Windows Server 2003 安全：锁定

Windows Server 2003 安全：锁定

关闭不必要的服务、端口和帐户使 Windows Server 2003 固若金汤。黑客通常通过不使用的(没有配置或者不安全的)端口和服务访问服务器，比如 Internet 信息服务（IIS）。为了限制入口点，服务器强化包括阻止不使用的端口和协议，同时中止不必要的服务。微软最近发布的 Windows Server 2008 可能备受关注，但是大部分组织仍然会使用 Server 2003，直到微软不再支持它为止。虽然 Server 2003 可能不是最新的，也不是功能最强大的，但你采取一些简单——但必要的——步骤来强化你的系统。

从开始阶段考虑安全问题

构建一个强化的服务器意味着从最初的安装中推行安全进程。新的计算机应该安装在独立的网络中，在操作系统强化之前，谨防可能的不利流量进入计算机。

- 锁定 Windows Server 2003 （一）

设定安全策略

强化 Windows Server 2003 的最简单方法是利用服务器配置向导(SCW)，它可以帮你创建一个安全的策略，一个专门基于网络中的服务器功能的安全策略。

- 锁定 Windows Server 2003 （二）

中止或删除不必要的帐户、端口以及服务

在安装期间，可以自动创建三个当地的用户帐户——管理员、客户、以及 Help-Assistant，Help-Assistant 是用 Remote Assistance 安装的。管理员帐户拥有系统的密

钥。它可以分配用户权限和访问控制。尽管不能删除这个主要的帐户，但为了使黑客更难访问该帐户，可以将其中止或者重新命名。

❖ 锁定 Windows Server 2003 （三）

建立物理计算机和逻辑组件合适访问控制

从你按下电源开关到操作系统启动以及所有服务激活，这个时间段仍然存在邪恶行为活动的空间。不要说操作系统，就是经过良好强化、启动时需要密码、基本输入输出系统（BIOS）/固件受到保护的计算机，也会受到威胁。此外，在基本输入输出系统（BIOS）层面，应当建立设备引导指令，以防未授权的引导系统受到可选媒介的威胁。

❖ 锁定 Windows Server 2003 （四）

你的工作尚未完成

保护你的主要服务器是一个持续不断的过程。千万不要认为，只要已经将服务器强化的像坚果一样强硬，无法破碎时，你的工作就完成了。还需要执行制定功能强大的审计和日志策略等步骤，确保你的所有工作不会化为乌有。

❖ 锁定 Windows Server 2003 （五）

锁定 Windows Server 2003 （一）

关闭不必要的服务、端口和帐户使 Windows Server 2003 固若金汤。

黑客通常通过不使用的(没有配置或者不安全的)端口和服务访问服务器，比如 Internet 信息服务（IIS）。为了限制入口点，服务器强化包括阻止不使用的端口和协议，同时中止不必要的服务。微软最近发布的 Windows Server 2008 可能备受关注，但是大部分组织仍然会使用 Server 2003，直到微软不再支持它为止。虽然 Server 2003 可能不是最新的，也不是功能最强大的，但你采取一些简单——但必要的——步骤来强化你的系统，你就可以保持一个更好的安全状态。

1 从开始阶段考虑安全问题

构建一个强化的服务器意味着从最初的安装中推行安全进程。新的计算机应该安装在独立的网络中，在操作系统强化之前，谨防可能的不利流量进入计算机。

在安装的前几步中，会要求你选择 FAT(文件分配表)，或者 NTFS(新技术文件系统)。所有都选择 NTFS。FAT 是微软为早期操作系统所设计的原始文件系统。NTFS 是在 Windows NT 中引入的，它提供了大量的 FAT 所不能提供的安全性能：包括访问控制表（ACLs）和文件系统日志，在把它们提交给主要文件系统之前，可以记录下变化。接下来，使用最新的 Service Pack (SP2)和任何可用的补丁。虽然 Service Pack 中的许多补丁相对比较陈旧，但是它们囊括了许多熟知的漏洞，在威胁中攻击者可以利用这些漏洞，比如服务拒绝攻击、远程编码执行和跨站脚本攻击。

