# 商家系统服务端部署文档

# 目录

# 前言

其实要配置一台安全的服务器，简单来说就几句话：

能不开放的端口和可以不运行的服务全部关闭或禁用；

使用可进行端口通讯访问策略配置的防火墙；

严格控制系统中各种程序对各个目录创建、修改与删除可执行脚本、动态链接库与程序的

权限；

对于网站目录，能写入的目录或文件不能有执行权限，有执行权限的目录不可以赋给写入

权限。（这条最为关键）

# 部署环境

## 服务器环境信息

服务器软件环境：

|  |  |
| --- | --- |
| **名称** | **说明** |
| 磁盘阵列 | RAID 10 |
| 操作系统 | Windwos2008 R2 Enterprise 64Bit  （其实本人最熟悉的还是win2003服务器，由于公司购买的Dell R820服务器不再支持低端系统，没办法只能将自己升级起来，当前如果你的服务器还是使用win2003的话，查看本文还是有一定帮助的，两者只是在配置某些地方有不一样，但整体的安全思想是一致的） |
| IIS | 7.5 |
| DB | ORACLE |
| .NET Framework | .net 4.0 |
| 杀毒软件与防火墙 | McaFee 64位vse880;  HostIPS Client700； |
| 邮件发送软件 | JMail |
| IP地址 | 您来配 |

# 磁盘阵列配置

具体配置请查看《RAID配置中文手册》，链接地址：  
http://support1.ap.dell.com/cn/zh/forum/thread.asp?fid=20&tid=61244  
配置前，请提前备份好硬盘里的数据，重新做过阵列后，硬盘中的数据将全部丢失。

# 安装操作系统

具体安装操作步骤，请查看《R820服务器安装指南》  
1)    通过Lifecycle 安装 windows 2008：  
http://zh.community.dell.com/support\_forums/poweredge/f/279/t/2812.aspx  
这个方法是开机直接按F10，进行安装操作系统，可以快速的安装。 其它官方支持的系统安装，只是在选择操作系统的时候，选择对应的就可以进行快速的安装。  
  
2)    手动安装2012 ：  
http://zh.community.dell.com/support\_forums/poweredge/f/279/t/9621.aspx  
这个方法是直接通过2012的安装光盘，从光驱启动进行安装的操作方法。  
在选择安装磁盘时，可将本文档所在文件夹中的RAID驱动解压到U盘中，将U盘插入服务器后手动选择载入驱动进行安装。  
  
其他安装过程的操作方法同平时安装操作系统一样，这里就不做详细描述了。

# 安装软件

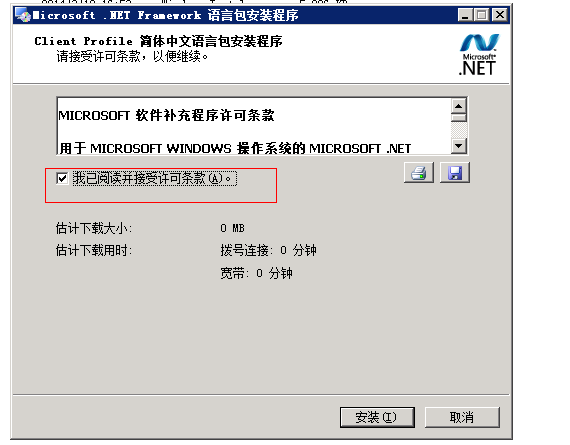
## 安装.NET Framework4

运行dotNetFx40\_Full\_x86\_x64.exe安装.net4框架



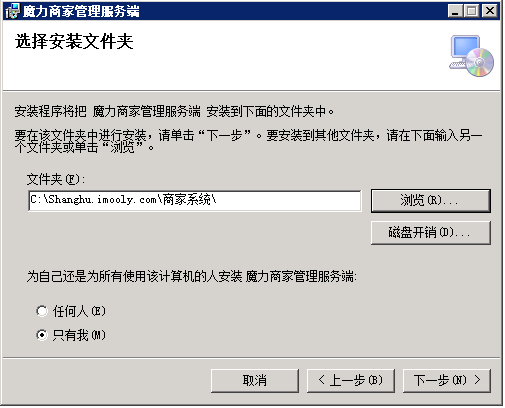
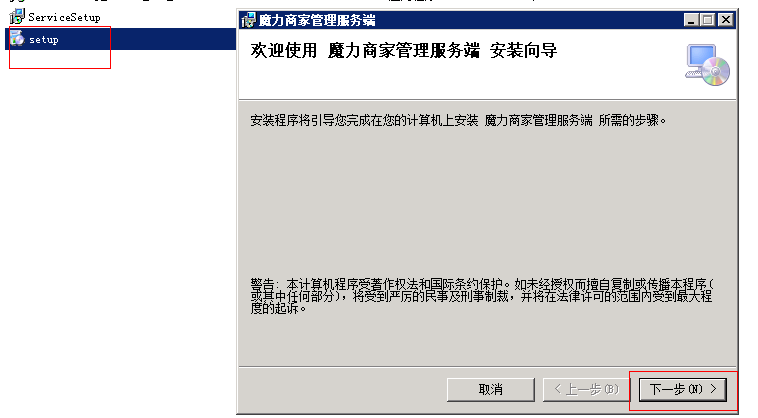
## 安装.NET Framework4 Client Profile

