WindowsServer2003安全最佳实践经验 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/139/2021_2022_WindowsSer_c100_139674.htm 新的理念是，服务器缺省就应该是安全的。这的确是一个不错的理念，不过微软贯彻得还不够彻底。虽然缺省的 Windows 2003安装绝对比确省的Windows NT或Windows 2000安装安全许多，但是它还是存在着一些不足。下面让我们来讨论如何让Windows Server 2003更加安全。 理解你的角色 理解服务器角色绝对是安全进程中不可或缺的一步。Windows Server可以被配置为多种角色，Windows Server 2003 可以作为域控制器、成员服务器、基础设施服务器、文件服务器、打印服务器、IIS服务器、IAS服务器、终端服务器等等。一个服务器甚至可以被配置为上述角色的组合。 现在的问题是每种服务器角色都有相应的安全需求。例如，如果你的服务器将作为IIS服务器，那么你将需要开启IIS服务。然而，如果服务器将作为独立的文件或者打印服务器，启用IIS服务则会带来巨大的安全隐患。 我之所以在这里谈到这个的原因是我不能给你一套在每种情况下都适用的步骤。服务器的安全应该随着服务器角色和服务器环境的改变而改变。 因为有很多强化服务器的方法，所以我将以配置一个简单但安全的文件服务器为例来论述配置服务器安全的可行性步骤。我将努力指出当服务器角色改变时你将要做的。请谅解这并不是一个涵盖每种角色服务器的完全指南。 物理安全 为了实现真正意义上的安全，你的服务器必须被放置在一个安全的位置。通常地，这意味着将将服务器放置在上了锁的门后。物理安全是相当重要的，因为现有的许多管理和灾难恢复工

具同样也可以被黑客利用。任何拥有这样工具的人都能在物理接入到服务器的时候攻击服务器。唯一能够避免这种攻击的方法是将服务器放置在安全的地点。对于任何角色的Windows Server 2003，这都是必要的。 创建基线 除了建立良好的物理安全以外，我能给你的最佳建议是，在配置一系列Windows Server 2003的时候，应该确定你的安全需求策略，并立即部署和执行这些策略 。 实现这一目的最好的方法是创建一个安全基线(security baseline)。安全基线是文档和公认安全设置的清单。在大多数情况下，你的基线会随着服务器角色的不同而产生区别。因此你最好创建几个不同的基线，以便将它们应用到不同类型的服务器上。例如，你可以为文件服务器制定一个基线，为域控制器制定另一个基线，并为IAS服务器制定一个和前两者都不同的基线。 Windows 2003包含一个叫"安全配置与分析"的工具。这个工具让你可以将服务器的当前安全策略与模板文件中的基线安全策略相比较。你可以自行创建这些模板或是使用内建的安全模板。 安全模板是一系列基于文本的INF文件，被保存在%SYSTEMROOT%\SECURITY|TEMPLATES 文件夹下。检查或更改这些个体模板最简单的方法是使用管理控制台(MMC)。 要打开这个控制 台，在RUN提示下输入MMC命令，在控制台加载后，选择添加/删除管理单元属性命令，Windows就会显示添加/删除管理单元列表。点击"添加"按钮，你将会看到所有可用管理单元的列表。选择安全模板管理单元，接着依次点击添加，关闭和确认按钮。 在安全模板管理单元加载后，你就可以察看每一个安全模板了。在遍历控制台树的时候，你会发现每个模板都模仿组策略的结构。

模板名反映出每个模板的用途。例如，HISECDC模板就是一个高安全性的域控制器模板。 如果你正在安全配置一个文件服务器，我建议你从SECUREWS模板开始。在审查所有的模板设置时，你会发现尽管模板能被用来让服务器更加安全，但是不一定能满足你的需求。某些安全设置可能过于严格或过于松散。我建议你修改现有的设置，或是创建一个全新的策略。通过在控制台中右击C:\ WINDOWS\Security\Templates文件夹并在目标菜单中选择新建模板命令，你就可以轻轻松松地创建一个新的模板。 在创建了符合需求的模板后，回到添加/删除管理单元属性面板，并添加一个安全配置与分析的管理单元。在这个管理单元加载后，右击"安全配置与分析"容器，接着在结果菜单中选择"打开数据库"命令，点击"打开"按钮，你可以使用你提供的名称来创建必要的数据库。 接下来，右击"安全配置与分析"容器并在快捷菜单中选择"导入模板"命令。你将会看到所有可用模板的列表。选择包含你安全策略设置的模板并点击打开。在模板被导入后，再次右击"安全配置与分析"容器并在快捷菜单中选择"现在就分析计算机"命令。Windows将会提示你写入错误日志的位置，键入文件路径并点击"确定"。