Sécuriser l'accès au cube

Le cube est maintenant finalisé ! Enfin presque… Car il nous faut penser maintenant à la mise à disposition des données aux utilisateurs et donc à la mise en place de la sécurité qui sera associée à cette nouvelle base de données.

Il est pertinent de penser à la sécurisation du cube DataWarehouse avant de commencer le développement des flux ETL, car notre expérience nous a prouvé à plusieurs reprises que la sécurité pouvait avoir une incidence non négligeable sur sa modélisation. Dans certains cas, l'impact était simplement la mise à disposition de nouvelles dimensions (fonctionnelles ou purement techniques), mais dans d'autres cas, il nous a fallu dupliquer des groupes de mesures en supprimant ou en ajoutant des liaisons avec certaines dimensions. Réfléchir à la mise en place de la sécurité apporte toujours un point de vue intéressant et neuf sur la modélisation finalisée que vous envisagez de mettre en place. C'est donc un excellent moyen de l'éprouver.

C'est pourquoi nous vous proposons dans cette section de découvrir les principes de restriction des accès dans Analysis Services.

1. Donner l'accès au cube

Nous allons commencer par apprendre à donner accès au cube. Par défaut, un cube n'est accessible qu'aux seuls administrateurs de l'instance Analysis Services définis lors de son installation. Nous allons donc voir comment mettre à jour la liste des comptes administrateurs de l'instance, puis, dans un second temps, nous verrons comment configurer des accès à des comptes utilisateurs.

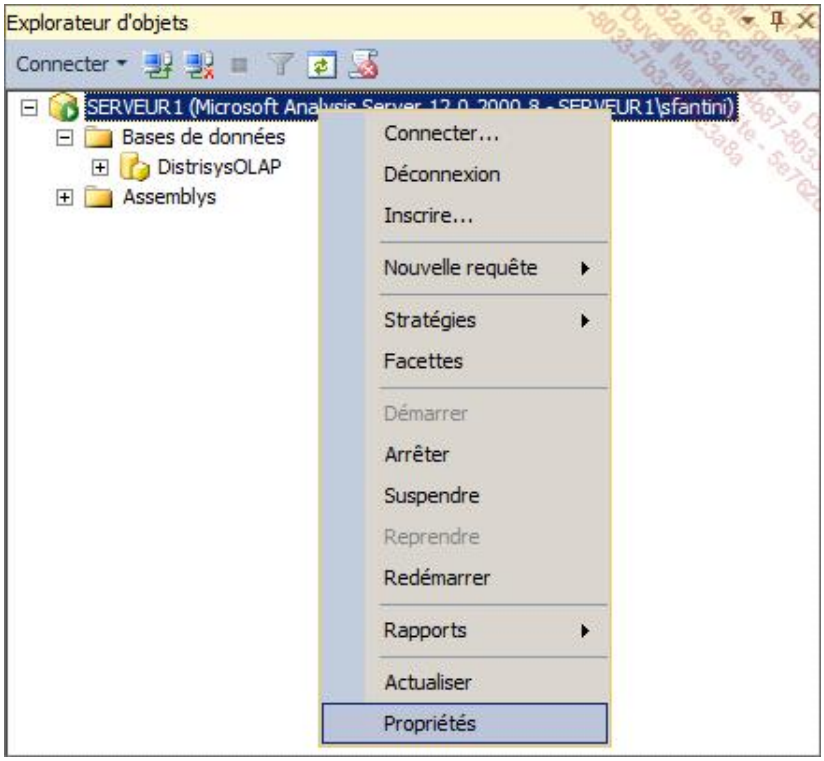
a. Donner l'accès aux administrateurs

Analysis Services accepte uniquement l'authentification Windows. C'est pourquoi seuls les utilisateurs disposant d'un compte Windows (de domaine de préférence) pourront accéder aux données d'une base de données Analysis Services.

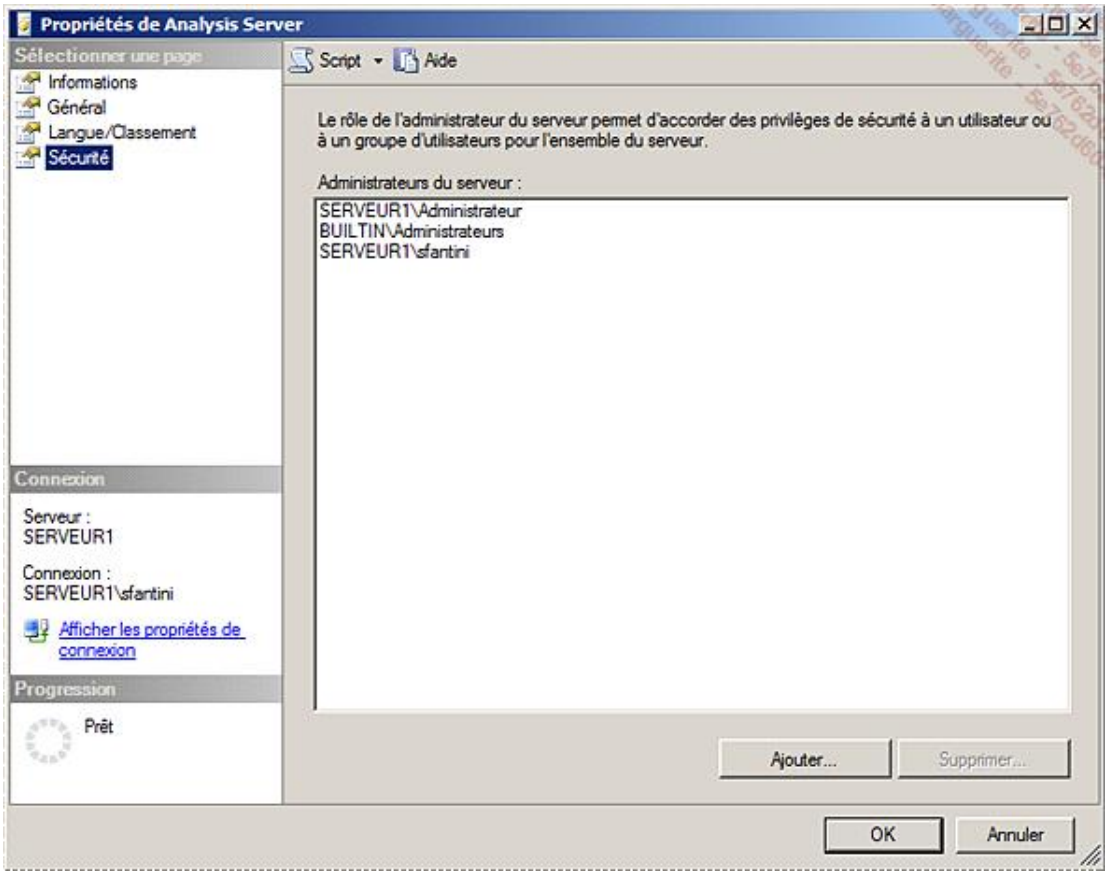
Les droits se donnent donc soit au travers d'un compte utilisateur, soit au travers d'un groupe de sécurité.