运行dotnetfx40lp\_client\_x86\_x64zh-hans.exe 安装.net4客户端



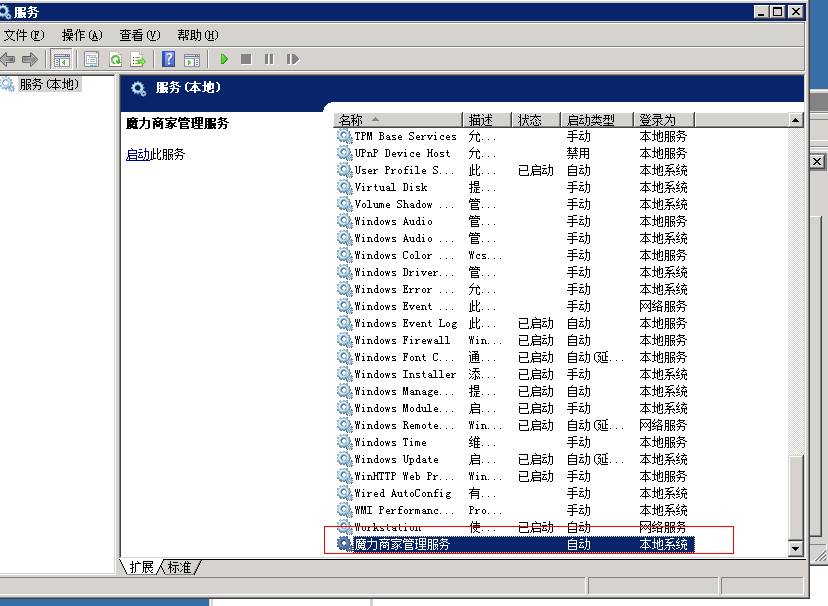
## 安装魔力商家系统服务端

执行商家系统服务端安装程序



一直下一步，直到安装完成。

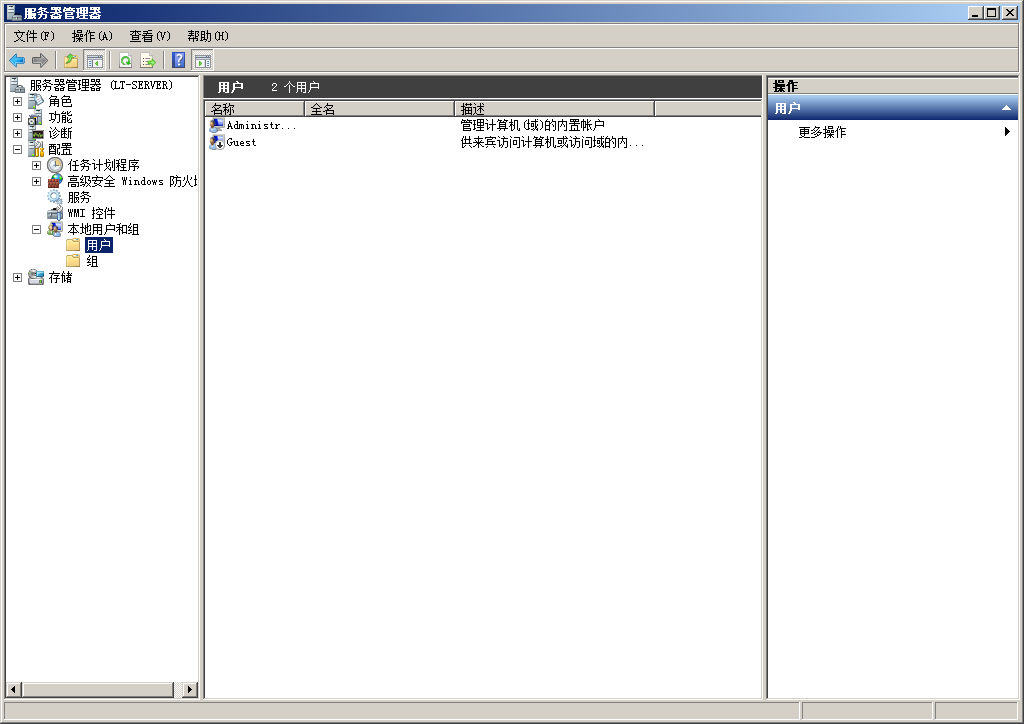
启动服务：



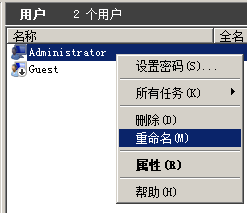
# 服务器与安全配置

## 修改系统默认帐户名

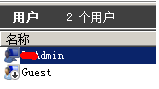
修改系统默认帐户名并新建一个Administrator帐户作为陷阱帐户，设置超长密码，并去掉所有用户组。(就是在用户组那里设置为空即可.让这个帐号不属于任何用户组)，同样改名禁用掉Guest用户。



