China-pub.com
下载

第11章 安 全

本章目标

本章主要内容如下：

- 在OLAP数据库中创建安全角色。
- 在数据库和立方体层次上管理安全角色。
- 限制对维和维的某些部分的访问。
- 为不同的角色创建定制计算成员。
- 创建多维表达式（MDX）适应单元格层次安全。

在大多数实际的应用程序中，OLAP数据库都要求回答不同用户群体所提的各种问题。例如，商品经销代理可能会对特定区域某类产品某种用户的销售额感兴趣。区域经理可能会对一个区域某种产品某类用户的总销售额感兴趣。而技术支持代表则会对某种产品某类用户的电话咨询数量感兴趣。

在许多情况下，这些答案都可以在一系列的立方体中找到。在特定的条件下，上述所有信息都保留在一个立方体中。如果你希望商品经销代理只能查看自身的销售信息，而不能查看其他商品经销代理的信息，那么就必须实现安全机制。本章，你将了解 Microsoft SQL Server 2000 Analysis Services中的安全机制是如何工作的。

开始

在Analysis Manager中，右键单击服务器文件夹并单击 Restore Database。接着在包含本书示例文件的目录中查找 Chapter 11，选择 Chapter 11，单击 Open。单击 Restore，然后关闭 Restore Database Progress对话框。

11.1 创建安全角色

Analysis Services安全机制基于 Microsoft Windows NT（不论是 Windows NT 4还是 Microsoft Windows 2000）并集成于其中。当要在 Analysis Services中定义安全机制时，可在OLAP数据库中创建安全角色。每个角色包含操作系统中所定义的一个或多个用户账号或用户组。一旦创建了数据库安全角色，就可以将该角色与 OLAP数据库中的立方体或虚拟立方体相连。另外，还可以通过限制对元数据（维中的成员）和数据（立方体中存储的值）的访问在立方体中调整安全机制。

注意 Analysis Services自动在操作系统中创建OLAP Administrators组。要使用Analysis Manager，则当前用户必须是OLAP Administrators组的成员。OLAP Administrators组的

需要全本请访问 www.ertongbook.com

China-pub.com
下载

任何成员都能完全访问服务器中的每个立方体和数据库。换句话说，你不能创建这样一种安全机制，即用户可以管理某个数据库，却不能管理其他的数据库。为了防止Analysis 服务器被病毒或宏损害，属于OLAP Administrators组的用户账号不能用来访问Web网页或使用支持脚本和宏的多产性和电子邮件应用程序。

警告 不能删除OLAP Administrators组。OLAP Administrators组是在Analysis Services安装过程中自动创建的。如果没有 OLAP Administrators组，则任何用户都不能使用Analysis Manager管理Analysis 服务器。

1. 创建示例用户和组

Analysis Services的安全性依赖于操作系统 User（用户）账号和 Group（组）账号。如果某人要获得使用 Windows 2000或Winows NT服务器的权利，那么服务器管理员必须先为他创建一个用户账号。该用户账号可以被指定为属于一个和多个适当的组。本章中，将使用Windows用户和组来创建安全机制。如果只有缺省用户和组，那么应该先创建一些示例用户与组用于测试。如果在 Windows服务器中已经有自己可用的用户和组，那么就可以用它们来进行测试。

尽管一般性的原则没有改变，但是添加新用户和组的详细步骤还是取决于所使用的是Windows NT，还是具有本地用户和组的 Windows 2000，或者是具有活动目录用户和计算机的Windows 2000。下面的操作步骤适用于在不具有活动目录服务（ Active Directory Services）的Windows 2000 Server中创建本地用户与组。

注意 如果使用的是Windows NT，先单击Start按钮，将鼠标指针指向Programs，再指向Administrative Tools（Common），接着单击User Manager。如果使用Windows 2000管理活动目录用户和计算机，那么先单击 Start按钮，将鼠标指针指向 Administrative Tools，再单击 Active Directory Users and Computers。在User Manager中，创建Windows NT或Windows 2000 Active Directory的新用户和组与在Windows 2000中管理本地用户和组是相似的。

1) 在Windows 2000中，单击 Start菜单，将鼠标指针指向 Programs，在指向 Administrative Tools，然后单击 Computer Management。在 System Tools文件夹中，展开 Local Users And Groups文件夹，如图 11-1所示。

2) 右键单击 Users文件夹，并单击 New User。在User Name框中输入 _jsmith。（这里的下划线用于方便地查找和删除示例用户和组。）在Full Name框中输入 Joe Smith。保留 Password框为空，并选中 User Must Change Password At Next Logon复选框。接着单击 Create按钮。创建了新的用户之后 New User对话框将被清空，如图 11-2所示。

3) 在User Name框中输入第二个示例用户的名字 _mjturner。在Full Name框中输入 Mary Jane Turner。保留 Password框为空，并选中 User Must Change Password At Next Logon复选框。接着单击 Create按钮，并单击 Close按钮。

