2021 年全国职业院校技能大赛（中职组）

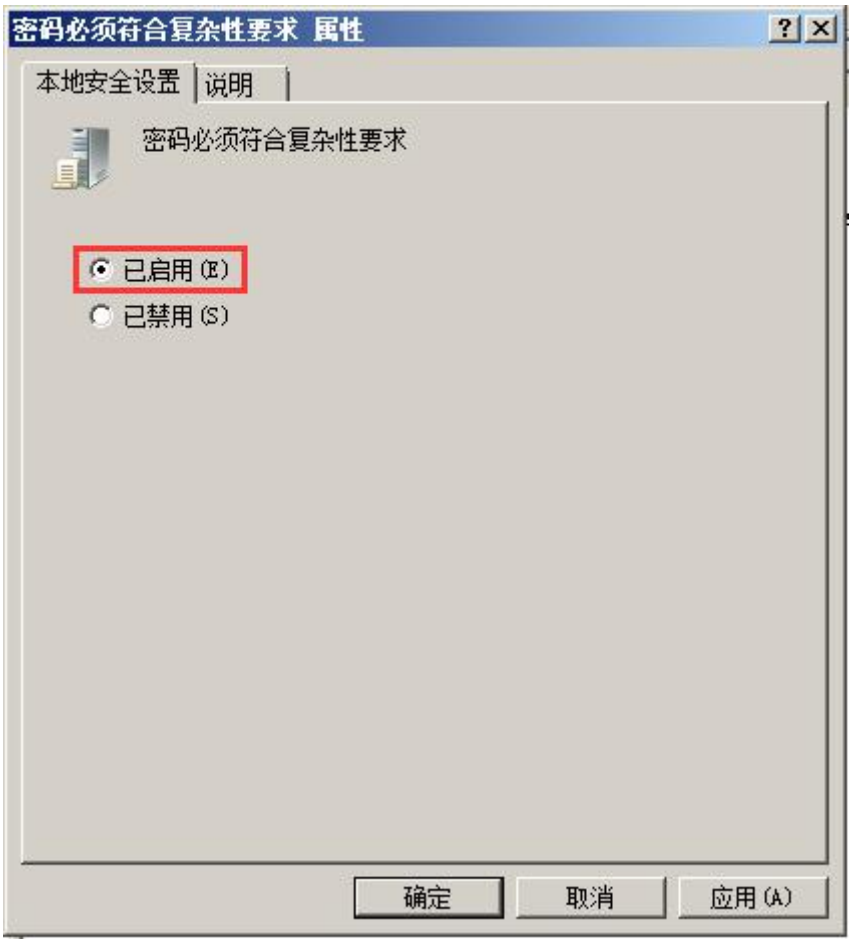
网络安全竞赛 A 模块评分标准

A-1 任务一 登录安全加固（Windows，Linux）

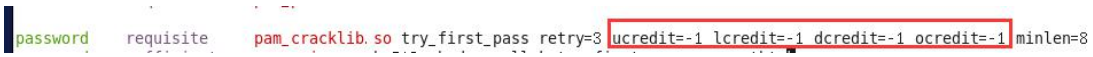
请对服务器 Windows、Linux 按要求进行相应的设置，提高服务器的安全性。

