

# Comprendre et mettre en oeuvre la sécurité sous Microsoft Access

par Fabrice CONSTANS ([autres articles](#))

Date de publication : 05/01/1999

Dernière mise à jour : 19/03/2008

Ce tutorial traite des moyens de sécuriser une application Microsoft ACCESS. Nous ne traiterons que la sécurité d'applications de type mdb utilisant le moteur de base de données propriétaire (JET) de Microsoft ACCESS. Nous n'aborderons pas les pages d'accès aux données ni les applications basées sur le moteur SQL Server ou via ODBC.

- I - Introduction
  - I-A - Avertissement
- II - Architecture
  - II-A - Fichier unique
  - II-B - Fichier Serveur (Pseudo client serveur)
- III - Sécurité Système
  - III-A - Concept - Méthode
  - III-B - Utilité des accès et fichier ldb
- IV - Sécurité applicative
  - IV-A - Méthode Compilation MDE
    - IV-A-1 - Contraintes
    - IV-A-2 - Générer un fichier MDE
  - IV-B - Méthode Mot de passe
    - IV-B-1 - Mot de passe au démarrage
      - IV-B-1-a - Mettre en place ce mot de passe
      - IV-B-1-b - Retirer le mot de passe
    - IV-C - Méthode Mot de passe sur le code
- V - Bases de la Sécurité utilisateur
  - V-A - Théorie
  - V-B - Définition et organisation des groupes, utilisateurs, droits...
    - V-B-1 - Groupe de travail
    - V-B-2 - Groupe d'utilisateurs
    - V-B-3 - Compte d'utilisateur
    - V-B-4 - Droits
    - V-B-5 - Objets
    - V-B-6 - Héritage
    - V-B-7 - Propriétaire
- VI - Groupe de travail
  - VI-A - Démonstration
  - VI-B - Création d'un groupe de travail
- VII - Groupes d'utilisateurs
  - VII-A - Définition des groupes d'utilisateurs
  - VII-B - Création de groupes
  - VII-C - Suppression de groupes
- VIII - Droits d'accès
  - VIII-A - Droits et dépendances
  - VIII-B - Groupes des utilisateurs
- IX - Les comptes utilisateurs
  - IX-A - Création des comptes
    - IX-A-1 - Définir les mots de passe des comptes
  - IX-B - Affectation des comptes
  - IX-C - L'administrateur un cas particulier
  - IX-E - Activer les comptes
  - IX-D - Propriétaire
- X - Mots de passe et dégradation
  - X-A - Les autres objets
- XI - Tests
  - XI-A - Avec le fichier MDW sécurisé
  - XI-B - Avec le fichier MDW standard
- XII - Les requêtes et la protection
  - XII-A - Plus loin avec ce type de requête
- XIII - Codes, SQL et astuces
  - XIII-A - Fichier MDW et options de démarrage
  - XIII-B - Sécurité et code VBA

XIII-B-1 - Changement du mot de passe de la base de données courante

XIII-B-2 - Changement du mot de passe de l'utilisateur courant

XIII-B-3 - Renvoi le nom de l'utilisateur ACCESS courant

XIII-B-4 - Renvoi le nom de l'utilisateur WINDOWS courant

XIII-C - Sécurité et DAO

XIII-C-1 - DAO - Créer un groupe

XIII-C-2 - DAO - Créer un utilisateur

XIII-C-3 - DAO - Suppression Groupe

XIII-C-4 - DAO - Suppression Utilisateur

XIII-C-5 - DAO - Affecter un utilisateur à un groupe

XIII-B-6 - DAO - Lister les groupes et utilisateurs

XIII-D - SQL et la sécurité


XIV - Liens importants


XV - Remerciements

## I - Introduction

Il existe plusieurs méthodes pour sécuriser une application Microsoft ACCESS. Elles sont indépendantes et souvent complémentaires. Nous allons expliquer chacune d'elle et proposer un exemple pour sa mise en oeuvre.

### I-A - Avertissement

 *L'utilisation de la touche F1 est vivement conseillée à tous les stades de l'utilisation d'ACCESS. L'amélioration constante de l'aide en fait un partenaire de choix dans l'apprentissage permanent d'ACCESS. Personnellement, je ne peux m'en passer, ne serait-ce que pour mémoire.*

 *Avant d'effectuer les manipulations décrites dans ce tutoriel veuillez à faire une sauvegarde des fichiers de votre application.*

## II - Architecture

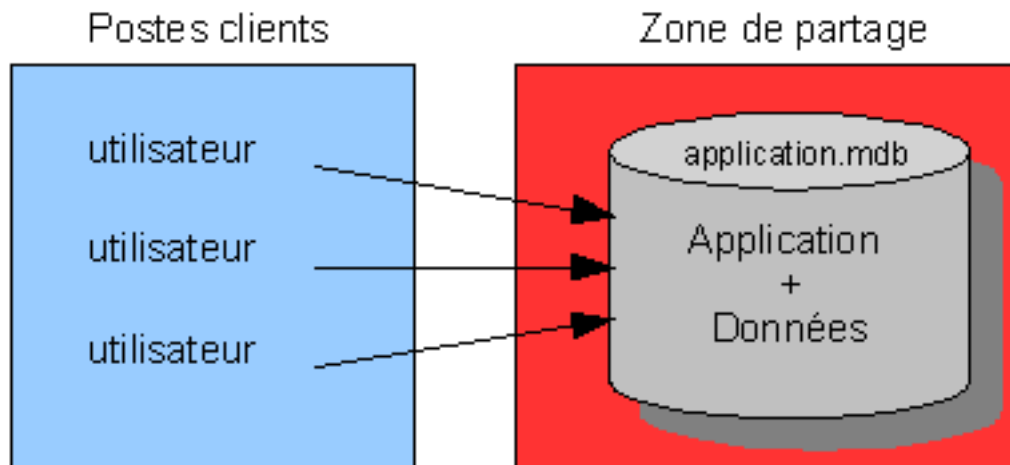
Pour comprendre la sécurité nous devons faire un bref rappel des types d'architecture d'application possibles avec Microsoft ACCESS.

### II-A - Fichier unique

Dans ce type d'architecture les données (tables) et l'interface (formulaires, états, requêtes, code, macro) sont dans le même fichier. Il est employé par de nombreux utilisateurs de Microsoft ACCESS pour des applications personnelles et mono-utilisateur.

Chaque utilisateur se connecte à l'espace de partage et lance le même fichier.

Notez que la zone de partage peut être située sur un serveur dédié ou poste utilisateur ayant un répertoire en partage.



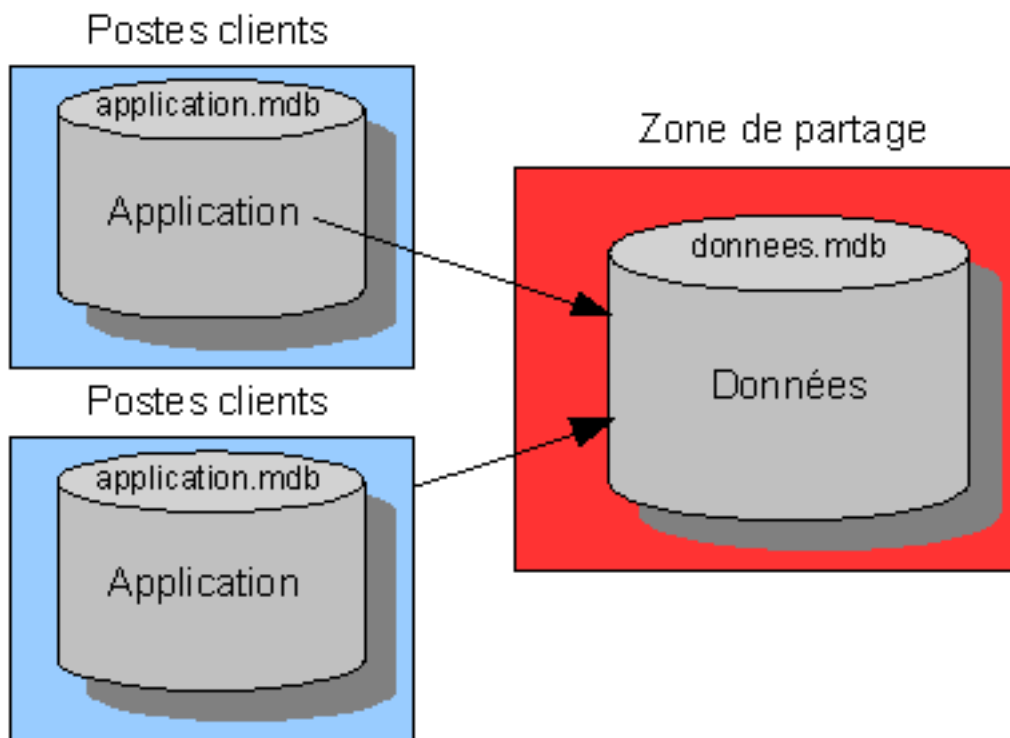
Architecture fichier unique

Bien que ce fichier puisse être partagé et donc être accessible à plusieurs utilisateurs, il est fortement déconseillé de l'employer à cet effet.

- Les accès sont fortement ralentis ;
- L'infrastructure surcharge le réseau ;
- Les méthodes de conception à base de tables temporaires deviennent lourdes à gérer ;
- Le blocage d'un utilisateur peut se répercuter sur l'ensemble.

### II-B - Fichier Serveur (Pseudo client serveur)

Dans cette architecture les tables sont séparées de l'interface et le fichier de l'interface (*frontal*) est installé sur chaque poste client. Le fichier de données (*dorsal*) est en partage et les tables sont liées par un attachement dans chaque fichier frontal.



*Architecture fichier serveur*

Celle-ci est conseillée pour les applications ayant une forte charge (plus d'un utilisateur simultanée/volume de données important).

C'est cette dernière que nous prendrons comme exemple pour mettre en place les diverses sécurités.

### III - Sécurité Système

Bien que ne faisant pas partie de Microsoft Access mais des systèmes d'exploitation dérivés de NT (NT 3.51 et 4, Windows 2000 et XP) nous ne pouvons pas faire l'impasse sur cet aspect de la protection.

#### III-A - Concept - Méthode

La sécurité système permet entre autre de contrôler les accès aux répertoires. Elle est mise en place le plus souvent dans le cadre d'une application partagée ou sur des espaces de stockages multi-utilisateurs. Une fois configurée seul l'utilisateur déclaré aura accès au répertoire et aux fichiers présents.

Les utilisateurs de l'application doivent avoir les accès systèmes suivants sur l'ensemble des répertoires de l'application :

- Création,
- Modification,
- Suppression.

Dans le cas d'une application "**fichier serveur**" les utilisateurs doivent avoir accès aux 2 répertoires avec les droits indiqués précédemment:

- Le répertoire contenant l'application appelée **Frontale**.
- Le répertoire contenant le(s) fichier(s) de données appelé(s) **Dorsal(s)**.

#### III-B - Utilité des accès et fichier ldb

Pourquoi avoir autant d'accès est si important pour l'utilisation d'une application ?

Un fichier est créé dans le répertoire à chaque accès à l'un des fichiers d'une application, ce comportement est valable pour toute application quelque soit l'architecture et le nombre d'utilisateurs. Les fichiers créés portent le nom du fichier Microsoft ACCESS qui est ouvert (mdb, mde) suivi de l'extension **ldb** (Lock file for Access DataBase).

Par exemple :

Pour le fichier **Monapplication.mdb** le fichier portera le nom de **Monapplication.ldb**.

Ce fichier contient des informations importantes : l'identification unique de l'utilisateur connecté et non du poste accédant à la base.

Le tableau suivant dresse les actions simplifiées opérées sur les fichiers Ldb dans le cadre de l'utilisation d'une application de type "**fichier serveur**" par plusieurs utilisateurs.

Les fichiers applicatifs portent les noms respectifs de **application.mdb** (ou mde) pour la partie applicative et **données.mdb** pour la partie contenant les données.

Action	fichier Ldb frontal : application.ldb	fichier Ldb dorsal : données.ldb
Le premier utilisateur ouvre l'application	création du fichier, l'utilisateur est inscrit dans le fichier ldb.	aucun effet
Le premier utilisateur accède à une table	table résidente : aucun effet	table attachée : création du fichier ldb sur le fichier frontal
Un deuxième utilisateur se connecte	modification du fichier ldb (l'utilisateur est inscrit)	aucun effet
Le premier utilisateur ferme l'application	désinscription de l'utilisateur dans le fichier ldb	suppression du fichier ldb
Le deuxième utilisateur accède à une table	table résidente : aucun effet	table attachée : création du fichier ldb sur le fichier frontal
Le deuxième utilisateur n'accède plus à la table	table résidente : aucun effet	suppression du fichier ldb
Le deuxième utilisateur se déconnecte	suppression du fichier ldb	aucun effet

Dans de rares cas il arrive que le fichier **ldb** ne soit pas supprimé automatiquement par Microsoft ACCESS à la sortie du dernier utilisateur, dans ce cas vous pouvez le supprimer manuellement.

## Une application de lecture des informations du fichier Ldb par Argyronet.


## IV - Sécurité applicative

La sécurité applicative consiste à empêcher l'utilisateur de modifier les formulaires, les états, les macros et le code.

Il existe 3 méthodes de protection qui protègent plus ou moins l'application.

### IV-A - Méthode Compilation MDE

Pour sécuriser simplement et rapidement une interface l'un des moyens les plus utilisés est la "compilation" MDE. Il n'y a aucune connaissance technique à avoir puisque cela se fait à partir du menu de Microsoft ACCESS.

 *Notez que cette méthode est la plus simple, la plus rapide mais également la plus efficace.*

#### IV-A-1 - Contraintes


Il existe quelques contraintes à l'utilisation de cette méthode.

#### **Pour générer ce type de fichier il faut impérativement que**

- le code soit exempt de toute erreur de compilation même si le code contenant les erreurs n'est jamais exécuté ;
- Il ne faut pas que le code modifie les objets en mode création.

Un nouveau fichier "compilé" est créé à partir de l'ancien, ce dernier n'étant ni modifié, ni effacé.

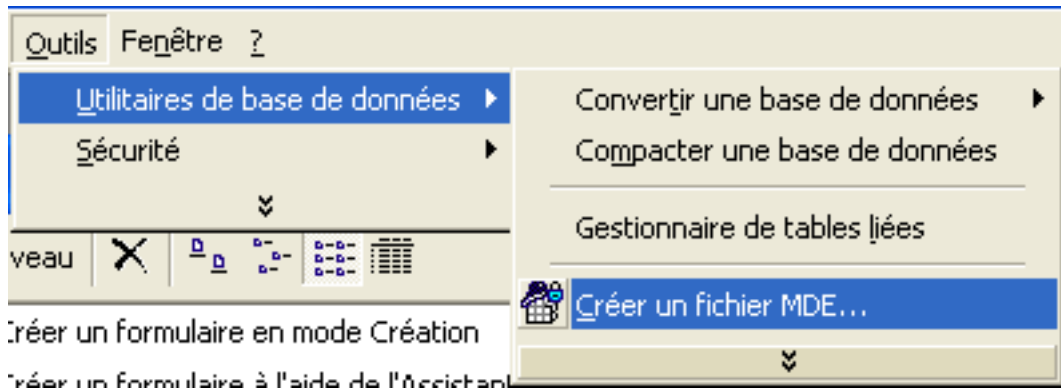
L'extension de ce nouveau fichier n'est plus **MDB** mais **MDE**.