4) 右键单击 Groups文件夹，并单击 New Group。在 Group Name框中输入 _Budget Analysts。

China-pub.com 下载

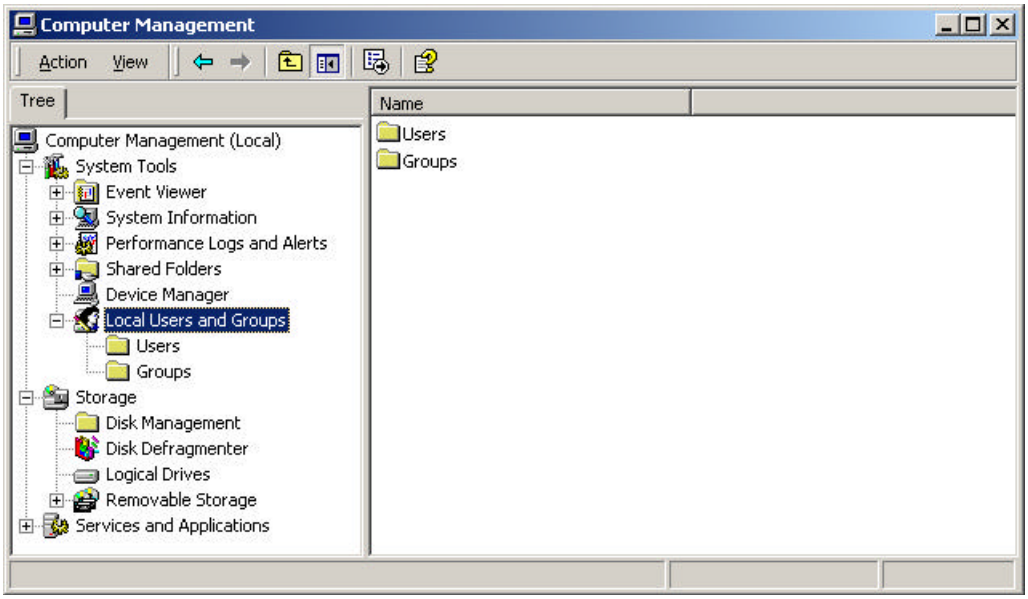


图 11-1

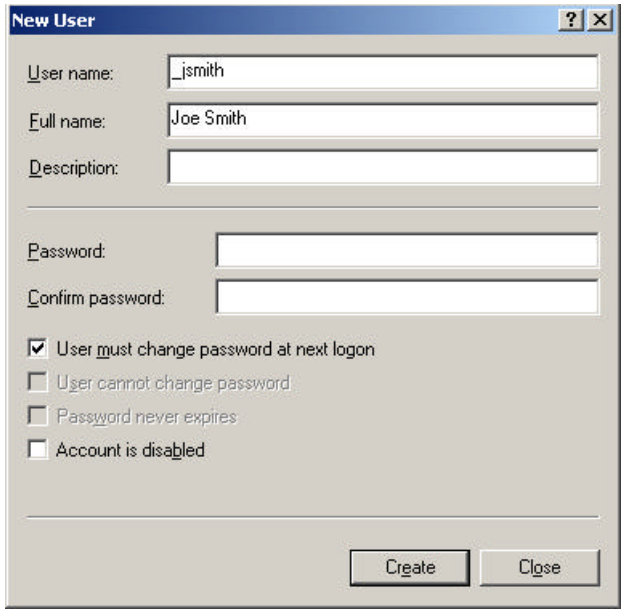


图 11-2

5) **单击** Members**框下方的** Add**按钮。选择** _jsmith**，并单击** Add**按钮，最后单击** OK**按钮，如图**11-3**所示。**

6) **单击**Create**按钮创建新的组。接着继续创建第二个组，在** Group Name**框中输入** _Budget Reviewers**。**

China-pub.com
下载

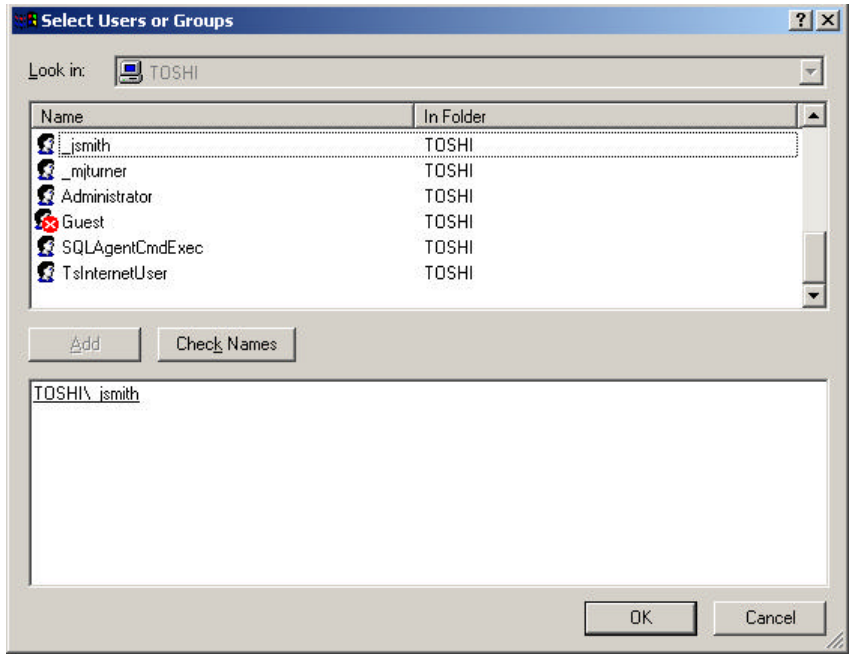


图 11-3

7) **单击** Members**框下方的** Add**按钮。单击** _jdmith**，按住** Ctrl**键同时单击** _mjturner**，接着单击** Add**按钮并单击** OK**按钮。单击** Create**按钮创建新的组，然后单击** Close**按钮关闭** New Group **对话框，如图** 11-4**所示。**

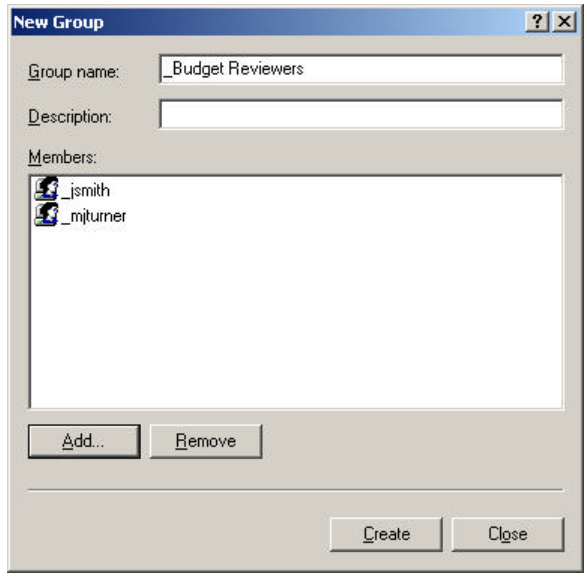


图 11-4

China-pub.com 下载

8) 关闭Computer Management窗口。

重点 学习完本章后，应该把这些示例用户和组删除。

只有将创建的新用户和新组明确地添加到指定的数据库中它们才会生效。当然，在现有的OLAP Administrators组中添加用户账号将改变能够运行 Analysis Manager应用程序并且能够在无安全限制的条件下浏览立方体的人员。

2. 为所有用户创建角色

创建新数据库和立方体时，将会自动地获得一个隐藏的内部角色，该角色赋予 OLAP Administrators组成员所有权力，并允许管理员使用 Analysis Manager。客户端立方体浏览器应用程序能够浏览属于 OLALP Administrators组的用户提供的立方体。不属于 OLAP Administrators组的用户是没有任何权力的，既不能够管理立方体，也不能浏览立方体。如果你创建了一个立方体并允许其他用户访问，他们还是无法浏览 cube的任何内容。

在许多情况下，你需要让所有的用户浏览立方体，却又不能让他们使用 Analysis Manager。要实现这一点，就必须创建新的角色。

1) 在Analysis Manager控制树中，展开 Chapter 11 OLAP数据库和 Cubes文件夹，右键单击Sales立方体，并单击 Manage Roles，如图11-5所示。

