网 管 手 册

（上）

王继刚 主编

目　　录

安全配置 Windows2000 服务器

怎么装

一、 版本的选择

笔者强烈建议：在语言不成为障碍的情况下，请一定使用英文版。要知道，微软的产品是以“漏洞加补丁（Bug & Patch）”而著称的，中文版的 Bug 远远多于英文版，而补丁一般还会迟至少半个月（也就是说一般微软公布了漏洞后你的服务器还会有半个月处于无保护状态）。

二、 组件的定制

WIN2K 在默认情况下会安装一些常用的组件，但是正是这个默认安装是非常危险的，根据安全原则“最少的服务+最小的权限=最大的安全”，只安装确实需要的服务即可。这里特别提醒注意的是：“Indexing Service”、“FrontPage 2000 Server Extensions”、“ Internet Service Manager”这几个危险服务。

三、 管理应用程序的选择

选择一个好的远程管理软件是非常重要的事，这不仅仅是安全方面的要求，也是应用方面的需要。WIN2K 的 Terminal Service 是基于 RDP（远程桌面协议）的远程控制软件，它的速度快，操作方便，比较适合用来进行常规操作。但是，Terminal Service 也有其不足之处，由于它使用的是虚拟桌面，再加上微软编程的不严谨，当你使用 Terminal Service 进行安装软件或重启服务器等与真实桌面交互的操作时，往往会出现哭笑不得的现象，例如：使用 Terminal Service 重启微软的认证服务器（Compaq, IBM 等）可能会直接关机。所以，为了安全起见，建议再配备一个远程控制软件作为辅

此为试读，需要完整PDF请访问：www.ertongbook.com

助，和 Terminal Service 互补，如 PcAnyWhere 就是一个不错的选择。

四、 分区和逻辑盘的分配

至少建立两个分区，一个系统分区，一个应用程序分区。这是因为，微软的 IIS（Internet Ihformation Server）经常会有漏洞，如果把系统和 IIS 放在同一个驱动器会导致系统文件的泄漏，甚至让入侵者远程获取管理权。

推荐建立三个逻辑驱动器，第一个用来装系统和重要的日志文件；第二个放 IIS；第三个放 FTP，这样无论 IIS 或 FTP 出了安全漏洞都不会直接影响到系统目录和系统文件。

五、 安装顺序的选择

不要觉得只要能装上系统，就算完事了，其实 WIN2K 的安装顺序是非常重要的。

首先，要注意接入网络的时间。WIN2K 在安装时有一个漏洞，就是在输入 Administrator 的密码后，系统会建立“$ADMIN”的共享，但是并没有用刚输入的密码来保护它，这种情况一直会持续到计算机再次启动。在此期间，任何人都可以通过“$ADMIN”进入系统；同时，只要安装一完成，各种服务就会自动运行，而这时的服务器还到处是漏洞，非常容易从外部侵入。因此，在完全安装并配置好 WIN2K Server 之前，一定不要把主机接入网络。

其次，注意补丁的安装。补丁应该在所有应用程序安装完之后再安装，因为补丁程序往往要替换或修改某些系统文件，如果先安装补丁的话可能无法起到应有的效果。

怎么设

即使正确地安装了 WIN2K Server，系统也有很多漏洞，还需要进一步进行细致的配置。

一、 端口

端口是计算机和外部网络相连的逻辑接口，也是计算机的第一道屏障，端口配置正确与否直接影响到主机的安全。

二、 IIS

IIS 是微软的组件中问题最多的一个，平均两三个月就要出一个漏洞，而微软的 IIS 默认安装又实在不敢恭维，所以 IIS 的配置是我们的重点。

首先，删除 C 盘下的 Inetpub 目录，在 D 盘建一个 Inetpub，在 IIS 管理器中将主目录指向 D:\Inetpub。

其次，把 IIS 安装时默认的 scripts 等虚拟目录也一概删除，如果你需要什么权限的目录可以以后再建（特别注意写权限和执行程序的权限）。

然后是应用程序的配置。在 IIS 管理器中把无用映射都统统删除（当然必须保留如 ASP、ASA 等）。在 IIS 管理器中“主机·属性·WWW 服务编辑·主目录配置·应用程序映射”，然后开始一个个删吧。接着再在应用程序调试书签内，将“脚本错误消息”改为“发送文本”。点击“确定”退出时别忘了让虚拟站点继承刚才设定好的属性。