1.密码策略（Windows，Linux）

a1.密码策略必须同时满足大小写字母、数字、特殊字符（Windows），将密码必须符合复杂性要求的属性配置界面截图：



a2.密码策略必须同时满足大小写字母、数字、特殊字符（Linux），将/etc/pam.d/system-auth 配置文件中对应的部分截图：



b1.最小密码长度不少于 8 个字符（Windows），将密码长度最小值的属性配置界面截图：

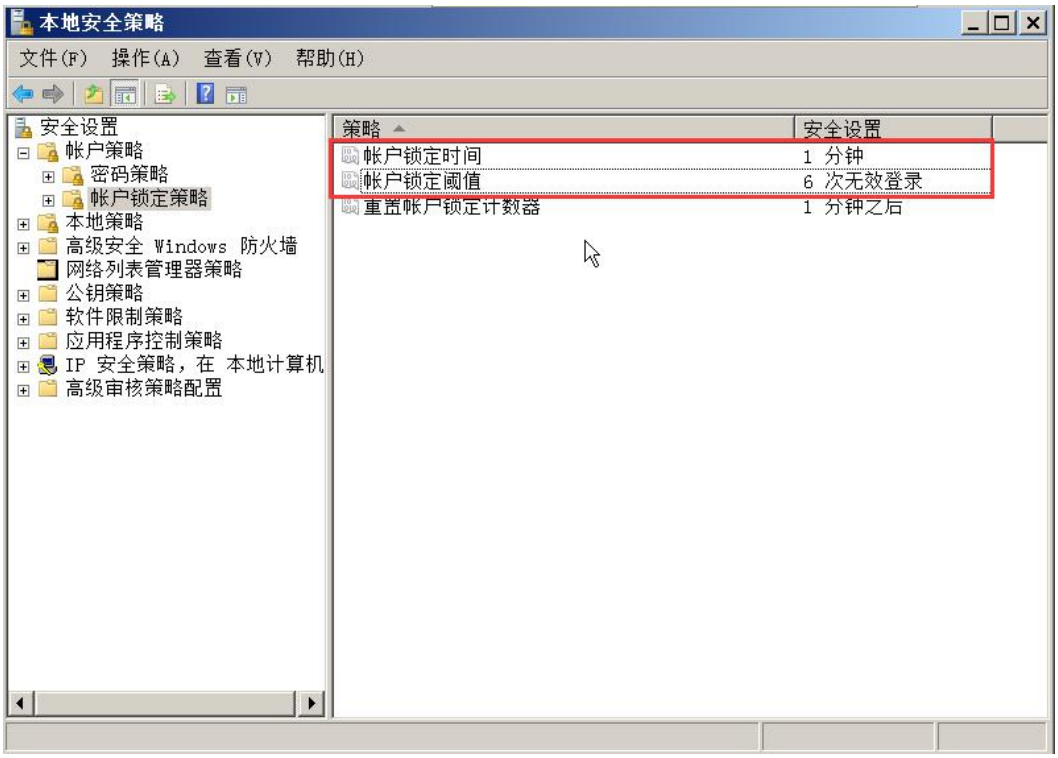
b2.最小密码长度不少于 8 个字符（Linux），将/etc/login.defs 配置文件中对应的部分截图：

```
PASS_MAX_DAYS   99999
PASS_MIN_DAYS   0
PASS_MIN_LEN    8
PASS_WARN_AGE   7
```

