Windows 2008服务器安全加固方案

Windows 2008服务器安全加固方案(一)

因为IIS(即Internet Information Server)的方便性和易用性，使它成为最受欢迎的Web服务器软件之一。但是，IIS的安全性却一直令人担忧。如何利用IIS建立一个安全的Web服务器，是很多人关心的话题。要创服务器安全检测建一个安全可靠的Web服务器，必须要实现Windows 2003和IIS的双重安全，因为IIS的用户同时也是Windows 2003的用户，并且IIS目录的权限依赖Windows的NTFS文件系统的权限控制，所以保护IIS安全的第一步就是确保Windows 2000操作系统的安全，所以要对服务器进行安全加固，以免遭到黑客的攻击，造成严重的后果。

我们通过以下几个方面对您的系统进行安全加固：

1.
系统的安全加固：我们通过配置目录权限，系统安全策略，协议栈加强，系统服务和访问控制加固您的系统，整体提高服务器的安全性。

2.
IIS手工加固：手工加固iis可以有效的提高iweb站点的安全性服务器安全加固，合理分配用户权限，配置相应的安全策略，有效的防止iis用户溢出提权。

3.
系统应用程序加固，提供应用程序的安全性，例如sql的安全配置以及服务器应用软件的安全加固。

系统的安全加固:

1.目录权限的配置:

1.1
除系统所在分区之外的所有分区都赋予Administrators和SYSTEM有完全控制权，之后再对其下的子目录作单独的目录权限，如果WEB站点目录，你要为其目录权限分配一个与之对应的匿名访问帐号并赋予它有修改权限，如果想使网站更加坚固，可以分配只读权限并对特殊的目录作可写权限。

1.2
系统所在分区下的根目录都要设置为不继承父权限，之后为该分区只赋予Administrators和SYSTEM有完全控制权。

1.3 因为服务器只有管理员有本地登录权限，所在要配置Documents and Settings这个目录权限只保留Administrators和SYSTEM有完全控制权，其下的子目录同样。另外还有一个隐藏目录也需要同样操作。因为如果你安装有PCAnyWhere那么他的的配置信息都保存在其下，使用webshell或FSO可以轻松的调取这个配置文件。

1.4 配置Program files目录，为Common Files目录之外的所有目录赋予Administrators和SYSTEM有完全控制权。

1.5
配置Windows目录，其实这一块主要是根据自身的情况如果使用默认的安全设置也是可行的，不过还是应该进入SYSTEM32目录下，将

cmd.exe、ftp.exe、net.exe、scrrun.dll、shell.dll这些杀手锏程序赋予匿名帐号拒绝访问。

1.6审核MetBase.bin，C:\WINNT\system32\inetsrv目录只有administrator只允许Administrator用户读写。

2.组策略配置:

在用户权利指派下，从通过网络访问此计算机中删除Power Users和Backup Operators;

启用不允许匿名访问SAM帐号和共享;

启用不允许为网络验证存储凭据或Passport;

从文件共享中删除允许匿名登录的DFS$和COMCFG;

启用交互登录:不显示上次的用户名;

启用在下一次密码变更时不存储LANMAN哈希值;

禁止IIS匿名用户在本地登录;

3.本地安全策略设置:

开始菜单—>管理工具—>本地安全策略

A、本地策略——>审核策略

审核策略更改□成功□失败

审核登录事件□成功□失败

审核对象访问失败

审核过程跟踪□无审核

审核目录服务访问失败

审核特权使用失败

审核系统事件□成功□失败

审核账户登录事件□成功□失败

审核账户管理□成功□失败

注:在设置审核登陆事件时选择记失败,这样在事件查看器里的安全日志就会记录登陆失败的信息。

B、本地策略——>用户权限分配

关闭系统:只有Administrators组、其它全部删除。

通过终端服务拒绝登陆:加入Guests、User组

通过终端服务允许登陆:只加入Administrators组,其他全部删除

C、本地策略——>安全选项

交互式登陆:不显示上次的用户名□启用

网络访问:不允许SAM帐户和共享的匿名枚举启用

网络访问:不允许为网络身份验证储存凭证□启用

网络访问:可匿名访问的共享□全部删除

网络访问:可匿名访问的命全部删除

网络访问:可远程访问的注册表路径全部删除

网络访问:可远程访问的注册表路径和子路径全部删除

帐户:重命名来宾帐户重命名一个帐户

帐户:重命名系统管理员帐户□重命名一个帐户

****

Windows Server 2008用户权限管理

几十年来，大型机和服务器一直使用“超级用户”和“用户”这种用户控制方案。这种方案存在一个明显的安全问题：它需要防止普通用户获取非法访问权限。

在DOS电脑以及随后的Windows操作系统中，访问控制模式更加复杂。早期的Windows操作系统不能在同一台机器上设置不同的用户权限；所有的行动都需要超级用户执行。但是，Windows NT系统最终定义了管理员角色和用户角色，尽管在实际情况中大多数用户还是需要超级用户的访问权限来执行他们平时的操作。

今天，许多企业的业务模式都要求大范围（地理位置上的）的联合操作，Windows NT中简单的特权/非特权用户管理功能已经不够用了。意识到这一趋势之后，微软在2009年开发了Windows Server 2008，该系统具有以多级权限属性系统为基础的多层次管理模式。该模式可以限制标准用户，让他们只能用非特权的形式运行应用程序软件，只留给他们操作所需要的最小管理权限，从而改进了微软Windows的安全性。比如，服务台用户只能改变其他用户的密码。通过这种方式，大型企业中的用户管理权限可以受到限制，操作中的超级用户数量减少。在本文中，我们将讨论一下如何使用Windows Server 2008对权限分配进行控制。

域上的权限管理

在Windows Server 2008环境中，有两种政策：活动目录（AD）全局域政策以及本地服务器安全帐户

管理器(SAM)注册表政策。AD利用它的目录架构来控制任何给定Windows服务器域(支持通用安全政策的一组服务器)的组权限。这使得AD可以对域中的所有用户帐户执行公共帐户权限管理。

当有新的Windows服务器添加进来时，他们会连接到活动目录，活动目录会检查所有的组政策对象(Group Policy Objects，GPO)——

用户能够执行的应用程序和服务——并把这些权限链接到该目录下的Active Directory Users and
Computers(活动目录用户和计算机)分支中的域根用户。然后AD把这些定义的、默认的权限传递到新服务器上，开始管理其用户。AD目录下的组织单元(Organization
Unit，OU)分支也可以定义，人们可以用OU为计算机创建本地帐户政策。比如，服务台OU可以定义一系列全局政策，帮助服务台人员执行具有公共权限的活动。

Windows Server
2008的活动目录还引进了一个新的功能，叫做多元密码政策(Fine-Grained Password
Policy)，其中包括一个锁定政策。有了这个新功能后，公司可以在同一个域中对不同的用户使用不同的密码和锁定政策。这个功能出现之前，整个域中只有一个政策。为了充分利用这个功能，活动目录管理员必须创建一个新的对象，名为密码设置对象(Password Settings
Object，PSO)。他或她可以在PSO中设定同样的密码最长期限、复杂度要求、锁定阈值，等等。然后，PSO会连接到一个活动目录组:组的范围为全局(Global)(不是

本地(Local或者通用(Univeral)),组的类型为安全(Security)(不是分布(Distribution))。所有的组成员都会继承链接到该组的PSO中定义的密码和锁定政策。

本地多级控制

域上的全局政策配置完成以后,人们就可以在单独的Windows Server 2008系统中通过用户权利分配(User Rights Assignment, URA)功能定义本地权限。用户权利能够控制用户在计算机上执行哪些任务。这些权利包括登录权限和特权。登录权限控制哪些人有权登录到计算机上,以及他们如何登录:通过网络还是本地,作为批处理工作还是作为服务登录。特权则控制计算机和域资源的访问,并可以覆盖特定对象上设定的权限,比如备份文件和目录、创建全局对象、调试程序等等。这些特权由系统URA对象下的组政策(Group Policy)进行管理,而且两种用户权利都是由管理员分配到组或者单独用户,作为系统安全设置的一部分。请注意,管理员应该尽可能地通过分组来管理本地权利,确保与企业政策的一致性以及最小化单独系统中权限管理的困难程度。

为了访问本地URA对象,添加、删除或者修改权限,管理员必须在Windows Server 2008中用Windows控制面板打开本地安全设置(Local Security Settings)。他或她可以在左边看见一个树状目录。点击本地政策(Local Policies),然后选择用户权利分配(User Rights Assignment),就能够编辑所有的39个登录权利和权限了。

确保适当的权限

Windows Server
2008中有九个审计政策，分成两个子类，它们可以确保Windows管理员正确设置用户权限。安全团队可以在计算机中打开本地安全政策（Local Security Policy）控制台，进入Security Settings\Local Policies\Audit Policy目录，查看系统审计政策设置。下文简要地描述了每个政策，以及它们的用法：

审计帐户登录事件——

跟踪所有试图用域用户帐户登录的活动，不管这种尝试源自何处。开启这项政策以后，工作站或者成员服务器会记录所有使用计算机SAM中存储的本地帐户的登录尝试。

审计帐户管理——

用来监视用户帐户和组的变化，对管理员和服务台工作人员的审计活动有参考价值。该政策记录密码重置、新创建的帐户以及组成员和Active Directory控制器的变化。该政策还记录域用户、域分组以及计算机帐户的变化。

审计目录服务访问——提供Active Directory中对象变化的低级别审计跟踪。该政策跟踪的活动与审计帐户管理事件中跟踪的相同，但是级别低很多。使用这个政策可以识别用户帐户的哪些领域或者任何其他Active Directory对象被访问过。审计帐户管理事件可以提供更好的用户帐户和组的监视维护信息，但是审计目录服务访问是跟踪OU和GPO变化的唯一途径，这对于变化控制来说很重要。

审计登录事件——

记录本地计算机上的登录尝试，无论使用域帐户还是本地帐户登录。在Active Directory域控制器中，该政策只记录访问域控制器的尝试。

审计对象访问——处理Active Directory之外所有对象的访问审计。该政策可以用来审计任何类型的Windows对象访问，包括注册表键值、打印机、以及服务。（注意：如果服务器的对象太多，该政策可能会大大影响该服务器的性能。）

审计政策变化——

提供本地系统中重要安全政策的变化通知，比如系统审计政策的变化；当本地系统是一个Active Directory域控制器时，该政策会提供信任关系的变化。

审计权限使用---跟踪Security Settings\Local Policies\User Right Assignment目录下本地安全政策（Local Security Policy）的用户权利活动

审计过程跟踪——

跟踪每一个被执行的程序，不管该程序是由系统还是最终用户执行的。它还可以决定程序运行的时间。结合该政策，加上审计登录事件和审计对象访问事件，以及在这些不同的事件描述中使用Logon ID, Process ID 和Handle ID等，我们就可以详细地描绘出用户活动了。

审计系统事件——

与安全相关的系统事件综合，包括系统启动和关闭。Windows的安全基础设施是

模块化设计，可以利用微软和第三方供应商提供的新型、插件安全功能。这些插件可以是认证软件包、合法登录进程或者通知软件包。因为这些插件是值得信赖的扩展操作系统的代码模块，Windows加载每个插件时都会做记录，使用从这个分类中的事件。(注意:不推荐在这个层面上管理审计政策，因为这样会产生很多噪声，应该使用子类型。)

即使有些用户偶尔得到了不必要的权限，这些政策也可以让公司的安全人员核实这些用户是否利用管理权限做伤害公司的事情，不管是有意的还是无意的。企业应该尽可能多的启用这些审计政策，但是请记住，加载所有的政策可能会影响Windows系统的性能。

当启用这些政策时，企业有多种选择:可以让它们产生成功事件，失败事件或者两者都产生，这取决于公司政策。所有九个审计政策都可以产生成功事件，某些政策可以产生失败事件，作为一种最佳实践，企业不该忽略成功事件(会产生大量的安全日志)而只开启失败事件。一个常见的误解是:只有失败事件审计政策才能警告安全团队注意所有的可疑活动。实际上，安全日志中许多最重要的事件是成功事件，比如关键用户帐户和组的变化、帐户锁定的变化，以及安全设置的变化等等。

总结

随着Windows Server
2008的发布，微软最终提供了权限管理功能，能够创建复杂的用户权限分组，却不需要复杂的管理技术。但是复杂的权限分组可能会引起权限的错误配置，不能识别某个人的错误。所以，了解与该功能相关的审计服务同样重要。

归功于适当的考虑和规划，Windows Server 2008最终赋予企业期待已久的功能：成功地匹配了用户的能力和权限。这不仅满足业务需求和信任要求，而且验证了他们的方法是正确的。

Web专用网站服务器的安全设置(1)

IIS的相关设置:

删除默认建立的站点的虚拟目录，停止默认web站点，删除对应的文件目录c:inetpub，配置所有站点的公共设置，设置好相关的连接数限制，
带宽设置以及性能设置等其他设置。配置应用程序映射，删除所有不必要的应用程序扩展，只保留asp，php，cgi，pl，aspx应用程序扩展。对于php和cgi，推荐使用isapi方式解析，用exe解析对安全和性能有所影响。用户程序调试设置发送文本错误信息给客户。

对于数据库，尽量采用mdb后缀，不需要更改为asp，可在IIS中设置一个mdb的扩展映射，将这个映射使用一个无关的dll文件如C:WINNTsystem32inetsrvssinc.dll来防止数据库被下载。设置IIS的日志保存目录，调整日志记录信息。设置为发送文本错误信息。修改403错误页面，将其转向到其他页，可防止一些扫描器的探测。另外为隐藏系统信息，防止telnet到80端口所泄露的系统版本信息可修改IIS的banner信息，可以使用winhex手工修改或者使用相关软件如banneredit修改。

对于用户站点所在的目录，在此说明一下，用户的FTP根目录下对应三个文件佳，wwwroot，database，logfiles，分别存放站点文件，数据库备份和该站点的日志。如果一旦发生入侵事件可对该用户站点所在目录设置具体的权限，图片所在的目录只给予列目录的权限，程序所在目录如果不需要生成文件（如生成html的程序）不给予写入权限。因为是虚拟主机平常对脚本安全没办法做到细致入微的地步。

方法

用户从脚本提升权限:

ASP的安全设置:

设置过权限和服务之后，防范asp木马还需要做以下工作，在cmd窗口运行以下命令:

```
regsvr32/u C:\WINNT\System32\wshom.ocx
del C:\WINNT\System32\wshom.ocx
regsvr32/u C:\WINNT\system32\shell32.dll
del C:\WINNT\system32\shell32.dll
```

即可将WScript.Shell, Shell.application, WScript.Network组件卸载，可有效防止asp木马通过wscript或shell.application执行命令以及使用木马查看一些系统敏感信息。另法:可取消以上文件的users用户的权限，重新启动IIS即可生效。但不推荐该方法。

另外，对于FSO由于用户程序需要使用，服务器上可以不注销掉该组件，这里只提一下FSO的防范，但并不需要在自动开通空间的虚拟商服务器上使用，只适合于手工开通的站点。可以针对需要FSO和不需要FSO的站点设置两个组，对于需要FSO的用户组给予c:winntsystem32scrrun.dll文件的执行权限，不需要的不给权限。重新启动服务器即可生效。

对于这样的设置结合上面的权限设置，你会发现海阳木马已经在这里失去了作用！

PHP的安全设置:

默认安装的php需要有以下几个注意的问题:

C:\winnt\php.ini只给予users读权限即可。在php.ini里需要做如下设置:

Safe_mode=on 原为:On

register_globals = Off

allow_url_fopen = Off 原为:On

display_errors = Off

magic_quotes_gpc = On [默认是on，但需检查一遍] 原为:Off

open_basedir =web目录

disable_functions

=passthru,exec,shell_exec,system,phpinfo,get_cfg_var,popen,chmod 原为:空

默认设置com.allow_dcom = true修改为false[修改前要取消掉前面的;]

MySQL安全设置:

如果服务器上启用MySQL数据库，MySQL数据库需要注意的安全设置为:

