

保护SQLServer的十个步骤 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/454/2021\\_2022\\_\\_E4\\_BF\\_9D\\_E6\\_8A\\_A4SQLS\\_c98\\_454323.htm](https://www.100test.com/kao_ti2020/454/2021_2022__E4_BF_9D_E6_8A_A4SQLS_c98_454323.htm) 这里介绍了为提高 sql server 安装的安全性，您可以实施的十件事情：1.安装最新的服务包。为了提高服务器安全性，最有效的一个方法就是升级到 sql server 2000 service pack 3a (sp3a)。另外，您还应该安装所有已发布的安全更新。2.使用 microsoft 基线安全性分析器 ( mbsa ) 来评估服务器的安全性。 mbsa 是一个扫描多种 microsoft 产品的不安全配置的工具，包括 sql server 和 microsoft sql server 2000 desktop engine (msde 2000)。它可以在本地运行，也可以通过网络运行。该工具针对下面问题对 sql server 安装进行检测：1) 过多的sysadmin固定服务器角色成员。2) 授予sysadmin以外的其他角色创建 cmdexec 作业的权利。3) 空的或简单的密码。4) 脆弱的身份验证模式。5) 授予管理员组过多的权利。6) sql server数据目录中不正确的访问控制表(acl)。7) 安装文件中使用纯文本的sa密码。8) 授予guest帐户过多的权利。9) 在同时是域控制器的系统中运行sql server。10) 所有人 ( everyone ) 组的不正确配置，提供对特定注册表键的访问。11) sql server 服务帐户的不正确配置。12) 没有安装必要的服务包和安全更新。microsoft 提供 mbsa 的免费下载。3.使用 windows 身份验证模式。在任何可能的时候，您都应该对指向 sql server 的连接要求 windows 身份验证模式。它通过限制对microsoft windows&reg.用户和域用户帐户的连接，保护 sql server 免受大部分 internet 的工具的侵害，而且，您的服务器也将从 windows 安全增强机制中

获益，例如更强的身份验证协议以及强制的密码复杂性和过期时间。另外，凭证委派（在多台服务器间桥接凭证的能力）也只能在 windows 身份验证模式中使用。在客户端，windows 身份验证模式不再需要存储密码。存储密码是使用标准 sql server 登录的应用程序的主要漏洞之一。要在 sql server 的 enterprise manager 安装 windows 身份验证模式，请按下列步骤操作：1) 展开服务器组。2) 右键点击服务器，然后点击属性。3) 在安全性选项卡的身份验证中，点击仅限 windows。4. 隔离您的服务器，并定期备份。物理和逻辑上的隔离组成了 sql server 安全性的基础。驻留数据库的机器应该处于一个从物理形式上受到保护的地方，最好是一个上锁的机房，配备有洪水检测以及火灾检测/消防系统。数据库应该安装在企业内部网的安全区域中，不要直接连接到 internet。定期备份所有数据，并将副本保存在安全的站点外地点。5. 分配一个强健的 sa 密码。sa 帐户应该总拥有一个强健的密码，即使在配置为要求 windows 身份验证的服务器上也该如此。这将保证在以后服务器被重新配置为混合模式身份验证时，不会出现空白或脆弱的 sa。要分配 sa 密码，请按下列步骤操作：1) 展开服务器组，然后展开服务器。2) 展开安全性，然后点击登录。3) 在细节窗格中，右键点击 sa，然后点击属性。4) 在密码方框中，输入新的密码。

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](http://www.100test.com)