最后，为了保险起见，可以使用 IIS 的备份功能，将刚刚的设定全部备份下来，这样就可以随时恢复 IIS 的安全配置。还有，如果怕 IIS 负荷过高导致服务器死机，也可以在性能中打开 CPU 限制，如将 IIS 的最大 CPU 使用率限制在 70%。

三、 账号安全

首先，WIN2K 的默认安装允许任何用户通过空用户得到系统所有账号和共享列表，这本来是为了方便局域网用户共享资源和文件的，但是，同时任何一个远程用户也可以通过同样的方法得到你的用户列表，并可能使用暴力法破解用

户密码给整个网络带来破坏。很多人都只知道更改注册表 Local_Machine\System\CurrentControlSet\Control\LSA-RestrictAnonymous = 1 来禁止空用户连接，实际上 WIN2K 的本地安全策略里（如果是域服务器就是在域服务器安全和域安全策略里）就有这样的选项 RestrictAnonymous（匿名连接的额外限制），其中有三个值：

“0”：None， Rely on default permissions（无，取决于默认的权限）

“1”：Do not allow enumeration of SAM accounts and shares（不允许枚举 SAM 账号和共享）

“2”：No access without explicit anonymous permissions（没有显式匿名权限就不允许访问）

“0”这个值是系统默认的，没有任何限制，远程用户可以知道你机器上所有的账号、组信息、共享目录、网络传输列表(NetServerTransportEnum)等，对服务器来说这样的设置非常危险。“1”这个值是只允许非 NULL 用户存取 SAM 账号信息和共享信息。“2”这个值只有 WIN2K 才支持，需要注意的是，如果使用了这个值，就不能再共享资源了，所以还是推荐把数值设为“1”比较好。

四、 安全日志

这里需要注意：WIN2K 的默认安装是不开任何安全审核的！那么就应该到“本地安全策略·审核策略”中打开相应的审核，这里需要说明的是，审核项目如果太少的话，你万一想查看的时候发现没有记录那就一点办法都没有，但是审核项目如果太多，不仅会占用大量的系统资源，而且你也可能根本没空去全部看完，这样就失去了审核的意义。推荐的审核如下：

“账户管理”、“登录事件”、“策略更改”、“系统事件”、“账户登

录事件”需要把“成功”和“失败”都打开；“对象访问”、“特权使用”、“目录服务访问”就只打开“失败”。

与之相关的还有，在“账户策略·密码策略”中设定：“密码复杂性要求启用”、“密码长度最小值 6 位”、“强制密码历史 5 次”、“最长存留期 30 天”；在“账户策略·账户锁定策略”中设定：“账户锁定 3 次错误登录”、“锁定时间 20 分钟”、“复位锁定计数 20 分钟”等。

Terminal Service 的安全日志默认也是不启用的，可以在“Terminal Service Configration（远程服务配置）·权限·高级”中配置安全审核，一般来说只要记录登录、注销事件就可以了。

五、 目录和文件权限

为了控制好服务器上用户的权限，同时也为了预防以后可能的入侵和溢出，还必须非常小心地设置目录和文件的访问权限。NT 的访问权限分为：读取、写入、读取及执行、修改、列目录、完全控制。在默认的情况下，大多数的文件夹对所有用户（Everyone 这个组）是完全敞开的（Full Control），你需要根据应用的需要进行权限重设。在进行权限控制时，请记住以下几个原则：

1. 权限是累计的，如果一个用户同时属于两个组，那么他就有了这两个组所允许的所有权限。

2. 拒绝的权限要比允许的权限高（拒绝策略会先执行）。如果一个用户属于一个被拒绝访问某个资源的组，那么不管其他的权限设置给他开放了多少权限，他也一定不能访问这个资源。

3. 文件权限比文件夹权限高。

4. 利用用户组来进行权限控制是一个成熟的系统管理员必须具有的优良习惯。

此为试读，需要完整PDF请访问：www.ertongbook.com

5. 只给用户真正需要的权限，权限的最小化原则是安全的重要保障。

6. 预防 ICMP 攻击：ICMP 的风暴攻击和碎片攻击也是 NT 主机比较头疼的攻击方法，其实应付的方法也很简单，WIN2K 自带一个 Routing & Remote Access 工具，这个工具初具路由器的雏形。在这个工具中，我们可以轻易地定义输入输出包过滤器。如设定输入 ICMP 代码 255 丢弃就表示丢弃所有的外来 ICMP 报文。

