première ligne

- Exemple

```
objectClass,sAMAccountName,DN,member
group,Marketing,"CN=Marketing,OU=Role,OU=Groups,
      DC=contoso,DC=com",
      "CN=Linda Mitchell,OU=Employees,OU=User Accounts,
      DC=contoso,DC=com;CN=Scott Mitchell,OU=Employees,
      OU=User Accounts,DC=contoso,DC=com"
```

- csvde -i -f "*nomfichier*" [-k]
  - **-i**. Importation (mode par défaut : exportation)
  - **-f**. Nom du fichier
  - **-k**. Poursuivre en cas d'erreur (par exemple si un objet existe déjà)
- CSVDE permet de créer des groupes, pas de modifier les groupes existants

Importation de groupes avec LDIFDE

- Fichier LDIF (LDAP Data Interchange Format)

```
DN: CN=Finance,OU=Role,OU=Groups,DC=contoso,DC=com
changeType: add
CN: Finance
description: Finance Users
objectClass: group
SAMAccountName: Finance

DN: CN=Research,OU=Role,OU=Groups,DC=contoso,DC=com
changeType: add
CN: Research
description: Research Users
objectClass: group
SAMAccountName: Research
```

- Ldifde -i -f *nomfichier* [-k]
  - **-i**. Importation (mode par défaut : exportation)
  - **-f**. Nom du fichier
  - **-k**. Poursuivre en cas d'erreur (par exemple si un objet existe déjà)

Conversion d'étendue et de type de groupe

- Le composant Utilisateurs et ordinateurs Active Directory permet de modifier le type d'un groupe
  - Sécurité > distribution (* perte des autorisations attribuées au groupe)
  - Distribution > sécurité
- Le composant Utilisateurs et ordinateurs Active Directory permet de modifier l'étendue d'un groupe :
  - Global en universel
  - Locale de domaine > universelle
  - Universelle > globale
  - Universelle > locale de domaine
  - Vous ne pouvez pas changer LD → G ou G → LD directement, mais vous *pouvez* changer LD → U → G *ou* G → U → LD.
  - Modification impossible si les membres sont incorrects : corriger et essayer à nouveau
- dsmod group *DNGroupe* –secgrp { yes | no } –scope { l | g | u }

Modification des membres des groupes avec DSMod

- dsmod group "*DNGroupe*" [*options*]
  - -addmbr "Member DN"
  - -rmmbr "Member DN"

```
dsmod group "CN=Research,OU=Role,OU=Groups,
DC=contoso,DC=com" -addmbr "CN=Mike Danseglio,
OU=Employees,OU=User Accounts,DC=contoso,DC=com"
```

Modification des membres des groupes avec LDIFDE

- Fichier LDIF

```
dn: CN=Finance,OU=Role,OU=Groups,DC=contoso,DC=com
changetype: modify
add: member
member: CN=April Stewart,OU=Employees,OU=User Accounts,
      dc=contoso,dc=com
member: CN=Mike Fitzmaurice,OU=Employees,OU=User Accounts,
      dc=contoso,dc=com
-
```

- Changetype: modify
- 3e ligne : Quel type de modification ? Ajouter une valeur à un membre
  - Supprimer un membre, modifier pour supprimer : member
- L'opération de modification se termine par une ligne contenant uniquement –

Extraction des membres des groupes avec DSGet

- Aucune option pour obtenir la *liste complète* des membres d'un groupe dans Utilisateurs et ordinateurs Active Directory
- DSGet permet d'obtenir la liste complète (y compris des membres imbriqués)
- dsget group "*DNGroupe*" –members [-expand]
  - Liste des membres d'un groupe (*DNGroupe*), pouvant inclure les membres imbriqués (-expand)
- dsget {user|computer} "*DNObjet*" –memberof [-expand]
  - Liste des appartenances d'un utilisateur ou un ordinateur (DNObjet), pouvant inclure les appartenances à des groupes imbriqués (-expand)

