

服务器基础安全设置指南

一、密码策略

1、密码复杂性和密码最小长度

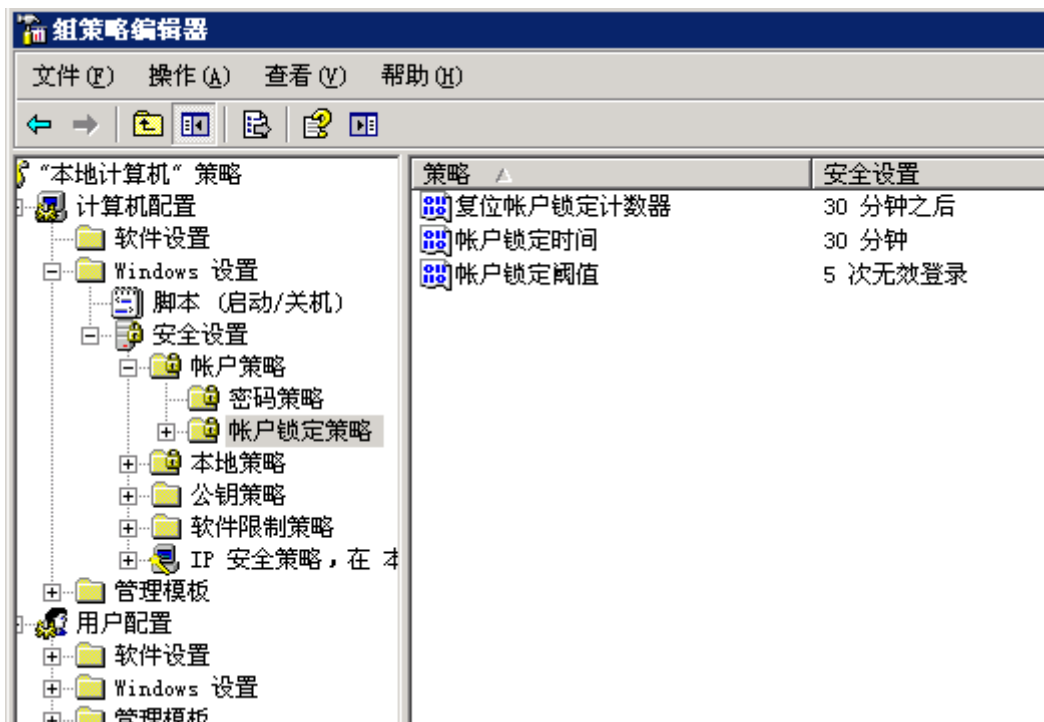
服务器上的密码包括：系统密码 数据库密码 FTP 密码

密码复杂性：所设置密码要包含字母（大写、小写）、数字、符号

密码长度：12 位以上

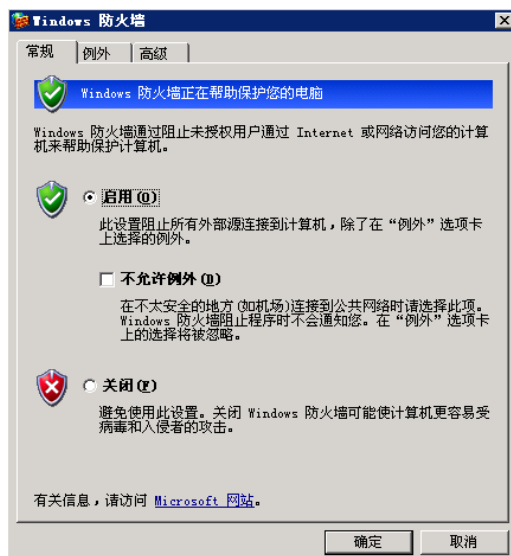
2、账户锁定策略

在开始——运行中输入 gpedit.msc 打开组策略编辑器，在安全设置中将账户锁定阈值设置为 5 次无效登陆或 3 次无效登陆即锁定 30 分钟。

