ALIBABA CLOUD

阿里云

阿里云安全产品和技术
安全部署指南

文档版本：20220601

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.操作系统安全加固

1.1. Windows操作系统安全加固

本文档旨在指导系统管理人员或安全检查人员进行Windows操作系统的安全合规性检查和配置。

1.1账户

默认账户安全

- 禁用Guest账户。
- 禁用或删除其他无用账户（建议先禁用账户三个月，待确认没有问题后删除）。

操作步骤

打开**控制面板>管理工具>计算机管理**，在**系统工具>本地用户和组>用户**中，双击**Guest**账户，在属性中选中**账户已禁用**，单击**确定**。

按照用户分配账户

按照用户分配账户。根据业务要求，设定不同的用户和用户组。例如，管理员用户，数据库用户，审计用户，来宾用户等。

操作步骤

打开**控制面板>管理工具>计算机管理**，在**系统工具>本地用户和组**中，根据您的业务要求设定不同的用户和用户组，包括管理员用户、数据库用户、审计用户、来宾用户等。

定期检查并删除与无关账户

定期删除或锁定与设备运行、维护等与工作无关的账户。

操作步骤

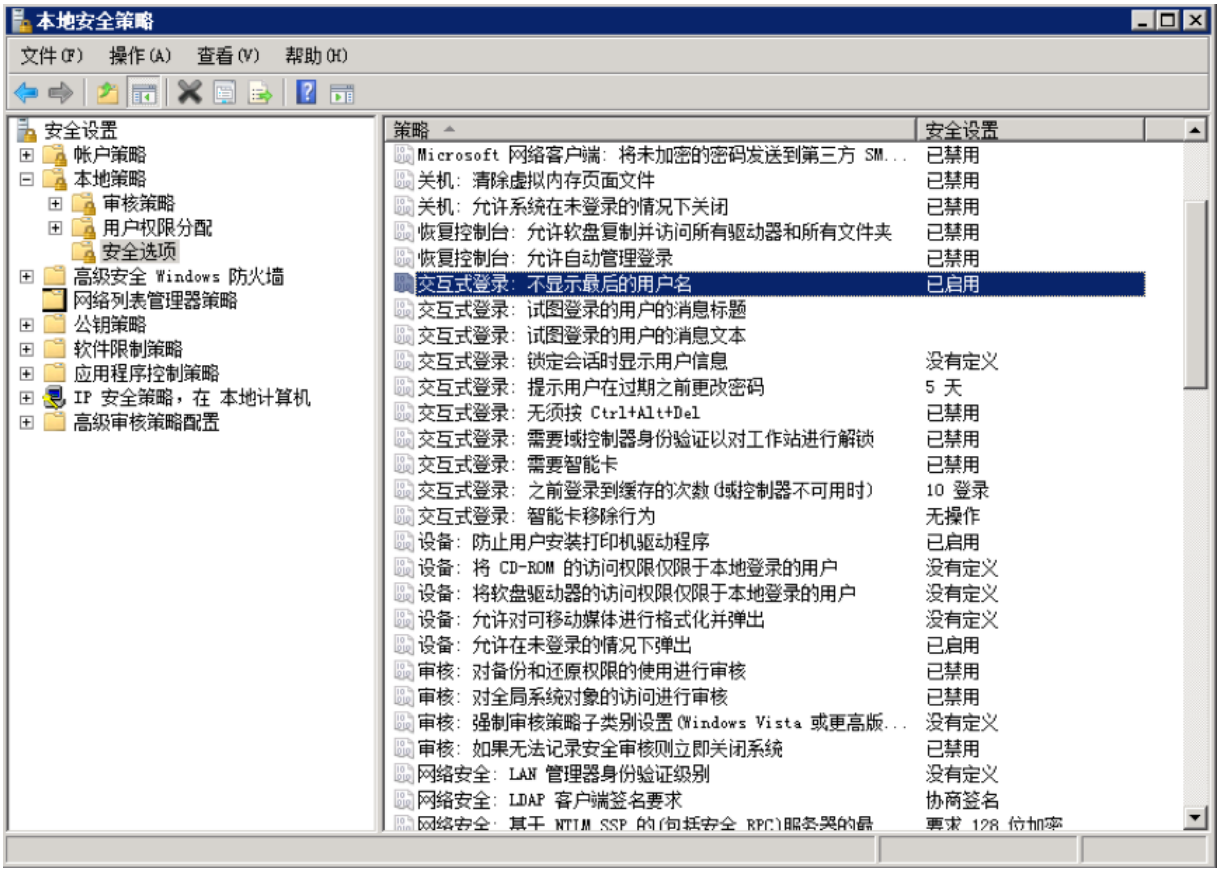
打开**控制面板>管理工具>计算机管理**，在**系统工具>本地用户和组**中，删除或锁定与设备运行、维护等与工作无关的账户。

不显示最后的用户名

配置登录登出后，不显示用户名称。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>安全选项**中，双击**交互式登录:不显示最后的用户名**，选择**已启用**并单击**确定**。



1.2口令

密码复杂度

密码复杂度要求必须满足以下策略：

- 最短密码长度要求八个字符。
- 启用本机组策略中密码必须符合复杂性要求的策略。即密码至少包含以下四种类别的字符中的两种：
  - 英语大写字母A,B,C,...Z
  - 英语小写字母a,b,c,...z
  - 西方阿拉伯数字0,1,2,...9
  - 非字母数字字符，如标点符号，@,#,$,%,&,*等

操作步骤

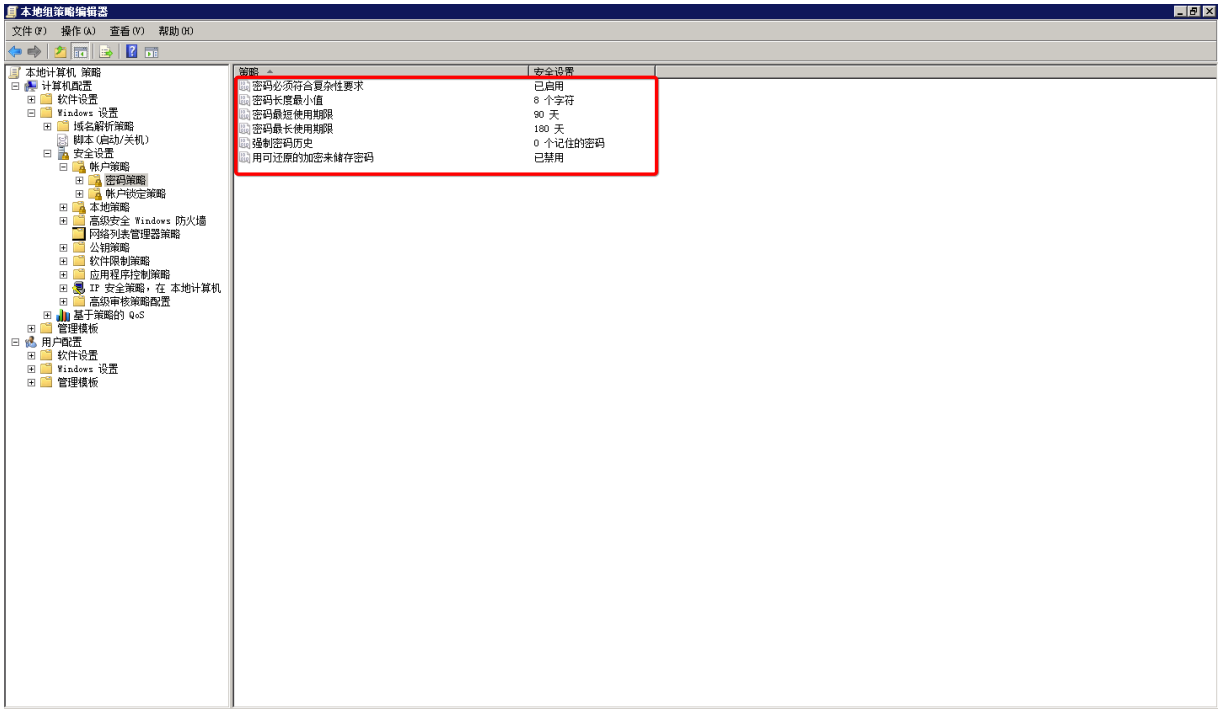
打开**控制面板>管理工具>本地安全策略**，在**账户策略>密码策略**中，确认**密码必须符合复杂性要求**策略已启用。

密码最长留存期

对于采用静态口令认证技术的设备，账户口令的留存期不应长于90天。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**账户策略>密码策略**中，配置**密码最长使用期限**不大于90天。