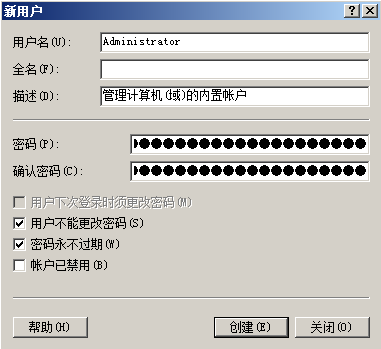
先对原Administrator用户进行重命名



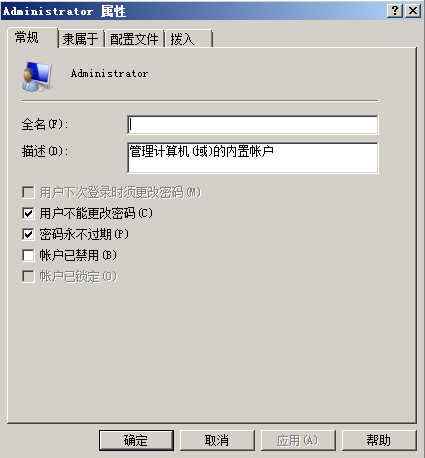
修改为你自己喜欢的名称



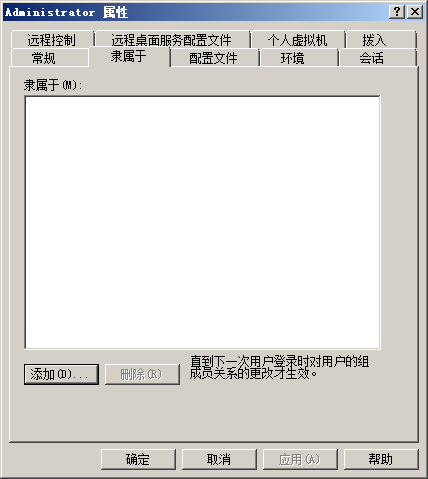
然后新建一个Administrator欺骗帐户，设置混合超长密码



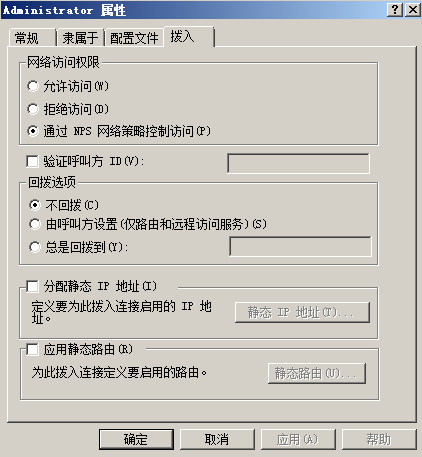
对它进行编辑



删除隶属的组



因这个是欺骗帐户，所以充许网络策略控制访问

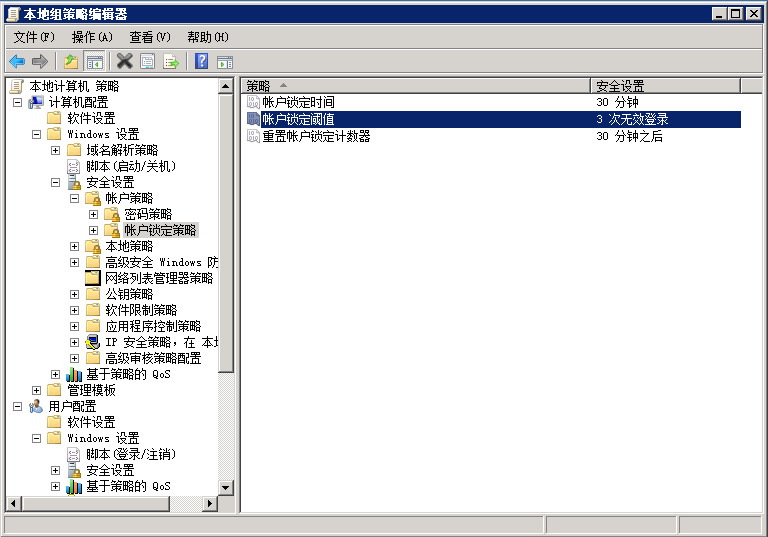


将Guest也进行重命名操作



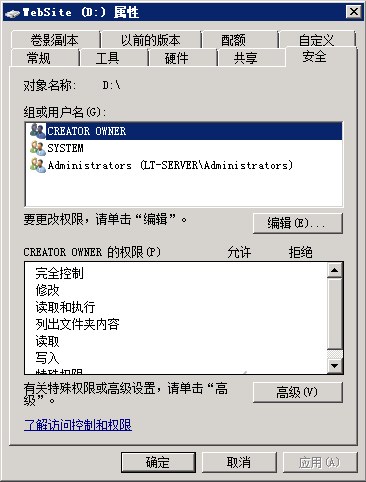
## 配置帐户锁定策略

在运行中输入gpedit.msc回车，打开组策略编辑器，选择计算机配置-Windows设置-安全设置-账户策略-账户锁定策略，将账户设为“三次登陆无效”，“锁定时间30分钟”，“复位锁定计数设为30分钟”。



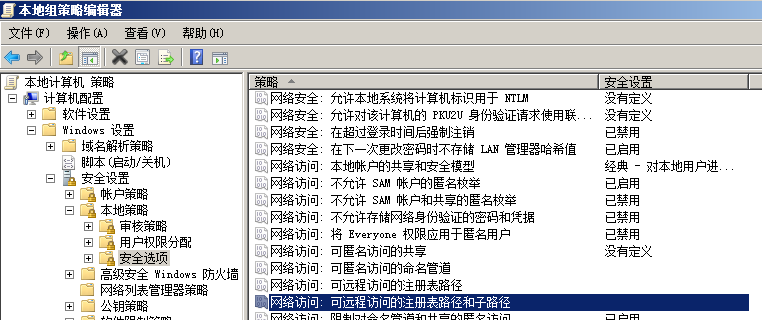
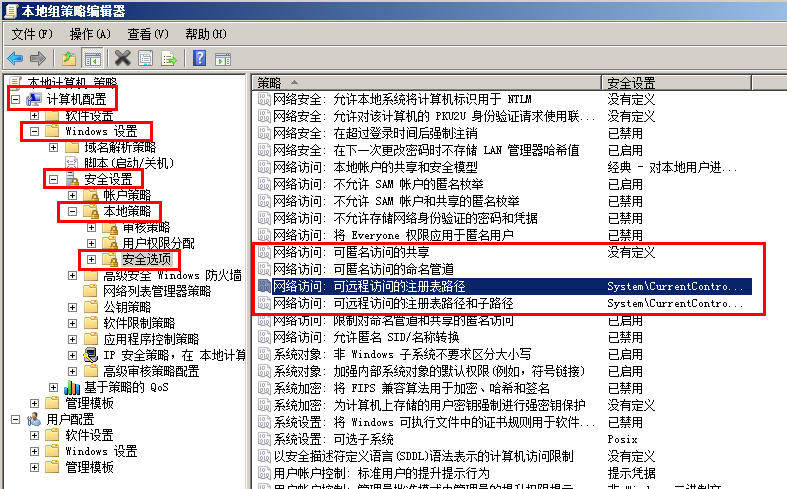
## 服务器硬盘安全访问安全配置

所有磁盘除CREATOR OWNER、administrators和system的用户权限全部删除（C盘必须保留Users用户组，理论上来说是要删除Users用户组的，但很多朋友如果这里直接删除，操作不当的话，网站有可能就访问不了，必须对系统目录下的不少目录重新配置权限非常麻烦，所以本文建议保留，只要按下面的一些设置做到位，这里也不会有多大的安全隐患的）