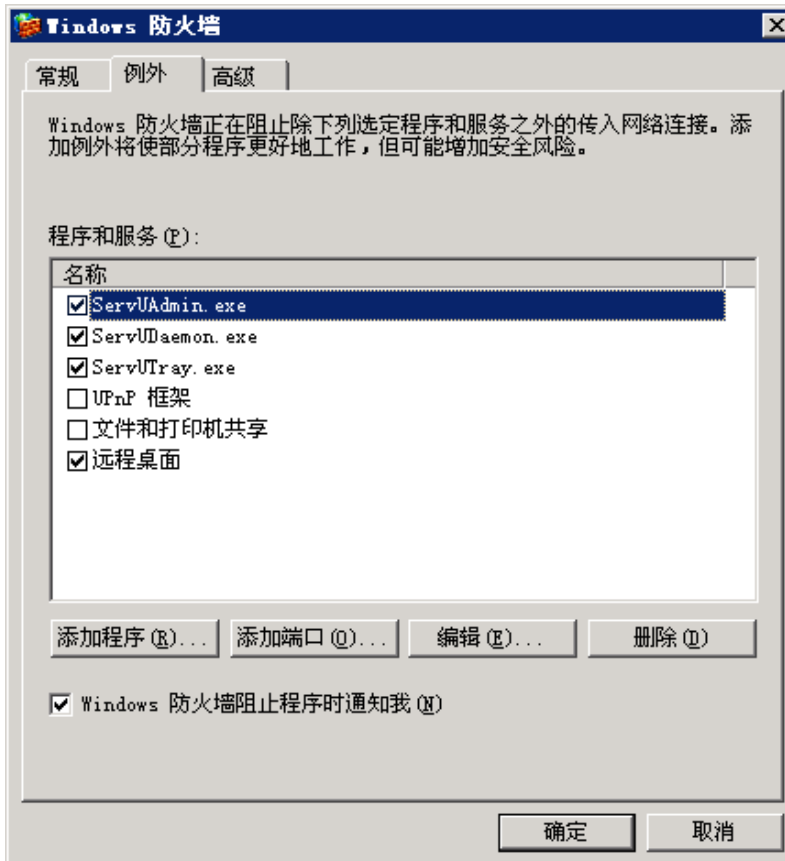


二、windows 防火墙策略

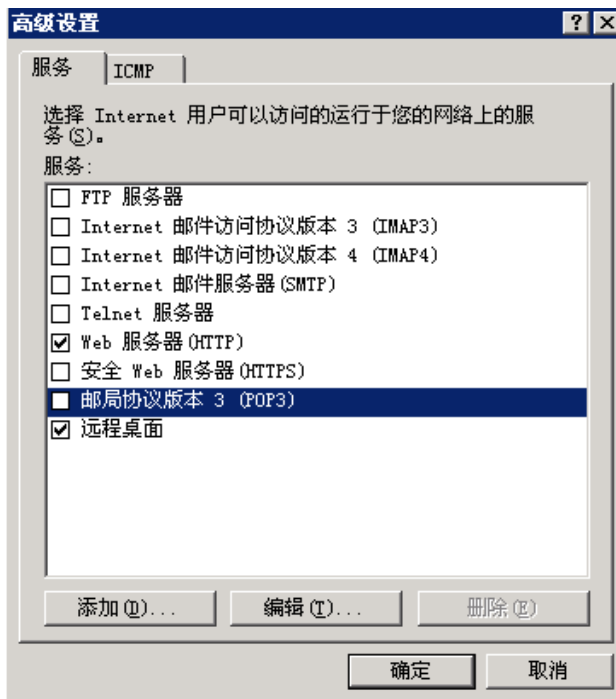
1、开启 windows 防火墙 控制面板——windows 防火墙



2、例外中——放行远程桌面、serv-u 进程



3、高级——本地连接——设置中放行 WEB 服务器 和远程桌面

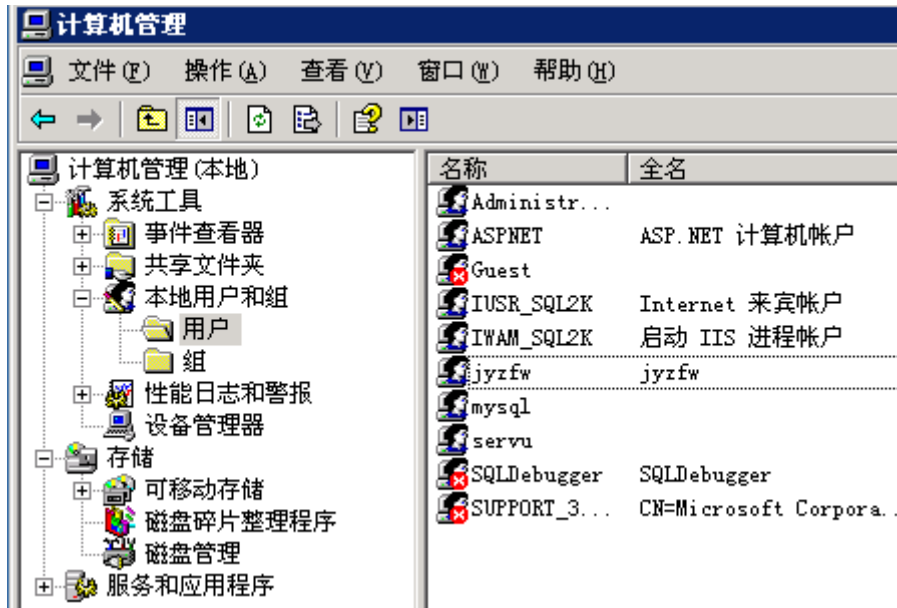


三、权限设置

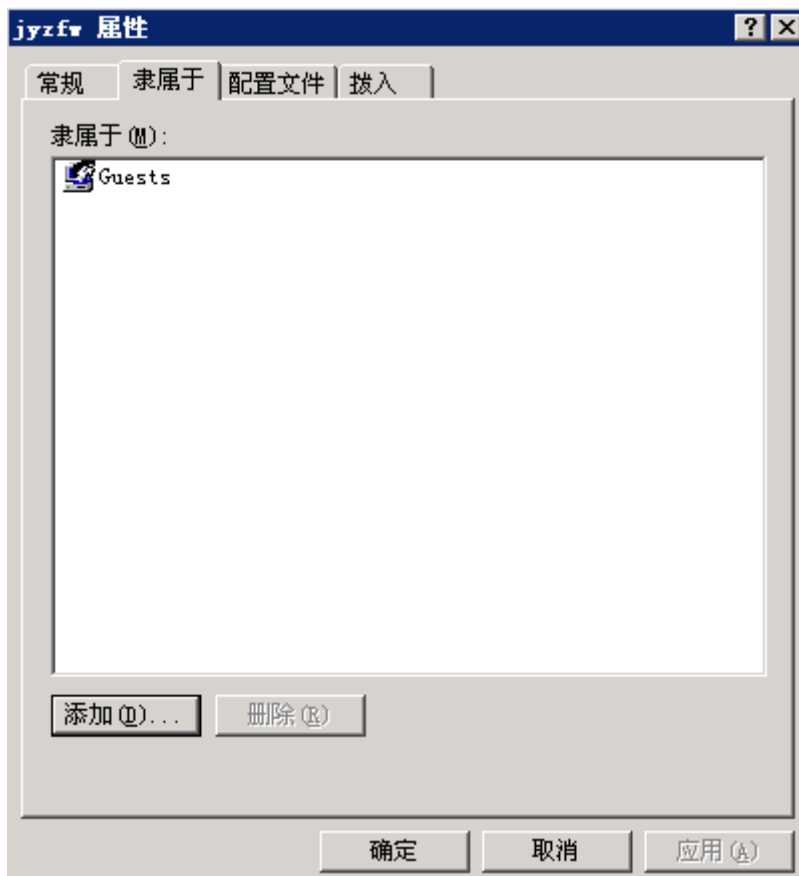