Copie des membres de groupes

- Copie des membres d'un groupe dans un autre

```
dsget group "CN=Sales,OU=Role,OU=Groups,DC=contoso,DC=com" –members |
dsmod group "CN=Marketing,OU=Role,OU=Groups,DC=contoso,DC=com" –addmbr
```

- Copie des appartenances d'un utilisateur sur un autre

```
dsget user "DNUtilisateurSource" –memberof |
      dsmod group –addmbr "DNUtilisateurCible"
```

Déplacer et renommer des groupes

- Utilisateurs et ordinateurs Active Directory
  - Cliquez avec le bouton droit sur le groupe, puis cliquez sur Déplacer ou Renommer
- Commande DSMove
  - dsmove *DNObjet* [-newname *NouveauNom*] [-newparent *DNUOcible*]
    - DNObjet est le DN du groupe
    - **-newparent** *DNUOcible* déplace le groupe dans une nouvelle UO
    - **-newname** *NouveauNom* modifie le cn du groupe
      - Il faut utiliser DSMod Group pour modifier sAMAccountName

```
dsmove "CN=Public Relations,OU=Role,OU=Groups,DC=contoso,DC=com"
   -newparent "OU=Marketing,DC=contoso,DC=com"

dsmove "CN=Marketing,OU=Role,OU=Groups,DC=contoso,DC=com"
   -newname "Public Relations"
dsmod group "CN=Public Relations,OU=Role,OU=Groups,DC=contoso,DC=com"
   -samid "Public Relations"
```

Suppression de groupes

- Utilisateurs et ordinateurs Active Directory : Clic droit, Supprimer
- Commande DSRm
  - dsrm *DNObjet* ... [-subtree [-exclude]] [-noprompt] [-c]
    - -noprompt évite les demandes de confirmation de chaque suppression
    - -c permet de continuer en cas d'erreur (refus d'accès par exemple)
    - -subtree supprime l'objet et tous les objets enfants
    - -subtree -exclude supprime tous les objets enfants mais pas l'objet lui-même

```
dsrm "CN=Public Relations,OU=Role,OU=Groups,
     DC=contoso,DC=com"
```

- La suppression d'un groupe de sécurité entraîne des conséquences importantes
  - Le SID est perdu et ne peut plus être rétabli même si le groupe est à nouveau créé
  - Conseil : D'abord, enregistrez puis supprimez tous les membres durant une période de test, pour évaluer tous les effets indésirables possibles

Atelier pratique A : Administration des groupes

- Exercice 1 : Implémenter la gestion à base de rôles en utilisant des groupes
- Exercice 2 : Gérer les membres des groupes via l'invite de commandes
- Exercice 3 (facultatif avancé) : Analyse des outils de génération de rapports des membres des groupes
- Exercice 4 (facultatif avancé) : Compréhension des autorisations « Compte inconnu »

Informations de connexion

Ordinateur virtuel	6238B-HQDC01-A
Nom d'ouverture de session utilisateur	Pat.Coleman
Nom d'utilisateur administrateur	Pat.Coleman Admin
Mot de passe	Pa$$w0rd

Durée approximative : 15 minutes

Scénario de l'atelier pratique

- Pour améliorer la gestion des accès aux ressources chez Contoso, Ltd., vous avez décidé d'implémenter la gestion à base de rôles. La première opération consistera à déterminer les personnes autorisées à accéder aux informations des ventes. Vous devez créer des groupes afin de gérer l'accès à ces informations confidentielles. Selon les règles de l'entreprise, les employés des services Sales et Marketing et de l'équipe des Consultants sont autorisés à consulter les dossiers des ventes (Sales). De plus, Bobby Moore nécessite un accès en lecture. Enfin, on vous a demandé de rechercher un moyen de produire la liste des membres des groupes, y compris ceux des groupes imbriqués, et la liste des appartenances aux groupes d'un utilisateur, y compris les appartenances indirectes ou imbriquées.

