服务器加固配置参考手册

XXXX科技股份有限公司

* 文档说明

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 文档名称 | SFSS-SSEC-M00001文档模板v1.0 | | | |
| 文档管理编号 |  | | | |
| 保密级别 | 商密 | 文档版本号 | | V1.0 |
| 制作人 | XXXX安全服务团队 | 制作日期 | | 2018-05-14 |
| 复审人 | XXXX安全服务团队 | 复审日期 | |  |
| 扩散范围 | 限“XXXX科技股份有限公司项目组”、xx | | | |
| 分发控制 | XXXX：创建、修改、读取 | | xxxx项目组：读取 | |

* 版本变更记录

|  |  |  |  |
| --- | --- | --- | --- |
| 修改日期 | 版本 | 说明 | 修改人 |
|  |  |  |  |
|  |  |  |  |

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明，版权均属XXXX所有，受到有关产权及版权法保护。任何个人、机构未经XXXX的书面授权许可，不得以任何方式复制或引用本文的任何片断。

目录

1 服务器安全加固 4

1.1 windows安全加固 4

1.1.1 账户管理和认证授权 4

1.1.2 日志配置 8

1.1.3 IP协议安全配置 11

1.1.4 文件权限 11

1.1.5 服务安全 12

1.1.6 安全选项 13

1.1.7 其他安全配置 15

1.2 Linux安全加固 16

1.2.1 账号管理和认证授权 16

1.2.2 日志配置 23

1.2.3 1.2.3协议安全 24

1.2.4 1.2.4其他安全配置 26

2 Web中间件安全加固 32

2.1 Tomcat安全加固 32

2.2 IIS安全加固 36

2.3 Apache安全加固 42

2.4 Nginx安全加固 48

3 数据库安全加固 51

3.1 MYSQL数据库加固 51

3.2 MSSQL数据库加固 57

3.3 3.3 Oracle数据库加固 62

4 网站安全加固 68

4.1 PHP环境安全加固 68

# 服务器安全加固

## windows安全加固

### 账户管理和认证授权

1. 默认账户安全

实施目的：禁用或删除其他无用账户。

加固方法：

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：缺省帐户Administrator－>属性Guest帐号->属性

2. 按照用户分配帐户

实施目的：按照用户分配帐户。根据业务要求，设定不同的帐户和帐户组，管理员用户，数据库用户，审计用户，来宾用户等。

加固方法：

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：根据系统的要求，设定不同的帐户和帐户组，管理员用户，数据库用户，审计用户，来宾用户。

3. 定期检查并删除与无关帐户

实施目的：删除或锁定与设备运行、维护等与工作无关的帐户。

加固方法：

进入“控制面板->管理工具->计算机管理”，在“系统工具->本地用户和组”：删除或锁定与设备运行、维护等与工作无关的帐户。

4. 不显示最后的用户名

实施目的：配置登录登出后，不显示用户名称。

加固方法：

进入“控制面板->管理工具->本地安全策略”，打开“本地策略”->“安全选项”->选择“交互式登录:不显示最后的用户名” 设置“已启用”



5. 密码复杂度

实施目的：检查密码复杂度。

加固方法：

密码复杂度要求满足以下策略：

最短密码长度 8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2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

参考配置：

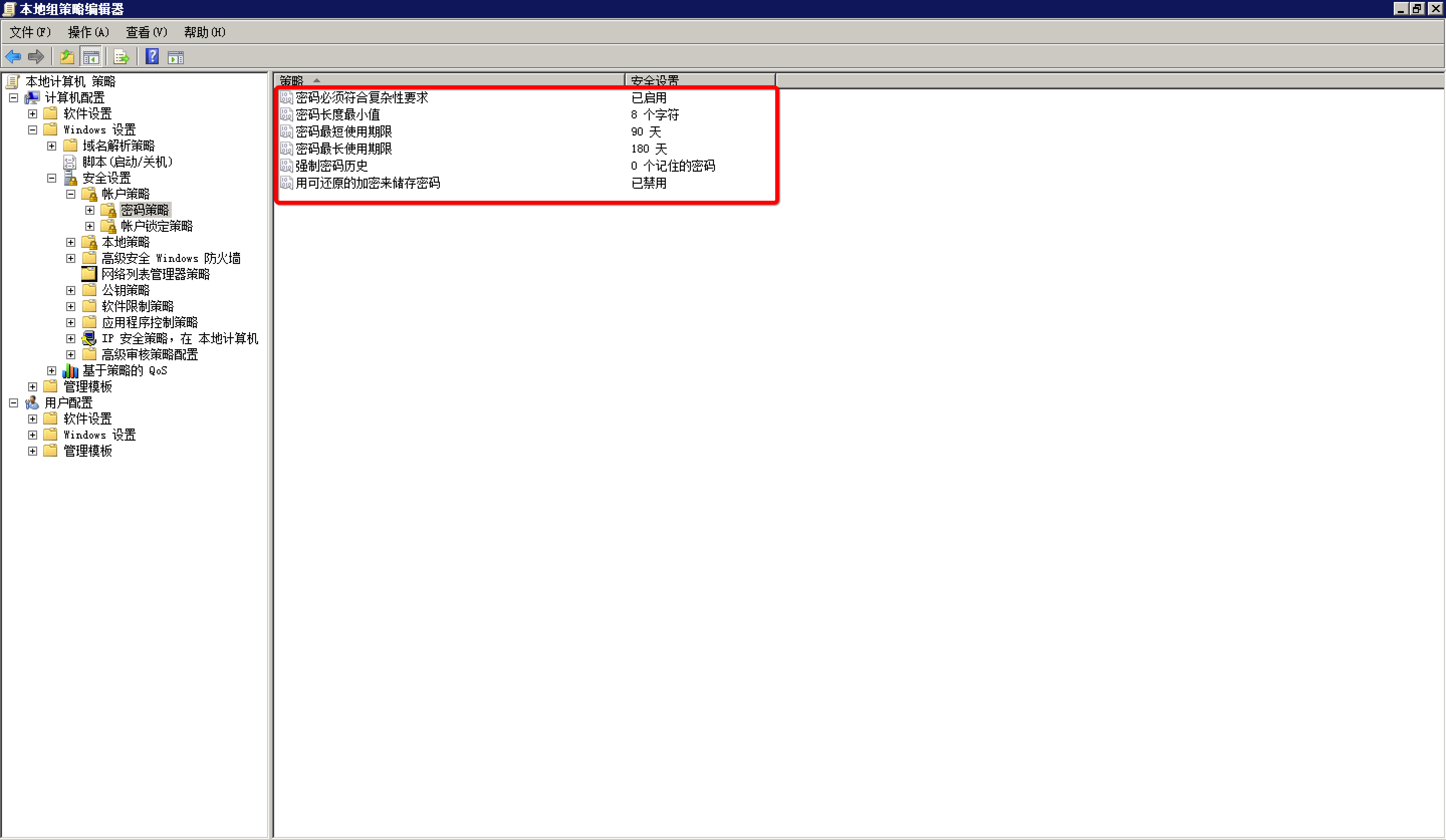
进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：查看是否“密码必须符合复杂性要求”选择“已启动”

6. 密码最长留存期

实施目的：对于采用静态口令认证技术的设备，帐户口令的生存期不长于90天。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->密码策略”：配置“密码最长存留期”

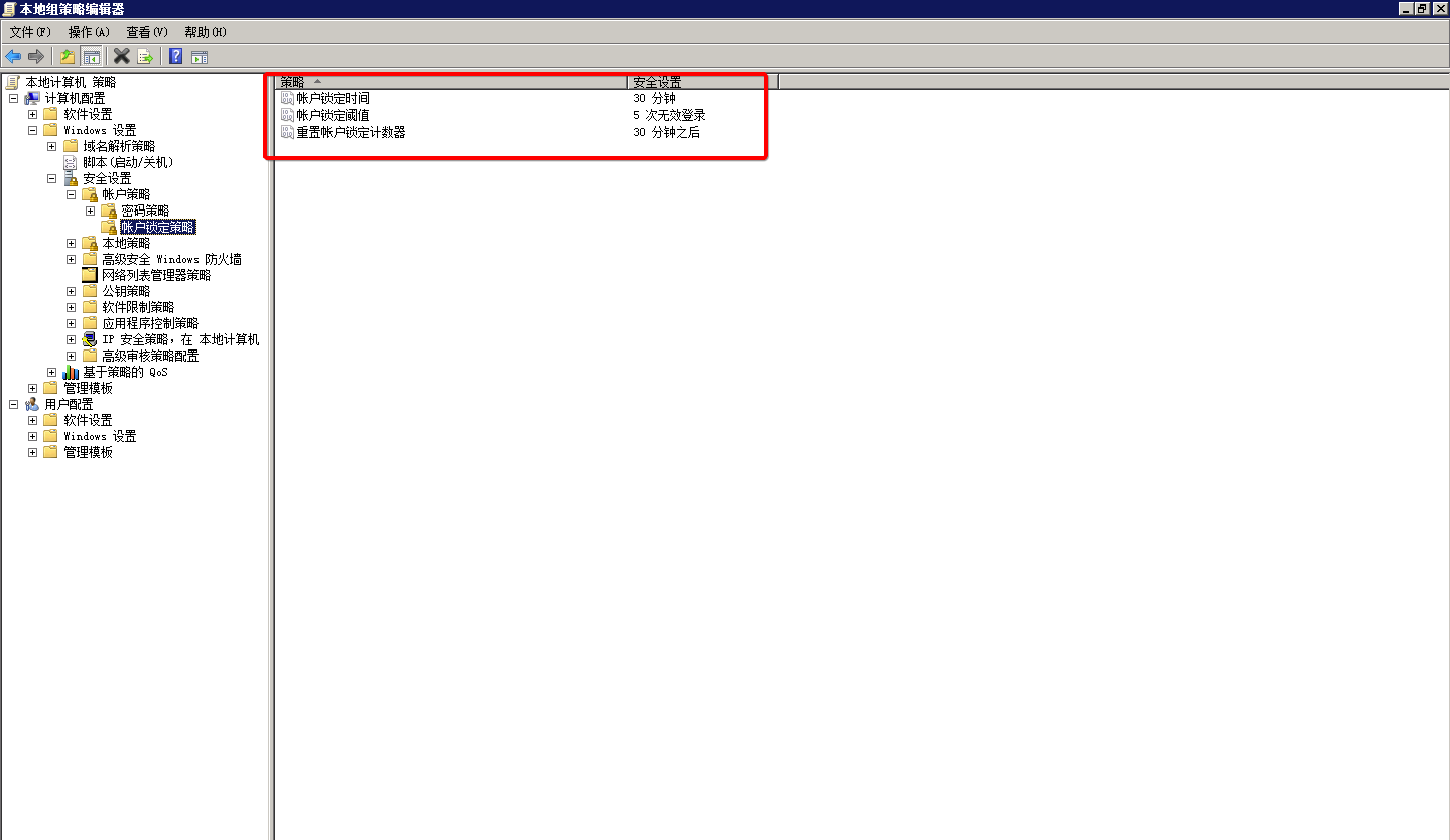


7. 帐户锁定策略

实施目的：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，锁定该用户使用的帐户。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“帐户策略->帐户锁定策略”：配置“帐户锁定阀值”设置。



8. 远程关机

实施目的：在本地安全设置中从远端系统强制关机只指派给Administrators组。

加固方法：

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”:配置“从远端系统强制关机”设置

9. 本地关机

实施目的：在本地安全设置中关闭系统仅指派给Administrators组。

加固方法：

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”:授权配置“关闭系统”设置

10. 用户权限指派

实施目的：在本地安全设置中取得文件或其它对象的所有权仅指派给Administrators。

加固方法：

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”：“取得文件或其它对象的所有权”设置用户。

11. 远程关机

实施目的：配置登录登出后，不显示用户名称。

加固方法：

12. 授权帐户登陆

实施目的：在本地安全设置中配置指定授权用户允许本地登陆此计算机。

加固方法：

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”“从本地登陆此计算机”设置为“指定授权用户”

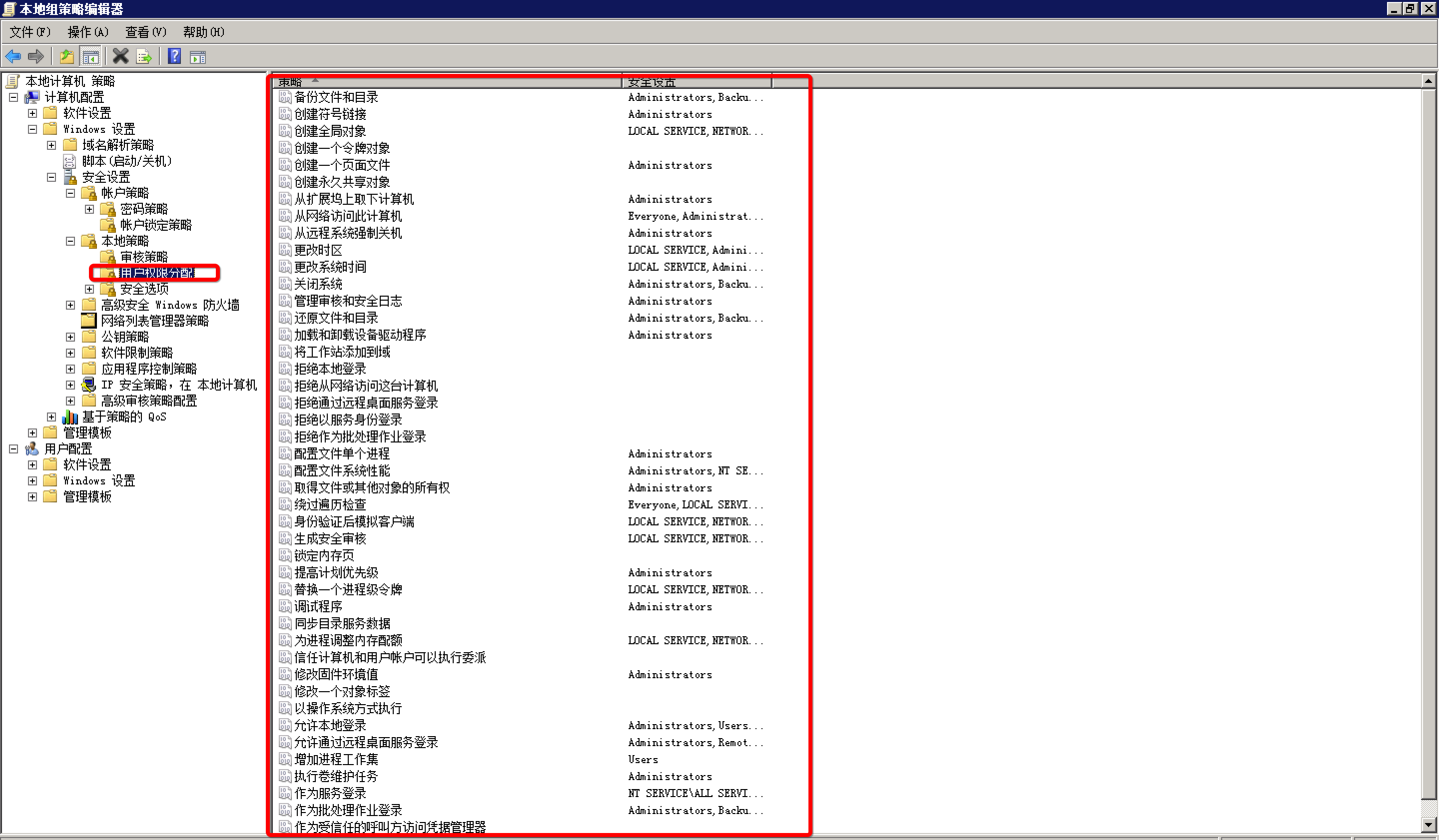
13. 授权帐户从网络访问

实施目的：在组策略中只允许授权帐号从网络访问(包括网络共享等，但不包括终端服务)此计算机。

加固方法：

在组策略中只允许授权帐号从网络访问(包括网络共享等，但不包括终端服务)此计算机。

参考配置：



### 日志配置

1. 审核登录

实施目的：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帐户，登录是否成功，登录时间，以及远程登录时，用户使用的IP地址。