权限设置主要指 IIS 中每一个 WEB 站点都要使用独立的账户运行。

1、首先我的电脑右键——管理——计算机管理——本地用户和组——用户

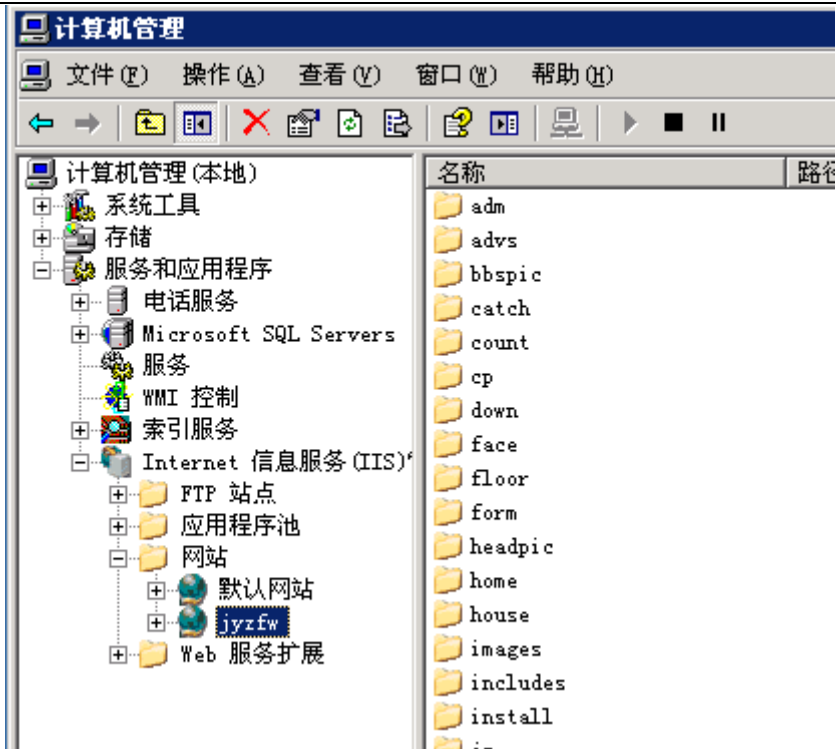
中新建账户



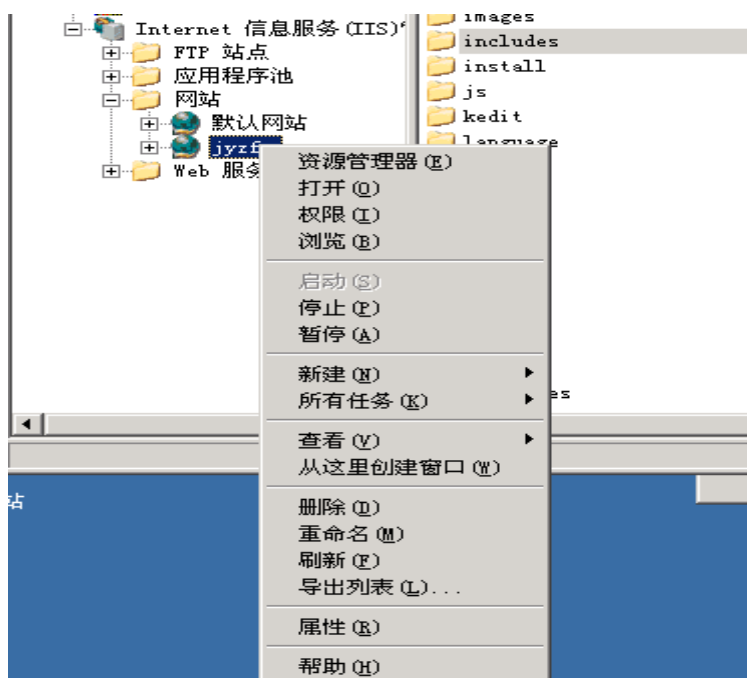
新建账户设置隶属于 GUEST 组

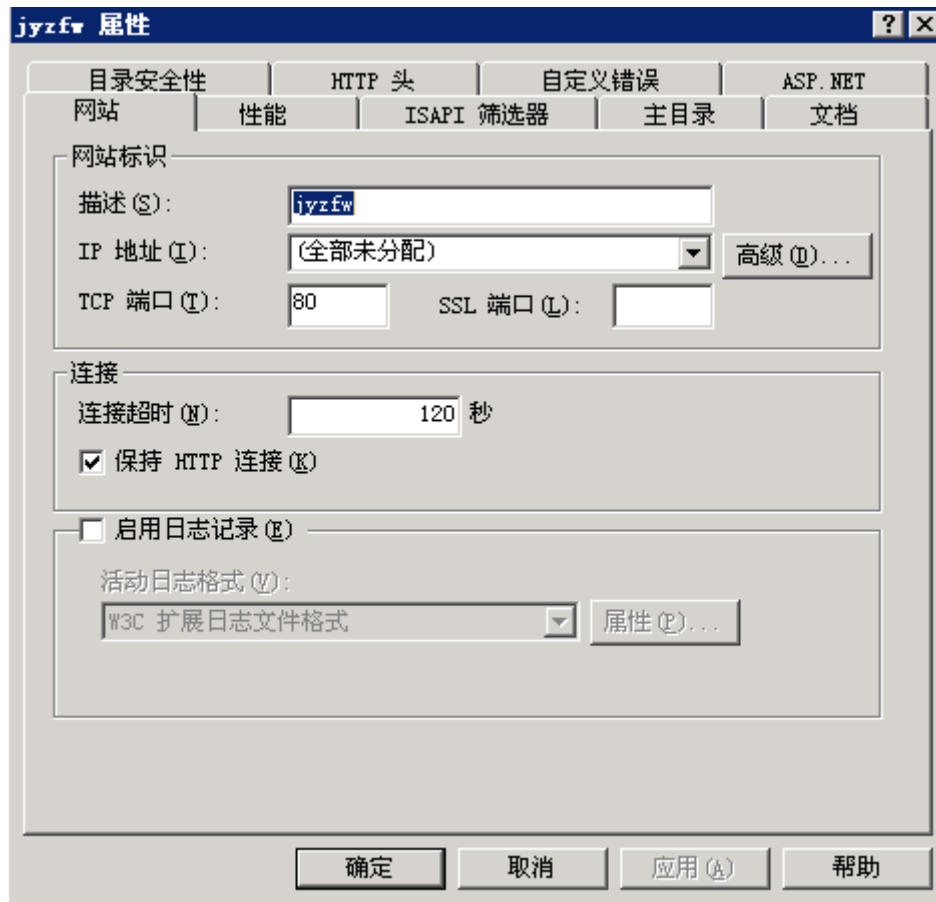


2、在我的电脑右键——管理——计算机管理——服务和应用程序——Internet 信息服务——网站中选择要设置的站点

