

Microsoft SQL Server 2000 安装配置

(V 1.0.4)

1、安装 Microsoft SQL Server 时要注意不要安装到默认的路径 C:\Program Files\Microsoft SQL Server，而是指定其他的安装目录，例如 D:\SQL（本文以下的说明都以该安装目录为例说明）。

2、由于 SQL Server 有不少注入漏洞，为防止被注入后获得系统权限，为 SQL Server 设置单独的用户来运行，而不是使用默认的 System 系统账户来运行，例如我们为 SQL Server 运行设立独立的组 SQL_WPG 和用户 IUSER_MSSQL。在计算机管理中->用户和组->创建 SQL_WPG 组 和 IUSER_MSSQL 用户，并把 IUSER_MSSQL 隶属的组设置为 SQL_WPG，为 IUSER_MSSQL 设置一个复杂的密码（在下面的安装和配置过程中，还需要用到该密码，先临时记住这个密码）。并在“管理工具”->“本地安全策略”->“本地策略”->“用户权限分配”->“作为服务登录”里面添加 IUSER_MSSQL 用户。

3、执行 SQL Server 安装程序，在选择 SQL Server 安装目录的时候，指定 SQL Server 程序的安装目录为 D:\SQL。在选择运行账户和密码的地方，填写上 IUSER_MSSQL 和刚才设置的密码，其他按照正常程序安装。对于已经安装好的 SQL Server 可以在企业管理器里面把相关 SQL Server 的运行账户修改成 IUSER_MSSQL。

4、安装好 SQL Server 之后要确保打好最新补丁

5、为 SQL Server 运行的磁盘和文件夹添加权限，首先对所在磁盘根目录设置属性，D:\ 属性 -> 安全 -> 高级 -> 添加里面添加 SQL_WPG 组，设置权限“遍历文件夹/运行文件”，“列出文件夹/读取数据”，“读取属性”，“读取扩展属性”这 4 项为允许，并选中“只应用于该文件夹”选项，这点很重要，然后确定保存设置。对 SQL Server 系统目录 C:\Program Files\Microsoft Sql Server 文件夹添加组 SQL_WPG，赋予完全控制权限。程序安装目录 D:\SQL 文件夹添加组 SQL_WPG，赋予完全控制权限，并注意删除 SYSTEM 的权限。SQL Server 可以为每个数据库指定数据文件的存储地方，所以如果另外还指定了 SQL Server 数据文件的存储文件夹，那同样需要对该文件所在磁盘设置组 SQL_WPG 的权限（“遍历文件夹/运行文件”，“列出文件夹/读取数据”，“读取属性”，“读取扩展属性”），以及该文件夹的 SQL_WPG 完全控制权限。另外如果数据库的备份目标文件夹也是独立的文件夹，则参照数据文件夹的权限设置。

6、MS SQL Server 配置

1) 企业管理器->local 属性->常规->选中自动启动 SQL Server 代理服务，测试这个在执行备份等定期任务时候需要运行。

2) 企业管理器->local 属性->内存->最大使用内存不要超过 2G，这个根据服务器具体配置和运行性能来配置，Microsoft 的建议 SQL Server 运行内存需要达到 2G。

3) 企业管理器->local 属性->安全->身份验证选择 SQL Server 和 Windows

4) 企业管理器->工具->选项->高级->登陆超时 设置为 600 秒（重要）

5) 一定要为 sa 设定复杂的密码, 客户可以不知道该密码, 通过企业管理器自行修改。

7、为了系统运行更加安全, 将有安全隐患的 SQL 过程删除, 可以删除 SQL Server 调用 shell, 注册表, COM 组件的破坏权限。在"SQL 查询分析器"里执行下面的命令:

```
use master
EXEC sp_dropextendedproc 'xp_cmdshell'
EXEC sp_dropextendedproc 'Sp_OACreate'
EXEC sp_dropextendedproc 'Sp_OADestroy'
EXEC sp_dropextendedproc 'Sp_OAGetErrorInfo'
EXEC sp_dropextendedproc 'Sp_OAGetProperty'
EXEC sp_dropextendedproc 'Sp_OAMethod'
EXEC sp_dropextendedproc 'Sp_OASetProperty'
EXEC sp_dropextendedproc 'Sp_OAStop'
EXEC sp_dropextendedproc 'Xp_regaddmultistring'
EXEC sp_dropextendedproc 'Xp_regdeletekey'
EXEC sp_dropextendedproc 'Xp_regdeletevalue'
EXEC sp_dropextendedproc 'Xp_regenumvalues'
EXEC sp_dropextendedproc 'Xp_regread'
EXEC sp_dropextendedproc 'Xp_regremovemultistring'
EXEC sp_dropextendedproc 'Xp_regwrite'
drop procedure Sp_makewebtask
```

这部分的删除一定要注意, 如果在系统实际运行中有用到这些存储过程, 则不能删除, 或者按照需要再重建。

8、在 SQL Server 的实际使用中, 给每个独立的数据库应用都指定独立的数据库帐户连接数据库, 不要使用 sa 来连接数据库, 很多网站或应用都会用明码保存数据库连接, 使用 sa 会加大泄漏 sa 密码的风险。对于建立的数据库账户指定最小的权限, 一般只需要给 public 和 db_owner 的权限。