加固方法：

开始->运行-> 执行“ 控制面板->管理工具->本地安全策略->审核策略”审核登录事件。

2. 审核策略

实施目的：启用组策略中对Windows系统的审核策略更改，成功和失败都要审核。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中“审核策略更改”设置。

3. 审核对象访问

实施目的：启用组策略中对Windows系统的审核对象访问，成功和失败都要审核。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核对象访问”设置。

4. 审核事件目录服务访问

实施目的：启用组策略中对Windows系统的审核目录服务访问，失败。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核目录服务器访问”设置。

5. 审核特权使用

实施目的：用组策略中对Windows系统的审核特权使用，成功和失败都要审核。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核特权使用”设置。

6. 审核系统事件

实施目的：启用组策略中对Windows系统的审核系统事件，成功和失败都要审核。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核系统事件”设置。

7. 审核帐户管理

实施目的：启用组策略中对Windows系统的审核帐户管理，成功和失败都要审核。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核帐户管理” 设置。

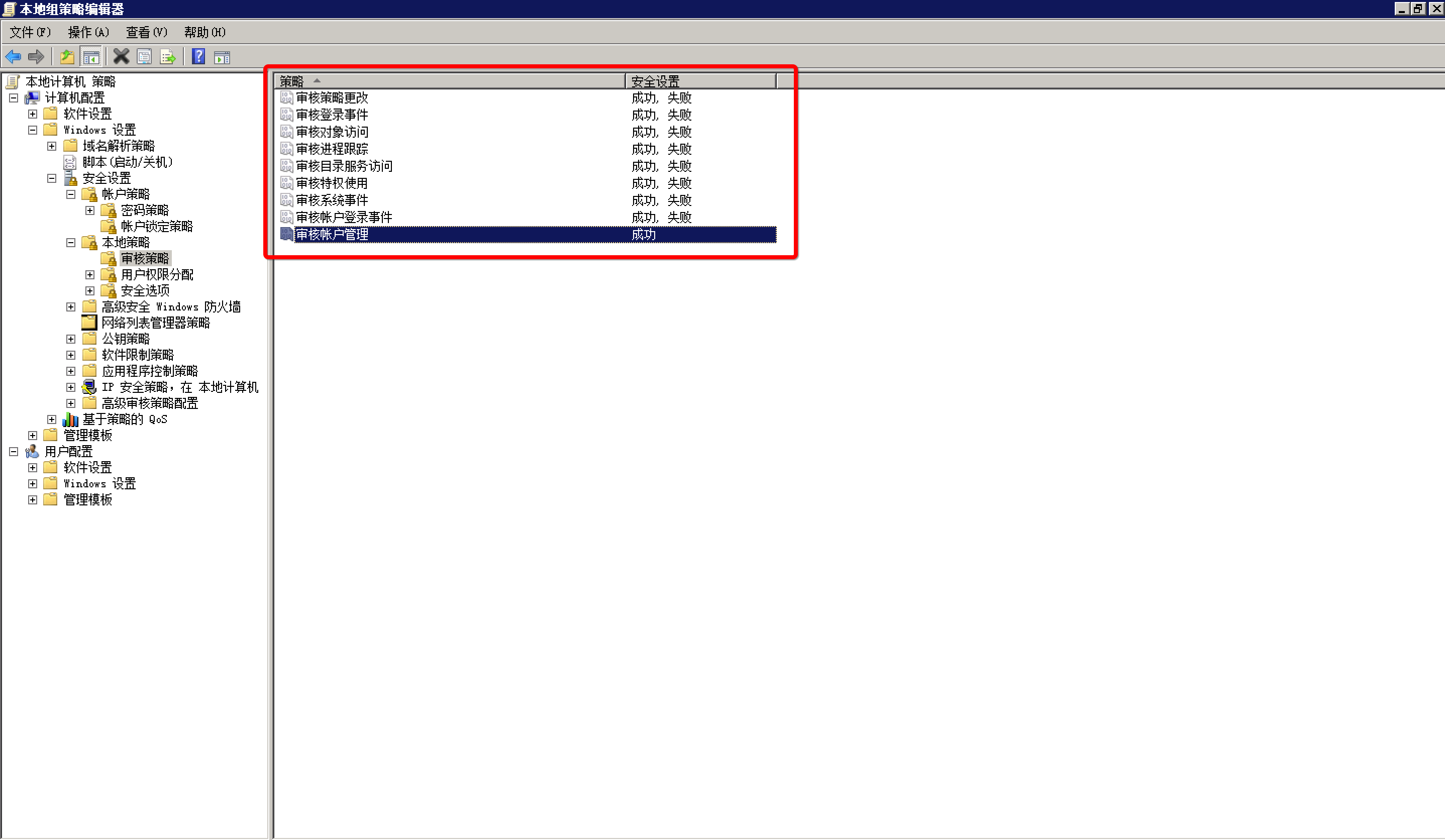
8. 审核过程追踪

实施目的：启用组策略中对Windows系统的审核过程追踪失败。

加固方法：

进入“控制面板->管理工具->本地安全策略”，在“本地策略->审核策略”中：“审核过程追踪”设置。

参考配置：



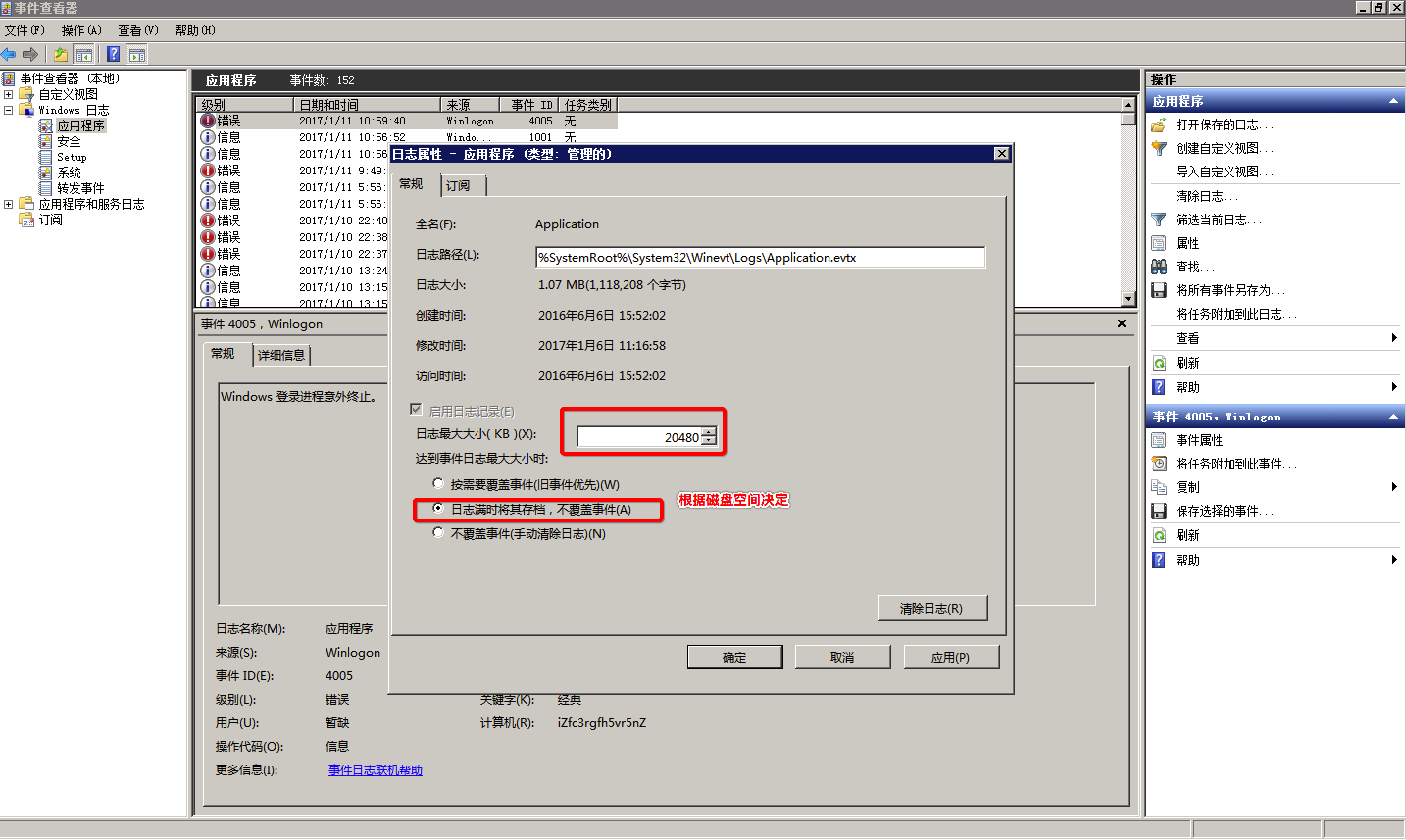
9. 日志文件大小

实施目的：设置应用日志文件大小至少为8192KB，可以根据磁盘空间配置日志文件大小，尽可能的记录的日志越多越好，设置当达到最大的日志尺寸时，按需要轮询记录日志。

加固方法：

进入“控制面板->管理工具->事件查看器”，在“事件查看器（本地）”中：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。

参考配置：



### IP协议安全配置

1. 启用SYN攻击保护

实施目的：启用SYN攻击保护。

加固方法：

在“开始->运行->键入regedit”，推荐值配置：

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; 推荐值数据：500。

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TcpMaxHalfOpenRetried。推荐值数据：400。

### 文件权限

1. 关闭默认共享

实施目的：非域环境中，关闭Windows硬盘默认共享，例如C$，D$。

加固方法：

进入“开始－>运行－>Regedit”，进入注册表编辑器，推荐值配置：

HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer 键，值为 0。

2. 共享文件夹授权访问

实施目的：每个共享文件夹的共享权限，只允许授权的帐户拥有权限共享此文件夹。

加固方法：

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”。进入“控制面板->管理工具->计算机管理”，进入“系统工具－>共享文件夹”：查看每个共享文件夹的共享权限。

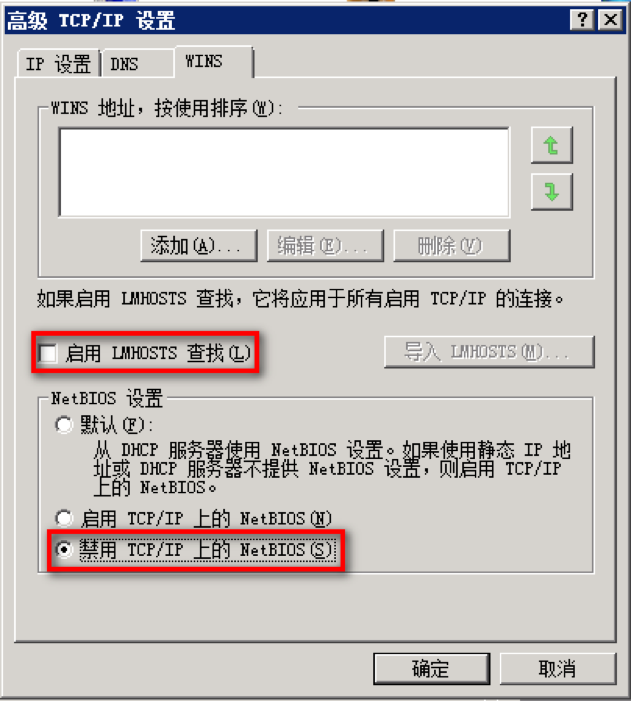
### 服务安全

1. 审核过程追踪

实施目的：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。

加固方法：

在系统服务里禁用“TCP/IP NetBIOS Helper”服务。打开网络连接属性“Internet协议版本4（TCP/IPv4）”，点击“高级”，在“WINS”选项卡里，设置如下：