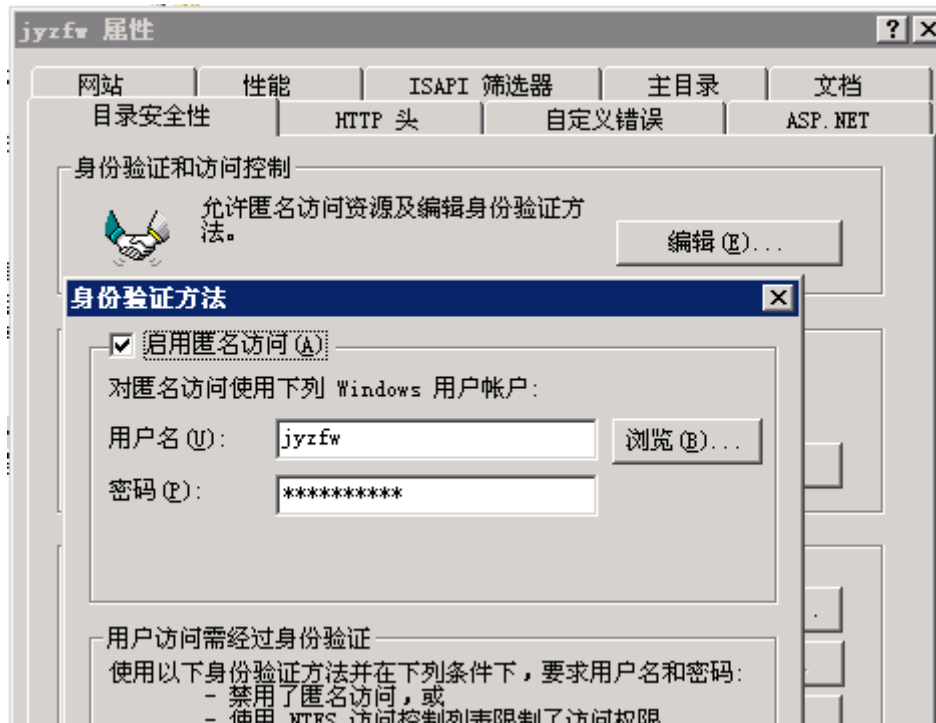


在站点上点击右键进入属性页：



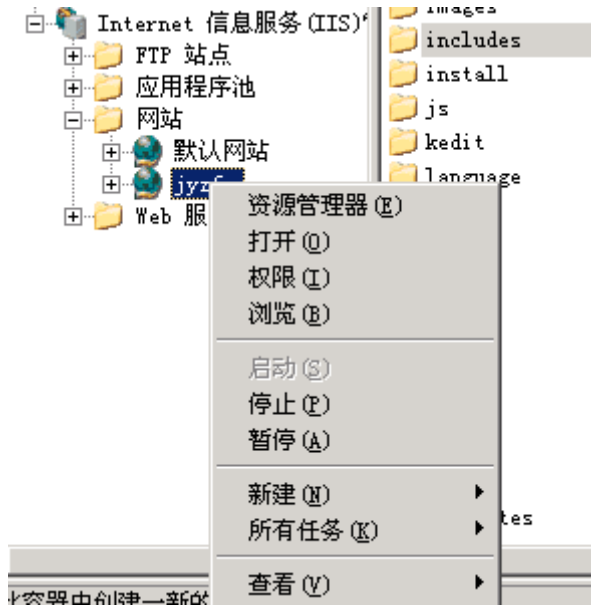


在目录安全性中编辑身份验证和访问控制，将账户设置为刚才建立的账户。

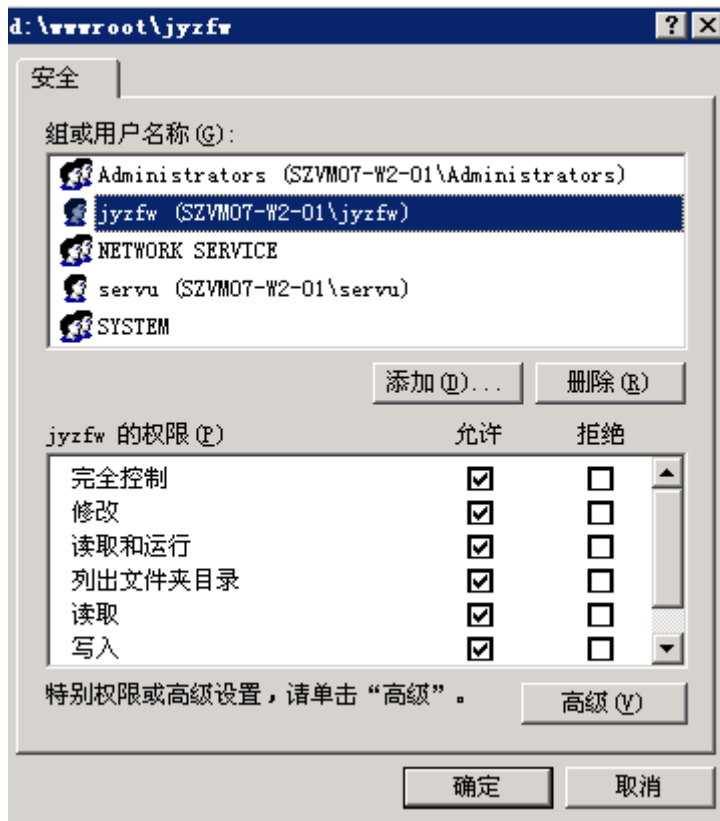


以上设置要确保每一个站点都由一个单独的账户运行，且要保证此账户密码够复杂。

3、在站点属性页——权限中可以设置独立运行账户的权限



