

Windows 安全策略与审计实验

一【实验目标】

- 掌握 Windows Server 2012 中安全审计策略的配置方法
- 掌握 Windows Server 2012 IE 浏览器安全设置的方法

二【实验环境】

- Windows Server 2012 操作系统

三【实验原理】

Windows Server 2012 作为微软公司 Windows 系列比较常用的服务器操作系统，在系统中设置很多安全和审计策略，以此来监控并防御各项具备可疑动机的行为。使用者可通过配置 Windows Server 2012 的账户策略、本地策略、审计策略和 IE 的增强安全策略全面地提升系统的安全性能。

账户策略为用户的安全登录提供了保障，它包括密码策略和账户锁定策略。其中，在密码策略中，使用者可设置密码的长度、使用的期限和修改的情况等；在账户锁定策略中，使用者可设置账户锁定的时间和锁定的阈值等。

本地策略详细设置全局管控。其中，使用者可对登录事件、对象访问、账户登录和驱动程序等进行管控。

审计策略获取并存储系统和应用程序生成的错误警告和其他信息，这些信息被存储为一条条记录，每条记录包括事件发生时间、事件源、事件号和所属类别、机器名、用户名和事件本身的详细描述。

四【实验步骤】

输入密码 Admin123456 进入 Windows Server 2012。

任务一：安全策略与审计功能的应用

1、点击【开始】→【管理工具】→【本地安全策略】。如图 1 所示

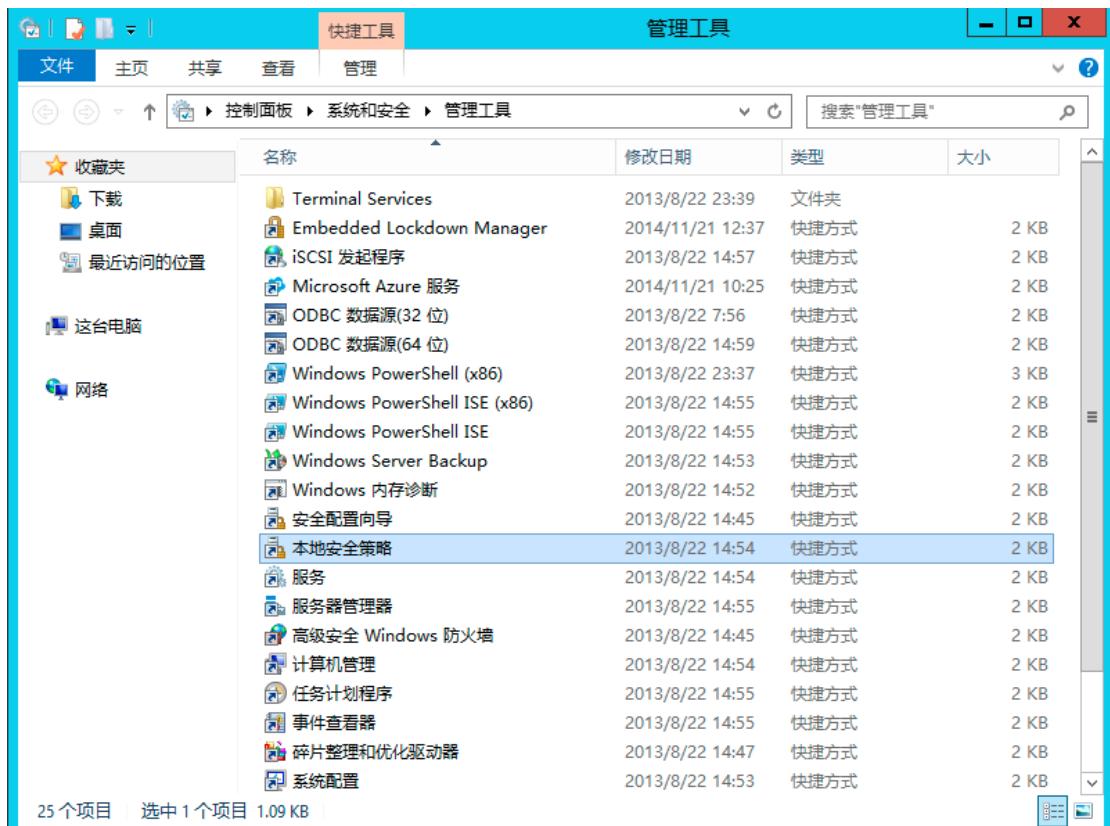


图 1：打开本地安全策略

2、点击【账户策略】→【密码策略】。如图 2 所示

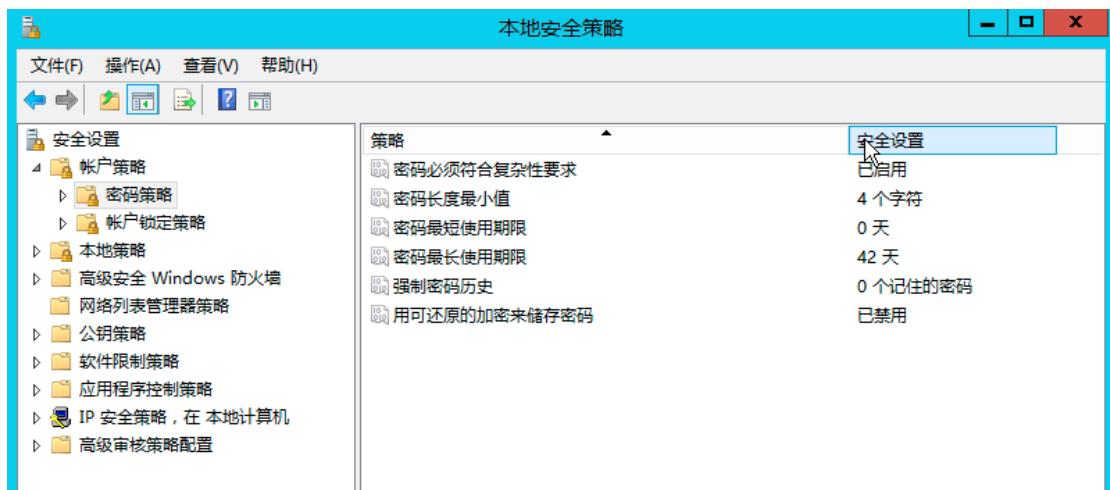


图 2：修改密码长度最小值

3、选中“密码长度最小值”，右键鼠标选择【属性】。如图 3 所示

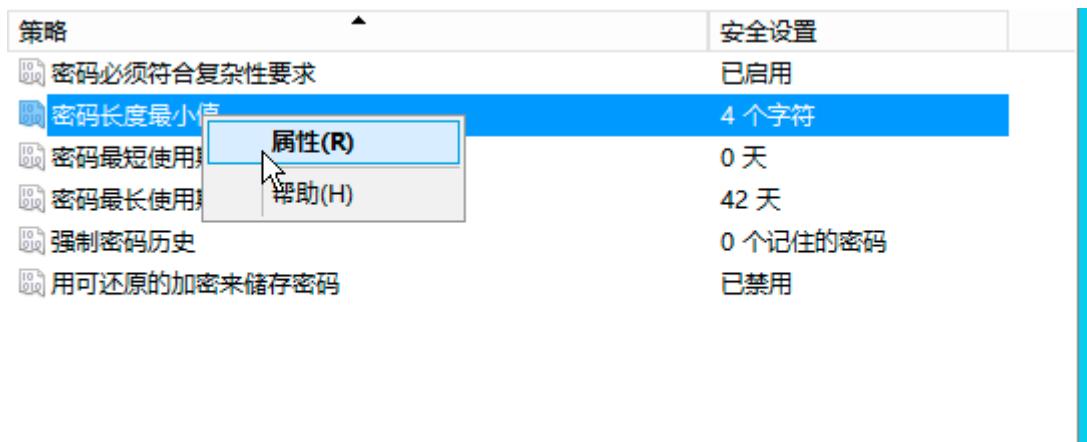


图 3：密码长度最小值属性

4、点击【说明】，该选项卡解释了该策略的含义。如图 4 所示

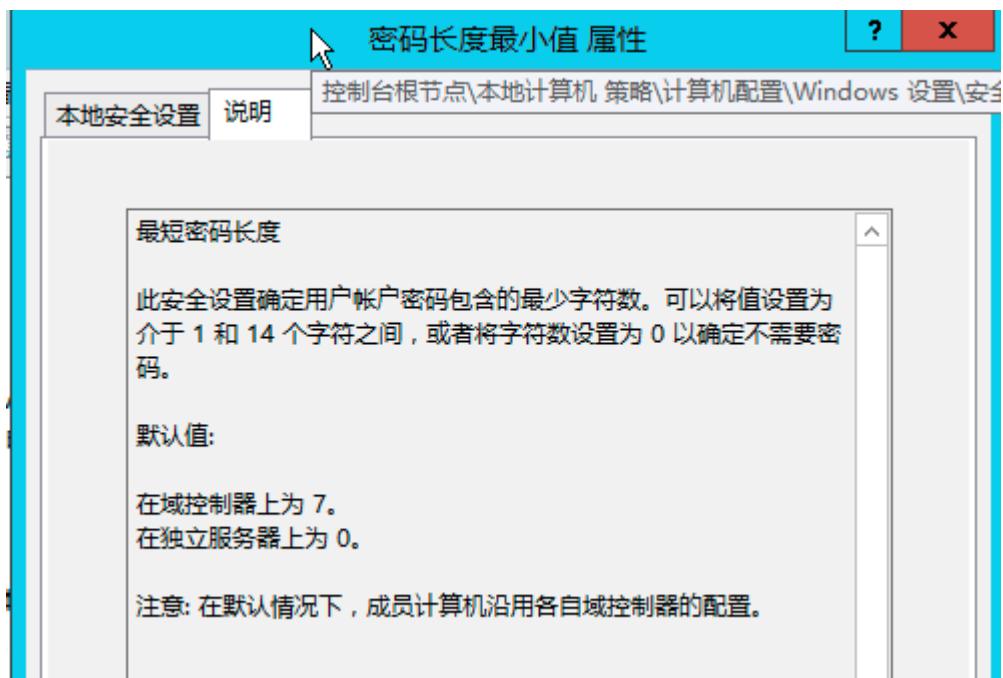


图 4：密码长度最小值说明

5、点击【本地安全设置】，输入“4”即密码最少为 4 个字符，点击【确定】。如图 5 所示



图 5：设置密码长度最小值

6、可以看到密码最小长度已经改为 4。如图 6 所示

| 策略 | 安全设置 |