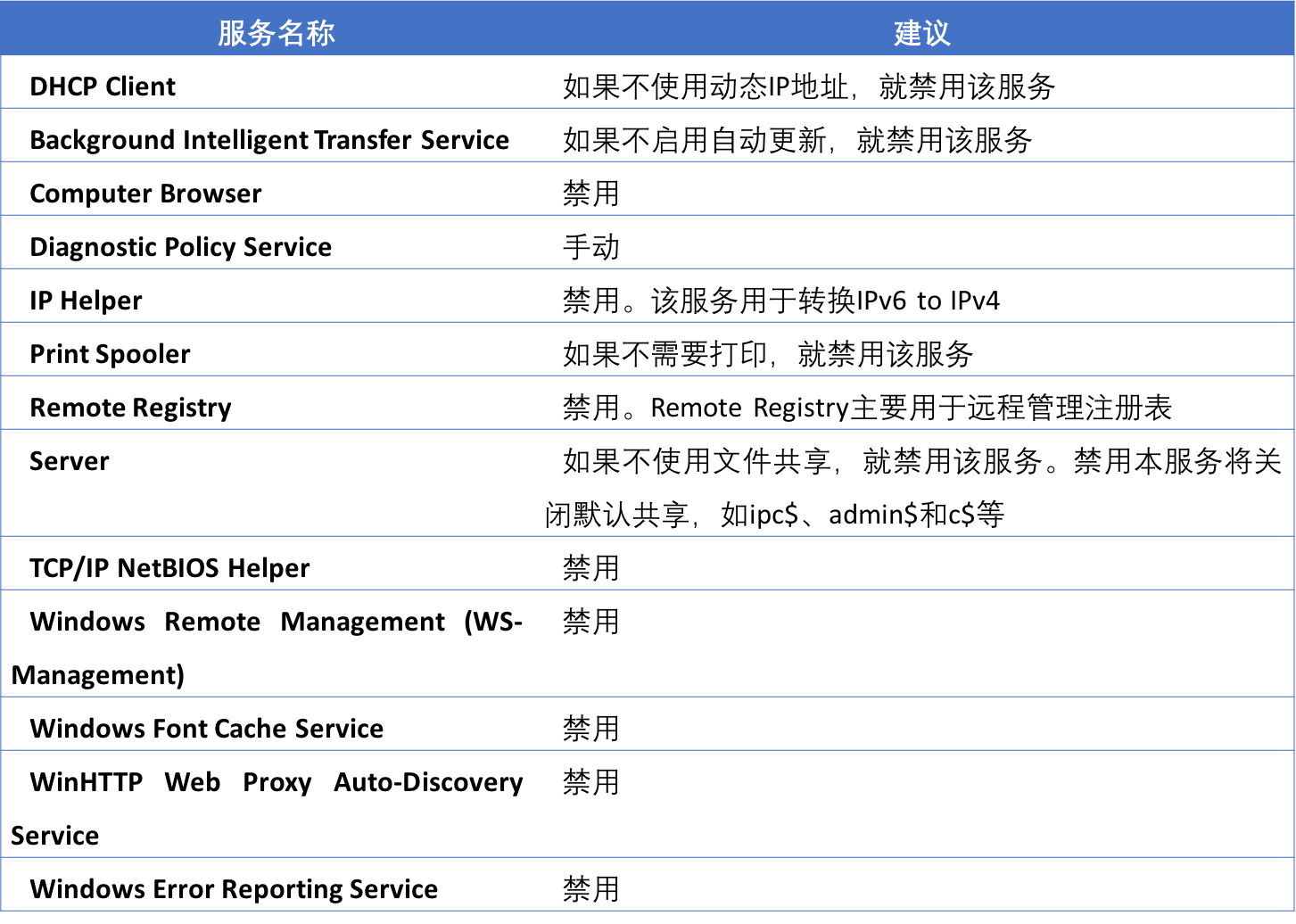


2. 禁用不必要的服务

实施目的：关闭不必要的服务。

加固方法：

建议关闭的服务：



### 安全选项

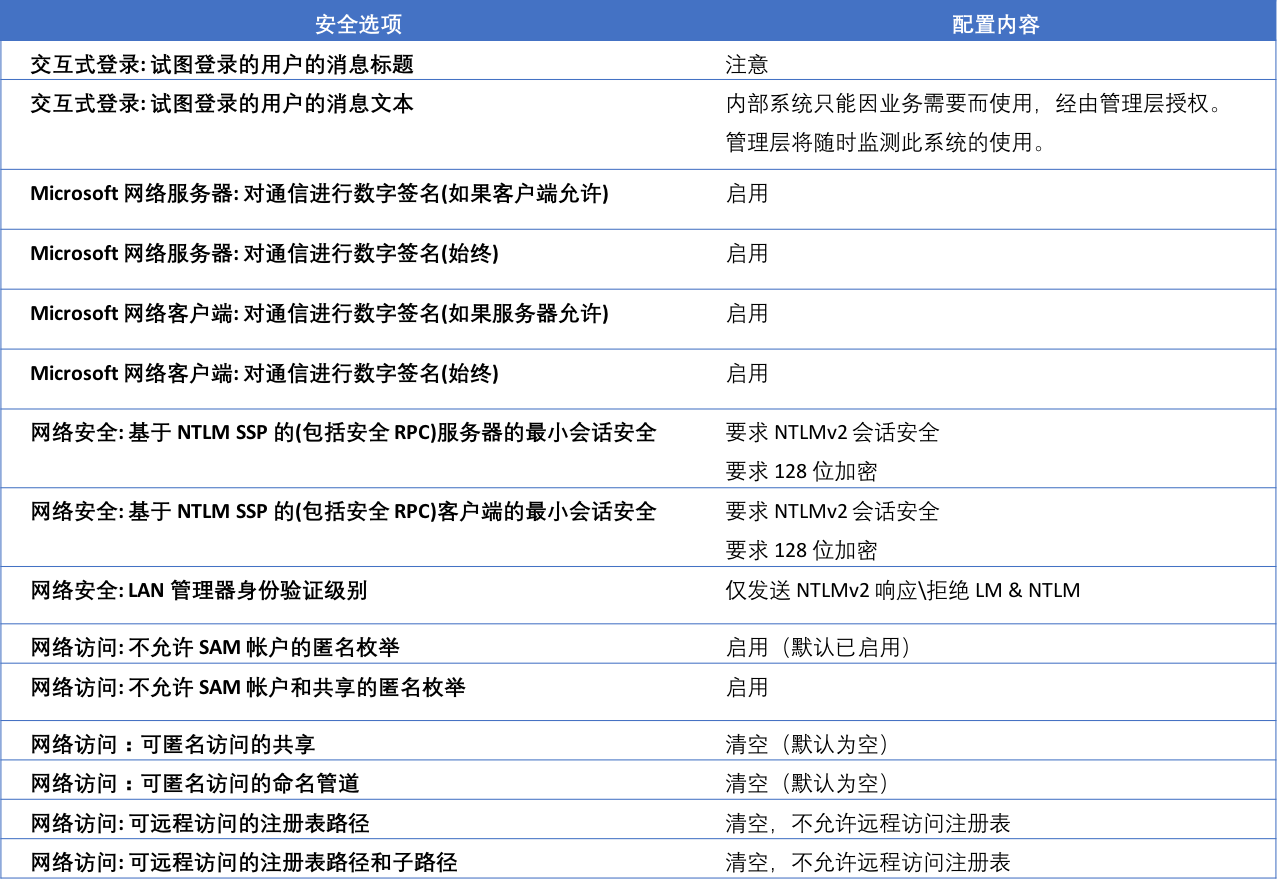
1. 启用安全选项

实施目的：禁启用安全选项。

加固方法：

“本地安全策略”——“安全设置”——“本地策略”——“安全选项”，找到对应的项配置。

参考配置：



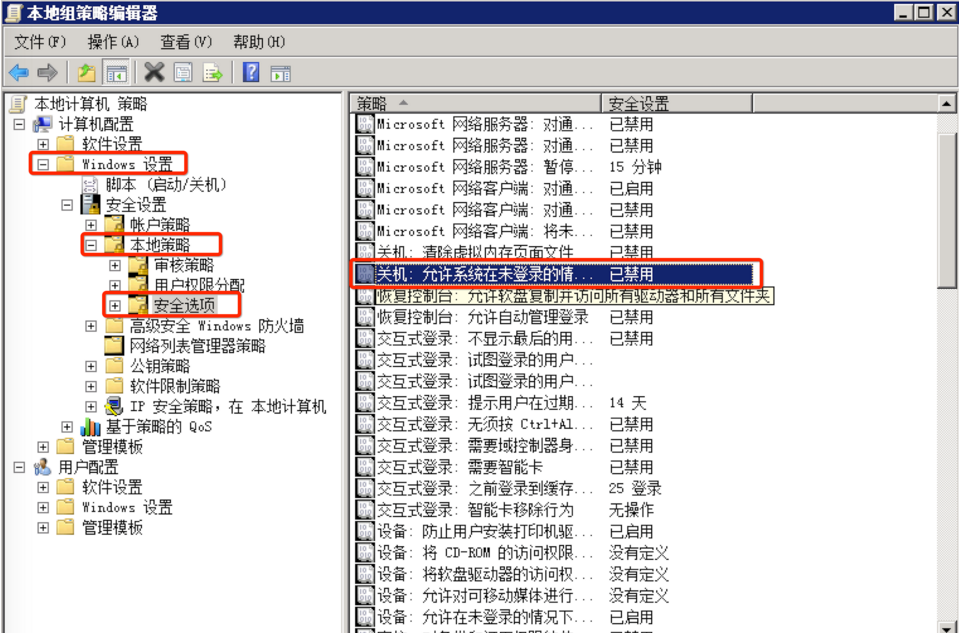
2. 禁用未登录前关机

实施目的：服务器默认是禁止显示在开机未进入系统前的，如果启用此设置，那么服务器安全性就大大降低，给与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。

加固方法：

开始—运行—输入gpedit.msc，打开组策略，然后点击 计算机配置—windows设置—本地策略—安全选项——关机: 允许系统在未登录前关机。

参考配置：



### 其他安全配置

1. 防病毒管理

实施目的：Windows系统需要安装防病毒软件。

加固方法：

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。

2. 设置屏幕保护密码和开启时间

实施目的：设置带密码的屏幕保护，并将时间设定为5分钟。

加固方法：

启用屏幕保护程序，设置等待时间为“5分钟”，启用“在恢复时使用密码保护”。进入“控制面板－>显示－>屏幕保护程序”：查看是否启用屏幕保护程序，设置等待时间为“5分钟”，启用“在恢复时使用密码保护”。

3. 限制远程登陆空闲断开时间

实施目的：对于远程登陆的帐号，设置不活动断连时间15分钟。

加固方法：

“Microsoft网络服务器”设置为“在挂起会话之前所需的空闲时间”为15分钟。进入“控制面板->管理工具->本地安全策略”，在“本地策略->安全选项”：查看是否“Microsoft网络服务器”设置为“在挂起会话之前所需的空闲时间”为15分钟。

4. 操作系统补丁管理

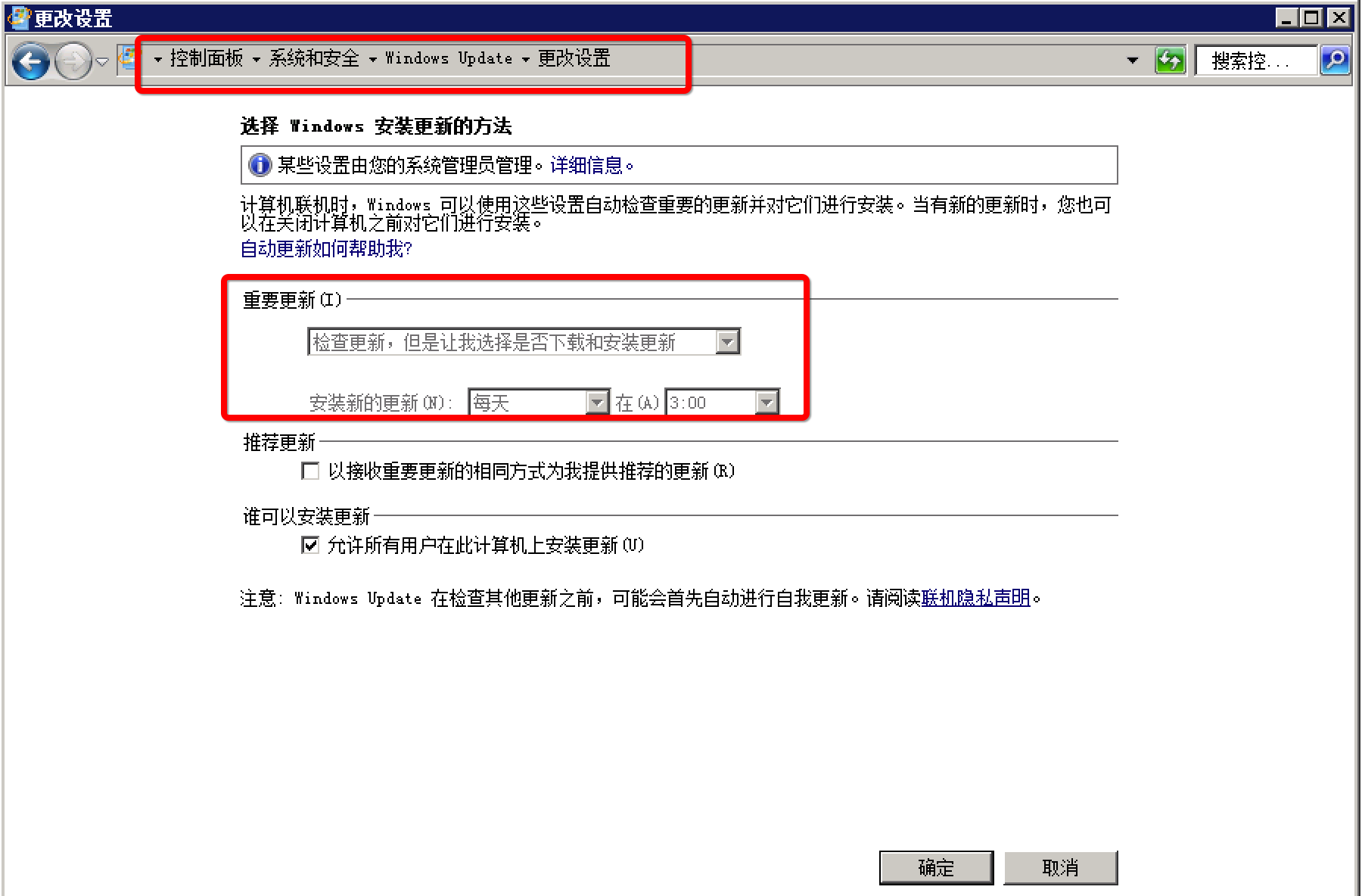
实施目的：安装最新的Hotfix补丁。对服务器系统应先进行兼容性测试。

加固方法：

安装最新的Hotfix补丁。对服务器系统应先进行兼容性测试。

注意：对于生产服务器，建议通知并自动下载更新，但是由管理员选择是否安装更新，而不应自动安装更新，防止自动更新补丁对生产环境产生影响。

参考配置：



## Linux安全加固

### 账号管理和认证授权

1. 为不同的管理员分配不同的账号

实施目的：根据不同类型用途设置不同的帐户账号，提高系统安全。

加固方法：

为用户创建账号：

#useradd username #创建账号

#passwd username #设置密码

修改权限：

#chmod 750 directory #其中 755 为设置的权限，可根据实际情况设置相应的权限， directory 是要更改权限的目录)使用该命令为不同的用户分配不同的账号，设置不同的口令及权限信息等。

2. 去除不需要的帐号-修改默认帐号的 shell 变量

实施目的：删除系统不需要的默认帐号、更改危险帐号缺省的shell变量。

加固方法：

# userdel lp

# groupdel lp

如果下面这些系统默认帐号不需要的话，建议删除。

lp, sync, shutdown, halt, news, uucp, operator, games, gopher

修改一些系统帐号的 shell 变量，例如 uucp,ftp 和 news 等，还有一些仅仅需要 FTP 功能的帐号，一定不要给他们设置/bin/bash 或者/bin/sh 等 Shell 变量。可以在/etc/passwd 中将它们的 shell 变量设为/bin/false 或者/dev/null 等，也可以使用usermod -s /dev/null username 命令来更改 username 的 shell为/dev/null。

3. 限制超级管理员远程登录

实施目的：限制具备超级管理员权限的用户远程登录。远程执行管理员权限操作，应先以普通权限用户远程登录后，再切换到超级管理员权限账。

加固方法：

参考配置

SSH:

#vi /etc/ssh/sshd\_config

把PermitRootLogin yes改为PermitRootLogin no

重启 sshd 服务

#service sshd restart

CONSOLE:

在/etc/securetty文件中配置：CONSOLE = /dev/tty01

4. 对系统账号进行登录限制

实施目的：对系统账号进行登录限制，确保系统账号仅被守护进程和服务使用。

加固方法：

参考配置

Vi /etc/passwd

例如修改

lynn:x:500:500::/home/lynn:/sbin/ bash

更改为：

lynn:x:500:500::/home/lynn:/sbin/nologin

该用户就无法登录了。

禁止所有用户登录。

touch /etc/nologin

除 root 以外的用户不能登录了。

补充：

禁止交互登录的系统账号，比如 daemon,bin,sys、 adm、 lp、

uucp、nuucp、smmsp 等等

5. 为空口令用户设置密码

实施目的：禁止空口令用户，存在空口令是很危险的，用户不用口令认证就能进入系统。

加固方法：

awk -F: '($2 == ""){print $1}' /etc/passwd

用 root 用户登陆 Linux 系统，执行 passwd 命令，给用户增加口令。

例如：passwd test test。

6. 帐号与口令检查

实施目的：检查是否存在除 root 之外 UID 为 0 的用户。

加固方法：

删除除了root以外的 UID为0的用户。

7. 缺省密码长度限制

实施目的：防止系统弱口令的存在，减少安全隐患。对于采用静态口令认证技术的设备，口令长度至少8位。

加固方法：

参考配置

# vi /etc/login.defs

把下面这行

PASS\_MIN\_LEN 5 改为

PASS\_MIN\_LEN 8

8. 缺省密码生存周期限制

实施目的：对于采用静态口令认证技术的设备，帐户口令的生存期不长于 90 天，减少口令安全隐患。

加固方法：

参考配置

运行 cat /etc/login.defs 查看状态，并记录。

PASS\_MAX\_DAYS 90

PASS\_MIN\_DAYS 0

9. 口令过期提醒

实施目的：口令到期前多少天开始通知用户口令即将到期。

加固方法：

参考配置操作

运行 cat /etc/login.defs 查看状态，并记录。

PASS\_WARN\_AGE 7

10. 设置关键目录的权限

实施目的：在设备权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

加固方法：

参考配置操作

通过 chmod 命令对目录的权限进行实际设置。

补充说明

etc/passwd 必须所有用户都可读， root 用户可写–rw-r—r—

/etc/shadow 只有 root 可读 –r--------

/etc/group 必须所有用户都可读， root 用户可写–rw-r—r—

使用如下命令设置：

chmod 644 /etc/passwd

chmod 600 /etc/shadow

chmod 644 /etc/group

如果是有写权限，就需移去组及其它用户对/etc 的写权限

（特殊情况除外）

执行命令#chmod -R go-w /etc

11. 修改umask值

实施目的：控制用户缺省访问权限，当在创建新文件或目录时，屏蔽掉新文件或目录不应有的访问允许权限。防止同属于该组的其它用户及别的组的用户修改该用户的文件或更高限制。

加固方法：

参考配置操作

more /etc/profile

more /etc/csh.login

more /etc/csh.cshrc

more /etc/bashrc

检查是否包含 umask 值

设置默认权限：

vi /etc/profile

vi /etc/csh.login

vi /etc/csh.cshrc

vi /etc/bashrc

在末尾增加 umask 027

修改文件或目录的权限，操作举例如下：

#chmod 444 dir ; #修改目录 dir 的权限为所有人都为只读。

根据实际情况设置权限；

补充说明

如果用户需要使用一个不同于默认全局系统设置的 umask，可以在需要的时候通过命令行设置，或者在用户的 shell 启动文件中配置。

umask 的默认设置一般为 022，这给新创建的文件默认权限755（777-022=755），这会给文件所有者读、写权限，但只给组成员和其他用户读权限。

umask 的计算：

umask 是使用八进制数据代码设置的，对于目录，该值等于八进制数据代码 777 减去需要的默认权限对应的八进制数据代码值；对于文件，该值等于八进制数据代码 666 减去需要的默认权限对应的八进制数据代码值。

12. 资源限制

实施目的：限制用户对系统资源的使用，可以避免拒绝服务（如：创建很多进程、消耗系统的内存，等等）这种攻击方式。这些限制必须在用户登录之前设定。

加固方法：

参考配置

第一步

编辑“limits.conf”文件（vi /etc/security/limits.conf），加入或改变下面

这些行：

\* soft core 0

\* hard core 0

\* hard rss 5000

\* hard nproc 20

如果限制 limitu 用户组对主机资源的使用，

加入：

@limitu soft core 0

@limitu hard nproc 30

@limitu - maxlogins 5

这些行的的意思是：“core 0”表示禁止创建 core 文件；“nproc 20”把最多进程数限制到 20；“rss 5000”表示除了 root 之外，其他用户都最多只能用 5M 内存。上面这些都只对登录到系统中的用户有效。通过上面这些限制，就能更好地控制系统中的用户对进程、core 文件和内存的使用情况。星号“\*”表示的是所有登录到系统中的用户。

第二步

必须编辑“/etc/pam.d/login”文件，在文件末尾加入

下面这一行：

session required /lib/security/pam\_limits.so

补充说明：

加入这一行后“/etc/pam.d/login”文件是这样的：

#%PAM-1.0

auth required /lib/security/pam\_securetty.so

auth required /lib/security/pam\_pwdb.so shadow nullok

auth required /lib/security/pam\_nologin.so

account required /lib/security/pam\_p wdb.so

password required /lib/security/pam\_cracklib.so

password required /lib/security/pam\_pwdb.so nullok

use\_authtok md5 shadow

session required /lib/security/pam\_pwdb.so

session required /lib/security/pam\_limits.so

#session optional /lib/security/pam\_con sole.sodaemon

统计进程数量

ps ax | grep httpd | wc -l

13. 设置目录权限

实施目的：设置目录权限，防止非法访问目录。

加固方法：

参考配置

查看重要文件和目录权限：ls –l

更改权限：

对于重要目录，建议执行如下类似操作：

# chmod -R 750 /etc/init.d/\*

这样只有 root 可以读、写和执行这个目录下的脚本。

14. 设置关键文件的属性

实施目的：增强关键文件的属性，减少安全隐患，使 messages 文件只可追加，使轮循的 messages 文件不可更改。

加固方法：

参考配置

# chattr +a /var/log/messages

# chattr +i /var/log/messages.\*

# chattr +i /etc/shadow

# chattr +i /etc/ passwd

# chattr +i /etc/ group

建议管理员对关键文件进行特殊设置（不可更改或只能追加等）。

15. 为ls、rm设置别名

实施目的：为 ls 设置别名使得 root 可以清楚的查看文件的属性（包括不可更改等特殊属性），为 rm 设置别名使得 root 在删除文件时进行确认，避免误操作。

加固方法：

参考配置

查看当前 shell：

# echo $SHELL

如果是 csh：

# vi ~/.cshrc

如果是 bash：

# vi ~/.bashrc

加入

alias ls ls -aol

alias rm rm -i

重新登录之后查看是否生效。

16. 使用PAM禁止任何人su为root

实施目的：避免任何人可以 su 为 root，减少安全隐患。

加固方法：

参考配置

编辑su文件(vi /etc/pam.d/su)，在开头添加下面两行：

auth sufficient /lib/security/pam\_rootok.so

auth required /lib/security/pam\_wheel.so group= wheel

这表明只有wheel组的成员可以使用su命令成为root用户。

可以把用户添加到wheel组，以使它可以使用su命令成为root 用户。添加方法为：

# chmod –G10 username

17. 查看/tmp目录属性

实施目的：开放 tmp 目录的权限。

加固方法：

参考配置

Chmod +t /tmp

T或T（Sticky）：/tmp 和/var/tmp目录供所有用户暂时存取文件，亦即每位用户皆拥有完整的权限进入该目录，去浏览、删除和移动文件。

### 日志配置

1. 启用日志记录功能

实施目的：登陆认证服务记录。

加固方法：

参考配置

cat /etc/syslog.conf

# The authpriv file has restricted access.

authpriv.\* /var/log/secure

\* auth, authpriv：主要认证有关机制，例如 telnet, login, ssh 等需要认证的服务都是使用此一机制。

2. 记录系统安全事件

实施目的：通过设置让系统记录安全事件，方便管理员分析。

加固方法：

参考配置

修改配置文件 vi /etc/syslog.conf，

配置如下类似语句：

\*.err;kern.debug;daemon.notice; /var/adm/message s

定义为需要保存的设备相关安全事件。

3. 对ssh、su登录日志进行记录

实施目的：对ssh、su登录日志进行记录。

加固方法：

参考配置操作

# vi /etc/syslog.conf

加入

# The authpriv file has restricted access.

authpriv.\* /var/log/secure

重新启动 syslogd：

# /etc/rc.d/init.d/syslog restart

4. 启用记录 cron 行为日志功能

实施目的：对所有的 cron 行为进行审计。

加固方法：

参考配置操作

Vi /etc/syslog.conf

# Log cron stuff

cron.\* /var/log/cron

5. 增加ftpd审计功能

实施目的：增加 ftpd 审计功能，增强 ftpd 安全性。

加固方法：

参考配置操作

# vi /etc/inetd.conf

ftp stream tcp nowait root /usr/libexec/ftpd

ftpd -l -r -A -S

其中：

-l 成功/失败的 ftp 会话被 syslog 记录

-r 使 ftpd 为只读模式，任何命令都不能更改文件系统

-A 允许 anonymous 用户登录， /etc/ftpwelcome 是欢迎信息

-S 对 anonymous ftp 传输进行记录

在/etc/syslog.conf 中，增加

ftp.\* /var/log/ftpd

使日志产生到/var/log/ftpd 文件

重新启动 inetd 进程：

# kill -1 `cat /var/run/inetd.pid`

### 1.2.3协议安全

1. 设置访问控制列表

实施目的：设置访问控制列表，使得只有可信主机才能访问服务器在/etc/(x)inetd.conf 中启用的特定网络服务。

加固方法：

参考配置

使用 TCP\_Wrappers 可以使系统安全面对外部入侵。最好的策略就是阻止所有的主机（在“/etc/hosts.deny”文件中加入“ ALL:ALL@ALL, PARANOID ”），然 后 再 在“/etc/hosts.allow”文件中加入所有允许访问的主机列表。

第一步： 编辑 hosts.deny 文件（vi /etc/hosts.deny），加入下面该行：

# Deny access to everyone.

ALL: ALL@ALL, PARANOID

第二步： 编辑 hosts.allow 文件（vi /etc/hosts.allow），加入允许访问的主机列表，如：

ftp: 202.54.15.99 foo.com

202.54.15.99 和 foo.com 是允许访问 ftp 服务的 IP 地址和主机名称。

第三步：tcpdchk 程序是 TCP\_Wrapper 设置检查程序。它用来检查你的 TCP\_Wrapper 设置，并报告发现的潜在的和真实的问题。设置完后，运行下面这个命令：

# tcpdchk

2. 更改主机解析地址的顺序

实施目的：更改主机解析地址的顺序，减少安全隐患。

加固方法：

“/etc/host.conf”说明了如何解析地址。编辑“/etc/host.conf”文件（ vi /etc/host.conf ）， 加入下面该行：

# Lookup names via DNS first then fall back to /etc/ho sts.

order bind,hosts

# We have machines with multiple IP addresses.

multion

# Check for IP address spoofing

nospoof on

第一项设置首先通过 DNS 解析 IP 地址，然后通过 hosts 文件解析。

第二项设置检测是否“/etc/hosts”文件中的主机是否拥有多个 IP 地址（比如有多个以太口网卡）。

第三项设置说明要注意对本机未经许可的 IP 欺骗。

3. 打开syncookie

实施目的：打开 syncookie缓解syn flood攻击

加固方法：

# echo 1 > /proc/sys/net/ipv4/tcp\_syncookies

可以加入/etc/rc.d/rc.local 中。

4. 不响应ICMP请求

实施目的：不响应 ICMP 请求,避免信息泄露。

加固方法：

不响应ICMP请求：

# echo 1 > /proc/sys/net/ipv4/icmp\_echo\_ignore\_all

5. 防syn攻击优化

实施目的：提高未连接队列大小。

加固方法：

参考配置

sysctl -w net.ipv4.tcp\_max\_syn\_backlog="2048"

### 1.2.4其他安全配置

1. 关闭无效服务

实施目的：关闭无效的服务，提高系统性能，增加系统安全性。

加固方法：

参考配置操作

取消所有不需要的服务，编辑“/etc/inetd.conf”文件，通过注释取消所有你不需要的服务（在该服务项目之前加一个“#”）。

第一步： 更改“/etc/inetd.conf”权限为 600，只允许 root 来读写该文件。

# chmod 600 /etc/inetd.conf

第二步： 确定“/etc/inetd.conf”文件所有者为 root。

# chown root /etc/inetd.conf

第三步： 编辑 /etc/inetd.conf 文件（vi /etc/inetd.conf），取消不需要的服务，如：ftp, telnet, shell, login, exec, talk, ntalk, imap, pop-2, pop-3, finger, auth 等等。把不需要的服务关闭可以使系统的危险性降低很多。

第四步： 给 inetd 进程发送一个 HUP 信号：

# killall -HUP inetd

第五步： 用 chattr 命令把/ec/inetd.conf 文件设为不可修改。

# chattr +i /etc/inetd.conf

/etc/inetd.conf 文件中只开放需要的服务。

对于启用的网络服务，使用 TCP Wrapper 增强访问控制和日志审计功能。

建议使用 xinetd 代替 inetd，前者在访问控制和日志审计方面有较大的增强。这样可以防止对inetd.conf的任何修改（以外或其他原因）。唯一可以取消这个属性的只有root。如果要修改inetd.conf文件，首先要取消不可修改属性：

# chattr -i /etc/inetd.conf

portmap（如果启动使用 nfs 等需要 rpc 的服务，建议关闭portmap 服务

cups 服务（Common Unix Printing Service，用于打印，建议关闭）

named 服务（除非主机是 dns 服务器，否则关闭 named 服务）

apache（http）服务

xfs（X Font Service）服务

vsftpd

lpd

linuxconf

identd

smb

2. 关闭无效服务和进程自动启

实施目的：禁止系统不需要启动的服务，减少安全隐患。防止黑客获取更多的系统信息。

加固方法：

参考配置

进入相应目录，将脚本开头大写S改为小写s即可。如：

# cd /etc/rc.d/rc6.d

# mv S45dhcpd s45dhcpd

3. 禁止/etc/rc.d/init.d 下某些脚本的执行

实施目的：禁止系统开机时不需要启动的服务，减少安全隐患。防止黑客获取更多的系统信息。

加固方法：

参考配置操作

# cd /etc/rc.d/init.d

在不需要开机自动运行的脚本第一行写入 exit 0。则开机时该脚本 exit 0 之后的内容不会执行。需要更改的服务包括：

identd lpd linuxconf netfs

portmap routed rstatd

rwalld rwhod

sendmail ypbind yppasswdd ypserv

具体操作时根据主机的角色请于管理员确认后再实施。

4. 加固 snmp 服务

实施目的：减少安全隐患避免信息泄露

加固方法：

参考配置

chkconfig snmpd off

chkconfig snmptrapd off

/etc/rc.d/init.d/snmpd stop

/etc/rc.d/init.d/snmptrapd stop

如果需要 SNMP 服务

如下方式修改/etc/snmp/snmpd.conf 文件

A、修改默认的 community string

com2sec notConfigUser default public

将 public 修改为你才知道的字符串

B、把下面的#号去掉

#view mib2 included .iso.org.dod.internet.mgmt.mib -2 fc

C、把下面的语句

access notConfigGroup "" any noauth exact systemview none none

改成：

access notConfigGroup "" any noauth exact mib2 none none

重启 snmpd 服务

#/etc/rc.d/init.d/snmpd restart

5. 修改ssh端口

实施目的：隐藏ssh信息

加固方法：

V i /etc/ssh/sshd\_config

修改 Port 22 修改成其他端口，迷惑非法试探者

Linux下SSH默认的端口是 22,为了安全考虑，现修改SS的端口为1433,修改方法如下：

/usr/sbin/sshd -p 1433

6. 隐藏系统提示信息

实施目的：减少系统提示信息，降低安全隐患。

加固方法：

参考配置

在缺省情况下，当你登录到 linux 系统，它会告诉你该 linux发行版的名称、版本、内核版本、服务器的名称。应该尽可能的隐藏系统信息。

首先编辑“/etc/rc.d/rc.local ” 文件，在下面显示的这些行前加一个“#”，把输出信息的命令注释掉。

# This will overwrite /etc/issue at every boot. So, make

any changes you want to make to /etc/issue here or you

will lose them when you reboot.