删除mysql中的所有默认用户，只保留本地root帐户，为root用户加上一个复杂的密码。赋予普通用户updatedeletealertcreatedrop权限的时候，并限定到特定的数据库，尤其要避免普通客户拥有对mysql数据库操作的权限。检查mysql.user表，取消不必要用户的shutdown_priv,reload_priv,process_priv和File_priv权限，这些权限可能泄漏更多的服务器信息包括非mysql的其它信息出去。可以为mysql设置一个启动用户，该用户只对mysql目录有权限。设置安装目录的data数据库的权限(此目录存放了mysql数据库的数据信息)。对于mysql安装目录给users加上读取、列目录和执行权限。

Serv-u安全问题:

安装程序尽量采用最新版本，避免采用默认安装目录，设置好serv-u目录所在的权限，设置一个复杂的管理员密码。修改serv-u的banner信息，设置被动模式端口范围（4001—4003）在本地服务器中设置中做好相关安全设置：包括检查匿名密码，禁用反超时调度，拦截“FTP bounce”攻击和FXP，对于在30秒内连接超过3次的用户拦截10分钟。域中的设置为：要求复杂密码，目录只使用小写字母，高级中设置取消允许使用MDTM命令更改文件的日期。

更改serv-u的启动用户：在系统中新建一个用户，设置一个复杂点的密码，不属于任何组。将servu的安装目录给予该用户完全控制权限。建立一个FTP根目录，需要给予这个用户该目录完全控制权限，因为所有的ftp用户上传，删除，更改文件都是继承了该用户的权限，否则无法操作文件。另外需要给该目录以上的上级目录给该用户的读取权限，否则会在连接的时候出现530 Not logged in, home directory does not exist。比如在测试的时候ftp根目录为d:soft，必须给d盘该用户的读取权限，为了安全取消d盘其他文件夹的继承权限。而一般的使用默认的system启动就没有这些问题，因为system一般都拥有这些权限的。

数据库服务器的安全设置

对于专用的MSSQL数据库服务器，按照上文所讲的设置TCP/IP筛选和IP策略，对外只开放1433和5631端口。对于MSSQL首先需要为sa设置一个强壮的密码，使用

混合身份验证,加强数据库日志的记录,审核数据库登陆事件的"成功和失败".删除一些不需要的和危险的OLE自动存储过程(会造成企业管理器中部分功能不能使用),这些过程包括如下:

Sp_OAcreate Sp_OADestroy Sp_OAGetErrorInfo Sp_OAGetProperty
Sp_OAMethod Sp_OASetProperty Sp_OAStop

去掉不需要的注册表访问过程,包括有:

Xp_regaddmultistring Xp_regdeletekey Xp_regdeletevalue
Xp_regenumvalues Xp_regread Xp_regremovemultistring
Xp_regwrite

去掉其他系统存储过程,如果认为还有威胁,当然要小心drop这些过程,可以在测试机器上测试,保证正常的系统能完成工作,这些过程包括:

xp_cmdshell xp_dirtree xp_dropwebtask sp_addsrvrolemember
xp_makewebtask xp_runwebtask xp_subdirs sp_addlogin
sp_addextendedproc

在实例属性中选择TCP/IP协议的属性。选择隐藏 SQL Server 实例可防止对1434端口的探测,可修改默认使用的1433端口。除去数据库的guest 账户把未经认可的使用者据之在外。例外情况是master和 tempdb 数据库,因为对他们guest帐户是必需的。另外注意设置好各个数据库用户的权限,对于这些用户只给予所在数据库的一些权限。在程序中不要用sa用户去连接任何数据库。网络上有建议大家使用协议加密的,千万不要这么做,否则你只能重装MSSQL了。

Web专用网站服务器的安全设置(2)

第二部分 入侵检测和数据备份

1.1 入侵检测工作

作为服务器的日常管理，入侵检测是一项非常重要的工作，在平常的检测过程中，主要包含日常的服务器安全例行检查和遭到入侵时的入侵检查，也就是分为在入侵进行时的安全检查和在入侵前后的安全检查。系统的安全性遵循木桶原理，木桶原理指的是：一个木桶由许多块木板组成，如果组成木桶的这些木板长短不一，那么这个木桶的最大容量不取决于长的木板，而取决于最短的那块木板。应用到安全方面也就是说系统的安全性取决于系统中最脆弱的地方，这些地方是日常的安全检测的重点所在。

日常的安全检测

日常安全检测主要针对系统的安全性，工作主要按照以下步骤进行：

1. 查看服务器状态：

打开进程管理器，查看服务器性能，观察CPU和内存使用状况。查看是否有CPU和内存占用过高等异常情况。

2. 检查当前进程情况

切换“任务管理器”到进程，查找有无可疑的应用程序或后台进程在运行。用进程管理器查看进程时里面会有一项taskmgr，这个是进程管理器自身的进程。如果正

在运行windows更新会有一项wuauclt.exe进程。对于拿不准的进程或者说不知道是服务器上哪个应用程序开启的进程，可以在网络上搜索一下该进程名加以确定[进程知识库:http://www.dofile.com/]。通常的后门如果有进程的话，一般会取一个与系统进程类似的名称，如svch0st.exe，此时要仔细辨别[通常迷惑手段是变字母o为数字0，变字母l为数字1。

3. 检查系统帐号

打开计算机管理，展开本地用户和组选项，查看组选项，查看administrators组是否添加有新帐号，检查是否有克隆帐号。

4. 查看当前端口开放情况

使用activeport，查看当前的端口连接情况，尤其是注意与外部连接着的端口情况，看是否有未经允许的端口与外界在通信。如有，立即关闭该端口并记录下该端口对应的程序并记录，将该程序转移到其他目录下存放以便后来分析。打开计算机管理==》软件环境==》正在运行任务在(此处可以查看进程管理器中看不到的隐藏进程)，查看当前运行的程序，如果有不明程序，记录下该程序的位置，打开任务管理器结束该进程，对于采用了守护进程的后门等程序可尝试结束进程树，如仍然无法结束，在注册表中搜索该程序名，删除掉相关键值，切换到安全模式下删除掉相关的程序文件。

5. 检查系统服务

运行services.msc，检查处于已启动状态的服务，查看是否有新加的未知服务并确定服务的用途。对于不清楚的服务打开该服务的属性，查看该服务所对应的可执行文件是什么，如果确定该文件是系统内的正常使用的文件，可粗略放过。查看是否有其他正常开放服务依存在该服务上，如果有，可以粗略的放过。如果无法确定该执行文件是否是系统内正常文件并且没有其他正常开放服务依存在该服务上，可暂时停止掉该服务，然后测试下各种应用是否正常。对于一些后门由于采用了hook系统API技术，添加的服务项目在服务管理器中是无法看到的，这时需要打开注册表中的HKEY_LOCAL_MACHINESYSTEMCurrentControlSetServices项进行查找，通过查看各服务的名称、对应的执行文件来确定是否是后门、木马程序等。

6. 查看相关日志

运行eventvwr.msc，粗略检查系统中的相关日志记录。在查看时在对应的日志记录上点右键选“属性”，在“筛选器”中设置一个日志筛选器，只选择错误、警告，查看日志的来源和具体描述信息。对于出现的错误如能在服务器常见故障排除中找到解决办法则依照该办法处理该问题，如果无解决办法则记录下该问题，详细记录下事件来源、ID号和具体描述信息，以便找到问题解决的办法。

7. 检查系统文件

主要检查系统盘的exe和dll文件，建议系统安装完毕之后用dir *.exe /s >1.txt将C盘所有的exe文件列表保存下来，然后每次检查的时候再用该命令生成一份当时的列表，用fc比较两个文件，同样如此针对dll文件做相关检查。需要注

意的是打补丁或者安装软件后重新生成一次原始列表。检查相关系统文件是否被替换或系统中是否被安装了木马后门等恶意程序。必要时可运行一次杀毒程序对系统盘进行一次扫描处理。

8. 检查安全策略是否更改

打开本地连接的属性，查看“常规”中是否只勾选了“TCP/IP协议”，打开“TCP/IP”协议设置，点“高级”==》“选项”，查看“IP安全机制”是否是设定的IP策略，查看“TCP/IP”筛选允许的端口有没有被更改。打开“管理工具”=》“本地安全策略”，查看目前使用的IP安全策略是否发生更改。

9. 检查目录权限

重点查看系统目录和重要的应用程序权限是否被更改。需要查看的目录有c:;c:winnt;
C:winntsystem32;c:winntsystem32inetsrv;c:winntsystem32inetsrvdata;c:documents and
Settings;然后再检查serv-u安装目录，查看这些目录的权限是否做过变动。检查system32下的一些重要文件是否更改过权限，包括：cmd，net，ftp，tftp，cacls等文件。

10. 检查启动项

主要检查当前的开机自启动程序。可以使用AReporter来检查开机自启动的程序。

发现入侵时的应对措施

对于即时发现的入侵事件，以下情况针对系统已遭受到破坏情况下的处理，系统未遭受到破坏或暂时无法察觉到破坏先按照上述的检查步骤检查一遍后再酌情考虑以下措施。系统遭受到破坏后应立即采取以下措施：

视情况严重决定处理的方式，是通过远程处理还是通过实地处理。如情况严重建议采用实地处理。如采用实地处理，在发现入侵的第一时间通知机房关闭服务器，待处理人员赶到机房时断开网线，再进入系统进行检查。如采用远程处理，如情况严重第一时间停止所有应用服务，更改IP策略为只允许远程管理端口进行连接然后重新启动服务器，重新启动之后再远程连接上去进行处理，重启前先用A Reporter检查开机自启动的程序。然后再进行安全检查。

以下处理措施针对用户站点被入侵但未危及系统的情况，如果用户要求加强自己站点的安全性，可按如下方式加固用户站点的安全：

站点根目录----只给administrator读取权限，权限继承下去。

wwwroot ------给web用户读取、写入权限。高级里面有删除子文件夹和文件权限

logfiles------给system写入权限。

database------给web用户读取、写入权限。高级里面没有删除子文件夹和文件权限

如需要进一步修改，可针对用户站点的特性对于普通文件存放目录如html、js、图片文件夹只给读取权限，对asp等脚本文件给予上表中的权限。另外查看该用户站点对应的安全日志，找出漏洞原因，协助用户修补程序漏洞。

1.2 数据备份和数据恢复

数据备份工作大致如下:

1. 每月备份一次系统数据。

2. 备份系统后的两周单独备份一次应用程序数据，主要包括IIS、serv-u、数据库等数据。

3. 确保备份数据的安全，并分类放置这些数据备份。因基本上采用的都是全备份方法，对于数据的保留周期可以只保留该次备份和上次备份数据两份即可。

数据恢复工作:

1. 系统崩溃或遇到其他不可恢复系统正常状态情况时，先对上次系统备份后发生的一些更改事件如应用程序、安全策略等的设置做好备份，恢复完系统后再恢复这些更改。

2. 应用程序等出错采用最近一次的备份数据恢复相关内容。

Web专用网站服务器的安全设置(3)

第三部分□服务器性能优化

3.1 服务器性能优化

系统性能优化

整理系统空间:

删除系统备份文件，删除驱动备份，删除不用的輸入法，删除系统的帮助文件，卸载不常用的组件。最小化C盘文件。

性能优化:删除多余的开机自动运行程序;减少预读取，减少进度条等待时间;让系统自动关闭停止响应的程序;禁用错误报告,但在发生严重错误时通知;关闭自动更新,改为手动更新计算机;

启用硬件和DirectX加速;禁用关机事件跟踪;禁用配置服务器向导;

减少开机磁盘扫描等待时间;将处理器计划和内存使用都调到应用程序上;调整虚拟内存;内存优化;修改cpu的二级缓存;修改磁盘缓存。

IIS性能优化

1、调整IIS高速缓存

HKEY_LOCAL_MACHINE\
System\CurrentControlSet\Services\InetInfoParametersMemoryCacheSize

MemoryCacheSize的范围是从0道4GB，缺省值为3072000(3MB)。一般来说此值最小应设为服务器内存的10%。IIS通过高速缓存系统句柄、目录列表以及其他常

用数据的值来提高系统的性能。这个参数指明了分配给高速缓存的内存大小。如果该值为0，那就意味着“不进行任何高速缓存”。在这种情况下系统的性能可能会降低。如果你的服务器网络通讯繁忙，并且有足够的内存空间，可以考虑增大该值。必须注意的是修改注册表后，需要重新启动才能使新值生效。

2. 不要关闭系统服务: “Protected Storage”

3. 对访问流量进行限制

A.对站点访问人数进行限制

B.站点带宽限制。保持HTTP连接。

C.进程限制, 输入CPU的耗用百分比

4. 提高IIS的处理效率

应用程序设置”处的“应用程序保护”下拉按钮，从弹出的下拉列表中，选中“低（IIS进程）”选项,IIS服务器处理程序的效率可以提高20%左右。但此设置会带来严重的安全问题，不值得推荐。

5. 将IIS服务器设置为独立的服务器

A.提高硬件配置来优化IIS性能

硬盘:硬盘空间被NT和IIS服务以如下两种方式使用:一种是简单地存储数据;另一种是作为虚拟内存使用。如果使用Ultra2的SCSI硬盘,可以显著提高IIS的性能。

B.可以把NT服务器的页交换文件分布到多个物理磁盘上,注意是多个“物理磁盘”,分布在多个分区上是无效的。另外,不要将页交换文件放在与WIndows NT引导区相同的分区中。

C.使用磁盘镜像或磁盘带区集可以提高磁盘的读取性能

D.最好把所有的数据都储存在一个单独的分区里。然后定期运行磁盘碎片整理程序以保证在存储Web服务器数据的分区中没有碎片。使用NTFS有助于减少碎片。推荐使用Norton的Speeddisk,可以很快的整理NTFS分区。

6. 起用HTTP压缩

HTTP压缩是在Web服务器和浏览器间传输压缩文本内容的方法。HTTP压缩采用通用的压缩算法如gzip等压缩HTML、JavaScript或CSS文件。可使用pipeboost进行设置。

7. 起用资源回收

使用IIS5Recycle定时回收进程资源。

3.2 服务器常见故障排除

1. ASP“请求的资源正在使用中”的解决办法:

该问题一般与杀毒软件有关，在服务器上安装个人版杀毒软件所致。出现这种错误可以通过卸载杀毒软件解决，也可尝试重新注册vbscript.dll和jscript.dll来解决，在命令行下运行：regsvr32 vbscript.dll 和regsvr32 jscript.dll即可。

2. ASP500错误解决办法：

首先确定该问题是否是单一站点存在还是所有站点存在，如果是单一站点存在该问题，则是网站程序的问题，可打开该站点的错误提示，把IE的“显示友好HTTP错误”信息取消，查看具体错误信息，然后对应修改相关程序。如是所有站点存在该问题，并且HTML页面没有出现该问题，相关日志出现“服务器无法加载应用程序‘/LM/W3SVC/1/ROOT‘。错误是‘不支持此接口‘”。那十有八九是服务器系统中的ASP相关组件出现了问题，重新启动IIS服务，尝试是否可以解决该问题，无法解决重新启动系统尝试是否可解决该问题，如无法解决可重新修复一下ASP组件：首先删除com组件中的关于IIS的三个东西，需要先将属性里的高级中“禁止删除”的勾选取消。

命令行中，输入“cd winnt\system32\inetsrv”字符串命令，单击回车键后，再执行“rundll32 wamreg.dll,createIISPackage”命令，接着再依次执行“regsvr32 asptxn.dll”命令、“iisreset”命令，最后重新启动一下计算机操作系统，这样IIS服务器就能重新正确响应ASP脚本页面了。

3. IIS出现105错误：

在系统日志中“服务器无法注册管理工具发现信息。管理工具可能无法看到此服务器” 来源：w3svc ID：105

解决办法：在网络连接中重新安装netbios协议即可，安装完成之后取消掉勾选。

4. MySQL服务无法启动【错误代码1067】的解决方法

启动MySQL服务时都会在中途报错！内容为：在 本地计算机

无法启动MySQL服务 错误1067：进程意外中止。

解决方法：查找Windows目录下的my.ini文件，编辑内容（如果没有该文件，则新建一个），至少包含basedir，datadir这两个基本的配置。

[mysqld]
# set basedir to installation path, e.g., c:/mysql
# 设置为MYSQL的安装目录
basedir=D:/www/WebServer/MySQL
# set datadir to location of data directory,
# e.g., c:/mysql/data or d:/mydata/data
# 设置为MYSQL的数据目录
datadir=D:/www/WebServer/MySQL/data