|--------------|----------|
| 密码必须符合复杂性要求 | 已启用 |
| 密码长度最小值 | 4 个字符 |
| 密码最短使用期限 | 0 天 |
| 密码最长使用期限 | 42 天 |
| 强制密码历史 | 0 个记住的密码 |
| 用可还原的加密来储存密码 | 已禁用 |

图 6：密码策略列表

7、启用“密码必须符合复杂性要求”。如图 7 所示

| 策略 | 安全设置 |
|--------------|----------|
| 密码必须符合复杂性要求 | 已启用 |
| 密码长度最小值 | 4 个字符 |
| 密码最短使用期限 | 0 天 |
| 密码最长使用期限 | 42 天 |
| 强制密码历史 | 0 个记住的密码 |
| 用可还原的加密来储存密码 | 已禁用 |

图 7：密码复杂性要求

8、在“密码必须符合复杂性要求”处右键选择【属性】。如图 8 所示

| 策略 | 安全设置 |
|--------------|----------|
| 密码必须符合复杂性要求 | 已启用 |
| 密码长度最小值 | 4 个字符 |
| 密码最短使用期限 | 0 天 |
| 密码最长使用期限 | 42 天 |
| 强制密码历史 | 0 个记住的密码 |
| 用可还原的加密来储存密码 | 已禁用 |

图 8：密码复杂性属性

9、在【说明】选项卡中可以看到对该策略的解释说明，点击【确定】。如图 9 所示

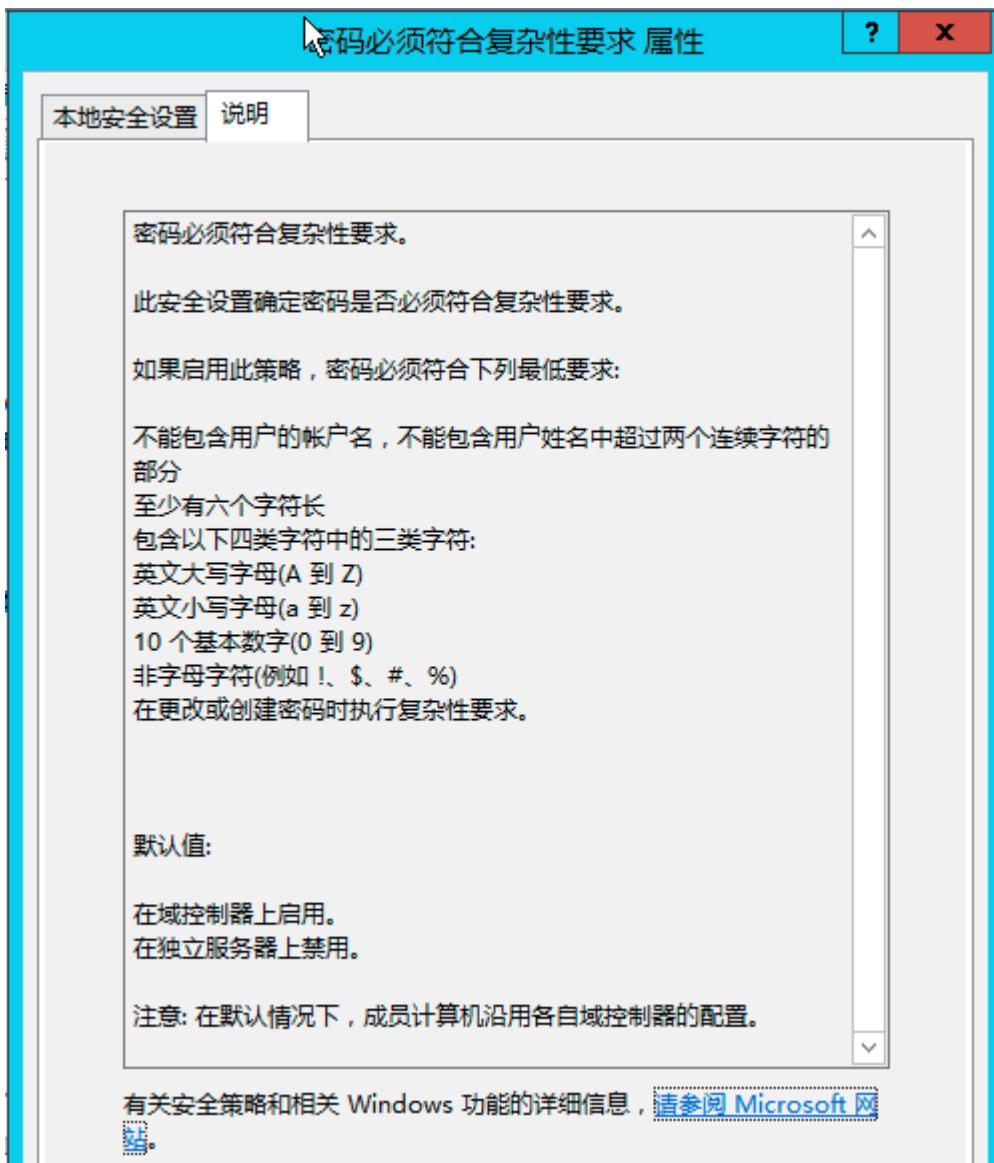


图 9：密码复杂性说明

10、点击【账户锁定策略】。如图 10 所示

The screenshot shows the '账户锁定策略' (Account Lockout Policies) section under '本地策略' (Local Policies) in the '安全设置' (Security Settings) console. The '账户锁定阈值' (Account lockout threshold) policy is selected, showing a value of '2 次无效登录' (2 failed logon attempts).

| 策略 | 安全设置 |
|---------------|----------------|
| 账户锁定时间 | 1 分钟 |
| 账户锁定阈值 | 2 次无效登录 |
| 重置账户锁定计数器 | 1 分钟之后 |