如需要读写权限即可在这里设置：



四、网站被上传木马原因、处理建议

有时会收到一些客户反映网站被黑，或被上传木马，当用户访问网站时就会下载病毒或者木马，杀毒软件弹出病毒的提示。这种情况是以下 2 种情况导致的：

第一种情况：客户网站存在文件上传漏洞，导致黑客可以使用这个漏洞，上传黑客文件。然后黑客可以对该用户网站所有文件进行任意修改，这种情况比较普遍。针对这种情况，用户需要找技术人员检查出网站漏洞并彻底修复，并检查网站是否还有黑客隐藏的恶意文件。

原因：很多网站都需要使用到文件上传功能，例如很多网站需要发布产品图片等。文件上传功能本来应该具有严格的限定。例如：只允许用户能上传 JPG，GIF 等图片。但由于程序开发人员考虑不严谨，或者是直接调用一些通用的文件上传组件，导致没对文件上传进行严格的检查。

处理：处理关键是要用户自己知道自己网站哪些地方使用到了文件上传功能。

重点针对这个文件上传功能进行检查，同时针对网站所有文件进行检查，排查可疑信息。同时也利用网站日志，对文件被修改时间进行检查：

1、查到哪个文件被加入代码：用户要查看自己网页代码。根据被加入代码的位置，确定到底是哪个页面被黑，一般黑客会去修改数据库连接文件或网站顶部/底部的文件，因为这样修改后用户网站所有页面都会被附加代码。

