Sql server 安全设置

1、使用安全的密码策略

我们把密码策略摆在所有安全设置的第一步，请注意，非常多数据库帐号的密码过于简单，这跟系统密码过于简单是个道理。对于 sa 更应该注意，同时不要让 sa 帐号的密码写于应用程式或脚本中。健壮的密码是安全的第一步！

SQL Server2000 安装的时候，如果是使用混合模式，那么就需要输入 sa 的密码，除非你确认必须使用空密码。这比以前的版本有所改进。

同时养成定期修改密码的好习惯。数据库管理员应该定期查看是否有不符合密码需求的帐号。比如使用下面的 SQL 语句：

```
Use master
Select name,Password from syslogins where password is null
```

2、使用安全的帐号策略

由于 SQL Server 不能更改 sa 用户名称，也不能删除这个终极用户，所以，我们必须对这个帐号进行最强的保护，当然，包括使用一个非常强壮的密码，最佳不要在数据库应用中使用 sa 帐号，只有当没有其他方法登录到 SQL Server 实例（例如，当其他系统管理员不可用或忘记了密码）时才使用 sa。建议数据库管理员新建立一个拥有和 sa 相同权限的终极用户来管理数据库。安全的帐号策略还包括不要让管理员权限的帐号泛滥。

SQL Server 的认证模式有视窗系统身份认证和混合身份认证两种。如果数据库管理员不希望操作系统管理员来通过操作系统登陆来接触数据库的话，能在帐号管理中把系统帐号“BUILTIN \ Administrators”删除。不过这样做的结果是一旦

sa 帐号忘记密码的话，就没有办法来恢复了。

非常多主机使用数据库应用只是用来做查询、修改等简单功能的，请根据实际需要分配帐号，并赋予仅仅能够满足应用需求和需要的权限。比如，只要查询功能的，那么就使用一个简单的 public 帐号能够 select 就能了。

3、加强数据库日志的记录

审核数据库登录事件的“失败和成功”，在实例属性中选择“安全性”，将其中的审核级别选定为全部，这样在数据库系统和操作系统日志里面，就周详记录了所有帐号的登录事件。

请定期查看 SQL Server 日志检查是否有可疑的登录事件发生，或使用 DOS 命令。

findstr /C:"登录" d: \ Microsoft SQL Server \ MSSQL \ LOG \ *.*

4、管理扩展存储过程

对存储过程进行大手术，并且对帐号调用扩展存储过程的权限要慎重。其实在多数应用中根本用不到多少系统的存储过程，而 SQL Server 的这么多系统存储过程只是用来适应广大用户需求的，所以请删除不必要的存储过程，因为有些系统的存储过程能非常容易地被人利用起来提升权限或进行破坏。

如果你不必扩展存储过程 xp_cmdshell 请把他去掉。使用这个 SQL 语句

```
use master
sp_dropextendedproc 'xp_cmdshell'
```

xp_cmdshell 是进入操作系统的最佳捷径，是数据库留给操作系统的一个大后门。如果你需要这个存储过程，请用这个语句也能恢复过来。

```
sp_addextendedproc 'xp_cmdshell', 'xpsql70.dll'
```

如果你不必请丢弃 OLE 自动存储过程（会造成管理器中的某些特征不能使用），这些过程包括如下：Sp_OACreate、 Sp_OADestroy、 Sp_OAGetErrorInfo、Sp_OAGetProperty 、Sp_OAMethod、 Sp_OASetProperty 、Sp_OAStop

去掉不必的注册表访问的存储过程，注册表存储过程甚至能够读出操作系统管理员的密码来，如下：Xp_regaddmultistring 、Xp_regdeletekey、Xp_regdeletevalue、 Xp_regenumvalues、Xp_regread、 Xp_regremovemultistring 、Xp_regwrite

5、使用协议加密

SQL Server 2000 使用的 Tabular Data Stream 协议来进行网络数据交换，如果不加密的话，所有的网络传输都是明文的，包括密码、数据库内容等等，这是个非常大的安全威胁。能被人在网络中截获到他们需要的东西，包括数据库帐号和密码。所以，在条件容许情况下，最佳使用 SSL 来加密协议，当然，你需要一个证书来支持。

6、不要让人随便探测到你的 TCP/IP 端口

默认情况下，SQL Server 使用 1433 端口监听，非常多人都说 SQL Server 设置的时候要把这个端口改动，这样别人就不能非常容易地知道使用的什么端口了。可惜，通过微软未公开的 1434 端口的 UDP 探测能非常容易知道 SQL Server 使用的什么 TCP/IP 端口了。

不过微软还是考虑到了这个问题，毕竟公开而且开放的端口会引起不必要的麻烦。在实例属性中选择 TCP/IP 协议的属性。选择隐藏 SQL Server 实例。如果

隐藏了 SQL Server 实例，则将禁止对试图枚举网络上现有的 SQL Server 实例的客户端所发出的广播作出响应。这样，别人就不能用 1434 来探测你的 TCP/IP 端口了（除非用 Port Scan）。

7、修改 TCP/IP 使用的端口

请在上一步设置的基础上，更改原默认的 1433 端口。在实例属性中选择网络设置中的 TCP/IP 协议的属性，将 TCP/IP 使用的默认端口变为其他端口。

8、拒绝来自 1434 端口的探测

由于 1434 端口探测没有限制，能够被别人探测到一些数据库信息，而且还可能遭到 DOS 攻击让数据库服务器的 CPU 负荷增大，所以对视窗系统 2000 操作系统来说，在 IPSec 过滤拒绝掉 1434 端口的 UDP 通讯，能尽可能地隐藏你的 SQL Server。

9、对网络连接进行 IP 限制

SQL Server 2000 数据库系统本身没有提供网络连接的安全解决办法，不过视窗系统 2000 提供了这样的安全机制。使用操作系统自己的 IPSec 能实现 IP 数据包的安全性。请对 IP 连接进行限制，只确保自己的 IP 能够访问，也拒绝其他 IP 进行的端口连接，把来自网络上的安全威胁进行有效的控制。