图 10：账户锁定阈值

11、在“账户锁定阈值”处鼠标右键选择【属性】。如图 11 所示

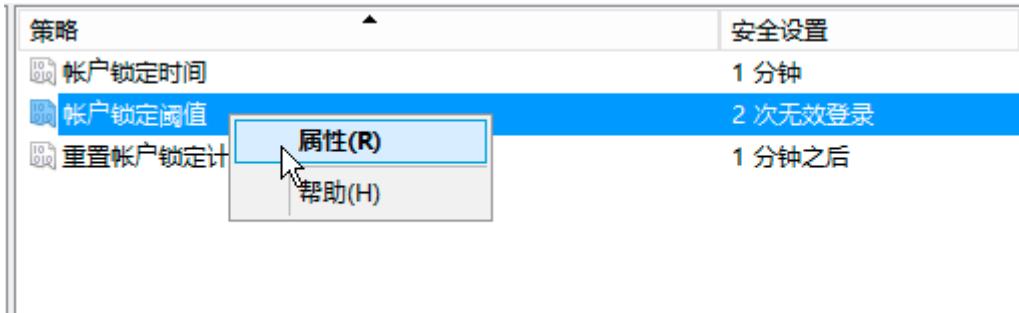


图 11：账户锁定阈值属性

12、点击【说明】选项卡，该选项卡可以看到对该策略的解释说明。如图 12 所示

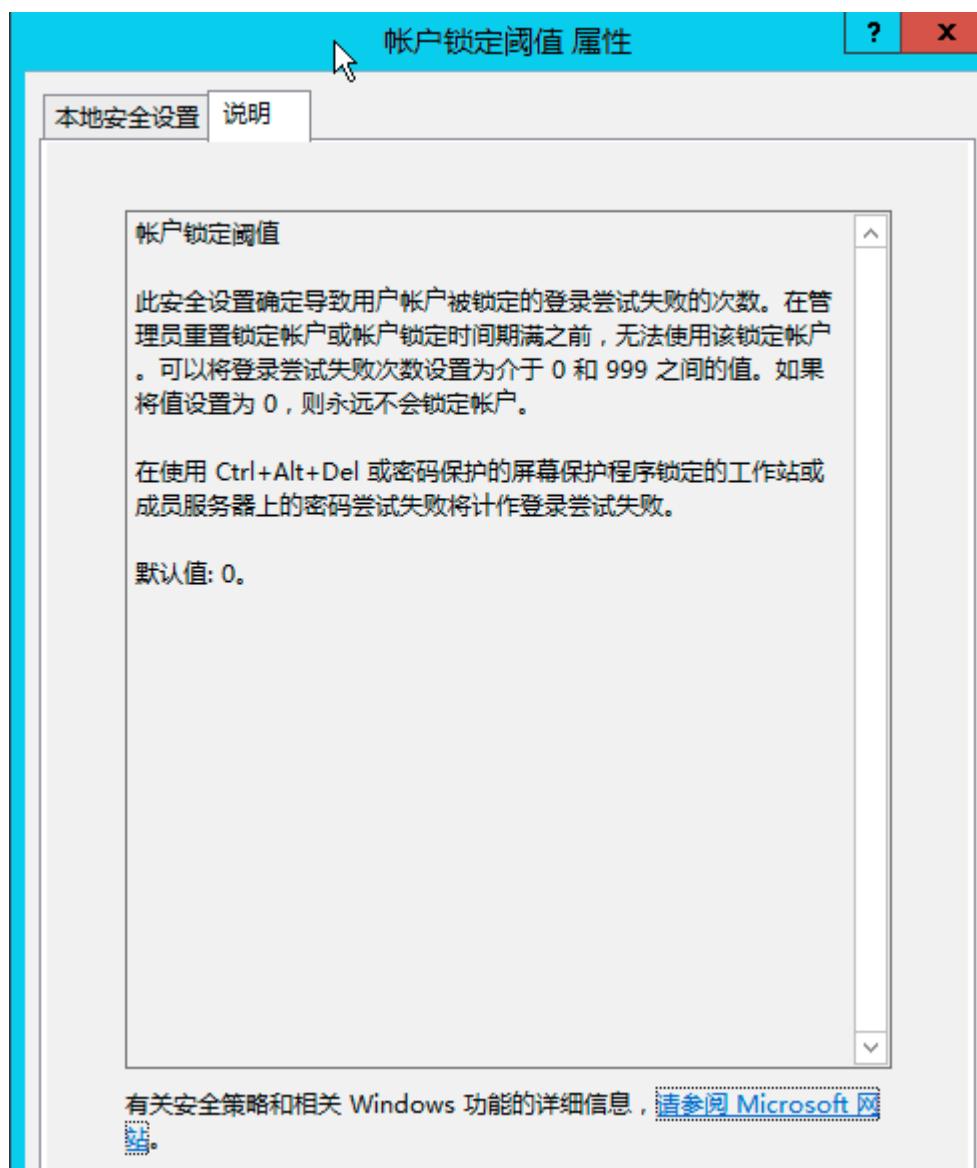


图 12：账户锁定阈值说明

13、点击【本地安全设置】，输入“2”，即当密码输入错误超过两次时，该账号

将会被锁住，点击【确定】。如图 13 所示

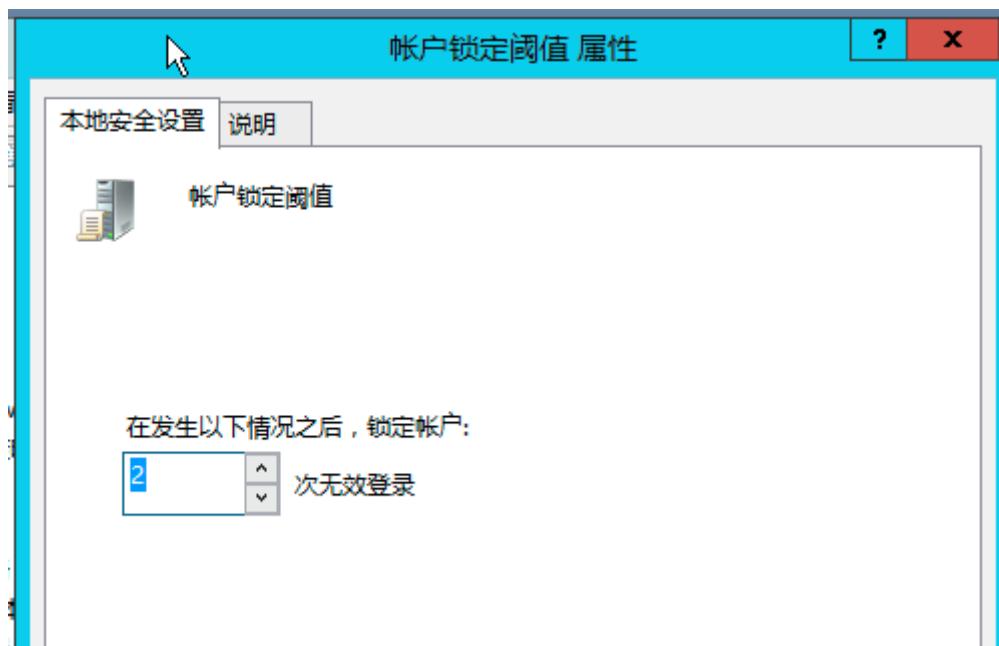


图 13：设置阈值

14、在弹出的窗口中点击【确定】。如图 14 所示

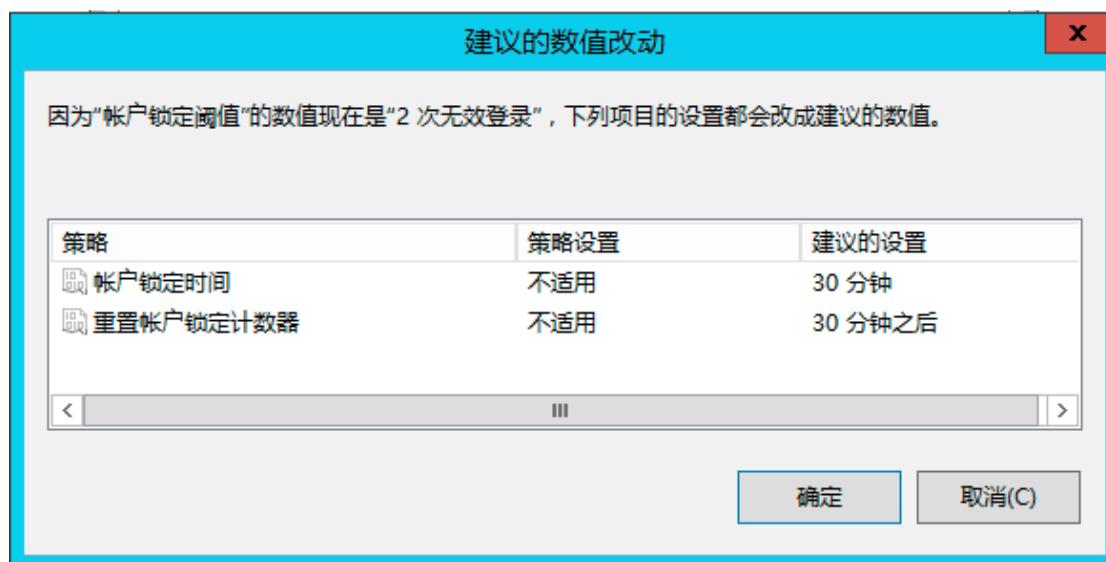


图 14：锁定时间

15、在“账户锁定时间”处鼠标右键选择【属性】。如图 15 所示

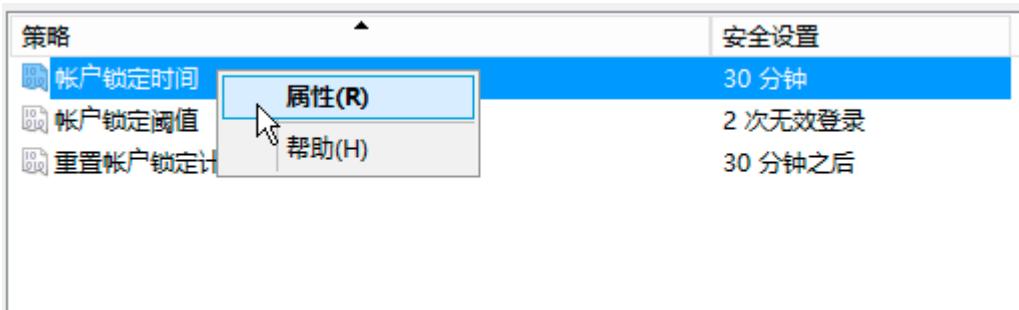


图 15：账户锁定时间属性

16、点击【说明】选项卡，该选项卡解释了该策略的含义、如图 16 所示