2. 登录策略

a. 设置账户锁定阈值为 6 次错误锁定账户，锁定时间为 1 分钟，复位账户锁定计数器为 1 分钟之后（Windows）,将账户锁定策略配置界面截图：

（注意，这里锁定阈值应为 6 次，截图中若为 5 次或其他则不计分）

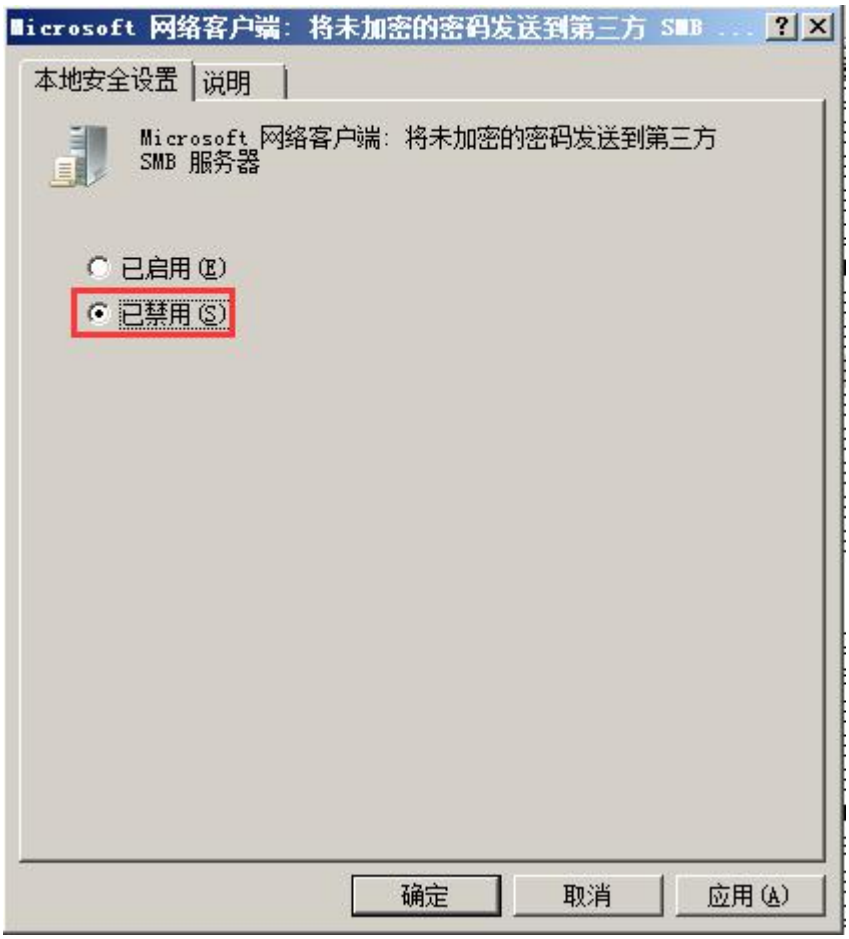


b. 一分钟内仅允许 5 次登录失败，超过 5 次，登录帐号锁定 1 分钟（Linux），将/etc/pam.d/login 配置文件中对应的部分截图：（注意，超过五次次锁定，所以这里锁定阈值应为 6 次，截图中若为 5 次则不计分）

```
auth        requisite     pam_tally2.so deny=6 unlock_time=60
```

3.用户安全管理(Windows)

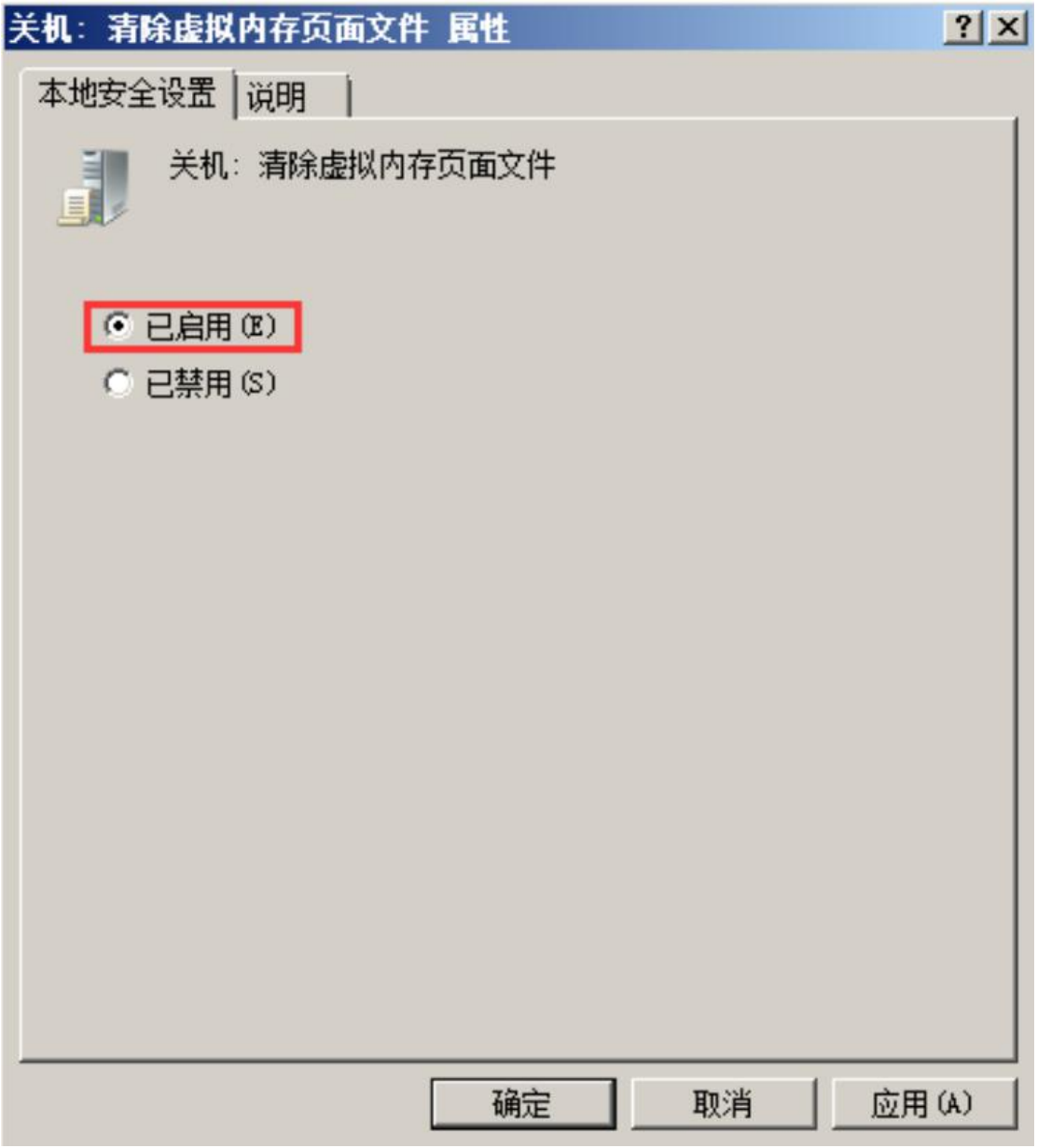
a.禁止发送未加密的密码到第三方 SMB 服务器，将 Microsoft 网络客户端：将未加密的密码发送到第三方 SMB 服务器的属性配置界面截图：



