SQLServer安全模型的使用 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/284/2021_2022_SQLServer_E5_c97_284879.htm 由于多种原因，进行安全设置的人们常常不理解数据的真正价值，所以，他们也无法对数据进行合适的保护。将你的数据只限于需要的人访问，并保证访问的人的合法性，是一个数据库管理人员的重要工作。然而，确保数据可以访问不是意味着数据向所有人公开，相反的，你必须很仔细地保护数据，并只对需要使用数据的人进行开放。 设置安全性过程 通用的软件维护和数据库更新都会对系统安全起着重要作用，通常包括以下步骤： 分配一个可靠的密码给缺省的系统管理(SA)帐号。然后，建立自己唯一命名的帐号，并将这一帐号放入sysadmin。一定要确认新帐号也有一个可靠的密码。 将独立的密码分配给每一个用户。更好的，使用Windows集成安全性，并让Windows遵循稳定密码规则。 决定哪些用户需要查看数据，然后分配合适的许可。请不要随便赋予用户各种权限。例如不要把每一个人的工资随便让其他人访问。 决定哪些用户需要更新数据，然后分配合适的许可。帐号管理人员应该可以查看所有用户的信息，但程序员一定要限制更新这些信息的权限。特别的，只有负责特定帐号的管理者是唯一可以更改用户数据的人。 通过这些系列信息你可以学会很多知识，但你应该从开始就具备这些观点。否则，数据库的任何用户就可以偷窃或删除你的重要数据。 什么东西最容易发生错误? 对于记录，应该知道SQL Server并非绝对安全的。你应该提出一些想法并努力有效地保护你的服务器。在安装服务器之前有两点你必须完成的： 设置管

理人员的帐号和密码。 保护系统防止受到Slammer worm的感染。 使一些特殊的东西安全化 SQL Server2000通过SA帐号而具有缺省的安全设置。在安装过程中，SQL Server自动建立一个管理的用户，并分配一个空白密码给SA用户名称。一些管理人员喜欢将SA密码设置为空白或者一个通用的密码以便每一个人都能知道。如果你犯这样的错误，进入你的数据库的任何人都可以为所欲为。具备管理者允许的任何人也可以做任何想做的事不仅仅是数据库，而是整个计算机。所以，必须限制用户根据他们的需要进行访问数据库，不要给他们权利太少，也不能太多。 暂且把每一天管理的SA帐号放在一边，让我们看看带有安全密码的帐号。建立另一帐号以便管理(或者是一个SQL Server帐号或者是一个Windows帐号，取决于你的认证模式)。你所要避免的是太容易地猜到帐号名称或者帐号密码，因为任何人得到这些帐号。 一个引起警戒的坏事Slammer worm(Slammer蠕虫) 2003年1月份出现了一些非常致命的恶意代码，即为Slammer worm。这一代码专门针对于SQL Server的安装进行攻击。通过利用SQL Servera代码中的缺欠，蠕虫能够在SQL Server安装的时候复制本身程序而损坏整个机器和其他机器。蠕虫生成时以15秒可以充满网络。微软已经花了很大力量来阻止这一蠕虫，但是蠕虫还是无法完全消除。有些人开始抱怨SQL Server的测试版本的原因，因为是它在安装时导致了系统的损坏。 很多月份已经过去了，有必要还要对蠕虫那么警惕吗?回答是肯定的。因为每一天还有很多Slammer的复制而感染机器。如果一个没有任何补丁的SQL Server连接到网络，你将会变成这一行为的牺牲品。从道德上而言，在将SQL Server与网络线连接之前，必须保护你

的服务器，并运行所有的新服务补丁。服务补丁的重要性 服务补丁在下载时是免费的。Slammer没有损坏你的数据，但它可以导致服务器的很多破坏，其危害是明显的。保护数据最简单的方法是下载Service Pack 3 或者Service Pack 3a。 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