 *Même si on le dit "compilé" ce fichier **n'est pas directement exécutable par le système**. Vous aurez toujours besoin de Microsoft ACCESS ou de son Runtime (livré sur le CD-ROM à partir de la version 2002 Professionnal) pour l'utiliser.*

#### IV-A-2 - Générer un fichier MDE

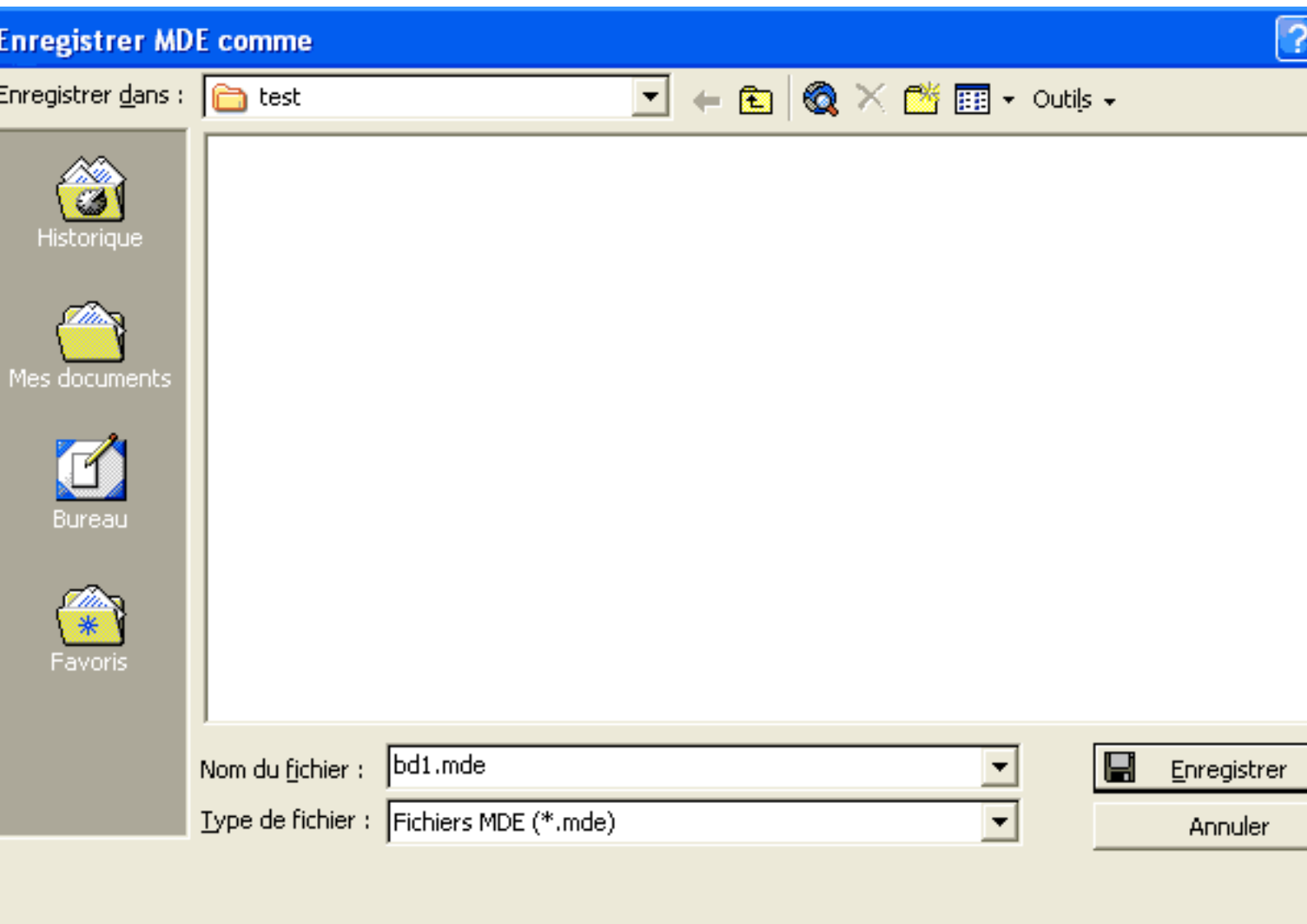
Pour générer un fichier MDE :

- 1 Commencez par ouvrir votre application.
- 2 Rendez-vous dans le menu **Outils** et choisissez le sous-menu **Utilitaires de base de données** et l'option **Créer un fichier MDE...**



Menu de création d'un MDE

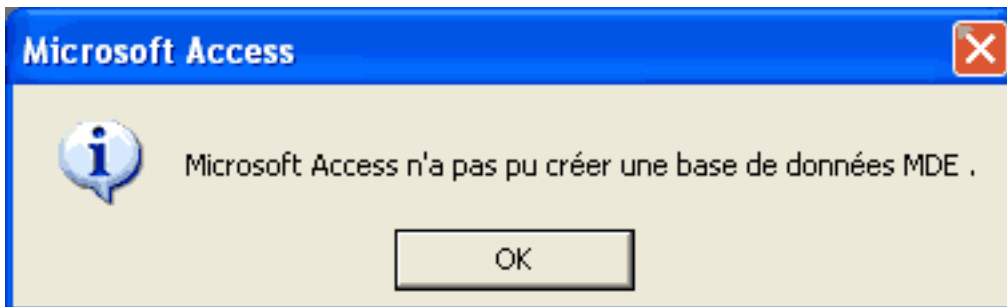
- 3 A l'ouverture de la fenêtre Enregistrer Fichier, donnez un nom au nouveau fichier (en principe le même que l'application d'origine)



La fenêtre d'enregistrement

#### 4 Cliquez sur **Enregistrer**


Si tout s'est bien passé vous n'aurez aucun message. Dans le cas contraire voici le message que vous verrez apparaître.




*Explicite ?*

Après que vous aurez validé le message en cliquant sur **Ok** le fichier d'origine se réouvre. Ce message est typique d'un code VBA posant problème.

Vous devez corriger l'erreur (ou les erreurs) avant de retenter la génération MDE.

 *Pour trouver l'erreur (ou les erreurs) ouvrez un module VBA (module ou formulaire) et compilez l'ensemble du code. Menu **Débugage** option **Compiler "nom du fichier"**. Corrigez les erreurs signalées et recommencez jusqu'à ce qu'il n'y en ait plus.*

 *Notez que pour un projet (fichier ADP) il y a également une version "compilée", l'extension de ce type de fichier est ADE.*

### IV-B - Méthode Mot de passe

Ce type de protection consiste à verrouiller l'accès à la base. Une fois le mot de passe fourni, l'application est non seulement utilisable mais également modifiable.

#### IV-B-1 - Mot de passe au démarrage

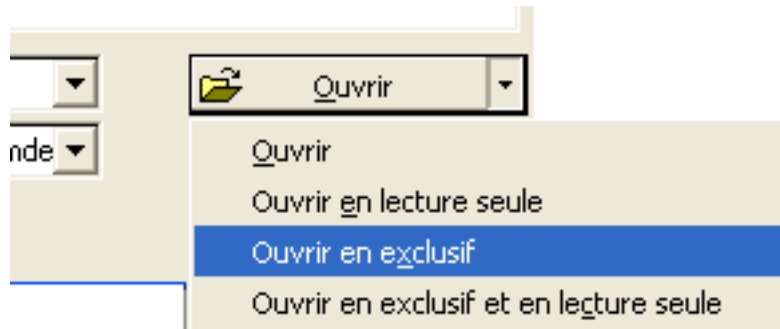
Le mot de passe au démarrage verrouille l'ensemble du fichier, il est impossible de lancer l'application sans celui-ci. Le mot de passe est demandé au démarrage de l'application. Une fois le mot de passe fourni, tous les objets sont modifiables.

Cette méthode n'est pas très utilisée sauf pour interdire l'accès d'une application mono-utilisateur.

##### IV-B-1-a - Mettre en place ce mot de passe

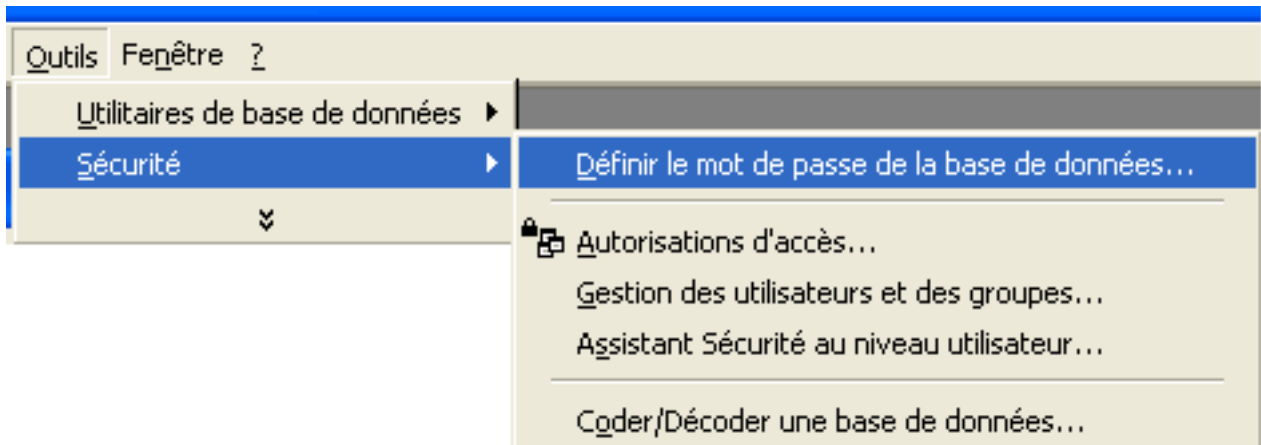
Pour mettre en place ce mot de passe :

- 1 Ouvrez l'application en mode exclusif,



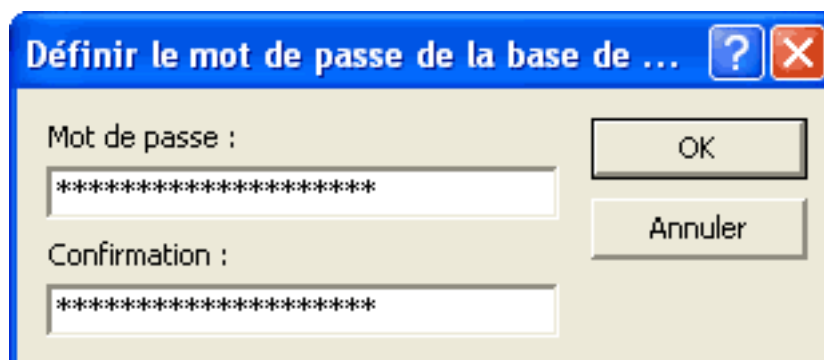
*Dans la fenêtre Ouvrir fichier*

- 2 Allez dans le menu **Outils** sous-menu **Sécurité**
- 3 Option **Définir le mot de passe pour la base de données.**



*Le menu Sécurité*

- 4 La fenêtre de définition du mot de passe apparaît. Entrez le mot de passe de votre choix. Il peut être composé d'un maximum de 20 caractères.

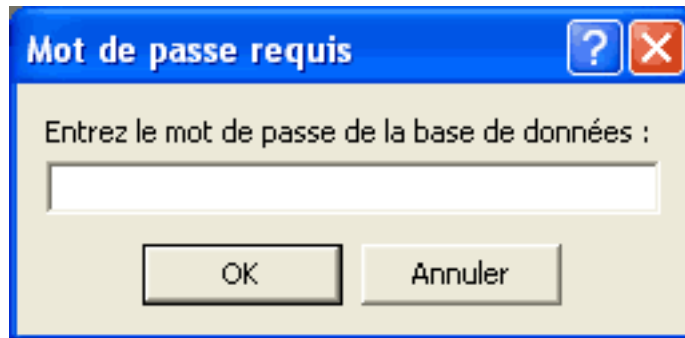


*2 fois le même !*

### IV-B-1-b - Retirer le mot de passe

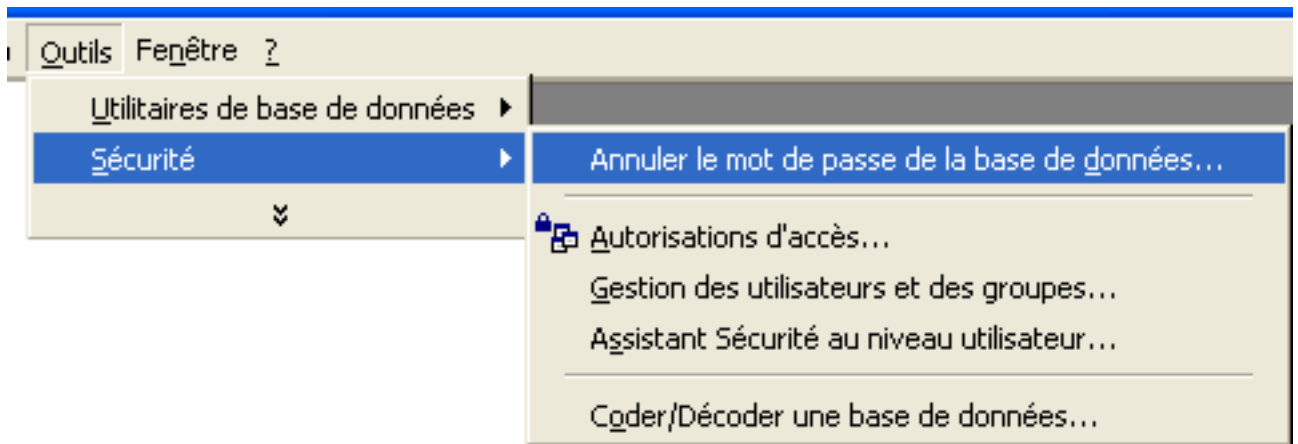
Pour enlever un mot de passe procédez de la même manière que pour le mettre :

- Ouvrez l'application en mode exclusif.



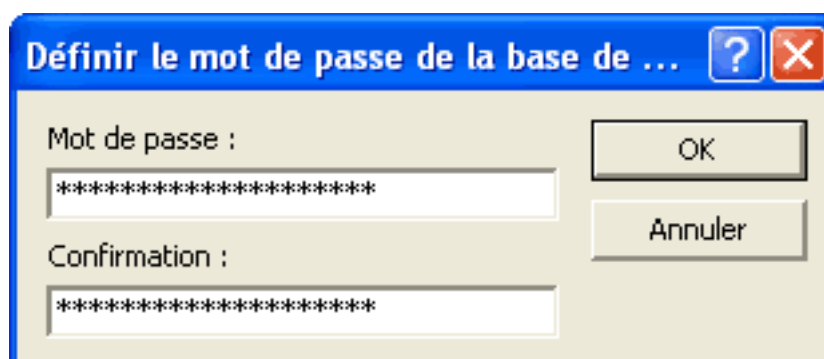
*Le mot de passe... mais le bon !*

- Allez dans le menu **Outils** sous-menu **Sécurité**
- Option **Définir le mot de passe pour la base de données.**



*Menu intelligent.*

- La fenêtre de définition du mot de passe apparaît. Entrez le mot de passe de votre choix. Il peut être composé d'un maximum de 20 caractères.



