中国广东·某某某核电运营管理有限公司

第 1 版

闭环访客系统

维 护 手 册

闭环访客系统

维护手册

【编写目的】

本文档仅供[某某系统]的系统管理员安装配置系统时参考使用，其中主要涉及软件系统安装及客户端配置、数据库配置与维护等内容说明。

【文档安全级别】

级别类型	级别代号	级别描述	本文档隶属级别
绝密	★★★★	仅对少数系统开发人员可知	
机密	★★★	系统管理员可知	√
一般	★★	少数用户可知	
公开	☆	普通用户可知	

2023 年 12 月

目录

第 1 章

主要内容：简单介绍某某系统

第1章 系统简介

闭环访客系统是为实施闭环访问管理而设计的软件系统，该系统采用浏览器/服务器模式；不同物理位置的用户可以通过浏览器访问 Web 服务器，实现分布式管理。

系统登录界面如图 1-1。

图 1-1 系统登录界面

登录系统后，菜单界面如图 1-2。

图 1-2 系统菜单界面

第 2 章

主要内容： 快速安装部署软件系统

第2 章 系统快速安装

本节介绍如何快速安装焊接技术管理系统。该系统基于 B/S 模式，需要 Web 服务器支持；客户端基于浏览器模式访问服务器站点。

2.1 服务器安装

2.1.1 服务器硬件环境

处理器： CPU Xeon 2.6GHZ 或以上，建议配置双路 CPU
内存 2GB 或以上
硬盘 120G 以上
网卡 100M

2.1.2 服务器软件环境

步骤 1：安装 Window Server 2003 操作系统
步骤 2：完全安装 office2003
步骤 3：完全安装 SQL Server 2000 数据库管理系统(必须是企业版)
步骤 4：安装 IIS(Internet Information Server，微软提供的 Web 服务器

2.1.3 服务器应用程序安装

2.2 数据库配置

2.2.1 数据库初始化

【基本步骤】

步骤 1：创建数据库 visite_system,建表 build_appointment，car_long_appointment，car_long_record，car_short_appointment，car_short_record，common_appointment，common_record，dept，enter_record，user，vip_appointment，vip_examine

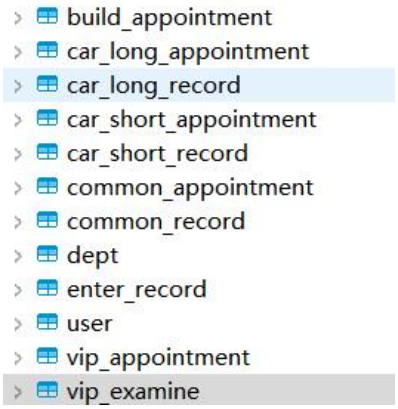

图 2-1

步骤 2：利用查询分析器，打开提供的数据库脚本文件，按照编号依次执行，完成数据库创建及数据初始化工作。

2.2.2 添加访问用户

【前提条件】SQL Server2000 数据库安装成功。

【基本步骤】

步骤 1：打开 SQL Server 企业管理器

点击　开始—>程序—>Microsoft SQL Server—>企业管理器 如图 2-2 所示。

步骤 2：打开图 2-2 所示控制台根目录“安全性”按钮，添加一个用户。

用户名：15295707696

密码　：123456

步骤 3：设置用户名 cgnpc 的属性，指定能够访问的数据库为：

2.3 客户端配置

(1) 客户端软件

- 确保安装 pdf 浏览工具 Adobe Reader 9.0 及以上；
- Internet Explor 6.0 及以上。

(2) 设置 IE，允许弹出窗口。

焊接管理系统登录页面需要弹出窗口，如果用户机器中安装了具有弹出窗口拦截功能的软件，将使得页面无法正常打开，功能无法正常被执行。为了正常使用本系统，您需要关闭弹出窗口拦截功能。

目前可以拦截弹出页面的软件很多，我们列举了一些常用的拦截弹出页面的软件的解决方法，您可以根据您的情况选择对应解决方法。具体如下：

(一) Windows XP SP 2 允许弹出窗口解决方法

下面向您讲述如何在运行 Windows XP Service Pack 2 的计算机上如何打开弹出窗口阻止程序：
首先判别操作系统：右键点击桌面上“我的电脑”图标，然后选择“属性”。