Récapitulatif

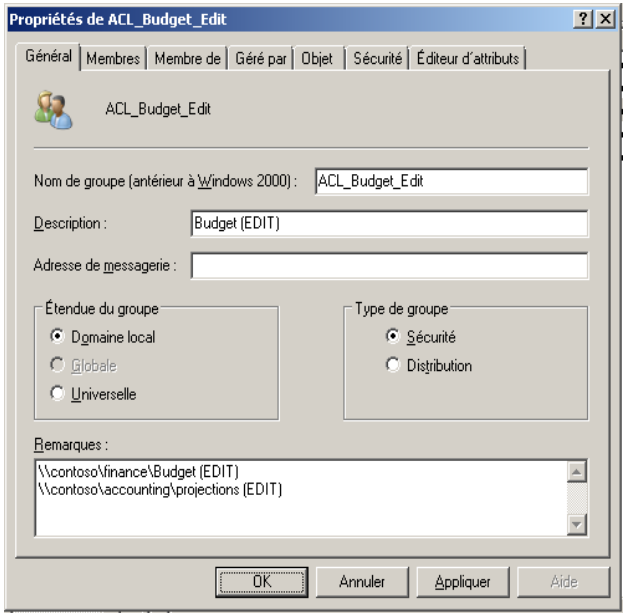
- Décrivez la fonction des groupes globaux dans le cadre de la gestion à base de rôles.
- Quels types d'objets peuvent appartenir à un groupe global ?
- Décrivez la fonction des groupes locaux de domaine dans le cadre de la gestion des accès aux ressources en fonction de rôles.
- Quels types d'objets peuvent appartenir à un groupe local de domaine ?
- Vous avez implémenté la gestion à base de rôles et on vous demande la liste des utilisateurs autorisés à consulter les dossiers Sales. Quelle commande utilisez-vous ?

Leçon 3 : Pratiques recommandées pour la gestion des groupes

- Pratiques recommandées pour la documentation des groupes
- Protéger les groupes contre la suppression accidentelle
- Déléguer la gestion des membres avec l'onglet Géré par
- Groupes par défaut
- Identités spéciales

Pratiques recommandées pour la documentation des groupes

- Pourquoi décrire les groupes ?
  - Faciliter leur identification lors des recherches
  - Mieux comprendre comment et quand utiliser un groupe
- Établir et respecter une convention d'appellation stricte
  - Un préfixe, par exemple, permet de différencier APP_Budget et ACL_Budget_Edit
  - Un préfixe facilite la *recherche* d'un groupe dans la boîte de dialogue de sélection
- Indiquer la fonction d'un groupe avec son attribut de description
  - Apparaît dans le volet d'informations du composant Utilisateurs et ordinateurs Active Directory
- Détailler la fonction d'un groupe dans la zone des commentaires