注意，我在更改系统的temp目录之后没有对更改后的目录给予system用户的权限也出现过该问题。

5. DllHotst进程消耗cpu 100%的问题

服务器正常CPU消耗应该在75%以下，而且CPU消耗应该是上下起伏的，出现这种问题的服务器，CPU会突然一直处100%的水平，而且不会下降。

查看任务管理器，可以发现是DLLHOST.EXE消耗了所有的CPU空闲时间，管理员在这种情况下，只好重新启动IIS服务，奇怪的是，重新启动IIS服务后一切正常，但可能过了一段时间后，问题又再次出现了。

直接原因：

有一个或多个ACCESS数据库在多次读写过程中损坏，

MDAC系统在写入这个损坏的ACCESS文件时，ASP线程处于BLOCK状态，结果其他线程只能等待，IIS被死锁了，全部的CPU时间都消耗在DLLHOST中。

解决办法：把数据库下载到本地，然后用ACCESS打开，进行修复操作。再上传到网站。如果还不行，只有新建一个ACCESS数据库，再从原来的数据库中导入所有表和记录。然后把新数据库上传到服务器上。

6. Windows installer出错：

在安装软件的时候出现“不能访问windows installer

服务。可能你在安全模式下运行 windows，或者windows installer

没有正确的安装。请和你的支持人员联系以获得帮助”

如果试图重新安装InstMsiW.exe，提示：“指定的服务已存在”。

解决办法：

关于installer的错误，可能还有其他错误提示，可尝试以下解决办法：

首先确认是否是权限方面的问题，提示信息会提供相关信息，如果是权限问题，给予winnt目录everyone权限即可[安装完把权限改回来即可]。如果提示的是上述信息，可以尝试以下解决方法：运行“msiexec /unregserver”卸载Windows Installer服务，如果无法卸载可使用SRVINSTW进行卸载，然后下载windows installer的安装程序[地址：http://www.newhua.com/cfan/200410/instmsiw.exe]，用winrar解压该文件，在解压缩出来的文件夹里面找到msi.inf文件，右键单击选择“安装”，重新启动系统后运行“msiexec /regserver”重新注册Windows Installer服务。

新闻评论

当前没有评论信息

用户名 密码 (匿名用户请直接使用Guest用户名) 观点：不知所云 不赞成 中立 赞成 堪为精品 Ctrl+回车 提交评论.

请自觉遵守互联网相关政策法规,评论字数2-200字.请不要发广告。您发表的问题不代表本站观点。一切后果由发表者负责

Web专用网站服务器的安全设置(4)

第四部分 服务器管理

4.1 服务器日常管理安排

服务器管理工作必须规范严谨，尤其在不是只有一位管理员的时候，日常管理工作包括：

1. 服务器的定时重启。每台服务器保证每周重新启动一次。重新启动之后要进行复查，确认服务器已经启动了，确认服务器上的各项服务均恢复正常。对于没有启动起来或服务未能及时恢复的情况要采取相应措施。前者可请求托管商的相关工作人员帮忙手工重新启动，必要时可要求让连接上显示器确认是否已启动起来；后者需要远程登陆上服务器进行原因查找并根据原因尝试恢复服务。

2. 服务器的安全、性能检查，每服务器至少保证每周登陆两次粗略检查两次。每次检查的结果要求进行登记在册。如需要使用一些工具进行检查，可直接在e:tools中查找到相关工具。对于临时需要从网络上找的工具，首先将IE的安全级别调整到高，然后在网络上进行查找，不要去任何不明站点下载，尽量选择如华军、天空等大型网站进行下载，下载后确保当前杀毒软件已升级到最新版本，升级完毕后对下载的软件进行一次杀毒，确认正常后方能使用。对于下载的新工具对以后维护需要使用的话，将该工具保存到e:tools下，并在该目录中的readme.txt文件中做好相应记录，记录该工具的名称，功能，使用方法。并且在该文件夹中的rar文件夹中保留一份该工具的winrar压缩文件备份，设置解压密码。

3. 服务器的数据备份工作，每服务器至少保证每月备份一次系统数据，系统备份采用ghost方式，对于ghost文件固定存放在e:ghost文件目录下，文件名以备份的日期命名，如0824.gho，每服务器至少保证每两周备份一次应用程序数据，每服务器至少保证每月备份一次用户数据，备份的数据固定存放在e:databak文件夹，针对各种数据再建立对应的子文件夹，如serv-u用户数据放在该文件夹下的servu文件夹下，iis站点数据存放在该文件夹下的iis文件夹下。

4. 服务器的监控工作，每天正常工作期间必须保证监视所有服务器状态，一旦发现服务停止要及时采取相应措施。对于发现服务停止，首先检查该服务器上同类型的服务是否中断，如所有同类型的服务都已中断及时登陆服务器查看相关原因并针对该原因尝试重新开启对应服务。

5. 服务器的相关日志操作，每服务器保证每月对相关日志进行一次清理，清理前对应的各项日志如应用程序日志、安全日志、系统日志等都应选择“保存日志”。所有的日志文件统一保存在e:logs下，应用程序日志保存在e:logsapp中，系统程序日志保存在e:logssys中，安全日志保存在e:logssec中。对于另外其他一些应用程序的日志，也按照这个方式进行处理，如ftp的日志保存在e:logsftp中。所有的备份日志文件都以备份的日期命名，如20050824.evt。对于不是单文件形式的日志，在对应的记录位置下建立一个以日期命名的文件夹，将这些文件存放在该文件夹中。

6. 服务器的补丁修补、应用程序更新工作，对于新出的漏洞补丁，应用程序方面的安全更新一定要在发现的第一时间给每服务器打上应用程序的补丁。

7. 服务器的隐患检查工作，主要包括安全隐患、性能等方面。每服务器必须保证每月重点的单独检查一次。每次的检查结果必须做好记录。

8. 不定时的相关工作，每服务器由于应用软件更改或其他某原因需要安装新的应用程序或卸载应用程序等操作必须知会所有管理员。

9. 定期的管理密码更改工作，每服务器保证至少每两个月更改一次密码，对于SQL服务器由于如果SQL采用混合验证更改系统管理员密码会影响数据库的使用则不予修改。

相关建议:对每服务器设立一个服务器管理记载，管理员每次登陆系统都应该在此中进行详细的记录，共需要记录以下几项:登入时间，退出时间，登入时服务器状态[包含不明进程记录，端口连接状态，系统帐号状态，内存/CPU状态]，详细操作情况记录[详细记录下管理员登陆系统后的每一步操作]。无论是远程登陆操作还是物理接触操作都要进行记录，然后将这些记录按照各服务器归档，按时间顺序整理好文档。

对于数据备份、服务器定时重启等操作建议将服务器分组，例如分成四组，每月的周六晚备份一组服务器的数据，每周的某一天定时去重启一组的服务器，这样对于工作的开展比较方便，这些属于固定性的工作。另外有些工作可以同步进行，如每月一次的数据备份、安全检查和管理员密码修改工作，先进行数据备份，然后进行安全检查，再修改密码。对于需要的即时操作如服务器补丁程序的安装、服务器不定时的故障维护等工作，这些属于即时性的工作，但是原则上即时性的工作不能影响固定工作的安排。

4.2 管理员日常注意事项

在服务器管理过程中，管理员需要注意以下事项：

1. 对自己的每一次操作应做好详细记录，具体见上述建议，以便于后来检查。

2. 努力提高自身水平，加强学习。

新闻评论

当前没有评论信息

用户名 密码 (匿名用户请直接使用Guest用户名) 观点：不知所云 不赞成 中立 赞成 堪为精品 Ctrl+回车 提交评论.

请自觉遵守互联网相关政策法规,评论字数2-200字.请不要发广告。您发表的问题不代表本站观点。一切后果由发表者负责

http://technet.microsoft.com/zh-cn/library/cc754373(WS.10).aspx

Windows Server 2008 中的服务器安全策略管理

更新时间: 2008年5月

应用到: Windows Server 2008

在 Windows Server 2008 中，您可以使用许多工具来确保计算机的安全。本文将着重介绍三种工具，您可以单独或配合使用这些工具来管理服务器上的安全策略：

- 安全配置向导 (SCW) 和 Scwcmd 命令行工具
-
- “安全模板”管理单元
-
- “安全配置和分析”管理单元
-

虽然这些工具不是全新的工具，但使用这些工具的方法是全新的。

备注

本概述未包含保护网络和计算机安全的其他技术和工具，例如网络访问保护 (NAP)、Active Directory 域服务 (AD DS) 和组策略。

服务器安全策略管理能够确保在各种服务器配置随着时间发生变化时其安全设置仍为最新的设置。可通过以下策略管理操作来保护服务器的安全：

- 分析服务器的安全设置，以确保应用到服务器的策略适用于服务器角色。
-
- 在修改服务器配置时更新服务器策略。

-
- 为不包含在服务器管理器中的新应用程序角色或服务器角色创建策略。
-
- 使用安全策略管理工具来应用针对您所在环境的服务器安全策略设置。
-

在 Windows Server 2008 中，所设计的服务器在默认情况下是安全的。也就是说，在您通过服务器管理器安装角色、角色服务和功能时，将会自动配置特定服务器配置的安全设置。但是，您无法使用服务器管理器自定义更改安全设置。却可以使用安全策略管理工具进行这些更改。例如，如果需要修改特定服务器角色的设置，可以使用 SCW 轻松地编辑所提供的防火墙规则，以设置更具限制性的控制或访问权限。您可能需要安装服务器管理器中未提供的角色或功能，也可能需要轻松地为许多计算机部署策略更改。这都可以使用这些工具来完成上述以及其他的安全策略管理任务。

将根据所在组织的规模、安全要求以及修改服务器配置的频率来确定要使用哪些工具来保护服务器的安全。

使用 SCW 保护服务器

Windows Server 2008 中的 SCW 功能与 Windows Server 2003 Service Pack 1 (SP1) 中包含的此向导版本非常相似。您仍可以使用 SCW 创建和应用服务器安全策略，但是在大多数情况下，不需要使用 SCW 就可以在安装时保护服务器的安全。

在最初的服务器角色安装后，可以使用 SCW

检查服务器配置是否随着时间的变化产生了漏洞，并按要求对策略设置进行更新来保护服务器的安全。您可以在以下情形下使用 SCW

创建并应用服务器的安全策略：

- 在 Windows Server 2008 计算机上修改默认组件的配置。
-
- 在更改未通过服务器管理器安装的组件配置时，需要使用 SCW 更新服务器的安全策略。
-
- 为未通过服务器管理器安装的服务器角色（例如 SQL Server 或 Exchange Server）创建并应用策略。
-
- SCW 包含许多无法使用服务器管理器安装的服务器角色和功能。
-
- 为非 Microsoft 应用程序定义新的角色，并为这些角色创建和应用策略。
-
- SCW 具有一个组织可用来创建新角色的公共架构。在添加或删除非 Microsoft 应用程序时运行 SCW。
-

在中小型组织中，可以使用 SCW

中的默认设置快捷地创建一个策略，以帮助基于其角色保护服务器的安全并确保安全设置为最新状态。还可以将使用“安全模板”管理单元创建的自定义安全模

板并入到 SCW 策略中。这样便允许包含除 SCW

设置之外的其他设置。然后使用该向导将 SCW

策略应用到本地计算机中，也可使用组策略将其应用到许多计算机中。

有关使用 SCW 的信息，请参阅安全配置向导。

使用安全模板创建自定义策略

在配置 Windows Server 2008
时，将自动应用符合大多数组织安全要求的策略。但是，在某些组织中可能需要

对您网络的某些权限和本地策略作出更多的限制。在这种情况下，可以使用“安

全模板”管理单元来创建自定义的安全策略。

备注

在 Windows Server 2008
中，没有预定义的安全模板。

您可以使用“安全模板”管理单元，为计算机或网络创建安全策略。可以使用安全

模板来定义以下安全领域的策略设置：

- 帐户策略：密码策略、帐户锁定策略、Kerberos 策略
-
- 本地策略：审核策略、用户权限分配和安全选项
-
- 事件日志：应用程序、系统和安全事件日志设置
-
- 受限组：安全敏感组的成员

-
- 系统服务：系统服务的启动和权限
-
- 注册表：注册表项的权限
-
- 文件系统：文件夹和文件的权限
-

使用模板格式创建自定义策略后，可以将其应用到不同的领域，其中包括：

- 将模板导入到基于角色的 SCW

  策略中，并将其应用到一台或多台计算机中。

-
- 将模板导入到组策略对象 (GPO)

  中，并通过组策略将其应用到多台计算机中。

-
- 使用“安全配置和分析”管理单元将模板应用到本地计算机中。
-

有关使用“安全模板”管理单元的信息，请参阅分析和配置安全性。

若要了解如何减少针对服务器计算机和客户端计算机的威胁，请参阅威胁和对策指南 (http://go.microsoft.com/fwlink/?LinkId=106667)（可能为英文网页）。

此指南将包含所有安全设置，这些设置将为 Windows

操作系统所遭受的特定威胁提供对策。

使用组策略对象应用安全策略

此服务器版本与 Windows Server 2003

一样，您可以通过将模板或策略导入到 GPO

中，将“安全模板”管理单元创建的安全模板或 SCW

创建的策略应用到多台计算机中。创建 GPO 后，可以使用组策略管理控制台

(GPMC) 将 GPO 链接到目标组织单位 (OU)。有关使用 GPMC

的信息，请参阅组策略管理控制台

(http://go.microsoft.com/fwlink/?LinkId=105933)(可能为英文网页)。

有关使用 Windows Server 2008 中的 GPO 来应用安全策略的信息，请参阅 Windows Server 2008 安全指南
(http://go.microsoft.com/fwlink/?LinkId=105788)(可能为英文网页)。

分析服务器安全

还可以使用服务器安全策略管理工具，分析本地或远程计算机中的安全设置。通过常规分析可确保每台计算机都具有其相应的安全级别，以作为企业风险管理计划的一部分。您可以修改安全级别，尤为重要的是，可以检测系统随着时间的变化所出现的任何安全缺陷。

可以使用“安全配置和分析”管理单元或 SCW 来分析安全策略设置。

安全配置和分析
Windows Server 2008
未对如何使用“安全配置和分析”管理单元进行任何更改。您仍然可以使用此管理单元分析和配置本地计算机的安全。您可以使用此管理单元将本地计算机策略

与分析数据库进行比较，以确定数据库中的所需设置是否与本地策略之间存在任何差异。还可以使用现有的数据库，或导入使用“安全模板”管理单元创建的一个或多个模板，以使用更新的设置创建新数据库。此分析提供了针对当前系统设置的一些建议，并使用可视标志或备注来突出显示当前设置与建议的安全级别不一致的任何部分。您可以解决分析暴露出来的任何差异，并使用导入的模板直接配置本地系统的安全。

有关使用“安全和配置分析”管理单元的信息，请参阅分析并配置安全性。

若要分析多台远程计算机，可以使用 SCW。

安全配置向导

可以使用 Scwcmd 命令行工具，分析本地计算机或多台远程计算机的安全策略设置。可以将服务器的当前安全设置与服务器配置的最新设置进行比较。使用 **scwcmd analyze** 以确定计算机是否符合使用该向导创建的指定策略。若要分析多台计算机，请指定要在分析中使用的策略文件以及要分析的计算机列表。然后，使用 **scwcmd view** 命令查看分析结果。

安全策略循序渐近指南:创建和部署基于角色的策略

更新时间: 2008年5月

应用到: Windows Server 2008

在 Windows Server® 2008 操作系统中，可以使用安全配置向导 (SCW) 通过修改角色、角色服务和功能的安全设置来减少服务器的受攻击面。使用 SCW 可帮助在使用服务器管理器初始安装角色之后维护安全的服务器配置。