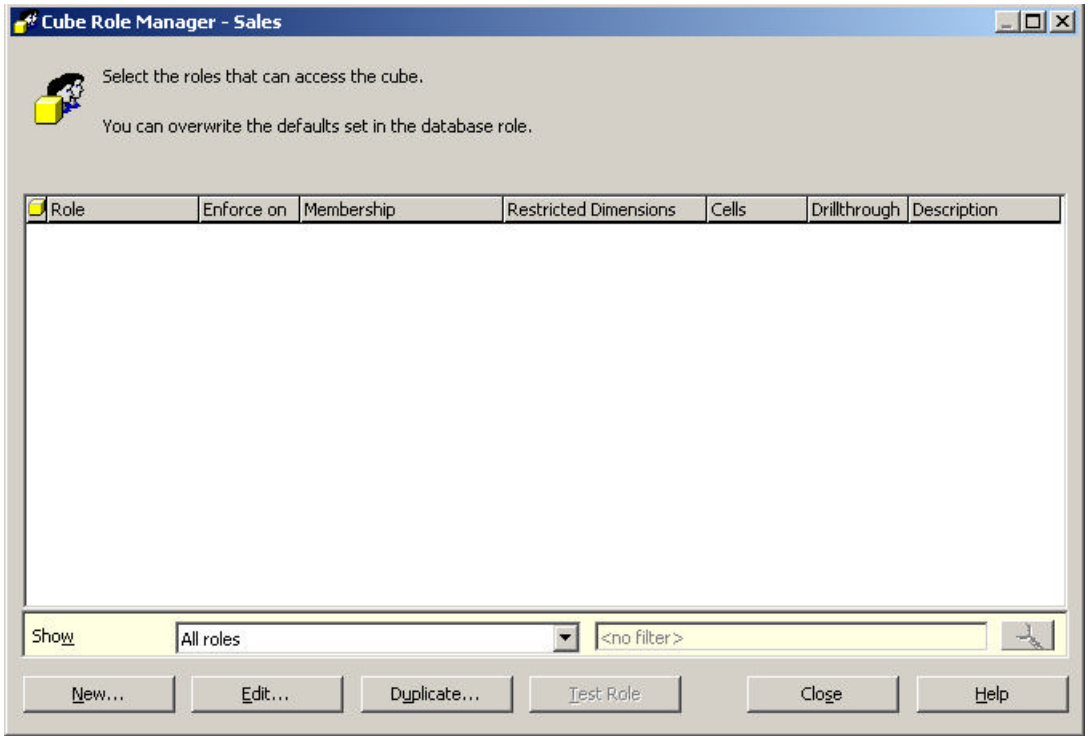


图 11-5

执行上述操作后将弹出 Cube Role Manager对话框，该对话框显示数据库中现有的所有角

需要全本请访问 www.ertongbook.com

China-pub.com
下载

色。同时，它也允许你创建新的角色。

2) 单击对话框底部的 New按钮。在弹出的 Create A Cube Role对话框的 Role Name框中输入All Users，如图 11-6所示。

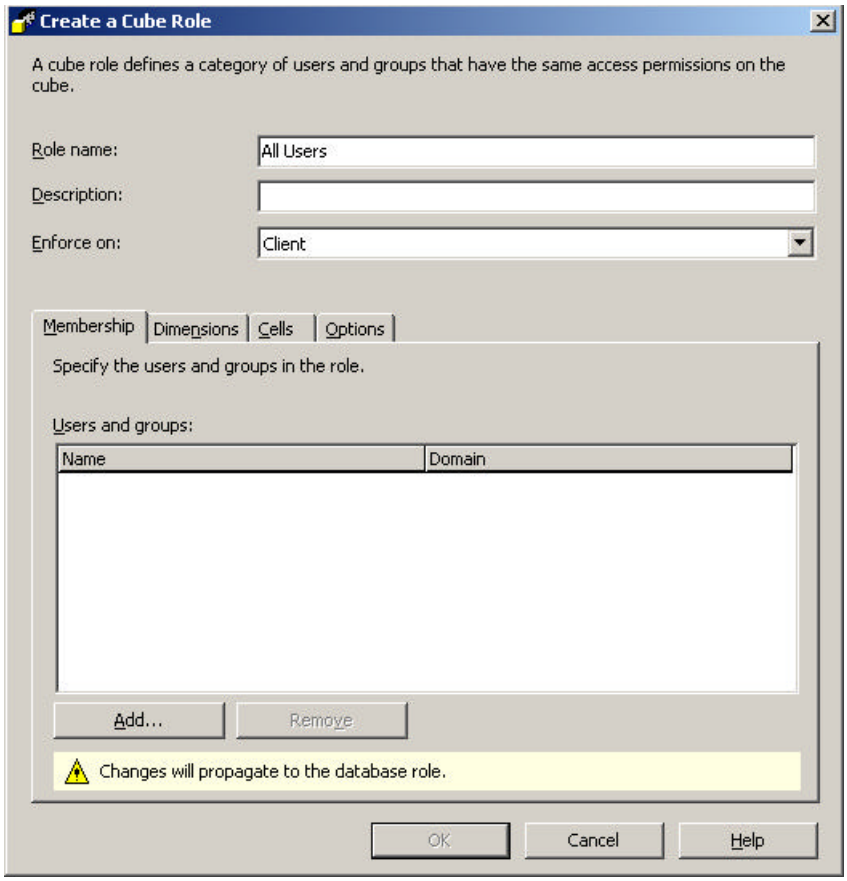


图 11-6

一个角色可包含一个或多个来自于操作系统的用户和组。在角色中添加用户和组之前，这些用户和组必须已经存在。

3) 单击 Add按钮，如图 11-7所示。

Add Users And Groups对话框显示当前服务器中所有可用的组。如果需要，可从 List Names From下拉列表中选择其他的服务器。在缺省情况下， Names列表中只显示组。如果你还要显示用户的话，单击 Show Users按钮即可。一般来说，使用组可以更容易地管理安全机制，因为没有必要在某个用户来时或离开时频繁进行修改。对于新的 All Users角色，需要应用于所有的用户。标准的 Everyone组指的是任何连接到服务器上的用户。

4) 单击Everyone，并单击 Add按钮将该组名字添加到 Add Names列表中，然后单击 OK按钮。

注意 仅仅选择组还是不够的，还必须单击 Add按钮将组名字添加到Add Names列表中。

China-pub.com 下载

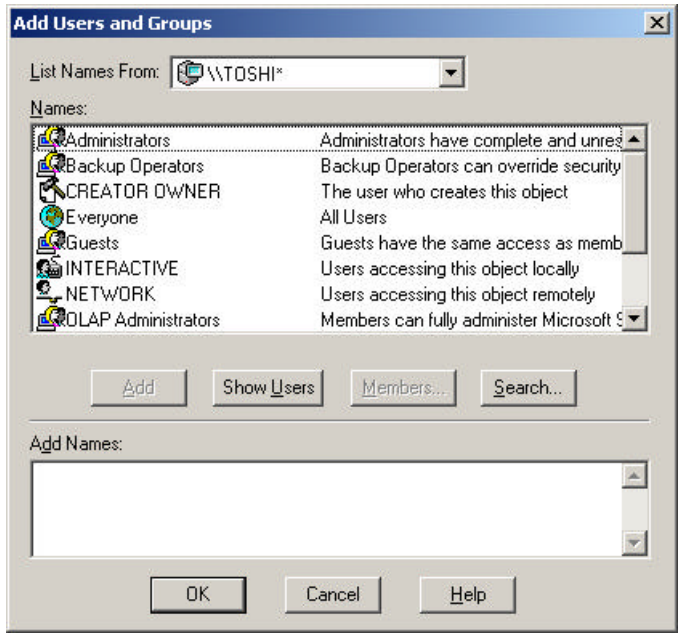


图 11-7

添加组之后， Create A Group Role**对话框的** Membership**选项卡显示组成该角色的用户和组。你还可以使用** Remove**按钮删除某些用户或组。单击** Add**按钮将弹出** Add Users And Groups**对话框，如图** 11-8**所示。**