*2 fois le même !*

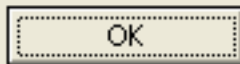
Voici le message qui apparaît lorsque vous tentez d'annuler un mot de passe sans avoir ouvert l'application en mode exclusif.

## Microsoft Access

**Vous devez ouvrir la base de données en mode exclusif pour définir ou annuler le mot de passe de la base de données.**



Pour ouvrir la base de données en mode exclusif, fermez la base de données et rouvrez-la en utilisant la commande Ouvrir dans le menu Fichier. Dans la boîte de dialogue Ouvrir, cliquez sur la flèche située à droite du bouton Ouvrir et choisissez Ouvrir en mode exclusif.



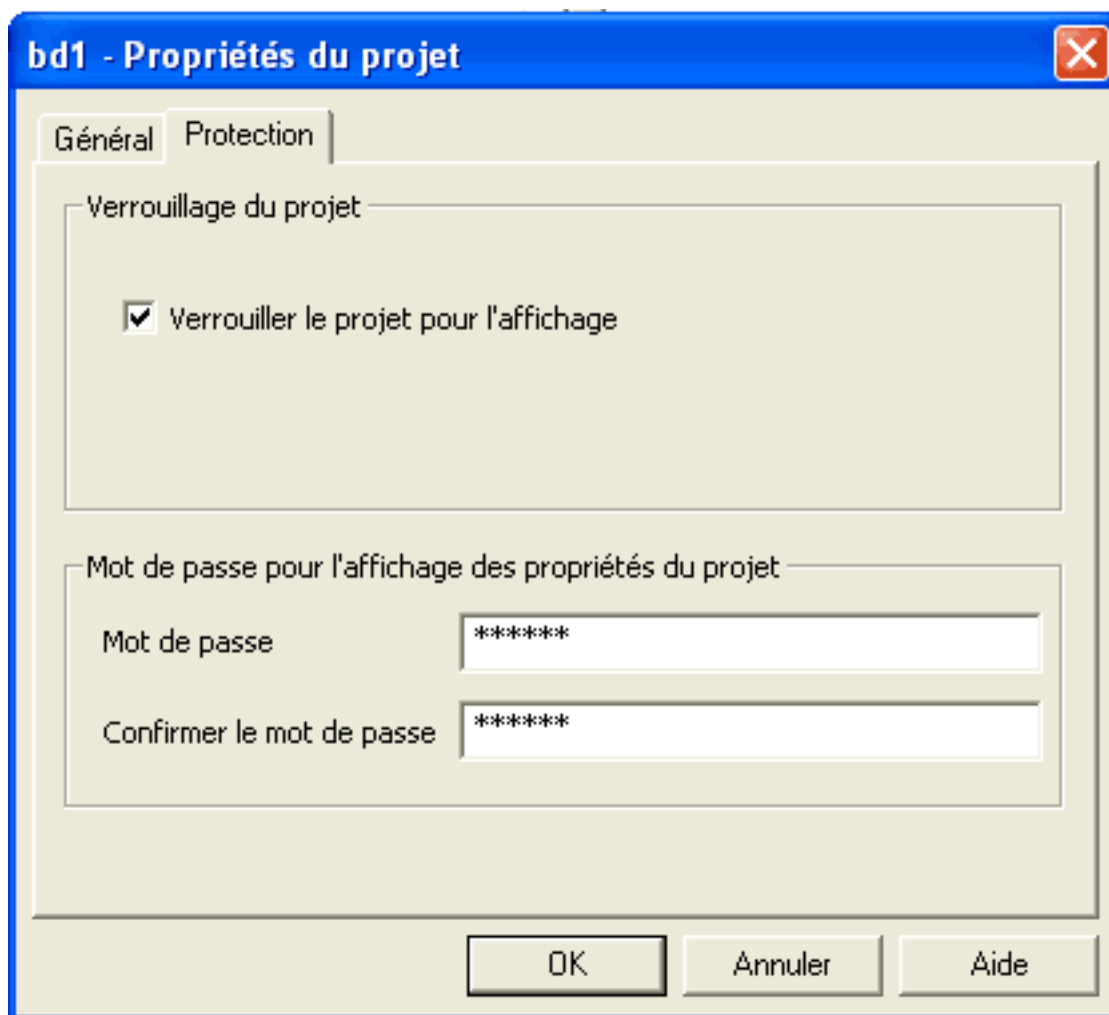
*Ce message est exclusif...*

### IV-C - Méthode Mot de passe sur le code

Cette protection interdit l'affichage, la modification et les propriétés du code contenu dans les modules, les formulaires ainsi que les états. Il ne protège pas les macros.

Pour mettre en place ce mot de passe :

- Ouvrez n'importe quel module (ou module de formulaire ou d'état)
- Ouvrez le menu **Outils, Propriétés "Nom de la base"**
- Cliquez sur l'onglet **Protection**




L'onglet de sécurité

- Cochez la case **Verrouillez le projet pour l'affichage**
- Entrez le mot de passe dans les 2 zones de texte.

Si la case n'est pas cochée l'utilisateur peut voir et modifier le code. Seules les propriétés de l'application sont protégées. Le mot de passe est demandé avant l'affichage du code.

Pour enlever le mot de passe décochez la case **Verrouillez le projet pour l'affichage** et videz les zones de texte contenant le mot de passe.

Cette méthode de protection est utile pour protéger uniquement le code et les propriétés, ce qui en fait une protection plutôt faible. En effet l'utilisateur a accès à tout le reste de l'application. Elle peut venir en complément de la protection par **Sécurité utilisateur** que nous allons aborder dans le prochain chapitre.

 *Aucun mot de passe n'est inviolable et il existe de nombreux produits shareware ou freeware pour retrouver les mots de passe des fichiers Office. Mon conseil est d'éviter la protection à partir d'un mot de passe sauf si vous y êtes contraint.*

## V - Bases de la Sécurité utilisateur

A partir de ce chapitre nous allons traiter de la protection par droit d'accès. Celle-ci ne s'improvise pas (comme les méthodes vu précédemment) et met en oeuvre des concepts de groupes, d'utilisateurs, de droits, et d'héritage. De plus une bonne étude du fonctionnement de l'application et des tâches des utilisateurs sont obligatoires.

### V-A - Théorie

Si vous êtes un habitué de la gestion des utilisateurs avec Windows vous pouvez directement passer à la mise en oeuvre sinon lisez ce qui suit.

Pour bien comprendre cette méthode il est nécessaire d'en expliquer le fonctionnement.

Chaque utilisateur effectue des tâches bien précises dans l'application. Dans l'exemple d'une société, un commercial n'aura pas accès aux mêmes informations de l'entreprise qu'un acheteur ou qu'un magasinier. Ils font tous partis du même *groupe de travail* puisqu'ils utilisent la même application à des niveaux différents.

Comme il n'y a pas qu'un seul **utilisateur** acheteur, commercial ou magasinier il est nécessaire de pouvoir créer des **groupes d'utilisateurs** ayant les mêmes accès.

Ces accès sont appelés **droits**. Ils déterminent qui peut faire quoi dans l'application.

### V-B - Définition et organisation des groupes, utilisateurs, droits...



### *Organisation*

Voici le schéma d'organisation de la sécurité Microsoft ACCESS.

#### V-B-1 - Groupe de travail

Le **groupe de travail** est l'entité la plus haute dans l'organisation, elle contient les **groupes d'utilisateurs**.

- 1 Elle peut être utilisée par une ou plusieurs applications.
- 2 On ne peut utiliser plusieurs groupes de travail pour une seule application.
- 3 On peut changer de groupe de travail automatiquement ou manuellement.

#### V-B-2 - Groupe d'utilisateurs

Le **groupe d'utilisateurs** est contenu dans le **groupe de travail**, il contient des **utilisateurs**.

- 1 Le groupe possède des droits
- 2 Il y a plusieurs groupes d'utilisateurs dans un groupe de travail.
- 3 Les groupes d'utilisateur natifs Administrateurs, Utilisateurs qui ne peuvent être effacés.

#### V-B-3 - Compte d'utilisateur

Le compte d'utilisateur permet l'identification unique de l'utilisateur. Il est doté d'un nom, d'un mot de passe et éventuellement de droits.

- Il est obligatoirement inscrit dans le groupe **Utilisateurs**.
- Il peut être inscrit dans plusieurs groupes.
- Il hérite des droits de chaque groupe dans lequel il est inscrit.
- Les utilisateurs natifs **Administrateur**, **Utilisateur** et **Engine** ne peuvent être supprimés.

## V-B-4 - Droits


Il s'agit de l'ultime définition. Les droits autorisent ou interdisent les actions sur les objets de la base (tables, requêtes...). Ils peuvent être définis au niveau du groupe d'utilisateurs ou du compte d'utilisateur. Ils sont définis sur chaque objet de l'application.


## V-B-5 - Objets

Vous connaissez déjà les objets puisqu'ils composent une application Access.

### Liste des objets

- Base de données
- Tables
- Requêtes
- Formulaires
- Etats
- Macro

 *Remarquez que les **Modules** et les **Pages** ne figurent pas dans la liste des objets pouvant être sécurisés. Un nouvel objet fait par contre son apparition, il s'agit de la **Base de données**.*

 *Pour les **Modules** et dans le cas où vous ne pouvez pas mettre en place la protection par compilation vous pouvez vous servir de la protection par mot de passe sur le code.*

## V-B-6 - Héritage

L'héritage est la notion pivot de la sécurité. Lorsqu'un utilisateur est inscrit dans un groupe, il hérite automatiquement des droits de ce groupe.

Un exemple très simple permet de bien comprendre ce concept.

- Le groupe 1 a le droit de supprimer les données,
- Le groupe 2 a le droit de modifier les données,
- L'utilisateur A a le droit d'ajouter des données.

Si vous inscrivez l'utilisateur A dans le groupe 1 :

Il pourra supprimer des données (héritage du groupe 1) et en ajouter (ses propres droits).

Vous l'inscrivez dans le groupe 1 et 2 :


Il pourra supprimer, modifier des données (héritage du groupe 1 et 2) et en ajouter (ses propres droits).

- L'utilisateur hérite des droits du (ou des) groupe(s) dans lequel il est inscrit.
- Ces propres droits sont prioritaires sur ceux du groupe.
- Les droits déclarés pour un utilisateur n'est valide que pour lui.
- Un utilisateur cumule les droits de tous les groupes dans lesquels il est inscrit en plus des siens.
- En aucun cas un utilisateur étant inscrit dans le même groupe qu'un autre utilisateur bénéficiera des droits de ce dernier.
- Seul le droit d'**Administrer** ne peut être hérité il est toujours lié à un compte d'utilisateur.

## V-B-7 - Propriétaire

Voici une définition particulière liée uniquement à l'objet. Il s'agit du propriétaire de l'objet.

- Il ne peut y avoir qu'un propriétaire par objet.
- Il peut y avoir plusieurs propriétaires d'objets dans une application.
- Seul le propriétaire **Engine** ne peut être changé. Il régit tous les objets systèmes d'un fichier Microsoft Access.

 *Cette propriété n'empêche pas un administrateur d'opérer des modifications sur un objet dont il n'est pas propriétaire.*

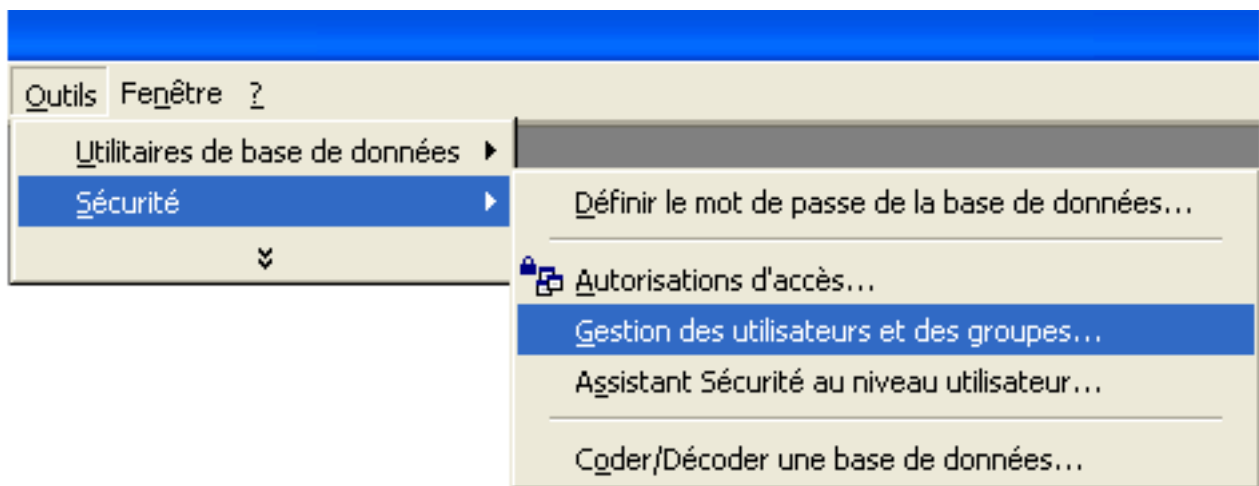
## VI - Groupe de travail

Dans ce chapitre nous allons mettre en application les concepts théoriques du chapitre précédent.