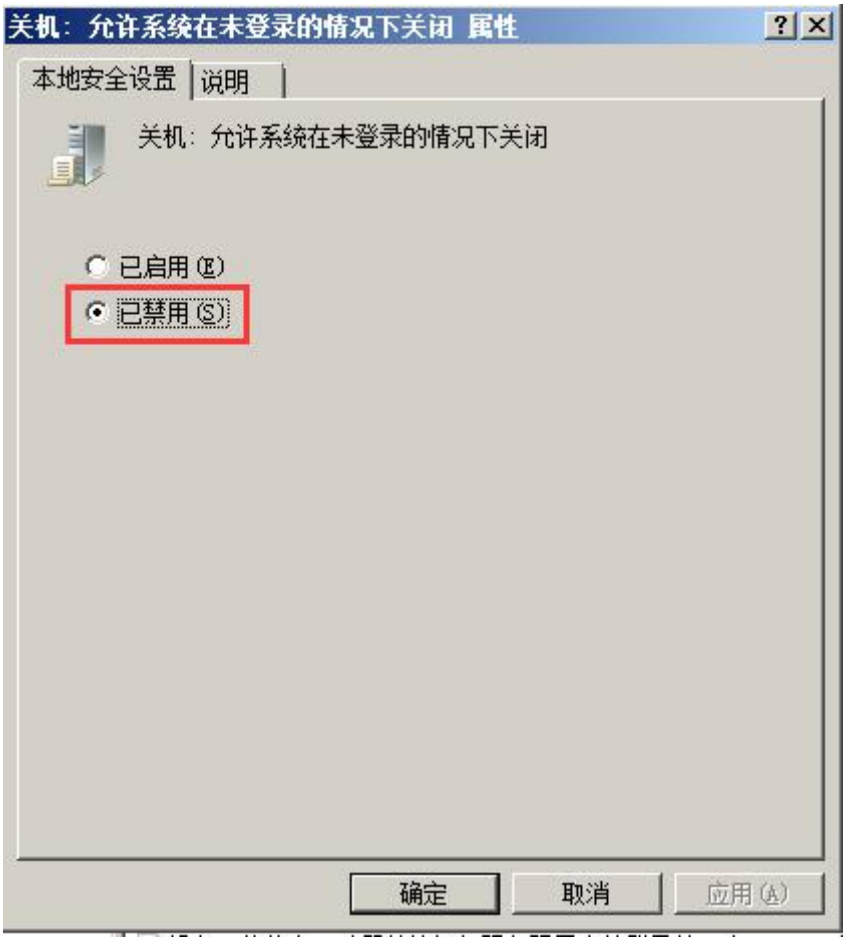
b.禁用来宾账户，禁止来宾用户访问计算机或访问域的内置账户，将账户：来宾账户状态的属性配置界面截图：