#echo "" > /etc/issue

#echo "$R" >> /etc/issue

#echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue

#cp -f /etc/issue /etc/issue.net

#echo >> /etc/issue

其次删除"/etc"目录下的 isue.net 和 issue 文件：

# mv /etc/issue /etc/issue.bak

# mv /etc/issue.net /etc/issue.net.bak

7. 设置登录超时时间

实施目的：对于具备字符交互界面的设备，应配置定时帐户自动登出。

加固方法：

参考配置

在 unix 系统中 root 账户是具有最高特权的。如果系统管理员在离开系统之前忘记注销 root 账户，那将会带来很大的安全隐患，应该让系统自动注销。通过修改账户中“TMOUT”

参数，可以实现此功能。TMOUT 按秒计算。编辑 profile 文件（vi /etc/profile ），在“HISTFILESIZE= ”后面加入下面这行：

TMOUT=180

表示 180 秒，也就是表示 3 分钟。这样，如果系统中登录的用户在 3 分钟内都没有动作，那么系统会自动注销这个账户。也可以在个别用户的“.bashrc”文件中添加该值，以便系

统对该用户实行特殊的自动注销时间。改变这项设置后，必须先注销用户，再用该用户登录才能激活这个功能。

8. 启动LILO时需要密码

实施目的：password 用于系统启动时应当输入密码；restricted 用于命令行启动系统时（如：进入单用户模式）需要输入密码。

加固方法：

参考配置

第一步：编辑 lilo.conf 文件（vi /etc/lilo.conf），加入或改变这三个参数（加#的部分）：

boot=/dev/hda

prompt

timeout=00 # 把该行改为 00，系统启动时将不再等待，而直接启动 LINUX

message=/boot/message

linear

default=linux

restricted # 加入该行

password= lilopassforbocotest # 加入该行并设置自己的密码（明文）

image=/boot/vmlinuz-2.4.18

label=linux

root=/dev/hda6

read-only

第二步：因为“/etc/lilo.conf”文件中包含明文密码，所以要把它设置为 root 权限读取。

# chmod 0600 /etc/lilo.conf

第三步：更新系统，以便对“/etc/lilo.conf”文件做的修改起作用。

# /sbin/lilo -v

第四步：使用“chattr”命令使“/etc/lilo.conf”文件不可改变。 # chattr +i /etc/lilo.conf

这样可以在一定程度上防止对“/etc/lilo.conf”任何改变（意外或其他原因）最后将/etc/lilo.conf 文件权限改为 600

# chmod 600 /etc/lilo.conf

补充说明

通过对“/etc/lilo.conf”加 i 属性使文件不可更改。如果要对文件作修改的话，先去掉 i 属性，即# chattr -i /etc/lilo.conf为 LILO 设置密码不能防止黑客从软盘、CD-ROM 启动系统、加载根分区，需要在 BIOS 中设置密码。

9. 查找SUID/SGID程序

实施目的：去除不必要的SUID/SGID权限

加固方法：

参考配置

给文件加 SUID 和 SUID 的命令如下：

chmod u+s filename 设置 SUID 位

chmod u-s filename 去掉 SUID 设置

chmod g+s filename 设置 SGID 位

chmod g-s filename 去掉 SGID 设置

补充说明

suid 是 4000，sgid 是 2000，sticky 是 1000

比如 rwsr-xr-x 就是 4755

SUID 是 Set User ID, SGID 是 Set Group ID 的意思。

SUID 的程序在运行时，将有效用户 ID 改变为该程序的所有者 ID，使得进程在很大程度上拥有了该程序的所有者的特权。如果被设置为 SUID root，那么这个进程将拥有超级用

户的特权(当然，一些较新版本的 UNIX 系统加强了这一方面的安全检测，一定程度上降低了安全隐患)。当进程结束时，又恢复为原来的状态。

10. 查找/dev下的非设备文件

实施目的：查找/dev下的非设备文件

加固方法：

参考配置

find /dev -type f -exec ls -l {} \;

记录可以文件

11. 查找非/dev下的设备文件

实施目的：查找非/dev下的设备文件

加固方法：

参考配置

find / -type b -print | grep -v '^/dev/'

find / -type c -print | grep -v '^/dev/'

12. 查找所有人可写的文件

实施目的：查找所有人可写的文件

加固方法：

参考配置

find / -perm -2 ! -type l –ls

find / -type d \( -perm -002 -o -perm -020 \) -ls

13. 查找没有属主的文件

实施目的：查找没有属主的文件

加固方法：

参考配置

find / -nouser -o -nogroup -print

14. 查找 rhosts 文件

实施目的：查找 rhosts 文件

加固方法：

参考配置

find / -name .rhosts -print

补充说明

远程登录（rlogin）是一个 UNIX 命令，它允许授权用户进入网络中的其它 UNIX 机器并且就像用户在现场操作一样。一旦进入主机，用户可以操作主机允许的任何事情，比如：

读文件、编辑文件或删除文件等。rlogin 设计的初衷是方便同名的用户从一台机器直接登录到另一台机器。比如机器 A 上有用户 test1，机器 B 上该用户也有一个同名账号 test1, 如果机器 B 上设置好.rhosts 的话就 test1 就可以从机器 A 上直接登录机器 B。通常在配 HA 的时候，会将+放进/.rhosts，因为这样做同步的时候就会比较方便，但记得在配置完的时候，把这个+去掉。

15. 查找 netrc 文件

实施目的：查找 netrc 文件

加固方法：

参考配置

find / -name .netrc -print

补充说明

有些 命令通过检查 $HOME/.netrc 文件（包含远程主机上使用的用户名和密码）来提供自动登录的功能。如果没有远程主机的 $HOME/.netrc 文件中的有效项，将提示输入登录标识和密码。

16. 文件系统-检查异常隐含文件

实施目的：文件系统-检查异常隐含文件

加固方法：

find / -name ".. \*" –print

补充说明

在系统的每个地方都要查看一下有没有异常隐含文件（点号是起始字符的，用“ls”命令看不到的文件） 。在 UNIX 下，一个常用的技术就是用一些特殊的名，如：“„”、“.. ”

（点点空格）或“..^G”（点点 control-G），来隐含文件或目录。

# Web中间件安全加固

## Tomcat安全加固

1. 删除文档和示例程序

实施目的：删除文档和示例程序，防止泄露敏感信息。

加固方法：

在tomcat安装目录下找到${tomcat}/webapps文件夹，默认存在docs和examples文件夹，建议删除docs和examples文件夹

1. 检测控制台口令

实施目的：加固tomcat控制台，设置复杂口令，删除无效账户。

加固方法：

1. 默认通过http://ip:8080/manager/html可以访问tomcat manager，如果不需要使用tomcat管理后台，建议删除${tomcat}/webapps/manager和${tomcat}/webapps/host-manager文件夹；

(2) 修改${tomcat}/config/tomcat-users.xml配置文件，删除与工作无关的帐号。

<tomcat-users>

<role rolename="tomcat"/>

<role rolename="role1"/>

<user username="tomcat" password="tomcat" roles="tomcat"/>

<user username="both" password="tomcat" roles="tomcat,role1"/>

<user username="role1" password="tomcat" roles="role1"/>

</tomcat-users>

例如 tomcat 与运行、维护等工作无关，删除该帐号

1. 对于采用静态口令认证技术的设备，口令长度至少 8 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2 类来提升密码复杂度。

在 ${tomcat}/conf/tomcat-user.xml 配置文件中设置密码

<user username=”tomcat” password=”Tomcat!234”

roles=”admin”>

1. 设置SHUTDOWN字符串

实施目的：防止恶意用户telnet到8005端口后，发送SHUTDOWN命令停止tomcat服务。

加固方法：

打开${tomcat}/conf/server.xml，查看是否设置了复杂的字符串

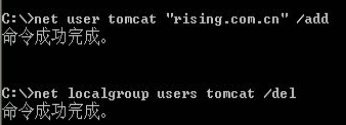
<Server port="8005" shutdown="复杂的字符串"> 防止恶意用户猜测。

1. Tomcat降权

实施目的：在Windows环境下，Tomcat默认以System权限运行，这样的后果是一旦成功入侵WEB应用，将直接得到一个高权限的Webshell，并且不需要提权操作就可以完全控制服务器。

加固方法：

首先新建一个用户，设置复杂的密码，并且让它不属于任何用户组。



接着打开“本地安全策略”--->“本地策略”--->“用户权限分配”，找到“作

为服务登录”项，把刚刚新建的用户添加进去。





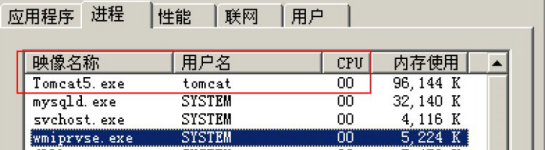
然后打开“服务（service.msc）”组件，找到Tomcat 的服务，右键“属性”--->“登录”，用刚新建的tomcat 帐号运行Tomcat 服务。



再找到Tomcat安装目录，只为“Administrators 组”和“tomcat”帐户分配完全控制权限，并将其他帐户权限全部删除。如果不为tomcat帐户分配权限，Tomcat 服务将无法启动。然后需要以最小权限原则为Tomcat日志目录和WEB目录单独分配权限。日志目录只需要分配“读取”和“写入”权限即可。WEB目录权限分配可依据以下原则：有写入权限，一定不要分配执行权限；有执行权限，一定不要分配写入权限。

网站上传目录和数据库目录一般需要分配“写入”权限，但一定不要分配执行权限。其他目录一般只分配“读取”权限即可。

配置好后，需要重启Tomcat 服务才能生效。



1. 禁止列目录

实施目的：防止直接访问目录时由于找不到默认主页而列出目录下所有文件。

加固方法：

打开应用程序 ${tomcat}/conf/tomcat-user.xml 配置文件，查看listings是否设置为false 。

<init-param>

<param-name>listings</param-name>

<param-value>false</param-value>

</init-param>

1. 启用日志记录

实施目的：数据库应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号、登录是否成功、登录时间以及远程登录时用户使用的 IP 地址。

加固方法：

编辑 ${tomcat}/conf/server.xml 配置文件，在<HOST>标签中增加记录日志功能

将以下内容的注释标记< ! -- -- >取消

<valve

classname=”org.apache.catalina.valves.AccessLogValve”

Directory=”logs” prefix=”localhost\_access\_log.” Suffix=”.txt”

Pattern=”common” resloveHosts=”false”/>

启用access\_log后，重启tomcat，在 ${tomcat}/logs中可以看到访问日志

补充操作说明

classname: This MUST be set to

org.apache.catalina.valves.AccessLogValve to use the default

access log valve. &<60

Directory:日志文件放置的目录，在 tomcat 下面有个 logs 文件夹，那里面是专门放置日志文件的，也可以修改为其他路径；

Prefix: 这个是日志文件的名称前缀，日志名称为localhost\_access\_log.200 8-10-22.txt ， 前面的前缀就是这个localhost\_access\_log；

Suffix: 文件后缀名；

Pattern: common 方式时，将记录访问源 IP、本地服务器 IP、记录日志服务器 IP、访问方式、发送字节数、本地接收端口、访问 URL 地址等相关信息在日志文件中resolveHosts:值为 true 时，tomcat 会将这个服务器 IP 地址通过 DNS 转换为主机名，如果是 false，就直接写服务器 IP 地址。

1. 启用日志记录

实施目的：自定义Tomcat返回的错误信息。

加固方法：

修改应用程序的${tomcat}/conf/web.xml，在最后</web-app>一行之前加入以下内容

1. 表示出现404未找到网页的错误时显示404.html页面

<error-page>

<error-code>404</error-code>

<location>/404.html</location>

</error-page>

<error-page>

<error-code>403</error-code>

<location>/403.html</location>

</error-page>

建议自定义403，404，500错误的页面。

1. 表示出现java.lang.NullPointerException错误时显示 error.jsp页面 <error-page> <exception-type>java.lang.NullPointerException</exception-type>

<location>/ error.jsp</location>

</error-page>

1. 登录超时设置

实施目的：对于具备字符交互界面的设备，应支持定时账户自动登出，登出后用户需再次登录才能进入系统。

加固方法：

编辑 ${tomcat}/conf/server.xml 配置文件，修改为 30 秒

<Connector

port="8080" maxHttpHeaderSize="8192" maxThreads="150"

minSpareThreads="25" maxSpareThreads="75"、

enableLookups="false" redirectPort="8443" acceptCount="100"

connectionTimeout="300" disableUploadTimeout="true" />

## IIS安全加固

1. 关闭并删除默认站点

实施目的：阻止除指定文件外运行，给 Web 服务器带来安全性问题。

加固方法：

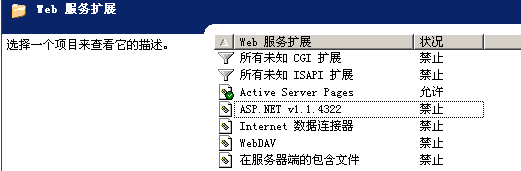
开始->管理工具->Internet 信息服务(IIS)管理器->删除默认 FTP 站点、默认 Web 站点

2. 禁用不必要的Web服务扩展

实施目的：禁用不必要的Web服务扩展，给 Web 服务器带来安全性问题。

加固方法：

开始->管理工具->Internet 信息服务(IIS)管理器，打开IIS 管理器，检查是否有不必要的“Web服务扩展”，如果有则禁用掉。



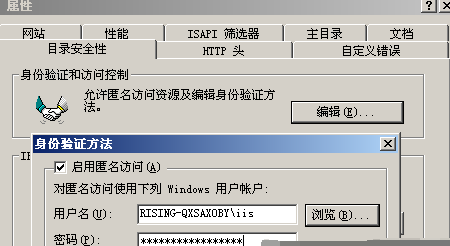
3. IIS访问权限配置

实施目的：IIS中有多个网站，建议为每个网站配置不同的匿名访问账户，提高系统，网站程序安全性。。

加固方法：

开始->管理工具->计算机管理->本地用户和组，新建一个账号，加入Guests组。

开始->管理工具->Internet 信息服务(IIS)管理器，选择网站，选择“属性”->“目录安全性”->“身份验证和访问控制”，把“启用匿名访问”处，用刚新建的账户代替默认账户。