### VI-A - Démonstration

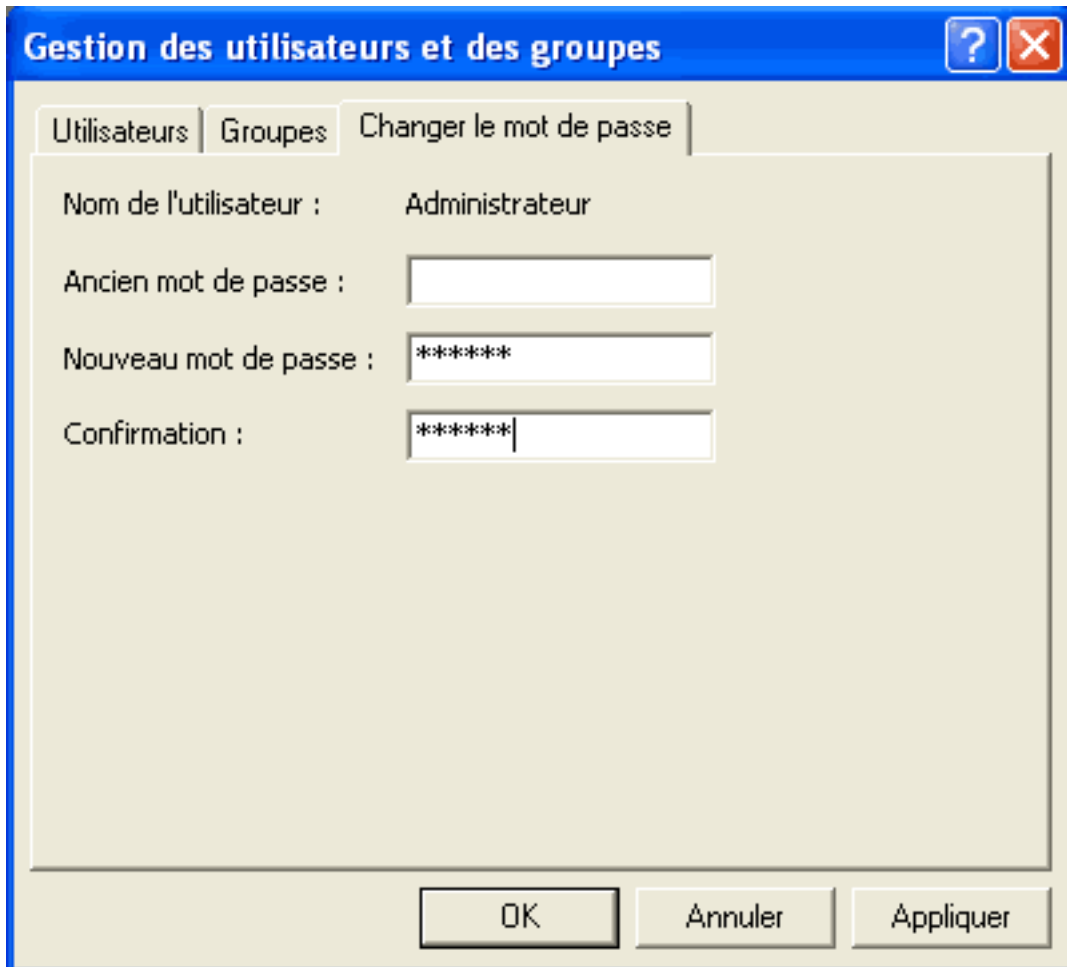
Le groupe de travail est toujours présent dans une application même s'il est momentanément transparent pour l'utilisateur. Nous allons en apporter la preuve :

- Ouvrez une application
- Allez dans le menu **Outils / Sécurité / Gestion des utilisateurs et des groupes...**



*Menu sécurité*

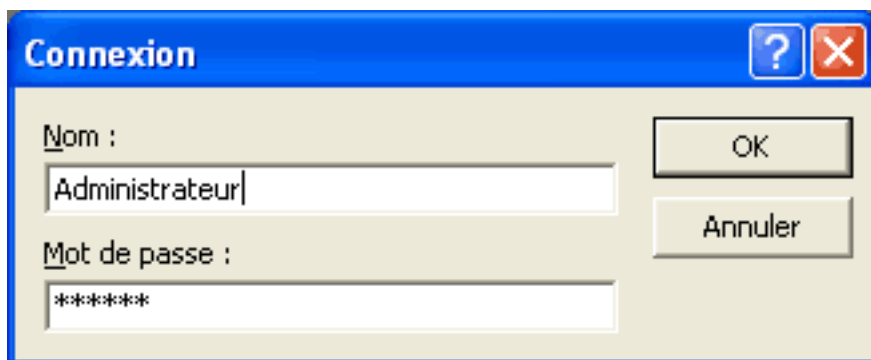
- Cliquez sur l'onglet **Changer le Mot de passe**
- Saisissez un mot de passe dans les zones de texte **Nouveau** et **Confirmation**




*Dans le vif du sujet*

- Confirmez en cliquant sur **Ok** ou **Confirmer** et **Ok**
- Fermez Access puis réouvrez une application.

**Attention !!** Sur les systèmes Windows XP le nom d'utilisateur dans la fenêtre de connexion est le nom du compte de connexion Windows. Ceci est pratique en exploitation, mais ici il faut mettre **Administrateur** car c'est le compte par défaut.



*CQFD !*

 Une fois connecté et tant que vous ne fermez pas Microsoft Access vous restez avec le compte de connexion et le groupe de travail précédent.

Remettez le mot de passe à blanc :

- Allez dans le menu **Outils / Sécurité /Gestion des utilisateurs et des groupes...**
- Cliquez sur l'onglet **Changer le Mot de passe**
- Entrez le mot de passe dans **Ancien mot de passe** n'entrez rien dans les autres zones de texte
- Confirmez en cliquant sur **Ok** ou **Confirmer** et **Ok**
- Fermez Access puis réouvrez une application.

 Notez que cette manipulation permet également de changer le mot de passe.

Ces manipulations sont identiques pour initialiser, supprimer ou changer le mot de passe de n'importe quel utilisateur déclaré.


Après ces quelques manipulations simples nous allons créer un nouveau groupe de travail.

## VI-B - Création d'un groupe de travail

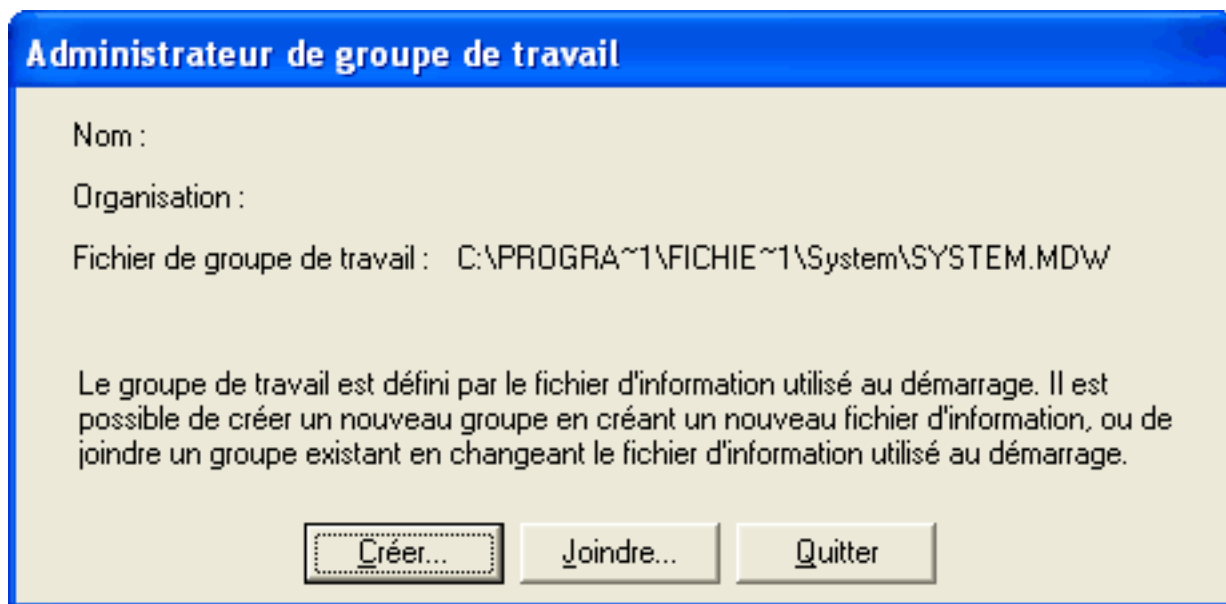
Pour une protection optimale il est obligatoire de créer un nouveau groupe de travail. Dans le cas contraire n'importe quel utilisateur utilisant le groupe de travail pas défaut est en mesure d'accéder à la sécurité utilisateur.

Il existe une différence d'appel du gestionnaire de groupe de travail entre les versions antérieure à la 2002 (XP) qui est présentée dans le tableau ci-dessous.

Pour les versions Access 2000 et antérieures	Access 2002 (XP) et 2003
Recherchez le programme <b>WRKGADM.EXE</b>  (dans le répertoire <b>Microsoft Office</b> pour la version 2000  (dans le répertoire <b>Windows/system32</b> pour les versions 97 et antérieures)  Double-cliquez sur l'icône	Allez dans le menu <b>Outils / Sécurité / Gestionnaire des groupes de travail</b>

 Pour l'instant le format 2007 ne supporte pas cette sécurité.

Dans la fenêtre du gestionnaire de groupe de travail vous pouvez lire plusieurs informations importantes.




Gestionnaire de groupe de travail

Si vous utilisez le groupe standard les informations **Nom** et **Organisation** apparaissent vides.

L'information **Fichier de groupe de travail** indique le fichier qui est utilisé pour le groupe de travail courant.

Vous pouvez remarquer que ce fichier s'appelle **SYSTEM.MDW**.

 *Avant d'effectuer les manipulations suivantes veillez à faire une sauvegarde du fichier de sécurité actif. C'est celui indiqué dans **Fichier Groupe de travail**. En cas de problème vous pouvez le récupérer sur votre CD-Rom d'installation d'Office ou de Microsoft ACCESS.*

 *Notez que le fichier **SYSTEM.MDW** original est strictement identique pour toutes les licences Microsoft Access. Si vous l'ouvrez vous constaterez qu'il ne contient que des tables.*

- Cliquez sur le bouton **Créer...** pour créer un nouveau fichier de groupe de travail (extension Mdw).
- La fenêtre suivante s'affiche.

**Information du propriétaire de groupe de travail**

Le nouveau fichier d'information de groupe de travail est identifié par le nom, l'organisation, et l'identificateur de groupe de travail (respect de la casse) spécifiés.

Utilisez le nom et l'organisation proposés ci-dessous, ou tapez un nom et une organisation différentes. Pour vous assurer que votre groupe de travail est unique, tapez également un identificateur de groupe de travail unique de 20 chiffres/lettres.

Nom : mongroupedetravail

Organisation : masociété


Identificateur de groupe de travail : 12345678901234567890

OK Annuler

*Paramètres du nouveau groupe*

- Entrez le nom du groupe de travail dans la zone **Nom**. En principe un nom explicite désignant soit l'application, soit un groupe d'utilisateurs d'applications (nom d'un service...).
- Entrez le nom de votre société dans la zone **Organisation**.
- **Identificateur de groupe de travail** est un numéro unique servant de clef de unique. Vous pouvez entrer jusqu'à 20 caractères alpha-numériques.
- Validez les paramètres en cliquant sur **Ok**.

L'ensemble de ces informations constitue une protection contre la création d'un nouveau fichier mdw.

 *Enregistrez ces informations pour qu'en cas de problème vous puissiez le recréer. En effet dans le cas où après avoir sécurisé une application vous perdiez le fichier MDW correspondant il ne vous sera plus possible d'accéder l'application.*

**Fichier d'information de groupe de travail**

Utilisez le chemin et le nom ci-dessous, ou entrez un chemin et un nom différents pour le nouveau fichier d'information de groupe de travail.

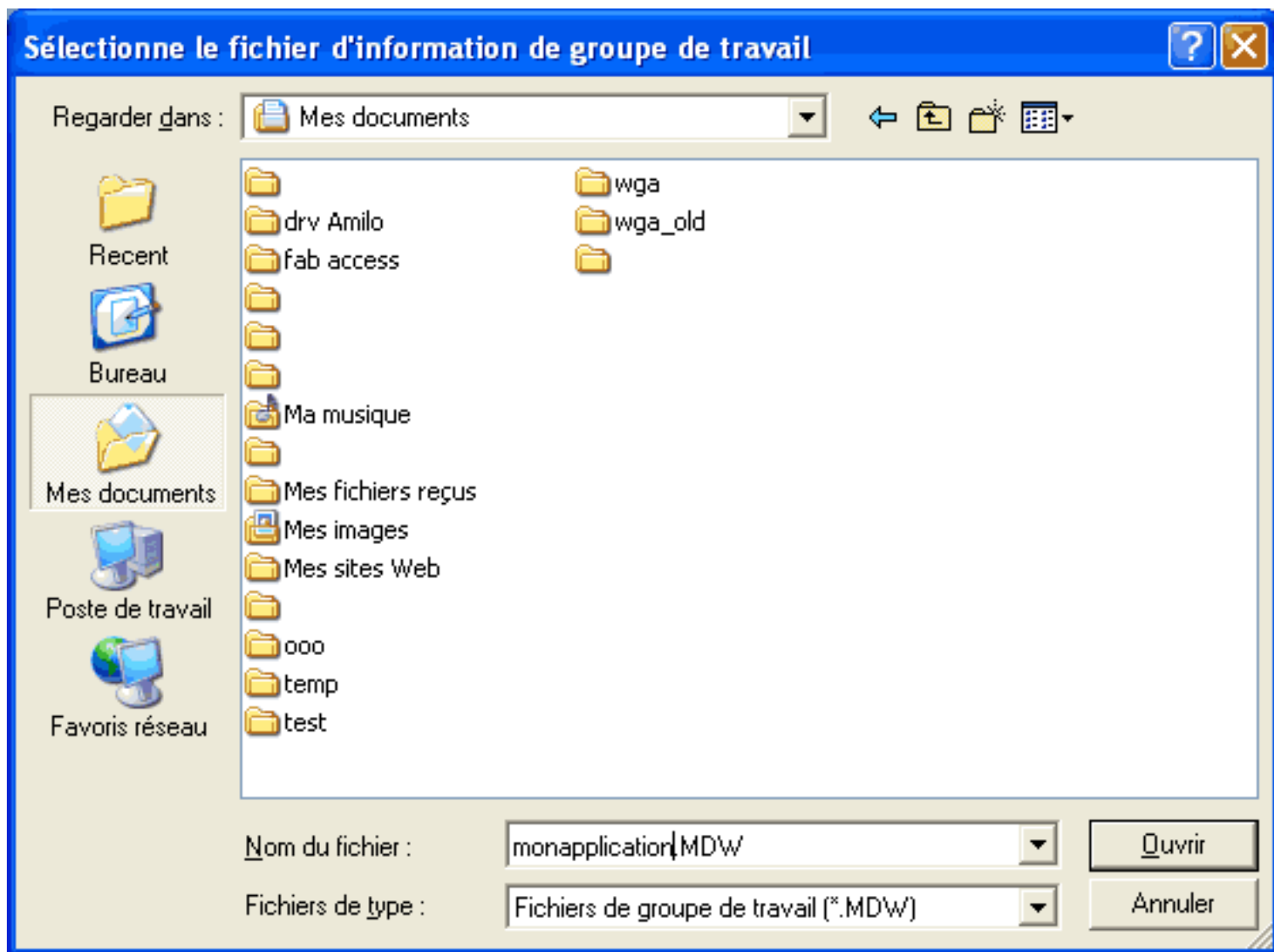
Base de données : A~1\FICHIE~1\SYSTEM\SYSTEM.MDW Parcourir...

OK Annuler

*Chemin pour le fichier*


- 1 Indiquez le chemin et le nom d'un fichier mdw
- 2 Utilisez le bouton **Parcourir** pour placer le fichier où vous le souhaitez.

Je vous conseille un nom explicite, soit le nom de l'application auquel il est destiné, soit un nom plus générique dans le cas d'applications multiples. Toujours différent de **system.mdw** pour éviter toute confusion.