L'affectation des administrateurs d'une instance Analysis Services se fait à l'aide de la console SQL Server Management Studio.

- Ouvrez la console **SQL Server Management Studio**.
- Connectez-vous à l'instance **Analysis Services** souhaitée.
- Sélectionnez l'instance, puis faites un clic droit pour faire apparaître le menu contextuel. Cliquez alors sur **Propriétés**.



Lorsque la fenêtre **Propriétés de Analysis Server** est ouverte, cliquez sur l'onglet **Sécurité**.



Dans cette fenêtre, vous pouvez alors consulter la liste des utilisateurs ou des groupes d'utilisateurs ayant des droits étendus sur l'instance Analysis Services.

Les droits sont étendus, car les membres de cette liste disposent de tous les privilèges sur l'ensemble des bases

de données contenues dans l'instance. Ces utilisateurs peuvent lire le contenu, mettre à jour les droits ou traiter les données de toutes les bases de données de l'instance. Ils peuvent également sauvegarder, restaurer ou créer une nouvelle base de données multidimensionnelle.

C'est donc ici que figureront les quelques utilisateurs chargés de l'exploitation de l'ensemble de l'instance Analysis Services.

Les membres du groupe Administrateurs local au serveur où est installée l'instance d'Analysis Services sont d'office administrateurs de l'instance. Donc, même si vous supprimez le groupe BUILTIN\Administrateurs de la liste, les membres de ce groupe auront toujours des droits étendus sur l'instance Analysis Services.

b. Donner accès aux utilisateurs

Analysis Services permet toutefois de définir beaucoup plus finement les accès à son contenu.

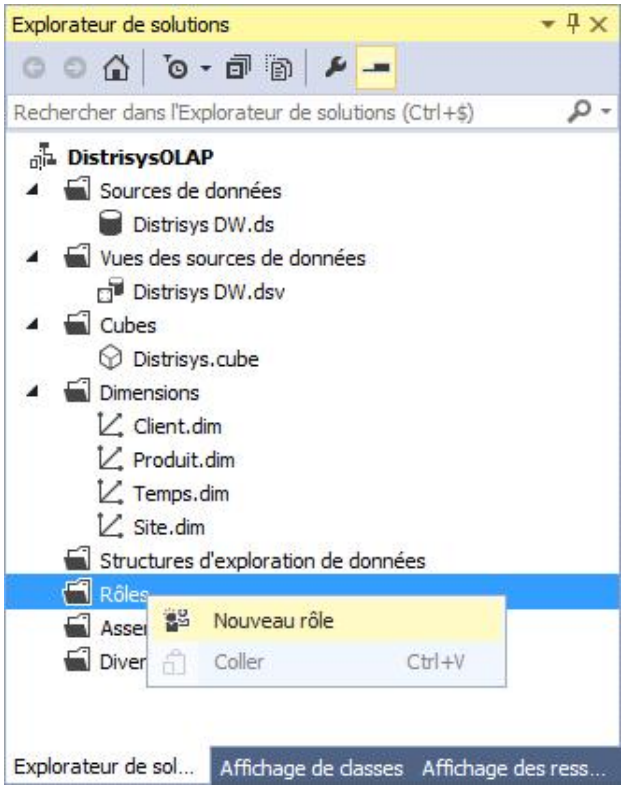
L'affectation des accès à de simples utilisateurs consommateurs de données se fait par le biais de rôles de sécurité configurables au niveau de chacune des bases de données multidimensionnelles.

Les actions de création, suppression ou mise à jour des rôles de sécurité peuvent se faire soit depuis la console SQL Server Data Tools, soit dans SQL Server Management Studio.

Pour commencer, nous allons créer un premier rôle de sécurité, qui donnera aux contrôleurs de gestion du groupe Distrisys un accès en lecture sans restriction au cube DataWarehouse.

Nous allons créer le rôle avec SSDT.

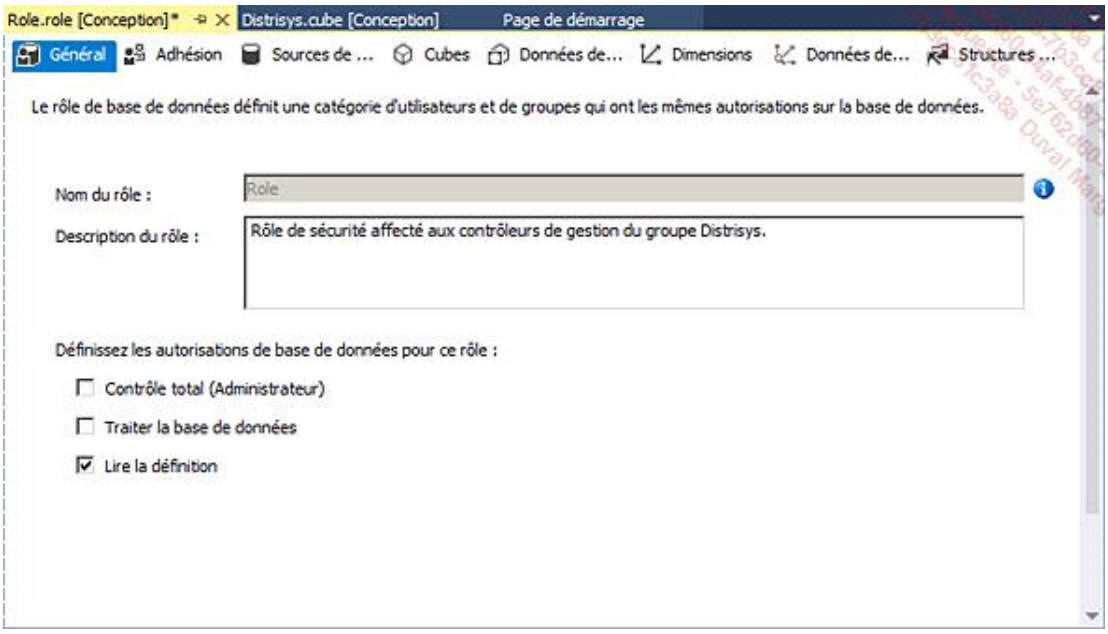
- Dans **SSDT**, au niveau de l'**Explorateur de solutions**, faites un clic droit sur **Rôles**, puis cliquez sur **Nouveau rôle**.