4. 网站目录权限配置

实施目的：通过控制网站权限来提高系统，网站程序安全性。

加固方法：

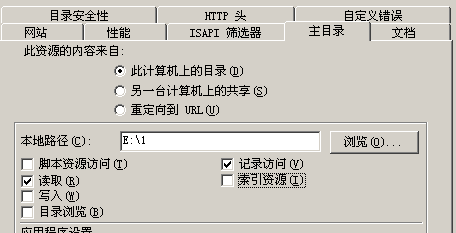
目录有写入权限，一定不要分配执行权限；

目录有执行权限，一定不要分配写入权限；

网站上传目录和数据库目录一般需要分配“写入”权限，但一定不要分配执行权限；

其他目录一般只分配“读取”和“记录访问”权限即可。

开始->管理工具->Internet 信息服务(IIS)管理器，选择网站，选择“属性”->“主目录”，选择相应的权限

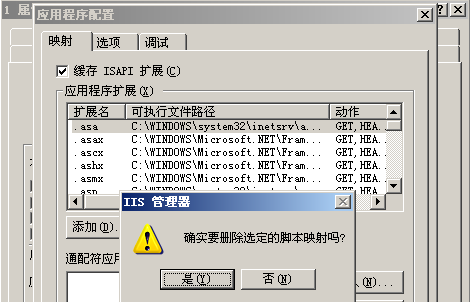


5. 保留必要的应用程序扩展

实施目的：根据网站的实际情况，只保留必要的应用程序扩展，其他的一律删除，如cer、asa这样极其危险的扩展，删除这些高危的拓展提高网站程序安全性。

加固方法：

开始->管理工具->Internet 信息服务(IIS)管理器，选择网站，选择“属性”->“主目录”->“配置”->“映射”选择需要保留的拓展名。



6. 修改IIS日志文件配置

实施目的：当发生安全事件时，我们可以通过分析日志来还原攻击过程，否则将无从查起。加固方法：

检查是否启用了日志记录，如未启用，则启用它。日志格式设置为W3C扩展日志格式，IIS中默认是启用日志记录的。

接着修改IIS日志文件保存路径，默认保存在“C:\WINDOWS\system32\LogFiles”目录下，可以修改为自定义路径。建议保存在非系统盘路径，并且设置IIS日志文件所在目录只允许Administrators组用户和SYSTEM用户访问。

开始->管理工具->Internet 信息服务(IIS)管理器，选择网站，选择“属性”->“网站”->“启用日志记录”->“属性”->“浏览”选择存在日志的文件夹。

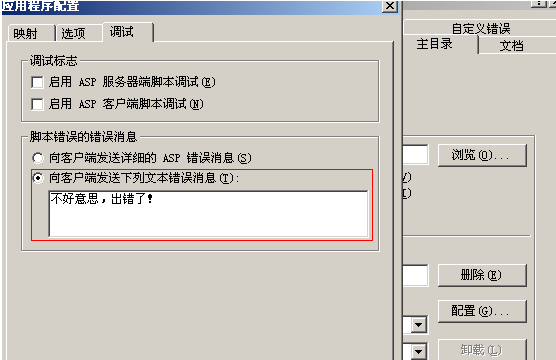
7. 防止信息泄露

实施目的：防止信息泄露，提高网站的安全性。

加固方法：

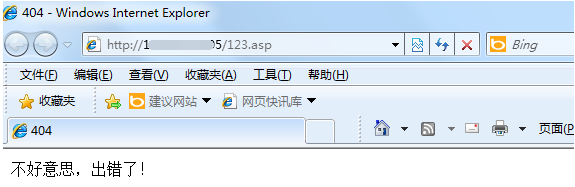
1. 禁止向客户端发送详细的ASP错误信息

“IIS管理器”->“属性”->“主目录”->“配置”->“调试”，选择“向客户端发送下列文本错误消息”项，自定义出错时返回的错误信息。



b. 修改默认错误页面

“IIS管理器”--->“属性”--->“自定义错误”，用自定义的错误页面替换默认的默认页面。下面是我自定义的一个404错误页面，当网站发生404错误时，将向客户端返回这个页面。

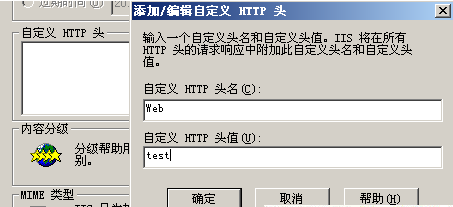


8. 自定义IIS Banner信息

实施目的：默认Banner信息会泄露服务器类型、版本等相关信息，我们需要对其进行修改，这样可以防止信息泄露，还可以骗过一些自动化扫描、攻击工具。

加固方法：

打开“IIS管理器”--->“属性”--->“HTTP头”，在“自定义HTTP头”选中默 认的HTTP头信息，进行编辑，或者删除掉默认的，自己添加一个新的HTTP头信息。

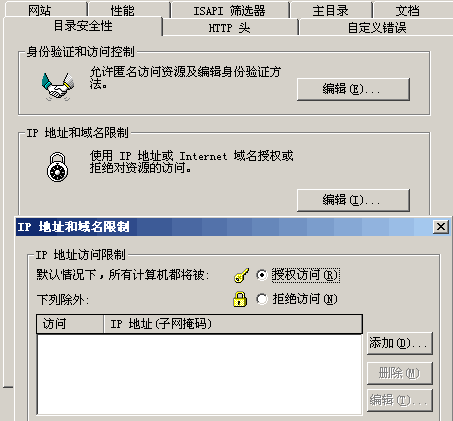


1. IP地址控制

实施目的：阻止非法 IP 访问。

加固方法：

开始->管理工具->Internet 信息服务(IIS)管理器 选择相应的站点，然后右键点击“属性”->目录安全性->ip地址和域名限制->编辑，进行 ip 范围限制。



1. IIS 记录安全事件安全基线要求项

实施目的：设备应配置日志功能，记录与设备相关的安全事件。

加固方法：

(1) 进入“控制面板->管理工具->本地安全策略”， 在“本地策略->审核策略”中配置相应 “审核对象访问”、“审核目录服务器访问”、“审核系统事件”、“审核帐号管理”、“审核过程追踪”选项。

1. 运行 IIS 管理器->“Internet 信息服务”->“应用相关站点”属性->“网站”->“属性”->“高级”，选择“时间”、“日期”、“扩展属性”根据需要进行选择。

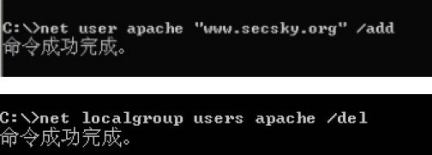
## Apache安全加固

1. Apache降权

实施目的：在Windows环境下，Apache默认以System权限运行，一旦攻击者成功入侵WEB应用，将直接得到一个高权限的Webshell，以特定用户运行服务,不使用系统管理员账号启动 APACHE，来提高系统安全性。

加固方法：

新建一个用户，设置复杂的密码，并且让它不属于任何用户组。



接着打开“本地安全策略”--->“本地策略”--->“用户权限分配”，找到“作

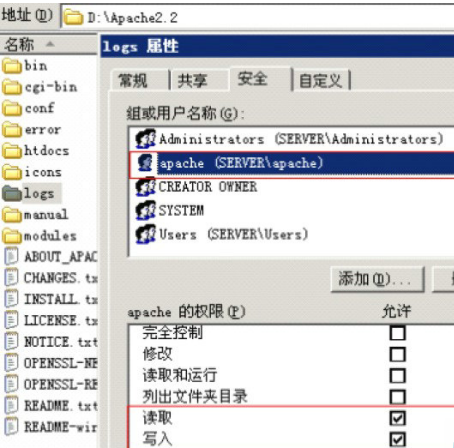
为服务登录”项，把刚刚新建的用户添加进去。



然后打开“服务”组件，找到Apache 的服务，右键“属性”--->“登录”，用刚新建的apache 帐户运行Apache 服务。



再找到Apache 日志目录，为apache 帐户分配“读取”和“写入”权限，否则Apache 服务不能启动。



配置好之后，重启Apache 服务生效，现在Apache 服务就已apache 低权限帐户运行了。

Linux环境下不必关心这个问题，Apache主进程以root 权限启动，子进程默认是以apache、daemon或其他用户身份运行的，这是一个低权限用户。

1. ServerRoot目录权限

实施目的：非超级用户不能修改该目录中的内容

加固方法：

Apache 的主目录对应于Apache Server 配置文件httpd.conf的ServerRoot 控制项中，应为：

Linux：ServerRoot /usr/local/apache（apache的目录）

Windows：ServerRoot "D:/phpStudy/Apache"（apache的目录）

1. 控制哪些主机能够访问服务器的一个区域

实施目的：只让某个网段或者某个IP接入，防止恶意攻击。

加固方法：

如：你想限制你的 intranet，只能被 176.16.网段接入：

Order Deny,Allow

Deny from all

Allow from 176.16.0.0/16

1. 禁止访问外部文件

实施目的：禁止 Apache 访问 Web 目录之外的任何文件。

加固方法：

编辑 httpd.conf 配置文件，设置可访问目录。

<Directory /web>

Order Allow,Deny

Allow from all

</Directory>

其中/web 为网站根目录。

1. 目录列表访问限制

实施目的：禁止 Apache 列表显示文件。

加固方法：

(1) 编辑 httpd.conf 配置文件，

<Directory "/web">

Options FollowSymLinks

AllowOverride None

Order allow,deny

Allow from all

</Directory>

将 Options Indexes FollowSymLinks 中的 Indexes 去掉，就可以禁止Apache 显示该目录结构。Indexes 的作用就是当该目录下没有index.html 文件时，就显示目录结构。

(2)设置 Apache 的默认页面，编辑%apache%\conf\httpd.conf 配置文件，

<IfModule dir\_module>

DirectoryIndex index.html

</IfModule>

其中 index.html 即为默认页面，可根据情况改为其它文件。

(3) 修改.htaccess文件——在.htaccess文件里加入“Options -Indexes”（没有双引号）就可以阻止目录列表的显示了。

修改完成之后重新启动 Apache 服务。

1. 网站目录权限配置

实施目的：通过控制网站权限来提高系统，网站程序安全性。

加固方法：

原则：目录有写入权限，一定不要分配执行权限；目录有执行权限，一定不要分配写入权限。

网站上传目录和数据库目录一般需要分配“写入”权限，但一定不要分配执行权限。其他目录一般只分配“读取”和“记录访问”权限即可。

1. 审核登陆

实施目的：对运行错误、用户访问等进行记录，记录内容包括时间，用户使用的 IP 地址等内容。

加固方法：

编辑 httpd.conf 配置文件，设置日志记录文件、记录内容、记录格式。

LogLevel notice

ErrorLog logs/error\_log

LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Accept}i\"

\"%{Referer}i\" \"%{User-Agent}i\"" combined

CustomLog logs/access\_log combined

ErrorLog 指令设置错误日志文件名和位置。错误日志是最重要的日志文件，Apache httpd 将在这个文件中存放诊断信息和处理请求中出现的错误。若要将错误日志送到Syslog，则设置：ErrorLog syslog。

CustomLog 指令设置访问日志的文件名和位置。访问日志中会记录服务器所处理的所有请求。

LogFormat 设置日志格式。LogLevel 用于调整记录在错误日志中的信息的详细程度，建议设置为 notice。

1. 更改默认端口

实施目的：更改 Apache 服务器默认端口，防止非法访问。

加固方法：

修改 httpd.conf 配置文件，更改默认端口到 8080，Listen x.x.x.x:8080，重启Apache服务。

1. 关闭并删除默认站点

实施目的：禁用 Apache Server中的执行功能，避免用户直接执行 Apache 服务器中的执行程序，而造成服务器系统的公开化。

加固方法：

在配置文件 access.conf 或 httpd.conf 中的 Options 指令处加入Includes NO EXEC 选项，用以禁用 Apache Server 中的执行功能。

<Directory />

Options **Includes NO EXEC** +FollowSymLinks +ExecCGI

AllowOverride All

Order allow,deny

Allow from all

Require all granted

</Directory>

1. 修改Apache默认banner信息

实施目的：隐藏 Apache 的版本号及其它敏感信息

加固方法：

打开httpd.conf配置文件，添加ServerTokens和ServerSignature到httpd.conf中。

ServerSignature Off

ServerTokens Prod

1. Apache 413 错误页面跨站脚本漏洞修复

实施目的：修复 Apache HTTP Server 处理畸形用户请求时存在漏洞

加固方法：

打开Apache 配置文件 httpd.conf 添加 ErrorDocument 413 语句禁用默认的 413 错误页面

ErrorDocument 413

1. 错误页面处理

实施目的：Apache 错误页面重定向。

加固方法：

(1) 修改 httpd.conf 配置文件：

ErrorDocument 400 /custom400.html

ErrorDocument 401 /custom401.html

ErrorDocument 403 /custom403.html

ErrorDocument 404 /custom404.html

ErrorDocument 405 /custom405.html

ErrorDocument 500 /custom500.html

Customxxx.html 为要设置的错误页面。

1. 重新启动 Apache 服务

13.拒绝服务防范

实施目的：合理设置 session 时间，防止拒绝服务攻击。

加固方法：

编辑 httpd.conf 配置文件:

Timeout 10 #客户端与服务器端建立连接前的时间间隔

KeepAlive On

KeepAliveTimeout 15 #限制每个 session 的保持时间是 15 秒 注：此处为一建议值，具体的设定需要根据现实情况。

修改之后重新启动 Apache 服务。

注：默认Timeout 120 KeepAlive Off，KeepAliveTimeout 15，该项设置涉及性能调整，一般不做。

14.关闭 TRACE功能

实施目的：关闭 TRACE，防止 TRACE 方法被访问者恶意利用。

加固方法：

配置修改httpd.conf文件

添加 “TraceEnable Off”

注：适用于 Apache 2.0 以上版本

## Nginx安全加固

1. Nginx版本的选择与安装注意事项

实施目的：Nginx关注Nginx是否存在安全漏洞和版本的稳定性。

加固方法：

在选择Nginx版本时需要关注是否存在安全漏洞和版本的稳定性。在生产环境中，一般选择最新的稳定版本，这样可以在稳定性和安全之间取得一个平衡。在升级Nginx版本前建议先在测试环境中测试通过后再正式升级，以避免由于兼容性带来其他不可预知的问题。

关于Nginx的安全漏洞可以关注Nginx官方发布的安全公告（http://nginx.org/en/security\_advisories.html）或到其他一些漏洞发布平台上查找。

在安装Nginx时建议使用自定义安装路径，如果采用默认安装路径，很容易被攻击者和一些自动化攻击工具猜测到，为其进行下一步的攻击提供便利。

2. 隐藏Nginx Banner信息

实施目的：隐藏Nginx Banner信息。

加固方法：

编辑nginx.conf, 在http段中添加

server\_tokens off;

3. 屏蔽某些IP

实施目的：屏蔽某些IP

加固方法：

conf文件中http或server段添加

location / {

......

allow 10.0.0.0/8;

deny all;

}

4. 预防PHP 解析漏洞

实施目的：预防PHP 解析漏洞

加固方法：

如果Nginx启用了php fastcgi功能，建议添加如下配置，以预防文件名解析漏洞：

server {

….

if ( $fastcgi\_script\_name ~ \..\*\/.\*php ) {

return 403;

}

….