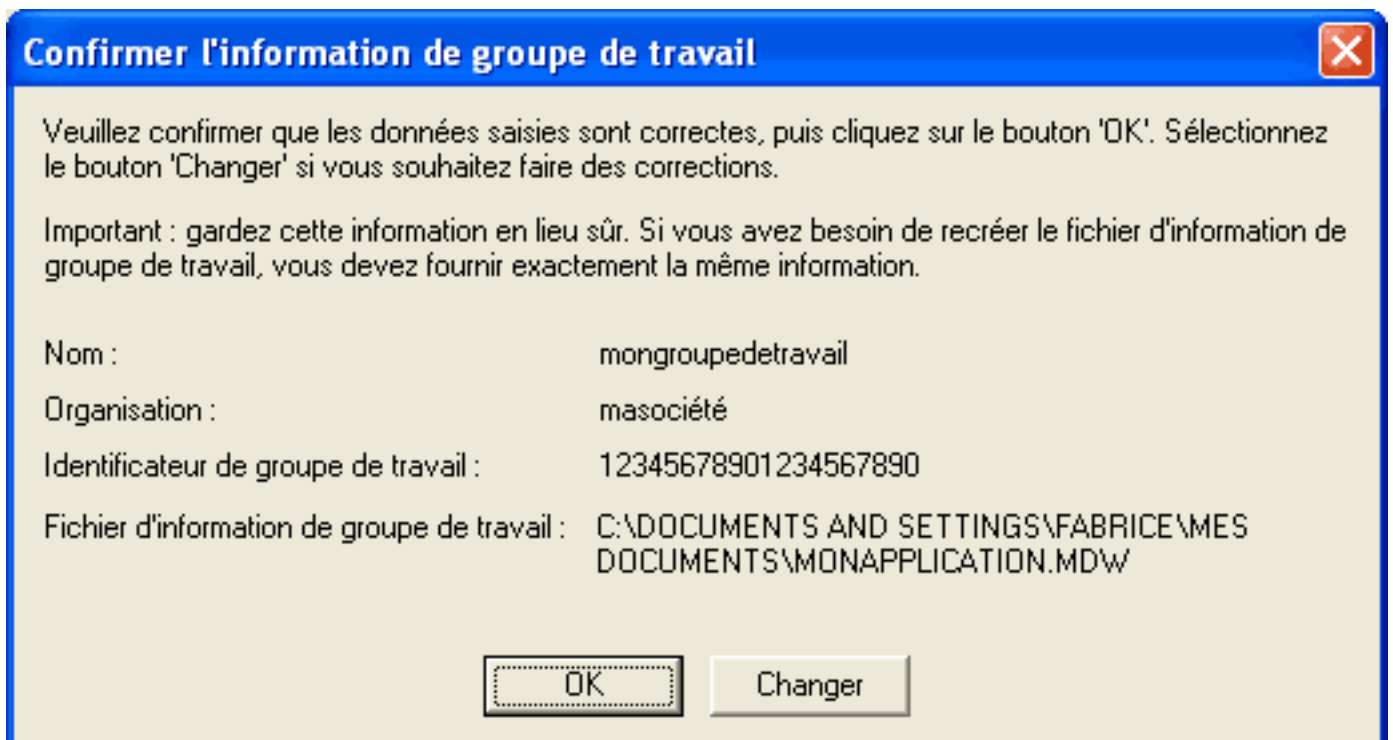


Le nom et l'emplacement

Je ne pense pas que vous ayez besoin d'explication pour le fonctionnement de cette fenêtre.

 *Il est conseillé de placer le fichier de sécurité dans le même répertoire que l'application. Cela évite de l'égarer sur vos disques et de ne plus savoir quel fichier va avec quelle(s) application(s).*

- 1 Une fenêtre rappelant les informations apparaît.
- 2 Cliquez sur le bouton **Ok** pour confirmer ou **Changer** pour revenir à la fenêtre précédente pour faire des modifications.



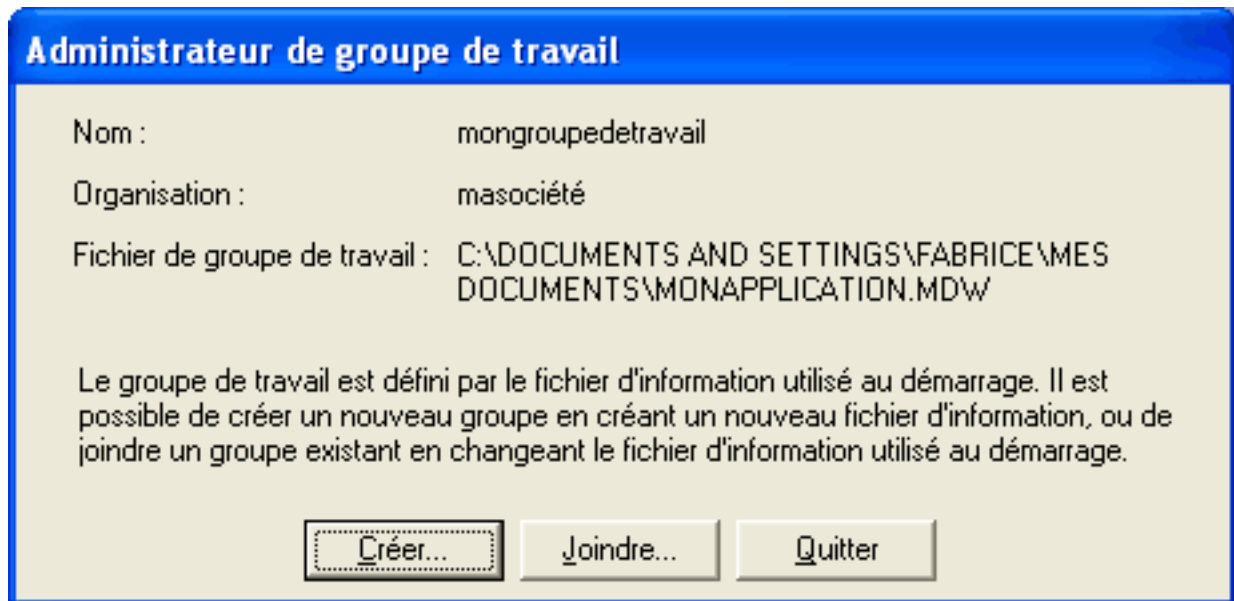
*Nouveau groupe en cours de création*

- 3 Enfin une fenêtre apparaît confirmant la création du fichier de sécurité. Cliquez sur **Ok**



*Confirmation*

Voici l'ultime phase de la création du fichier, vous venez de retourner sur le premier écran. Vous pouvez constater que le nouveau fichier est devenu actif.



*Enfin ! c'est fait...*

Pour activer un autre fichier de sécurité, l'original par exemple :

- 1 Cliquez sur le bouton **Joindre...** et suivez les instructions.
- 2 Sinon le bouton **Quitter** vous permet de fermer cette fenêtre.
- 3 Fermer la fenêtre.


Cette manipulation ne constitue aucun problème en soit, mais il faut bien la maîtriser car vous serez amené à l'utiliser souvent.

## VII - Groupes d'utilisateurs

En règle générale il est préférable d'attribuer des droits aux groupes et non aux utilisateurs, sauf pour les comptes d'**administration/développeur**. La raison en est simple, lorsque vous définissez des droits sur des groupes il suffit d'ajouter l'utilisateur aux différents groupes souhaités pour qu'il hérite immédiatement des droits. Si vous vous amusez à définir les droits directement sur les comptes utilisateurs vous devrez faire la même définition autant de fois qu'il y a d'utilisateurs avec les risques d'erreurs que cela comporte.

### VII-A - Définition des groupes d'utilisateurs

Pour définir les groupes d'utilisateurs il faut d'abord définir une stratégie d'utilisation de l'application. Le mieux est d'organiser tout cela sous forme de tableau.


 *Je fais ce tableau sur **Microsoft Excel**, cela me permet de faire facilement des modifications. Une fois le tableau préparé j'ai une vue synthétique de du travail à faire.*

Voici l'exemple d'un tableau réalisé. Notez que n'importe quel tableur ou logiciel permettant de faire des tableaux fait l'affaire. A défaut une simple feuille de papier, une règle, un crayon et une gomme peuvent convenir.

L=Lecture / A=Ajout / M= Modification / S = Suppression

Tables		Client				Commande				Tarif				Stock			
		L	A	M	S	L	A	M	S	L	A	M	S	L	A	M	S
Groupes	Commerciaux	0	0	0		0	0	0	0	0				0			
	Acheteurs					0		0		0	0	0	0	0			
	Magasin	0				0		0						0	0	0	0
	Comptabilité	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

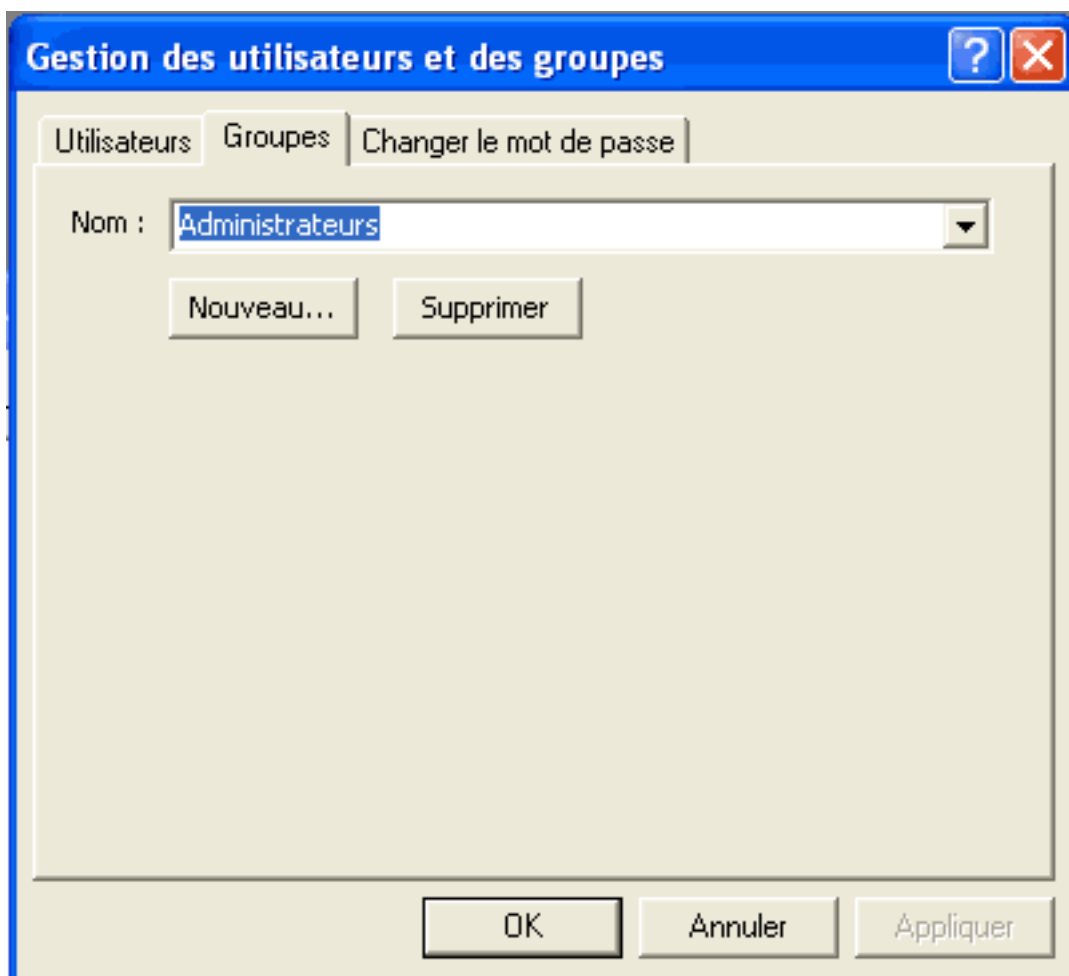
*Tableau des droits*

 *Vous pouvez remarquer que les groupes d'administration ne sont pas représentés dans ce tableau. C'est normal car il s'agit d'un groupe ayant tout pouvoir il est donc inutile de faire une analyse.*

### VII-B - Création de groupes

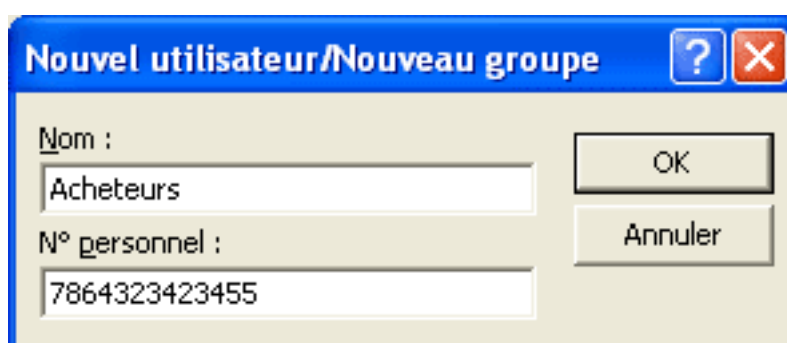
Nous allons créer les groupes nécessaires.

- Ouvrez la base si ce n'est pas déjà fait.
- Allez dans le menu **Outils/sécurité/Gestion des utilisateurs et des groupes**
- Cliquez sur l'onglet **Groupes**



Gestion des groupes

- Puis sur le bouton **Nouveau...**



Nom et PID


- Indiquez le Nom du Groupe et le Numéro d'Identification unique ou PID Personnel ID.
- Recommencez l'opération autant de fois qu'il y a de groupes.

**⚠ Attention le numéro d'identification (PID) est très important, il ne faut pas mettre le même numéro pour tous les groupes et/ou utilisateurs.**

## VII-C - Suppression de groupes

La suppression se fait dans la même fenêtre que la création.

- Sélectionnez le groupe que vous souhaitez supprimer.
- Cliquez sur le bouton **Supprimer**

 *La suppression d'un groupe n'entraîne pas la suppression des utilisateurs qui y sont inscrits, seuls leurs droits seront perdus.*

 *Les groupes natifs (Administrateurs et Utilisateurs) ne peuvent pas être supprimés.*

## VIII - Droits d'accès

### VIII-A - Droits et dépendances

Certains droits en impliquent d'autres, dans le tableau suivant nous dressons l'inventaire exhaustif pour les tables.

Droit choisi	Droit(s) lié(s)
<b>Lire la structure</b>	aucun
<b>Modifier la structure</b>	Lire la structure,  Modifier les données,  Supprimer des données
<b>Lire les données</b>	Lire la structure
<b>Modifier les données</b>	Lire les données,  Lire la structure
<b>Ajouter des données</b>	Lire les données,  Lire la structure
<b>Supprimer des données</b>	Lire les données,  Lire la structure
<b>Administrer</b>	Lire la structure,  Modifier la structure,  Lire les données  Modifier les données,  Ajouter des données,  Supprimer des données

Certains droits en impliquent d'autres, dans le tableau suivant nous dressons l'inventaire exhaustif pour les autres objets (formulaires, macros et états).

Droit choisi	Droit(s) lié(s)
<b>Ouvrir/Exécuter</b>	Aucun
<b>Lire la structure</b>	Aucun.
<b>Modifier la structure</b>	Lire la structure.
<b>Administrer</b>	Ouvrir/Exécuter,  Modifier la structure,  Lire la structure,  Modifier la structure.

## VIII-B - Groupes des utilisateurs

D'après le tableau des droits que nous avons défini précédemment nous allons définir les droits pour chacun des groupes d'utilisateurs.