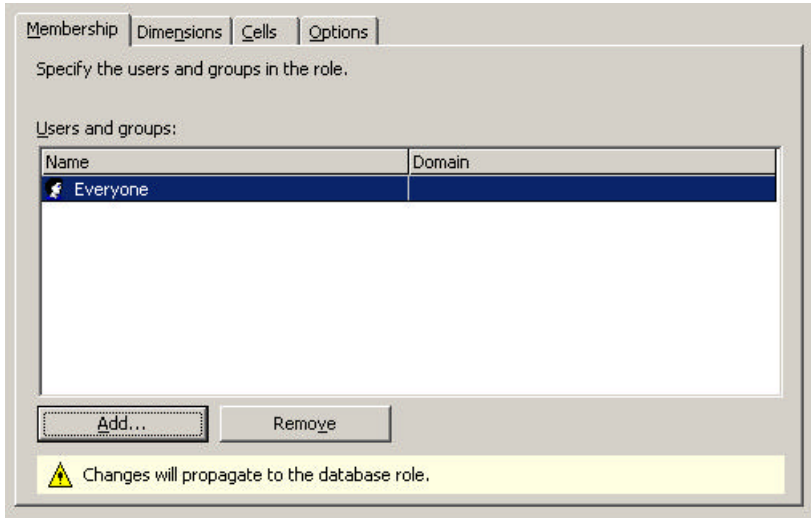


图 11-8

5) **单击**OK**按钮结束创建角色过程。**

China-pub.com
下载

Cube Role Manager对话框中显示新创建的角色，如图 11-9所示。

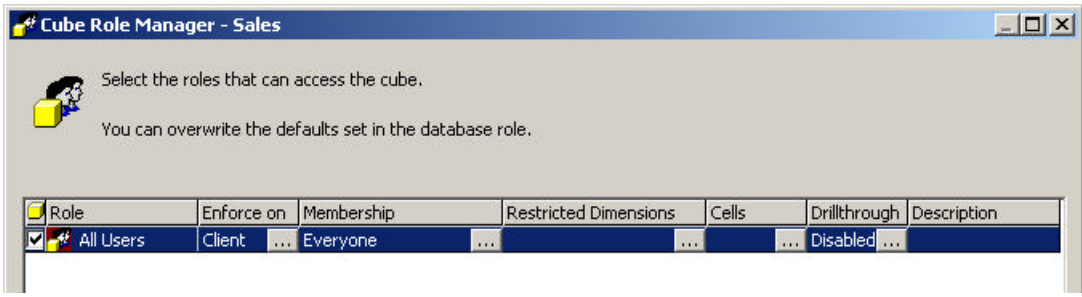


图 11-9

6) 单击Close按钮关闭对话框。

现在，Sales立方体可被任何连接到服务器上的用户浏览。如果你打算使所有 OLAP立方体都能够被你公司的成员自由访问，上述操作步骤就是你需要知道的有关 Analysis Services中安全机制的全部内容。

3. 在数据库层次创建角色

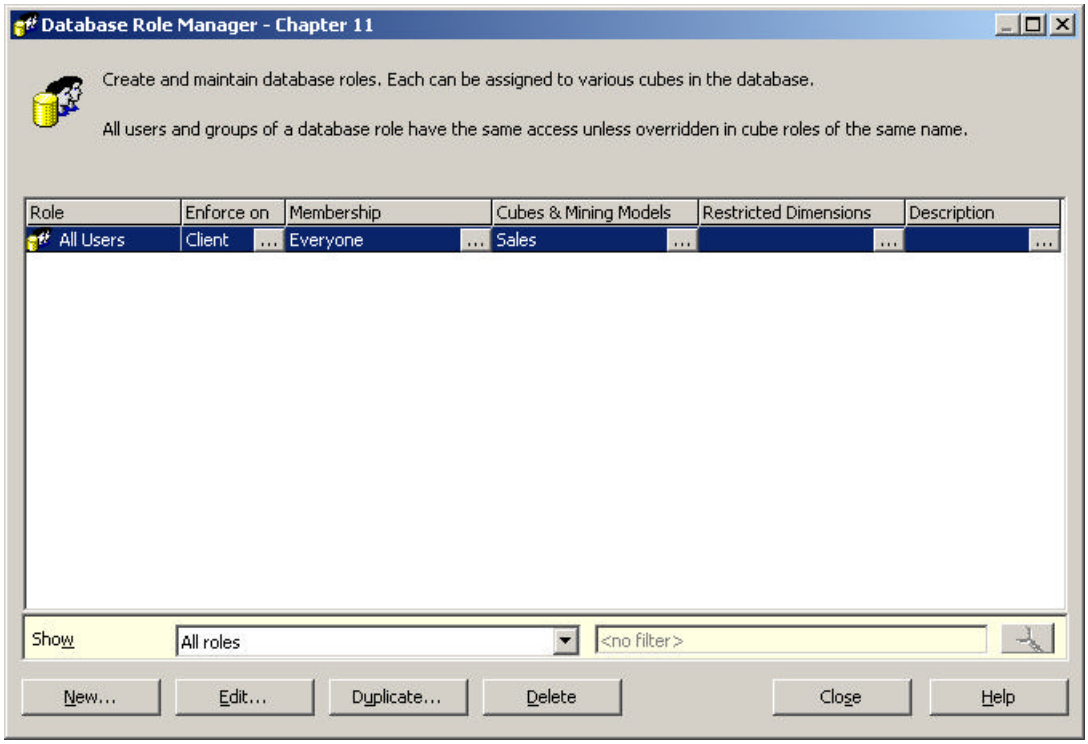


图 11-10

有些立方体中的内容不能让所有的用户使用。要限制不同用户的访问权限，则必须创建

China-pub.com 下载

新角色，并将指定的用户和组放置到该角色中。角色总是存在于数据库层次，即使你创建新的立方体角色，实际上也是创建了新的数据库角色。不管数据库中的哪个立方体使用该角色，它都包含相同的用户和组（也就是说，具有相同的 Membership）。可以直接在数据库层次中创建角色，然后按所需将这些角色应用于立方体中。在这一节中，将为预算分析员和预算审阅者创建角色。

1) 在控制树中，右键单击 Chapter 11 OLAP数据库下的 Database Roles对象，然后单击 Manage Roles，如图 11-10所示。

Database Role Manager对话框看起来与 Cube Role Manager对话框十分相似。两者都显示数据库中现有的角色。可以看到，在 Sales立方体中创建的 All Users角色也显示在数据库角色列表中。可以使用 Cube Role Manager来创建新的数据库角色，但是却必须使用 Database Role Manager来删除数据库角色。继续往后学习，你将会了解更多有关这两个角色管理器的相同点和不同点。