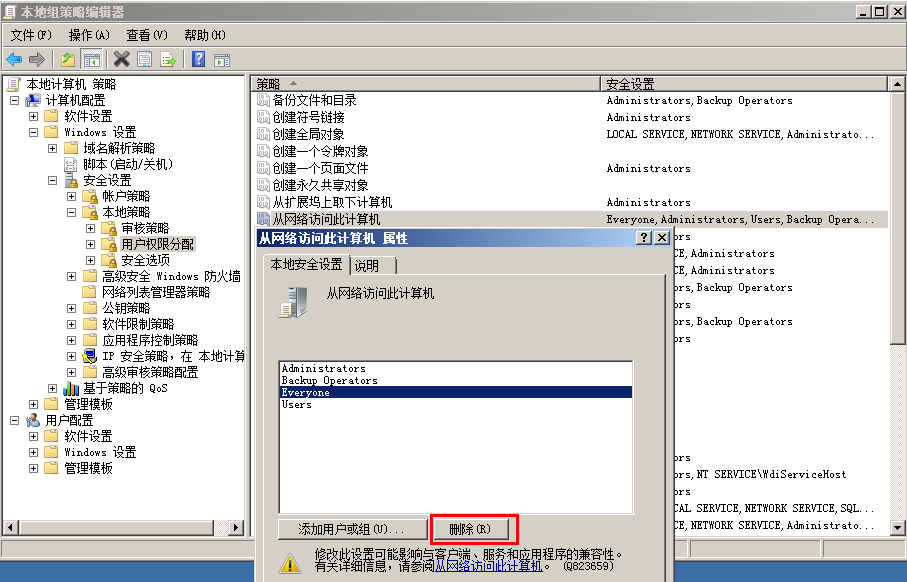
## 设置网络访问策略

在运行中输入gpedit.msc回车，打开组策略编辑器，选择计算机配置-Windows设置-安全设置-本地策略-安全选项，将   
网络访问:可匿名访问的共享;   
网络访问:可匿名访问的命名管道;    
网络访问:可远程访问的注册表路径;   
网络访问:可远程访问的注册表路径和子路径;   
以上四项清空



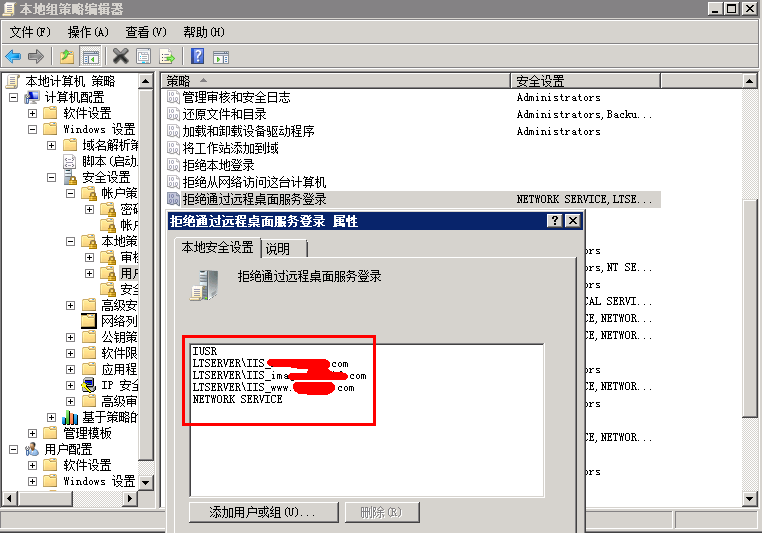
## 设置用户权限分配策略

在运行中输入gpedit.msc回车，打开组策略编辑器，选择计算机配置-Windows设置-安全设置-本地策略-用户权限分配  
将“从网络访问此计算机”策略中的“Everyone”删除



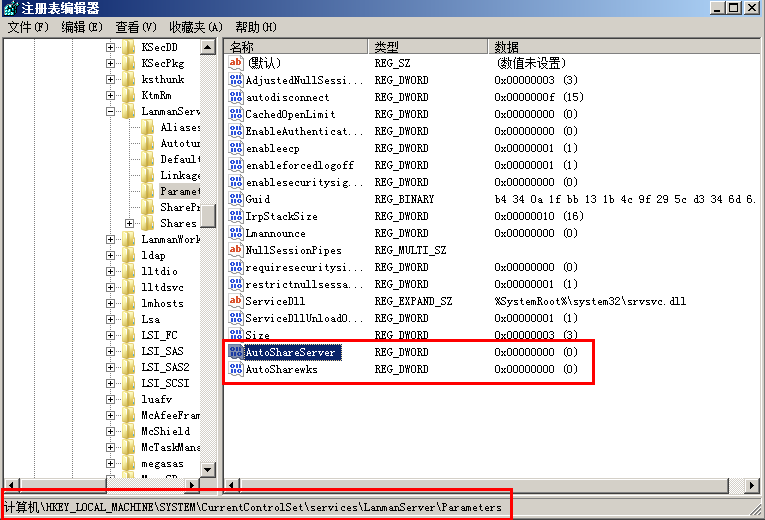
在“拒绝通过远程桌面服务登陆”策略中，添加下面用户组和用户

**另外，在添加新站点时，也必须将创建的新用户添加到这里**



## 关闭默认共享

打开注册表  
[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters]  
新建DOWRD值，名称为“AutoShareServer”、“AutoShareWKs”，设置值为“0”