- Allez dans le menu **Outils/Sécurité/Autorisations d'accès**
- Cliquez sur le bouton d'option **Groupes**
- Les groupes définis apparaissent dans la liste déroulante.
- Sélectionnez le groupe **Commerciaux**.
- Sélectionnez la table **Client**
- Sélectionnez les droits **Lire** les données, **Ajouter** les données et **Modifier** les données
- Cliquez sur **Appliquer** pour enregistrer la modification.
- Sélectionnez la table **Commande**
- Sélectionnez les droits **Lire** les données, **Ajouter** les données, **Modifier** les données et Supprimer les données
- Cliquez sur **Appliquer** pour enregistrer la modification.
- Sélectionnez la table **Tarif**
- Sélectionnez les droits **Lire** les données
- Cliquez sur **Appliquer** pour enregistrer la modification.
- Sélectionnez la table **Stock**
- Sélectionnez les droits **Lire** les données
- Cliquez sur **Appliquer** pour enregistrer la modification.

Nous venons de définir les droits du groupe Commerciaux pour les tables. Recommencez l'opération pour Acheteurs, Magasiniers, Comptabilité.

## IX - Les comptes utilisateurs

### IX-A - Création des comptes

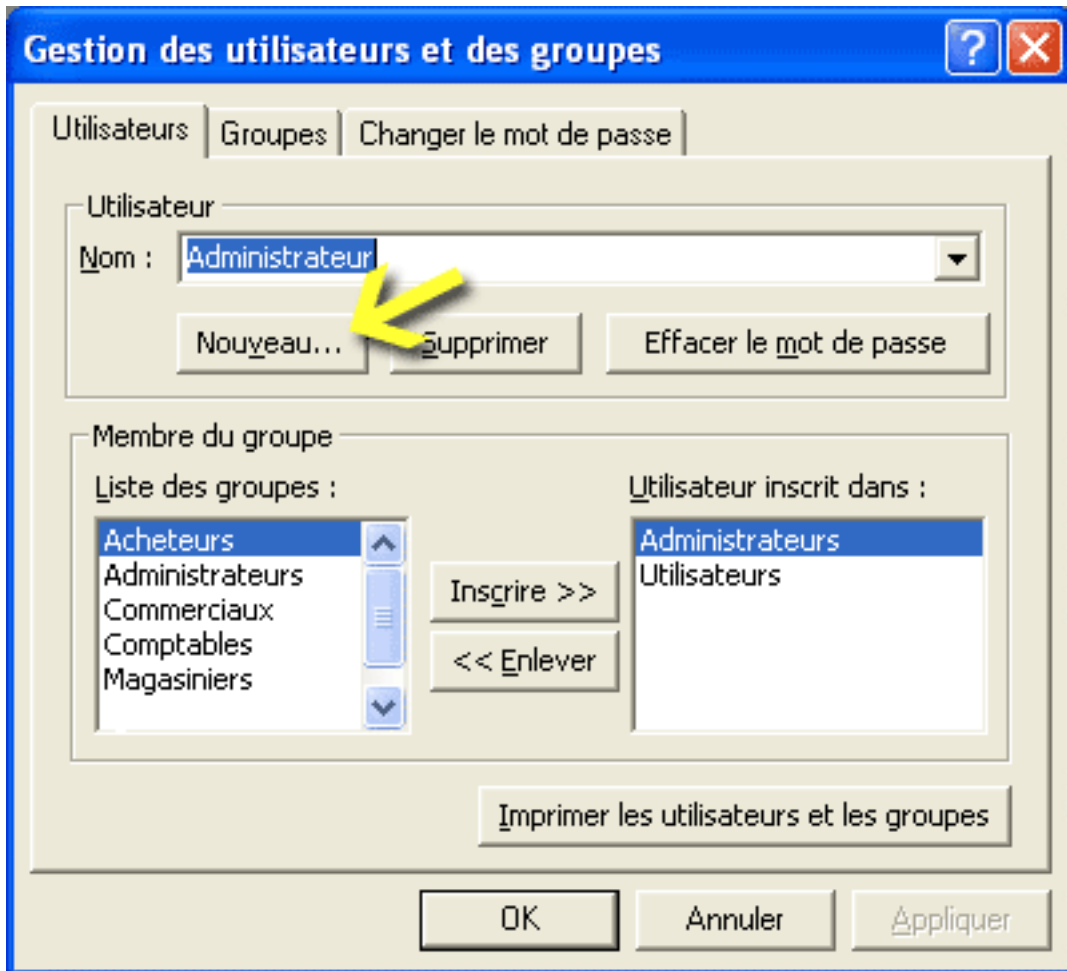
La procédure de création des comptes utilisateurs est très semblable à celle de la création des groupes.

Il y a un utilisateur qui doit être créé avant tous les autres. Il s'agit de l'utilisateur qui va remplacer le compte d'administration natif. Cet utilisateur aura tous les droits sur tous les objets de la base. Ces tâches seront :

- Créer des groupes ou des utilisateurs,
- Supprimer des utilisateurs,
- Réinitialiser des mots de passe utilisateurs,
- Modifier les droits des groupes,
- Affecter les utilisateurs dans les groupes,
- Faire les opérations de maintenance sur la base.
- Créer, modifier, supprimer tout objet de la base.

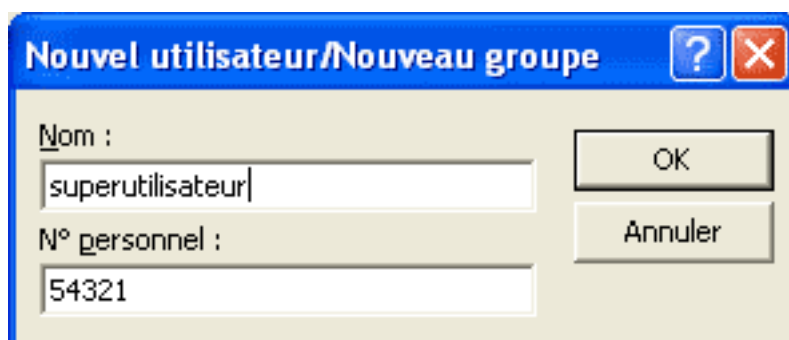
Pour le créer suivez les instructions suivantes :

- Allez dans le menu **Outils/sécurité/Gestion des utilisateurs et des groupes**
- Cliquez sur l'onglet **Utilisateurs**



Créer un compte d'utilisateur

- Puis sur le bouton **Nouveau...**



Un air de déjà vu...

- Indiquez comme nom **superutilisateur** et un Numéro d'Identification unique ou PID Personnel ID.
- Recommencez l'opération pour les autres comptes d'utilisateurs.

**⚠** Comme pour les groupes n'oubliez pas de bien noter chaque N° PID pour permettre leur création.

## IX-A-1 - Définir les mots de passe des comptes

Pour qu'un compte soit sécurisé il faut définir un mot de passe, sans quoi n'importe qui pourrait se connecter à l'application s'il connaît le nom d'un utilisateur. Nous verrons cette manipulation plus loin dans ce tutoriel.

## IX-B - Affectation des comptes

A l'exception des comptes d'administration il est inutile de définir les droits pour chaque utilisateur, il faut simplement les affecter aux groupes correspondants.

- Allez dans le menu **Outils/sécurité/Gestion des utilisateurs et des groupes**
- Déroulez la liste **Utilisateurs** pour choisir **superutilisateur**
- Dans la liste Groupe sélectionnez le groupe **Administrateurs**
- Cliquez sur le bouton **Inscrire**
- Recommencez l'opération pour les autres comptes d'utilisateurs dans leur(s) groupe(s) respectif(s).
- Lorsque vous avez terminé cliquez sur **Ok**

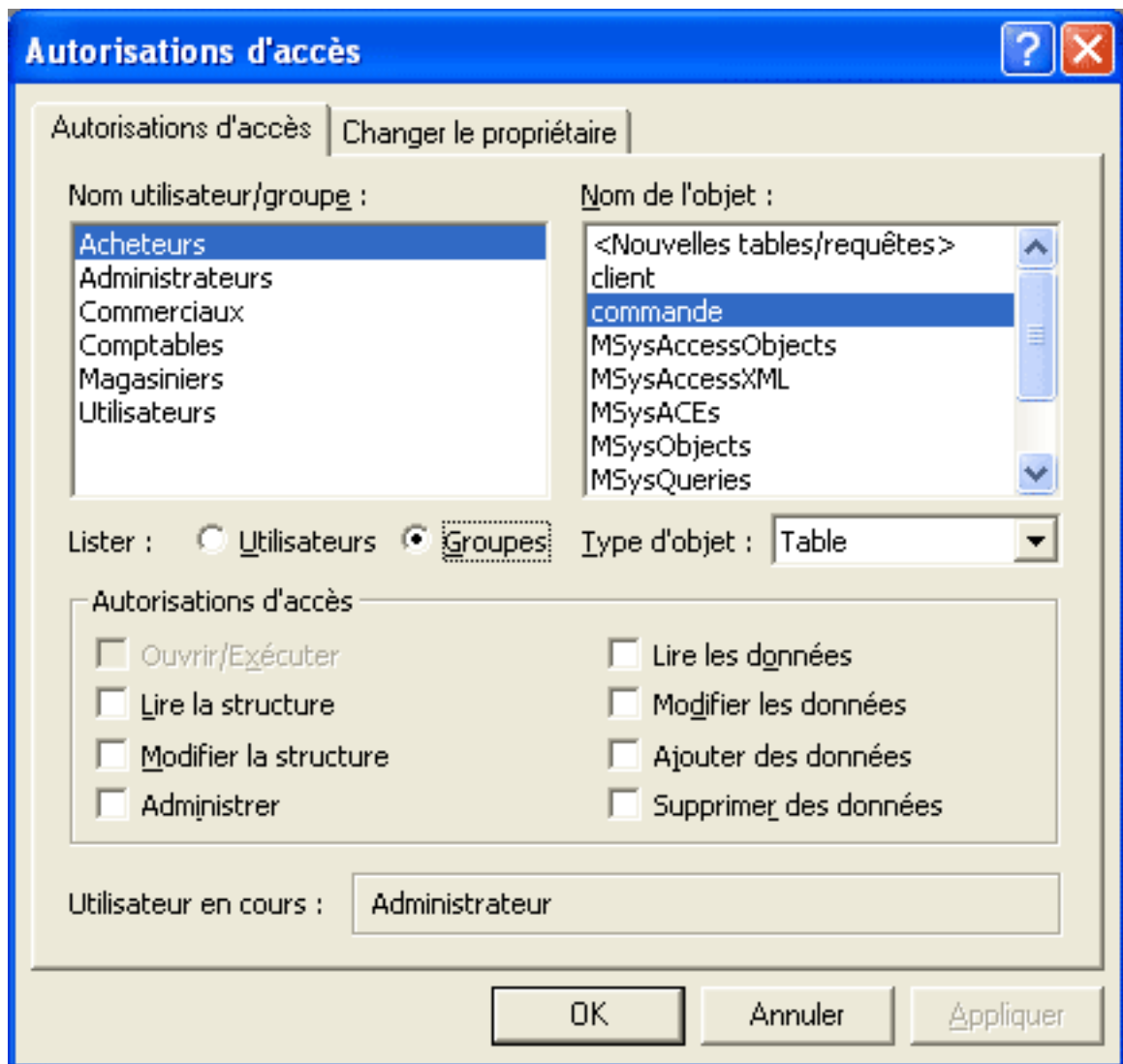
 *Vous pouvez remarquer que tous les utilisateurs sont inscrits dans le groupe **Utilisateurs**. C'est tout à fait normal, le groupe **Utilisateurs** est un groupe natif, tous les comptes utilisateurs en font partie. Comme le groupe **Administrateurs** il ne peut être supprimé et on ne peut désinscrire ses membres.*

Vous pouvez inscrire un utilisateur dans plusieurs groupes. Ceci aura pour effet de combiner les droits des groupes.

## IX-C - L'administrateur un cas particulier

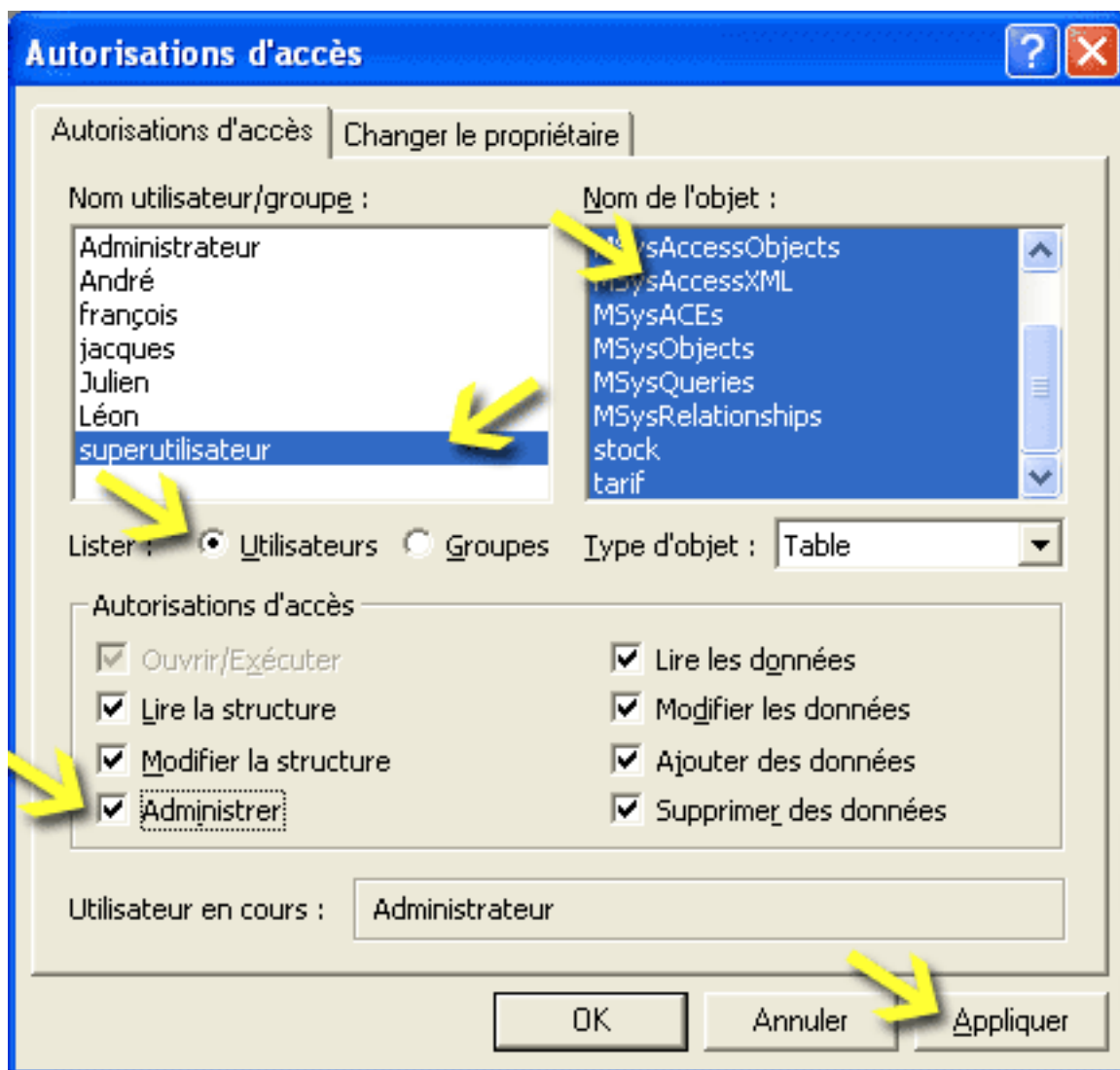
Nous allons d'abord définir les droits pour l'administrateur. Comme nous l'avons déjà vu il s'agit d'un cas particulier car le droit d'**Administrer** n'est pas soumis à l'héritage.

