## 6 数据库安全性

Web环境下，数据库的安全尤为重要，数据库安全性的保证，就是网络网站安全的护盾。在各种SQL注入，侵略，攻击的层层威胁下，保证Web数据库的安全性已成为新的课题。

**1、对用户安全管理**

首先要保证的就是数据库用户的权限的安全性，用户在访问数据库时，必须经过身份认证，对非超管用户，必须设定有限的权限和专用的密码。

比如，root是超管用户，其他用户就不能使用这个验证。

**2、定义视图**

为不同的用户定义不同的视图，可以限制用户的访问范围。通过视图机制把需要保密的数据对无权存取这些数据的用户隐藏起来，可以对数据库提供一定程度的安全保护。

**3、数据加密**

数据安全隐患无处不在，因此对数据的加密，是保护数据库安全的有效措施。

数据加密是应用最广、成本最低廉而相对最可靠的方法。数据加密是保护数据在存储和传递过程中不被窃取或修改的有效手段。

**4、启动事务管理和故障恢复**

事务管理和故障恢复主要是对付系统内发生的自然因素故障，保证数据和事务的一致性和完整性。

故障恢复的主要措施是进行日志记录和数据复制；事务运行的每一步结果都记录在系统日志文件中，并且对重要数据进行复制，发生故障时根据日志文件利用数据副本准确地完成事务的恢复。

**5、数据库备份与恢复**

数据库系统必须采取必要的措施，以保证发生故障时，可以恢复数据库。

数据备份需要仔细计划，制定出一个策略测试后再去实施，备份计划也需要不断地调整。

### 6****、****数据库验证方式

应用程序端连接数据库时使用的数据库验证方式为SQL Server验证。数据库连接串将使用CAPICOM技术加密存储在系统配置文件中。

## 

## 7 数据库管理和设置

将从系统的数据库运行角度出发，对本数据库的属性设置和备份恢复策略提出指导性说明。

另外，我们在数据库的物理结构上还做了优化：数据库表设计满足 3NF，减少了冗余数据。表中的所有数据元素不但要能唯一地被主关键字所标识,而且它们之间还必须相互独立，不存在其他的函数关系接口。

### ****1、****数据库备份恢复策略

数据备份是容灾的基础，是指为防止系统出现操作失误或系统故障导致数据丢失，而将全部或部分数据集合从应用主机的硬盘或阵列复制到其它的存储介质的过程。传统的数据备份主要是采用内置或外置的磁带机进行冷备份。但是这种方式只能防止操作失误等人为故障，而且其恢复时间也很长。随着技术的不断发展，数据的海量增加，不少的企业开始采用网络备份。网络备份一般通过专业的数据存储管理软件结合相应的硬件和存储设备来实现。

1、完全备份(Full Backup)

完全备份就是使用磁带对整个系统进行备份，不依赖文件的存档属性来确定备份文件。备份过程中，任何的标记都清除，都标记为已备份。这种备份的优点是：只要一盘磁带就可以恢复数据，并且大大节省了恢复时间。但因为每天都要对数据进行备份，造成备份的数据大量重复。这些重复的数据占用了大量的磁带空间，增加了成本。同时也因为备份的数据量大，对此，那些业务量大，繁忙的公司，这种备份策略是不明智的。

2、增量备份 (Incremental Backup )

增量备份就是只对当天新的或被修改过的数据进行备份。但它的缺点在于，当灾难发生时，数据的恢复比较麻烦上一次完全备份是在周一，此时，周四产生了故障，若要将数据恢复至周三晚上的状态，则需要先使用周一的完全备份，然后使用周二的差异备份，再使用周三的差异备份，而此时如果周二的差异备份坏了就会导致数据无法恢复至周三的状态。

3、差异备份(Differential Backup)

差异备份就是在进行了上一次备份后至今，将在这个时间段中产生差异的数据进行备份，这种备份策略的优点是节省了磁带空间，缩短了备份时间。只需要两盘磁带，即全备份磁带与灾难发生前一天的差异备份磁带，就可以将系统恢复。

在实际应用中，备份策略通常是以上三种的结合。例如每周一至周六进行一次增量备份或差异备份，每周日进行完全备份，每月底进行一次完全备份，每年底进行一次完全备份。

**目前我们的方案是使用定时脚本进行数据库的定期自动备份和事件清理。**

### 2、数据库运行日常维护

数据库的运行和维护阶段的主要工作有：  
对数据库性能的监测、分析和改善。  
数据库的转储和恢复。  
维持数据库的安全性和完整性。  
数据库的重组和重构。