要注意

实际上，安全和应用在很多时候是矛盾的，因此，你需要在其中找到平衡点，毕竟服务器是给用户用的，如果安全原则妨碍了系统应用，那么这个安全原则也不是一个好的原则。

网络安全是一项系统工程，它不仅有空间的跨度，还有时间的跨度。很多朋友（包括部分系统管理员）认为进行了安全配置的主机就是安全的，其实这里有个误区，我们只能说一台主机在一定的情况下一定的时间内是安全的，随着网络结构的变化、新的漏洞的发现、管理员和用户的操作，主机的安全状况是随时随地变化着的，只有让安全意识和安全制度贯穿整个过程才能做到真正的安全。

用 Apache 实现虚拟主机服务

什么是虚拟主机服务

所谓的虚拟主机服务就是指将一台机器虚拟成多台 WEB 服务器。举个例子来说，一家公司想从事提供主机代管服务，它为其它企业提供 WEB 服务。那么它肯定不是为每一家企业都各准备一台物理上的服务器，而是用一台功能较强

大的大型服务器，然后用虚拟主机的形式，提供多个企业的 WEB 服务，虽然所有的 WEB 服务就是这台服务器提供的，但是让访问者看起来却是在不同的服务器上获得 WEB 服务一样。

具体地说，就是，我们可以利用虚拟主机服务将两个不同公司 www.company1.com 与 www.company2.com 的主页内容都存放在同一台主机上。而访问者只需输入公司的域名就可以访问到它想得到的主页内容。

用 Apache 设置虚拟主机服务通常可以采用两种方案：基于 IP 地址的虚拟主机和基于名字的虚拟主机，下面我们分别介绍一下它们的实现方法。以便大家在具体的应用中能够选择最合适的实现方法。

6.2 设置实现基于 IP 地址的虚拟主机服务

实现前提

这种方式需要在机器上设置 IP 别名，也就是在一台机器的网卡上绑定多个

IP 地址去为多个虚拟主机服务。而且要使用这项功能还要确定在你的 LINUX 内核中必须支持 IP 别名的设置，否则你还必须重新编译内核。

下面举一个拥有两个虚拟主机的服务设置，以供参考。

2．配置步骤

假设，我们用来实现虚拟主机服务的机器，首先已经为自己提供了 WEB 服务，现在将为新的一家公司 www.company1.com 提供虚拟主机服务。

规划 IP 地址：为虚拟主机申请新的 IP 地址。（假设本机

IP 地址为 202.101.2.1）

Www.company1.com 202.101.2.2

2) 让 ISP 作好相应的域名解析工作。

3) 为网卡设置 IP 别名：

/sbin/ifconfig eth0:0 202.101.2.2 netmask 255.255.255.0

4) 重新设置“/etc/httpd/conf/httpd.conf”,在文件中加入：

<VirtualHost 202.101.2.2>

ServerAdmin webmaster@yourdomain.com

DocumentRoot /home/httpd/www.company1.com

ServerName www.company1.com

ErrorLog /var/log/httpd/www.company1.com/error.log

</VirtualHost>

5）建立相应的目录。

mkdir /home/httpd/www.company1.com

mkdir /var/log/httpd/www.company1.com/error.log

6)将相应的主页内容存放在相应的目录中即可。

3．不利因素

这种虚拟主机的实现方法有一个严重的不足，那就是，每增加一个虚拟主机，就必须增加一个 IP 地址。而由于 IP 地址空间已经十分紧张，所以通常情况下是无法取得这么多的 IP 地址的。而且从某种意义上说，这也是一种 IP 地址浪费。

6.3 设置实现基于名字的虚拟主机服务

而基于名字的虚拟主机服务，是比较适合使用的一种方案。因为它不需要更多的 IP 地址，而且配置简单，无须什么特殊的软硬件支持。现代的浏览器大都支持这种虚拟主机的实现方法。当然，这也就是指一些早期的客户端浏览器也许

