

标准化管理处编码[BBX968T-XBB8968-NNJ668-MM9N]

**服务器主机安全规范**

# **服务器主机安全规范**

## **启用防火墙**

阿里云windows Server 2008 R2默认居然没有启用防火墙。2012可能也是这样的，不过这个一定要检查！

## **补丁更新**

启用windows更新服务，设置为自动更新状态，以便及时打补丁。

阿里云windows Server 2008 R2默认为自动更新状态，2012可能也是这样的，不过这个一定要检查！

## ****账号口令****

### ****优化账号****

|  |  |
| --- | --- |
| 操作目的 | 减少系统无用账号，降低风险 |
| 加固方法 | “Win+R”键调出“运行”->compmgmt.msc（计算机管理）->本地用户和组。  1、删除不用的账号，系统账号所属组是否正确。云服务刚开通时，应该只有一个administrator账号和处于禁用状态的guest账号；  2、确保guest账号是禁用状态  3、买阿里云时，管理员账户名称不要用administrator |
| 备注 |  |

### ****口令策略****

|  |  |
| --- | --- |
| 操作目的 | 增强口令的复杂度及锁定策略等，降低被暴力破解的可能性 |
| 加固方法 | “Win+R”键调出“运行”->secpol.msc （本地安全策略）->安全设置  1、账户策略->密码策略  密码必须符合复杂性要求：启用  密码长度最小值：8个字符  密码最短使用期限：0天  密码最长使用期限：90天  强制密码历史：1个记住密码  用可还原的加密来存储密码：已禁用  2、本地策略->安全选项  交互式登录：不显示最后的用户名：启用 |
| 备注 | “Win+R”键调出“运行”->gpupdate /force立即生效 |

## ****网络服务****

### **优化服务**（1）****

|  |  |
| --- | --- |
| 操作目的 | 关闭不需要的服务，减小风险 |
| 加固方法 | “Win+R”键调出“运行”->services.msc，以下服务改为禁用：  Application Layer Gateway Service（为应用程序级协议插件提供支持并启用网络/协议连接）  Background Intelligent Transfer Service（利用空闲的网络带宽在后台传输文件。如果服务被停用，例如Windows Update和MSN Explorer的功能将无法自动下载程序和其他信息）  Computer Browser（维护网络上计算机的更新列表，并将列表提供给计算机指定浏览）  **DHCP Client**  **Diagnostic Policy Service**  **Distributed Transaction Coordinator**  **DNS Client**  **Distributed Link Tracking Client**  **Remote Registry（**使远程用户能修改此计算机上的注册表设置**）**  **Print Spooler（**管理所有本地和网络打印队列及控制所有打印工作**）**  **Server（不使用文件共享可以关闭，关闭后再右键点某个磁盘选属性，“共享”这个页面就不存在了）**  **Shell Hardware Detection**  **TCP/IP NetBIOS Helper（**提供TCP/IP (NetBT)服务上的NetBIOS和网络上客户端的NetBIOS名称解析的支持，从而使用户能够共享文件、打印和登录到网络**）**  Task Scheduler（使用户能在此计算机上配置和计划自动任务）  **Windows Remote Management**(47001端口，Windows远程管理服务，用于配合IIS管理硬件，一般用不到)  Workstation（创建和维护到远程服务的客户端网络连接。如果服务停止，这些连接将不可用） |
| 备注 | 用服务需谨慎，特别是远程计算机 |

### **优化服务（2）**

* 在"网络连接"里，把不需要的和服务都移除

2 去掉Qos数据包计划程序

2?**关闭Netbios服务（关闭139端口）**

网络连接->本地连接->属性->Internet协议版本 4->属性->高级->WINS->禁用TCP/IP上的NetBIOS。

说明：关闭此功能，你服务器上所有共享服务功能都将关闭，别人在资源管理器中将看不到你的共享资源。这样也防止了信息的泄露。

2 Microsoft网络的文件和打印机共享

网络连接->本地连接->属性，把除了“Internet协议版本 4”以外的东西都勾掉。

2 ipv6协议

先关闭网络连接->本地连接->属性->Internet协议版本 6 (TCP/IPv6)

然后再修改注册表：HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters，增加一个Dword项，名字：DisabledComponents，值：ffffffff（十六位的8个f）

重启服务器即可关闭ipv6

2 microsoft网络客户端（主要是为了访问微软的网站）

* 关闭445端口

445端口是netbios用来在局域网内解析机器名的服务端口，一般服务器不需要对LAN开放什么共享，所以可以关闭。

修改注册表：HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters，则更加一个Dword项：SMBDeviceEnabled，值：0

* 关闭LLMNR（关闭5355端口）

什么是LLMNR？本地链路多播名称解析，也叫多播DNS，用于解析本地网段上的名称，没啥用但还占着5355端口。

使用组策略关闭，运行->gpedit.msc->计算机配置->管理模板->网络->DNS客户端->关闭多播名称解析->启用

### ****网络限制****

|  |  |
| --- | --- |
| 操作目的 | **网络访问限制** |
| 加固方法 | “Win+R”键调出“运行”->secpol.msc ->安全设置->本地策略->安全选项  网络访问: 不允许 SAM 帐户的匿名枚举：已启用  网络访问: 不允许 SAM 帐户和共享的匿名枚举：已启用  网络访问: 将 Everyone权限应用于匿名用户：已禁用  帐户: 使用空密码的本地帐户只允许进行控制台登录：已启用 |
| 备注 | “Win+R”键调出“运行”->gpupdate /force立即生效 |