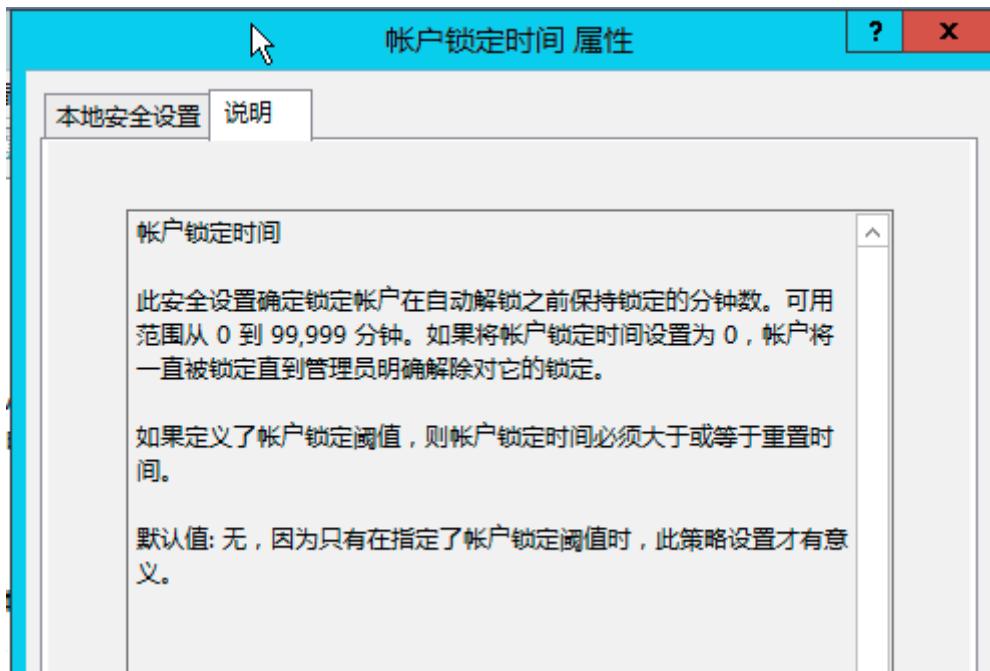


图 16：账户锁定时间说明

17、点击【本地安全设置】，输入“1”，即账户锁定一分钟后自动解锁，点击【确定】。如图 17 所示



图 17：修改账户锁定时间

18、在弹出的窗口中点击【确定】。如图 18 所示

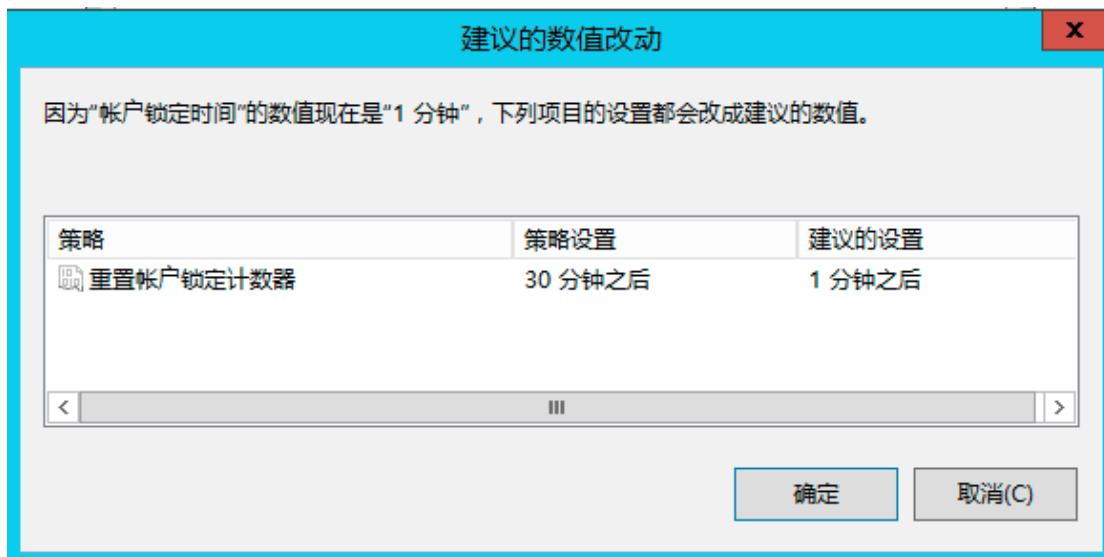


图 18：确认修改账户锁定时间

19、可以看到账户锁定时间已经改为 1 分钟。如图 19 所示

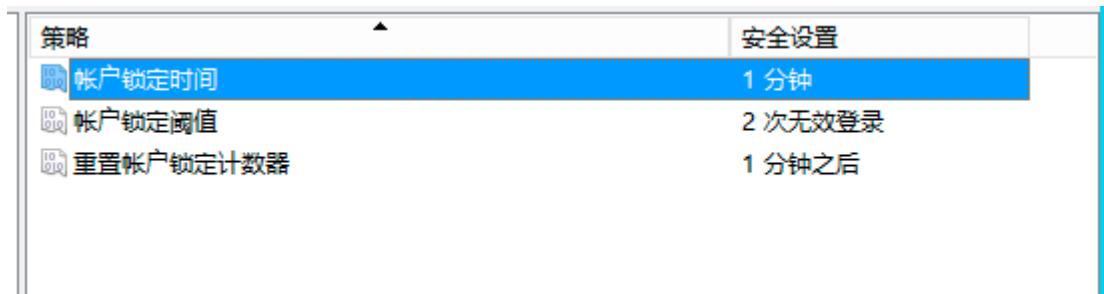


图 19：账户锁定时间修改完成

20、点击【本地策略】→【审核策略】。如图 20 所示



图 20：审核策略列表

21、在“审核对象访问”处鼠标右键选择【属性】。如图 21 所示

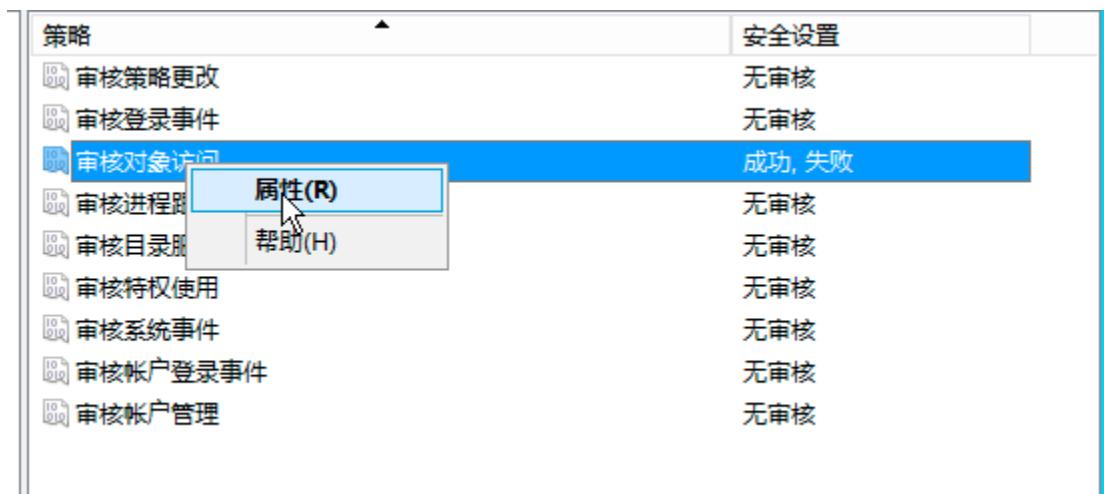


图 21：审核对象访问属性

22、点击【说明】可以查看该策略的含义。点击【本地安全设置】，勾选“成功”和“失败”，点击【确定】。如图 22 所示