L'interface de gestion d'un rôle est identique dans SSDT et SSMS.

Comme nous souhaitons créer un rôle de sécurité donnant aux membres du contrôle de gestion l'accès au cube DistrisysDW, un accès en lecture est suffisant.

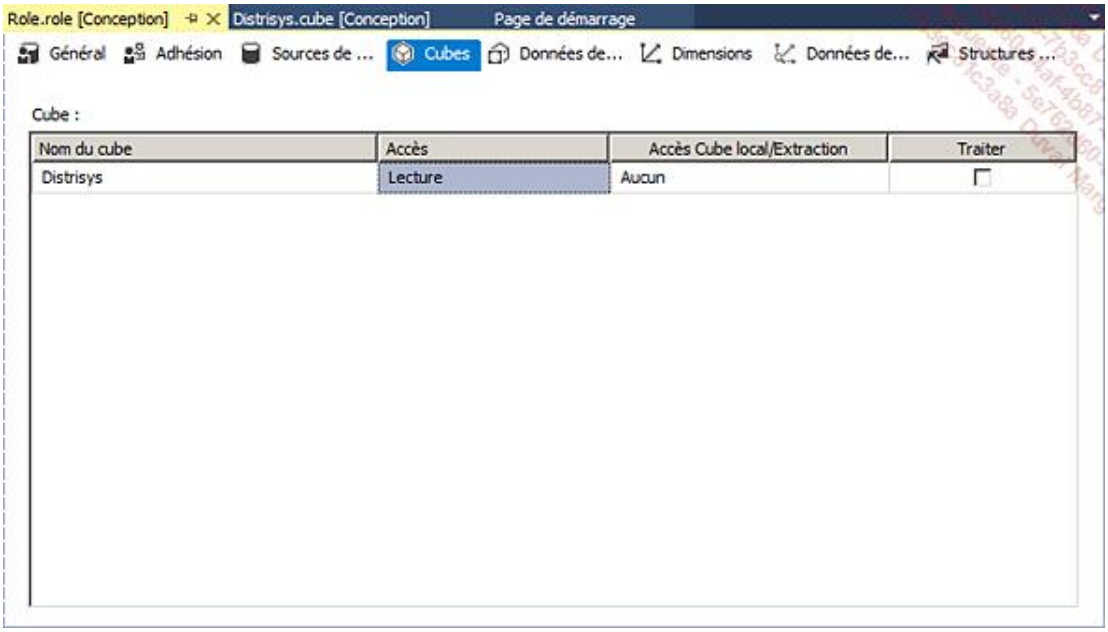
- Cochez la case **Lire la définition**.



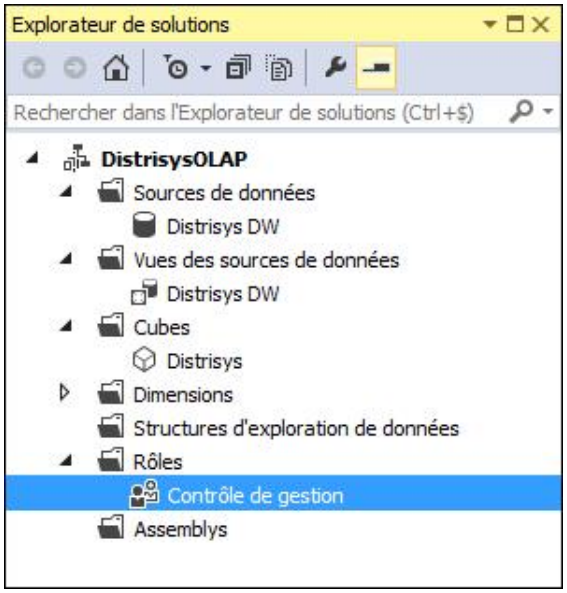
Interface de gestion d'un rôle de sécurité

- Cliquez maintenant sur l'onglet **Adhésion**, afin d'identifier les utilisateurs faisant partie de ce nouveau rôle de sécurité.
- Ajoutez les utilisateurs ou groupes de votre choix. Dans notre cas, nous allons ajouter le groupe de sécurité Contrôle de gestion. Il s'agit du groupe Windows dont font partie tous les contrôleurs de gestion du groupe Distrisys.

- Cliquez maintenant sur l'onglet **Cubes**, et au niveau du cube **Distrisys**, affectez à la colonne **Accès** la valeur **Lecture**.



- Enregistrez vos modifications, puis dans l'**Explorateur de solutions**, renommez le nouveau rôle de sécurité **role.role** en **Contrôle de gestion.role**.



- Pour finir, déployez et traitez la base DistrisysDW.

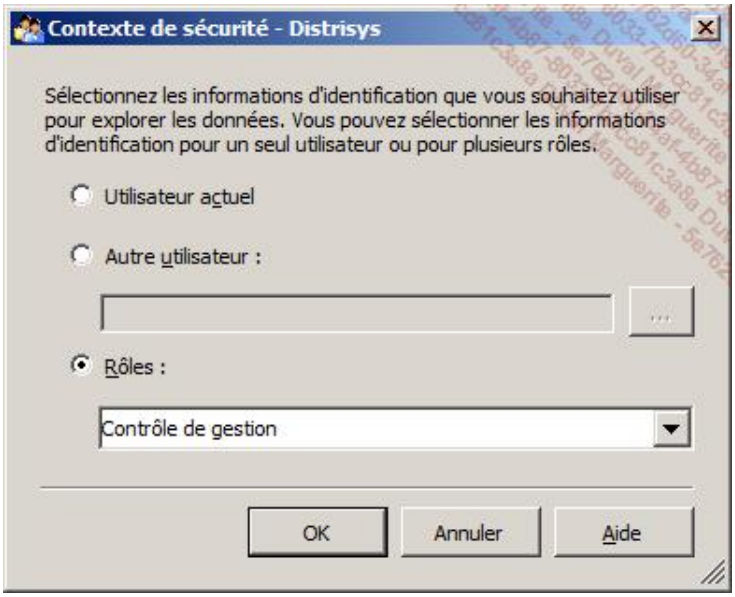
Afin de vérifier que les droits sont correctement définis, nous allons utiliser une fonctionnalité d'Analysis Services qui permet aux administrateurs du cube d'accéder aux données en simulant un utilisateur ou un membre d'un rôle.