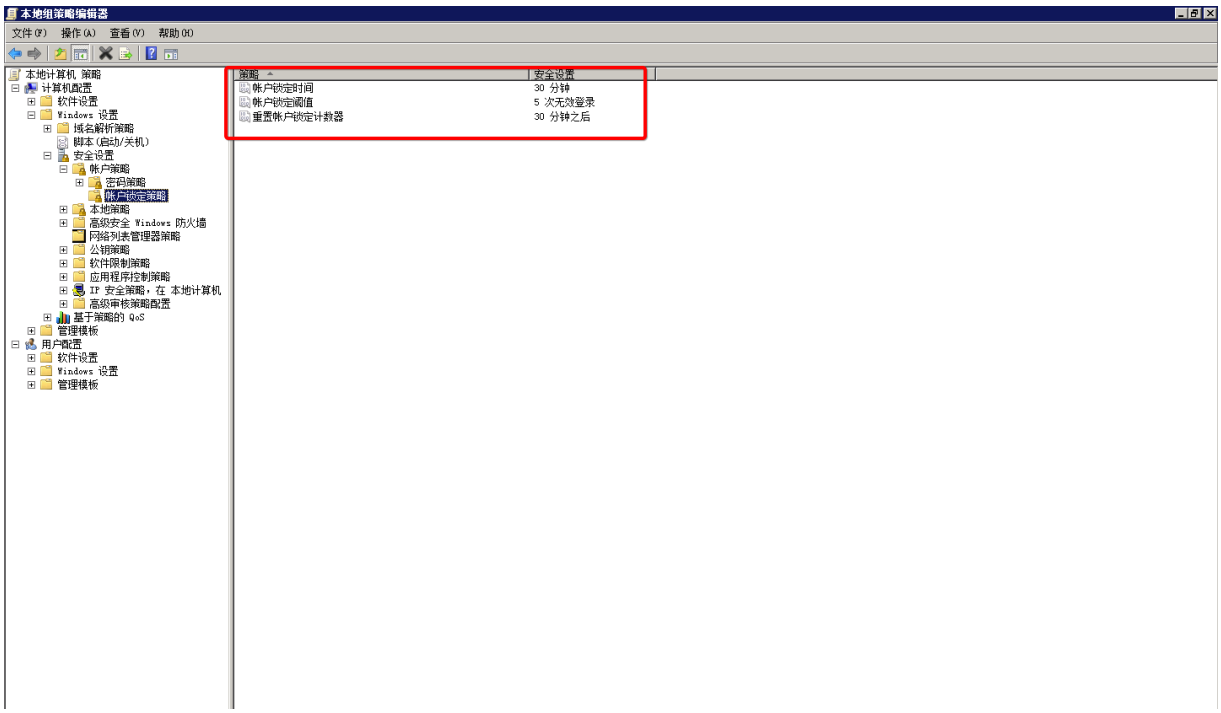
账户锁定策略

对于采用静态口令认证技术的设备，应配置当用户连续认证失败次数超过10次后，锁定该用户使用的账户。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**账户策略>账户锁定策略**中，配置**账户锁定阈值**不大于10次。

配置样例：



1.3授权

远程关机

在本地安全设置中，从远端系统强制关机权限只分配给Administrators组。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>用户权限分配**中，配置**从远端系统强制关机**权限只分配给Administrators组。

本地关机

在本地安全设置中关闭系统权限只分配给Administrators组。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>用户权限分配**中，配置**关闭系统**权限只分配给Administrators组。

用户权限指派

在本地安全设置中，取得文件或其它对象的所有权权限只分配给Administrators组。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>用户权限分配**中，配置**取得文件或其它对象的所有权**权限只分配给Administrators组。

授权账户登录

在本地安全设置中，配置指定授权用户允许本地登录此计算机。

操作步骤

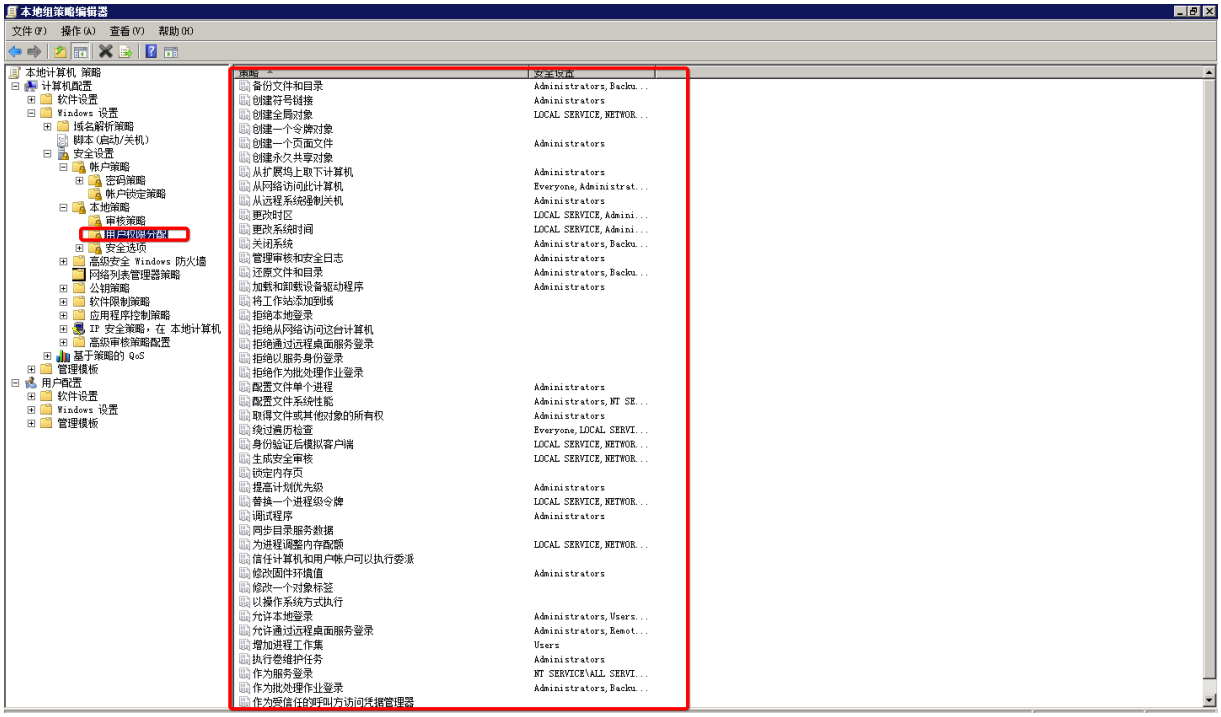
打开**控制面板>管理工具>本地安全策略**，在**本地策略>用户权限分配**中，配置**允许本地登录**权限给指定授权用户。

授权账户从网络访问

在本地安全设置中，只允许授权账号从网络访问（包括网络共享等，但不包括终端服务）此计算机。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>用户权限分配**中，配置**从网络访问此计算机**权限给指定授权用户。



2.日志配置操作

2.1日志配置

审核登录

设备应配置日志功能，对用户登录进行记录。记录内容包括用户登录使用的账户、登录是否成功、登录时间、以及远程登录时、及用户使用的IP地址。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>审核策略**中，设置**审核登录事件**。

审核策略

启用本地安全策略中对Windows系统的审核策略更改，成功和失败操作都需要审核。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>审核策略**中，设置**审核策略更改**。

审核对象访问

启用本地安全策略中对Windows系统的审核对象访问，成功和失败操作都需要审核。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>审核策略**中，设置**审核对象访问**。

审核事件目录服务访问

启用本地安全策略中对Windows系统的审核目录服务访问，仅需要审核失败操作。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>审核策略**中，设置**审核目录服务器访问**。

审核特权使用

启用本地安全策略中对Windows系统的审核特权使用，成功和失败操作都需要审核。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>审核策略**中，设置**审核特权使用**。

审核系统事件

启用本地安全策略中对Windows系统的审核系统事件，成功和失败操作都需要审核。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>审核策略**中，设置**审核系统事件**。

审核账户管理

启用本地安全策略中对Windows系统的审核账户管理，成功和失败操作都要审核。

操作步骤

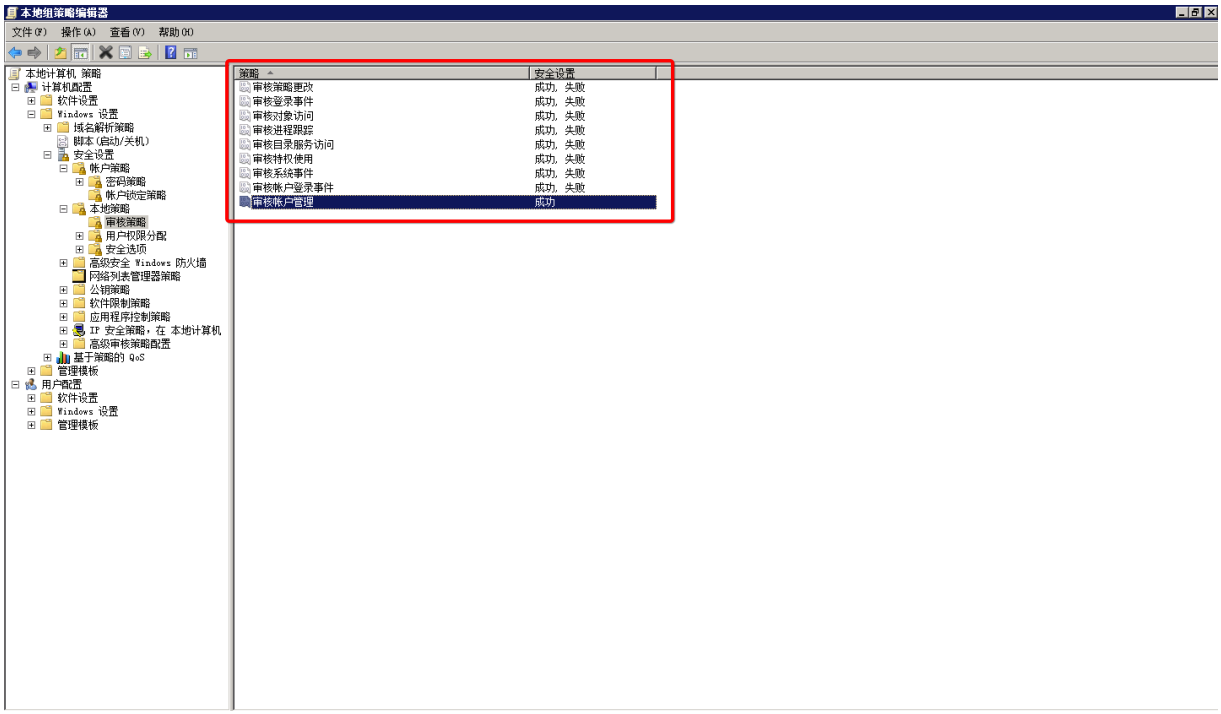
打开**控制面板>管理工具>本地安全策略**，在**本地策略>审核策略**中，设置**审核账户管理**。

审核过程追踪

启用本地安全策略中对Windows系统的审核进程追踪，仅失败操作需要审核。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>审核策略**中，设置**审核进程追踪**。