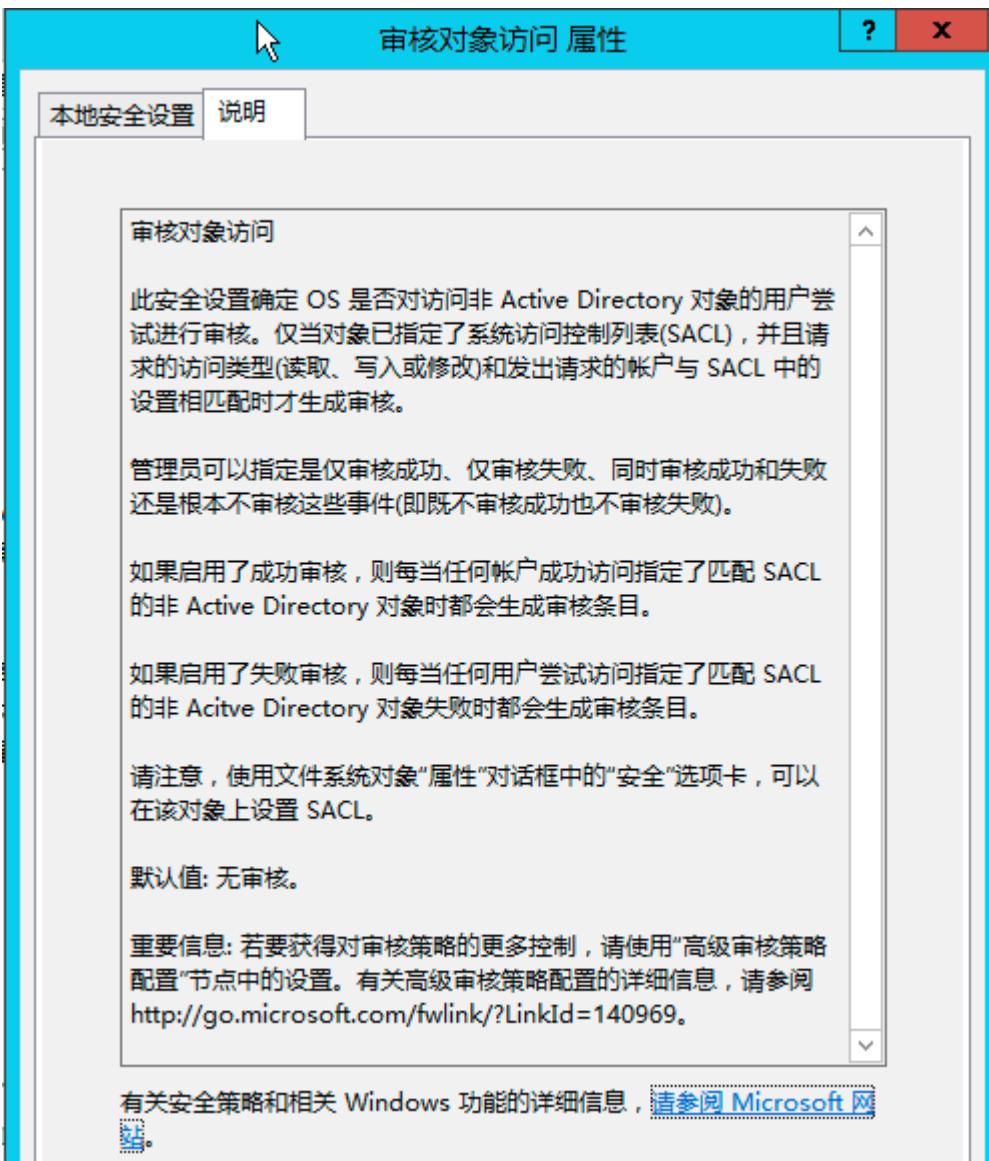


图 22：审核成功和失败事件

23、在【审核登录事件】处右击鼠标选择【属性】勾选“成功”和“失败”，点击【确定】。如图 23 所示



图 23：审核成功和失败事件

24、在【审核账户登录事件】处鼠标右键选择【属性】，在【本地安全设置】页面中勾选“成功”和“失败”，点击【确定】。如图 24 所示



图 24: 审核成功和失败事件

25、在【审核账户管理】处右键鼠标，选择【属性】，点击【本地安全设置】，勾选“成功”和“失败”，点击【确定】。如图 25 所示



图 25: 审核成功和失败事件

26、查看审核策略配置。如图 26 所示

| 策略 | 安全设置 |
|----------|--------|
| 审核策略更改 | 无审核 |
| 审核登录事件 | 成功, 失败 |
| 审核对象访问 | 成功, 失败 |
| 审核进程跟踪 | 无审核 |
| 审核目录服务访问 | 无审核 |
| 审核特权使用 | 无审核 |
| 审核系统事件 | 无审核 |
| 审核帐户登录事件 | 无审核 |
| 审核帐户管理 | 成功, 失败 |