- Pour tester notre nouveau rôle, rendez-vous sur l'onglet **Navigation**.

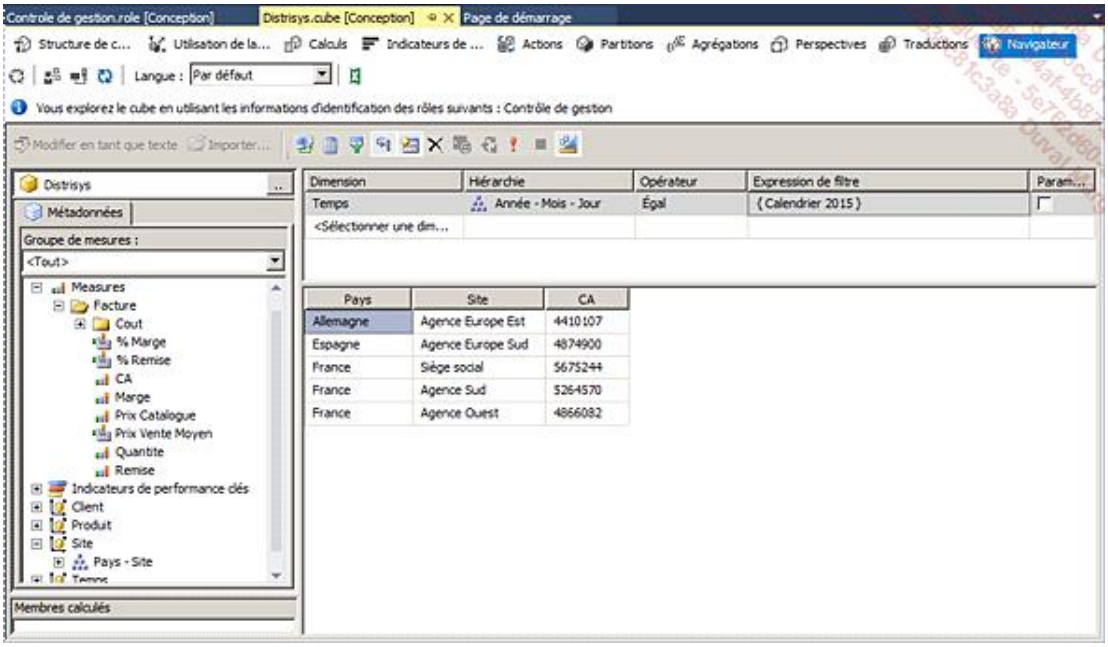
- Cliquez ensuite sur le bouton **Changer d'utilisateur** 

Une fenêtre vous demande alors de sélectionner les informations d'identification que vous souhaitez emprunter.

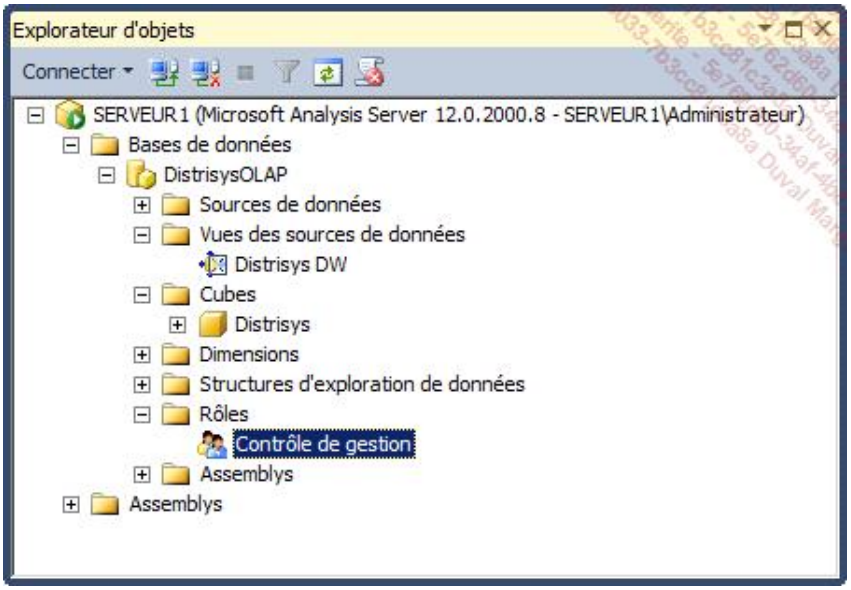
- Dans notre cas, nous sélectionnons le rôle de sécurité **Contrôle de gestion**.



On constate alors que l'accès au cube est ouvert correctement sans restriction pour tous les membres du rôle Contrôle de gestion.



En vous connectant avec SSMS à la base Analysis Services, vous constatez que l'on retrouve le rôle nouvellement créé. SSMS dispose d'une interface similaire à SSDT qui offre les mêmes fonctionnalités pour la gestion des rôles.



La gestion des rôles se fait également sous SSMS.

Vous savez maintenant créer un rôle de sécurité et donner à des utilisateurs l'accès à l'ensemble d'un cube.

2. Restreindre l'accès

Dans la réalité, peu d'utilisateurs accèdent à l'entrepôt de données sans restriction. La plupart n'ont accès qu'à un sous-ensemble des données. Ces sous-ensembles sont définis :

- soit par leur étendue fonctionnelle : un utilisateur ne voit que quelques domaines fonctionnels. Par exemple, l'accès ne peut concerner que la facturation, que les commandes clients, ou uniquement les stocks et les commandes fournisseurs… Les données qui concernent les autres domaines fonctionnels de l'entrepôt de données sont alors invisibles pour cette personne.
- soit par leur profondeur : un utilisateur a accès à tous les domaines fonctionnels, mais uniquement dans un périmètre donné, comme une agence ou une ligne de produits.
- soit par la combinaison des deux : par exemple, un responsable des ventes local n'a accès qu'à la facturation et aux commandes clients, et uniquement sur le périmètre de son agence.

Nous allons donc voir comment appliquer ces restrictions.

- La restriction de l'étendue fonctionnelle sera traitée comme une restriction sur des mesures.
- La restriction sur la profondeur sera traitée comme une restriction sur des membres d'attribut de dimension.

Pour illustrer ces restrictions, nous allons créer un nouveau rôle : Commercial - Europe de l'Est.