- Allez dans le menu **Outils/Sécurité/Autorisations d'accès**
- Cliquez sur le bouton d'option **Utilisateurs**



*Le coeur est ici.*

- Les utilisateurs définis apparaissent dans la liste déroulante.
- Sélectionnez l'utilisateur *superutilisateur*
- Sélectionnez l'intégralité des tables (Shift + Clic)



Définition des droits du groupe

- Cliquez sur **Administrer**.
  - Lorsque vous sélectionnez **Administrer** tous les droits se sélectionnent.
- Pour les objets suivants les droits sont légèrement différents mais il faut tous les cocher.
- Recommencez l'opération pour les objets Formulaires et **<Nouveaux Formulaires>**
- Recommencez l'opération pour les objets Etats et **<Nouveaux Etats>**
- Recommencez l'opération pour les objets Macros et **<Nouvelles Macros>**
- Recommencez l'opération pour les objets Requêtes et **<Nouvelles Tables/Requêtes>**
- Cliquez sur **Appliquer** pour enregistrer la modification.

## IX-E - Activer les comptes

Les comptes sont actifs puisque nous les avons créés et affectés aux groupes.

Mais alors pourquoi nous n'y avons pas accès ?

Pour accéder à la gestion des comptes il faut définir un mot de passe pour le compte Administrateur, n'oubliez pas que c'est le compte par défaut. C'est avec lui que l'ensemble des utilisateurs de Microsoft Access dans le monde, lorsqu'ils n'ont pas mis en place la sécurité, se connectent.

Activons le mot de passe pour le compte par défaut.

- Allez dans le menu **Outils/sécurité/Gestion des utilisateurs et des groupes**
- Cliquez sur l'onglet **Changer le mot de passe**
- **Administrateur** est le compte actif dans cette session
- **Ancien mot de passe** doit rester vide.

The screenshot shows a dialog box titled "Gestion des utilisateurs et des groupes" with three tabs: "Utilisateurs", "Groupes", and "Changer le mot de passe". The "Changer le mot de passe" tab is active. It contains four input fields: "Nom de l'utilisateur" (Administrateur), "Ancien mot de passe" (empty), "Nouveau mot de passe" (\*\*\*\*\*), and "Confirmation" (\*\*\*\*\*). At the bottom are buttons for "OK", "Annuler", and "Appliquer".

*Un mot de passe ?*

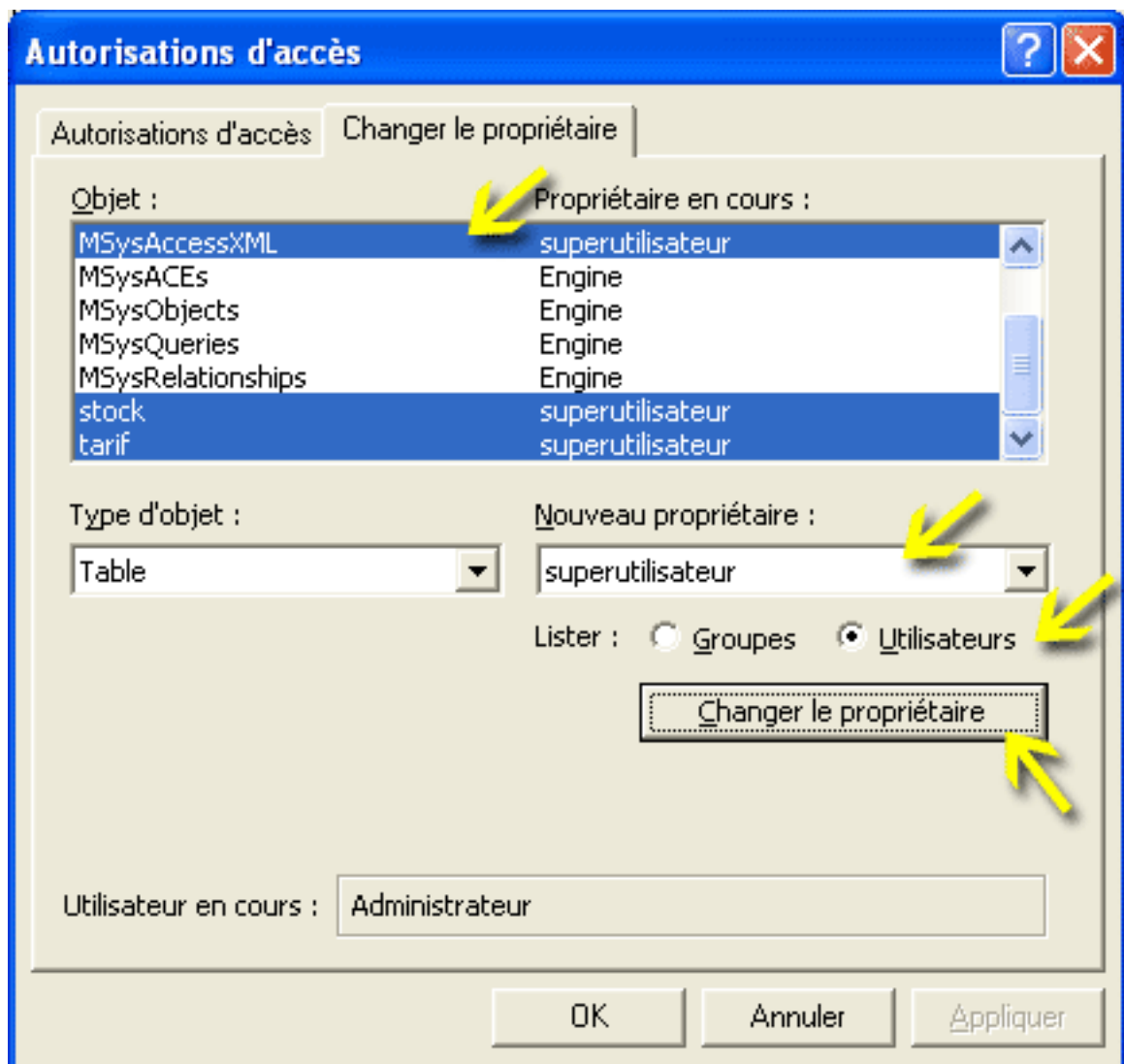
- **Nouveau mot de passe** entrez *admin*
- **Confirmation** entrez de nouveau *admin*
- Cliquez sur **Appliquer** et **Ok**
- Fermez Microsoft ACCESS

La sécurisation est pratiquement terminée, il ne reste que quelques manipulations à effectuer pour verrouiller complètement notre fichier.

## IX-D - Propriétaire

Comme nous avons créé un compte d'administrateur (**superutilisateur**) nous allons changer la valeur **Propriétaire** des objets. Le propriétaire est celui qui a l'autorisation de modification des objets lui appartenant.

- Allez dans le menu **Outils/sécurité/Autorisations d'accès**
- Cliquez sur l'onglet **Changer de propriétaire**
- Sélectionnez chaque objet ayant comme propriétaire **Administrateur** (ctrl + click)
- Cliquez sur le bouton d'option **Lister : Utilisateurs**



*Changement de Propriétaire*

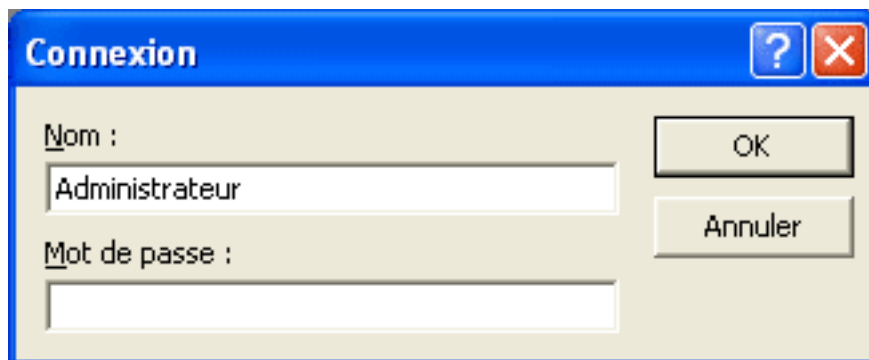
- Sélectionnez l'utilisateur **superutilisateur**.
- Cliquez sur **Changer le propriétaire**

Nous avons donc changer le propriétaire *Administrateur* par *superutilisateur*.

## X - Mots de passe et dégradation

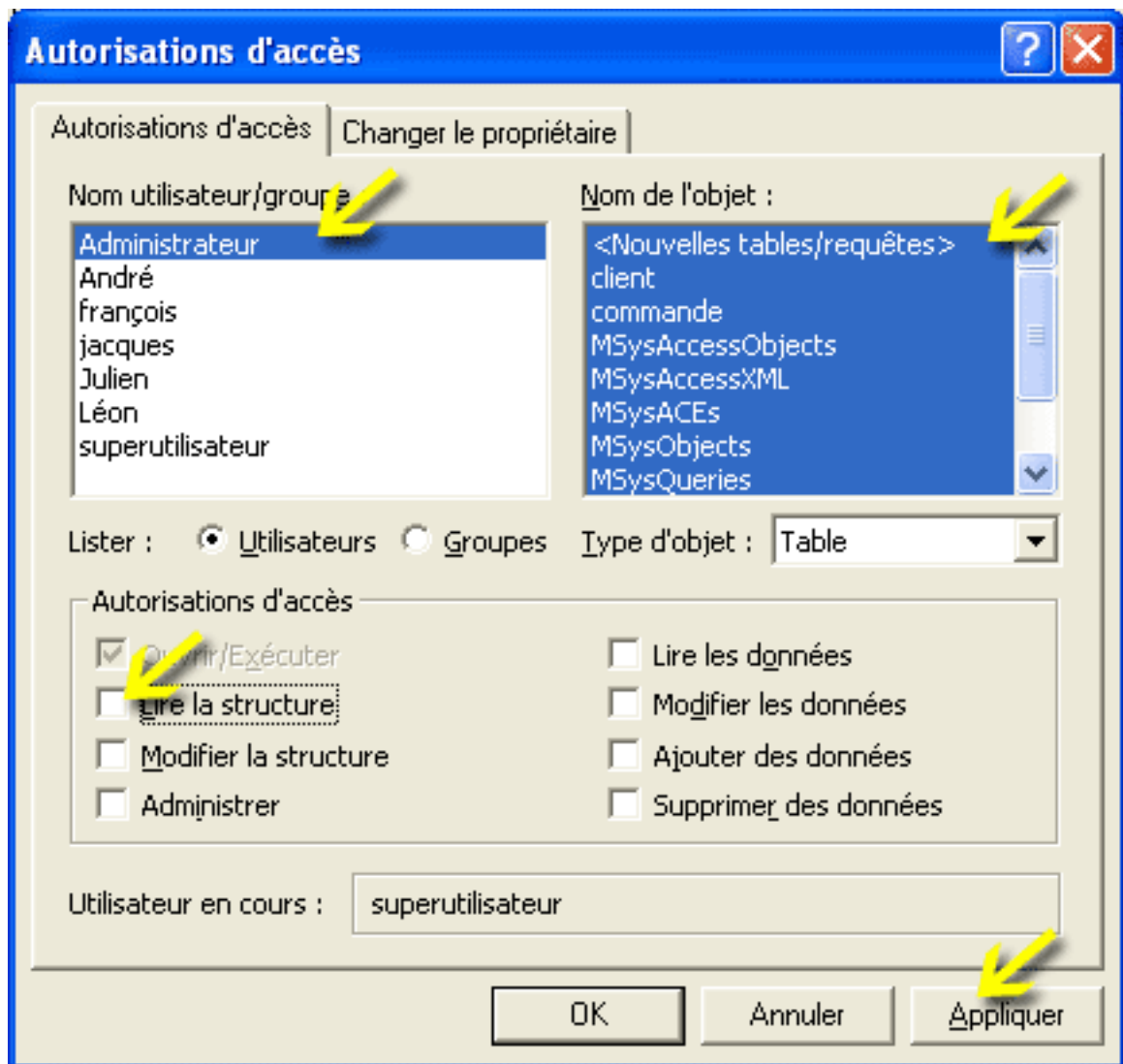
Ultime phase de la protection : la dégradation des droits qui va empêcher l'accès à l'application avec un fichier mdw standard. Pour faire cette manipulation il faut se connecter avec le nouveau compte d'administration que nous avons appelé **superutilisateur**.

- Ouvrez Microsoft ACCESS et l'application.



*On demande un mot de passe...*

- Remplacez le nom **Administrateur** par **superutilisateur**
- Cliquez sur **Ok**
- Ouvrez le menu **Outils/Sécurité/Autorisations d'accès...**
- Sélectionnez **Administrateur**
- Sélectionnez tous les objets **Tables** de la liste
- Cliquez 2 fois sur l'option **Lire Structure** pour tout décocher

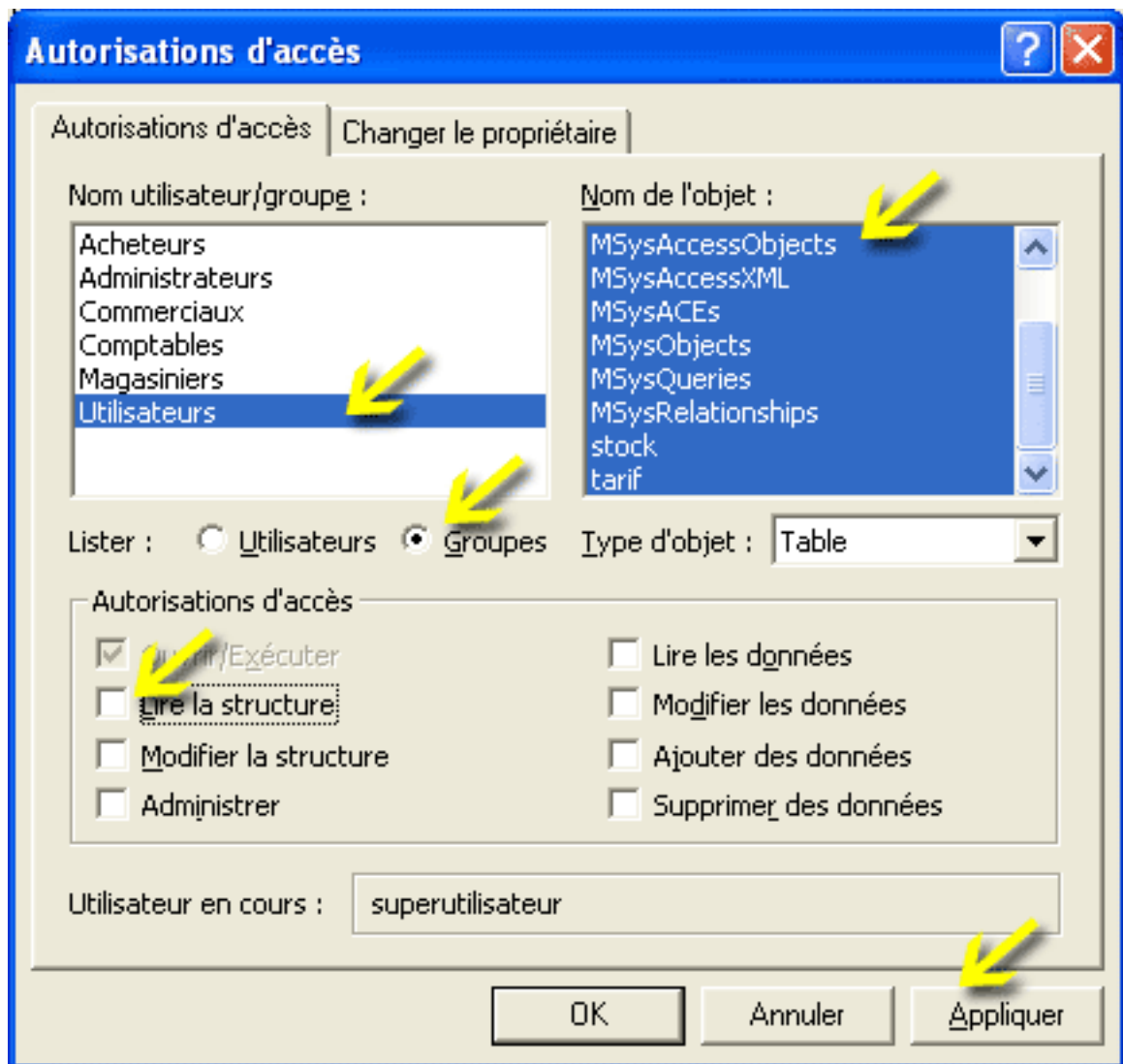


*Dégrader Administrateur*

- Cliquez sur **Appliquer**
- Cliquez sur **Ok**

Il manque encore une dégradation à faire, celle du groupe **Utilisateurs**.