图 26: 审核策略列表

27、运行 IE 浏览器，可以看到阻止连接的页面，这是由于默认主页不是可信任站点，浏览器阻止其连接。点击【添加】。如图 27 所示



图 27：添加可信站点

28、在弹出的窗口中点击【添加】之后点击【关闭】。如图 28 所示

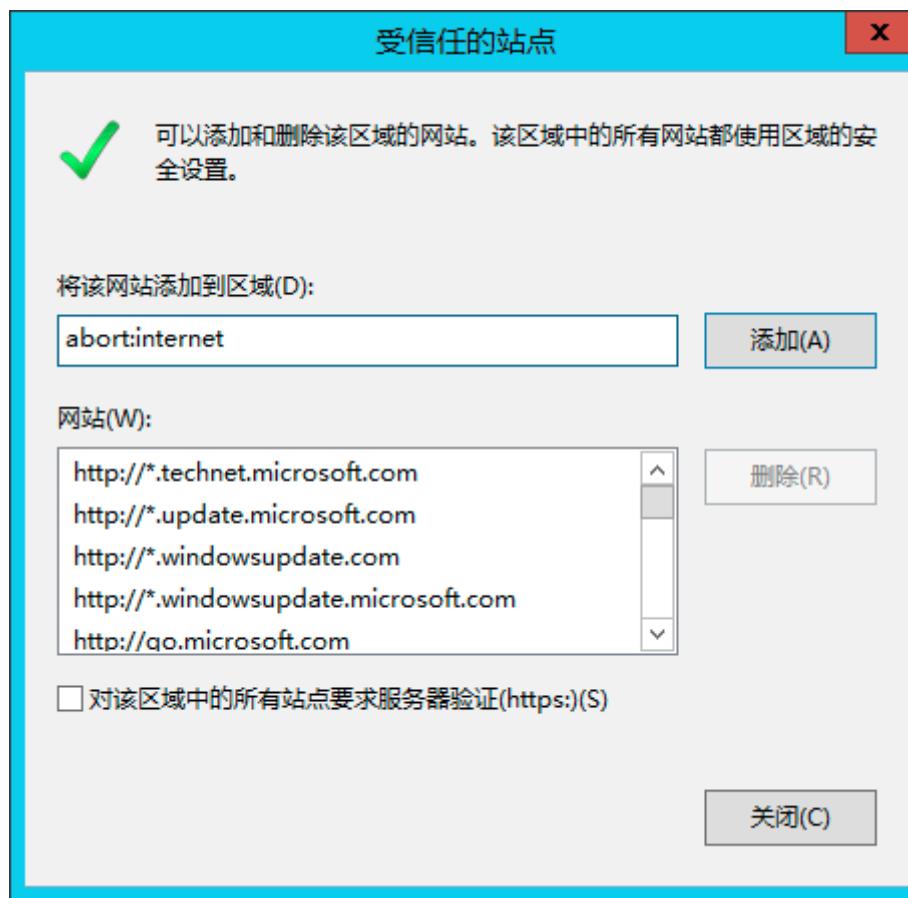


图 28：添加可信站点

29、点击【工具】→【Internet 选项】。如图 29 所示

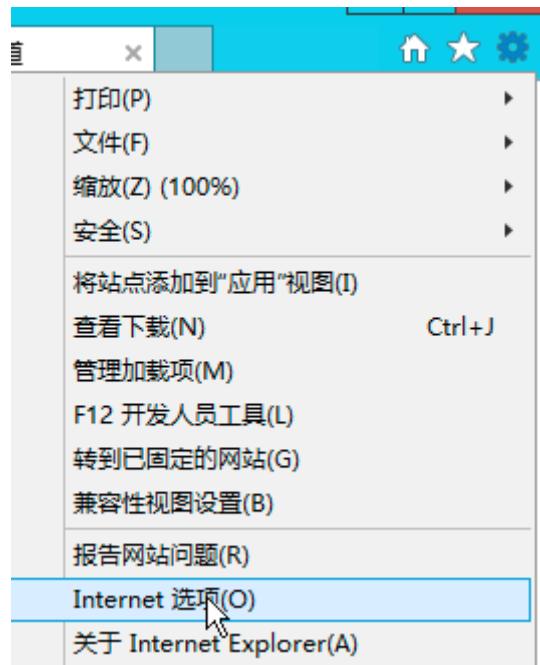


图 29：打开 Internet 选项

30、点击【安全】→【受信任的站点】→【站点】。如图 30 所示



图 30：点击站点

31、可以看到刚刚添加的主页，点击【关闭】。如图 31 所示