随后弹出“系统属性”对话框，如下图所示，从这来判别操作系统的版本：（从图中可以看出这是：Windows XP Professional SP2 操作系统）

当打开另一张网页时，如果出现如下图所示的拦截条时，请右键点击该条，在弹出的下拉框中选择‘总是允许来自此站点的弹出窗口’，然后刷新网页。如下图所示：

或者使用如下方法允许网站的弹出窗口，强烈推荐方法三，可以一劳永逸：
方法一：
1. 在 IE 浏览器的“工具”菜单上，指向“弹出窗口阻止程序”，然后单击“启用弹出窗口阻止程序”。

方法二：从“Internet 选项”配置弹出窗口阻止程序，请按照下列步骤操作：
1. 在 IE 浏览器的“工具”菜单上，单击“Internet 选项”。
2. 单击“隐私”选项卡，然后清除“阻止弹出窗口”复选框以关闭弹出窗口阻止程序。
3. 单击“应用”，然后单击“确定”。

方法三：可以通过将某个网站添加到“允许的站点”列表中，从而允许在该网站中打开弹出窗口。为此，请按照下列步骤操作：
1. 在 IE 浏览器的“工具”菜单上，指向“弹出窗口阻止程序”，然后单击“弹出窗口阻止程序设置”。
2. 在“要允许的网站地址”框中，键入网站的地址（v.noahedu.com），然后单击“添加”。
3. 单击“关闭”。
4. 或在方法二的第二步时，选择“设置”，在“要允许的网站地址”框中，键入网站的地址（v.noahedu.com），然后单击“添加”-“关闭”-“确定”。

（二）针对 MSN 搜索工具栏的解决方案

从下图中可以看出，在地址栏的下方有‘已经阻止了弹出窗口显示’拦截条(这是系统自带的拦截功能)

直接单击该拦截条就出现了“允许弹出窗口显示”的提示，然后刷新网页。此时就失去了拦截功能，如图所示：

或是点击拦截条边的“倒三角形”，在下拉框中选择“允许此站点的弹出窗口显示”，然后刷新网页。

（三）针对“上网助手”的解决方案

打开一个新的浏览器窗口，在窗口上方查看是否有上网助手的工具条。如果没有，依次点击窗口菜单项“查看”=>“工具栏”=>“上网助手”，使上网助手的工具条显示出来。

点击上网助手工具条上的“已拦截:xx ”按钮，再点击“广告拦截设置... ”菜单项，打开广告拦截设置窗口。

在广告拦截设置窗口中，取消“拦截弹出广告”选项的选中，然后点击“确定”按钮。

“上网助手”的弹出窗口拦截功能已被取消。

(四) 针对“百度搜霸”的解决方案

打开一个新的浏览器窗口，在窗口上方查看是否有百度搜霸的工具条。如果没有，依次点击窗口菜单项“查看”=>“工具栏”=>“百度超级搜霸”，使百度搜霸的工具条显示出来。

点击百度搜霸工具条上的“广告拦截”按钮，打开广告拦截设置界面。在界面中取消“拦截弹出窗口广告”和“拦截弹出插件广告”选项的选中。

向下滚动页面，找到并点击“马上设置”按钮。

“百度搜霸”的弹出窗口拦截功能已被取消。

(五) 针对“诺顿网络安全特警”(Norton Internet Security)的解决方案

在界面右下方找到诺顿网络安全特警的小图标，点击右键菜单打开诺顿网络安全特警的主界面。点击“禁止广告”，然后点击右边出现的“配置”按钮，打开“禁止广告”设置窗口。

在“禁止广告”设置窗口”中，取消“启用禁止弹出窗口”选项的选中，然后点击“确定”按钮。

“诺顿网络安全特警”的弹出窗口拦截功能已被取消。

(六) 针对 google 拦截工具条的解决方案(Norton Internet Security)的解决方案

安装完 google 拦截工具条后，会在 IE 地址栏的下方（或周边的某个位置）出现如下图所示的工具栏，图中显示已经拦截了 12 个弹出窗口或页面；

直接点击‘12 个已拦截’这个按钮，此时就转变成“允许显示网站的弹出式窗口”，然后刷新网页。这样弹出窗口或页面将无法被拦截。如下图所示；

(七) 针对 Yahoo 拦截工具解决方案
点击 Yahoo 工具条上的‘倒三角形’图标，然后在弹出的下拉菜单里面将各项打钩去掉，最后刷新页面，即可；如下图所示：