A-2 任务二 本地安全策略设置（Windows）

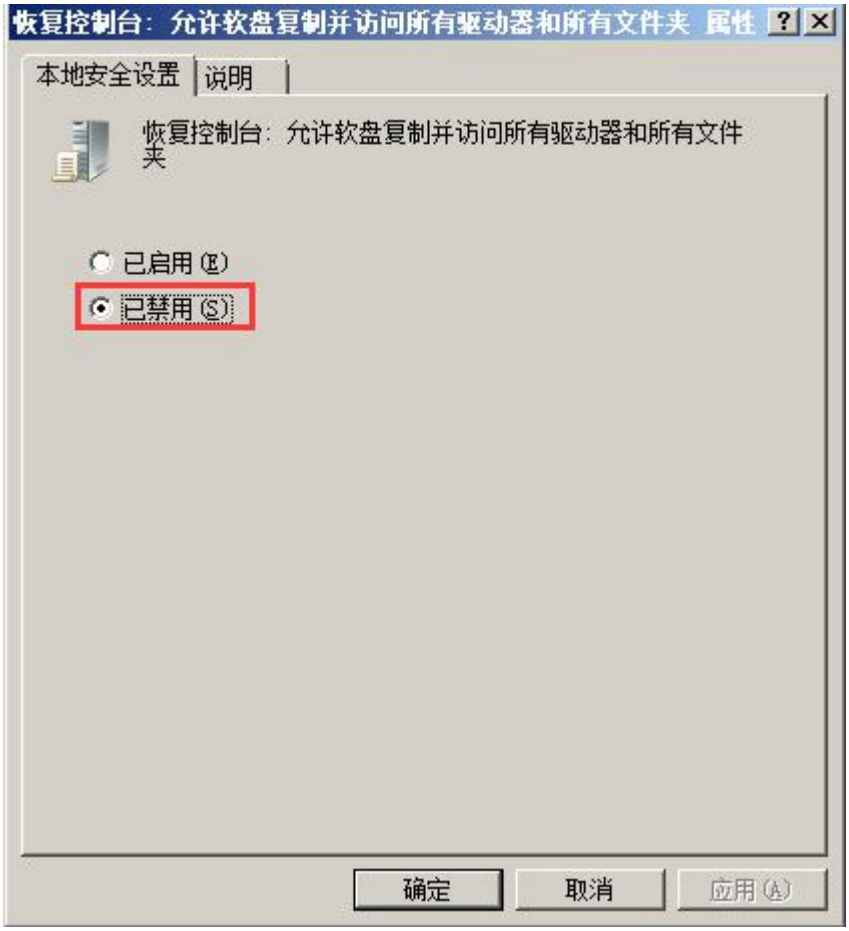
4.关闭系统时清除虚拟内存页面文件，将关机：清除虚拟内存页面文件的属性配置界面截图：