(作者：Sandra Kay Miller 译者：李娜娜 来源：Techtarget 中国)

锁定 Windows Server 2003 （二）

2．设定安全策略

现在，你已经准备好开始认真考虑严肃的工作。强化 Windows Server 2003 的最简单方法是利用服务器配置向导(SCW)，它可以帮你创建一个安全的策略，一个专门基于网络中的服务器功能的安全策略。（见下图 1）

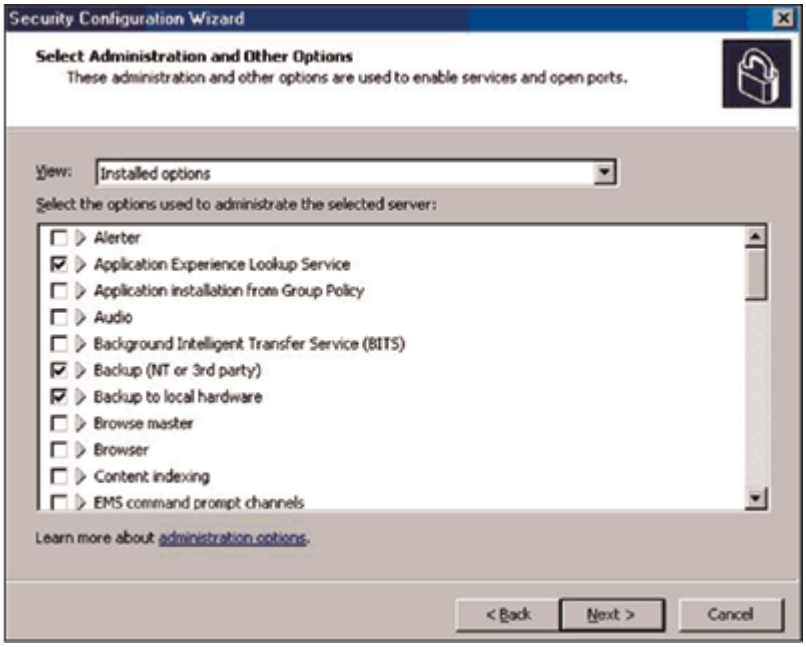


图 1：服务器配置向导允许你设置功能、客户特征、服务和端口、以及管理选项。选择这些选项可以激活合适的端口和服务。

SCW 与配置你的服务器向导(Configure Your Server Wizard)不同。SCW 不安装服务器组件，但是可以对端口和服务进行检测，并且配置注册表和审计设置。SCW 并不是默认安装的，因此你必须通过控制面板中的“添加/删除程序”来添加 SCW。选择“添加/删除

Windows 组件”按钮，并选定“安全配置向导”（SCW）。一旦安装之后，就可以从 Administrative Tools 访问 SCW。

SCW 所创建的安全策略是 XML 文件，它可以配置服务、网络安全、特定注册表参数、审计策略，此外，如果合适的话，它还可以配置 IIS。通过配置界面，可以创建新的安全策略，而且可以审查现有的策略或者将其应用到网络中的其它服务器中。如果新的策略造成了冲突或者不稳定，它可以将其调整为原来的状态。

SCW 涵盖了 Server 2003 安全的方方面面。该向导以安全配置数据库（Security Configuration Database）开始，包含所有功能、客户特征、管理选项、服务和端口的信息。对于应用程序，也有一个详尽的知识库。这意味着当被选定的服务器功能必须要应用程序的时候——诸如自动更新的客户特性或者例如文件备份的管理程序之类的——Windows 防火墙将会开放必需的端口。当应用程序关闭时，端口会自动隔断。