Tips：如果在打开另一张网页时，屏幕只是一闪而过，而且新的页面又没打开，那说明要打开的这张网页已经被拦截了，此时要判断是被哪种拦截工具给拦截了，然后再加以解决，其解决方法基本类似，另外还有一个应急的办法：用手先按住键盘上的 Ctrl 键不放，然后再用鼠标点击“页面上的链接”，这样可以躲过拦截功能。

第 3 章

主要内容： 系统数据库配置、维护等策略

第3 章 系统配置与维护

本服务器可以使用基于 Windows 的操作系统，Web 服务器选择 IIS。

3.1 Web 服务器端配置

3.1.1 运行环境与软件要求

Windows 2000 以上 （不包括 Windows XP Home 版）

IIS 4.0 以上

3.1.2 IIS 的安装与配置

a. 安装 IIS

若操作系统中还未安装 IIS 服务器，可打开“控制面板”，然后单击启动 “添加/删除程序”， 在弹出的对话框中选择 “添加/删除 Windows 组件”，在 Windows 组件向导对话框中选中“Internet 信息服务（IIS）”，然后单击“下一步”，按向导指示，完成对 IIS 的安装。

b. 启动 Internet 信息服务（IIS）

Internet 信息服务简称为 IIS，单击 Windows 开始菜单---所有程序---管理工具---Internet 信息服务（IIS）管理器，即可启动“Internet 信息服务”管理工具

c. 配置 IIS

IIS 安装后，系统自动创建了一个默认的 Web 站点，该站点的主目录默认为 C:\Inetpub\www.root。

用鼠标右键单击“默认 Web 站点”，在弹出的快捷菜单中选择“属性”，此时就可以打开站点属性设置对话框，在该对话框中，可完成对站点的全部配置。

主目录与启用父路径

单击“主目录”标签，切换到主目录设置页面，该页面可实现对主目录的更改或设置。注意检查启用父路径选项是否勾选，如未勾选将对以后的程序运行有部分影响。主目录—配置---选项。

设置主页文档

单击“文档”标签，可切换到对主页文档的设置页面，主页文档是在浏览器中键入网站域名，而未制定所要访问的网页文件时，系统默认访问的页面文件。常见的主页文件名有index.htm、index.html、index.asp、index.php、index.jap、default.htm、default.html、default.asp 等

IIS 默认的主页文档只有 default.htm 和 default.asp，根据需要，利用“添加”和“删除”按钮，可为站点设置所能解析的主页文档。

启动与停止 IIS 服务

在 Internet 信息服务的工具栏中提供有启动与停止服务的功能。单击 可启动 IIS 服务器；单击 则停止 IIS 服务器。

3.2 数据库安全维护

3.2.1 SQL Server 数据库安全性控制

微软在 SQL Server 7.0 整合了太多的自动管理功能——正是这一点，使许多企业都认为它们已经不再需要一个专职的 DBA，而只需让一名 Windows 2000 或 Windows NT 的系统管理员来处理通常由 DBA 负责管理的事务即可。另一方面，企业又将许多机密的信息存储到了 SQL Server 数据库中。如果你是一名 DBA 新手，则需要了解 SQL Server 的安全模式和如何配置其安全设置，以保证“合法”用户的访问并阻止“非法”访问。与以前的老版本相比，SQL Server 7.0 的安全模式有了很大改进，并且与 Windows 2000 和 Windows NT 的安全模式的集成非常紧密。本部分内容针对 Windows NT 4.0 上运行的 SQL Server 7.0，但在 Windows 2000 上的 SQL Server 2000，这些指令和安全问题也同样适用。

安全层次和模式

SQL Server 支持三级安全层次。第一个层次是，用户必须登录到 SQL Server，或者已经成功登录了一个映射到 SQL Server 的 NT 帐号。在 SQL Server 登录成功并不意味着用户已经可以访问 SQL Server 上的数据库。第二层次的安全权限允许用户与一个特定的数据库相连接，第三个层次的安全权限允许用户拥有对指定数据库中一个对象的访问权限。例如，可以指定用户有权使用哪些表和视图、运行哪些存储过程。这种三层次的安全结构与 Windows 2000、Windows NT 安全结构相似，你所掌握的 Windows 安全知识也适用将会对掌握 SQL Server 有很大帮助。