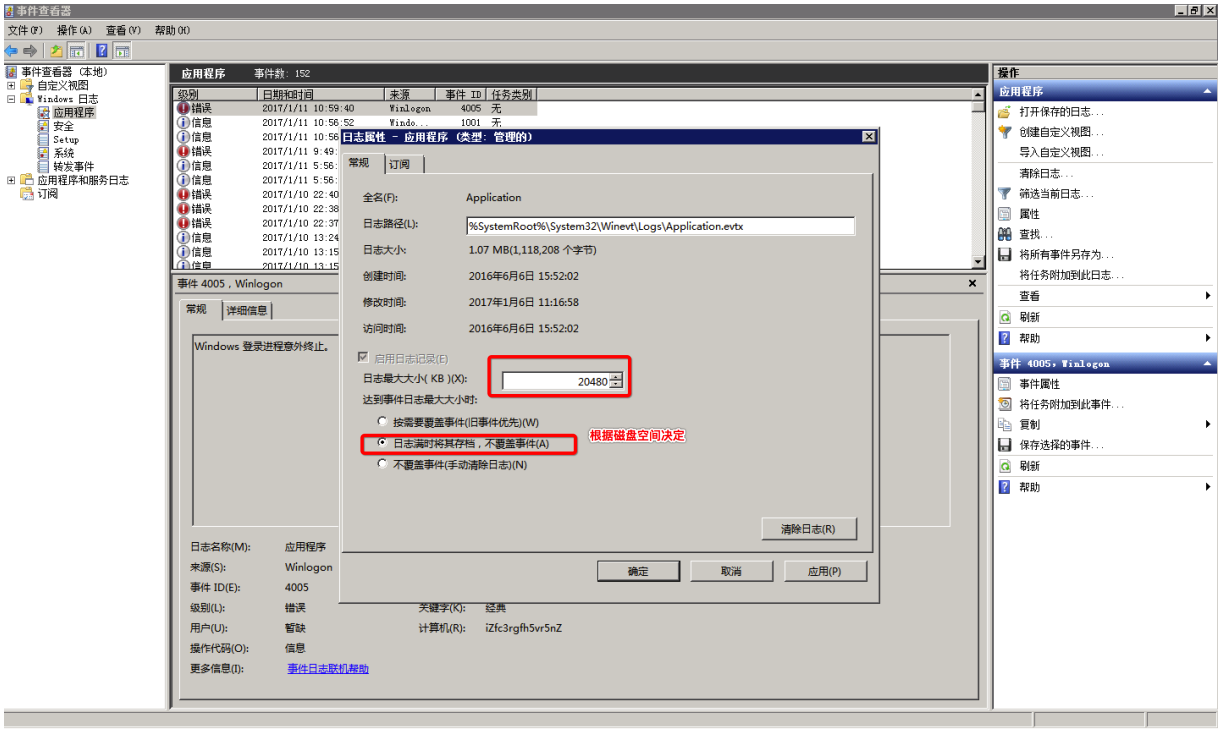


日志文件大小

设置应用日志文件大小至少为8192 KB，可根据磁盘空间配置日志文件大小，记录的日志越多越好。并设置当达到最大的日志尺寸时，按需要轮询记录日志。

操作步骤

打开**控制面板>管理工具>事件查看器**，配置应用日志、系统日志、安全日志属性中的日志大小，以及设置当达到最大的日志尺寸时的相应策略。



3.IP协议安全配置

3.1IP协议安全

启用SYN攻击保护

启用SYN攻击保护。

- 指定触发SYN洪水攻击保护所必须超过的TCP连接请求数阈值为5。
- 指定处于SYN_RCVD状态的TCP连接数的阈值为500。
- 指定处于至少已发送一次重传的SYN_RCVD状态中的TCP连接数的阈值为400。

操作步骤

打开**注册表编辑器**，根据推荐值修改注册表键值。

Windows Server 2012

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect` 推荐值：2
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxHalfOpen` 推荐值：500

Windows Server 2008

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SynAttackProtect` 推荐值：2
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxPortsExhausted` 推荐值：5

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpen` 推荐值：500
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpenRetried` 推荐值：400

4.文件权限

4.1共享文件夹及访问权限

关闭默认共享

非域环境中，关闭Windows硬盘默认共享，例如C，D。

操作步骤

打开**注册表编辑器**，根据推荐值修改注册表键值。

> 注意
>
> Windows Server 2012版本已默认关闭Windows硬盘默认共享，且没有该注册表键值。

`HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer` 推荐值：0

共享文件夹授权访问

每个共享文件夹的共享权限，只允许授权的账户拥有共享此文件夹的权限。

操作步骤

每个共享文件夹的共享权限仅限于业务需要，不要设置成为**Everyone**。打开**控制面板>管理工具>计算机管理**，在**共享文件夹**中，查看每个共享文件夹的共享权限。

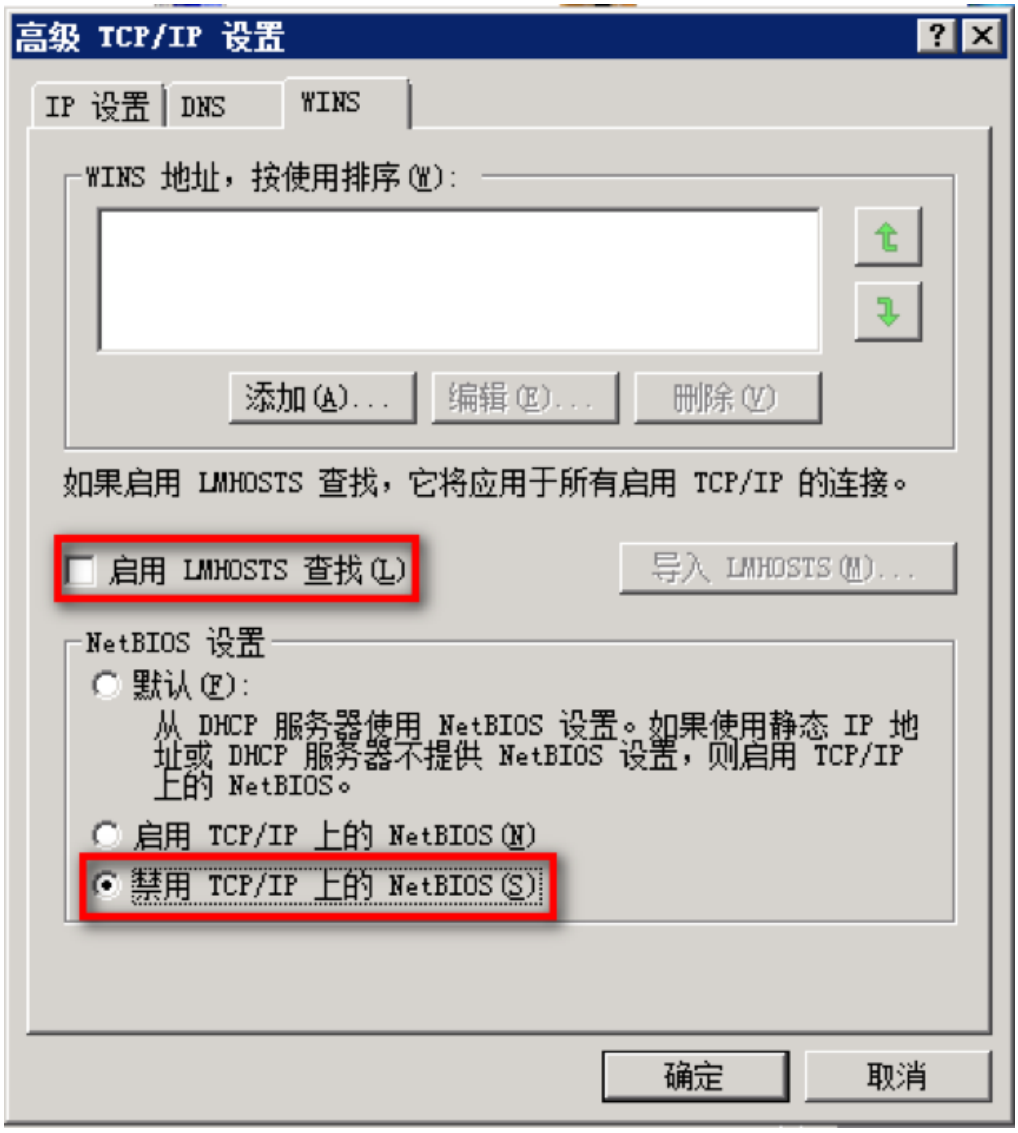
5.服务安全

5.1禁用TCP/IP上的NetBIOS

禁用TCP/IP上的NetBIOS协议，可以关闭监听的UDP 137（netbios-ns）、UDP 138（netbios-dgm）以及TCP 139（netbios-ssn）端口。

操作步骤

1. 在**计算机管理>服务和应用程序>服务**中禁用TCP/IP NetBIOS Helper服务。
2. 在网络连接属性中，双击**Internet协议版本4（TCP/IPv4）**，单击**高级**。在**WINS**页签中，进行如下设置：



禁用不必要的服务

禁用不必要的服务，请参考：

服务名称	建议
DHCP Client	如果不使用动态IP地址，就禁用该服务
Background Intelligent Transfer Service	如果不启用自动更新，就禁用该服务
Computer Browser	禁用
Diagnostic Policy Service	手动
IP Helper	禁用。该服务用于转换IPv6 to IPv4
Print Spooler	如果不需要打印，就禁用该服务
Remote Registry	禁用。Remote Registry主要用于远程管理注册表
Server	如果不使用文件共享，就禁用该服务。禁用本服务将关闭默认共享，如ipc$、admin$和c$等
TCP/IP NetBIOS Helper	禁用
Windows Remote Management (WS-Management)	禁用
Windows Font Cache Service	禁用
WinHTTP Web Proxy Auto-Discovery Service	禁用
Windows Error Reporting Service	禁用

