小议M QLServer2000的安全及管理 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/460/2021_2022__E5_B0_8F_E8_AE_AEM_QL_c98_460912.htm 通俗地讲，资料库是储存具有某些特性的资料的数据库。通常，我们把使用资料库系统的用户划分为四类，资料库设计者、资料库管理者、应用程序设计者及一般使用者。其中资料库管理者负责账号的管理与维护，决定所有资料库使用者的使用权限。资料库安全管理可说是资料库管理者最重要的工作。sql server是microsoft的企业级资料库，它是个功能强大、易于使用的资料库，可直接与windows nt/2000的使用者账号做安全机制整合。 那么，到底什么是安全管理呢？简而言之，安全管理是指对需要登入服务器的人员进行管理。在应用程序中，我们会对资料库的各类使用者设置资料操作权限，通常是直接在应用程序中做账号与密码的管理，但这种做法需要撰写程序控制。而sql server具有亲切、易操作的图形使用界面，可以方便地管理使用者对sql server的存取权限。 sql server 安全管理可分为3个层次，即登入账户、资料库的管理与连接特定资料库的权限和使用者对所连接资料库部分的操作权限。下面，我们将针对这3个层次做详细说明。一、登入账户 任何需要存取 sql server 的使用者皆需要有一组服务器认可的账户和密码。sql server支持2种登入方式，一种为windows验证，另一种为sql server验证。前者只要在sql server中建立与windwos nt/2000对应的登入账户，让使用者登入windows nt/2000时所用的账户能与在sql server中的账户相互对应，即可顺利连上sql server，由此，我们完成了对windows nt/2000安全管理机制的整合。 接下来，

资料库管理者在windows nt上登入账号，可直接将windows nt中的群组加到sql server中，从而成为一个登入账户。 通过上述操作，windows nt登入群组中的成员皆可连接sql server。如果该群组中某一成员不允许其登入sql server，可在sql server中将该成员的个人账户设为拒绝存取。如果把sql server安装在windows 95、windows 98或windows me中，则无法使用windows验证方式。 如果使用sql server验证，必须在sql server中为要连接sql server的使用者建立登入的账号名称和密码，这些账号和密码与windows nt/2000的账户无关。二、管理与连接特定资料库的权限 在建立登入账户后，使用者便能进入sql server中，但并不代表使用者有连接sql server特定资料库的权限，必须对使用者或群组设置对sql server的操作权限。sql server中对资料库的操作权限可分为服务器自身的操作权限与资料库的存取权限。对sql server的操作权限可由服务器角色来设置，资料库的存取权限则可由角色与使用者对个别表格的存取权限来设置。那么，服务器角色与角色之间有什么不同呢？ 1. 服务器角色 sql server系统内建8种服务器角色(可把角色想像成windows nt账号中的群组)，它不能更改或新增。当对某一使用者或群组设置好服务器角色后，其便拥有该服务器角色所拥有的权限。服务器角色是将sql server的各项管理工作加以分类，如建立账号和资料库备份等，它与资料库角色不一样，后者为对个别资料库的操作权限。 我们简单列出8种服务器角色所拥有的权限。 system administrators 表示系统管理员可执行任何动作。 security administrators 表示管理登入账户。 server administrators 表示设置sql server的各项参数。 setup administrators 表示有关replication(复制)的设置与管理扩充预

存程序。 process administrators 表示管理sql server所有执行中的程序。 disk administrators 表示管理资料库文件。 database administrators 表示建立和更改资料库属性。 bulk insert administrators 表示对可执行bulk insert操作的管理。 2. 角色 sql server内建10种资料库角色，它不能更改或删除，但可对个别资料库增加角色。若给予使用者有内建角色中的资料库拥有者权限，它便拥有该资料库的完整操作权。其余各角色的详细权限说明可参考sql server的bol(即sql server books online)，通过查询关键字roles，进入标题为roles的项目，其中有包含内建服务器角色与资料库角色的完整说明，在此不多赘述。需要注意的是，在对使用者分别设置了各种角色(每一使用者或群组可具有多种角色)后，它便拥有所有角色联集的权限，但若其中有某一角色对某一操作权(如对某一表格的0select权)设置了拒绝，它将失去了该项权限，换句话说，拒绝权限优于授予权限。三、资料库中部件的存取权限 对于sql server的管理与可连接特定资料库的权限，由sql server所提供的服务器角色与资料库角色基本上可以符合我们大部份需求。另外，可直接对使用者或群组设置对资料库中部件的个别存取权限，这些个别的存取权限有0select、insert、0update、0delete、exec和dri，其中exec与dri分别表示对预存程序的执行权限和对表格有效性的验证权限。在做直接的权限设置时，我们也可针对特殊的使用者(如内建资料库角色不能满足时)，当然，如果使用相同权限方式的用户比较多时，可以增加一个符合需求的资料库角色，或将这些使用者在windows nt/2000上先归于某群组，再对该群组设置权限，这样做比较方便于管理与维护。 除上述内容之外，在实际运行时，笔者对于资料库安

全的把关总结出以下几点建议。 1. 除非必要，否则尽量以windows验证来管理可连接sql server的使用者，以整合windows nt/2000的安全机制。 2. 善用sql server的服务器角色与资料库角色功能。 3. 善用sql server的加密功能。 sql server提供了登入账号、网络传输、虚拟表和预存程序的加密功能。其中账号的密码加密是预设的，而网络间传输资料则可用ssl方式进行加密，要启动此功能必须启动net-library的加密功能，同时要配合windows 2000的ca功能，并在服务器端与用户端设置完成，从而双方在传输资料前，便会在ssl加密后再进行传输。由于虚拟表和预存程序的定义是以明码保存在系统资料表中，若要将虚拟表和预存程序加密，可在其建立时在enterprise manager中设置加密选项或以 alter 叙述来设置加密。 4. 系统安装完毕后，务必更改预设的sa密码，免得有其他使用者"义务"管理您的sql server。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com