不支持这种虚拟主机的实现方法。

正是以上原因，我们没有理由不使用基于名字的虚拟主机服务而使用基于 IP 地址的虚拟主机服务。配置基于名字的虚拟主机服务需要修改配置文件："/etc/httpd/conf/httpd.conf"，在这个配置文件中增加以下内容。

```
NameVirtualHost 202.101.2.1
<VirtualHost 202.101.2.1>
ServerAdmin webmaster@yourdomain.com
DocumentRoot /home/httpd/www.company1.com
ServerName www.company1.com
ErrorLog /var/log/httpd/www.company1.com/error.log
</VirtualHost>
<VirtualHost 202.101.2.1>
ServerAdmin webmaster@yourdomain.com
DocumentRoot /home/httpd/www.company2.com
ServerName www.company2.com
ErrorLog /var/log/httpd/www.company2.com/error.log
</VirtualHost>
```

也就是在基于 IP 地址的配置基础上增加一句：NameVirtualHost 202.101.2.1 而已。在本例中，为了体现只需要增加一次，所以特别地设置了两个虚拟主机服务。

最后也是建立相应的目录，将主页内容放到相应的目录中去就可以了。

WIN2003 下配置 ASP、CGI、PHP 环境

我们要使 IIS 实现 ASP,CGI,PERL 和 PHP 所需软件(都要是 For Windows 的)：ActivePerl、PHP,ASP(WINDOWNS2

此为试读，需要完整PDF请访问：www.ertongbook.com

003 自带)ActivePerl 下载：http://tj-http.skycn.net:8080/down/ActivePerl-5.6.1.633-MSWin32-x86.zip

PHP 下载：http://tj-http.skycn.net:8080/down/php-4.3.1-Win32.zip

一.ASP 支持： 按装 IIS 后,打开 INTERNET 信息服务(IIS)管理器,打开允许 ASP 环境,现在我们就可以使用 ASP 环境了.

二.CGI,PERL 支持:

1.安装 ActivePerl

运行下载的 ActivePerl 一步一步安装(注意:安装路径请选择到根目录的/usr/下(默认是 perl),这样对以后调试程序省很多事)

2.配置 IIS 打开"Internet 信息服务"(在'管理工具'里),点开默认站点的属性选择 "主目录" 选项卡，然后点 "配置(G)然后 "添加(D)"推荐"c:\usr\bin\perl.exe" 记得一定要在后面加上" %s %s "",不然没法执行 cgi 的，大家一定要在最后那个 %S 后加",还要系统会提示"包含空格的项目的文件/路径部分需要用括号括起来",确定后。用同样的方法添加扩展.pl，最后使开启系统的允许 CGI 环境现在你的 IIS 已经支持 cgi,perl 了！

三.PHP、MYSQL 支持：

1.安装 PHP 运行下载的 PHP 一步一步安装就行了（装到哪里都行,一般现在网上流行的都是安装过的 PHP,没有安装程序 c:\php 下）

2 配置 IIS：和刚才配置 cgi 一样，添加.php 现在基本上完成了环境使需求,我们完成最后的工作，把"执行权限" 该成："脚本和可执行文件" ,勾上资源访问,点确定最后再进到站点属性的"配置(G)..."---->"选项"---->"勾上启用父路径"--->

确定；到这里就算是完成了这次配置,接下来的工作就是你们的啦.

整理一些 WIN2000 的常用服务列表

WIN2000 提供服务的列表，包括详细的描述，服务名称，显示名称，可执行文件的路径！

在命令提示符下可以启动，停止下面的服务。

net start 服务名称

net start 停止服务

例：

net start Telnet

开启了 Telnet 服务，我们就可以用:telnet ip

net start Telnet

停止 Telnet 服务

服务名称：Alerter

显示名称：Alerter

描述：通知所选用户和计算机有关系统管理级警报。

可执行文件的路径：C:\WINNT\System32\services.exe

服务名称：AppMgmt

显示名称：Application Management

描述：提供软件安装服务，诸如分派，发行以及删除。

可执行文件的路径：C:\WINNT\system32\services.exe

服务名称：Ati HotKey Poller

显示名称：Ati HotKey Poller

描述：[]