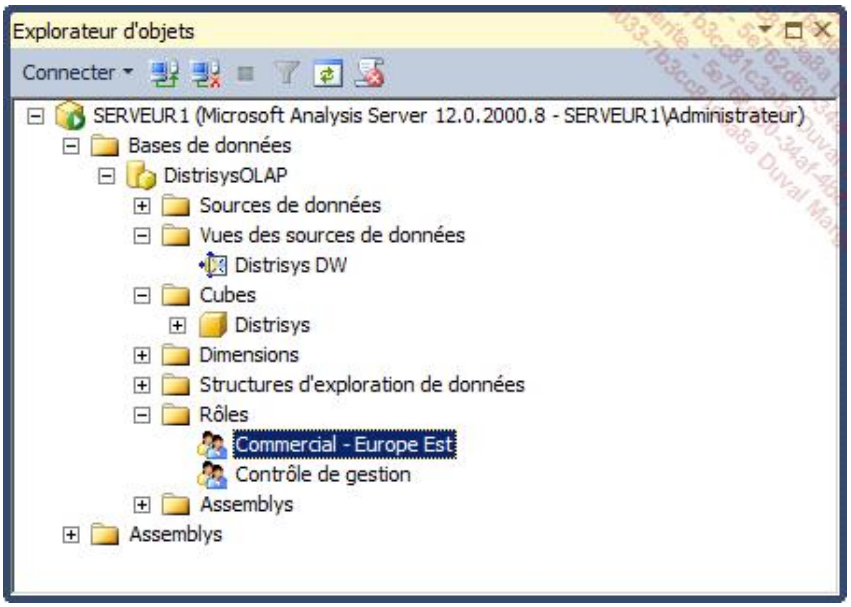
Ce rôle Commercial - Europe de l'Est, dont fait partie l'utilisatrice Cécile Aubert, donnera accès à la facturation mais pas à l'analyse des marges, jugée trop critique par la direction, et son champ sera réduit uniquement aux données de ventes émanant de la zone commerciale Europe de l'Est.

a. Restreindre l'accès aux membres d'une dimension

Nous allons commencer par créer un nouveau rôle *Commercial - Europe Est*.

- Pour cela, dans **SSDT**, au niveau de l'**Explorateur de solutions**, copiez le rôle **Controle de gestion** et collez-le sous le nom **Commercial - Europe Est**.

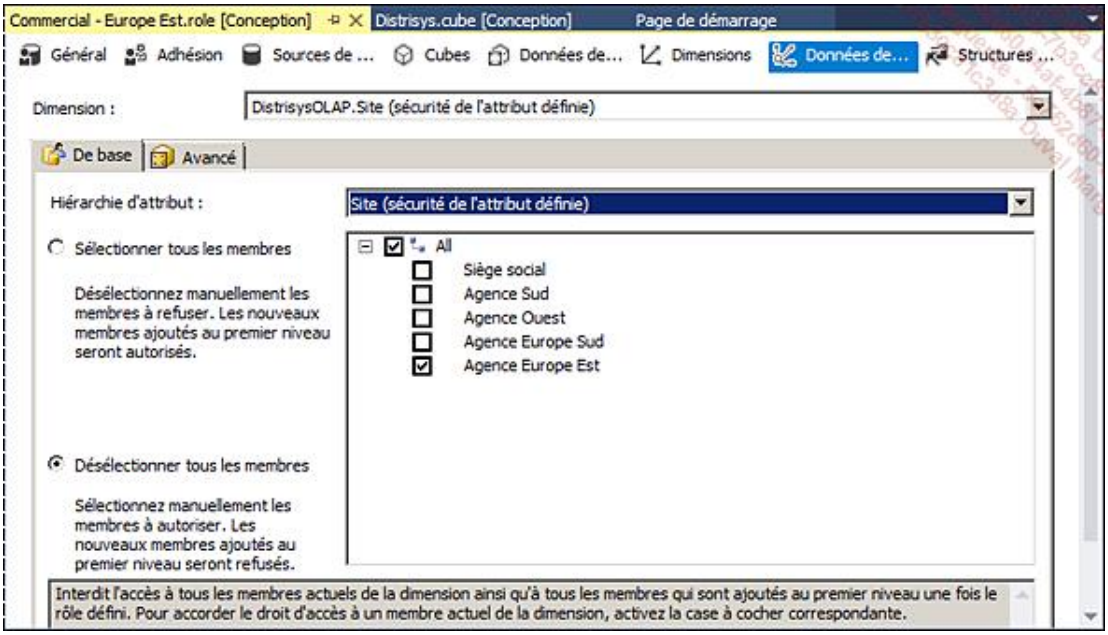
Vous devriez ainsi obtenir ceci dans l'Explorateur de solutions :



- Éditez le rôle, et dans l'onglet **Affectation**, remplacez le groupe précédent (**Contrôle de gestion**) par le compte de l'utilisateur (pour nous, **caubert**).
- Déployer le cube et vérifiez que le rôle fonctionne correctement et donne bien accès à l'ensemble du cube *Distrisys*.

Maintenant que le rôle est correctement créé, nous allons pouvoir limiter l'accès à la zone commerciale Europe de l'Est, en appliquant une restriction sur l'attribut *Site* de la dimension *Site*.