关于本指南

本指南提供在测试环境中使用 SCW 创建安全策略并将其应用于原型服务器的循序渐进步骤。

方案概述

影响多台计算机的设置、配置或行为的任何技术的安全使用要求在部署之前进行规划。SCW 的安全使用包括在生产环境中应用策略之前测试工具和策略。

使用代表您的生产环境中服务器配置的原型服务器执行本指南中的步骤(在测试方案中)。验证了创建的 SCW 策略并在为您的原型服务器提供所需的安全性的此测试方案中应用之后，可以将在测试环境中创建的策略应用于生产环境中的服务器。

当您继续此方案时，将执行以下任务:

- 使用 SCW 根据服务器的角色为服务器创建一个包含所有所需安全设置的安全策略。
-

- 使用 SCW 和 Scwcmd 命令行工具将此安全策略应用于目标计算机。
- 使用 Scwcmd 命令行工具查看和分析此安全策略。
- 使用 Scwcmd 命令行工具将安全策略保存为组策略对象 (GPO) 格式。

建立策略原型

在 SCW 上下文中，“建立策略原型”意味着在原型计算机上为具有相同角色的一组服务器创建一个安全策略。原型计算机为模型服务器，其配置代表组中的每台计算机。

组件

可以使用三个主要的组件来创建和应用安全策略：

- SCW
- Scwcmd 命令行工具
- 安全配置数据库

SCW

SCW 将指导您完成根据使用服务器管理器配置的服务器角色创建、编辑、应用或回滚安全策略的过程。使用 SCW 创建的安全策略是 XML 文件，应用该文件后，可以配置服务、网络安全、特定注册表值和审核策略。

在此方案中，您将使用 SCW 来创建策略并将其应用于原型服务器。

Scwcmd 命令行工具

SCW 包含 Scwcmd.exe 命令行工具。可以使用 Scwcmd 来执行以下任务:

- 使用 SCW 生成的策略配置一台或多台服务器。
-
- 针对 SCW 生成的策略分析一台或多台服务器。
-
- 查看采用 HTML 格式的分析结果。
-
- 回滚 SCW 策略。
-
- 将 SCW 生成的策略转换为组策略支持的文件。
-
- 使用 SCW 注册安全配置数据库扩展。
-

可以使用 Scwcmd 在运行 Windows Server 2008 的远程服务器上配置、分析或回滚策略。

在此方案中，将使用 Scwcmd 执行以下操作:

- 将安全策略应用于一台或多台远程服务器。
-
- 分析并查看服务器的安全策略。
-
- 采用 GPO 格式保存策略。
-

安全配置数据库

安全配置数据库由一组 XML 文档组成，这些文档列出 SCW

支持的每个服务器角色所需的服务和端口。这些文件安装在

%Systemroot%\Security\Msscw\Kbs

中。选择了服务器之后，将扫描该服务器，以确定下列事项：

- 服务器上已安装的角色
-
- 服务器可能正在执行的角色
-
- 已安装但是未在安全配置数据库中的服务
-
- 为服务器配置的 IP 地址和子网
-

SCW 将此服务器特定的信息合并到一个名为 Main.xml 的 XML

文件中。如果单击“处**理安全配置数据库**”页上的“查**看安全配置数据库**”，SCW

将显示 Main.xml。

可以通过为非 Microsoft

应用程序创建自定义角色定义扩展安全配置数据库。SCW 在

%Systemroot%\Security\Msscw\Kbs

目录中包含许多扩展，可用来构建新的扩展（角色定义）。

技术回顾

此部分简要介绍与使用 SCW 创建和应用安全策略有关的其他技术。当使用 SCW 创建安全策略时，您拥有用于应用该策略的不同选项。此部分回顾了这些选项以及它们如何影响应用于安全设置的优先规则。

在 Active Directory 环境中应用策略

对于远程管理，您可以使用 Active Directory® 域服务 (AD DS) 组织单位 (OU) 通过 GPO 将 SCW 策略轻松应用于服务器。使用 SCW 为服务器创建原型策略之后，通过使用 Scwcmd 命令行工具将其转换为 GPO，然后您只需将此 GPO 链接到一个或多个 OU。

组策略管理控制台

组策略管理控制台 (GPMC) 已集成到 Windows Server 2008 操作系统中。您可以使用 GPMC 将 GPO 链接到 OU。链接是将 GPO 应用于 OU 中的用户和计算机的机制。

有关使用 GPMC 跨企业管理组策略的信息，请参阅“组策略管理控制台”(http://go.microsoft.com/fwlink/?LinkId=105933)(可能为英文网页)。

安全模板

除了使用 SCW 创建安全策略之外，还可以使用 SCW 通过安全模板应用安全设置。安全模板是一些 .inf 文件，其默认位置为 *%Systemroot%*\security\templates。您可以在 GPMC 中的以下位置查看安全模板设置：*GPO_Name*\计算机配置\Windows 设置\安全设置。

某些安全设置可以使用 SCW

或“安全模板”管理单元进行更改，某些安全设置只能使用 SCW

进行更改，而其他安全设置只能使用“安全模板”管理单元进行更改。例如，SCW

包含任何安全模板中不包含的防火墙设置。相反，安全模板可以包含不能使用 SCW
进行配置的软件限制策略之类的项目。某些配置更改（如审核策略）可以通过使

用 SCW、创建或编辑 SCW

策略时附加安全模板进行设置，也可以同时使用这两种方法进行设置。但是，如

果您同时使用这两种方法，则使用优先规则来解决冲突的策略设置。

有关使用“安全模板”的详细信息，请参阅“如何使用安全模板”(http://go.microsoft.com/fwlink/?LinkId=106530)（可能为英文网页）。

优先规则

在使用组策略、SCW 以及多个安全模板的 Active Directory

环境中，使用以下规则预期安全设置的优先级：

- 与使用策略文件（.xml 文件）通过 SCW 或 Scwcmd

  命令行工具远程应用的安全策略相比，通过 GPO

  应用的安全策略具有较高的优先级。

-

- 创建每个 GPO 的方式（是否使用 Scwcmd）不会影响 GPO

  之间的优先级。仅标准的 Active Directory

继承规则(其中连续应用本地、站点、域和 OU GPO)和链接顺序确定 GPO 的优先级。

-

- 与在附加到 .xml 策略文件的 .inf 安全模板中设置的冲突策略相比，在 SCW 中设置的安全策略具有较高的优先级。

-

- 如果将多个安全模板附加到 .xml 文件，则在 SCW 的**“包括安全模板”**对话框中在列表较高位置列出的模板优先于出现在较低位置的模板。

-

服务器管理器

对于 Windows Server 2008，默认情况下使用建议的安全设置配置服务器角色，并且只要安装该角色就应用这些设置。配置角色时，服务器管理器自动安装所有所需的服务和功能，并且自动配置支持新角色所需的任何防火墙规则。同样，当使用服务器管理器删除任何特定角色时，会修改服务器的服务和防火墙配置，以帮助确保服务器的配置仍然安全并且其他服务器角色的操作不会受到影响。但是，无法使用服务器管理器自定义安全设置。

服务器管理器和 SCW 是两个互补的工具。服务器管理器的重点是便于部署服务器，而 SCW 是用于长期维护安全设置的工具。SCW

能够更详细的控制服务器的受攻击面，并且可以帮助您根据组织的安全需要保护服务器的安全，防止攻击。

高级安全 Windows 防火墙

在 Windows Server 2008 中，SCW 与“高级安全 Windows 防火墙”集成在一起。SCW 将“高级安全 Windows 防火墙”配置为允许到操作系统要求的重要端口以及侦听应用程序的入站网络流量。如果需要其他防火墙规则（或防火墙例外），可以使用向导来创建它们。这种功能简化了网络强化的管理。也可以使用 SCW 简化使用远程过程调用 (RPC) 和动态端口的服务的网络筛选器配置。

重要事项

如果在 SCW 的“网络安全”部分配置了设置，将删除不需要的防火墙规则。

有关“高级安全 Windows 防火墙”的详细信息，请参阅“Windows 防火墙”(http://go.microsoft.com/fwlink/?LinkID=98308)（可能为英文网页）。

创建和应用安全策略的最佳操作

SCW 通过创建专为特定角色设计的安全策略，帮助减少服务器的受攻击面。管理员可以通过在创建安全策略之前确定执行相同或相似任务的服务器组来简化策略创建和分发。为了帮助您实现这些目标，请在开始此方案之前查看以下最佳操作。

- **在服务级别配置目标服务器之后，建立原型服务器的模型。**通过其创建安全策略的原型服务器应该与目标服务器具有相同的服务级别。安全策略禁用服务器上包含在“安全配置数据库”中，但创建策略时不在原型服务器上的任何服务。例如，如果 DCOM Server Process Launcher 服务在“安全配置数据库”中列出，但不在原型服务器上，则通过原型服务器创建的安全策略会将 DCOM Server Process Launcher 状态设置为禁用。将安全策略应用于其他服务器时，DCOM Server Process Launcher 服务将在其他服务器上被禁用。
-
- **将执行相同功能的服务器分组在一个 OU 中。**为了简化策略分发，将执行相同功能且具有相同配置的服务器分组在一个 OU 中。可以将目标是 OU 中所有服务器的新的或修改的安全策略以 GPO 格式保存，这样将便于使用组策略进行分发。
-
- 为一组服务器创建一个策略。SCW 根据服务器执行的角色和功能配置安全策略。可以用相同的安全策略配置执行相同或非常相似的功能的其他服务器。可以使用 SCW 一次创建一个安全策略，保存该策略并将其应用于执行相同角色或角色集的所有服务器。一个包含特定类型服务器所需的所有安全设置的安全策略也可以简化配置、回滚和分析。
-

- 为不同的软件版本创建不同的策略。对于特定于 64

位版本软件的服务或端口，在 64

位计算机上创建策略。然后将这些策略仅应用于其他 64 位计算机（非 32

位计算机）以确保正确标识和配置服务。

-

- **部署之前脱机测试新的安全策略。**在新的安全策略中配置的设置可能会

造成应用程序或服务的兼容性问题。因此，在将新的安全策略应用于生产服

务器之前，应仔细测试这些策略。

-

此方案的要求

SCW 的所有组件都自动随 Windows Server 2008

一起安装，您可以在“服务器管理器”或“管理工具”中访问

SCW。将应用原型安全策略的服务器还必须运行 Windows Server 2008。

备注

SCW 不能用于客户端操作系统或 Windows
小型企业服务器。

使用 SCW 时应注意下列事项：

- SCW 禁用不需要的服务并提供对“高级安全 Windows 防火墙”的支持。

-

- 使用 SCW 创建的安全策略与安全模板不同，后者是扩展名为 .inf

的文件。安全模板包含的安全设置要多于可以使用 SCW

设置的安全设置。但是，可以在 SCW 安全策略文件中包含安全模板。

-
- 可以使用组策略来部署使用 SCW 创建的安全策略。
-
- SCW

不会安装或卸载服务器执行角色时所需的组件。可以通过服务器管理器安装

角色特定的组件。

-

SCW 根据您在“选择服务器角色”页上选择的角色来启用服务器所需的服务。

重要事项

将禁用不需要的服务，如果在 SCW
的“网络安全”部分配置了设置，将删除不需要的防火墙规则。

若要开始此方案，您需要：

- 一个安装了 Windows Server 2008

用于创建安全策略的原型服务器以及应用策略的一个或多个基于 Windows

Server 2008 的附加服务器。

-

配置将应用安全策略的服务器的方法与配置原型服务器的方法相同。

重要事项

目标计算机的配置必须与原型服务器的配置相匹配。在基于 Windows Server 2008 的计算机上创建的 SCW 策略与在基于 Windows Server 2003
的计算机上创建的 SCW
策略不兼容。如果操作系统或角色不同，可能会错误配置设置，也可能会禁用必需的角色或服务，或者出现其他问题。

- 一个 Active Directory 服务器 OU 结构，其中一个 OU

中的服务器具有相同配置，包括代表您的生产环境的操作系统、角色和功能以及应用程序。

-

创建和应用基于角色的安全策略的步骤

可以使用以下步骤根据您在生产环境中拥有的不同服务器类型创建一个或多个原型策略。

在此方案中，将根据代表生产环境中服务器的原型服务器的现有配置创建安全策略。

步骤 1：创建原型安全策略

该过程指导您完成一个简单策略的创建过程，其中不会对默认选择进行更改。

根据原型服务器创建和应用安全策略的步骤

单击**「开始」**，指向**“管理工具”**，然后单击**“安全配置向导”**。

阅读**“欢迎使用”**页，然后单击**“下一步”**。

在**“配置操作”**页上，单击**“新建安全策略”**，然后单击**“下一步”**。

在**“选择服务器”**页上，键入原型服务器的名称，然后单击**“下一步”**。

备注

默认情况下，选择本地计算机。

在“正在处理安全配置数据库”页上，完成处理后单击“下一步”。

此时，根据服务器角色配置“安全配置数据库”。

在“基于角色的服务配置”页上，单击“下一步”。

在“选择服务器角色”页上，确保向导检测到并选择原型服务器上安装的所有服务器角色，然后单击“下一步”。

在“选择客户端功能”页上，确保向导检测到并选择原型服务器上安装的所有功能，然后单击“下一步”。

在“选择管理和其他选项”页上，确保向导检测到并选择原型服务器上安装的所有选项，然后单击“下一步”。

在“选择其他服务”页上，确保向导检测到并选择原型服务器上所需的所有服务，然后单击“下一步”。

备注

如果您将原型服务器配置为具有所有所需的角色并且安装了任何其他所需的软件（如备份代理或防病毒软件），则应该不需要修改任何以前的“基于角色的服务配置”页。

在“处理未指定的服务”页上，单击“下一步”。

备注

未指定的服务是未出现在“安全配置数据库”中的服务，这些服务当前未安装在所选服务器上，但是可能已安装在要应用安全策略的其他服务器上。这些服务也可

能在以后安装在所选服务器上。任何未知的服务将出现在**“未指定的服务”**页的 SCW 中。

在**“确认服务更改”**页上，查看 SCW

将包含在所得到的安全策略中的服务模式更改，然后单击**“下一步”**。

在**“网络安全”**页上，单击**“下一步”**。

在**“网络安全规则”**页上，确保 SCW 检测到它将用来配置“高级安全 Windows 防火墙”的适当端口和应用程序，然后单击**“下一步”**。

在**“注册表设置”**页上，选中**“跳过这一部分”**复选框，然后单击**“下一步”**。

在**“审核策略”**页上，选中**“跳过这一部分”**复选框，然后单击**“下一步”**。

备注

注册表设置和审核策略是可选的选项，在此方案中将不对其进行配置。

在**“保存安全策略”**页上，单击**“下一步”**。

在**“安全策略文件名”**页上，键入原型策略的名称，然后单击**“下一步”**。

注意

不要使用原型计算机的名称，因为 Scwcmd 使用 *computername.xml* 来保存分析结果，您创建的策略也不应使用相同的名称。

备注

默认情况下，基于 XML 的策略文件保存在服务器的安装文件夹(通常位于 C:\Windows)下的 Security\msscw\policies 文件夹中。但是，SCW 允许您指定任何位置。

在“应用安全策略”页上，单击“稍后应用”，然后单击“下一步”。

在“正在完成安全配置向导”页上，单击“完成”。

此时，您便创建并保存了该策略，但该策略尚未应用于计算机。

步骤 2：将安全策略应用到服务器

对于此步骤，将首先使用向导将策略应用于本地计算机。在此步骤的第二部分中，使用 Scwcmd 将策略应用于一台或多台远程计算机。

使用向导将安全策略应用于服务器的步骤

单击「开始」，指向“管理工具”，然后单击“安全配置向导”。

在“欢迎使用”页上，单击“下一步”。

在“配置操作”页上，单击“应用现有安全策略”，然后单击“下一步”。

如果已经创建了多个策略，则单击“浏览”，然后双击策略的名称。

在“选择服务器”页上，键入要应用策略的服务器的名称，然后单击“下一步”。

在“应用安全策略”页上，单击“下一步”。

可以单击“查看安全策略”首先验证所有策略设置。

在**“应用安全策略”**页上，等待处理完成，然后单击**“下一步”**。

在**“正在完成安全配置向导”**页上，单击**“完成”**。

使用 Scwcmd 命令行工具将安全策略应用于多台计算机的步骤

在命令提示符下，键入：

scwcmd configure i: *MachineList.xml*

MachineList.xml 包含计算机和要应用的相应策略列表。在 %*windir*%\Security\SampleMachineList.xml 中有一个示例文件。