SQL Server 有两种验证模式：NT 安全模式和混合模式。如果你选择的是 NT 安全模式并把 NT 用户登录映射到了 SQL Server 登录上，那么合法的 NT 用户也就连到了 SQL Server 上，不是 NT 合法用户的用户则不能连接到 SQL Server 上。在混合模式中，NT 用户访问 NT 和 SQL Server

的方式与 NT 安全模式下相同，而一个非法的 NT 用户则可以通过合法的用户名和口令访问 SQL Server（当然，合法的 NT 用户也可以通过其他合法的用户名和口令而不通过 NT 登录访问 SQL Server）。除非必须使用混合模式，我们建议使用 NT 安全模式。

如果要查验或改变 SQL Server 系统的安全设置，需要打开 Microsoft Management Console（MMC）中的 SQL Server Enterprise Manager 插件，右击服务器的名字，选择“Properties”，再选择“Security”标签。

如果要改变 SQL Server 系统的安全设置，需要中止 SQL Server 的运行并重新启动它（无需重新启动系统。）。在 SQL Server 的程序文件夹中，选择“Service Manager”，使用它中止 SQL Server 服务并重新启动 SQL Server 服务和 SQL Server Agent 服务（在中止服务器的运行时同时也中止了代理服务的运行）。

SQL Server 的登录和服务器角色

在 SQL Server 7.0 中，可以把一个 NT 组映射到一个 SQL Server 登录上。无需为每个用户添加一个登录脚本，一个允许与 SQL Server 连接的 NT 组中的用户无需输入用户名和口令就可以与一个 SQL Server 连接。SQL Server 根据每个用户各自的 NT SID 而非它们的组 NT SID 对用户进行跟踪，因此即使是通过组连接到 SQL Server 的，在 SQL Server 也可以判断出每个用户的变化。在一个 NT 组中增加用户时，该用户即可自动地拥有对 SQL Server 的访问权，从这个 NT 组中删除用户时，该用户也就失去了对 SQL Server 的访问权限。需要牢记的一点是，当在一个 NT 组中增加用户时，这些用户可以同时获得了对 SQL Server 的访问权限。

考虑到 NT 组和 SQL Server 之间的联系，在设置 SQL Server 安全性时首先需要规划 NT 组和用户策略。如果指定了 NTFS 访问权限，就可以建立一个全局组并将所有用户都放入这个组中，然后可以打开 SQL Server Enterprise Manager，为这个组增加一个 SQL Server 登录。如果是作为一个 NT 系统管理员登录的，就会拥有 SQL Servers 的缺省安全设置，可以以 DBA 的身份登录 SQL Server。

在 Enterprise Manager 窗口的左部，依次扩展 Microsoft SQL Servers、SQL Server Group、你要登录的服务器和“Security”。稍后我们将说明如何用“Logins”条目把 NT 中的组和用户与 SQL Server 连接，非 Windows 用户如何设置用户名和口令。

在 Logins 之下是“Server Roles”条目，在开始添加登录前点击“Server Roles”，熟悉一下各种不同的角色。

这些角色与 NT 的特别操作者本地组（例如服务器操作者和备份操作者）有点类似，它们已经被指派了不同的权限。我们不能增加新的服务器角色，也不能对由 SQL Server 提供的这些服务器角色修改。我们可以把服务器角色看作是本地组。

双击一个角色打开一个标签对话框，可以在一个角色上增加新的登录，观察这个角色的成员和权限。“System Administrators”角色与超级用户等价，可以在 SQL Server 中进行任何操作，为了满足那些真正需要这些权限的用户的需求，应该保留这个角色。你还应该为开发人员指派“Database Creators”权限，使他们可以建立测试性的数据库。你还可以指派给初级管理人员“Security Administrators”和“Server Administrators”权限，以便在没有系统管理员的情况下他们也可以管理服务器的资源和安全性。

在熟悉了服务器角色后，又该来讨论登录问题了。唯一预定义的登录是系统管理员的登录，如果你使用的是混合模式的安全设置，首先你需要键入系统管理员口令。缺省状态下，在安装完

SQL Server 后的口令是空格，双击“Save”按钮，键入新的口令。如果在 NT 安全模式下运行 SQL Server，用户不会被要求提供口令，也就无需在这里建立口令。
要为 NT 组或用户增加新的登录，可以右击“Logins”，选择“New Login”来打开 SQL Server 的登录属性——“New Login”对话框，