## **远程访问**

### **一定要使用高强度密码**

### **更改远程终端默认端口号**

步骤：

1.防火墙中设置

1.控制面板——windows防火墙——高级设置——入站规则——新建规则——端口——特定端口tcp（如13688）——允许连接 2.完成以上操作之后右击该条规则作用域——本地ip地址——任何ip地址——远程ip地址——下列ip地址—— 添加管理者ip 同理其它端口可以通过此功能对特定网段屏蔽（如80端口）。

请注意：不是专线的网络的IP地址经常变，不适合限定IP。

2.运行regedit 2.[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\Wds \rdpwd\Tds \tcp] 和 [HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\TerminalServer\WinStations\RDP-TCP]，看见PortNamber值了吗？其默认值是3389，修改成所希望的端口即可，例如13688

3.[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentContro1Set\Control\Tenninal Server\WinStations\ RDP\Tcp]，将PortNumber的值（默认是3389）修改成端口13688（自定义）。

4.重新启动电脑，以后远程登录的时候使用端口13688就可以了。

## **文件系统**

### ****检查Everyone权限****

|  |  |
| --- | --- |
| **操作目的** | **增强Everyone权限** |
| **加固方法** | 鼠标右键系统驱动器（磁盘）->“属性”->“安全”，查看每个系统驱动器根目录是否设置为Everyone有所有权限  删除Everyone的权限或者取消Everyone的写权限 |
| **备注** |  |

### **NTFS权限设置**

注意：

1、2008 R2默认的文件夹和文件所有者为TrustedInstaller，这个用户同时拥有所有控制权限。 2、注册表同的项也是这样，所有者为TrustedInstaller。 3、如果要修改文件权限时应该先设置 管理员组 administrators 为所有者，再设置其它权限。 4、如果要删除或改名注册表，同样也需先设置 管理员组 为所有者，同时还要应该到子项，直接删除当前项还是删除不掉时可以先删除子项后再删除此项。

步骤：

1. C盘只给administrators 和system权限，其他的权限不给，其他的盘也可以这样设置（web目录权限依具体情况而定）
2. 这里给的system权限也不一定需要给，只是由于某些第三方应用程序是以服务形式启动的，需要加上这个用户，否则造成启动不了。
3. Windows目录要加上给users的默认权限，否则ASP和ASPX等应用程序就无法运行（如果你使用IIS的话，要引用windows下的dll文件）。
4. c:/user/ 只给administrators 和system权限

## **日志和授权**

### ****增强日志****

|  |  |
| --- | --- |
| **操作目的** | **增大日志量大小，避免由于日志文件容量过小导致日志记录不全** |
| **加固方法** | “Win+R”键调出“运行”->eventvwr.msc ->“windows日志”->查看“应用程序”“安全”“系统”的属性  建议设置：  日志上限大小：20480 KB  Windows server 2008 R2默认就是这样设置的 |
| **备注** |  |

### **增强审核**

|  |  |
| --- | --- |
| **操作目的** | **对系统事件进行审核，在日后出现故障时用于排查故障** |
| **加固方法** | “Win+R”键调出“运行”->secpol.msc ->安全设置->本地策略->审核策略  建议设置：  审核策略更改：成功  审核登录事件：成功，失败  审核对象访问：成功  审核进程跟踪：成功，失败  审核目录服务访问：成功，失败  审核系统事件：成功，失败  审核帐户登录事件：成功，失败  审核帐户管理：成功，失败 |
| **备注** | “Win+R”键调出“运行”->gpupdate /force立即生效 |

### **授权**

进入“控制面板->管理工具->本地安全策略”，在“本地策略->用户权利指派”:

把“关闭系统”设置为“只指派给Administrators组”

把“从远端系统强制关机”设置为“只指派Administrators组”

设置“取得文件或其它对象的所有权”设置为“只指派给Administrators组

## **攻击保护**

### **关闭ICMP**

也就是平时说的PING，让别人PING不到服务器，减少不必要的软件扫描麻烦。

在服务器的控制面板中打开?**windows防火墙**， 点击**高级设置**：

点击?**入站规则**——找到**文件和打印机共享(回显请求 - ICMPv4-In)**，启用此规则即是开启ping，禁用此规则IP将禁止其他客户端ping通，但不影响TCP、UDP等连接。

# **应用服务安全**

## **IIS**

### **web.config配置不能返回详细的应用异常**

<customErrors>标记的“mode”属性不能设置为“Off”，这样用户能看到异常详情。

### **在IIS角色服务中去掉目录浏览、 ASP、CGI、在服务器端包含文件**

IIS用户

匿名身份验证不能使用管理员账号，得使用普通用户账号。