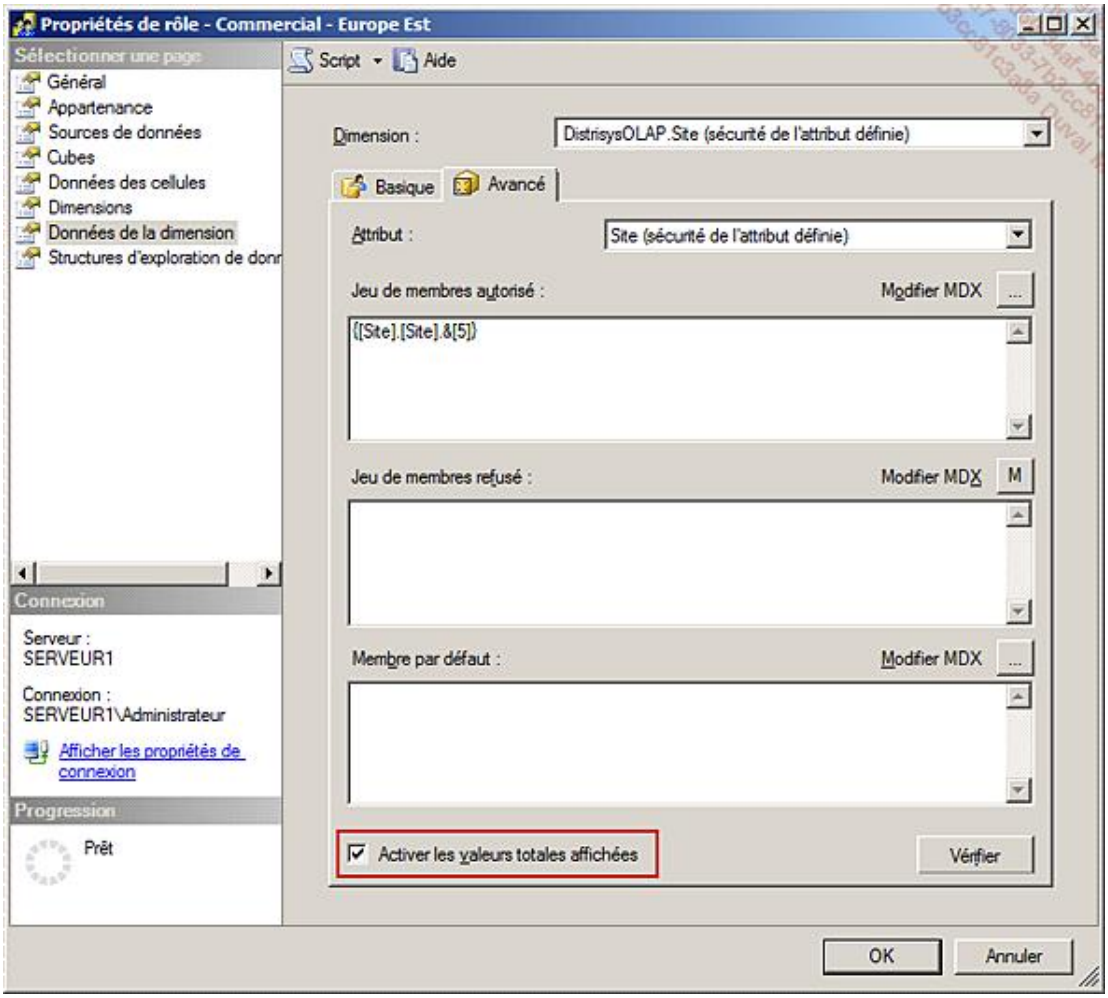
- Pour cela, dans le rôle **Commercial - Europe Est**, sélectionnez l'onglet **Données de dimension**.
- Dans la liste **Dimension**, sélectionnez la dimension **Site**.
- Dans la liste **Hiérarchie d'attribut**, sélectionner l'attribut **Site**.
- Enfin, cochez la case **Désélectionner tous les membres** et sélectionnez le membre **Agence Europe Est**.



Appliquer une restriction sur un membre d'un attribut.

Cette sélection signifie que les membres de ce rôle n'ont par défaut accès à aucun membre de l'attribut *Site*, mis à part celui ou ceux qui sont sélectionnés. Dans notre cas, seul le membre Agence Europe Est sera accessible.

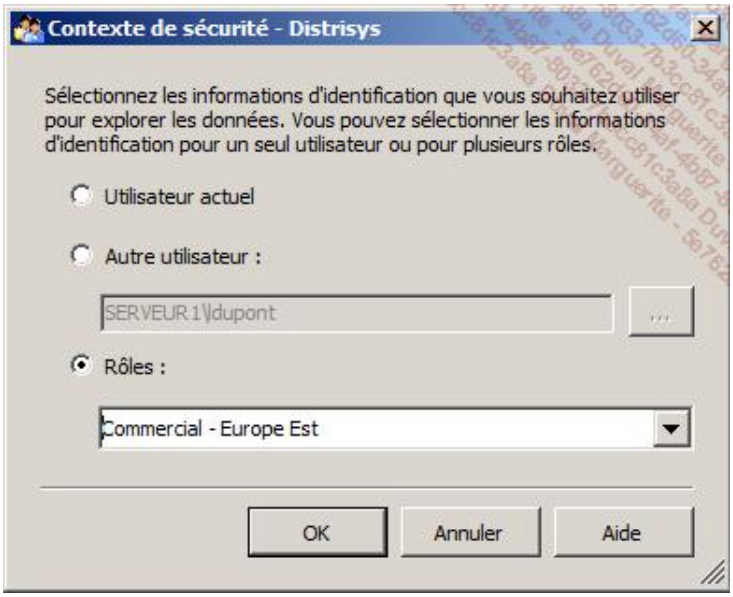
- Ouvrez l'onglet **Avancé** et cochez la case **Activer les valeurs totales affichées**. Cette option, qui pourrait s'appeler *Filtrer les valeurs totales*, permet de limiter les totaux aux membres autorisés de la dimension. Si vous ne la cochez pas, Cécile Aubert verra l'ensemble du CA de Distrisys, mais n'accédera qu'au détail de l'Agence Europe Est.



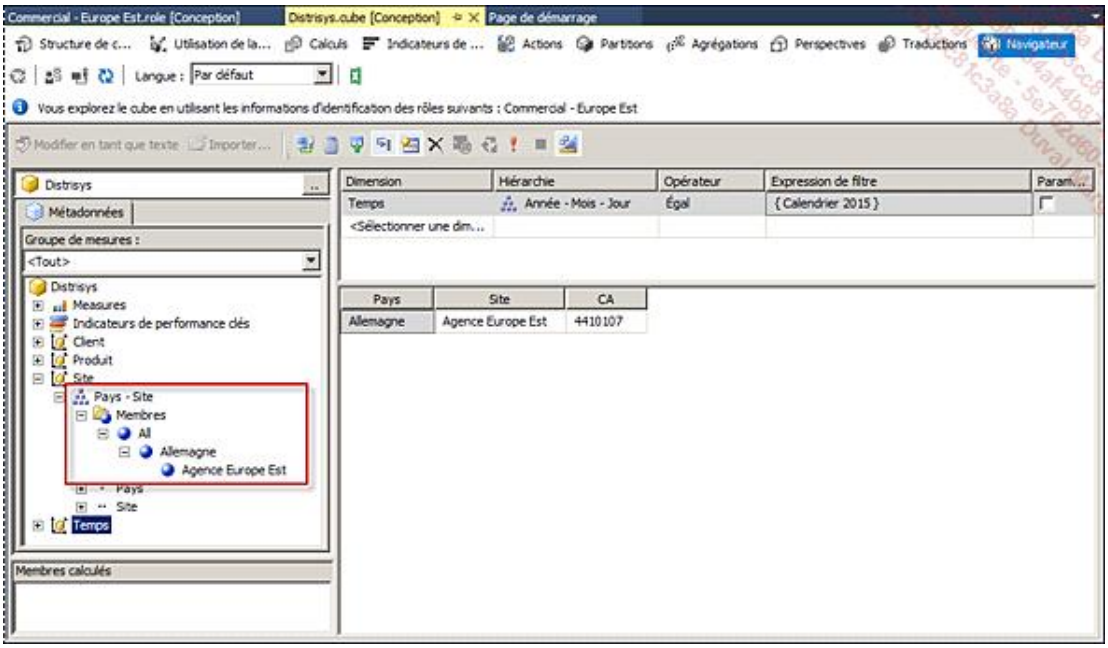
Limiter les totaux aux membres autorisés.