用于网络和注册表协议的安全设置，以及服务信息块（SMB）的安全签名增强了对主要服务器特性的保护。为了与外部资源连接，带外认证设置决定了认证所要求的水平。

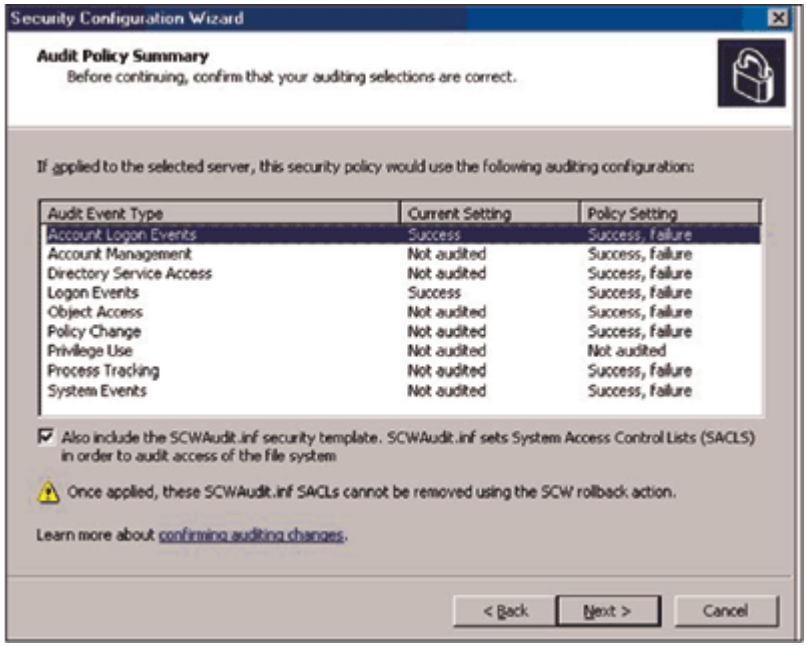


图 2：你也可以在服务器配置向导中设置审计策略。对于所有成功以及失败的活动都应当审计并记录。

SCW 的最后一步包括审计策略（见上图 2）。默认状态下，Server 2003 仅仅对成功的活动进行审计，但是对于一个强化的系统而言，所有成功与失败的活动都应该审计并记入日志。一旦向导完成，安全策略就可以存储为 XML 文件，可以立即应用到服务器中，保存起来已备后用，或者应用到其它服务器。是否需要返回安装时没有强化的服务器上呢？SCW 也可以在现有的服务器上安装并运行。

（作者：Sandra Kay Miller 译者：李娜娜 来源：Techtarget 中国）

锁定 Windows Server 2003 （三）

3. 中止或者删除不必要的帐户、端口以及服务

在安装期间，可以自动创建三个当地的用户帐户——管理员、客户、以及 Help-Assistant，Help-Assistant 是用 Remote Assistance 安装的。管理员帐户拥有系统的密钥。它可以分配用户权限和访问控制。尽管不能删除这个主要的帐户，但为了使黑客更难访问该帐户，可以将其中止或者重新命名。相反，你应该为单个用户或者组群目标分配管理权限。这使黑客更难确定哪个用户拥有管理权限。这一点在审计过程中也是关键的。设想一下：一个 IT 部门中，任何人都可以使用一个单一的管理账号和密码登录到该服务器中。这就是主要的安全问题。最好的方法就是根本不要使用管理员帐户。

同样地，对于那些了解 Server 2003 操作方式的人来说，客户和 Help-Assistant 帐户为他们提供了易于攻击的目标。选择 Computer Management 选项，通过 Administrative Tools 菜单下的控制面板，中止这些帐户。右击你想要改变的用户帐户，然后单击属性。确保这些帐户在网络中和本地已经被中止。