}

上述配置将拦截类似这样的请求：

/1.jpg/x.php

/my.dir/x.php

5. 上传目录禁止执行

实施目的：上传目录禁止执行。

加固方法：

如果web应用确实需要支持文件上传功能，nginx启动帐号需要对web某些目录具有写权限，应在nginx里面限制上传目录无脚本执行权限。

注：这里指的不是去除文件系统rwx权限中的x，文件系统权限中的x可以保留，无影响。

假设上传目录为”/upload”，配置示例如下：

server {

….

location ~ ^/upload/.\*\.php {

return 403;

}

….

location ~ \.php$ {

fastcgi\_pass \*;

}

}

注：”location ~ ^/upload/.\*\.php”必须写在前面！对于location的正则表达式，nginx是按照先后顺序来匹配的，具体可参见[http://wiki.nginx.org/HttpCoreModule#location](http://wiki.nginx.org/HttpCoreModule" \l "location)

6. 禁止访问敏感扩展名文件

实施目的：禁止访问敏感扩展名文件

加固方法：

在nginx.conf中添加配置

location ~\* \.( rar|zip|gz|tar|tgz|tar.gz|7z|z|bz2|tar.bz2|sql|log|rar|ini|bak|conf|

DS\_Store|idea|swp|svn/entries|git/config)$ {

deny all;

}

7. 禁用autoindex

实施目的：禁用autoindex

加固方法：

修改nginx.conf配置文件上禁用autoindex，即autoindex off或者没有配置autoindex。

8. 自定义缓存

实施目的：自定义缓存

加固方法：

修改nginx.conf配置

http{

......

server{

... ...

client\_body\_buffer\_size 16K;

client\_header\_buffer\_size 1k;

client\_max\_body\_size 1m;

large\_client\_header\_buffers 4 8k;

......

注：上述的参数不是最优参数，仅供参考。

9. 设置timeout

实施目的：设置timeout设低来防御DOS攻击。

加固方法：

修改nginx.conf配置

http {

......

client\_body\_timeout 10;

client\_header\_timeout 30;

keepalive\_timeout 30 30;

send\_timeout 10;

10. 限制访问的方法

实施目的：限制访问的方法

加固方法：

修改nginx.conf配置

server{

......

if ($request\_method !~ ^(GET|HEAD|POST)$ ) {

return 444;

}

# 数据库安全加固

## MYSQL数据库加固

1. 禁止Mysql以管理员帐号权限运行

实施目的：禁止Mysql以管理员帐号权限运行。

加固方法：

Linux

编辑my.cnf配置文件，添加如下内容

[mysql.server]

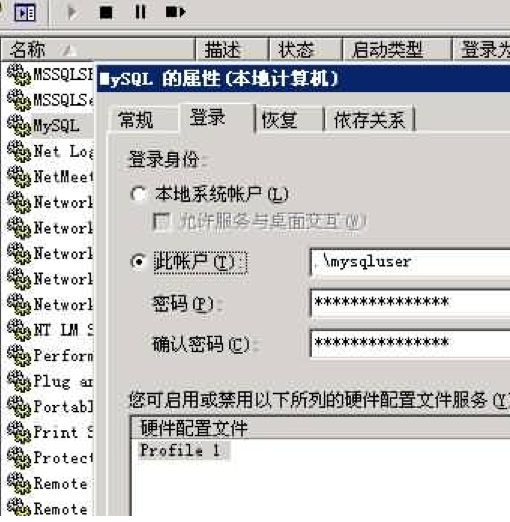
user=mysql

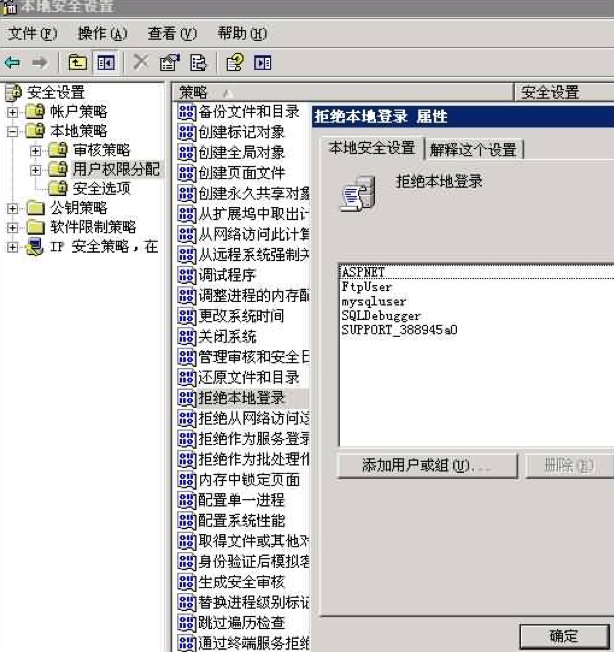
Windows

添加一个mysql启动用户，设置此用户为guest组；

  
设置d:\mysql目录为administrators组、system、新加的用户完全权限；

  
设置mysql服务的启动帐户为新加的用户，重新启动mysql服务；

  
设置拒绝本地登陆。



2. 避免不同用户间共享帐号

实施目的：避免不同用户间共享帐号。

加固方法：

mysql> insert into mysql.user(Host,User,Password,ssl\_cipher,x509\_issuer,x509\_sub

ject) values("localhost","pppadmin",password("passwd"),'','','');

这样就创建了一个名为：phplamp 密码为：1234 的用户。

然后登录一下。

mysql>exit;

>mysql -u phplamp -p

>输入密码

mysql>登录成功

3. 删除无关帐号

实施目的：删除无关帐号。

加固方法：

DROP USER语句用于删除一个或多个MySQL账户。要使用DROP USER，必须拥有mysql数据库的全局CREATE USER权限或DELETE权限。账户名称的用户和主机部分与用户表记录的User和Host列值相对应。

DROP USER user;

4. 检查帐户默认密码和弱密码

实施目的：检查帐户默认密码和弱密码。

加固方法：

 口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类。且5次以内不得设置相同的口令。密码应至少每90天进行更换。

修改帐户弱密码

如要修改密码，执行如下命令：

mysql> update user set password=password('test!p3') where user='root';

mysql> flush privileges;

或

[mysql](http://www.linuxnote.org/tag/mysql)> set password for root@localhost=password('test!p3');

5. 数据库授权

实施目的：在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

加固方法：

查看数据库授权情况：

mysql> use mysql;

mysql> select \* from user;

mysql>select \* from db;

mysql>select \* from host;

mysql>select \* from tables\_priv;

mysql>select \* from columns\_priv;

回收不必要的或危险的授权，可以执行revoke命令：

mysql> help revoke

Name: 'REVOKE'

Description:

Syntax:

REVOKE

priv\_type [(column\_list)]

[, priv\_type [(column\_list)]] ...

ON [object\_type]

{

\*

| \*.\*

| db\_name.\*

| db\_name.tbl\_name

| tbl\_name

| db\_name.routine\_name

}

FROM user [, user] ...

6. 开启日志审计功能

实施目的：配置数据库日志，便于记录运行状况和操作行为。

加固方法：

mysql有以下几种日志：

错误日志： -log-err

查询日志： -log （可选）

慢查询日志: -log-slow-queries （可选）

更新日志: -log-update

二进制日志： -log-bin

在mysql的安装目录下，打开my.ini,在后面加上上面的参数，保存后重启mysql服务就行了。

例如：

#Enter a name for the binary log. Otherwise a default name will be used.

#log-bin=

#Enter a name for the query log file. Otherwise a default name will be used.

#log=

#Enter a name for the error log file. Otherwise a default name will be used.

log-error=

#Enter a name for the update log file. Otherwise a default name will be used.

#log-update=

上面只开启了错误日志，要开其他的日志就把前面的“#”去掉

1、 补充操作说明

show variables like 'log\_%';查看所有的log命令

show variables like 'log\_bin';查看具体的log命令

7. 删除默认的数据库和用户

实施目的：删除默认的数据库和用户。

加固方法：

mysql> drop database test; mysql> use mysql; mysql> delete from db; mysql> delete from user where not(host="localhost" and user="root"); mysql> flush privileges;

8. 提高本地安全性

实施目的：防止mysql对本地文件的存取。

加固方法：

提高本地安全性,主要是防止mysql对本地文件的存取,如黑客通过mysql获取/etc/passwd,会对系统构成威胁。mysql对本地文件的存取是通过SQL语句来实现,主要是通过Load DATA LOCAL INFILE来实现,我们能够通过禁用该功能来防止黑客通过SQL注射等获取系统核心文件.禁用该功能必须在my.cnf的[mysqld]部分加上一个参数:

set-variable=local-infile = 0

9. 禁止远程连接mysql

实施目的：禁止远程连接mysql。

加固方法：

配置**my.cnf**文件,在**[mysqld]**部分添加**skip-networking**参数，使mysql不监听任何TCP/IP连接,增加安全性.如果要进行mysql的管理的话,可以在服务器本地安装一个phpMyadmin来进行管理。

10. 控制数据库访问权限

实施目的：控制数据库访问权限。

加固方法：

建立一个用户只针对某个库有update、select、delete、insert、drop table、create table等权限,这样就很好避免了数据库用户名和密码被黑客查看后最小损失.比如下面我们创建一个数据库为db1,同时建立一个用户test1能够访问该数据库。

mysql> create database db1;

mysql> grant select,insert,update,delete,create,drop privileges on db1.\* to test1@localhost identified by 'admindb';

11. 设置可信IP地址访问控制

实施目的：仅允许信任的IP地址才能通过监听器访问数据库。

加固方法：

执行命令：

mysql> GRANT ALL PRIVILEGES ON db.\* TO 用户名@'IP子网/掩码';

12. 连接数设置

实施目的：根据机器性能和业务需求，设制最大最小连接数。

加固方法：

编辑MySQL配置文件：my.cnf 或者是 my.ini

在[mysqld]配置段添加：

max\_connections = 1000

保存，重启MySQL服务。

## MSSQL数据库加固

1. 为不同的管理员分配不同的账号

实施目的：为不同的管理员分配不同的账号，按照用户分配账号，避免不同用户间共享账号,

提高安全性。

加固方法：

use master

Select name,password from syslogins order by name

查看用户列表

执行SQL语句：

sp\_addlogin 'user\_name\_1','password1'

sp\_addlogin 'user\_name\_2','password2'

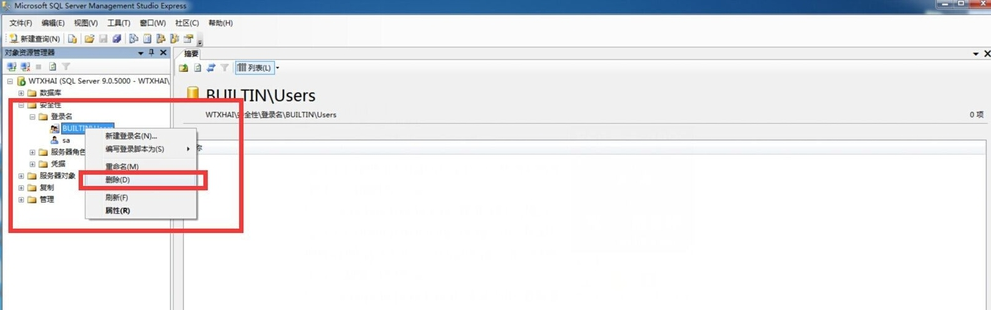
建立角色，并给角色授权，把角色赋给不同的用户或修改用户属性中的角色和权限。

2. 删除或锁定无效账号

实施目的：删除或锁定无效账号。

加固方法：

Mssql 企业管理器->安全性->单击展开，选中要删除的“用户名”，右键点击选中“删除”。

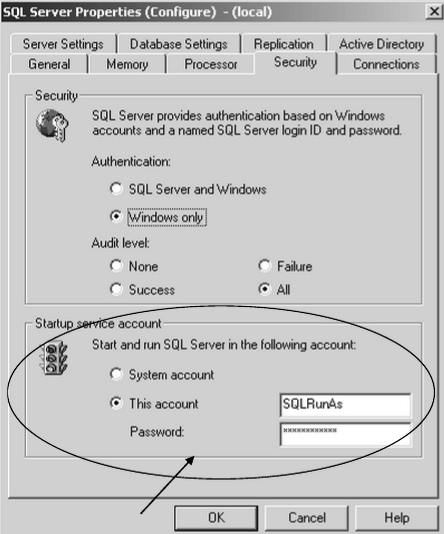


3. 限制启动账号权限

实施目的：限制启动账号权限。

加固方法：

新建 SQL server 服务账号后，建议将其从 User 组中删除，且不要把该账号提升为 Administrators 组的成员。授予以下 windows SQLRunAs 账户最少的权限启动 SQL Server 数据库。



4. 数据库角色

实施目的：使用数据库角色（ROLE）来管理对象的权限。

加固方法：

调整角色属性中的权限，赋予角色中拥有对象对应的SELECT、INSERT、UPDATE、DELETE、EXEC、DRI权限。

5. 用户属性检查

实施目的：对用户的属性进行安全检查，包括空密码、密码更新时间等。修改目前所有账号的口令，确认为强口令。特别是 sa 账号，需要设置至少 10 位的强口令。

加固方法：

select \* from sysusers

Select name,Password from syslogins where password is null order by name # 查看口令为空的用户