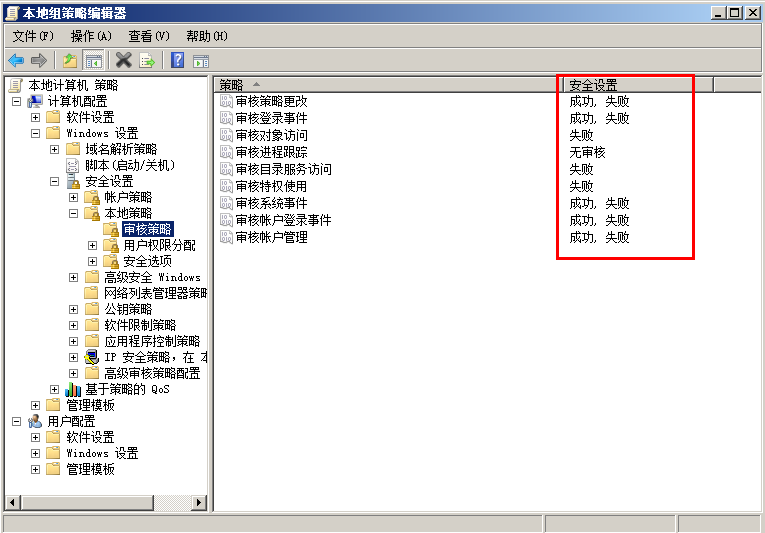
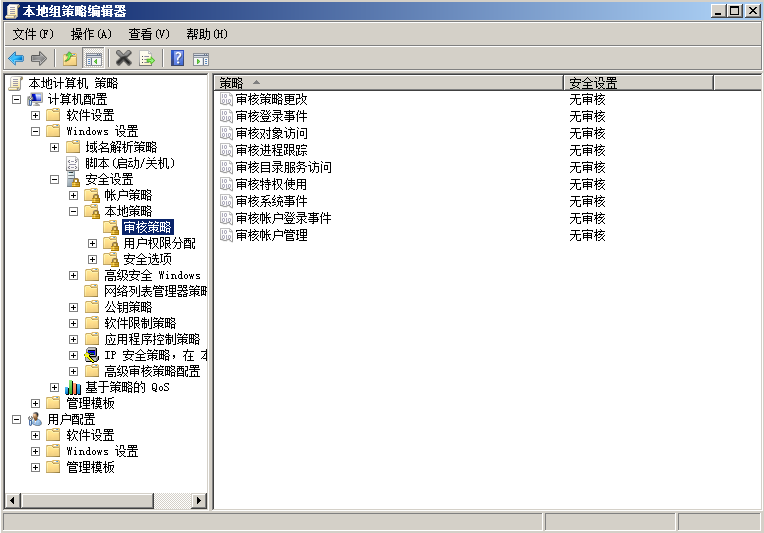