开放的端口是高风险区。共有 65535 个端口可用，而且你的服务器并不都需要它们。防火墙，包括在 SP1 中，允许管理员中止不必要的 TCP 和 UDP 端口。这些端口可以分为三个不同的范围：众所周知的端口（0-1023），已注册的端口（1024-49151），以及动态/私有端口（49152-65535）。对于操作系统功能而言，熟知的端口是至关重要的。已注册的端口仅仅能够用于服务或者应用程序。剩余的端口是“西大荒”，有待开发使用。

获取一列端口，以及相关的服务和应用程序，管理员就可以确定哪些是主要性能所要求的。比如，为了防止任何远程登录或者 FTP 流量，可以阻断与这些应用程序相关的已知端口。类似地，已知的软件和恶意软件也有已知的相关端口，所有端口都可以阻断，进而创建一个更安全的服务器状态。最佳方式就是关闭所有不使用的端口。确认计算机上哪些

端口是开放状态、哪些是监听与阻隔状态的最佳方法是，使用免费 Nmap 工具。SCW 在默认状态下关闭了所有的端口，然后按照安全策略的设置再打开它们。

你可以在线获得有关端口职能的信息。

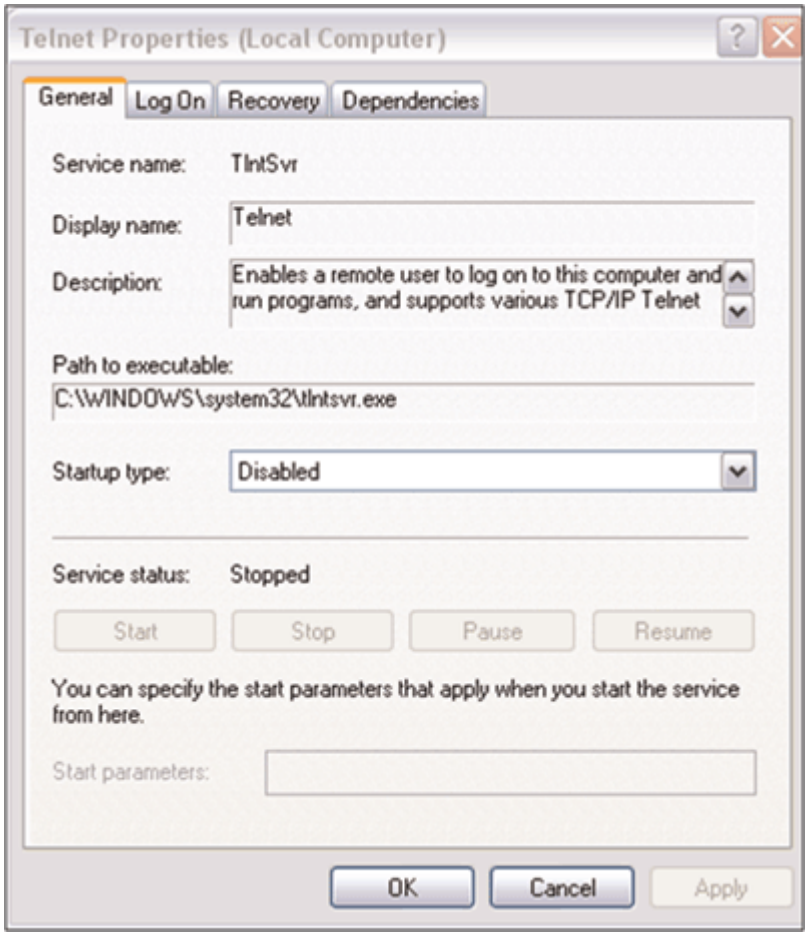


图 3：使用 Control Panel 中的 Administrative Tools 菜单可以中止不需要的服务——本例中指远程登录。

强化服务器的最有效的方法就是不要安装任何与操作不相关的应用程序，并关闭不需要的服务。虽然服务器上安装有电子邮件客户机程序或者生产性工具，给管理员带来了方便，但是，如果它们与服务器的性能没有直接关系，就不应该安装。在 Windows Server 2003 中可以中止 100 多项服务。比如，DHCP 是包含在基本安装之中的。然而，如果你不