2) 单击New按钮开始创建新的数据库角色。在 Role Name框中输入 Budget Analysts，并单击Add按钮在角色中添加新的组。

3) 选择 _Budget Analysts组或其他想要选择的组，然后单击 Add按钮，如图 11-11所示。

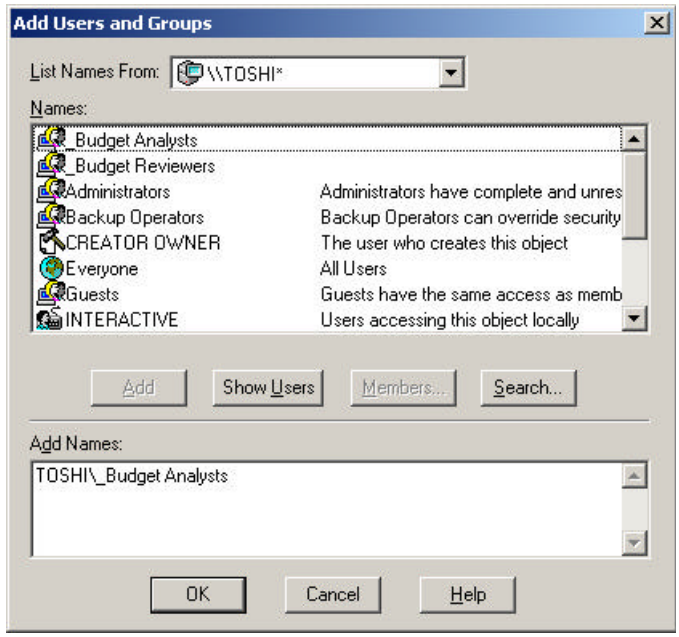


图 11-11

4) 单击OK按钮在角色成员关系中添加组。单击 OK按钮创建角色，如图 11-12所示。

对话框底部显示一条信息，告诉你角色成员关系的改变将会传播到使用该角色的立方体。角色对于数据库来说是整体共用的，但是也可被数据库中的一个或多个立方体使用。成员关系是角色内在固有的，而且对该角色的所有使用都是相同的。

China-pub.com
下载

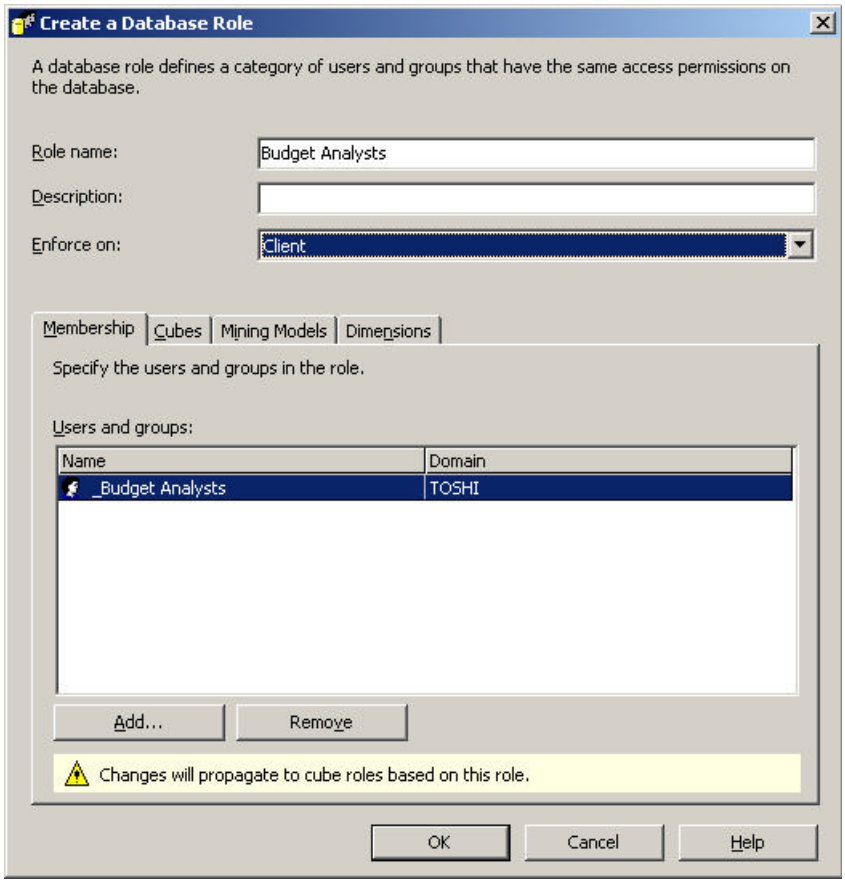


图 11-12

注意 Create A Database Role对话框中有一个名为Enforce On的下拉列表。该下拉列表中有两个值：Server和Client。在第1章“数据分析基础”的“分析服务用户工具”一节中讲述过，PivotTable Service组件保留客户端计算机数据的高速缓存。这个高速缓存使得获取数据更加快速并使网络流量最小化。当你使用安全机制时，客户端高速缓存中的一些数据将受限制。如果你选择客户端强制性安全机制，PivotTable Service将会决定客户端是否能够使用高速缓存中的数据。但是一般来说，受限制的数据将忽略网络连接。网络连接使得某些蓄意破坏人员有可能中途阻止数据的传输。如果你在服务器上选择强制性安全机制，则可以有效地使用客户端高速缓存。客户端的强制性安全机制更加有效，但是与服务器上的强制性安全机制相比安全性稍差一些。

5) 单击New按钮，输入Budget Reviewers，并单击Add按钮。选择_Budget Reviewers操作系统组（或依据所需选择其他的组）。单击Add按钮后，单击OK按钮，如图11-13所示。

当创建新的数据库角色时，对话框中将显示Membership选项卡。Membership是角色的详细定义属性。然而，对话框中还有其他一些选项卡。例如，你可以在创建角色时将角色指

China-pub.com 下载

定到立方体中。

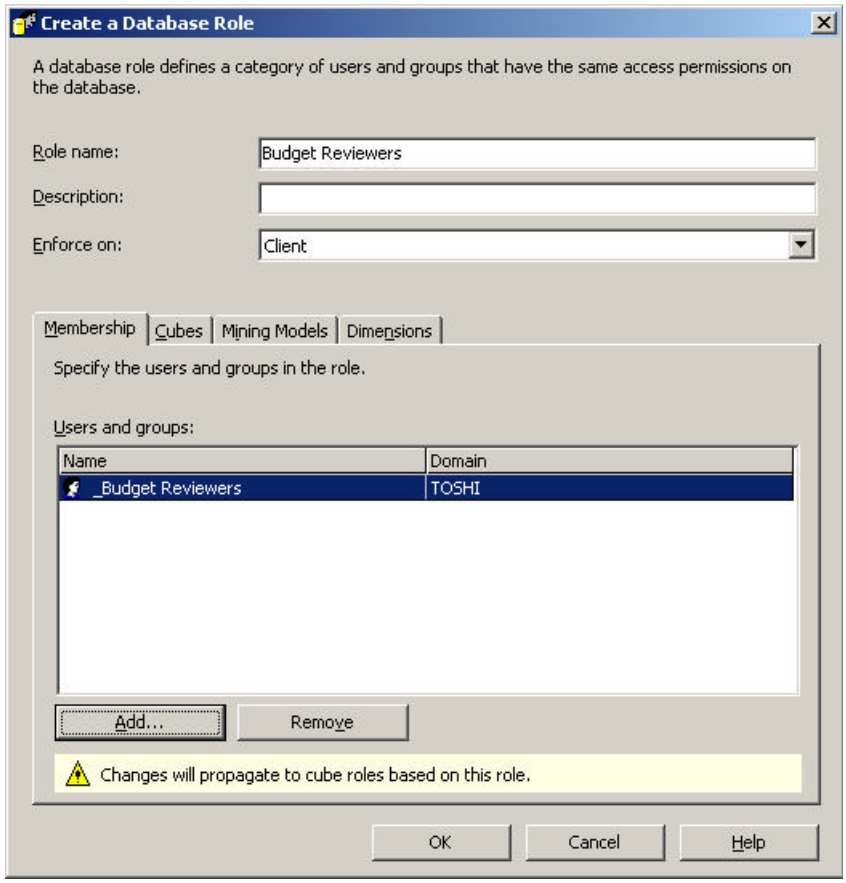


图 11-13

6) 单击Cubes选项卡显示数据库中的立方体列表。单击选中 Finance和Sales复选框，如图11-14所示。

7) 单击OK按钮创建角色，如图 11-15所示。

现在列表中显示所有的 3个角色。正如你在 Cubes & Mining Models列中看到的一样，通常把All Users角色指定到 Sales立方体中，把 Budget Reviewers角色指定到 Sales和Finance立方体中，而 Budget Analysts角色则没有指定到任何立方体。