- Sélectionnez **Lister : Groupe**
- Sélectionnez **Groupe**
- Sélectionnez tous les objets **Tables**
- Cliquez 2 fois sur l'option **Lire Structure** pour tout décocher



Dégrader Groupe Utilisateurs


- Cliquez sur **Appliquer**
- Cliquez sur **Ok**

La base est maintenant sécurisée.

## X-A - Les autres objets

Vous avez remarqué que nous avons protégé seulement les tables. Vous pouvez choisir également de protéger les formulaires, états et requêtes. Dans le cas d'une protection avec compilation mde l'utilisateur ne pourra pas faire de modification sur les formulaires, états et codes. Lorsqu'un utilisateur consulte un formulaire, état ou requête dont il ne possède pas les droits de lecture l'objet apparait sans aucun contrôle et données.

Maintenant est-il opportun d'en informer l'utilisateur ?

 *Pour créer ou modifier des objets formulaires, états et macros vous devez vous ouvrir l'application en mode exclusif.*

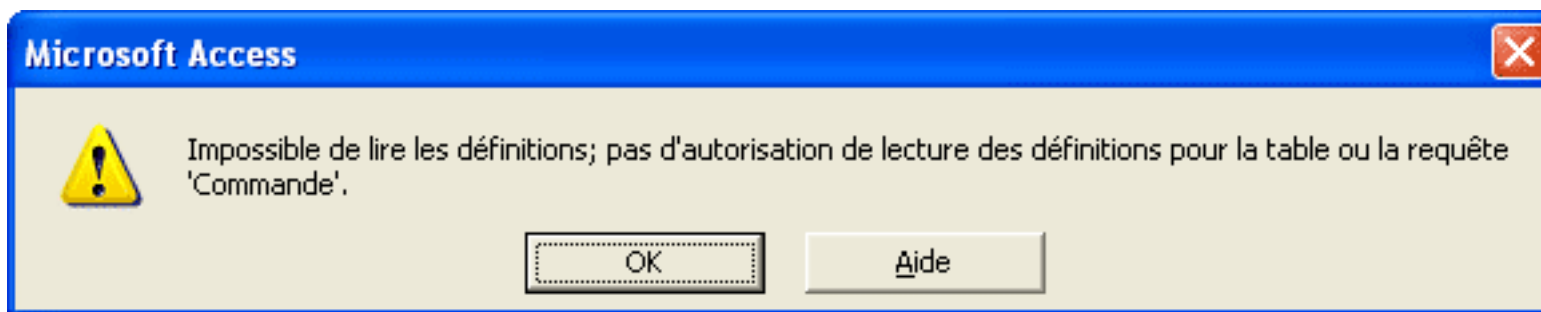
## XI - Tests

Pour nous assurer que la base est sécurisée nous allons faire quelques tests.

### XI-A - Avec le fichier MDW sécurisé

Nous allons faire le test avec le compte administrateur.

- Fermez ACCESS
- Ouvrez l'application
- Connectez-vous avec le compte **Administrateur**
- Essayez d'ouvrir l'une des tables
- Vous obtenez le message suivant :




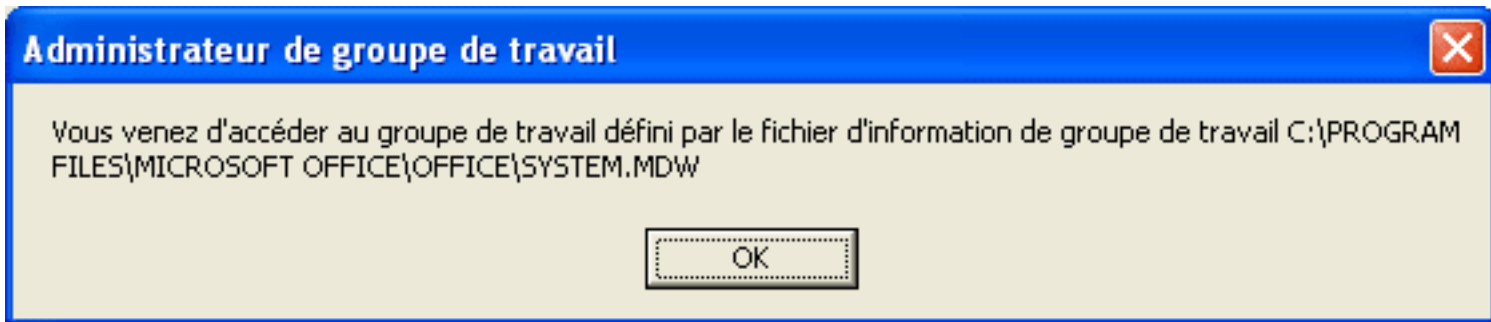
*Test concluant*

### XI-B - Avec le fichier MDW standard

Nous allons faire le test avec le compte administrateur.

- Fermez ACCESS
- Exécutez le programme **MS Access Workgroup Administrateur**
- Cliquez sur le bouton **Joindre...**
- Cliquez sur le bouton **Parcourir...**
- Sélectionnez le fichier **system.mdw** présent dans le répertoire Office.

 *Dans le cas ou vous ne trouvez pas le fichier **system.mdw** utilisez la recherche de Windows.*



*Groupe standard*

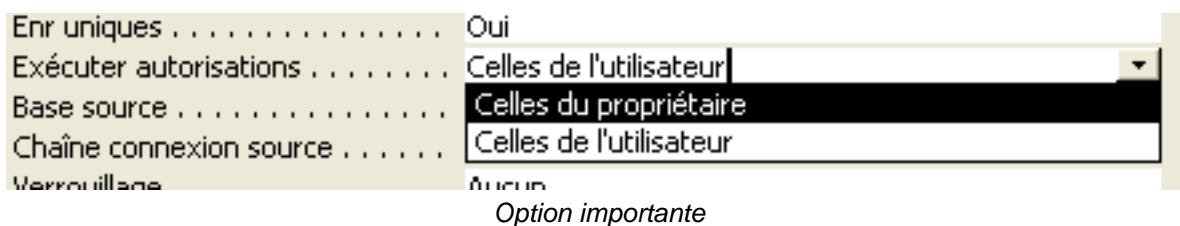
- Ouvrez l'application, notez qu'aucun mot de passe ne vous est demandé.
- Essayez d'ouvrir l'une des tables
- Vous obtenez le message même message que précédemment.

## XII - Les requêtes et la protection

Lorsque la sécurité est en place, les requêtes dépendent des droits sur les tables. Pourtant certaines requêtes doivent pouvoir s'exécuter par un utilisateur ayant des droits restreints sur la ou les tables concernées.

Microsoft Access permet de faire cela.

- 1 Ouvrez ou créez une requête avec le compte **superutilisateur**.
- 2 Faites un **clic droit** dans la zone des tables.
- 3 Dans le menu contextuel choisissez **Propriétés...**
- 4 Dans **Exécuter Autorisations** choisissez **Celles du propriétaire**.



- 5 Fermez la fenêtre **Propriétés...**
- 6 Sauvegardez la requête.

Il est évident que le propriétaire de la requête doit avoir les droits sur les tables concernées.

Si vous regardez le résultat de cette manipulation vous pourrez constater que la chaîne SQL comporte une option supplémentaire :

### WITH OWNERACCESS OPTION

Voici une requête avec l'option Propriétaire

```
SELECT CLIENT.N_CLIENT, CLIENT.NOM
FROM CLIENT
WITH OWNERACCESS OPTION;
```

Vous pouvez utiliser cette option pour tous les types de requêtes.

## XII-A - Plus loin avec ce type de requête

Vous pouvez choisir de concevoir l'application uniquement avec des requêtes de ce type. Dans ce cas vous devez respecter les directives suivantes :

- Pas d'accès direct aux tables,
- Toutes les requêtes doivent comporter le paramètre
- Les formulaires et états sont basées sur des requêtes,
- Les contrôles de zone liste et zone liste modifiable sont basés sur des requêtes,

## XIII - Codes, SQL et astuces

### XIII-A - Fichier MDW et options de démarrage

Il est souvent plus pratique de se servir des options de démarrage de Microsoft Access pour paramétrer le fichier mdw correspondant à l'application.

Ceci permet d'éviter de manipuler le programme **MS Access Workgroup Administrateur**, de toujours utiliser le bon fichier mdw et surtout d'utiliser par défaut le fichier mdw standard.

Consultez mon tutoriel sur  **Les options de démarrage.**

### XIII-B - Sécurité et code VBA

Voici un inventaire non-exhaustif des syntaxes VBA liées à la sécurité.

#### XIII-B-1 - Changement du mot de passe de la base de données courante

```
CurrentDb.NewPassword "Ancien_pass", "Nouveau_pass"
```

"Ancien\_pass" et "Nouveau-pass" peuvent être remplacés par des variables string.

#### XIII-B-2 - Changement du mot de passe de l'utilisateur courant

```
With DBEngine.Workspaces(0)  
  .Users(.UserName).NewPassword "ancienmotdepasse", "nouveaumotdepasse"  
End With
```

#### XIII-B-3 - Renvoi le nom de l'utilisateur ACCESS courant

```
Application.CurrentUser
```

Il s'agit de l'utilisateur connecté à l'application Microsoft ACCESS.

#### XIII-B-4 - Renvoi le nom de l'utilisateur WINDOWS courant

```
Environ("USERNAME")
```

Il s'agit de l'utilisateur connecté à Microsoft Windows, il peut être différent de celui de Microsoft ACCESS. Certains programmeurs utilisent le même nom pour Windows et ACCESS.

### XIII-C - Sécurité et DAO

### XIII-C-1 - DAO - Créer un groupe

```
Sub CreateGrp()  
    ' necessite librairie DAO  
    Dim wrk As Workspace  
    Dim grp As DAO.Group  
  
    Set wrk = DBEngine.Workspaces(0)  
  
    With wrk  
  
        Set grp = .CreateGroup("Mongroupe", "AZeRtY12456")  
        .Groups.Append grp  
  
    End With  
End Sub
```

### XIII-C-2 - DAO - Créer un utilisateur

```
Sub CreateUsr()  
    ' necessite librairie DAO  
    Dim wrk As Workspace  
    Dim usr As DAO.User  
  
    Set wrk = DBEngine.Workspaces(0)  
  
    With wrk  
  
        Set usr = .CreateUser("Jacques", "567AzERTY89", "mon_motdepasse")  
        .Users.Append usr  
  
    End With  
End Sub
```

### XIII-C-3 - DAO - Suppression Groupe

```
Sub DeleteGrp()  
    ' necessite librairie DAO  
    Dim wrk As Workspace  
  
    Set wrk = DBEngine.Workspaces(0)  
  
    With wrk  
  
        .Groups.Delete "Mongroupe"  
  
    End With  
End Sub
```

### XIII-C-4 - DAO - Suppression Utilisateur

```
Sub DeleteUsr()  
  
    ' necessite librairie DAO
```

```
Dim wrk As Workspace

Set wrk = DBEngine.Workspaces(0)

With wrk

    .Users.Delete "Jacques"

End With

End Sub
```

### XIII-C-5 - DAO - Affecter un utilisateur à un groupe

```
Sub AffectUsrGrp()
' necessite librairie DAO
Dim Wrk As Workspace
Dim Usr As DAO.User
Dim Grp As DAO.Group
Dim grpAffect As DAO.Group

Set Wrk = DBEngine.Workspaces(0)

With Wrk

    Set Usr = .Users("Jacques")

    Set Grp = .Groups("Mongroupe")

    Set grpAffect = Usr.CreateGroup("Mongroupe")
    Usr.Groups.Append grpAffect

End With

End Sub
```

### XIII-B-6 - DAO - Lister les groupes et utilisateurs

```
Sub lstGrpUsr()
Dim Wrk As Workspace
Dim Grp As DAO.Group
Dim Usr As DAO.User

Set Wrk = DBEngine.Workspaces(0)

With Wrk

    Debug.Print "Groupes :"

    For Each Grp In .Groups
        Debug.Print " " & Grp.Name
        Debug.Print "   Contient les membres suivants:"

        If Grp.Users.Count <> 0 Then
            For Each Usr In Grp.Users
                Debug.Print "     " & Usr.Name
            Next Usr
        Else
            Debug.Print "     Aucun Membre"
        End If

    Next Grp

End Sub
```

```
End With  
End Sub
```

## XIII-D - SQL et la sécurité

SQL dispose de tout un ensemble de commandes permettant de gérer les comptes utilisateurs, groupes et permissions (droits). Cependant cette fonctionnalité intéressante n'est disponible qu'avec ADO. En mode exécution directe et DAO il renvoie un message d'erreur.

## XIV - Liens importants

Quelques liens importants :

 [Administrer une base de données \(FAQ\)](#)

 [Renseignement sur l'utilisateur \(FAQ\)](#)

 [Code VBA sur la sécurité DAO et ADO par Tofalu](#)

 [Plus loin avec ADOX par J.M. RABILLOUD](#)

 [Advanced MS JET SQL for ACCESS 2000](#)

## XV - Remerciements

Je tiens à remercier : **Dolphy35** et **Kikof** pour le temps passé en relecture et correction.

À l'équipe de **Developpez.com** pour la qualité du site.

À **Nono40** pour son super éditeur XML qui se bonifie avec le temps comme un bon Bordeaux.

Je présente mes plus plates excuses à ceux que j'aurais omis de remercier.