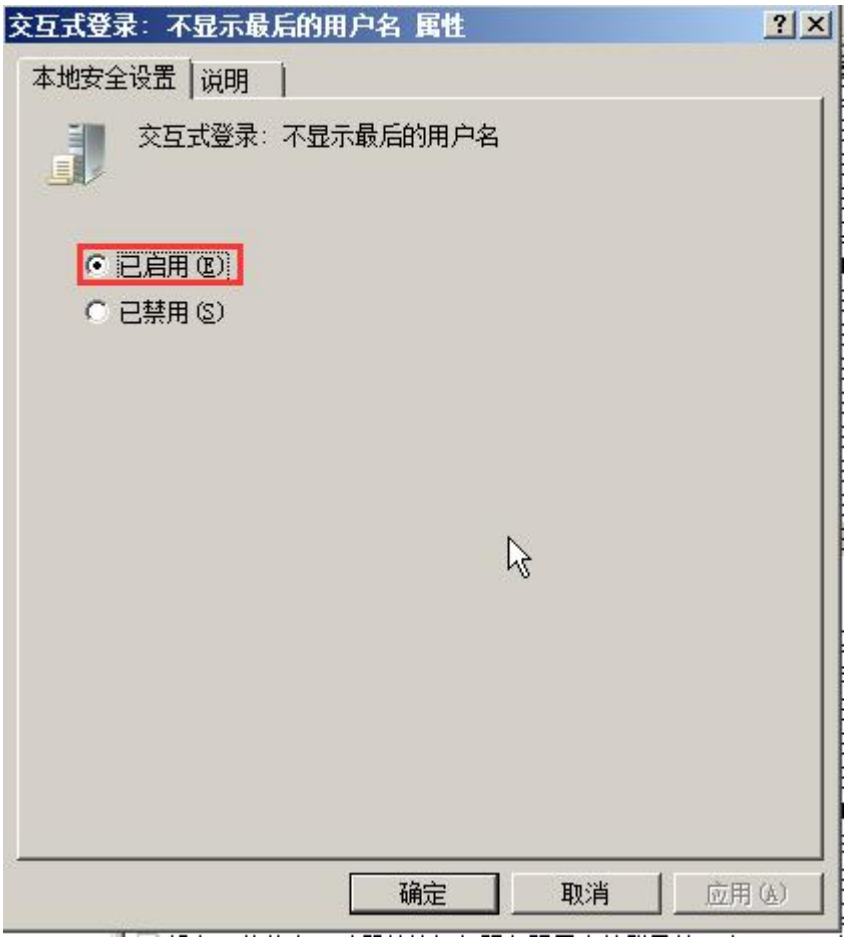
5.禁止系统在未登录的情况下关闭，将关机：允许系统在未登录的情况下关闭的属性配置界面截图：



6. 禁止软盘复制并访问所有驱动器和所有文件夹，将恢复控制台：允许软盘复制并访问所有驱动器和所有文件夹的属性配置界面截图：

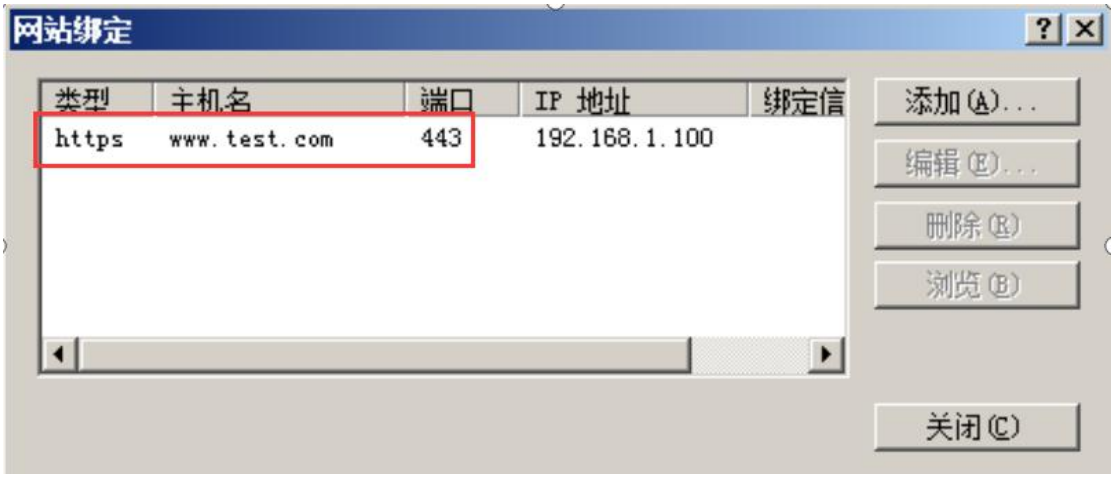


7.禁止显示上次登录的用户名，将交互式登录：不显示最后的用户名的属性配置界面截图：



A-3 任务三 流量完整性保护（Windows，Linux）

8.创建 www.chinaskills.com 站点，在 C:\web 文件夹内中创建名称为 chinaskills.html 的主页，主页显示内容“热烈庆祝 2021 年全国职业技能大赛开幕”，同时只允许使用 SSL 且只能采用域名（域名为 www.test.com）方式进行访问，将网站绑定的配置界面截图：