您可以在命令提示符下键入 **scwcmd configure** 了解这些参数。

步骤 3：分析和查看服务器的安全策略

可以使用 Scwcmd 命令行工具查看应用于服务器的 SCW 安全策略的设置。为此，需要首先分析服务器设置。

使用 Scwcmd 命令行工具分析并查看安全策略的步骤

在命令提示符下，键入：

scwcmd analyze /m: *Machine* **/p:** *Policy.xml* **/o:** *Resultdir*

使用要分析的计算机名称替换 *Machine*，使用用于执行分析的安全策略的文件名替换 *Policy.xml*，使用分析结果文件的所在位置替换 *Resultdir*。

完成分析后，键入：

scwcmd view /x: *xmlfile.xml* **/s:scwanalysis.xsl**

使用在上一步中创建的分析结果文件替换 *xmlfile.xml*。Scwanalysis.xsl 是一个随 SCW
一起安装的文件，该文件将格式化分析结果以便进行显示。这两个文件必须位于同一目录中。

步骤 4：以 GPO 格式保存安全策略

当希望使用组策略将 SCW 安全策略应用于 Active Directory 环境中的多台服务器时，可使用此步骤。此步骤采用 GPO 格式保存策略。

> **备注**
>
> 无法回滚通过组策略应用的 SCW 安全策略。

采用 GPO 格式保存 SCW 安全策略的步骤

在命令提示符下，键入：

scwcmd transform /p: *Policy.xml* **/g:** *GPOName*

Policy.xml 是您早期使用 SCW 创建的策略。*GPOName* 是您在本地组策略编辑器中或 GPMC 中查看时，GPO 将显示的名称。

完成 **scwcmd transform** 命令后，便已经在 AD DS 中创建了 GPO，但不会应用它包含的策略，直到将 GPO 链接到某个站点、域或 OU。有关链接 GPO 的说明，请参阅“组策略管理控制台”(http://go.microsoft.com/fwlink/?LinkId=105933)(可能为英文网页)。

其他参考

- Windows Server 2008 安全指南 (http://go.microsoft.com/fwlink/?LinkID=105788)(可能为英文网页)
-
- “安全配置向导中的新增功能”(http://go.microsoft.com/fwlink/?LinkId=108137)(可能为英文网页)
-
- “扩展安全配置向导”(http://go.microsoft.com/fwlink/?LinkID=43450) (Windows Server 2003)(可能为英文网页)
-

windows server 2008 WEB服务器安全初级设置篇

以下配置仅供参考，如有问题，欢迎大家指正。将服务器上所有的磁盘格式化为NTFS。在CMD 下敲命令：convert c:/fs:ntfs 将C 盘转为NTFS 格式。其他盘类推。

1：所有盘根目录只给system 和administrators 的权限，其余全部删除

2：设置win2k8 的屏幕保护，并选择在“恢复时显示登陆屏幕”

3：关闭光盘和磁盘的自动播放功能，在“控制面板”中双击“自动播放”，在弹出框中取消“为所有媒体和设备使用自动播放”的选择，点保存。

4：删除系统默认共享，不明白徽软为什么还要在win2008 中默认开启它们？可以使用 net share 命令查看。这些默认共享全部删除。

```
net share c$ /del
net share d$ /del
net share e$ /del
net share f$ /del
net share ipc$ /del
net share admin$ /del
```

也可以在“服务”中直接禁用“server”服务。

5：重命名帐户Administrator 和Guest。禁用Guest 账号，并加一个超级复杂的密码，密码可以是复制一段文本进去。禁用SQLDebugger 帐号。

重命名管理员用户组Administrators

6：创建一个陷阱用户即创建一个名为“Administrator”的本地用户，把它的权限降最低，并且加上一个超过16 位的超级复杂密码。这样，可以让哪些HACKER 忙一段时间了。

7：本地安全策略设置开始菜单—>管理工具—>本地安全策略

一、本地策略——>审核策略

审核策略更改 成功 失败

审核登录事件 成功 失败

审核对象访问 失败

审核过程跟踪 无审核

审核目录服务访问 失败

审核特权使用 失败

审核系统事件 成功 失败

审核账户登录事件 成功 失败

审核账户管理 成功 失败

二、本地策略——>用户权限分配关闭系统：只有Administrators 组、其它的全部删除。通过终端服务允许登陆：只加入Administrators,Remote Desktop Users 组，

其他全部删除在组策略中，计算机配置 > 管理模板 > 系统显示“关闭事件跟踪程序”更改为已禁用

三、本地策略——>安全选项交互式登陆：不显示最后的用户名 启用

网络访问:不允许SAM 帐户和共享的匿名枚举 启用
网络访问: 不允许存储网络身份验证的凭据或 .NET Passports 启用
网络访问:可匿名访问的共享 全部删除
网络访问:可匿名访问的命名管道 全部删除
网络访问:可远程访问的注册表路径 全部删除
网络访问:可远程访问的注册表路径和子路径 全部删除
9:禁止dump file 的产生系统属性>高级>启动和故障恢复把写入调试信息改成“无”。

10:禁用不必要的服务。控制面板———管理工具———服务:把下面的服务全部停止并禁用。

TCP/IP NetBIOS Helper
Server
Distributed Link
Tracking Client
Microsoft Search
Print Spooler
Remote Registry
Workstation

11:只开启需要用的端口,关闭不必要的,以减少攻击面。

80:IIS7
21:FTP
3389:远程
3306:Mysql
1433:Mssql

以上是我常用的端口,用不到的端口一律不要开启。

12:下列系统程序都只给管理员权限,别的全部删除。

arp.exe
attrib.exe
cmd.exe
format.com
ftp.exe
tftp.exe
net.exe
net1.exe
netstat.exe
ping.exe
regedit.exe
regsvr32.exe
telnet.exe
xcopy.exe
at.exe

所有的*.cpl 和*.msc 文件也只给管理员权限。

13:打开Windows 高级防火墙。设置一些规则,具体的规则我们在以后专门的防火墙设置里讲一下。

14:站点属性设置:删除 C:\ inetpub

目录更改站点路径，最好和系统盘分开。在安装IIS7
时，目录浏览功能不用安装，因为此功能容易爆路径。

安装角色时，以最小化角色运行服务器，即只安装你要用到的角色功能，如果你的服务器没有ASP 的站点，那ASP 角色就不需要安装，这样可以减少受攻击的面。

一般给站点目录权限为：

System 完全控制
Administrator 完全控制
Users 读
IIS_Iusrs 读、写

在 IIS7 中删除不常用的映射

15：安装一款杀毒软件，推荐Mcafee，再配合Windows
防火墙，它们俩应该是一个不错的组合。应该是 windows 2008
里面的黄金搭挡了。

16：经常关注徽软补丁更新情况，一些高危补丁要及时更新。通过以上配置，服务器安全性比原来默认又提升了一级。好了，这节就写到这里了。

阿江的WINDOWS服务器安全设置

阿江的WINDOWS服务器安全设置

[返回首页] [返回作品首页] [返回探针首页]

(如需引用或者转载此文，请注明：作者: 阿江 出处:www.ajiang.net)

前言

其实，在服务器的安全设置方面，我虽然有一些经验，但是还谈不上有研究，所以我写这篇文章的时候心里很不踏实，总害怕说错了会误了别人的事。

本文更侧重于防止ASP漏洞攻击，所以服务器防黑等方面的讲解可能略嫌少了点。

基本的服务器安全设置

安装补丁

安装好操作系统之后，最好能在托管之前就完成补丁的安装，配置好网络后，如果是2000则确定安装上了SP4，如果是2003，则最好安装上SP1，然后点击开始→Windows Update，安装所有的关键更新。

安装杀毒软件

虽然杀毒软件有时候不能解决问题，但是杀毒软件避免了很多问题。我一直在用诺顿2004，据说2005可以杀木马，不过我没试过。还有人用瑞星，瑞星是确定可以杀木马的。更多的人说卡巴司机好，不过我没用过。

不要指望杀毒软件杀掉所有的木马，因为ASP木马的特征是可以通过一定手段来避开杀毒软件的查杀。

设置端口保护和防火墙、删除默认共享

都是服务器防黑的措施，即使你的服务器上没有IIS，这些安全措施都最好做上。这是阿江的盲区，大概知道屏蔽端口用本地安全策略，不过这方面的东西网上攻略很多，大家可以撅出来看看，晚些时候我或者会复制一些到我的网站上。

权限设置

阿江感觉这是防止ASP漏洞攻击的关键所在，优秀的权限设置可以将危害减少在一个IIS站点甚至一个虚拟目录里。我这里讲一下原理和设置思路，聪明的朋友应该看完这个就能解决问题了。

权限设置的原理

WINDOWS用户，在WINNT系统中大多数时候把权限按用户(組)来划分。在【开始→程序→管理工具→计算机管理→本地用户和组】管理系统用户和用户组。

NTFS权限设置，请记住分区的时候把所有的硬盘都分为NTFS分区，然后我们可以确定每个分区对每个用户开放的权限。【文件(夹)上右键→属性→安全】在这里管理NTFS文件(夹)权限。

IIS匿名用户，每个IIS站点或者虚拟目录，都可以设置一个匿名访问用户(现在暂且把它叫“IIS匿名用户”)，当用户访问你的网站的.ASP文件的时候，这个.ASP文件所具有的权限，就是这个“IIS匿名用户”所具有的权限。

权限设置的思路

要为每个独立的要保护的个体(比如一个网站或者一个虚拟目录)创建一个系统用户，让这个站点在系统中具有惟一的可以设置权限的身份。

在IIS的【站点属性或者虚拟目录属性→目录安全性→匿名访问和验证控制→编辑→匿名访问→编辑】填写刚刚创建的那个用户名。

设置所有的分区禁止这个用户访问，而刚才这个站点的主目录对应的那个文件夹设置允许这个用户访问(要去掉继承父权限，并且要加上超管组和SYSTEM组)。

这样设置了之后，这个站点里的ASP程序就只有当前这个文件夹的权限了，从探针上看，所有的硬盘都是红叉叉。

我的设置方法

我是先创建一个用户组，以后所有的站点的用户都建在这个組里，然后设置这个组在各个分区没有权限或者完全拒绝。然后再设置各个IIS用户在各在的文件夹里的权限。

因为比较多，所以我很不想写，其实知道了上面的原理，大多数人都应该懂了，除非不知道怎么添加系统用户和組，不知道怎么设置文件夹权限，不知道IIS站点属性在那里。真的有那样的人，你也不要着急，要沉住气慢慢来，具体的方法其实自己也能摸索出来的，我就是这样。当然，如果我有空，我会写我的具体设置方法，很傲能还会配上图片。

改名或卸载不安全组件

不安全组件不惊人

我的在阿江探针1.9里加入了不安全组件检测功能(其实这是参考7i24的代码写的，只是把界面改的友好了一点，检测方法和他是基本一样的)，这个功能让很多站长吃惊不小，因为他发现他的服务器支持很多不安全组件。

其实，只要做好了上面的权限设置，那么FSO、XML、strem都不再是不安全组件了，因为他们都没有跨出自己的文件夹或者站点的权限。那个欢乐时光更不用怕，有杀毒软件在还怕什么时光啊。

最危险的组件是WSH和Shell，因为它可以运行你硬盘里的EXE等程序，比如它可以运行提升程序来提升SERV-U权限甚至用SERVU来运行更高权限的系统程序。

谨慎决定是否卸载一个组件

组件是为了应用而出现的，而不是为了不安全而出现的，所有的组件都有它的用处，所以在卸载一个组件之前，你必须确认这个组件是你的网站程序不需要的，或者即使去掉也不关大体的。否则，你只能留着这个组件并在你的ASP程序本身上下工夫，防止别人进来，而不是防止别人进来后SHELL。

比如，FSO和XML是非常常用的组件之一，很多程序会用到他们。WSH组件会被一部分主机管理程序用到，也有的打包程序也会用到。

卸载最不安全的组件

最简单的办法是直接卸载后删除相应的程序文件。将下面的代码保存为一个.BAT文件，（以下均以 WIN2000 为例，如果使用2003，则系统文件夹应该是 C:\WINDOWS\ ）

```
regsvr32/u C:\WINNT\System32\wshom.ocx
del C:\WINNT\System32\wshom.ocx
regsvr32/u C:\WINNT\system32\shell32.dll
del C:\WINNT\system32\shell32.dll
```

然后运行一下，WScript.Shell, Shell.application, WScript.Network就会被卸载了。可能会提示无法删除文件，不用管它，重启一下服务器，你会发现这三个都提示“×安全”了。

改名不安全组件

需要注意的是组件的名称和Clsid都要改，并且要改彻底了。下面以Shell.application为例来介绍方法。

打开注册表编辑器【开始→运行→regedit回车】，然后【编辑→查找→填写Shell.application→查找下一个】，用这个方法能找到两个注册表项：“{13709620-C279-11CE-A49E-

444553540000}”和“Shell.application”。为了确保万无一失，把这两个注册表项导出来，保存为 .reg 文件。

比如我们想做这样的更改

13709620-C279-11CE-A49E-444553540000 改名为 13709620-C279-11CE-A49E-444553540001

Shell.application 改名为 Shell.application_ajiang

那么，就把刚才导出的.reg文件里的内容按上面的对应关系替换掉，然后把修改好的.reg文件导入到注册表中（双击即可），导入了改名后的注册表项之后，别忘记了删除原有的那两个项目。这里需要注意一点，Clsid中只能是十个数字和ABCDEF六个字母。

下面是我修改后的代码（两个文件我合到一起了）：

```
Windows Registry Editor Version 5.00
[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-444553540001}]
@="Shell Automation Service"
[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-
444553540001}\InProcServer32]
@="C:\\WINNT\\system32\\shell32.dll"
"ThreadingModel"="Apartment"
[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-
444553540001}\ProgID]
@="Shell.Application_ajiang.1"
[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-
444553540001}\TypeLib]
@="{50a7e9b0-70ef-11d1-b75a-00a0c90564fe}"
[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-
444553540001}\Version]
@="1.1"
[HKEY_CLASSES_ROOT\CLSID\{13709620-C279-11CE-A49E-
444553540001}\VersionIndependentProgID]
@="Shell.Application_ajiang"
[HKEY_CLASSES_ROOT\Shell.Application_ajiang]
@="Shell Automation Service"
[HKEY_CLASSES_ROOT\Shell.Application_ajiang\CLSID]
@="{13709620-C279-11CE-A49E-444553540001}"
[HKEY_CLASSES_ROOT\Shell.Application_ajiang\CurVer]
```

@="Shell.Application_ajiang.1"

你可以把这个保存为一个.reg文件运行试一下，但是可别就此了事，因为万一黑客也看了我的这篇文章，他会试验我改出来的这个名字的。

防止列出用户组和系统进程

我在阿江ASP探针1.9中结合7i24的方法利用getobject("WINNT")获得了系统用户和系统进程的列表，这个列表可能会被黑客利用，我们应当隐藏起来，方法是：【开始→程序→管理工具→服务】，找到Workstation，停止它，禁用它。

防止Serv-U权限提升

其实，注销了Shell组件之后，侵入者运行提升工具的可能性就很小了，但是prel等别的脚本语言也有shell能力，为防万一，还是设置一下为好。

用Ultraedit打开ServUDaemon.exe查找Ascii：LocalAdministrator，和#l@$ak#.lk;0@P，修改成等长度的其它字符就可以了，ServUAdmin.exe也一样处理。