可执行文件的路径：C:\WINNT\System32\Ati2evxx.exe

服务名称：ClipSrv

显示名称：ClipBook

描述：支持“剪贴簿查看器”，以便可以从远程剪贴簿查阅剪贴页面。

可执行文件的路径：C:\WINNT\system32\clipsrv.exe

服务名称：EventSystem

显示名称：COM+ Event System

描述：提供事件的自动发布到订阅 COM 组件。

可执行文件的路径：C:\WINNT\System32\svchost.exe -k netsvcs

服务名称：Browser

显示名称：Computer Browser

描述：维护网络上计算机的最新列表以及提供这个列表给请求的程序。

可执行文件的路径：C:\WINNT\System32\services.exe

服务名称：Dhcp

显示名称：DHCP Client

描述：通过注册和更改 IP 地址以及 DNS 名称来管理网络配置。

可执行文件的路径：C:\WINNT\System32\services.exe

服务名称：TrkWks

显示名称：Distributed Link Tracking Client

描述：当文件在网络域的 NTFS 卷中移动时发送通知。

可执行文件的路径：C:\WINNT\system32\services.exe

服务名称：MSDTC

显示名称：Distributed Transaction Coordinator

描述：并列事务，是分布于两个以上的数据库，消息队列，文件系统，或其它事务保护资源管

理器。

可执行文件的路径：C:\WINNT\System32\msdtc.exe

服务名称：Dnscache

显示名称：DNS Client

描述：**解析和缓冲域名系统** (DNS) **名称**。

可执行文件的路径：C:\WINNT\System32\services.exe

服务名称：Eventlog

显示名称：Event Log

描述：**记录程序和** Windows **发送的事件消息**。**事件日志包含对诊断问题有所帮助的信息**。**您**

可以在“事件查看器”中查看报告。

可执行文件的路径：C:\WINNT\system32\services.exe

服务名称：Fax

显示名称：Fax Service

描述：**帮助您发送和接收传真**

可执行文件的路径：C:\WINNT\system32\faxsvc.exe

服务名称：MSFTPSVC

显示名称：FTP Publishing Service

描述：**通过** Internet **信息服务的管理单元提供** FTP **连接和管理**。

可执行文件的路径：C:\WINNT\System32\inetsrv\inetinfo.exe

服务名称：IISADMIN

显示名称：IIS Admin Service

描述：**允许通过** Internet **信息服务的管理单元管理** Web **和** FTP **服务**。

可执行文件的路径：C:\WINNT\System32\inetsrv\inetinfo.exe

服务名称：cisvc

显示名称：Indexing Service

描述：本地和远程计算机上文件的索引内容和属性；通过灵活查询语言提供文件快速访问。

可执行文件的路径：C:\WINNT\System32\cisvc.exe

服务名称：Irmon

显示名称：Infrared Monitor

描述：支持安装在这台计算机上的红外设备并且检测在有效范围内的其它红外设备。

可执行文件的路径：C:\WINNT\System32\svchost.exe -k netsvcs

服务名称：SharedAccess

显示名称：Internet Connection Sharing

描述：为通过拨号网络连接的家庭网络中所有计算机提供网络地址转换、定址以及名称解析服

务。

可执行文件的路径：C:\WINNT\System32\svchost.exe -k netsvcs

服务名称：PolicyAgent

显示名称：IPSEC Policy Agent

描述：管理 IP 安全策略以及启动 ISAKMP/Oakley (IKE) **和 IP 安全驱动程序**。

可执行文件的路径：C:\WINNT\System32\lsass.exe

服务名称：dmserver

显示名称：Logical Disk Manager

描述：逻辑磁盘管理器监视狗服务

可执行文件的路径：C:\WINNT\System32\services.exe

服务名称：dmadmin

显示名称：Logical Disk Manager Administrative Servic

e

描述：磁盘管理请求的系统管理服务

可执行文件的路径：C:\WINNT\System32\dmadmin.exe /com

服务名称：Messenger

显示名称：Messenger

描述：发送和接收系统管理员或者“警报器”服务传递的消息。

可执行文件的路径：C:\WINNT\System32\services.exe

服务名称：MSUpdate

显示名称：Microsoft Windows Update Service

描述：Microsoft(R) Windows Update

可执行文件的路径：C:\WINNT\System32\wupdmgr32.exe

服务名称：Netlogon

显示名称：Net Logon

描述：支持网络上计算机 pass-through **帐户登录身份验证事件。**

可执行文件的路径：C:\WINNT\System32\lsass.exe

服务名称：mnmsrvc

显示名称：NetMeeting Remote Desktop Sharing

描述：允许有权限的用户使用 NetMeeting **远程访问** Windows **桌面。**

可执行文件的路径：C:\WINNT\System32\mnmsrvc.exe

服务名称：Netman

显示名称：Network Connections

描述：管理“网络和拨号连接”文件夹中对象，在其中您可以查看局域网和远程连接。

此为试读，需要完整PDF请访问：www.ertongbook.com