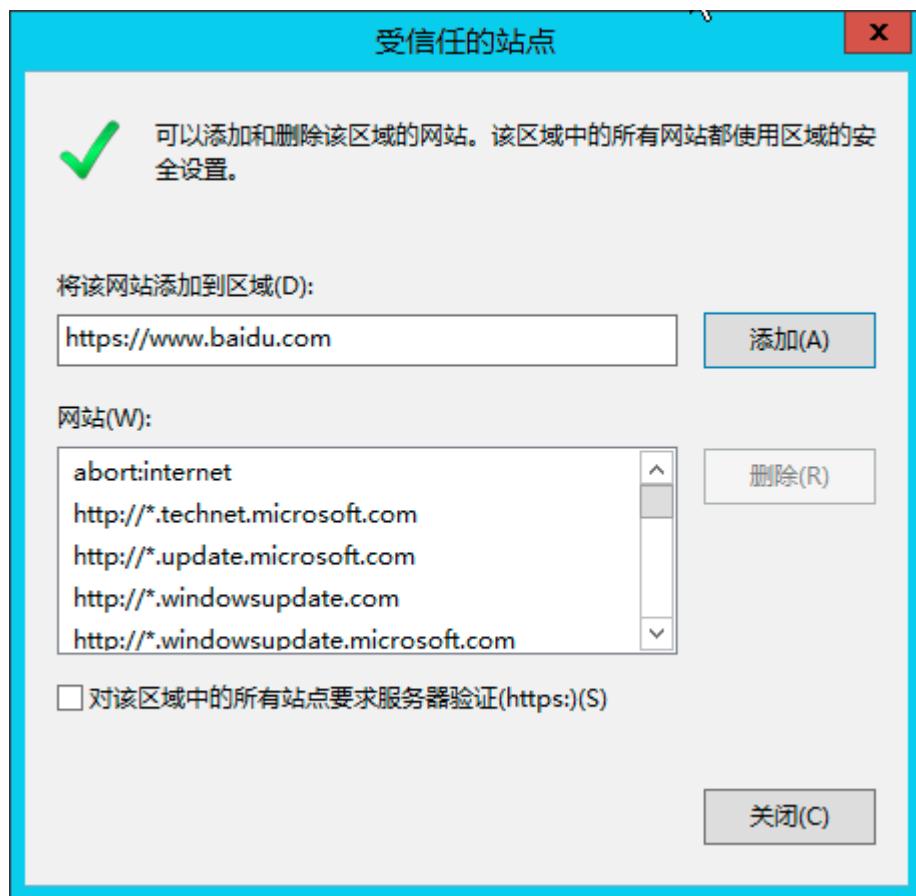


图 31：查看安全站点

32、点击【自定义级别】。如图 32 所示

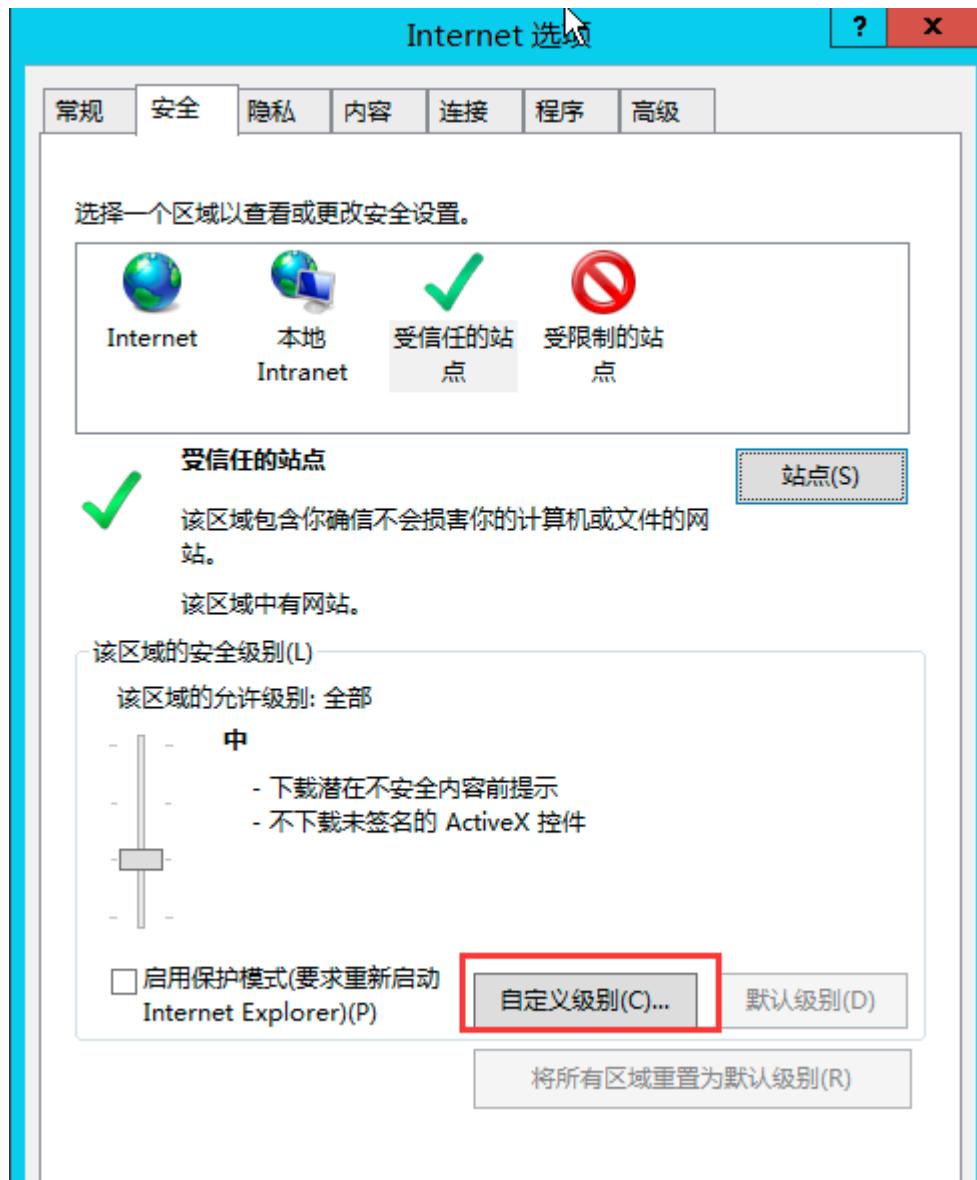


图 32：自定义级别

33、可以自定义受信任站点的安全级别，默认是“中”。如图 33 所示

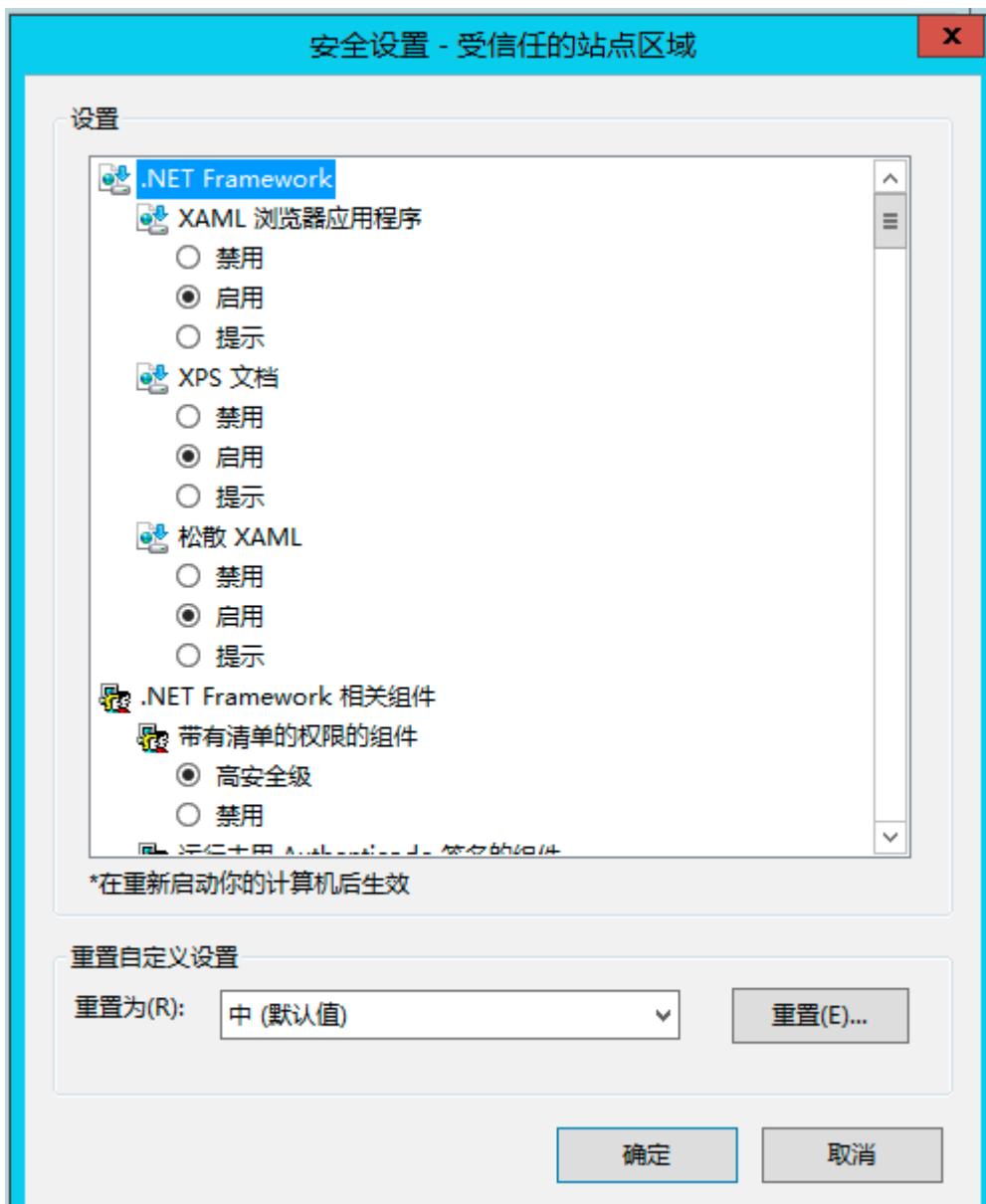


图 33: 自定义级别

34、点击【内容】，点击“自动完成”后面的【设置】。如图 34 所示

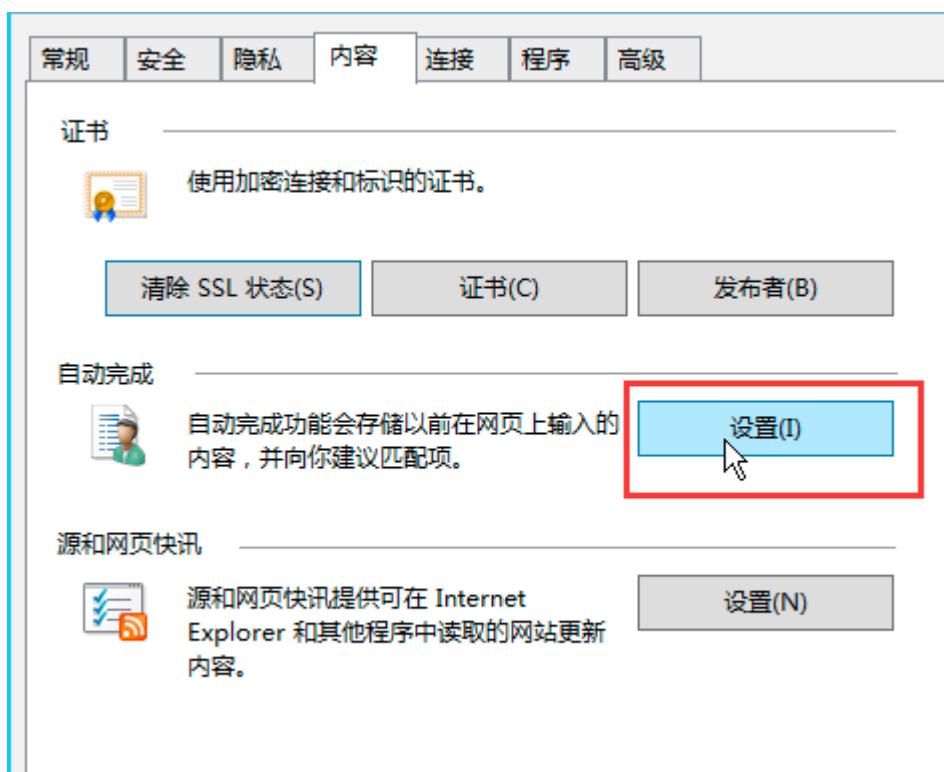


图 34：自动完成设置

35、浏览器的自动完成功能可以帮用户做很多事情，比如提醒用户记住密码，以便下次不再输入密码等等，根据需要来选择勾选的功能，这里保持默认设置，点击【确定】。如图 35 所示