6.安全选项

6.1启用安全选项

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>安全选项**中，进行如下设置：

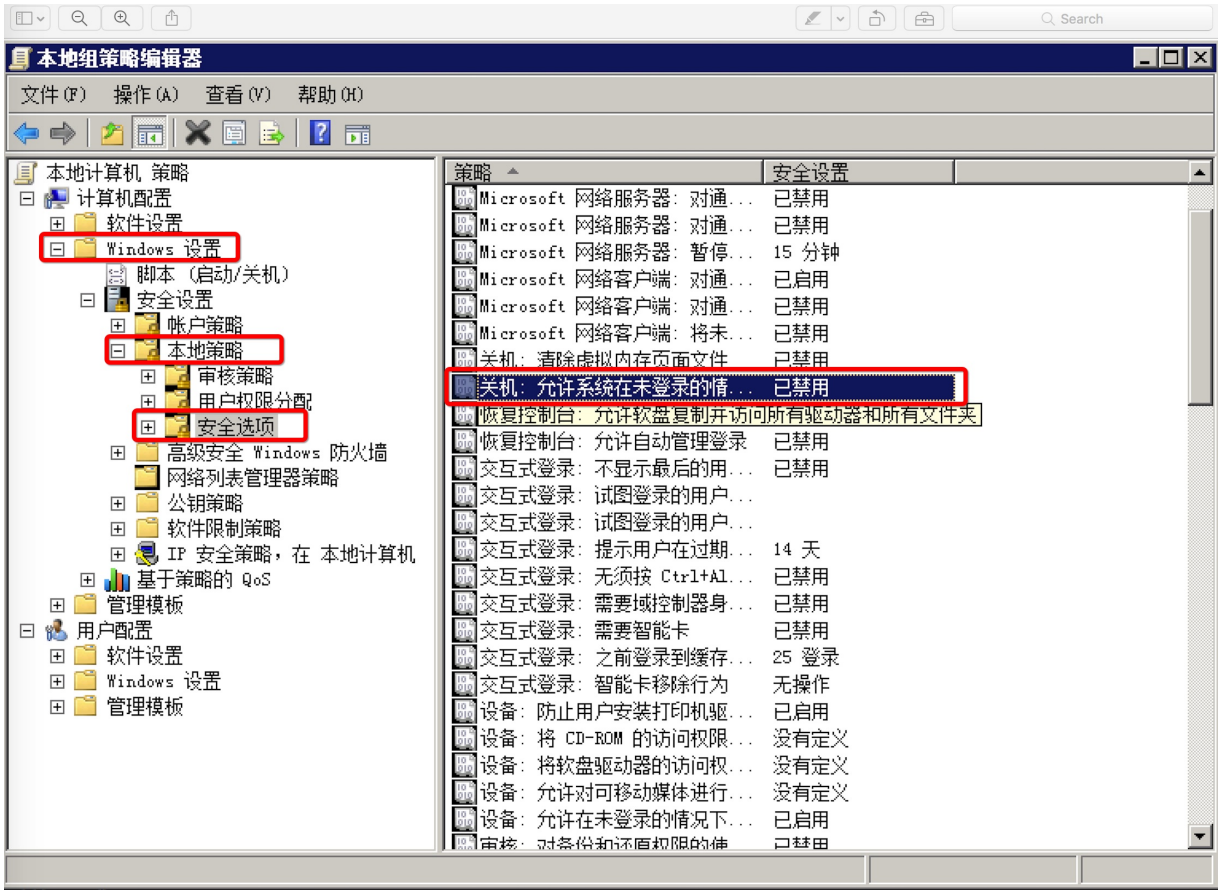
安全选项	配置内容
交互式登录: 试图登录的用户的消息标题	注意
交互式登录: 试图登录的用户的消息文本	内部系统只能因业务需要而使用，经由管理层授权。 管理层将随时监测此系统的使用。
Microsoft 网络服务器: 对通信进行数字签名(如果客户端允许)	启用
Microsoft 网络服务器: 对通信进行数字签名(始终)	启用
Microsoft 网络客户端: 对通信进行数字签名(如果服务器允许)	启用
Microsoft 网络客户端: 对通信进行数字签名(始终)	启用
网络安全: 基于 NTLM SSP 的(包括安全 RPC)服务器的最小会话安全	要求 NTLMv2 会话安全 要求 128 位加密
网络安全: 基于 NTLM SSP 的(包括安全 RPC)客户端的最小会话安全	要求 NTLMv2 会话安全 要求 128 位加密
网络安全: LAN 管理器身份验证级别	仅发送 NTLMv2 响应\拒绝 LM & NTLM
网络访问: 不允许 SAM 帐户的匿名枚举	启用（默认已启用）
网络访问: 不允许 SAM 帐户和共享的匿名枚举	启用
网络访问 : 可匿名访问的共享	清空（默认为空）
网络访问 : 可匿名访问的命名管道	清空（默认为空）
网络访问: 可远程访问的注册表路径	清空，不允许远程访问注册表
网络访问: 可远程访问的注册表路径和子路径	清空，不允许远程访问注册表

6.2禁用未登录前关机

服务器默认是禁止在未登录系统前关机的。如果启用此设置，服务器安全性将会大大降低，给远程连接的黑客造成可乘之机，强烈建议禁用未登录前关机功能。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>安全选项**中，禁用**关机:允许系统在未登录前关机**策略。



7.其他安全配置

7.1防病毒管理

Windows系统需要安装防病毒软件。

操作步骤

安装企业级防病毒软件，并开启病毒库更新及实时防御功能。

7.2设置屏幕保护密码和开启时间

设置从屏幕保护恢复时需要输入密码，并将屏幕保护自动开启时间设定为五分钟。

操作步骤

启用屏幕保护程序，设置等待时间为**5分钟**，并启用**在恢复时使用密码保护**。

7.3限制远程登录空闲断开时间

对于远程登录的账户，设置不活动超过时间15分钟自动断开连接。

操作步骤

打开**控制面板>管理工具>本地安全策略**，在**本地策略>安全选项**中，设置**Microsoft网络服务器：暂停会话前所需的空闲时间数量**属性为15分钟。

7.4操作系统补丁管理

安装最新的操作系统Hotfix补丁。安装补丁时，应先对服务器系统进行兼容性测试。

操作步骤

安装最新的操作系统Hotfix补丁。安装补丁时，应先对服务器系统进行兼容性测试。

> 注意
>
> 对于实际业务环境服务器，建议使用通知并自动下载更新，但由管理员选择是否安装更新，而不是使用自动安装更新，防止自动更新补丁对实际业务环境产生影响。

1.2. Linux操作系统加固

本帮助手册旨在指导系统管理人员或安全检查人员进行Linux操作系统的安全合规性检查和加固。

1. 账号和口令

1.1 禁用或删除无用账号

减少系统无用账号，降低安全风险。

操作步骤

- 使用命令 `userdel <用户名>` 删除不必要的账号。
- 使用命令 `passwd -l <用户名>` 锁定不必要的账号。
- 使用命令 `passwd -u <用户名>` 解锁必要的账号。

1.2 检查特殊账号

检查是否存在空口令和root权限的账号。

操作步骤

1. 查看空口令和root权限账号，确认是否存在异常账号：
   - 使用命令 `awk -F: '($2=="")' /etc/shadow` 查看空口令账号。
   - 使用命令 `awk -F: '($3==0)' /etc/passwd` 查看UID为零的账号。
2. 加固空口令账号：
   - 使用命令 `passwd <用户名>` 为空口令账号设定密码。
   - 确认UID为零的账号只有root账号。

1.3 添加口令策略

加强口令的复杂度等，降低被猜解的可能性。

操作步骤

1. 使用命令 `vi /etc/login.defs` 修改配置文件。
   - `PASS_MAX_DAYS 90 #新建用户的密码最长使用天数`

- `PASS_MIN_DAYS 0 #新建用户的密码最短使用天数`
- `PASS_WARN_AGE 7 #新建用户的密码到期提前提醒天数`

2. 使用chage命令修改用户设置。

   例如，`chage -m 0 -M 30 -E 2000-01-01 -W 7 <用户名>` 表示将此用户的密码最长使用天数设为30，最短使用天数设为0，密码2000年1月1日过期，过期前七天警告用户。

3. 设置连续输错三次密码，账号锁定五分钟。使用命令 `vi /etc/pam.d/common-auth` 修改配置文件，在配置文件中添加 `auth required pam_tally.so onerr=fail deny=3 unlock_time=300` 。

1.4 限制用户su

限制能su到root的用户。

操作步骤

使用命令 `vi /etc/pam.d/su` 修改配置文件，在配置文件中添加行。例如，只允许test组用户su到root，则添加 `auth required pam_wheel.so group=test` 。

1.4 禁止root用户直接登录

限制root用户直接登录。

操作步骤

1. 创建普通权限账号并配置密码,防止无法远程登录;
2. 使用命令 `vi /etc/ssh/sshd_config` 修改配置文件将PermitRootLogin的值改成no，并保存，然后使用 `service sshd restart` 重启服务。

2. 服务

2.1 关闭不必要的服务

关闭不必要的服务（如普通服务和xinetd服务），降低风险。

操作步骤

使用命令 `systemctl disable <服务名>` 设置服务在开机时不自动启动。

说明： 对于部分老版本的Linux操作系统（如CentOS 6），可以使用命令 `chkconfig --level <init级别> <服务名> off` 设置服务在指定init级别下开机时不自动启动。