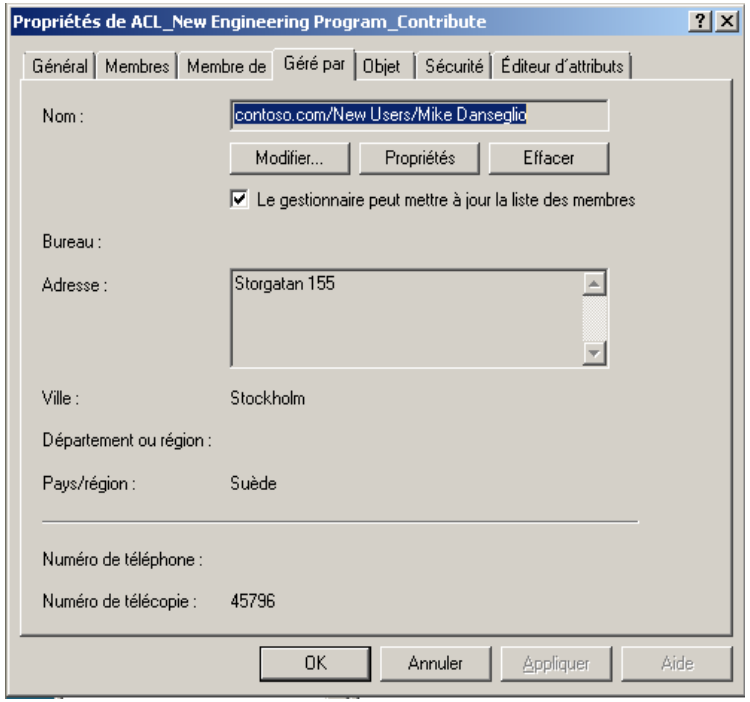


Protection des groupes contre la suppression accidentelle

1. Dans le composant Utilisateurs et ordinateurs Active Directory, cliquez sur le menu **Affichage** et sélectionnez **Fonctionnalités avancées**.
2. Ouvrez la boîte de dialogue **Propriétés** d'un groupe.
3. Dans l'onglet **Objet**, cochez la case **Protéger l'objet des suppressions accidentelles**.
4. Cliquez sur **OK**.

Délégation de la gestion des membres avec l'onglet Géré par

- L'onglet Géré par a deux fonctions :
  - Fournir des informations de contact indiquant qui gère le groupe
  - L'utilisateur (ou le groupe) indiqué peut modifier les membres des groupes si l'option "Le gestionnaire peut mettre à jour la liste des membres" est sélectionnée
- Conseil
  - Il faut cliquer sur OK (et pas uniquement sur Appliquer) pour changer l'ACL du groupe
  - Pour définir un groupe dans la zone Nom, cliquez sur Modifier, puis sur Types d'objet, puis sur Groupes



Groupes par défaut

- Groupes locaux par défaut dans les conteneurs BUILTIN et Utilisateurs
  - Administrateurs de l'entreprise, Administrateurs du schéma, Administrateurs, Admins du domaine, Opérateurs de serveur, Opérateurs de compte, Opérateurs de sauvegarde, Opérateurs d'impression
- Indiquez que leurs droits et privilèges sont décrits dans le manuel du stagiaire
  - Ces droits sont à connaître pour les examens de certification
- Problèmes liés à ces groupes
  - Excès de délégation
    - Les opérateurs de compte, par exemple, peuvent ouvrir des sessions sur un contrôleur du domaine (CD).
  - Protégé
    - Les utilisateurs appartenant à ces groupes sont protégés et le restent lorsqu'ils sont supprimés
- Recommandation : Laisser ces groupes vides et créer des groupes personnalisés avec les droits et privilèges nécessaires

Identités spéciales

- L'appartenance aux groupes est gérée par Windows :
  - Impossible de les afficher, les modifier ni les ajouter à d'autres groupes
  - Peuvent être utilisées sur les listes ACL
- Exemples
  - **Ouverture de session anonyme.** Représente les connexions à un ordinateur sans nom d'utilisateur ni mot de passe
  - **Utilisateurs authentifiés.** Représente les identités authentifiées, mais n'inclut pas l'identité Invité
  - **Tout le monde.** Inclut Utilisateurs authentifiés et Invité (mais *pas* Ouverture de session anonyme par défaut dans Windows Server 2003/2022)
  - **Interactif.** Utilisateurs connectés en session locale ou Bureau à distance
  - **Réseau.** Utilisateurs accédant à une ressource par le réseau

Atelier pratique B : Pratiques recommandées pour la gestion des groupes

- Exercice 1 : Implémenter les pratiques recommandées pour la gestion des groupes

Informations de connexion

Ordinateur virtuel	6238B-HQDC01-A
Nom d'ouverture de session utilisateur	Pat.Coleman
Nom d'utilisateur administrateur	Pat.Coleman Admin
Mot de passe	Pa$$w0rd

Durée approximative : 15 minutes

Scénario de l'atelier pratique

- Votre implémentation de la gestion à base de rôles chez Contoso est très efficace. Le nombre de groupes ayant augmenté dans le domaine, vous constatez qu'il est important de les documenter soigneusement et d'empêcher les administrateurs d'en supprimer accidentellement. Enfin, vous voulez permettre aux propriétaires des ressources de l'entreprise de gérer les accès à leurs ressources en leur délégant le droit de modifier les membres des groupes.

Récapitulatif

- Citez des avantages de l'utilisation des champs Description et Commentaires d'un groupe.
- Quels sont les avantages et les inconvénients de la délégation des membres des groupes ?