## 禁用不需要的和危险的服务

打开服务器管理器，进入“服务”管理，将下列服务禁用（用黄色标识的服务在2008系统中可能不存在）



## 修改审核策略

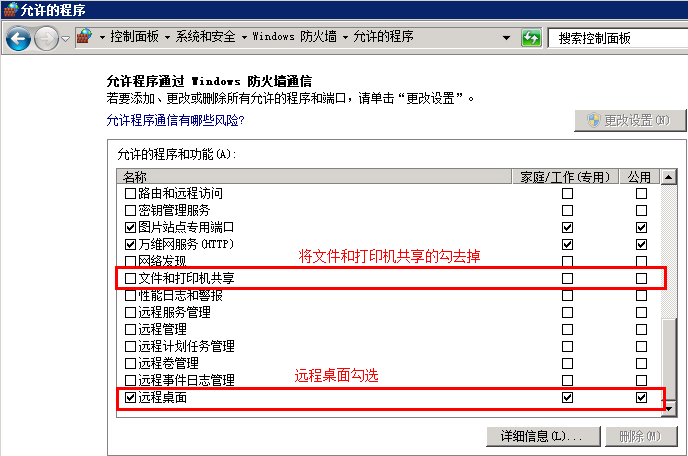


## 系统防火墙安全设置

开启系统防火墙（控制面板=》系统和安全=》Windwos防火墙=》打开或关闭Windows防火墙），如果远程操作的话就要小心，不要将自己的连接也给禁用了



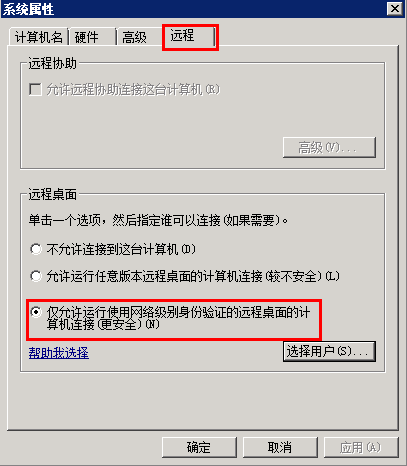
关闭“文件和打印共享”功能



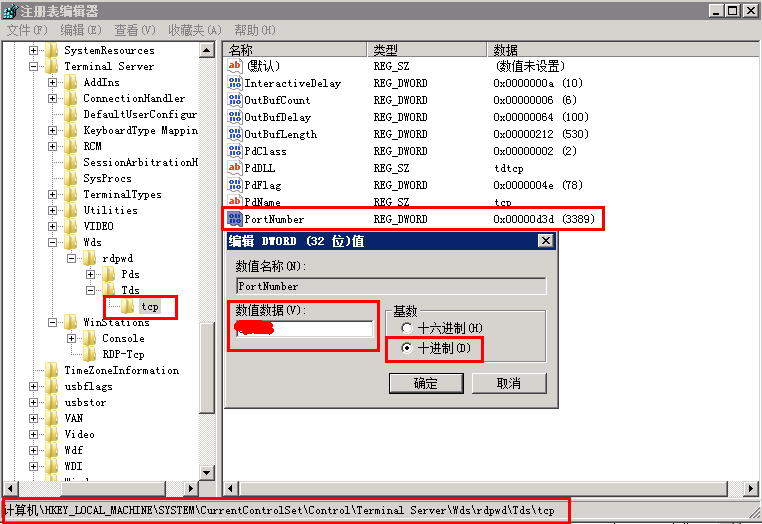
注：如果为了更安全的话，最好是将远程桌面关闭，使用更安全的第三方远程登陆程序。或者修改远程连接端口，一般来说做了前面的设置后，就算留了“肉鸡”在，问题也不是很大。  
添加新的防火墙规则，请参考6.13的相关操作