2.2 SSH服务安全

对SSH服务进行安全加固，防止暴力破解成功。

操作步骤

使用命令 `vim /etc/ssh/sshd_config` 编辑配置文件。

- 不允许root账号直接登录系统。

设置 PermitRootLogin 的值为 no。

- 修改SSH使用的协议版本。

  设置 Protocol 的版本为 2。

- 修改允许密码错误次数（默认6次）。

  设置 MaxAuthTries 的值为 3。

配置文件修改完成后，重启sshd服务生效。

3. 文件系统

3.1 设置umask值

设置默认的umask值，增强安全性。

操作步骤

使用命令 `vi /etc/profile` 修改配置文件，添加行 `umask 027` ，即新创建的文件属主拥有读写执行权限，同组用户拥有读和执行权限，其他用户无权限。

3.2 设置登录超时

设置系统登录后，连接超时时间，增强安全性。

操作步骤

使用命令 `vi /etc/profile` 修改配置文件，将以 `TMOUT=` 开头的行注释，设置为 `TMOUT=180` ，即超时时间为三分钟。

4. 日志

4.1 syslogd日志

启用日志功能，并配置日志记录。

操作步骤

Linux系统默认启用以下类型日志：

- 系统日志（默认）/var/log/messages
- cron日志（默认）/var/log/cron
- 安全日志（默认）/var/log/secure

注意：部分系统可能使用syslog-ng日志，配置文件为：/etc/syslog-ng/syslog-ng.conf。

您可以根据需求配置详细日志。

4.2 记录所有用户的登录和操作日志

通过脚本代码实现记录所有用户的登录操作日志，防止出现安全事件后无据可查。

操作步骤

1. 运行 `[root@xxx /]# vim /etc/profile` 打开配置文件。
2. 在配置文件中输入以下内容：

```
history
USER=`whoami`
USER_IP=`who -u am i 2>/dev/null| awk '{print $NF}'|sed -e 's/[()]//g'`
if [ "$USER_IP" = "" ]; then
USER_IP=`hostname`
fi
if [ ! -d /var/log/history ]; then
mkdir /var/log/history
chmod 777 /var/log/history
fi
if [ ! -d /var/log/history/${LOGNAME} ]; then
mkdir /var/log/history/${LOGNAME}
chmod 300 /var/log/history/${LOGNAME}
fi
export HISTSIZE=4096
DT=`date +"%Y%m%d_%H:%M:%S"`
export HISTFILE="/var/log/history/${LOGNAME}/${USER}@${USER_IP}_$DT"
chmod 600 /var/log/history/${LOGNAME}/*history* 2>/dev/null
```

3. 运行 `[root@xxx /]# source /etc/profile` 加载配置生效。

注意： /var/log/history 是记录日志的存放位置，可以自定义。

通过上述步骤，可以在 /var/log/history 目录下以每个用户为名新建一个文件夹，每次用户退出后都会产生以用户名、登录IP、时间的日志文件，包含此用户本次的所有操作（root用户除外）。

同时，建议您使用OSS服务收集存储日志。

1.3. NFS 服务安全加固

NFS（Network File System）是FreeBSD支持的一种文件系统，它允许网络中的计算机之间通过TCP/IP 网络共享资源。不正确的配置和使用NFS，会带来安全问题。

NFS的不安全性，主要体现于以下4个方面：

- 缺少访问控制机制
- 没有真正的用户验证机制，只针对RPC/Mount请求进行过程验证
- 较早版本的NFS可以使未授权用户获得有效的文件句柄
- 在RPC远程调用中,SUID程序具有超级用户权限

加固方案

为有效应对以上安全隐患，推荐您使用下述加固方案。

配置共享目录（/etc/exports）

使用anonuid，anongid配置共享目录，这样可以使挂载到NFS服务器的客户机仅具有最小权限。不要使用no_root_squash。

使用网络访问控制

使用安全组策略或iptable防火墙限制能够连接到NFS服务器的机器范围。

```
iptables -A INPUT -i eth0 -p TCP -s 192.168.0.0/24 --dport 111 -j ACCEPT
iptables -A INPUT -i eth0 -p UDP -s 192.168.0.0/24 --dport 111 -j ACCEPT
iptables -A INPUT -i eth0 -p TCP -s 172.16.0.1/8 --dport 111 -j ACCEPT
iptables -A INPUT -i eth0 -p UDP -s 172.16.0.1/8 --dport 111 -j ACCEPT
```

账号验证

使用Kerberos V5作为登录验证系统，要求所有访问人员使用账号登录，提高安全性。

设置 NFSD 的 COPY 数目

在Linux中NFSD的COPY数目定义在启动文件 `/etc/rc.d/init.d/nfs` 中，默认值为8。

最佳的COPY数目一般取决于可能的客户机数目。您可以通过测试来找到COPY数目的近似最佳值，并手动设置该参数。

选择传输协议

对于不同的网络情况，有针对地选择UDP或TCP传输协议。传输协议可以自动选择，也可以手动设置。

```
mount -t nfs -o sync,tcp,noatime,rsize=1024,wsize=1024 EXPORT_MACHINE:/EXPORTED_DIR /DIR
```

UDP协议传输速度快，非连接传输时便捷，但其传输稳定性不如TCP，当网络不稳定或者黑客入侵时很容易使NFS性能大幅降低，甚至导致网络瘫痪。一般情况下，使用TCP的NFS比较稳定，使用UDP的NFS速度较快。

- 在机器较少，网络状况较好的情况下，使用UDP协议能带来较好的性能。
- 当机器较多，网络情况复杂时，推荐使用TCP协议（V2只支持UDP协议）。
- 在局域网中使用UDP协议较好，因为局域网有比较稳定的网络保证，使用UDP可以带来更好的性能。
- 在广域网中推荐使用TCP协议，TCP协议能让NFS在复杂的网络环境中保持较好的传输稳定性。

限制客户机数量

修改 `/etc/hosts.allow` 和 `/etc /hosts.deny` 来限制客户机数量。

```
/etc/hosts.allow
portmap: 192.168.0.0/255.255.255.0 : allow
portmap: 172.16.0.1 : allow
/etc/hosts.deny
portmap: ALL : deny
```

改变默认的 NFS 端口

NFS默认使用的是111端口，使用port参数可以改变这个端口值。改变默认端口值能够在一定程度上增强安全性。

配置nosuid和noexec

SUID（Set User ID）或SGID（Set Group ID）程序可以让普通用户以超过自己权限来执行。很多 SUID/SGID可执行程序是必须的，但也可能被一些恶意的本地用户利用，获取本不应有的权限。

尽量减少所有者是root，或是在root组中却拥有SUID/SGID属性的文件。您可以删除这样的文件或更改其属性，如：

- 使用nosuid选项禁止set-UID程序在NFS服务器上运行，可以在 `/etc/exports` 加入一行：

```
/www www.aliyundoc.com(rw, root_squash, nosuid)
```

- 使用noexec禁止直接执行其中的二进制文件。

1.4. Rsync 服务安全加固

Rsync是一个通过检查文件的时间戳和大小，来跨计算机系统高效地传输和同步文件的工具。

通常情况下，管理程序在启动 Rsync 服务后，会直接运行传输任务。如果 Rsync 服务未经过安全加固，则很容易出现未授权访问等安全问题，其直接后果是传输数据裸露在互联网上，可以被任何人访问获取，带来严重的数据泄露风险。

建议您在使用 Rsync 服务端时，参考本文对 Rsync 服务进行安全加固，保障数据安全。

隐藏 module 信息

将配置文件修改为以下内容：

```
list = false
```

使用权限控制

将不需要写入权限的 module 设置为只读：

```
read only = true
```

限制网络访问

使用 安全组策略 或白名单，限制允许访问主机的 IP 地址。

```
hosts allow = 192.168.0.1
```

启用账户认证

只允许指定的用户，使用指定的密码，来调用 Rsync 服务。

- 服务端配置

```
auth users = ottocho
secrets file = /etc/rsyncd.secrets
```

在文件 `/etc/rsyncd.secrets` 中写入使用的账号密码，格式为：`username:password`，支持多行。

> 注意
>
> 密码要求满足强密码策略，必须是 8 位以上，且包括大小写字母、数字、特殊字符的字符串。此处的 password 使用明文。

- 客户端配置

  在客户端，使用 `--password-file=/etc/rsyncd.secrets` 参数，在 `/etc/rsyncd.secrets` 中写入密码。

```
Rsync -av --password-file=/etc/rsyncd.secrets aliyundoc.com::files /des/path
```

在上述 `/etc/rsyncd.secrets` 密码文件中，用户或用户组必须和实际使用者保持一致，且权限必须是 600。

数据加密传输

Rsync 默认不支持加密传输，如果需要使用 Rsync 传输重要性很高的数据，可以使用 SSH 模式。

Rsync 支持以下两种同步模式：

- 当源路径或目的路径的主机名后面包含一个冒号分隔符时，Rsync 使用 SSH 传输。
- 当源路径或目的路径的主机名后面包含两个冒号，或使用 `Rsync://URL` 时，Rsync 使用 TCP 直接连接 Rsync daemon。

在配置好 SSH 后，推荐参照以下方式来使用：

```
Rsync -av aliyundoc.com:/path/to/files /des/path
```

1.5. 如何在Windows和Windows Server中启用/禁用 SMBv1、SMBv2、SMBv3

本文介绍如何在SMB客户端和服务器组件上启用/禁用服务器消息块SMBv1、SMBv2和SMBv3。

> 注意
>
> - 建议由专业技术工程师完成本文的操作。
> - 我们建议不要禁用SMBv2或SMBv3。禁用SMBv2或SMBv3只能作为临时故障排除措施。请勿使SMBv2或SMBv3保持禁用状态。

禁用SMBv2的影响

在Windows 7和Windows Server 2008 R2中，禁用SMBv2会停用以下功能：

- 请求复合：允许发送多个SMB 2请求作为单个网络请求
- 大型读写：更好地利用更快速的网络
- 文件夹和文件属性缓存：客户端保留文件夹和文件的本地副本

- 持久句柄：如果临时断开连接，则允许连接以透明方式重新连接到服务器
- 改进的消息签名：HMAC SHA-256代替MD5作为哈希算法
- 改进的文件共享扩展性：每个服务器的用户数量、共享数量和打开文件数量大大增加
- 支持符号链接
- 客户端oplock租赁模式：限制在客户端和服务器之间传输的数据，从而提高高延迟网络性能并增强SMB 服务器的扩展性
- 大型MTU支持：可充分利用10千兆字节 (GB) 以太网
- 改进的能效：向服务器打开文件的客户端可以睡眠