另外注意设置Serv-U所在的文件夹的权限，不要让IIS匿名用户有读取的权限，否则人家下走你修改过的文件，照样可以分析出你的管理员名和密码。

利用ASP漏洞攻击的常见方法及防范

一般情况下，黑客总是瞄准论坛等程序，因为这些程序都有上传功能，他们很容易的就可以上传ASP木马，即使设置了权限，木马也可以控制当前站点的所有文件了。另外，有了木马就然后用木马上传提升工具来获得更高的权限，我们关闭shell组件的目的很大程度上就是为了防止攻击者运行提升工具。

如果论坛管理员关闭了上传功能，则黑客会想办法获得超管密码，比如，如果你用动网论坛并且数据库忘记了改名，人家就可以直接下载你的数据库了，然后距离找到论坛管理员密码就不远了。

作为管理员，我们首先要检查我们的ASP程序，做好必要的设置，防止网站被黑客进入。另外就是防止攻击者使用一个被黑的网站来控制整个服务器，因为如果你的服务器上还为朋友开了站点，你可能无法确定你的朋友会把他上传的论坛做好安全设置。这就用到了前面所说的那一大堆东西，做了那些权限设置和防提升之后，黑客就算是进入了一个站点，也无法破坏这个网站以外的东西。

后记

也许有安全高手或者破坏高手看了我的文章会嘲笑或者窃喜，但我想我的经验里毕竟还是存在很多正确的地方，有千千万万的比我知道的更少的人像我刚开始完全不懂的时候那样在渴求着这样一篇文章，所以我必须写，我不管别人怎么说我，我也不怕后世会有千千万万的人对我唾骂，我一个人承担下来，我也没有娘子需要交代的……

因为这其实只是抛砖引玉的做法，从别人的笑声中，我和我的读者们都可以学到更多有用的东西。

2008R2服务器安全加固

Windows server 2008R2基于WIN7操作系统核心,是新一代的操作系统拥有更稳定的性能和更好的处理能力。

服务器安全是针对操作系统核心进行安全加固和配置,同时是网站服务器安全的运行的一个最基础的要求,也是配置网站环境的一个前提。

云顿科技现针对Web服务器安全提供以下类型操作系统的安全加固服务:

一、Windows系统服务器安全/Windows Server 2008R2(Enterprise)

安全内容包括:

1.操作系统危险文件加固设置权限;

2.系统危险文件夹权限加固;

3.系统危险服务优化;

4.系统危险组件及注册表加固;

5.Ddos防御注册表加固;

6.服务器反病毒软件安装与配置;

7.远程桌面端口连接配置;

8.防火墙规则配置;

9.正版系统KEY在线激活;

10.防病毒软件安装配置;

11.ARP防火墙设置;

Web环境安全配置内容包括:

1.IIS安装配置;
2.asp/php;
3.MySQL/Mssql2008
4.ZendOptimizer/WinCache;
5.phpMyAdmin;

6.FTP:Serv-U/MS-FTP;
7.PHP安全配置;
8.IIS安全网站目录权限隔离设置;
9.数据库安全设置;
10.系统补丁修补;

小提示:

1.建议您安装完一个新的操作系统后立即做该项服务器安全配置

2.:配置一个正常的Web环境能够有效的使网站安全稳定运行,同时这也是稳定运行的前提和基础,不正常配置通常会给网站数据及服务器安全带来巨大的安全隐患

远程管理Win2008服务器的安全技巧

我目前远程治理着多台服务器，并且经常需要远程连接到客户的系统上解决问题或是向客户演示如何去完成非凡的任务，其中有些客户的系统位于200英里以外的地方。

在过去，我一直使用Virtual Network Computing来连接这种服务器或客户机，不过使用VNC需要在防火墙上打开某些特定的端口，这需要涉及防火墙和内部网络的配置，以及在防火墙上建立端口映射。因此，虽然VNC是免费软件并且也有很好的跨平台性能，但它仍需要我在网络的可访问性上花费不少时间。

使用类似VNC

这种远程控制软件的另一点不足就是你必须在远程系统中安装服务器端程序，并在自己的机器上安装客户端程序。这在通常情况下都是可以实现的，但假如你不得不使用公用电脑或出于其它某些原因无法安装相应的远程治理软件，此时远程桌面Web连接(Remote Desktop Web Connection，RDWC)就成为了一个很好的选择。

虽然RDWC仍然无法避免在防火墙上打开特定端口的问题，但它完全避免了远程访问客户端软件的问题。下面我就来介绍一下RDWC是如何工作的，如何用它治理你的服务器和工作站以及如何配置防火墙才能正常使用RDWC。

关于远程桌面Web连接的说明

RDWC集成在Windows Server 2003 以及Windows
XP系统中。带有RDWC的系统可以启动终端服务Web客户端(Terminal Services Web
ClIEnt)的计算机，以便Web浏览器可以访问。换句话说，客户端系统不需要运行远程桌面连接程序或终端服务(Terminal
Services)客户端程序来连接远程系统，而只需要使用常用的Web浏览器就可以进行连接了。

RDWC是由一个
ActiveX控件、几个简单的Web页面以及可以运行IIS4.0或以上版本进行远程连接服务的文件构成的。因此不论是Windows Server 2003、Windows NT、Windows 2000，或是Windows
XP，都可以作为被远程控制的系统。而实现远程控制的客户端必须采用运行Internet Explorer 5.0或以上版本的浏览器的Windows平台。

对于远程控制来说，RDWC是一个很好的解决方案，同时，对于远程治理以及远程技术支持来说，RDWC也非常合适。另外，对于需要远程访问数据的业务伙伴、移动办公用户以及其他不愿意安装客户端程序的用户来说，RDWC也是很好的选择。

那么RDWC是如何工作的呢?当你安装RDWC时，安装程序会在目标服务器的Administration
Web站点上安装一个Tsweb虚拟目录。当担任远程控制任务的电脑连接到这个目标服务器上时，远程电脑中的IE浏览器会自动下载一个CAB文件包，用来安装RDWC所需的ActiveX控件。假如远程电脑中已经带有这个控件，只是版本与目标服务器的版本不符，那么IE也会自动下载新的。自动安装好

ActiveX控件后，连接页面就会出现。稍后我会介绍从客户端系统的连接过程。现在我们先安装RDWC。在本文中，我假定你使用Windows Server 2003。当然，假如你使用上面提到的任何一种平台也是一样的。

在Windows Server 2003上配置RDWC 虽然RDWC包含在Windows Server 2003中，不过默认情况下它并不会被安装。要手动安装RDWC，你需要在控制面板中点开“添加删除程序”项。然后点击“添加/删除Windows组件”，激活Windows组件向导。点击“应用服务器(Application Server)”，然后点击“具体资料”，添加“互联网信息服务(IIS)”。依次点击“具体资料”/“WWW服务”/“具体资料”，然后添加“远程桌面Web连接”。之后点击完成让安装程序安装指定的组件。

安装完成后，打开IIS治理控制台，并展开Web站点\默认Web站点。你会发现这里出现了一个Tsweb虚拟目录，假如你点击它，右边会列出一系列文件，其中包括一个名为Msrdp.cab的文件。在IIS中，你不需要进行有关RDWC的配置，不过需要在系统属性中答应系统接受远程连接请求。

具体的做法是:右键点击“我的电脑”并选择“属性”，并打开“系统属性”对话框。点击“远程”选项卡并勾选“Allow Users To Connect Remotely To This Computer”。默认情况下，只有治理员组的用户可以连接到这台电脑中。至于如何让其他用户利用RDWC访问到该系统则要看服务器端的配置了。首先我们来看看独立或成员服务器的配置。

假如这台电脑不是域控制器，那么使能RDWC用户比较轻易。首先，在系统属性对话框中点击 “Remote”选项卡。然后点击“Select Remote Users”，在弹出的“Remote Desktop Users”对话框中点击“Add”，输入用户名后点击“OK”。假如有多个用户需要连接，重复这个步骤即可。

通过这种方法添加用户，Windows Server会将用户加入“Builtin\Remote Desktop Users”组。实际上“Remote Desktop Users”对话框就是简单的显示出了该组的成员，并为用户提供了一个修改该组成员的界面。在默认情况下，这个组的成员都具有“Allow Log On Through Terminal Services”权限，这使得该组成WEB服务器安全员都可以通过RDWC进行远程登录。假如你愿意，也可以从“Local Users And Computers”控制台完成相同的工作，而不必进入系统属性对话框。假如这台电脑是一个域的成员服务器，你同样可以在“local Remote Desktop Users”组中添加域账户来让这些用户可以通过RDWC连接到服务器。

假如这台电脑属于域控制器，你还需要更进一步答应非治理员组的成员通过RDWC登录系统。在“Administrative Tools”文件夹下点击“Domain Controller Security Policy”打开“Default Domain Controller Security Settings”控制台。进入“Local Policies\User Rights Assignment\Allow Log On Through Terminal Services”，然后打开该策略并设置为“Enabled”。然后添加治理员组、远程桌面用户组以及其它你希望具有远程访问权限的独立用户或用户组。当然，你需要清楚哪些用户或用户组在进行远程访问时对系统的安全性不会造成不利影响。

使用RDWC连接远程服务器

在服务器上安装好RDWC并配置好帐号后，就可以轻松的从远端连接到服务器上了。在远端的电脑上打开IE浏览器并输入http://server/tsweb，这里的“server”是指你希望远程连接的服务器的主机名。比如，这个服务器的主机名叫做bart，连接方法就是http://bart/tsweb 。

根据网络配置和服务器所处的位置，你也许需要在URL区域输入完整的域名(FQDN)。你可以检查服务器上的Default Web Site，来确定这个主机标题(host headers)。在“Administrative Tools”文件夹中打开“IIS Manager”控制台，右键点击“Default Web Site”，选择属性。在“Web Site”选项卡中选择“Advanced”，然后查看“Multiple Identities For This Web Site”列表找到主机标题。假如这个列表只有“Default”，那么你可以用IP地址来代替主机名进行连接，或者也可以考虑添加一个主机标题以便实现 RDWC连接。

当你连接到正确的URL，IIS会显示一个页面，让你指定所要连接网站服务器安全的服务器和所要使用的屏幕分辨率。假如你选择了 “Send Logon Information For This Connection”选项，该页面会显示“User Name and Domain”区域。

点击“Connect”后，你会看到一个登录对话框。假如选择了全屏模式，这时候你的电脑就会和远程服务器端的电脑画面一样，显示出全屏的“Remote Desktop Connection”进程。你可以通过[Ctrl][Alt][Pause]键在窗口和全屏模式间切换，在切换时你会发现，这种远程连接确实是在IE浏览器中进行的。输入用户名密码后点

击OK，就可以登录到远程服务器进行治理了。其界面和在本地电脑上登录一样，只不过某些操作受到帐号权限的限制罢了。

网管入门:巧妙设置让Win2008系统更安全

[05-26 10:08:20]出处:pconline作者:帷幄责任编辑:wenzhicheng

伴随着Internet网络中的病毒、黑客、木马不断泛滥，以及Windows系统漏洞的不断增多，无论是普通电脑还是服务器所受到的安全威胁也是越来越多。即使新推出的Windows Server 2008系统，在安全性方面有了很大的提高和改善，但是我们仍然难以保证它就一定不会受到病毒、黑客或木马的袭击;为了更好地保证Windows Server 2008系统的安全，相信多数网络管理员都会不惜重金“请”来各式各样的专业安全工具，对服务器系统进行安全“护驾”！其实，在手头没有任何专业安全工具可以利用的情况下，我们可以依靠Windows Server 2008系统自身的力量，来将该系统各方面的安全防范性能全部发挥起来，这样同样能够为Windows Server 2008安全运行“护航”！

让更少的人看到自己

一般来说，局域网中的普通电脑在默认状态下能通过“网上邻居”窗口看到网络中的所有共享主机，这当然也包括Windows Server 2008服务器主机;由于服务器系统中存储有许多重要的资源，它就特别容易受到普通用户的随意访问，这么一来服务器系统受到非法攻击的可能性也就增大了。为了不让Windows Server 2008服务器系统遭受非法攻击，我们只要想办法让普通电脑在默认状态下无法

使用“网上邻居”窗口找到目标服务器主机，要做到这一点，其实很简单，因为Windows Server 2008系统特意为我们提供了一个网络发现功能，只要将该功能给关闭掉，那么局域网中的任何一台普通电脑都无法从“网上邻居”窗口中找到Windows Server 2008服务器主机的“身影”，那样的话服务器系统自然也就不会受到来自普通电脑的非法威胁了;下面是关闭Windows Server 2008系统网络发现功能的具体操作步骤:

首先以系统管理员身份登录进Windows Server 2008服务器系统，在该系统桌面中用鼠标右键单击“网络”图标，从其后的快捷菜单中选择“属性”命令，打开服务器系统的“网络和共享中心”窗口，在这里的“共享和发现”列表下面，我们会看到不少与网络共享访问操作有关的设置内容;

接着单击“网络发现”选项旁边的下拉按钮，打开如图1所示的设置区域，选中“关闭网络发现”选项，再单击“应用”按钮，最后再将服务器系统重启一下，如此一来本地服务器主机的“身影”就不会被普通电脑看到了，那么普通用户也就不能通过网上邻居窗口来对服务器实施非法攻击了。

需要提醒各位注意的是，当Windows Server 2008服务器主机没有连接到网络中时，“网络发现”功能会自动处于关闭状态，此时我们是无法使用手工方法强行启用“网络发现”功能的。

网管入门:巧妙设置让Win2008系统更安全

[05-26 10:08:20]出处:pconline作者:帷幄责任编辑:wenzhicheng

关闭安全威胁端口

许多时候，不少网络管理员为了方便管理Windows Server 2008服务器系统，常常会将一些能危及服务器系统安全的端口打开；可是他们在管理好服务器系统后，又不及时将它们关闭掉，这样一来非法用户可能就会通过这些危险端口来对服务器系统进行非法攻击。为了有效保护服务器系统的安全，我们需要及时将本地服务器系统中的一些安全威胁端口关闭掉。

例如在关闭服务器系统的139端口时，我们可以按照如下操作步骤来进行：首先以系统管理员身份登录进Windows Server 2008服务器系统，打开该系统的“开始”菜单，从中依次选择“设置”/“网络连接”命令，在其后的列表窗口中用鼠标右键单击本地连接图标，并执行右键菜单中的“属性”命令，进入本地服务器系统的网络连接列表窗口；

其次选中“Internet协议版本4(TCP/IPv4)”选项，并单击“属性”按钮，在弹出的TCP/IPv4属性界面中单击“高级”按钮，进入高级属性设置窗口；单击该设置窗口中的“WINS”标签，打开如图2所示的标签设置页面；在该设置页面的“NetBios设置”处，选中“禁用TCP/IP的NetBios”选项，再单击“确定”按钮，如此一来就能将Windows Server 2008服务器系统的139安全威胁端口关闭掉了。

如果要将服务器系统中的445端口关闭时，我们可以先打开服务器系统的“开始”菜单，从中选择“运行”命令，在弹出的系统运行文本框中输入“regedit”字符串命令，单击回车键后，打开本地系统的注册表编辑窗口；

其次在该注册表编辑窗口的左侧显示窗格中，将鼠标定位于HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters注册表分支选项，检查“Parameters”分支选项下面是否存在“SMBDeviceEnabled”双字节值，要是没有的话，我们可以直接用鼠标右键单击“Parameters”分支选项，从其后出现的右键菜单中依次选择“新建”/“Dword(32位)值”选项，并将新生成的双字节值名称设置为“SMBDeviceEnabled”，最后再将该键值的数值修改为“0”就可以了。

网管入门:巧妙设置让Win2008系统更安全

[05-26 10:08:20]出处:pconline作者:帷幄责任编辑:wenzhicheng

用防火墙限制Ping

为了检验Windows Server 2008服务器系统是否在线，不少朋友总会使用Ping命令来对服务器系统进行连通性测试操作;虽然这样的操作不会给服务器系统造成太大的影响，不过要是若干个用户同时对服务器系统进行Ping测试操作的话，那么服务器系统的运行性能就会受到明显影响了，并且一些非法用户还能通过Ping命令获得服务器系统的一些状态信息，之后可能会根据该状态信息对服务器系统进行有针对性攻击。

为了避免Windows Server 2008服务器系统遭遇非法Ping测试操作，我们可以利用该系统自带的高级防火墙功能，来巧妙定制禁止ping测试操作的安全策略，下面就是使用防火墙定义禁止ping测试操作规则的具体步骤：