2、查到被篡改文件后，使用 FTP 查看文件最后被修改时间，例如 FTP 里面查看到 conn.asp 文件被黑，最后修改时间是 2008-05-16 03: 41 分，那么可以确定在 2008 年 5 月 16 日 03: 41 分这个时间，有黑客使用他留下的黑客后门，篡改了您的 conn.asp 这个文件。

注意：

1、很多用户网站被黑后，只是将被篡改的文件修正过来，或重新上传，这样并没有多大作用。如果网站不修复漏洞，黑客可以很快再次利用这漏洞，对用户网站再次入侵。

2、网站漏洞的检查和修复需要一定的技术人员才能处理。用户需要先做好文件的备份。

第二种情况：用户本地机器中毒了，修改了用户自己本地的网页文件，然后用户自己将这些网页文件上传到服务器空间上。这种情况比较少，如是这种情况用户要先彻底检查自己网站。

1、这种病毒一般是搜索本地磁盘的文件，在网页文件的源代码中插入一段带有病毒的代码，而一般最常见的方式是插入一个 iframe，然后将这个 iframe 的 src 属性指向到一个带有病毒的网址。

2、如何检测这种情况呢？

a、浏览网站，右键查看源代码，在源代码里搜索 iframe，看看有没有被插入了一些不是自己网站的页面，如果有，一般就是恶意代码。

b、也是右键查看源代码，搜索“script”这个关键字，看看有没有被插入一些不是自己域名下的脚本，如果有，并且不是自己放上去的，那很可能也有问题。

3、这种病毒怎么杀呢？

a、有些人会说用杀毒程序查过本地没有发现病毒，这就要看看本地的网站文件是否带有这

些恶意代码，如果有，那基本上可以肯定你的机器是曾经中过毒的，这些病毒可能不是常驻内存的，并且有可能执行一次之后就将自己删除，所以用查毒程序查不出来是很正常的。

b、就算这些病毒是常驻内存，杀毒程序也可能查不出来，因为这种病毒的原理很简单，其实就是执行一下文件磁盘扫描，找到那些网页文件（如：.asp .php .html 等格式的文件），然后打开它插入一段代码，然后再保存一下。因为它修改的不是什么系统文件，病毒防火墙一般不会发出警告，如果它不是挂在一些系统进程里，而是在某个特定的时刻运行一下就退出，这样被查出的可能性更少。

c、手工删除这些病毒的一般方法：

1) 调出任务管理器，看看有没有一些不知名的程序在运行，如果有，用 Windows 的文件查找功能找到这个文件，右键查看属性，如果这个可执行文件的摘要属性没有任何信息，而自己又不知道是什么东西，那很可能有问题，然后上 google 搜索一个这个文件的信息，看看网上的资料显示是不是就是病毒，如果是就先将其改名；

2) 打开注册表编辑器，查看一下

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 有没有一可疑的启动项，有的话就删除；

3) 查看本地机器的 Windows 控制面板，看看“任务计划”那里有没有一些不是自己定义的任务，如果有查看属性，找到这个任务所执行的可执行文件是哪个，重复前面步骤 1) 的方法进行查杀。可能还有其它一些方法，可以在 GOOGLE 上搜索下。

五、服务器中毒常见原因

1、 一般是因为上了一些垃圾网站，这些网站有木马，然后机器就中毒了。

2、 另外就是没有限制 IIS 站点的权限，由于网站上传组件的漏洞而被恶意上传病毒文件、添加后门的批处理文件。

3、 从服务器上下载各种软件，没有在本地对这些软件的安全性进行验证就直接在服务器上安装，从而导致中毒。

4、 在服务器上使用破解软件或软件破解补丁，随意下载网络上的文件都会造成很大的安全隐患，导致服务器中毒。

需要注意事项：

不在服务器上随意访问网站。

不在服务器上随意下载软件。

慎重使用破解软件。

确保上传到服务器上的文件是安全的。

六、新网代码保全服务

代码保全是新网为客户提供的一项代码检查的增值服务。

具体服务内容包括：代码漏洞查找

代码修改

安全设置建议

如您的网站被入侵且自己没有技术能力解决时，可联系新网各地分支机构销售人员购买代码保全服务。