4. 管理数据库角色

你还可以使用 Database Role Manager来更改现有的角色。例如，如果你需要一个与现有角色稍微不同的角色，那么可以复制现有的角色，然后再对它进行修改。

1) 选择Budget Reviewers，并单击 Duplicate按钮。

新角色与被复制角色之间的唯一不同就是名字，因此系统将提示你为新角色命名，如图11-16所示。

需要全本请访问 www.ertongbook.com

China-pub.com
下载

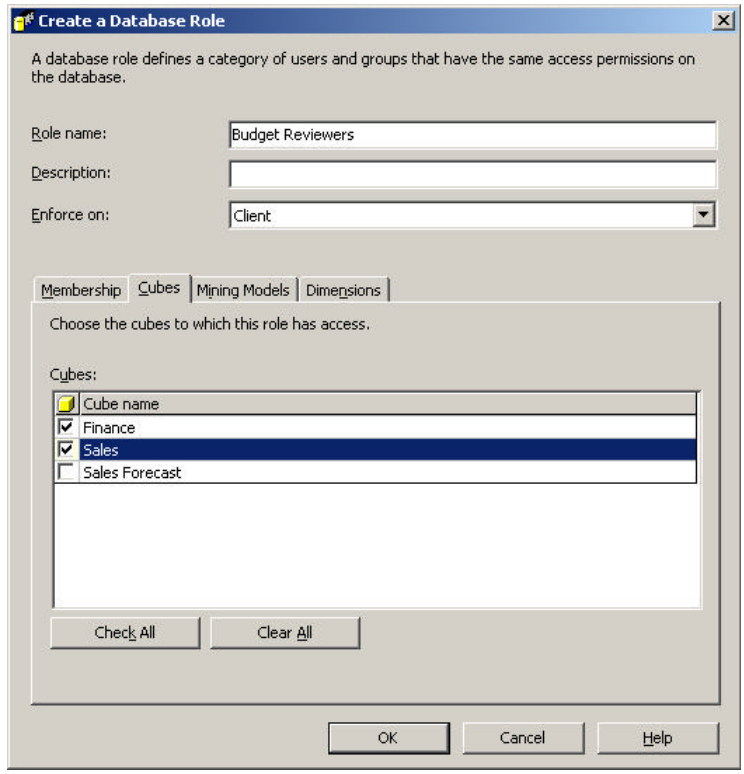


图 11-14

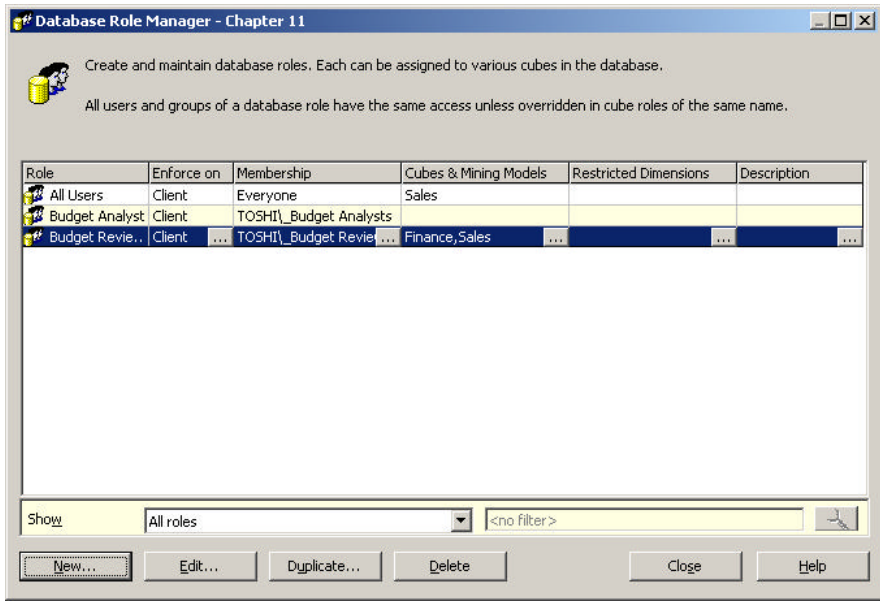


图 11-15

China-pub.com 下载

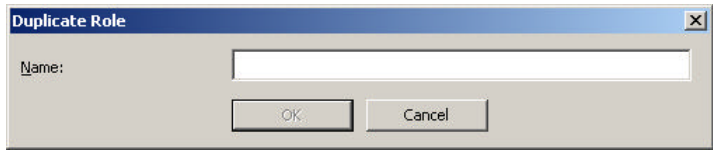


图 11-16

2) 将新角色命名为 Detailed Reviewers，然后单击 OK按钮，如图 11-17所示。

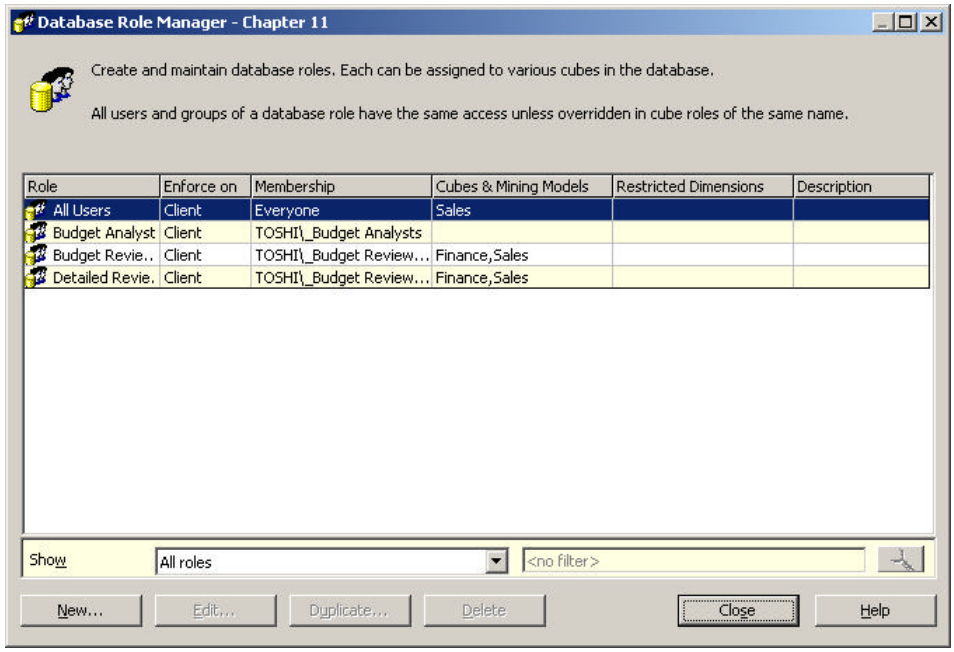


图 11-17

新角色完全是前一角色的复制版本。你可以对其进行编辑修改。

3) 选择 Detailed Reviewers角色，并单击 Cubes & Mining Model列中的省略号（...）按钮。弹出的对话框与 Create A Database Role对话框基本是一样的，只不过对话框标题不同，而且不能更改角色的名字。