首先以系统管理员身份登录进Windows Server 2008服务器系统，打开该系统的“开始”菜单，从中依次选择“程序”/“管理工具”/“服务器管理器”选项，在弹出的服务器管理器窗口中，依次展开左侧显示区域中的“配置”/“高级安全Windows防火墙”分支选项，进入Windows Server 2008服务器系统的防火墙高级安全设置窗口；

其次从该设置窗口中找到“查看和创建防火墙规则”设置项，单击该设置项下面的“入站规则”选项，之后在对应该选项的右侧操作列表中，单击其中的“新规则”选项，进入防火墙高级安全规则创建向导窗口，当向导窗口提示我们选择创建类型时，我们可以先选中“自定义”选项，并单击“下一步”按钮；

之后向导窗口会提示我们该规则应用于所有程序还是特定程序，此时我们可以选中“所有程序”选项，继续单击“下一步”按钮，打开如图3所示的向导设置界面，选中其中的“ICMPv4”选项，再单击“下一步”按钮，紧接着将此规则设置为匹配本地的“任何IP地址”以及远程的“任何IP地址”，再将连接条件参数设置为“阻止连接”，最后依照向导提示设置好适用该规则的具体网络环境，同时为这个刚刚创建好的高级安全规则取一个恰当的名称；等到上面的各项设置

操作完毕后，将Windows Server 2008系统重新启动一下，那样的话普通电脑就无法对服务器系统进行Ping测试操作了，那么服务器系统受到非法攻击的可能性就会明显减少了。

网管入门:巧妙设置让Win2008系统更安全

[05-26 10:08:20]出处:pconline作者:帷幄责任编辑:wenzhicheng

拒绝远程访问服务器

有时候，网络管理员没有妥善保管好服务器系统的账号信息，一旦别有用心的人意外获悉该账号时，他们就能通过远程方式来访问服务器系统，并对服务器系统做出一些破坏性操作，从而导致服务器系统无法正常为局域网用户服务。为了有效保护Windows Server 2008服务器系统的安全，我们需要禁止任何用户来对服务器系统进行远程管理，这么一来服务器系统的管理员账号即使发生了丢失，但非法用户由于无法到服务器现场，他们同样也无法对服务器进行各种非法破坏操作;下面，就是拒绝任何用户通过远程方式访问Windows Server 2008服务器系统的具体操作步骤:

首先以系统管理员身份登录进Windows Server 2008服务器系统，打开该系统的“开始”菜单，从中选择“运行”命令，在弹出的系统运行文本框中，输入字符串命令“gpedit.msc”，单击“确定”按钮后，打开服务器系统的组策略编辑窗口;

其次在该编辑窗口的左侧显示区域，选中“计算机配置”选项，再用鼠标依次展开该分支下面的“Windows设置”/“安全设置”/“本地策略”/“用户权限分配”选项，在对应该选项的右侧显示区域中，用鼠标双击“从网络访问此计算机”组策略选项，打开如图4所示的组策略选项设置对话框；

在这里，我们看到Windows Server 2008服务器系统在默认状态下会允许四类用户通过网络来远程访问服务器系统，为了禁止这些用户对服务器系统进行远程访问，我们可以将这里的所有用户账号依次选中，再单击“删除”按钮，如此一来任何用户也不能通过网络远程访问服务器系统了。

当然，要是我们只想限制用户通过网络远程关闭服务器系统时，那只需要打开“从远程系统强制关机”组策略属性设置窗口，在该设置窗口中删除所有的用户账号就可以了。

网管入门:巧妙设置让Win2008系统更安全

[05-26 10:08:20]出处:pconline作者:帷幄责任编辑:wenzhicheng

记忆非法账号登录信息

在对服务器系统进行管理维护的时候，网络管理员可能会碰到这样一种特殊情形，那就是网络管理员在短时间离开服务器现场一段时间后，可能有某个非法攻

击者趁机偷偷登录进服务器系统实施破坏攻击。很明显，倘若本地服务器系统中存储有非常重要的隐私信息时，那无疑会存在很大的安全隐患。事实上，我们可以对Windows Server 2008服务器系统的组策略参数进行适当设置，来让服务器能够对非法账号的登录信息进行自动记忆，以便帮助网络管理员日后能够找到故障“祸首”，下面就是设置服务器系统组策略的具体步骤:

首先以系统管理员身份登录进Windows Server 2008服务器系统，打开该系统的“开始”菜单，从中选择“运行”命令，在弹出的系统运行文本框中，输入字符串命令“gpedit.msc”，单击“确定”按钮后，打开服务器系统的组策略编辑窗口;

其次在该组策略编辑界面左侧显示窗格中选中“计算机配置”选项，再用鼠标双击该选项下面的“管理模板”/“Windows组件”/“Windows登录选项”组策略子项，在“Windows登录选项”下面用鼠标双击“在用户登录期间显示有关以前登录的信息”项目，打开如图5所示的组策略属性设置界面，检查其中的“已启动”选项是否处于选中状态，要是发现它还没有被选中时，我们可以及时将它选中，最后单击设置界面中的“确定”按钮，如此一来Windows Server 2008服务器系统就能对非法账号的登录状态信息进行自动记忆了。

日后，当网络管理员由于急事临时离开Windows Server 2008服务器主机现场时，如果某个非法攻击趁机偷偷登录进服务器系统时，那么

该非法用户的账号登录状态就会被服务器系统自动记忆下来;当网络管理员下次重新启动Windows Server 2008系统并输入登录密码,再单击“确定”按钮后,网络管理员就能从屏幕上看到究竟是哪位非法用户偷偷登录本地服务器的了,此时网络管理员就能采取有针对性的措施来进行安全防范了。

网管入门:巧妙设置让Win2008系统更安全

[05-26 10:08:20]出处:pconline作者:帷幄责任编辑:wenzhicheng

自动跟踪恶意攻击记录

为了阻止网络中的各种病毒、木马、黑客对Windows Server 2008服务器系统造成非法攻击,许多网络管理员肯定会想方设法地要在本地服务器系统中安装各种正版的防火墙软件或杀毒程序,然而多数情况下,我们手头并没有正版的专业防火墙或杀毒软件可以使用,在这种条件下我们不妨尝试使用服务器系统内置的防火墙工具来有效保护服务器系统的运行安全性。

这不,Windows Server 2008服务器系统内置的防火墙具有对各种已经的检测和未知的检测进行自动记录功能,巧妙地使用该功能,我们可以让服务器系统自动跟踪记忆那些企图对服务器系统进行恶意攻击的痕迹;以后,一旦服务器系统遇到安全故障或其他威胁时,网络管理员只要及时地打开防火墙程序对应的日志记录,说不定就能从中找

到攻击服务器的“罪槐祸首”了。在启用Windows Server 2008服务器系统内置防火墙的安全记录功能时，我们不妨依照如下步骤来进行：

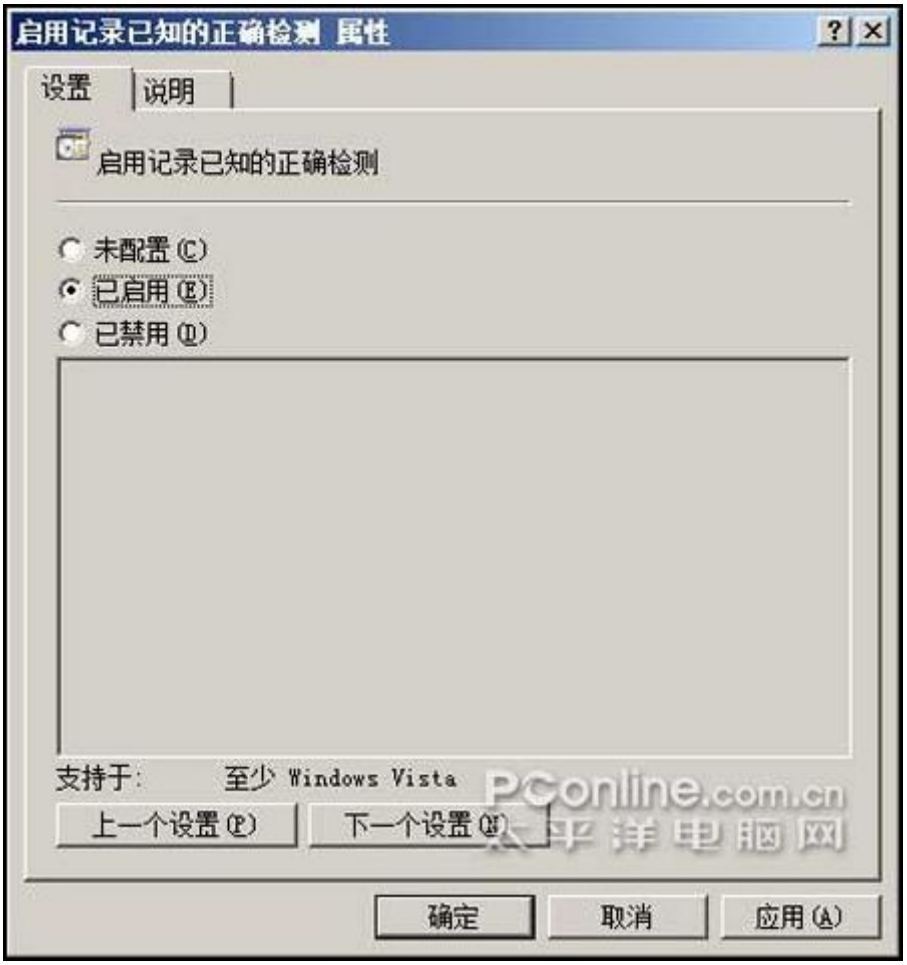

图6 自动跟踪恶意攻击记录

首先以系统管理员身份登录进Windows Server 2008服务器系统，打开该系统的“开始”菜单，从中选择“运行”命令，在弹出的系统运行文本框中，输入字符串命令“gpedit.msc”，单击“确定”按钮后，打开服务器系统的组策略编辑窗口；

其次在该组策略编辑界面左侧显示窗格中选中“计算机配置”选项，再用鼠标依次选择该选项下面的“管理模板”/“Windows组件”/“Windows

Defender”子项，从“Windows Defender”选项对应的右侧显示区域中找到“启用记录已知的正确检测”组策略项目，并用鼠标双击该项目，打开如图6所示的组策略属性设置界面，选中其中的“已启用”选项，再单击“确定”按钮，那样一来Windows Server 2008服务器系统防火墙就可以对已知文件进行跟踪测试，并将跟踪测试结果自动记录保存到对应日志文件中；

按照同样的操作办法，我们再依次展开“计算机配置”分支下面的“管理模板”/“Windows组件”/“Windows Defender”子项，并从“Windows Defender”子项对应的右侧显示区域中双击“启用记录未知检测”组策略选项，在其后出现的目标组策略属性设置界面中，也选中“已启用”项目，最后单击“确定”按钮，那样的话Windows Server 2008服务器系统内置的防火墙日后也会对未知的操作进行跟踪测试，并且会将跟踪测试结果保存到对应的日志文件中。以后，当Windows Server 2008服务器系统遇到安全故障时，我们只要打开相应的日志文件，说不定就能从中找到故障应对的办法了。

如何保障Server 2008服务器的远程桌面安全(图)

时间:2009-08-06 08:54 来源:bitsCN.com 字体:[大 中 小]

远程桌面是管理员对Windows系统实施远程管理和维护的首先工具，当然也是攻击者窥视和企图接管的对象。因此，一个有经验的系统管理员在客户端或者服务器上开启远程桌面后定会进行一定的安全部署。对于Windows Server 2008来说，远程桌面是终端服务的一个功能，Windows Server 2008的安全特性和相关细节，为用户进行远程桌面管理以及提升其安全性提供了更多选项。本文将和大家一道挖掘Windows Server 2008远程桌面管理中的相关技术细节。

1、启用远程桌面时应注意的细节

在Windows Server 2008中开启远程桌面的操作是非常简单的，但不同于此前的系统它提供了更多的安全选项，这些选项是我们应用注意的。另外，因为Windows Server 2008的安全特性，大家在开启远程桌面前或者开启之后还应用注意有关事项。

(1).慎重选择限制远程连接系统的版本

依次点击“控制面板”→“系统和维护”→“系统”进入系统管理页面，单击左窗格中的“远程设置”链接打开“系统属性”对话框，点击“远程”选项卡来到启用远程桌面窗口。对于启用远程桌面大家可谓轻车熟路，但该页面中启用Windows Server 2008远程桌面的两个选项希望引起大家的注意。首先是“允许运行任意版本远程桌面的计算机连接(较不安全)”选项，如果选择该项那么任意版本的Windows都可以通过远程桌面连接到该主机，毫无疑问，这是不安全的。在此，管理员应该

做考量是否限制远程连接的系统版本以提升远程桌面的安全，一般情况下管理员应该以自己平时使用的系统版本为依据进行选择。另外一个选项是“只允许运行带网络身份验证的远程桌面的计算机连接(更安全)”，如果选择该项，那么将只允许安装了Windows Vista、Windows Server 2008、Windows 7的计算机进行远程连接。如果条件允许，笔者当然建议大家选择该项，毕竟安全第一嘛。

(2).账户和防火墙相关的注意事项

在Windows Server 2008上开启远程桌面时还需注意，所有远程连接必须使用带有密码的账户创建，如果系统中的某个本地账户没有密码，那么就无法使用该账户进行远程连接。这是一些个人用户经常遇到的问题，明明开启了远程桌面但就是无法通过账户登录。

另外，考虑到Windows Server 2008的防火墙非常强大一般用户会选择时系统防火墙，此时如果开启远程桌面的话，系统防火墙会自动创建一个例外，允许远程桌面协议(RDP)连接穿透防火墙。默认情况下，该协议使用TCP 3389端口，同时在注册表的HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber键值中记录了该端口号。出于安全考虑，希望大家将该端口号更改为一个陌生的端口，更改的方法就是修改该注册表键值的值。如果计算机系统使用了其他第三方防火墙，则不行要在该防火墙中打开该端口，以允许建立传

入的远程桌面协议(RDP)连接。在此提醒的是，允许连接的端口是你更改后的端口而不是此前的TCP 3389端口。

2、对远程登录用户可采用的授权方法

默认情况下，Administrators组中的所有成员都可以远程登录，同时Windows Server 2008 Active Directory中的Remote Desktop Users组的成员也可以进行远程管理。处于安全考虑，我们必须更改默认授权而实施对特定的用户或者组授权。

(1).在远程桌面控制台中授权

在Windows Server 2008的“系统属性”对话框中，单击“远程”选项卡进入远程桌面设置窗口。在开启远程桌面后，单击其中的“选择用户”按钮，随后打开“远程桌面用户”对话框，同时所有Remote Desktop Users组的成员都会被列在这里。要添加新的用户或者组到该列表，单击“添加”按钮打开“选择用户或组”对话框。在该对话框中输入所选或默认域中用户或组的名称，然后单击“检查名称”。如果找到了多个匹配项目，则需要选择要使用的名称，然后单击“确定”。当然也可以单击“查找范围”按钮，选择其他位置通过查找功能添加相应的用户。如果还希望添加其他用户或者组，注意在它们直接输入分号(;)作为间隔。再次，笔者的建议是：删除对于组的授权，而只授予特定的用户远程连接权限。这样就会增加攻击者猜解用户账户的难度，从而提升了远程桌面的

安全。作为一个安全技巧，大家可以取消administrator账户的远程连接权限，而赋予其他对于攻击者来说比较陌生的账户的远程连接权限。

(2).通过组策略限制远程登录

在组策略中，Administrators和Remote Desktop Users组的成员默认具有“允许通过终端服务登录”的用户权限。如果修改过组策略，可能需要复查，以确保这个用户权限依然被分配给这些组。一般来说，可以针对具体的计算机复查设置，但也可以通过站点、域已经组织单元策略进行复查。打开相应的组策略对象，然后依次展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用权限指派”，双击“通过终端服务允许登录”策略，查看要使用的用户和组是否在列。