Vous noterez que les noms des dimensions ou attributs qui portent des restrictions sont suivis de la mention **(sécurité de l'attribut définie)**.

- Enregistrez, déployez et traitez le cube.
- Puis allez sur l'onglet **Navigation** pour emprunter l'identité d'un membre du rôle **Commercial - Europe Est**.



On constate alors que les membres de ce rôle ne peuvent accéder qu'au seul membre *Agence Europe Est*.

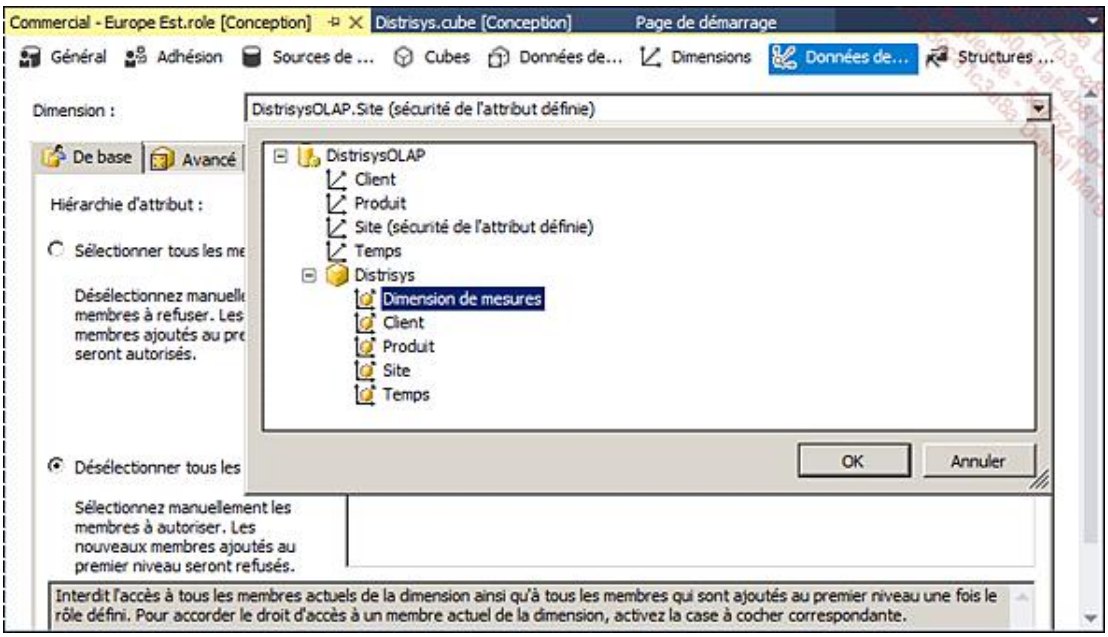


L'application de la restriction de sécurité au niveau des membres de l'attribut *Site* a fonctionné correctement.

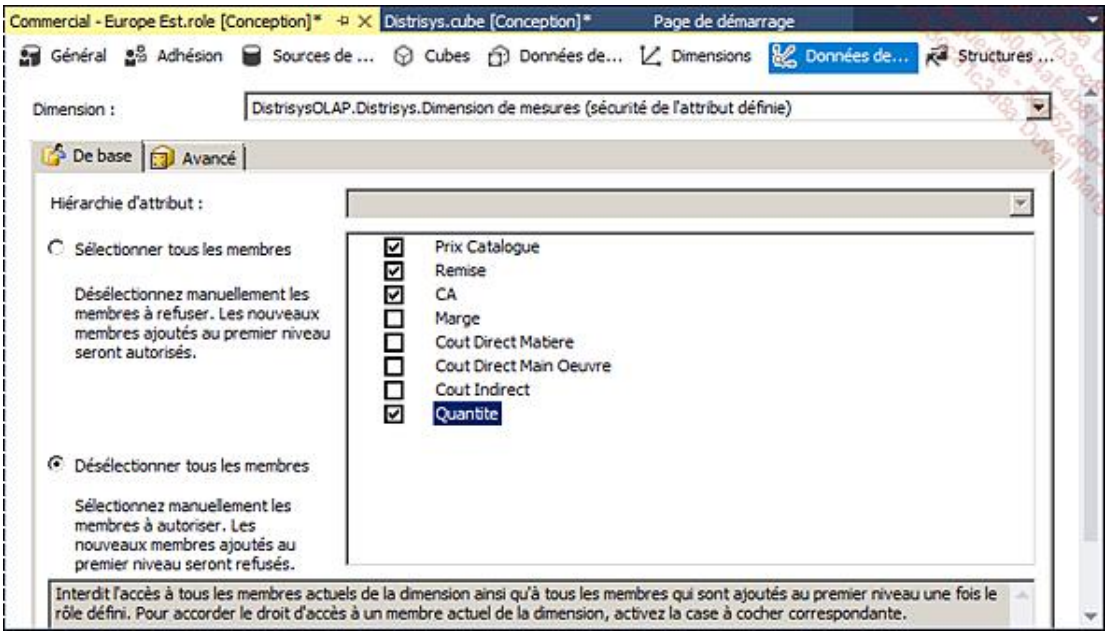
b. Restreindre l'accès aux mesures

Nous allons maintenant finaliser la création de ce rôle *Commercial - Europe Est* en interdisant l'accès aux mesures concernant la marge et les coûts. Ou plutôt, nous allons seulement autoriser aux membres de ce rôle l'accès aux mesures de la facture concernant le Chiffre d'affaires et le Prix Catalogue.