4) 清除 Sales立方体复选框，并选中 Sales Forecast复选框，如图 11-18所示。

5) 单击 OK按钮接受对角色的修改。

你也可对现有角色的成员关系进行修改。

6) 选中 Detailed Reviewers角色后，单击 Edit按钮，如图 11-19所示。

单击 Edit按钮后将弹出 Edit A Database Role对话框，之前我们看到过该对话框。仅有这么一个对话框能够定义数据库角色。要进入该对话框可以有以下几种途径：创建新的角色，选择现有角色并单击 Edit按钮，或者选择现有角色并单击某一列中的省略号按钮，单击列中的省略号按钮将提前激活对话框中适当的选项卡。

China-pub.com
下载

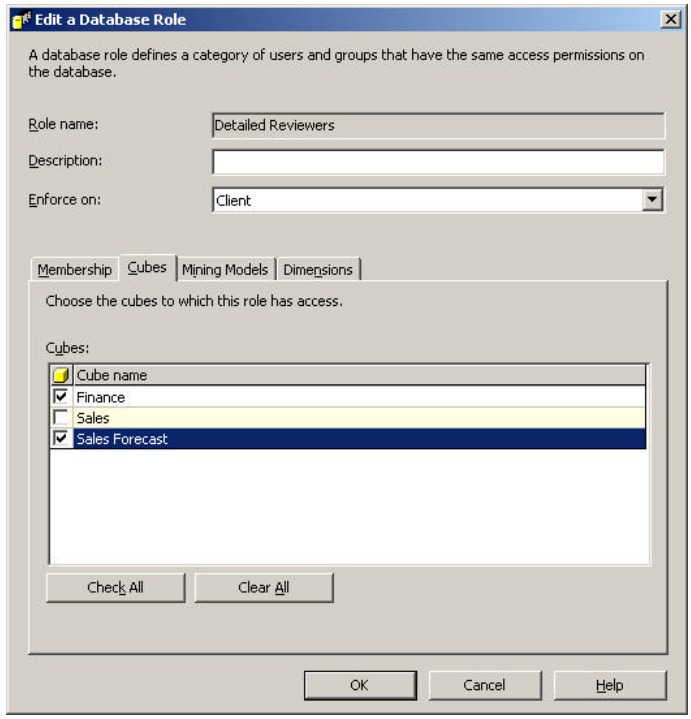


图 11-18

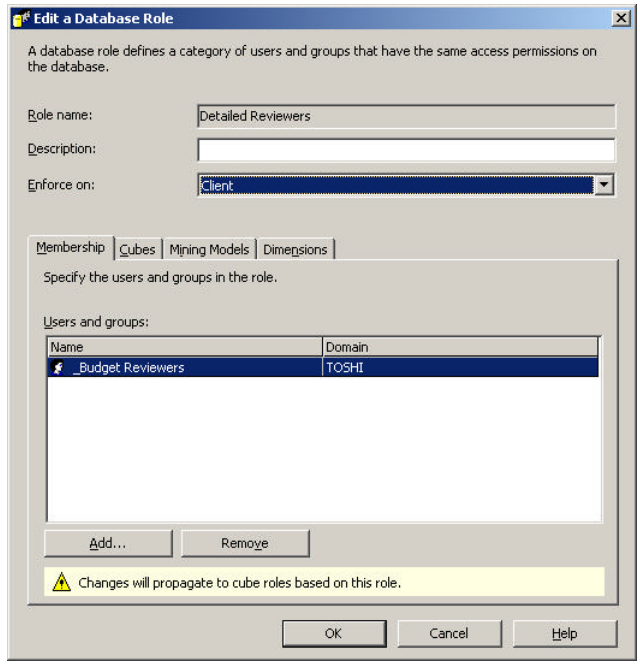


图 11-19

China-pub.com 下载

7) 单击Add按钮，双击 _Budget Analysts（或其他所需的组），然后单击OK按钮。接着单击OK按钮接受修改后的角色定义。

你也可以从Database Role manager中删除角色。

8) 选中Detailed Reviewers角色，单击Delete按钮。当系统要求确认是否删除时单击Yes按钮。单击Close按钮关闭Database Role Manager窗口。

所有数据库都有一个OLAP Administrators组的内部角色，该角色被自动赋予数据库中所有操作立方体的权限。除非你明确创建其他的角色并为其指定立方体，否则只有OLAP Administrators组中的成员能够使用立方体。使用Cube Role Manager创建新角色时，所创建的角色处于数据库层次并自动应用于当前立方体中。使用Database Role Manager创建新角色时，则必须明确地将该角色添加到某个立方体中。缺省角色能够毫无限制地访问所有维的信息，检索任何单元格中的值，但是却不能更改立方体。

11.2 在维中应用安全机制

在立方体层次上应用安全机制只能简单地允许或禁止对整个立方体的访问。这种操作虽然很常用，但是却不够灵活。你可能经常需要让管理人员查看一些其他个人所不允许看到的信息，或者不让市场营销部门中的个人看到制造部门的预算细节。维层次的安全就为你提供了这样一种功能强大而又简单的机制，允许用户访问立方体中的部分内容。

1. 完全限制维

限制对维访问最简单而又最实用的方法就是阻止除高层成员之外的成员对维的所有访问。在本章前一部分，为所有用户赋予了完全访问Sales立方体的权限。但是，你可能不想让所有的用户都看到财政年度的数据。

1) 在控制树中，右键单击Chapter 11数据库的Sales立方体，并单击Manage Roles，如图11-20所示。

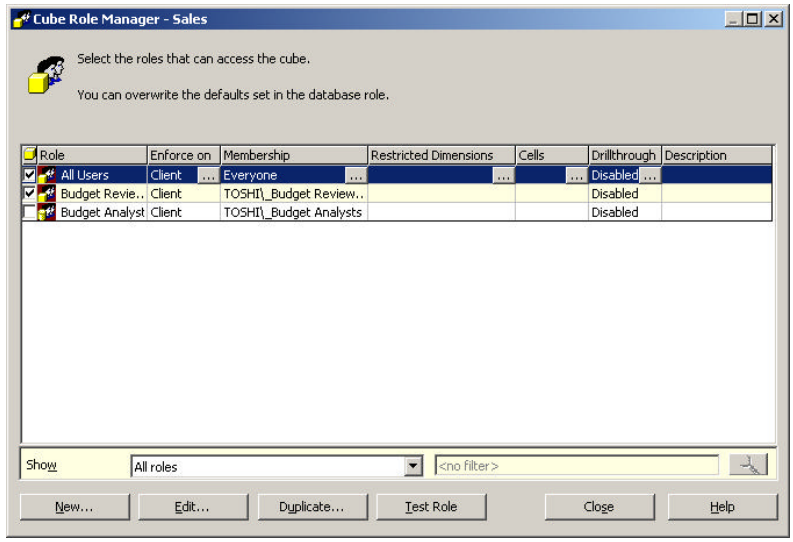


图 11-20

China-pub.com
下载

Cube Role Manager对话框中显示数据库中的所有角色，如果某个角色应用于该立方体，则其复选框被选中。如果要改变某个角色的成员关系，则所作的更改将应用于整个数据库，但是也可以只改变要应用的角色，而不影响其他使用该角色的立方体。