你需要做的第一件事是在“General”标签上键入一个名字，无下拉列表的对话框提供了一个可供选择的 NT 组或用户名的清单（在 SQL Server 2000 中也有这么一项功能，但你需要输入一个用户名）。如果输入一个 NT 组或用户名，从下拉列表中选择包含这个组或用户的域。在选择后，域名也将出现在“Name”字段中。

你还可以利用“General”标签来允许或拒绝用户对 SQL Server 的访问。如果某个组中的一个用户无权访问 SQL Server，你可以使这个组的其他成员拥有访问 SQL Server 的权限，而使这个用户不能访问 SQL Server。与在 NT 中一样，拒绝访问权限会覆盖掉这个用户的所有权限以及作为组用户而具有的权限。

一个 SQL Server 登录可以使组或用户拥有与 SQL Server 相连接的权限，但并没有给予组或用户访问任何数据库的权限。你可以利用“General”标签为每个登录设置一个缺省的数据库，但这并不能使它拥有访问这个数据库的权限，它只是表明在组或用户有权限访问数据库时，SQL Server 应该把哪个数据库与组或用户相连接。“Login Properties”属性对话框中的“Separate”标签可以指派数据库的访问权限，可以把组或用户指派给一个服务器角色。

数据库访问

SQL Server 安全性的第二个层次是对数据库访问的控制。SQL Server 可以在一个服务器上支持不止一个数据库，因此你可以使大多数用户拥有访问一个数据库的权限，而没有访问其他数据库的权限。除非你把这个登录作为一个数据库的用户，否则一个 SQL Server 登录没有访问这个数据库的权限。你可以在用户端或数据库端完成这个任务，通过“Login Properties”对话框可以使一个用户拥有对多个数据库的访问权限，此外，还可以在数据库系统上打开“New Database User”对话框，为某个数据库的所有用户添加登录。图 3-10 显示了如何利用“Login Properties”对话框的“Database Access”标签把一个用户添加到一个或多个数据库中。你可以指定一个与登录时不同的用户名，但我们不建议这样做，这样会给系统管理员带来不必要的麻烦。

在添加数据库用户登录时，你可以把这些登录放进数据库角色中，数据库角色是 SQL Server 7.0 中新引进的一个概念。与服务器角色一样，数据库角色与本地组有点类似，它也有一系列预定义的权限，你可以直接给用户指派权限，但在大多数情况下，只要通过简单地把用户放在正确的角色中就会给予它们所需要的权限。一个用户可以是多个角色中的成员，其权限等于多个角色权限的“和”，任何一个角色中的拒绝访问权限会覆盖这个用户所有的其他权限。与服务器角色相同的是，你不能修改预先定义的数据库角色，但可以合并现有的角色以使用户具有它们所需要的安全权限。你可以在任何时候修改角色的成员，但当把一个登录作为一个数据库用户时，无需指派它在所有角色中的登录。

公用数据库角色与 NT 中的“Everyone”相似。SQL Server 把所有指派了数据库访问权限的登录放在公用角色中，你既不能从公用角色中移去用户，也不能删除用户。缺省情况下，公用角色对你所创建的任何数据库没有访问权限。

把需要从数据库中读取数据的用户放入 db_datareader 角色中，对数据库中的数据进行更新操作的用户必须被同时放入 db_datareader 和 db_datawriter 两个角色中。如果一个 NT 组需要对一个

数据库进行访问而其中的一个用户却无须访问这个数据库，你就可以把这个组的 SQL Server 登录放入 db_datareader 和 db_ datawriter 角色中，而把这个用户的登录放入 db_denydatareader 和 db_denydatawriter 角色中。

使用 db_datareader 和 db_datawriter 角色会带来一些潜在的问题。一些数据库使用视图来强化安全性，视图是一种预定义的允许用户浏览的数据。例如，一个视图是一个表中的数据的子集，可以显示一些字段而隐藏另一些秘密的字段。在使用视图强化安全性时，你没有直接给予用户访问数据库的权限，而是给用户指派了访问特定的视图权限，你不能使用 db_datareader 和 db_datawriter 角色，因为这些角色会使用户拥有访问所有数据库、表的权限。

你可能希望委托一些数据库的管理权限。两个数据库角色可以交换这些角色中成员的有限的权限。db_accessadmin 角色中的成员可以把一个现有的 SQL Server 登录添加为一个数据库用户，db_securityadmin 角色中的成员可以向用户指派对表、视图等对象的权限。如果你希望一个人能完成两项任务，可以在两个角色中添加他的登录。

db_backupoperator 角色的概念与 NT Backup Operator 类似，这个角色中的成员只能在进行备份操作时读取数据，而可能没有其他的访问权限。db_backupoperator 角色可以对一个数据库进行备份但不能对它进行恢复，这个工作需要 DBA 或数据库所有者来完成。