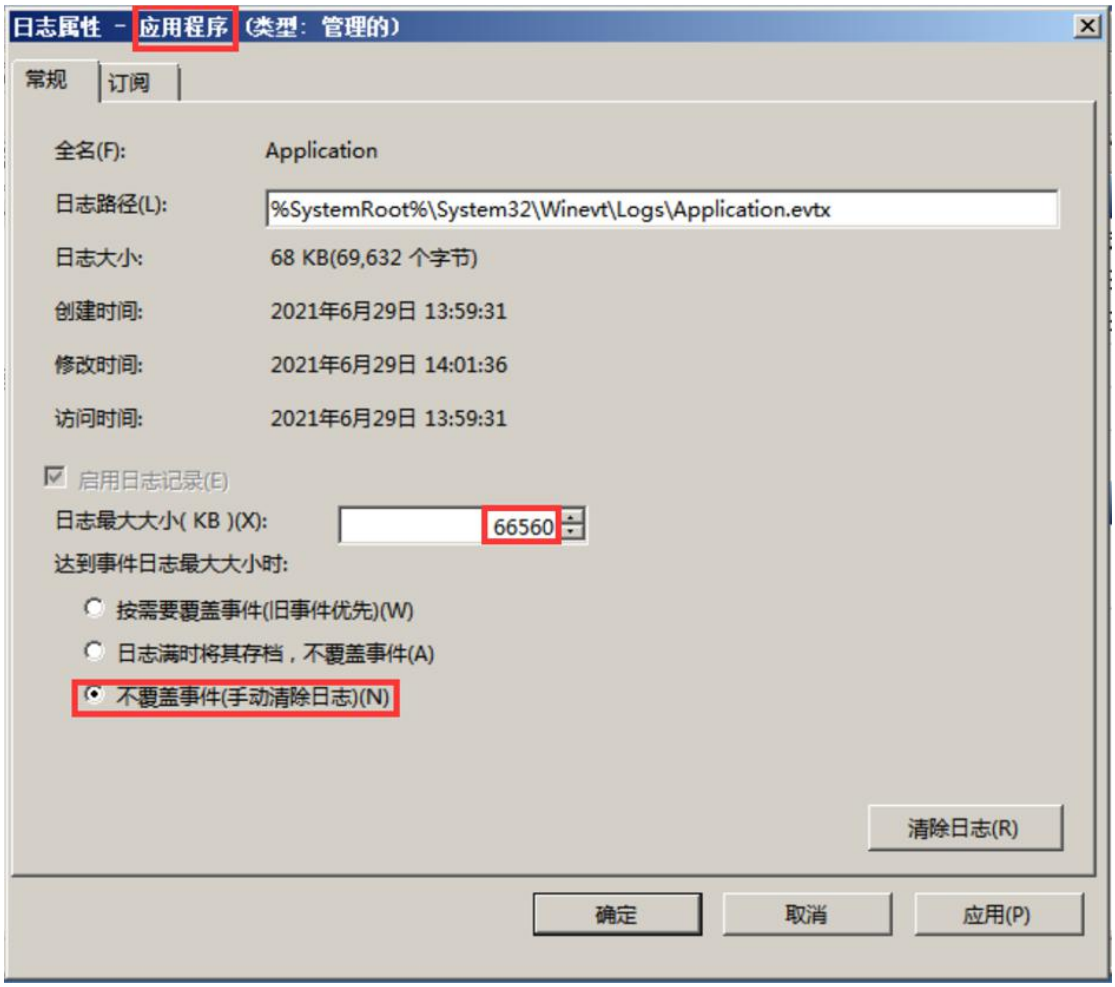
9.为了防止密码在登录或者传输信息中被窃取，仅使用证书登录 SSH（Linux），将/etc/ssh/sshd_config 配置文件中对应的部分截图：

```
# To disable tunneled clear text passwords, change to no here
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication no

#RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile     .ssh/authorized_keys
#AuthorizedKeysCommand none
#AuthorizedKeysCommandRunAs nobody
```