禁用SMBv3的影响

在Windows 8、Windows 8.1、Windows 10、Windows Server 2012和Windows Server 2016中，禁用SMBv3会停用以下功能（以及以上列表中所述的SMBv2功能）：

- 透明故障转移 ：在维护或故障转移期间，客户端会重新连接，不会干扰集群节点
- 扩展：并发访问所有文件集群节点上的共享数据
- 多通道：如果客户端和服务器之间有多个路径可用时，则聚合网络带宽和容错
- SMB直通：增加RDMA网络支持，实现极高的性能、低延迟和低CPU利用率
- 加密：提供端到端加密，并防止不可靠网络上的窃听
- 目录租赁：通过缓存改进分支机构中应用程序的响应时间
- 性能优化：对小型I/O随机读/写的优化

在SMB服务器上启用/禁用SMB协议

Windows 8和 Windows Server 2012

Windows 8和Windows Server 2012引入了新的Set-SMBServerConfiguration Windows PowerShell cmdlet。 通过此cmdlet，你可以在服务器组件上启用或禁用SMBv1、SMBv2 和 SMBv3协议。

> **说明**
>
> 因为SMBv2和SMBv3共用一个堆叠，所以在Windows 8或Windows Server 2012中启用或禁用 SMBv2 时，也会启用或禁用SMBv3。

使用PowerShell cmdlet

运行**Set-SMBServerConfiguration**cmdlet后，无须重启计算机。

- 若要获取SMB服务器协议配置的当前状态，请运行以下cmdlet：

```
Get-SmbServerConfiguration | Select EnableSMB1Protocol, EnableSMB2Protocol
```

- 若要在SMB服务器上禁用SMBv1，请运行以下cmdlet：

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

- 若要在SMB服务器上禁用SMBv2和SMBv3，请运行以下cmdlet：

```
Set-SmbServerConfiguration -EnableSMB2Protocol $false
```

- 若要在SMB服务器上启用SMBv1，请运行以下cmdlet：

```
Set-SmbServerConfiguration -EnableSMB1Protocol $true
```

- 若要在SMB服务器上启用SMBv2和SMBv3，请运行以下cmdlet：

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

Windows 7、Windows Server 2008 R2、Windows Vista和 Windows Server 2008

若要在运行Windows 7、Windows Server 2008 R2、Windows Vista或Windows Server 2008的SMB服务器上启用或禁用SMB协议，请使用Windows PowerShell或注册表编辑器。

使用Windows PowerShell 2.0或更高版本的PowerShell

- 若要在SMB服务器上禁用SMBv1，请运行以下cmdlet：

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SM
B1 -Type DWORD -Value 0 -Force
```

- 若要在SMB服务器上禁用SMBv2和SMBv3，请运行以下cmdlet：

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SM
B2 -Type DWORD -Value 0 -Force
```

- 若要在SMB服务器上启用SMBv1，请运行以下cmdlet：

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SM
B1 -Type DWORD -Value 1 -Force
```

- 若要在SMB服务器上启用SMBv2和SMBv3，请运行以下cmdlet：

```
Set-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters" SM
B2 -Type DWORD -Value 1 -Force
```

> **注意**
>
> 进行这些更改后，必须重启计算机。

使用注册表编辑器

以下内容包含有关如何修改注册表的信息。

> **注意**
>
> 修改注册表之前，一定要先对其进行备份。并且一定要知道在发生问题时如何还原注册表。有关如何备份、还原和修改注册表的更多信息，请查看 如何在 Windows 中备份和还原注册表。

- 若要在SMB服务器上启用或禁用SMBv1，请配置以下注册表项：
  - 注册表子项：`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters` 注册表项：SMB1
  - REG_DWORD： 0 = 已禁用
  - REG_DWORD： 1 = 已启用
  - 默认值： 1 = 已启用
- 若要在 SMB 服务器上启用或禁用SMBv2，请配置以下注册表项：
  - 注册表子项：`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters` 注册表项：SMB2
  - REG_DWORD： 0 = 已禁用
  - REG_DWORD： 1 = 已启用
  - 默认值： 1 = 已启用

在SMB客户端上启用/禁用SMB协议

Windows Vista、Windows Server 2008、Windows 7、Windows Server 2008 R2、Windows 8和Windows Server 2012

> **注意**
>
> 因为SMBv2和SMBv3共用一个堆叠，所以在Windows 8或Windows Server 2012中启用或禁用SMBv2时，也会启用或禁用SMBv3。

- 若要在SMB客户端上禁用SMBv1，请运行以下命令：

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb20/nsi
sc.exe config mrxsmb10 start= disabled
```

- 若要在SMB客户端上启用SMBv1，请运行以下命令：

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi
sc.exe config mrxsmb10 start= auto
```

- 若要在SMB客户端上禁用SMBv2和SMBv3，请运行以下命令：

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/nsi
sc.exe config mrxsmb20 start= disabled
```

- 若要在SMB客户端上启用SMBv2和SMBv3，请运行以下命令：

```
sc.exe config lanmanworkstation depend= bowser/mrxsmb10/mrxsmb20/nsi
sc.exe config mrxsmb20 start= auto
```

> 注意
>
> - 必须在提升的命令提示符中运行这些命令。
> - 进行这些更改后，必须重启计算机。

使用组策略禁用SMBv1服务器

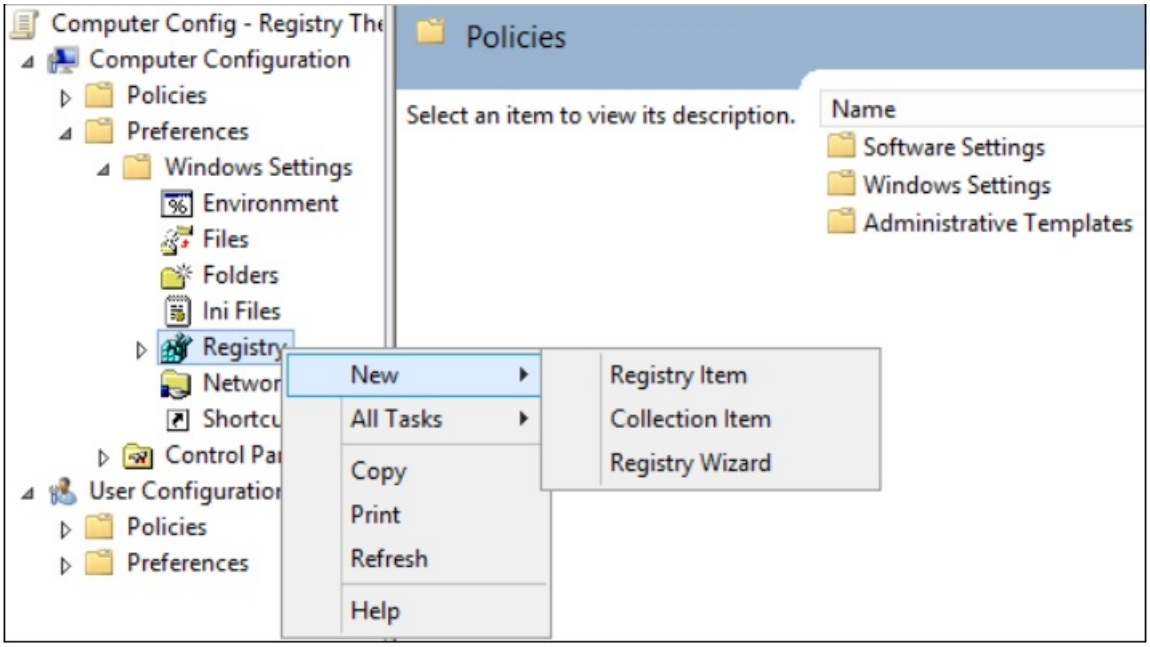
这将在注册表中配置以下新项：

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters` 注册表项：

SMB1 REG_DWORD: 0 = Disabled

使用组策略配置流程

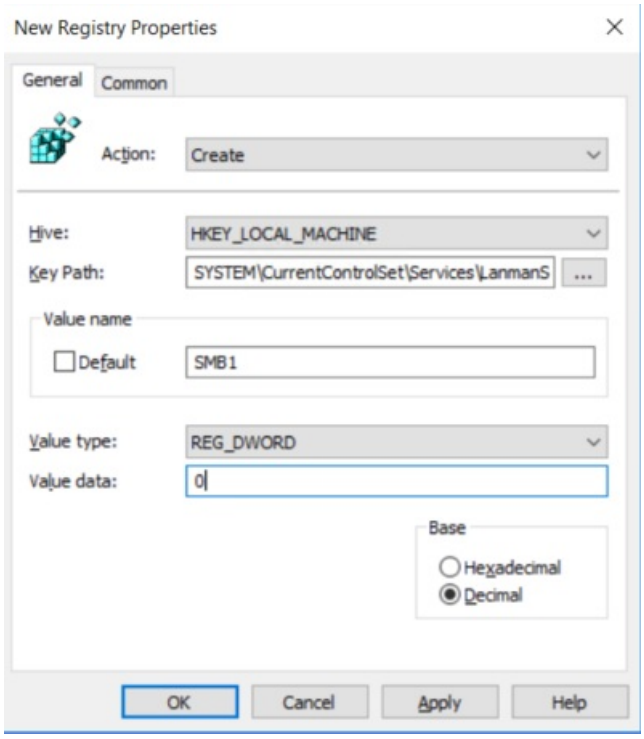
1. 打开组策略管理控制台。右键单击应包含新首选项的组策略对象 (GPO)，然后单击**编辑**。
2. 在**计算机配置**下的控制台树中，展开**首选项**文件夹，然后展开**Windows 设置**文件夹。
3. 右键单击**注册表**节点，指向**新建**，然后选择**注册表项**。



sg1

4. 在**新建注册表属性**对话框中，选择以下内容：
   - 操作： 创建
   - Hive： HKEY_LOCAL_MACHINE
   - 注册表项路径： SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
   - 值名称： SMB1