2) 选择All Users角色，单击 Restricted Dimensions列中的省略符号按钮，如图 11-21所示。

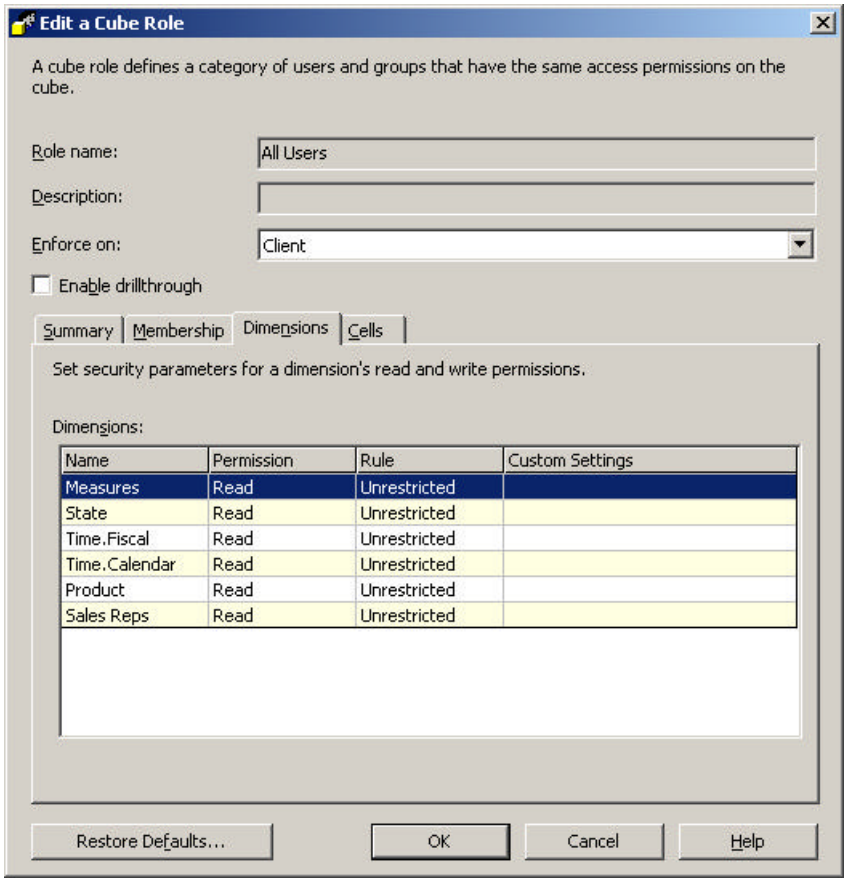


图 11-21

Edit A Cube Role对话框显示立方体中的所有维。每个维的缺省规则允许无任何限制条件的访问。我们可以看到，该对话框与 Edit A Database Role对话框是相似的。这两个对话框都有多个选项卡，而且都可以通过单击列中的省略号按钮或单击主角色管理器窗口底部的 Edit 按钮来显示这两个对话框。

3) 选择Time.Fiscal维，单击 Rule列，从下拉列表中选择 Fully Restricted，如图11-22所示。

4) 单击OK按钮改变维规则。

Cube Role Manager允许你像是以角色成员登录一样浏览立方体，这对于测试角色的行为是极大的方便，因为你不需要在两台计算机上进行操作，或者以不同用户身份进行连续的登录。

China-pub.com 下载

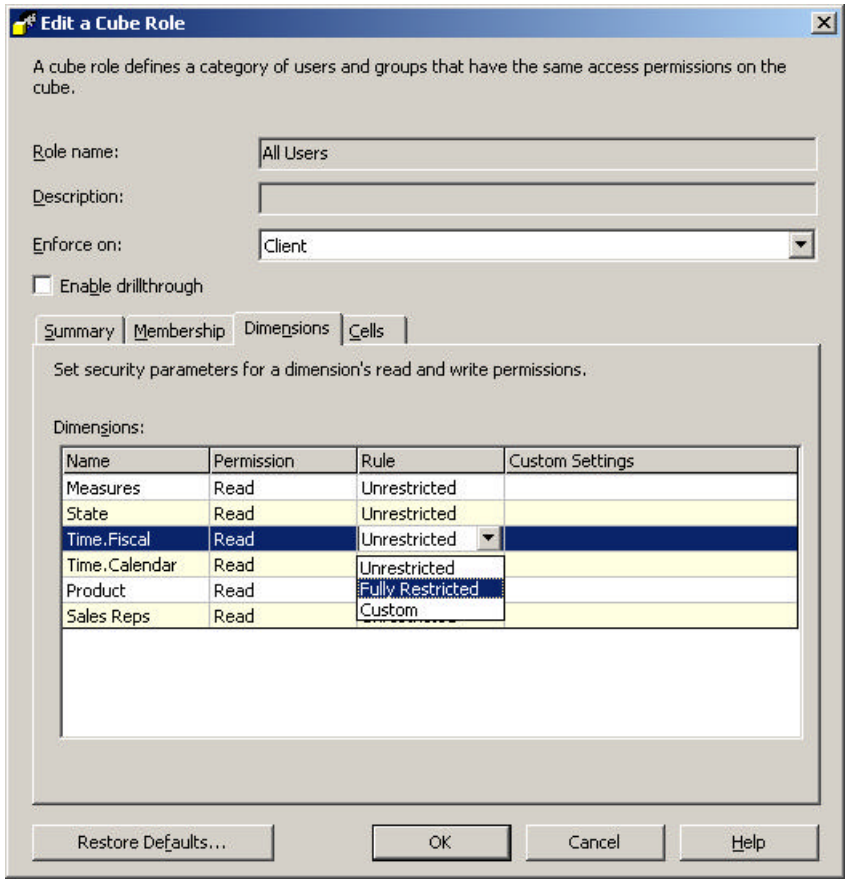


图 11-22

5) 单击Test Role按钮。如有必要可改变立方体浏览器的大小，如图 11-23所示。

Time.Fiscal维仍然是可用的。使用安全机制限制对维的访问并不会删除该维。如果要从浏览器中完全删除某个维，那么可使用第 4章“高级维与立方体”的“从立方体中删除维和量度”一节中讲述的虚拟维。但是，安全机制将限制你在维中可查看的成员。

6) 单击Time.Fiscal维下拉列表，如图 11-24所示。

All Time成员是维中唯一可用的成员。维安全机制有效地为属于 All Users角色的用户删除了其他所有的成员。

7) 按Esc键关闭立方体浏览器窗口。

2. 限制维的成员

你可能需要运行一组用户查看维的某一部分，而不是整个维。角色的维可使你实现这一点。例如，假设让所有的用户只能够查看产品类别和子类别的销售图表，而不能查看单个产品的销售图表。

1) 在Sales立方体的 Cube Role Manager中，选择 All Users角色，单击 Restricted Dimensions

需要全本请访问 www.ertongbook.com