执行语句：

Use master

exec sp\_password ‘旧口令’ ，‘新口令’,用户名

6. 限制sql server 使用的协议

实施目的：除去不必要的服务。

加固方法：

在 Microsoft SQL Server 程序组, 运行服务网络实用工具,查看协议列表,查看是否有多余协议。



7. 加固 TCP/IP 协议栈

实施目的：加固 TCP/IP 协议栈,加强系统防御网络攻击能力。

加固方法：

对于 TCP/IP 协议栈的加固主要是某些注册表键值的

修改。主要是以下几个：

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting

说明：该键值应设为 2，以防御源路由欺骗攻击。

HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect

说明：该键值应设为 0，以 ICMP 重定向。

HKLM\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect

说明：该键值应设为 2，防御 SYN FLOOD 攻击。

8. 停用不必要的存储过程

实施目的：停用 sql server中存在的危险存储过程。

加固方法：

use master

exec sp\_dropextendedproc 'xp\_cmdshell'

exec sp\_dropextendedproc 'xp\_dirtree'

exec sp\_dropextendedproc 'xp\_enumgroups'

exec sp\_dropextendedproc 'xp\_fixeddrives'

exec sp\_dropextendedproc 'xp\_loginconfig'

exec sp\_dropextendedproc 'xp\_enumerrorlogs'

exec sp\_dropextendedproc 'xp\_getfiledetails'

exec sp\_dropextendedproc 'Sp\_OACreate'

exec sp\_dropextendedproc 'Sp\_OADestroy'

exec sp\_dropextendedproc 'Sp\_OAGetErrorInfo'

exec sp\_dropextendedproc 'Sp\_OAGetProperty'

exec sp\_dropextendedproc 'Sp\_OAMethod'

exec sp\_dropextendedproc 'Sp\_OASetProperty'

exec sp\_dropextendedproc 'Sp\_OAStop'

exec sp\_dropextendedproc 'Xp\_regaddmultistring'

exec sp\_dropextendedproc 'Xp\_regdeletekey'

exec sp\_dropextendedproc 'Xp\_regdeletevalue'

exec sp\_dropextendedproc 'Xp\_regenumvalues'

exec sp\_dropextendedproc 'Xp\_regread'

exec sp\_dropextendedproc 'Xp\_regremovemultistring'

exec sp\_dropextendedproc 'Xp\_regwrit e'

drop procedure sp\_makewebtask

Go

删除测试或不必要的存储过程，一般情况下建议删除的存储

过程有：

sp\_OACreate

sp\_OADestroy

sp\_OAGetErrorInfo

sp\_OAGetProperty

sp\_OAMethod

sp\_OASetProperty

sp\_OAStop

sp\_regaddmultistring

xp\_regdeletekey

xp\_regdeletevalue

xp\_regenumvalues

xp\_regremovemultistring

除非应用程序需要否则以下存储过程也建议删除：

xp\_perfend

xp\_perfmonitor

xp\_perfsample

xp\_perfstart

xp\_readerrorlog

xp\_readmail

xp\_revokelogin

xp\_runwebtask

xp\_schedulersignal

xp\_sendmail

xp\_servicecontrol

xp\_snmp\_getstate

xp\_snmp\_raisetrap

xp\_sprintf

xp\_sqlinventory

xp\_sqlregister

xp\_sqltrace

xp\_sscanf

xp\_startmail

xp\_stopmail

xp\_subdirs

xp\_unc\_to\_drive

xp\_dirtree

sp\_sdidebug

xp\_availablemedia

xp\_cmdshell

xp\_deletemail

xp\_dirtree

xp\_dropwebtask

xp\_dsninfo

xp\_enumdsn

xp\_enumerrorlogs

xp\_enumgroups

xp\_enumqueuedtasks

xp\_eventlog

xp\_findnextmsg

xp\_fixeddrives

xp\_getfiledetails

xp\_getnetname

xp\_grantlogin

xp\_logevent

xp\_loginconfig

xp\_logininfo

xp\_makewebtask

xp\_msver

## 3.3 Oracle数据库加固

1. 为不同的管理员分配不同的账号

实施目的：按照用户分配账号，避免不同用户间共享账号,提高安全性。

加固方法：

create user abc1 identified by password1;

create user abc2 identified by password2;

建立 role，并给 role 授权，把 role 赋给不同的用户

2. 删除或锁定无效账号

实施目的：删除或锁定无效的账号，减少系统安全隐患。

加固方法：

执行语句

锁定用户：alter user username lock;

删除用户：drop user username cascade;

3. 限制超级管理员远程登录

实施目的：限制具备数据库超级管理员（SYSDBA）权限的用户远程登录。

加固方法：

（1）在 spfile 中设置 REMOTE\_LOGIN\_PASSWORDFILE=NONE 来禁止

SYSDBA 用 户 从 远 程 登 陆 。

（2）在 sqlnet.ora 中设置、SQLNET.AUTHENTICATION\_SERVICES=NONE 来禁用 SYSDBA 角色的自动登录。

4. 权限最小化

实施目的：在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

加固方法：

select \* from user\_sys\_privs;

select \* from user\_role\_privs;

select \* from user\_tab\_privs;

查看用户拥有的权限

给用户赋相应的最小权限： grant 权限 to username;

收回用户多余的权限： revoke 权限 from username;

5. 数据库角色

实施目的：使用数据库角色（ROLE）来管理对象的权限。

加固方法：

执行语句：

select \* from dba\_role\_privs;

select \* from user\_role\_privs;

记录用户拥有的 role

创建角色,修改角色：

（1）创建角色，不指定密码：

create role testrole；

（2）创建角色，指定密码：

create role testrole identified by passwd;

（3）修改角色：

alter role testrole identified by passwd;

（4）给角色授予权限。

Grant select on Table\_name to testrole;

把角色赋予用户：（特别说明，授予角色不是实时的。如下：）

grant testrole to User\_Name;

起用角色：给用户赋予角色，角色并不会立即起作用。

（1）角色不能立即起作用。必须下次断开此次连接，下次连接才能起作用。

（2）或者执行命令：有密码的角色set role testrole identified by passwd 立即生效；

（3）无密码的角色：set role testrole；

6. 用户profile

实施目的：对用户的属性进行控制，包括密码策略、资源限制等。

加固方法：

SELECT profile FROM dba\_users WHERE username=’user\_name’;

记录用户赋予的 profile

可通过下面类似命令来创建 profile，并把它赋予一个用户

SQL> show parameter resource\_limit

SQL> alter system set resource\_limit=true;

CREATE PROFILE profile\_name LIMIT

FAILED\_LOGIN\_ATTEMPTS 6

PASSWORD\_LIFE\_TIME 60

PASSWORD\_REUSE\_TIME 60

PASSWORD\_REUSE\_MAX 5

PASSWORD\_VERIFY\_FUNCTION verify\_f unction

PASSWORD\_LOCK\_TIME 1/24

PASSWORD\_GRACE\_TIME 90;

ALTER USER user\_name PROFILE profile\_name;

7. 数据字典保护

实施目的：启用数据字典保护，只有 SYSDBA 用户才能访问数据字典基础表。

加固方法：

Show parameter O7\_DICTIONARY\_ACCESSIBILITY

记录当前状态

通过设置下面初始化参数来限制只有 SYSDBA 权限的用户才

能访问数据字典。

alter system set O7\_DICTIONARY\_ACCESSIBILITY=FALSE scope=spfile;

8. 缺省密码长度复杂度限制

实施目的：对于采用静态口令进行认证的数据库，口令长度至少 6 位，并包括数字、小写字母、大写字母和特殊符号 4 类中至少 2类。

加固方法：

SELECT profile FROM dba\_users WHERE username=’user\_name’;

记录用户赋予的 profile

为用户建 profile，调整 PASSWORD\_VERIFY\_FUNCTION，指定密码复杂度。

示例:

SQL>CREATE OR REPLACE FUNCTION my\_password\_verify

(username VARCHAR2 ,password

VARCHAR2 ,old\_password VARCHAR2 ) RETURN BOOLEAN

IS

2 BEGIN

3 IF LENGTH(password) < 6 THEN

4

raise\_application\_error(-20001,''Password must be at least 6 characters long'');

5 END IF;

6 RETURN(TRUE);

7 END;

SQL> create profile TEST\_PROFILE limit 2 password\_verify\_function

MY\_PASSWORD\_VERIFY;

9. 修改默认密码

实施目的：更改数据库默认帐号的密码。

加固方法：

通过下面命令来更改默认用户的密码：

ALTER USER user\_name IDENTIFIED BY passwd;

以下是默认用户密码列表：

CTXSYS CTXSYS

DBSNMP DBSNMP

LBACSYS LBACSYS

MDDATA MDDATA

MDSYS MDSYS

DMSYS DMSYS

OLAPSYS MANAGER

ORDPLUGINS ORDPLUGINS

ORDSYS ORDSYS

OUTLN OUTLN

SI\_INFORMTN\_SCHEMA SI\_INFORMTN\_SCHEMA

SYS CHANGE\_ON\_INSTALL

SYSMAN CHANGE\_ON\_INSTALL

SYSTEM MANAGER

10. 启用日志记录功能

实施目的：数据库应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的账号、登录是否成功、登录时间以及远程登录时用户使用的 IP 地址。

加固方法：

create table login\_log --登入登出信息表

(

session\_id int not null, --sessionid

login\_on\_time date, --登入时间

login\_off\_time date, --登出时间

user\_in\_db varchar2(30), --登入的 db user

machine varchar2(20), -- 机器名

ip\_address varchar2(20), -- ip 地址

run\_program varchar2(20) -- 以何程序登入

);

create or replace trigger login\_on\_info -- 记录登入信息的触发器

after logon on database

Begin

insert into

login\_log(session\_id,login\_on\_time,login\_of

f\_time,user\_in\_db,machine,ip\_address,run\_program

)

select

AUDSID,sysdate,null,sys.login\_user,machine,SYS\_CO

NTEXT('USERENV','IP\_ADDRESS'),program

from v$session where AUDSID =

USERENV('SESSIONID'); --当前 SESSION

END;

create or replace trigger login\_off\_info -- 记录登出信息的触发器

before logoff on database

Begin

update login\_log set login\_off\_time =

sysdate

where session\_id = USERENV('SESSIONID'); --当前 SESSION

exception

when others then

null;

END;

11. 记录用户对设备的操作

实施目的：数据库应配置日志功能，记录用户对数据库的操作。

加固方法：

create table employees\_log(

who varchar2(30),

action varchar2(20));

when date);

create or replace trigger biud\_employ\_copy

before insert or update or delete

on employees\_copy

declare

l\_action employees\_log.action%type;

begin

if inserting then

l\_action:='insert';

elsif updating then

l\_action:='delete';

elsif deleting then

l\_action:='update';

else

raise\_application\_error(-2001,'you shoule never ever get this error.');

end if;

insert into employees\_log(who,action,when) values(user,l\_action,sysdate);

end biud\_employ\_copy;

12. 记录系统安全事件

实施目的：通过设置让系统记录安全事件，方便管理员分析。

加固方法：

create table jax\_event\_table(eventname

varchar2(30),time date);

create trigger tr\_startup

after startup ondatabase

begin

insert into jax\_event\_table values(ora\_sysevent,sysdate);

end;

create trigger tr\_shutdown

beforeshutdownondatabase

begin

insertinto jax\_event\_table values(ora\_sysevent,sysdate);

end;

13. 数据库审计策略

实施目的：根据业务要求制定数据库审计策略。

加固方法：

show parameter audit\_sys\_operations;

show parameter audit\_trail;

查看返回值,并记录。

参考配置:

SQL> alter system set audit\_sys\_operations=TRUE

scope=spfile;

SQL> alter system set audit\_trail=db scope=spfile;

SQL> show parameter audit;

SQL> audit all on table\_name;

14. 信任IP连接监听器

实施目的：设置只有信任的 IP 地址才能通过监听器访问数据库。

加固方法：

参考配置：

在文件$ORACLE\_HOME/network/admin/sqlnet.ora 中设置以下行：

tcp.validnode\_checking = yes

tcp.invited\_nodes = (ip1,ip2,)

15. 连接超时限制

实施目的：在某些应用环境下可设置数据库连接超时，比如数据库将自动断开超过 10 分钟的空闲远程连接。

加固方法：

参考配置

在sqlnet.ora中设置下面参数：

SQLNET.EXPIRE\_TIME=10

# 网站安全加固

## PHP环境安全加固

1. 启用php的安全模式

实施目的：打开PHP安全模式。

加固方法：

php的安全模式是个非常重要的内嵌的安全机制，能够控制一些php中的函数，比如system()，同时把很多文件操作函数进行了权限控制，也不允许对某些关键字文件的文件，比如/etc/passwd，但是默认的php.ini是没有打开安全模式。

修改php.ini配置文件

safe\_mode = on

2. 用户组安全

实施目的：对服务器网站目录下的文件进行操作。

加固方法：

修改php.ini配置文件

safe\_mode\_gid = off

3. 安全模式下执行程序主目录

实施目的：安全模式下执行程序主目录。

加固方法：

如果安全模式打开了，但是却是要执行某些程序的时候，可以指定要执行程序的主目录：

修改php.ini配置文件

safe\_mode\_exec\_dir = /usr/bin

一般情况下是不需要执行什么程序的，所以推荐不要执行系统程序目录，可以指向一个目录：然后把需要执行的程序拷贝过去，比如：

修改php.ini配置文件

safe\_mode\_exec\_dir = /temp/cmd

推荐不要执行任何程序，那么就可以指向网页目录：

修改php.ini配置文件

safe\_mode\_exec\_dir = /usr/www

4. 安全模式下包含文件

实施目的：安全模式下包含文件。

加固方法：

如果要在安全模式下包含某些公共文件，则修改php.ini配置文件

safe\_mode\_include\_dir = /usr/www/include/

注：一般php脚本中包含文件都是在程序已经写好了，可以根据具体需要设置。

5. 控制php脚本能访问的目录

实施目的：控制php脚本能访问的目录。

加固方法：

修改php.ini配置文件

open\_basedir = /usr/www

6. 关闭危险函数

实施目的：关闭危险函数。

加固方法：

如果打开了安全模式，那么函数禁止是可以不需要的，但是我们为了安全还是考虑进去。比如，我们觉得不希望执行包括system()等在内的执行明了的php函数，或者能够查看php信息的phpinfo()等函数，那么就可以禁止它们：

修改php.ini配置文件

disable\_functions = system, passthru, exec, shell\_exec, popen, phpinfo, escapeshellarg, escapeshellcmd, proc\_close, proc\_open, dl

如果需要禁止任何文件和目录的操作，那么可以关闭很多文件操作

修改php.ini配置文件

disable\_functions = chdir, chroot, dir, getcwd, opendir, readdir, scandir, fopen, unlink, delete, copy, mkdir, rmdir, rename, file, file\_get\_contents, fputs, fwrite, chgrp,chmod, chown

以上只是列了部分比较常用的文件处理函数，也可以把上面执行命令函数和这个函数结合，就能给抵制大部分的phpshell了。

7. 关闭php版本信息在http头中的泄露

实施目的：关闭php版本信息在http头中的泄露。

加固方法：

修改php.ini配置文件

expose\_php = off

8. 关闭注册全局变量

实施目的：关闭注册全局变量。

加固方法：

在PHP中提交的变量，包括使用POST或者GET提交的变量，都将自动注册为全局变量，能够直接访问，这是对服务器非常不安全的，所以我们不能让它注册为全局变量，就把注册全局变量选项关闭：

修改php.ini配置文件

register\_globals = off

9. SQL注入防护

实施目的：SQL注入防护。

加固方法：

修改php.ini配置文件

magic\_quotes\_gpc = on

10. 错误信息控制

实施目的：关闭错误信息提示。

加固方法：

修改php.ini配置文件

display\_errors = Off

11. 错误日志

实施目的：开启错误日志记录。

加固方法：

修改php.ini配置文件

log\_errors = On

error\_log = /usr/local/apache2/logs/php\_error.log