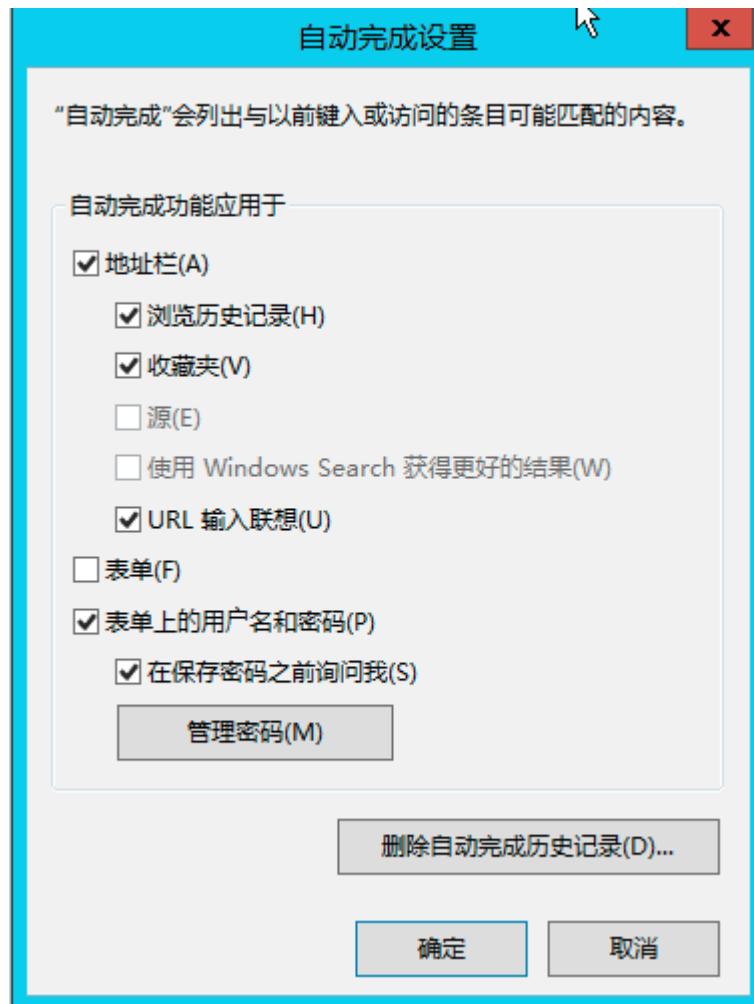


图 35：自动完成设置选项

36、点击【开始】→【命令提示符】。如图 36 所示



图 36：打开命令提示符

37、在命令行下输入“net user test1 Aa1234 /add”，新建一个用户名为“test1”的用户，密码为“Aa1234”，这里需要注意，设置密码需要满足密码策略即最小长度以及复杂性要求。如图 37 所示



```
管理员: 命令提示符
Microsoft Windows [版本 6.3.9600]
(c) 2013 Microsoft Corporation。保留所有权利。
C:\Users\Administrator>net user test1 Aa1234 /add
命令成功完成。

C:\Users\Administrator>
```

图 37：添加用户

【实验预期】

- 1、连续两次输入错误密码，“test1”用户被锁定。
- 2、Windows 日志记录用户的注销、登录以及账户修改情况。
- 3、IE 浏览器不再显示连接阻断页面。

【实验结果】

- 1、右击【开始】，点击“关机或注销”，点击【注销】。如图 38 所示

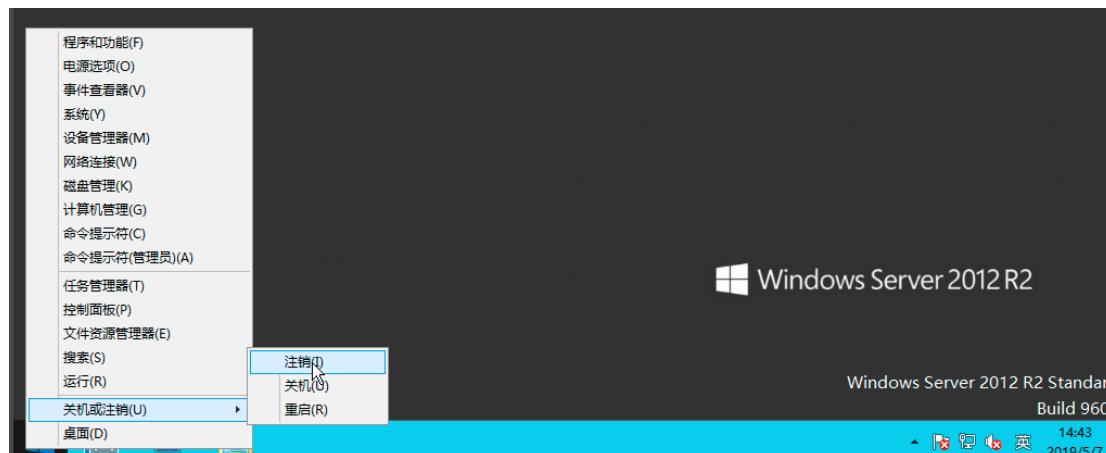


图 38：注销当前用户

- 2、以“test1”账户登录，连续两次输入错误密码，再次输入正确密码，“test”账户被锁定。如图 39 所示



图 39：账户锁定

3、等待一分钟以后，输入用户名“test1”，密码“Aa1234”，即可登录系统。
打开命令提示符，输入“whoami”，即可查看当前用户。如图 40 所示



图 40：查看当前用户

4、注销 test1 账户，以管理员账户（Administrator）登录，密码为“Admin123456”。点击【开始】→【管理工具】→【事件查看器】。如图 41 所示

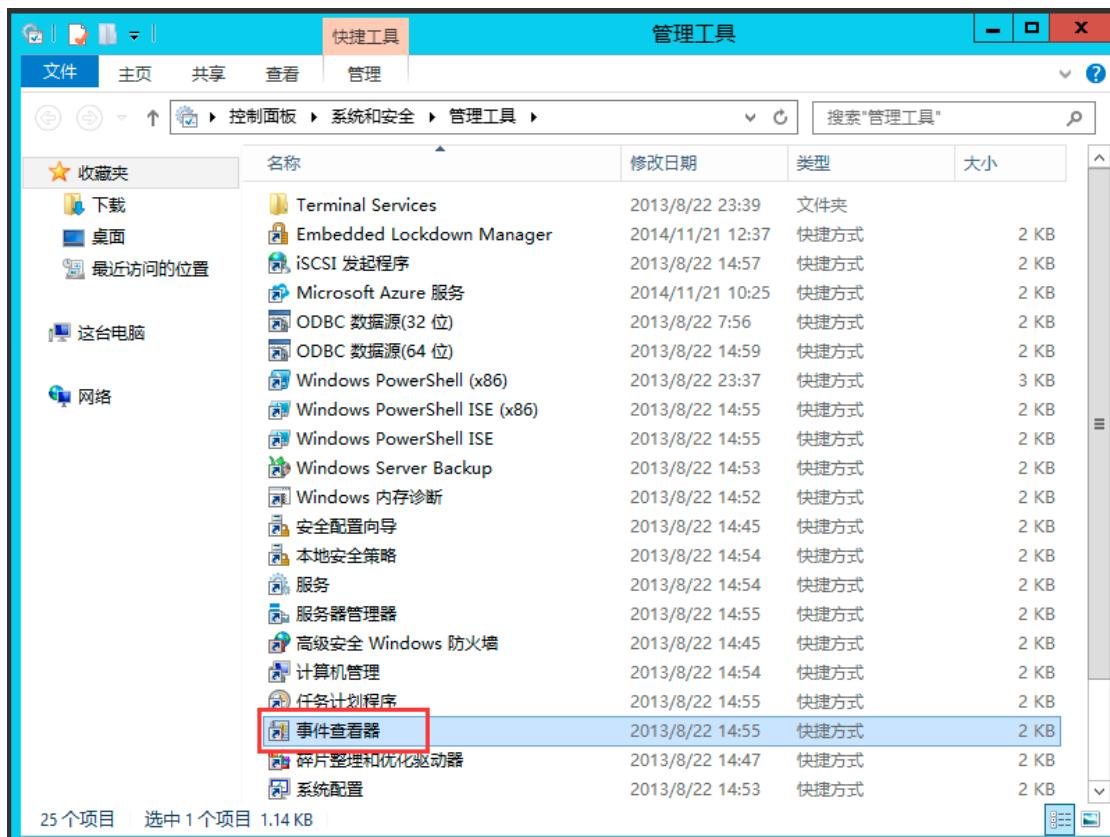


图 41：打开事件查看器

5、点击“Windows 日志”，点击“安全”，即可查看账户注销、登录、增加记录。如图 42 所示

| 安全 事件数: 33,208 (!) 可用的新事件 | | | | |
|---------------------------|-------------------|----------|-------|-----------|
| 关键字 | 日期和时间 | 来源 | 事件 ID | 任务类别 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 5152 | 筛选平台数据包丢弃 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 5152 | 筛选平台数据包丢弃 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 5152 | 筛选平台数据包丢弃 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 5152 | 筛选平台数据包丢弃 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 5152 | 筛选平台数据包丢弃 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 4624 | 登录 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 4648 | 登录 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 4776 | 凭据验证 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 5157 | 筛选平台连接 |
| 审核... | 2019/5/7 14:46:41 | Micro... | 5152 | 筛选平台数据包丢弃 |

图 42：查看事件日志

6、重启浏览器，发现之前的连接阻断页面已经消失。如图 43 所示



图 43：打开浏览器

五【实验思考】

- 用“net user”命令新建用户，并且使得所设密码不符合密码策略，查看结果。