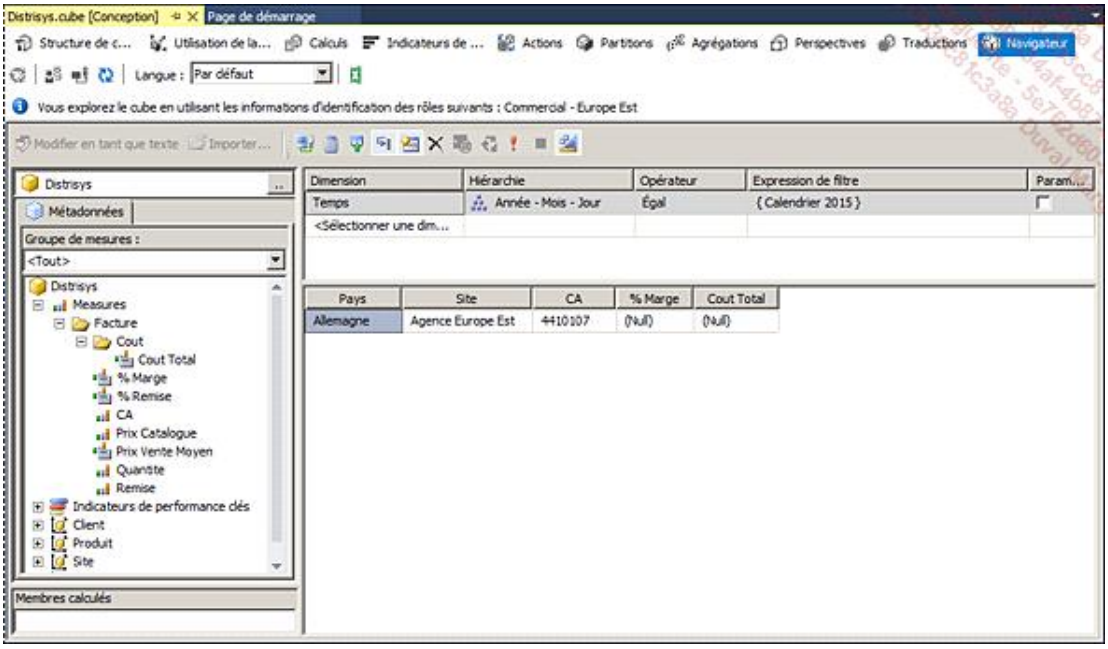
- Dans **SSTS**, retournez dans l'onglet rôle **Commercial - Europe Est.role**.
- Sélectionnez l'onglet **Données de dimension** puis au niveau de la liste **Dimension**, sélectionnez **Dimension de mesures**.



- Cochez la case **Désélectionner tous les membres** pour interdire l'accès à toutes les mesures sauf celles sélectionnées.
- Sélectionnez maintenant les mesures **Prix Catalogue**, **Remise**, **CA**, **Quantite**. Cela aura alors pour effet de masquer toutes les autres mesures, c'est-à-dire celles qui concernent les coûts et la marge.



- Enregistrez, déployez et traitez le cube.
- Puis allez sur l'onglet **Navigation** pour emprunter de nouveau l'identité d'un membre du rôle **Commercial - Europe Est**.



On constate que les mesures et les données concernant la marge ou les coûts ne sont plus disponibles ou accessibles.

La restriction s'est bien appliquée.

3. Pistes pour industrialiser la gestion des droits

Nous venons d'illustrer les principes d'application de restrictions d'accès aux données d'un cube Analysis Services. Nous pouvons restreindre les accès au niveau de chaque membre de chaque attribut de chaque dimension, et au niveau de chaque mesure. C'est un système extrêmement puissant qui permet de gérer très finement les accès.

Les restrictions fonctionnelles appliquées aux mesures permettent de regrouper des personnes par rapport à leur périmètre fonctionnel, donc leur rôle dans la société.

Par contre, les restrictions sur la profondeur, appliquées aux membres des dimensions, permettent de "spécialiser" chaque membre d'un rôle.

Au niveau global de Distrisys, nous avons identifié les principaux rôles suivants :

- Contrôleur de gestion : accès à tout, même ce qui est en cours de développement ou de recette.
- Direction : accès à tous les groupes de mesures qui ont été validés par le contrôle de gestion.
- Direction Site : accès à tous les groupes de mesures mais restreint à un seul site.
- Commercial : accès factures et commandes clients pour un seul site.
- Logistique : accès commandes client, commandes fournisseurs et stocks.
- Responsable produit : accès factures, commandes, stocks… Mais restreint uniquement à une famille de produits.

Les deux premiers rôles, qui ne nécessitent pas de restriction sur les dimensions, ne posent pas de problèmes et seront simples à mettre en œuvre.

Par contre, pour les rôles qui nécessitent une restriction par site, il nous faudra créer un rôle Analysis Services par site. Il en sera de même pour tous les rôles qui nécessitent une restriction par produit, client...

Dans le cas de Distrisys, on voit donc bien que cela peut donner lieu à beaucoup de rôles distincts dont la maintenance va s'avérer risquée et fastidieuse. Et encore, Distrisys n'a que cinq sites. Que penser alors des réseaux de plusieurs centaines de boutiques ? On voit bien que cette approche manuelle atteint rapidement ses limites.

La gestion des droits d'Analysis Services est puissante, mais Microsoft ne propose pas nativement un outil qui permettrait de canaliser et de gérer plus simplement la complexité que la sécurité peut engendrer. Notez également que l'interface de gestion des droits est donnée à un administrateur dans une console technique et qu'elle ne peut être mise dans les mains de fonctionnels qui, en toute logique, devraient se charger eux-mêmes de la sécurité de l'entrepôt de données, qui d'une certaine façon représente l'organisation fonctionnelle de la société.

Mais si cette application n'est pas fournie par Microsoft, la possibilité d'intégrer des développements spécifiques permet d'en envisager la réalisation. Le principe sera de gérer l'affectation des droits de chaque personne dans une base de données relationnelle, avec une interface dédiée et utilisable par des personnes du métier habilitées à définir les accès (il s'agit généralement du service Contrôle de gestion). Dans le rôle Analysis Services, au niveau de la définition des restrictions aux membres d'une dimension on utilisera une fonction qui interrogera la base de données relationnelle et qui renverra la liste des membres autorisés pour l'utilisateur courant. Nous n'aurons donc plus qu'un rôle Analysis Services par rôle fonctionnel, et les restrictions de périmètre seront gérées dynamiquement. Réaliser une telle application ne rentre pas dans le cadre de cet ouvrage. Néanmoins, nous vous proposons dans les éléments à télécharger des informations plus techniques qui vous permettront de mettre en place un tel système.