## 开启远程桌面功能

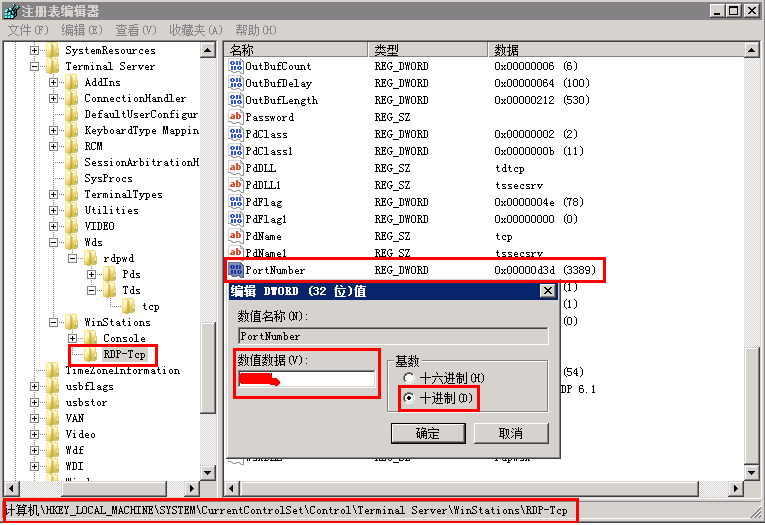
对我的电脑点击左键=》属性，打开系统属性窗口



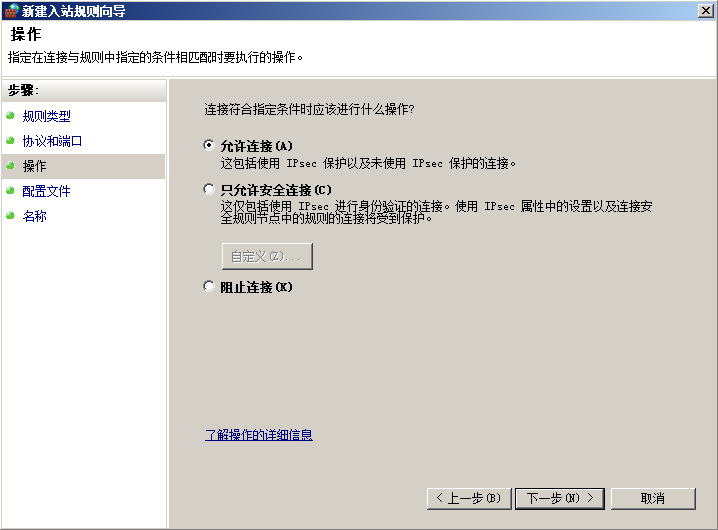
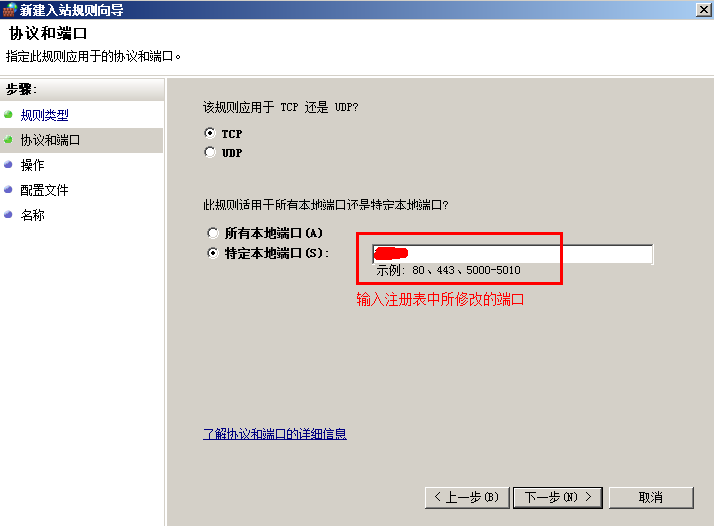
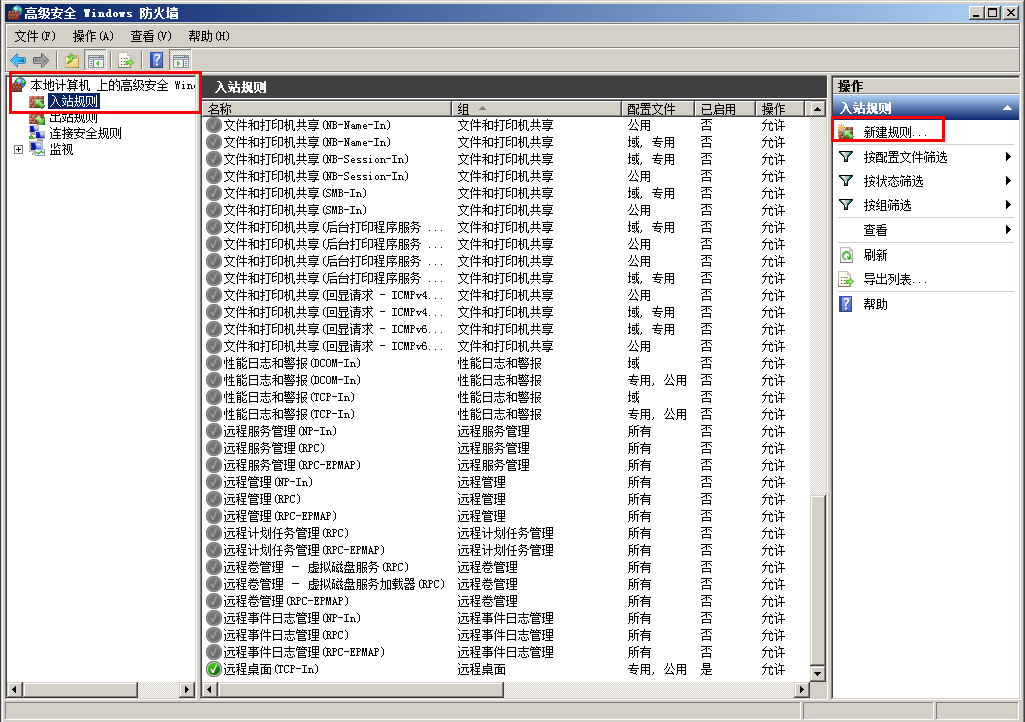
修改远程桌面链接端口  
点击开始菜单，输入regedit打开注册表  
将HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds\rdpwd\Tds\tcp项的PortNumber值由3389修改为比如：12345这些高端端口



将HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp项的PortNumber值由3389修改为12345



修改了远程桌面端口后，原防火墙的远程桌面规则就会失效了，需要重新创建规则  
打开Windows防火墙，点击“高级设置”



设置后重新电脑就马上生效了  
**注：如果是远程修改端口的话，需要同时修改McAfee防火墙，添加新的端口规则，这样才不会出现无法远程登陆的情况**

### 部署注意事项

1、更新前一定要经过自测和测试部门人员测试通过；  