如果希望限制用户对服务器进行远程登录，可以打开相应的组策略对象，展开“计算机配置”→“Windows 设置”→“安全设置”→“本地策略”→“用权限指派”节点，双击“通过终端服务拒绝登录”策略。在该策略的属性对话框中，选择“拒绝这些策略设置”，然后单击“添加用户或组”，在添加用户或组对话框中，单击“浏览”，并使用选择用户、计算机或组对话框输入希望拒绝通过终端服务进行本地登录的用户或组的名称，然后单击“确定”即可。另外，也可以在终端服务配置工具中修改组的默认权限。例如，可以将对终端访问对象具有完全控制权限的Administrators组删除。

如何保障Server 2008服务器的远程桌面安全(2)

时间:2009-08-06 08:54 来源:bitsCN.com 字体:[大 中 小]

3、在组策略中配置远程桌面管理

远程桌面管理是终端服务的一部分，当然也可使用组策略配置远程桌面。其实，微软也建议首先使用组策略作为终端服务和远程桌面管理功能的首选工具。在实战中，我们可以针对特定的计算机配置本地策略，或在域中的组织单元(OU)上设置。我们可以使用组策略对象编辑器进行修改，定位到“计算机配置”→“管理模板”→“Windows
组件”→“终端服务”节点以及“用户配置”→“管理模板”→“Windows
组件”→“终端服务”节点下进行设置。该节点下有6个配置项目，大家可以根据需要进行配置。一般来说，远程桌面管理都用于对企业内部的服务器进行管理，但终端服务服务器通常都会使用独立的OU被隔离在特定的组中。因此如果打算在企业内部使用终端服务服务器，则应该考虑为终端服务服务器创建独立的OU，这样就可以通过远程桌面单独管理终端服务服务器。

4、远程桌面连接客户端设置技巧

Windows Server
2008使用的远程桌面连接客户端(mstsc)是最新的第6版本，这个版本的连接客户端相比以前的版本有了较大的改进，增加了许多有趣而实用的功能。下面和大家共享几个使用mstsc进程远程桌面连接中的相关技巧。

(1).自定义显示分辨率

Windows Server

2008中的mstsc支持高达1680×1920或1920×1200或更高的分辨率。除了可以在mstsc的图形界面中设置分辨率外，当然最快捷的是直接通过命令设置。比如我们运行“mstsc /w:1920

/h:1200”即将客户端的分辨率设置为1920×1200，其中/h、/w是参数分别表示屏幕的高和宽。如果大家将某次桌面连接配置保存为RDP文件，我们可以打开该文件然后修改其中的desktopwidth和desktopheigh后面数值以改变屏幕大小。例如desktopwidth:i:1920或desktopheigh:i:1200。

(2).在远程桌面中使用多显示器

Windows Server

2008中的mstsc支持多显示器，这样就能够显示远程会话的所有内容。需要说明的是：要使用多显示器，那么这些显示器必须水平对齐，并使用同样的分辨率。要使用远程桌面的多显示器跨越功能，需要在mstsc中添加/span参数，例如“mstsc

/span”。当然，我们也可以通过修改RDP文件中的特定数值实现显示器跨越，比如“Span:i:1”

(3).调整传输数据的优先级

Windows Server

2008中的mstsc在显示远程系统的数据方面是有一定的优先级的。我们希望的

优先级是:显示器、键盘和鼠标的相关数据比其他类型的数据，比如打印机或文件传输更优先处理。默认情况下，显示器和输入数据将占可以带宽的70%，而其他通信只占可以带宽的30%。在某些特殊情况下，我们需要调整这个默认的优先级以符合我们的特殊需求。要修改这个优先级就需要在Windows Server 2008的注册表中进行修改，其注册表项是HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Servers\TermDD。需要条的子键是(如果没有这些键值可以自己创建，这些键值都是32位的DWORD值):

FlowControlDisable

将其值设置为“1”就会禁止显示数据的优先级，反之，所有不同的数据就请求都会被同等对待，其他是注册表值就会被忽略。

FlowControlDisplayBandWidth

该键值设置相对带宽优先级的比例，其默认值是70，最大允许的数值是255。

FlowControlChannelBandWidth

该键值设置其他数据比如打印机、文件传输等占用的可以带宽比例，其默认值是30，最大可以设置为255。

FlowControlChargePostCompression

该键值决定是否要根据演示前和压缩后的数据大小决定带宽的分配，默认值是“0”，意味着比例的计算是根据压缩前数据的大小进行的。大多数情况下，我们希望以这种方式进行，因为这样确保了客户端不要在发送数据前等待数据压缩完毕，节省了时间。

(4).选择连接客户端启动的方式

Windows Server

2008中启动远程桌面连接客户端可采用两种方式，即管理模式和虚拟会话模式。相比虚拟会话模式，管理模式能够极大地改善管理员成功执行程序、应用程序和进程的成功率。因此，作为管理员建议采用管理模式启动远程连接客户端。下面笔者分别说说这两种连接方式如何启动。

运行于虚拟会话模式

虚拟会话模式可被管理员和其他用户用于在远程系统上启动虚拟会话。要运行虚拟会话模式可执行下面的操作：在命令行或者运行对话框中运行命令“mstsc”，或者单击“开始”→“所有程序”→“附件”，然后选择“远程桌面连接”选项即可启动虚拟模式的远程桌面连接客户端。

运行于管理模式

管理模式可被管理员用于与远程系统的控制台进行完全的交互。要运行管理模式的客户端，必须根据客户端的类型进行下列操作：在命令行或者运行对话框中执行“mstsc /admin”或者“mstsc /console”。

如何保障Server 2008服务器的远程桌面安全(3)

时间:2009-08-06 08:54 来源:bitsCN.com 字体:[大 中 小]

5、远程登录用户的监视

Windows Server 2008是允许有多个用户同时通过远程桌面连接的，因此管理员一定要做好远程登录用户的监控，以甄别是否有可疑或者非法的远程连接。除了可以使用终端服务管理器查看登录会话外，我们还可以通过两种方法来监控远程登录的用户。

首先的使用quser命令，通过telnet连接到该服务器或在本地命令行先执行命令quser命令即可看到谁已经登录当前系统。或者我们也可以运行命令“quser /server:ServerName”来查看登录到远程服务器上的用户，其中ServerName的服务器的名称。如图所示，该服务器上有两个活动的会话，其中ctocio登录到了一个活动的RDP会话，会话ID是2，意味着是会话2。administrator登录到了本地控制台，会话ID是2，即会话1。

在此，笔者和大家共享一个技巧。有时候当有多个用户通过远程桌面登录到服务器，但并没有有效注销，此时当有其他的用户要通过远程桌面登录到服务器时会因为用户连接超过授权数而无法登录。此时，我们就可远程telnet到服务器或者在服务器的命令提示符中执行命令“logoff ID”来注销某个用户，其中ID就是会话序号，比如执行“logoff 2”就将强迫ctocio用户从系统注销。这样，其他的用户就可以通过远程桌面登录系统了。

除了命令外，我们还可以通过“任务管理器”查看用户会话。单击任务栏选择“任务管理”即可打开任务管理器窗口，点击“用户”选项卡可以看到当前登录服务器的用户。在此，我们可以对特定用户执行“断开”、“注销”操作，当然也可以“发送消息”。

笔者这里要强调一下，注销用户和断开用户是是完全不同的。如果断开一个会话，这会话将处于断开状态，但依然会在进程中执行。如果注销用户，则会结束该用户的会话，同时关闭该用户运行的所有应用程序，同时还会结束该用户运行的所有前台进程。笔者建议，管理员在远程维护完成后最好以“注销”的方式断开和服务器的连接。这样不仅会释放服务器资源，而且方便下一次的登录。往往有不少用户在远程登录完成后会直接关闭远程桌面客户端窗口，这样的操作就类似“断开”操作，它还占用着服务器会话通道，当达到服务器的用户授权上限时其他用户就不能够远程登录到服务器。**6、解惑远程登录验证证书无效或者过期**

有时候当我们通过远程桌面客户端连接服务器时，会收到“从远程计算机获得的验证证书无效或过期”的错误提示，这时什么原因呢?其实，在默认情况下在建立RDP连接之前，计算机还需要验证远程计算机的身份。如果远程计算机的验证证书无效或者过期，将无法连接，同时还会受到类似的警告信息。对此，我们首先应该检查一下两台计算机的日期和时间设置是否正确。因

为如果两台计算机之间的时间和日期有偏差，则可能会导致验证证书无效。当然，如果不希望计算机验证远程计算机的身份，我们可以禁用该功能。其具体设置方法是：在远程桌面连接器窗口中单击“选项”打开额外配置选项卡，进入高级选项卡，然后设置服务器验证选项为“连接并且不向我发送警告”即可。

总结：本文和大家共享了Windows Server 2008远程桌面管理中容易被忽略某些技术细节，同时也和朋友们分享了笔者的一些经验。最后希望这些细节和经验能够对大家有所帮助。

关于Windows 2008 R2 Web服务器环境搭建、安全流程

Windows Server 2008R2服务器安装及设置教程;

第一篇:系统安装与设置

前言:

本安装及设置教程适用于使用Windows2008R2为操作系统的服务器,目的是让服务器实现下列环境。

语言脚本环境:ASP、ASP.Net1.1、ASP.Net2.0、ASP.Net3.0、ASP.Net3.5、PHP(FastCGI模式)。

数据库环境:Access、MSSQL、MySQL。

FTP环境:Ser-U

常见组件:AspJpeg、Jmail、LyfUpload、动易、ISAPI_ReWrite。

一、系统准备

操作系统:Windows2008R2原版安装文件、服务器硬件驱动程序、SQL SERVER 2000安装盘、SQL SERVER 2000 SP4补丁,MySQL安装包,PHP压缩包,Zend Optimizer安装包,Serv-U

囧.0.6，Aspjpeg 2.0，JMail 4.5，LyfUpload，动易组件
1.8.6，ISAPI_ReWrite，GHOST。

Windows2008R2和SQL SERVER
2000安装文件可以购买正版光盘或其他途径获得。Windows2008R2最好是原版，
SQL SERVER 2000可以选择企业版或者标准版。

SQL SERVER 2000 SP4可以直接从微软网站下载获得。

服务器硬件驱动应该在购买服务器的同时附带了。

MySQL安装文件，PHP安装文件，Zend
Optimizer安装文件可以到其官方网站免费下载，或到其他下载网站获得。

Serv_U，Aspjpeg，Jmail，LyfUpload，动易组件，ISAPI_ReWrite和GHOST等
均可以通过购买或者其他途径来获得。

二、系统安装

分区：

服务器的硬盘是320G，分成了4个区，C盘做系统盘（30G），D盘做数据库和
软件盘（50G），E盘做网站目录（150G），F盘做备份盘（90G），以NTFS格式对4个
区进行格式化。

安装系统：

启动服务器，设置BIOS为光盘启动，重启，插入Windows2008R2安装盘至光
驱中，根据提示安装操作系统。

设置登录时不弹出“管理您的服务器”窗口：

启动计算机，弹出“管理您的服务器”窗口，勾选窗口左下方的“登录时不要显示此页”。

启动自动更新：

选择初始配置任务--启动自动更新和反馈--启动自动更新和反馈。

下载并安装更新：

选择初始配置任务--下载并安装更新--更改设置--重要更新--选择下载更新，但是让我选择是否安装更新--确定

修改计算机名：

选择初始配置任务--提供计算机名和域--更改--输入计算机名--确定--重启

安装驱动：

系统安装更新完毕，进入系统，按照主板-显卡-声卡-网卡-其他设备的顺序安装各类驱动程序。

安装WEB服务器：

01.进入服务器管理器

02.选择角色，添加角色

03选择WEB服务器，下一步

04.选择除FTP服务器外的所有选项，下一步

05.安装

安装.net 3.5功能：

01.进入服务器管理器

02.选择功能，添加功能

03.选择.net Framework 3.51功能，选择Windows 进程激活服务，选择XPS查看器

04.下一步，安装

安装更新：

点击右下角更新图标，选择更新，安装更新，重启计算机。

启用父路径

打开Internet 信息服务(IIS)管理器，选择本地服务器，选择ASP，选择启用父路径，将False改为True。

远程访问服务

一.启动远程访问服务

01.选择服务器管理器--启用远程桌面

02.选择允许运行任意版本远程桌面的计算机连接(较不安全)。备注:方便多种版本Windows远程管理服务器。

03.确定

二.修改远程访问服务端口

01.在开始--
运行菜单里,输入regedit,进入注册表编辑,按下面的路径进入修改端口的地方

02.HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp

03.找到右侧的

"PortNumber",用十进制方式显示,默认为3389,改为(例如)6666端口

04.HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp

05.找到右侧的

"PortNumber",用十进制方式显示,默认为3389,改为同上的端口

06.在控制面板--Windows 防火墙--高级设置--入站规则--新建规则

07.选择端口--协议和端口--TCP/特定本地端口:同上的端口

08.下一步,选择允许连接

09.下一步，选择公用

10.下一步，名称：远程桌面-新(TCP-In)，描述：用于远程桌面服务的入站规则，以允许RDP通信。[TCP 同上的端口]

11.删除远程桌面(TCP-In)规则

12.重新启动计算机

堵住资源共享隐患

打开“本地连接”界面，选择“属性”，左键点击“Microsoft网络客户端”，再点击“卸载”，在弹出的对话框中“是”确认卸载。点击“Microsoft网络的文件和打印机共享”，再点击“卸载”，在弹出的对话框中选择“是”确认卸载。

解除Netbios和TCP/IP协议的绑定

打开“本地连接”界面，选择“属性”，在弹出的“属性”框中双击“Internet协议版本（TCP/IPV4）”，点击“属性”，再点击“高级”—“WINS”，选择“禁用TCP/IP上的NETBIOS”，点击“确认”并关闭本地连接属性。

禁止默认共享

点击“开始”—“运行”，输入“Regedit”，打开注册表编辑器，打开注册表项“HKEY_LOCAL_MA

CHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters”，在右边的窗口中新建Dword值，名称设为AutoShareServer，值设为“0”。

提高系统性能

右键点击“计算机”，选择“属性”—“高级系统设置”—“高级”—“设置”，选择“调整为最佳性能”;确定。

修改虚拟内存的位置或禁用虚拟内存

两者选择其一，在内存足够大的情况下可以禁用虚拟内存。如果内存不是非常大，还是修改虚拟内存到硬盘的非系统盘。一般情况下不建议禁用虚拟内存。

1、 修改虚拟内存的位置:右键点击“计算机”，选择“属性”—“高级系统设置”—“高级”—“设置”—“高级”—“虚拟内存”—“更改”，取消勾选“自动管理所有驱动器的分页文件大小”，在“驱动器”选择框里面选中系统盘，选择“无分页文件”，在非系统盘如D盘，选择“自定义大小”，输入“初始大小”和“最大值”，点击“设置”，并确认修改。

2、 禁用虚拟内存:右键点击“计算机”，选择“属性”—“高级系统设置”—“高级”—“设置”—“高级”—“虚拟内存”—“更改”，取消勾选“自动管理所有驱动器的分页文件大小”，对所有驱动器都选择“无分页文件”，然后点击“设置”并确认修改。

本地安全策略

更改管理员账号和来宾账号

本地策略-安全选项-

账户，重命名系统管理员账户，把Administrator改名。重命名来宾账户，把Guest用户改名为Administrator，不过是什么权限都没有的那种，然后打开记事本，一阵乱敲，复制，粘贴到"密码"里去。

组策略

计算机配置—Windows设置—安全设置—本地策略—安全选项

交互式登陆:不显示最后的用户名(启用)

关闭自动播放

控制面板，自动播放，取消勾选，保存。

点击“开始”—

“运行”，输入“Gpedit.msc”，打开组策略编辑器，依次展开“计算机配置”—

“管理模板”—

“Windows组件”，在右侧窗口找到“自动播放策略”选项并打开，双击右侧关闭自动播放，在打开的对话框上部选择“已启用”，在对话框下部选择“所有驱动器”，点击“确定”完成设置。

备份系统

至此重启服务器，对刚刚做好的操作系统做一个GHOST。