- 值类型： REG_DWORD
- 值数据： 0



sg2

5. 将此组策略应用到域中所有必需的工作站、服务器和域控制器，以禁用 SMBv1 服务器组件。也可以将 WMI 筛选器设置为不包含不受支持的操作系统或选中的排除项（如 Windows XP）。

> 注意
>
> 在旧版Windows XP或Linux早期版本以及第三方系统（不支持SMBv2或SMBv3）需要访问 SYSVOL或其他文件共享（已启用SMB v1）的域控制器上进行这些更改时要谨慎小心。

使用组策略禁用SMBv1客户端

若要禁用SMBv1客户端，需要将服务注册表项更新为禁止MRxSMB10启动，然后还需要将MRxSMB10的依赖项从LanmanWorkstation项中删除，以便它可以正常启动（无需首先启动MRxSMB10）。

这将更新和替换注册表以下2个项中的默认值：

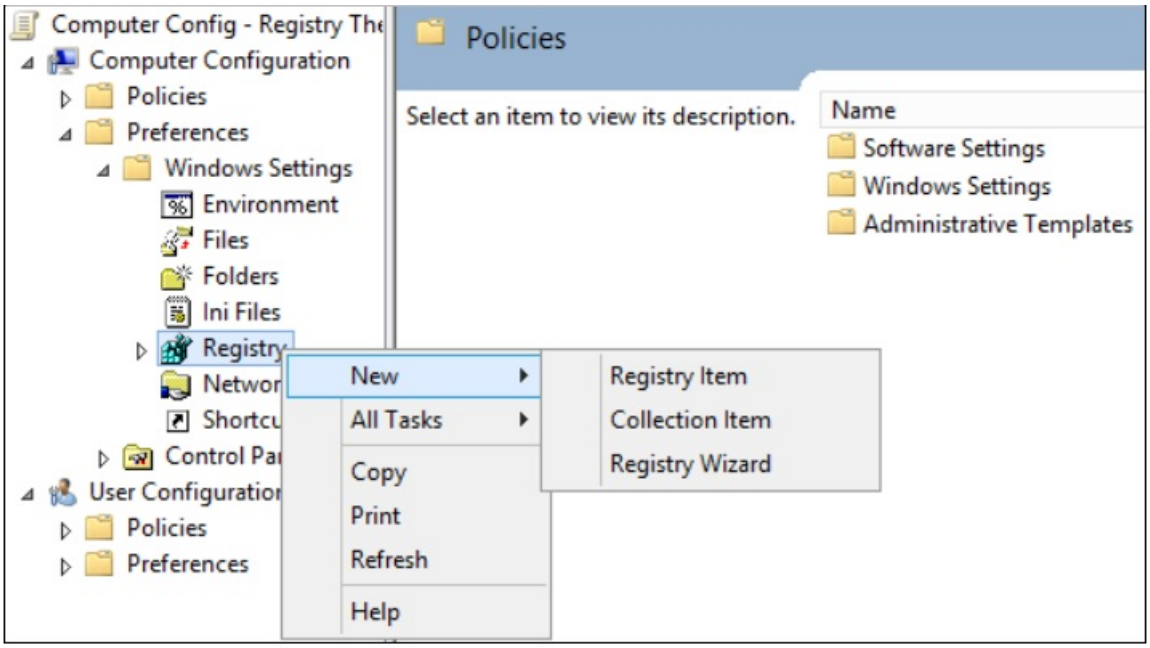
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\mrxsmb10` 注册表项： Start REG_DWORD: 4 = Disabled
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation` 注册表项： DependOnService REG_MULTI_SZ: “Bowser”,” MR

默认包含的 MRxSMB10 现已作为依赖项删除。

使用组策略配置流程

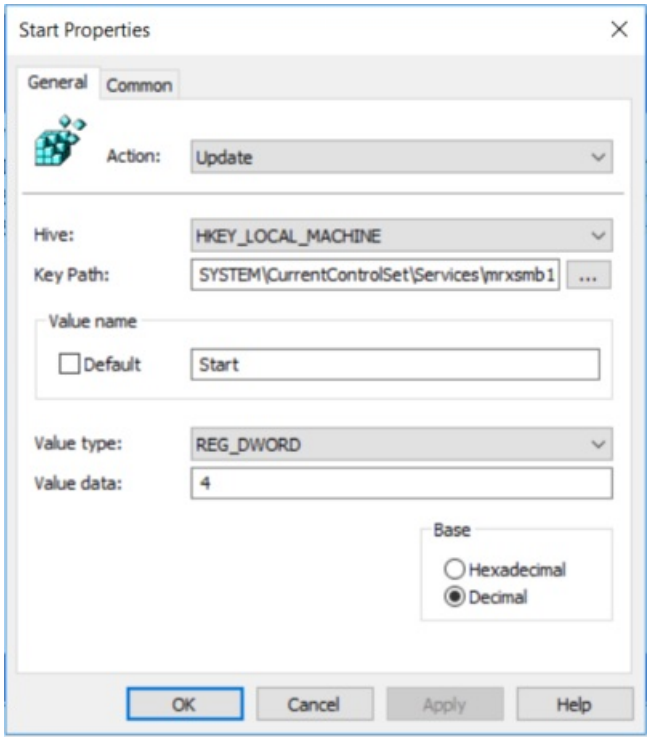
1. 打开组策略管理控制台。右键单击应包含新首选项的组策略对象 (GPO)，然后单击**编辑**。

2. 在**计算机配置**下的控制台树中，展开**首选项**文件夹，然后展开**Windows 设置**文件夹。
3. 右键单击**注册表**节点，指向**新建**，然后选择**注册表项**。



sg3

4. 在**新建注册表属性**对话框中，选择以下内容：
   - 操作： 更新
   - Hive： HKEY_LOCAL_MACHINE
   - 注册表项路径： SYSTEM\CurrentControlSet\services\mrxsmb10
   - 值名称： Start
   - 值类型： REG_DWORD
   - 值数据： 4

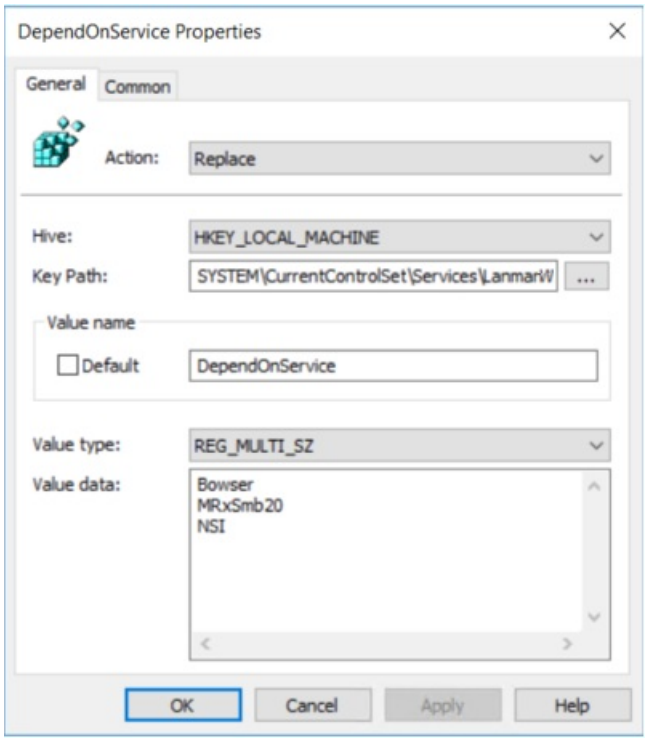


sg4

然后删除刚刚禁用的 MRxSMB10 的依赖项

5. 在**新建注册表属性**对话框中，选择以下内容：
   - 操作： 替换
   - Hive： HKEY_LOCAL_MACHINE
   - 注册表项路径： SYSTEM\CurrentControlSet\Services\LanmanWorkstation
   - 值名称： DependOnService
   - 值类型 REG_MULTI_SZ
   - 值数据：
     - Bowser
     - MRxSmb20
     - NSI

   这 3 个字符串不带项目符号（具体如下）：



在Windows的多个版本中，默认值包括MRxSMB10，通过将其替换为此多值字符串，实际上就删除了作为LanmanServer依赖项的MRxSMB10，结果是从四个默认值减少为上述这三个值。