将系统作为 DHCP 服务器使用，那么中止 tcpsvcs.exe 会阻止服务初始化和运行。然而，要切记的是，并非所有的服务都可以被中止。比如，尽管 Blaster 蠕虫可以利用远程过程调用（RPC）服务，但是由于它允许其它系统进程内部之间以及跨网络通信，所以不能中止这个服务。通过控制面板下的“管理工具 Admin- istrative Tools”菜单，访问 Services 界面，便可以关闭不需要的服务。双击 service，打开属性对话框，选择 Startup Type 框中的 Disabled（见上图 3）。

（作者：Sandra Kay Miller 译者：李娜娜 来源：Techtarget 中国）

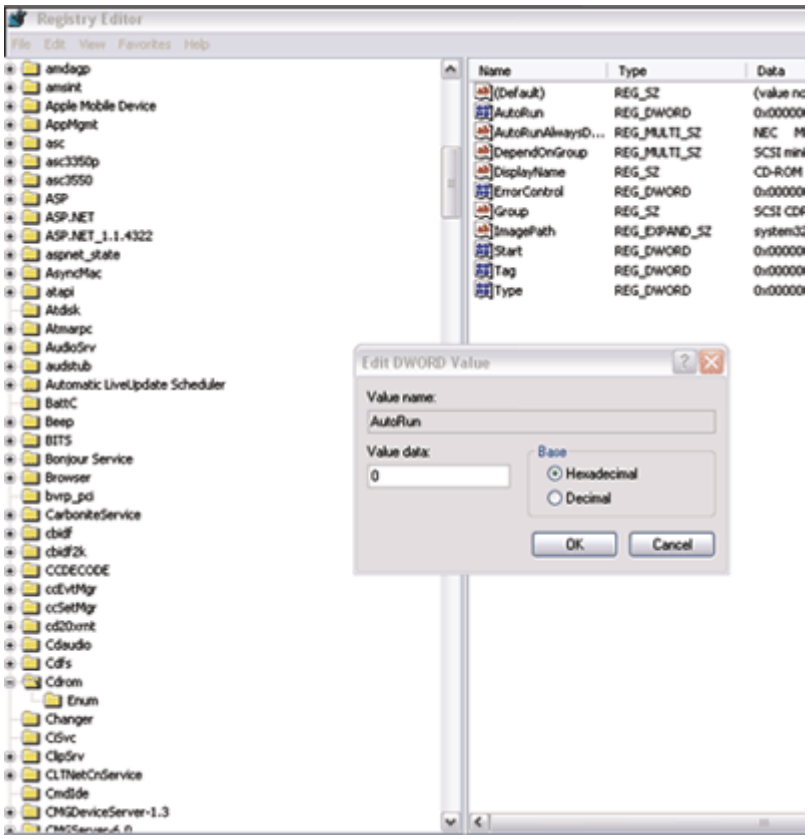
锁定 Windows Server 2003 （四）

4. 建立对物理计算机和逻辑组件的合适访问控制

从你按下电源开关到操作系统启动以及所有服务激活，这个时间段仍然存在邪恶行为活动的空间。不要说操作系统，就是经过良好强化、启动时需要密码、基本输入输出系统（BIOS）/固件受到保护的计算机，也会受到威胁。此外，在基本输入输出系统（BIOS）层面，应当建立设备引导指令，以防未授权的引导系统受到可选媒介的威胁。

电脑启动以后，立即按下 F2 键，进入 BIOS 设置，就可以建立访问控制。Alt-P 将你移动到 BIOS 的设置页面。在“启动顺序（Boot Order）”页面下，将第一个选项设置为 Internal HDD。在系统安全页面中，有“原始密码”、“管理密码”和“硬盘密码”三个选项。