2、修改网站任何配置都必须提前做好备份，方便回档；  
3、修改了服务器端的任何设置都必须提交做好拷屏与记录，方便网站出现任何问题时快速的找出问题；  
4、对服务器端的相关端口进行变动时，必须提前在Windows防火墙和McAfee防火墙提前开通对应的端口，修改好端口重启服务器或软件后，记得关闭原端口，并且做好测试工作，防止发生无法访问的情况，特别对于远程访问端口的修改必须小心，不然可能会造成无法远程登陆的情况；  
5、当发生某功能无法运行或出错的时候，请先检查Windows防火墙、McAfee访问保护和防火墙，看看是否是给访问保护规则阻止了。  
6、必须定期检查用户管理查看是否有多余的用户和用户隶属组是否改变；检查应用程序日志、安全日志、系统日志、IIS访问日志、网站后台管理记录的日志、网站目录中记录的操作日志与充值日志、McAfee访问保日志等，并做好备份工作；查看Windows防火墙、McAfee访问保护和防火墙是否运行中，有没有不小心关闭后忘记开启了；检查SQL的相关日志与记录增长量，检查SQL备份情况，备份空间是否足够等；（具体可查看我下一篇文章《服务器安全检查指引——日常维护说明》）  
7、除了做好服务器安全相关配置外，代码的安全也是非常重要的，所有提交的数据必须做好过滤操作，防SQL注入和XSS攻击，客户端定期杀毒查木马，定期修改登陆密码，以保证系统安全。