如果你有一个测试或开发用数据库，或者你需要对一个数据库进行修改，开发人员的登录需要登录被放在 db_ ddladmin 角色中，这个角色中的成员可以创建、修改或删除数据库对象。无需过多地考虑 db_owner 角色，SQL Server 中的每个对象都有一个所有者。一般情况下，谁创建了数据库，就是它的所有者。

SQL Server Enterprise Manager 不能将每个数据库角色的权限显示出来。关于角色的详细说明，请参阅《SQL Server 在线教程》（BOL），可以从 SQL Server 7.0 程序文件夹中或者 Enterprise Manager 中的“Help”选项中浏览 BOL。预定义的角色功能非常多，但如果它们不能满足你的所有需求，你至少有二种方法来解决这个问题。一种是直接给用户指派权限，另一种是从 Enterprise Manager 中添加自己的角色，扩展数据库，右击“Roles”，选择“New Database Role”。在对话框中，输入一个新的角色名字，选择“Standard Role”，并为这个角色添加新的成员。在为这个角色指派权限前，需要退出对话框并创建这个角色，然后双击这个角色为它指派权限。当然，你也可以在以后的工作中改变角色的成员和指派给它的权限。

权限的授予

无论你是希望向用户或角色授予数据库权限，你都可以首先从用户（请记住一个 SQL Server 用户可能对应着一个 NT 组）或角色着手完成这一任务，也可以从表、视图、存储过程着手，把对某一对象的访问权限授予适当的用户或自定义的数据库角色。

通过用户指派权限。展开 SQL Server Enterprise Manager，在指定的数据库下选择“Users”条目，在右边的窗口中双击指定的用户名打开“Database User Properties”对话框，点击“Permissions”按钮显示该用户拥有的对这个数据库中对象的访问权限。

需要注意的是这个对话框显示的仅仅是明确地授予这个用户的权限，该用户因是一个或多个角色、NT 组的成员而拥有的权限则不会显示在这里，实际上，要在 SQL Server 中得到用户所有权限的清单是相当困难的。

可以通过 SELECT 对话框授予用户读一个表或视图的访问权限。如果需要对数据库中的数据进行更新，一般情况下会使用 INSERT、UPDATE 和 DELETE 命令。然而，你希望数据录入人员能够插入记录但不能对它们进行修改或删除，删除数据记录可能是拥有更大权限、更多经验的

雇员的任务。要删除一个用户删除记录的权限，可以双击 DELETE 命令，出现一个红色的“X”符号，如图 5 所示。你可能有兴趣与开发人员讨论用户权限问题，但如果他们把有关的安全措施放入更新数据库记录的应用程序内部，你就无需操这份心了。然而，在数据库中实现安全措施更加安全，因为任何用户不可能通过修改应用程序的方法访问数据库中的数据。“Permissions”表显示用户 Caesar 可以对 Customers 表中的客户资料进行添加、更新等操作，但他无权删除一个客户，该表还同时显示 Caesar 无权对 Employee Territories 进行更新，但你需要记住的是他可能是拥有这一权限的组的成员。

Permissions 表中的 EXEC 字段控制着执行存储过程的能力。存储过程是用 T-SQL 写成的基于 SQL Server 的子程序，可以使 SQL Server 完成与数据库相关的操作。开发人员使用它们的原因是它们效率更高并且提供了新的安全手段，如果编程人员编写了存储过程，另外的用户则必须有这个存储过程的“Execute”权限才能运行它们。

除非开发人员特别地提醒，我们可以忽视 Declarative Referential Integrity（DRI）字段。有时用户在一个表中输入数据时，SQL Server 必须在另一个表中查找数据。例如，如果一个用户在一个合同表中输入物品的编号时，SQL Server 可能会通过另一个产品表验证输入的编号是否是一个可用的编号，这了能够完成这些验证，用户需要拥有对产品数据库的“Select”权限和合同数据库的“Insert”权限。有时，用户可能会需要通过其他的表来检验其输入的数据，但又不能直接地读取这个表，在这种情况下，用户就需要 DRI 权限而不是 Select 权限。