A-4 任务四 事件监控（Windows）

10.应用程序日志文件最大大小达到 65M 时将其存档，不覆盖事件，将日志属性-应用程序（类型：管理的）配置界面截图：



A-5 任务五 服务加固 SSH\VSFTPD\IIS（Windows，Linux）

11. SSH 服务加固（Linux）

a. SSH 禁止 root 用户远程登录，将/etc/ssh/sshd_config 配置文件中对应的部分截图：

```
#LoginGraceTime 2m
#PermitRootLogin yes
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 7
```

b. 设置 root 用户的计划任务。每天早上 7:50 自动开启 SSH 服务，22:50 关闭；每周六的 7:30 重新启动 SSH 服务，使用命令 crontab -l，

将回显结果截图；

```
[root@localhost ~]# crontab -l
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fr
i,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
50 7 * * * root service sshd start
50 22 * * * root service sshd stop
30 7 * * 6 root service sshd restart
[root@localhost ~]#
```

c.修改 SSH 服务端口为 2222，使用命令 netstat -anltp | grep sshd 查看 SSH 服务端口信息，将回显结果截图；

```
[root@localhost Desktop]# netstat -anltp | grep sshd
tcp        0      0 0.0.0.0:2222                0.0.0.0:*                   LISTEN      3710/sshd
tcp        0      0 :::2222                     :::*                        LISTEN      3710/sshd
[root@localhost Desktop]#
```

12.VSFTPD 服务加固（Linux）

a.设置数据连接的超时时间为 2 分钟，将/etc/vsftpd/vsftpd.conf 配置文件中对应的部分截图：

```
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
-- 插入 --                                                    64,1          44%
```

b.设置站点本地用户访问的最大传输速率为 1M，将/etc/vsftpd/vsftpd.conf 配置文件中对应的部分截图：1000000 或

1048576 均可

```
pasv_enable=YES
pasv_min_port=50000
pasv_max_port=60000
local_max_rate=1048576
-- 插入 --                                    127,23        底端
```

13. IIS 加固（Windows）

a. 防止文件枚举漏洞枚举网络服务器根目录文件，禁止 IIS 短文件名泄露，将配置命令截图：

```
C:\inetpub\wwwroot>fsutil 8dot3name set 1
```

b. 关闭 IIS 的 WebDAV 功能增强网站的安全性，将警报提示信息截图：

A-6 任务六 防火墙策略（Linux）

14. 只允许转发来自 172.16.0.0/24 局域网段的 DNS 解析请求数

据包，将 iptables 配置命令截图：

```
iptables -A FORWARD -p udp --dport 53 -s 172.16.0.0/24 -j ACCEPT
```

15. 禁止任何机器 ping 本机，将 iptables 配置命令截图：

```
iptables -A INPUT -p icmp --icmp-type 8 -j DROP
```

16. 禁止本机 ping 任何机器，将 iptables 配置命令截图：

```
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j DROP
```

17. 禁用 23 端口，将 iptables 配置命令截图：

```
iptables -A INPUT -p tcp --dport 23 -j DROP
iptables -A INPUT -p udp --dport 23 -j DROP
```

18. 禁止转发来自 MAC 地址为 29:0E:29:27:65:EF 主机的数据包，将 iptables 配置命令截图：

```
[root@localhost ~]# iptables -A FORWARD -m mac --mac-source 29:0E:29:27:65:EF -j
DROP
[root@localhost ~]#
```

19. 为防御 IP 碎片攻击，设置 iptables 防火墙策略限制 IP 碎片的数量，仅允许每秒处理 1000 个，将 iptables 配置命令截图：

```
[root@localhost ~]# iptables -A FORWARD -f -m limit --limit 1000/s --limit-burst
1000 -j ACCEPT
[root@localhost ~]#
```

20. 为防止 SSH 服务被暴力枚举，设置 iptables 防火墙策略仅允许 172.16.10.0/24 网段内的主机通过 SSH 连接本机，将 iptables 配置命令截图：

```
[root@localhost ~]# iptables -I INPUT -p tcp --dport 22 -s 172.16.10.0/24 -j ACCE
PT
```