同样地，也应该中止外部设备的自动运行功能，包括 CD-ROM、DVD 和 USB 驱动。在 HKEY_LOCAL_MACHINESYSTEMCurrent ControlSetServicesCdrom（或者其它设备名称）下的注册表中， 将自动运行值设置为 0。自动运行可以在便携式设备上自动启动恶意的应用程序。很容易便可以安装特洛伊木马、后门程序、按键记录器、监听设备等。（见下图 4）



防御的下一步是关于用户如何登录到系统中的。尽管认证有许多相关技术，比如生物认证、令牌、智能卡和单用密码，这些选项都可以保护 Windows Server 2003 的安全，大多数管理员同时使用用户名和密码，从本地或者远程登录到服务器上。通常都是默认的密码，这样就会带来麻烦（而且，请不要将默认选项中的 old 替换为@55w0rd！）。

虽然这应该是不言而喻的，但是如果你使用的是密码，那么就应该使用一个功能强大的策略：最少 8 个字母，包括大写字母、数字、以及非文字字符的组合，每隔一定时间进行更改，在特定的时间段内不要使用相同的密码。

一个强大的密码策略，加上多因素认证，这仅仅是开始。幸亏 NTFS 提供了 ACLs，可以给每个用户分配不同等级的多方面使用服务器的权力。文件访问控制和打印共享许可的合理设置应该是基于组群配置的，而不是基于“每个人”。这可以在服务器上操作，或者通过活动目录实现。

同样重要的是确保仅经过合理认证的用户才允许访问并编辑注册表。底线是要限制用户仅可以访问要求的服务和应用程序。

(作者：Sandra Kay Miller 译者：李娜娜 来源：Techtarget 中国)

锁定 Windows Server 2003 （五）

5. 你的工作尚未完成

保护你的主要服务器是一个持续不断的过程。千万不要认为，只要已经将服务器强化的像坚果一样强硬，无法破碎时，你的工作就完成了。

按照下面的步骤进行，确保你的所有工作不会化为乌有：

制定功能强大的审计和日志策略。虽然预防服务器中不必要的或者非故意的行为是强化服务器的主要目的，但是为了确保所采取的行动能够胜任任务，就要建立综合的事件日志和功能强大的审计策略。

随着遵守规则的出现，一个功能强大的审计策略应当是强化的 Windows Server 2003 的一部分。成功和失败的帐户登录与管理企图，以及权限的使用和策略的改变都应该初始化。

Windows Server 2003 创建了如下类型的日志：应用程序、安全、目录服务、文件复制服务和 DNS 服务器。事件阅览器可以监测到所有这些日志，也能提供硬件、软件、和系统问题方面的详细信息。每个日志记录中，事件阅览器列出了五种事件：错误、警告、信息、成功的审计、以及失败的审计。

创建一个基线备份。你已经采取了初步和定期的措施，来强化 Windows Server 2003，之后，最后一步是创建一个关于计算机和系统状态的“0/完全”级别的备份。计划保存这个备份，因为当安全事件发生以时，鉴别基线是与服务器的状态有关系的。在主要软件升级和操作系统更新以后，也要确保保存服务器的基线备份。

密切关注帐户。为了服务器的安全，管理帐户是一个不断进行的过程。用户帐户应当定期核查，并且任何不起作用的、完全相同的、共享的、普通的或者测试帐户，都应当删除。

保证补丁是最新的。强化服务器是一个持续的过程，并没有随着 SP2 而结束。为了保证补丁是最新的，通过控制面板中的“系统”菜单，激活“自动更新”。在“自动更新”框中，选择“自动下载和更新”，此外，设置服务器在不干扰服务器的功能时 安装这些补丁，这是因为大多数主要的更新要求服务器重新启动。

（作者：Sandra Kay Miller 译者：李娜娜 来源：Techtarget 中国）