通过对 SQL Server 安全性的介绍，我们已经可以开发自己的数据库安全策略了，你下一步所需要的可能就是产生一个 SQL Server 脚本了。在 SQL Server Enterprise Manager 中，右击一个数据库，选择“All Tasks”，选择“Generate SQL Scripts”，这个选项能够产生一个脚本，对包括安全策略在内的数据库进行更新。然后就该学习如何在 Query Analyzer 窗口中运行脚本了，如果要运行控制安全设置的一部分脚本你就需要这样做。一个脚本文件可以代替通过鼠标在 SQL Server 事件管理器中进行点击和选择的操作，大大减少 DBA 的工作量。

3.2.2 SQL Server 数据库备份与恢复

一、备份数据库

二、还原数据库

1、打开 SQL 企业管理器，在控制台根目录中依次点开 Microsoft SQL Server

2、SQL Server 组-->双击打开你的服务器-->点图标栏的新建数据库图标，新建数据库的名字自行取。

3、点击新建好的数据库名称（如 CGNPC）-->然后点上面菜单中的工具-->选择恢复数据库

4、在弹出来的窗口中的还原选项中选择从设备-->点选择设备-->点添加-->然后选择你的备份文件名-->添加后点确定返回，这时候设备栏应该出现您刚才选择的数据库备份文件名，备份号默认为 1（如果您对同一个文件做过多次备份，可以点击备份号旁边的查看内容，在复选框中选择最新的一次备份后点确定）-->然后点击上方常规旁边的选项按钮（如图 3-13,图 3-14）

5、在出现的窗口中选择在现有数据库上强制还原，以及在恢复完成状态中选择使数据库可以继续运行但无法还原其它事务日志的选项。在窗口的中间部位的将数据库文件还原为这里要按照你 SQL 的安装进行设置（也可以指定自己的目录），逻辑文件名不需要改动，移至物理文件名要根据你所恢复的机器情况做改动，如您的 SQL 数据库装在 D:\Program Files\Microsoft SQL

6、修改完成后，点击下面的确定进行恢复，这时会出现一个进度条，提示恢复的进度，恢复完成后系统会自动提示成功，如中间提示报错，请记录下相关的错误内容并询问对 SQL 操作比较熟悉的人员，一般的错误无非是目录错误或者文件名重复或者文件名错误或者空间不够或者数据库正在使用中的错误，数据库正在使用的错误您可以尝试关闭所有关于 SQL 窗口然后重新打开进行恢复操作，如果还提示正在使用的错误可以将 SQL 服务停止然后重起看看，至于上述其它的错误一般都能按照错误内容做相应改动后即可恢复。

三、收缩数据库

一般情况下，SQL 数据库的收缩并不能很大程度上减小数据库大小，其主要作用是收缩日志

四、设定每日自动备份数据库

强烈建议有条件的用户进行此操作！

1、打开企业管理器，在控制台根目录中依次点开 Microsoft SQL Server-->SQL Server 组-->双

五、数据的转移（新建数据库或转移服务器）

一般情况下，最好使用备份和还原操作来进行转移数据，在特殊情况下，可以用导入导出的

第4章

主要内容：系统配置常见问题及解决方法

第4章 常见问题集

关于本系统配置可能常见问题收集如下。

【问题01】

△问题描述：当浏览器第一次访问服务器站点时，未能显示界面信息；出现错误提示。提示信息如下：“asp访问 IIS 元数据库失败”。

△问题原因：主要是IIS 和VS2K5安装次序不对（应当是先IIS 再VS2K5 ）；引发aspnet_regiis注册服务问题。

△解决方法：

运行方法如下：到你的C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727中找，有个工具叫 aspnet_regiis.exe

1.开始-->运行-->输入cmd，运行

2.DOS窗口打开以后，在DOS窗口内进入上面的文件夹

3.输入 aspnet_regiis.exe -i -enable

接着可能还会出现“未能创建 Mutex”的问题

解决方法：

1、先关闭你的VS2005。

2、打开 C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files找到你刚才调试的程序的名字的目录删除它。

3、关闭IIS服务器，重开一次。

4、用IE浏览一下你的程序，问题解决。

要是不行，到IIS Default Site的属性中看看.NET 的版本号选的是1.4还是2.0

Tips：也可以在Dos命令窗口使用如下命令：

1、net stop iisadmin

2、运行：d:\winnt\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis -i -enable

3、iisrese