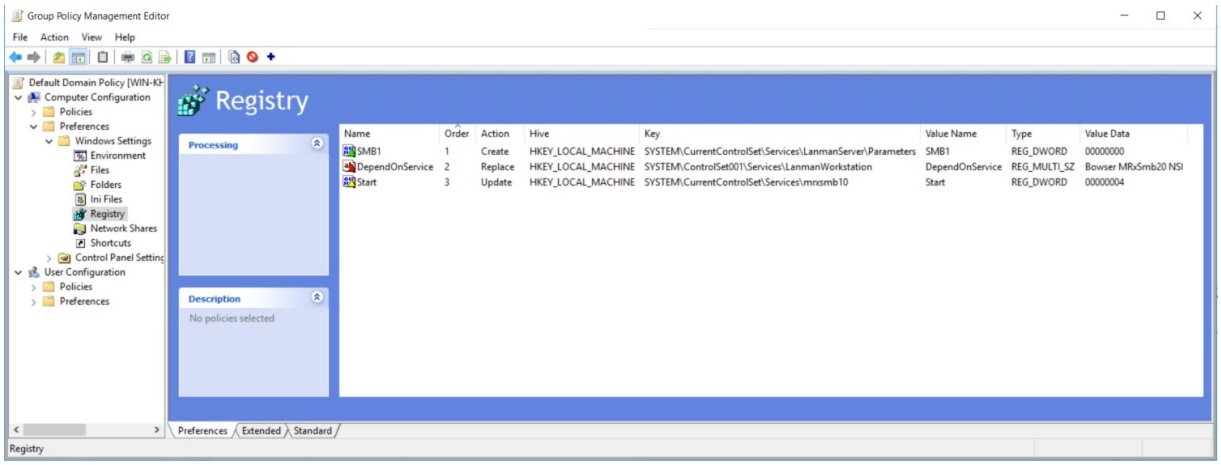
使用组策略管理控制台时，无需使用引号或逗号。只需在各行键入每个项，如上面所示。

需要重新启动

应用策略且正确设置注册表后，必须重新启动目标系统，然后才能禁用SMB v1。

摘要

如果所有设置均在同一组策略对象 (GPO) 中，组策略管理将显示以下设置。



sg6

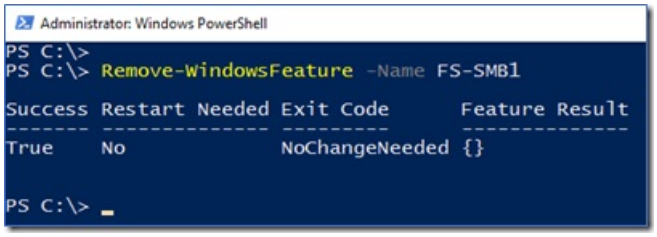
测试和验证

配置完成后即允许策略进行复制和更新。作为测试的必要步骤，请从 `CMD.EXE` 提示符处运行 `gpupdate/force` ，然后查看目标计算机，以确保注册表设置得以正确应用。确保 SMBv2 和 SMBv3 在环境中的所有其他系统中正常运行。

> 注意
>
> 请务必重新启动目标系统。

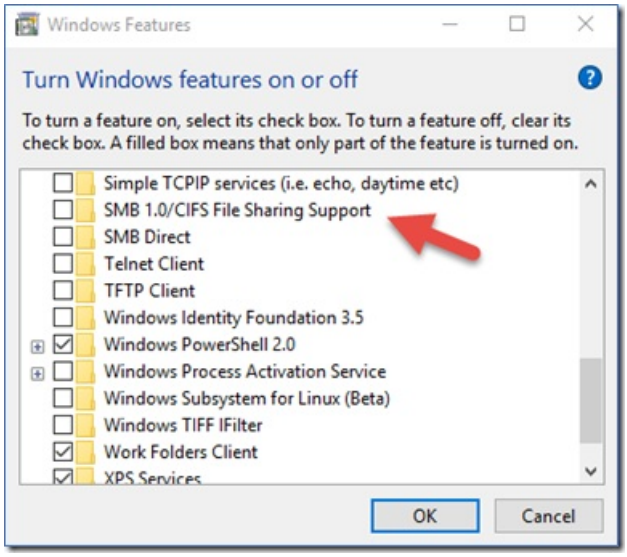
如何在 Windows 8.1、Windows 10、Windows 2012 R2和 Windows Server 2016中删除SMBv1

Windows Server：使用PowerShell (Remove-WindowsFeature FS-SMB1)



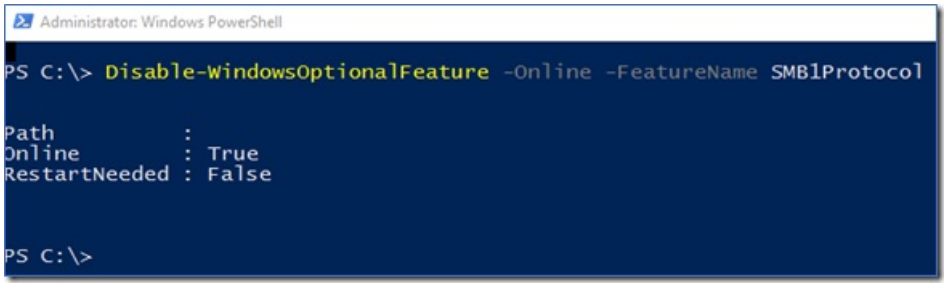
sg8

Windows客户端：使用 “添加或删除程序”



sg9

Windows客户端：使用PowerShell (Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol)



sg10

参考与适用性

本文来源自微软官方技术文档：如何在 Windows 和 Windows Server 中启用和禁用 SMBv1、SMBv2 和 SMBv3。

如有变化，以微软官方为准。

这篇文章中的信息适用于：

- Windows 10 Pro released in July 2015,
- Windows 10 Enterprise released in July 2015
- Windows Vista Enterprise
- Windows Vista Business
- Windows Vista Home Basic
- Windows Vista Home Premium
- Windows Vista Ultimate
- Windows 7 Enterprise
- Windows 7 Home Basic
- Windows 7 Home Premium
- Windows 7 Professional
- Windows 7 Ultimate
- Windows Server 2008 Datacenter
- Windows Server 2008 Enterprise
- Windows Server 2008 Standard
- Windows Server 2008 R2 Datacenter
- Windows Server 2008 R2 Enterprise
- Windows Server 2008 R2 Standard
- Windows 8
- Windows 8 Enterprise
- Windows 8 Pro
- Windows Server 2012 Datacenter
- Windows Server 2012 Essentials
- Windows Server 2012 Foundation

- Windows Server 2012 Standard
- Windows Server 2016

2.Web应用安全加固

2.1. 抵御Webshell入侵

本文介绍了Webshell的概念、入侵原理以及防护方法，帮助您抵御Webshell入侵，避免其带来的数据泄露等危害。

从字面上理解，"Web"指需要服务器开放Web服务，"shell"指取得对服务器的某种程度的操作权限。Webshell指匿名用户（入侵者）通过网站端口，获取网站服务器的一定操作权限。

Webshell通常是以ASP、PHP、JSP、ASA或者CGI等网页文件形式存在的一种命令执行环境，也称为网页后门。黑客在入侵网站后，通常会将Webshell后门文件与网站服务器Web目录下正常的网页文件混在一起；然后使用浏览器来访问这些后门，得到命令执行环境，以达到控制网站或者Web系统服务器的目的。

黑客如果想使用Webshell完成一些特殊的功能，就不可避免地用到一些特殊函数。通过对这些函数进行对照特征值检查，就能够定位Webshell，但是Webshell本身也会进行加密来躲避这种检测。

Webshell 样例

以下是一个ASP Webshell的样例。从界面看，它的功能还是比较全的，可以对服务器的文件目录进行读写操作。如果你是网站管理员的话，肯定不希望普通用户获得下面的权限。

Webshell

Webshell如何被注入

常见的Webshell植入方式以下类型：

- 利用站点上传漏洞，上传Webshell。

  系统前台的上传业务可被利用来上传Webshell脚本，而被上传的目录往往对用户开放可执行权限。在Web中有上传图像、资料文件的地方，上传完后通常会向客户端返回上传文件的完整URL信息；该URL一般是常见的image、upload等目录。

  如果Web服务器对网站存取权限或者文件夹目录权限控制不严，就可能被利用来实现Webshell攻击。攻击者可以利用上传功能上传一个脚本文件，然后通过URL访问并执行这个脚本；然后攻击者就可以上传Webshell到网站的任意目录中，从而拿到网站的管理员控制权限。

- 黑客获取管理员的后台密码，登录到后台系统，利用后台的管理工具向配置文件写入Webshell木马；或者私自添加上传类型，允许上传类似ASP、PHP格式的脚本程序文件。
- 利用数据库备份与恢复功能获取Webshell。例如，备份时把备份文件的后缀改成 .asp；如果后台有MySQL数据查询功能，黑客可以执行 `select..in To outfile` 查询输出PHP文件，并把代码插入到MySQL，从而生成Webshell的木马。
- 系统中其他站点被攻击，或者服务器上还搭载了FTP服务器。FTP服务器被攻击时被注入了Webshell的木马，导致网站系统被感染。
- 黑客直接攻击Web服务器系统漏洞，实现入侵。Web服务器在系统层面也可能存在漏洞，如果黑客利用其漏洞攻击服务器系统；在获取其权限后，黑客就可以在Web服务器目录里上传Webshell文件。

综上，Webshell能够入侵到系统，一般是由于以下原因：

- 通过Web站点漏洞上传Webshell。

  Webshell能够被注入，在很大程度是由于服务器或中间件的安全漏洞。例如，以下常见漏洞都可能被利用来注入Webshell：旧版本的IIS目录解析漏洞、文件名解析漏洞、应用后台暴露和弱口令、Fast-CGI解析漏洞、Apache文件解析漏洞、截断上传、后台数据库备份功能上传、数据库语句上传漏洞等。

- 站点部署时混入了Webshell文件。

  大量的用户在使用从网上下载的第三方开源代码时，其代码本身已经混入了Webshell的恶意脚本，造成二次入侵或多次入侵。所以在部署前期，如果不是新开发的代码，都需要对代码进行恶意文件扫描查杀，防止上线后被入侵。

如何防止系统被植入Webshell

- 配置必要的防火墙并开启防火墙策略；防止暴露不必要的服务，为黑客提供利用条件。
- 对服务器进行安全加固。例如，关闭远程桌面功能、定期更换密码、禁止使用最高权限用户运行程序、使用HTTPS加密协议。
- 加强权限管理，对敏感目录进行权限设置，限制上传目录的脚本执行权限，不允许配置执行权限等。
- 安装云安全中心产品，发现检测结果后，立即隔离查杀，并排查漏洞。
- 排查程序存在的漏洞，并及时修补漏洞。您可以通过应急响应服务人工界入，协助排查漏洞及入侵原因，同时可以选用阿里云商业Web应用防火墙进行防御，降低被入侵机率。