北京邮电大学网络空间安全学院
信息安全认知实习
实验报告

课程名称：信息安全认知实习

单元名称：操作系统安全实验

姓名：任子恒

学号：2017522133

班级：2017661801

专业：信息安全

指导教师：颉夏青

成绩：

日　　期：2018 年 9 月 15 日

一、 实验目的

通过学习并实现针对个人系统的安全配置，对自己操作系统的安全有一个初步的认知；初步学习组策略、系统日志等系统自带的配置工具。

本次实验主要针对 Windows 系统，今后会学习到与 Linux 系统相关的安全知识。

二、 实验原理

Windows 在所有专业版系统中都自带有用户管理工具和组策略管理(gpedit.msc)，即使没有这些工具，在命令行下也可以完成部分管理操作。

日志文件是 Windows 系统中一个比较特殊的文件，它记录着 Windows 系统中所发生的一切，如各种系统服务的启动、运行、关闭等信息。 Windows 日志包括应用程序、安全、系统等几个部分，它的存放路径是“%systemroot%\system32\config”，应用程序日志、安全日志和系统日志对应的文件名为 AppEvent.evt、SecEvent.evt 和 SysEvent.evt。这些文件受到“Event Log（事件记录）”服务的保护不能被删除，但可以被清空。（来自百度经验）

三、 实验环境

“配置本地安全策略”在 Windows 10 专业版 64 位系统下进行（10.0，版本 10240）。

“开启防火墙”和“审核 Windows 日志”在 Windows 10 家庭版 64 位系统下进行（10.0，版本 17134）。

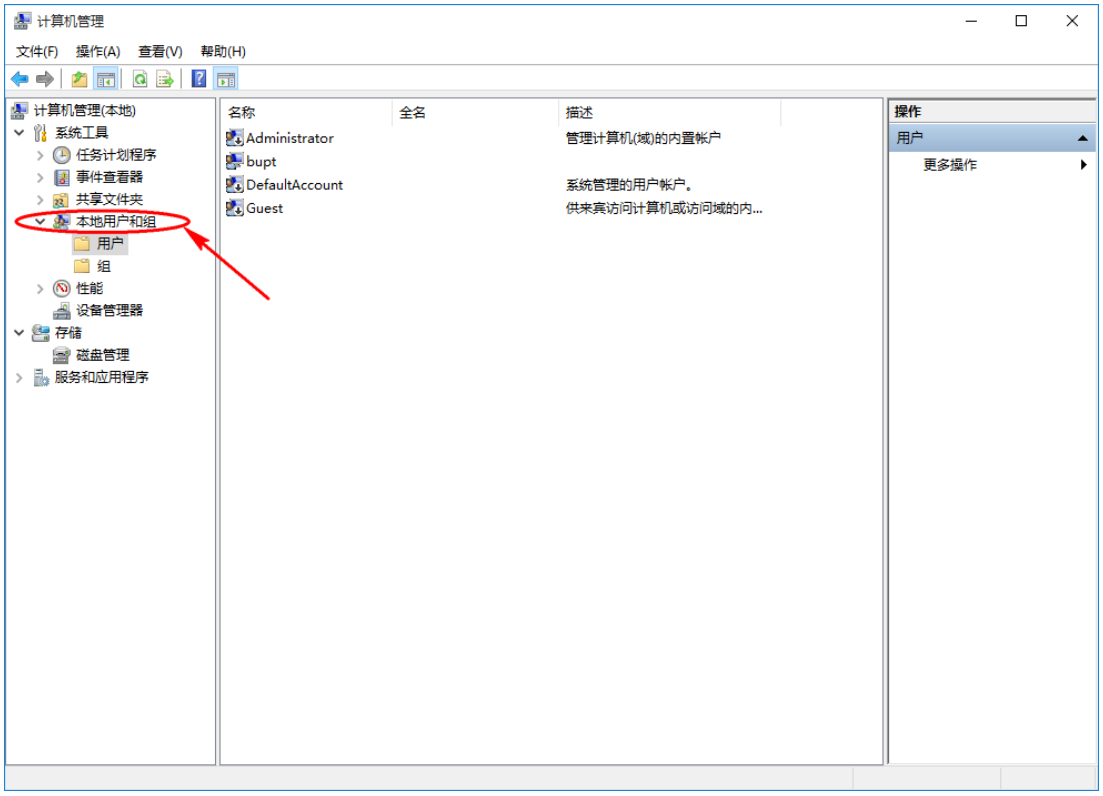
四、 实验过程及遇到的问题分析

4.1 实验过程

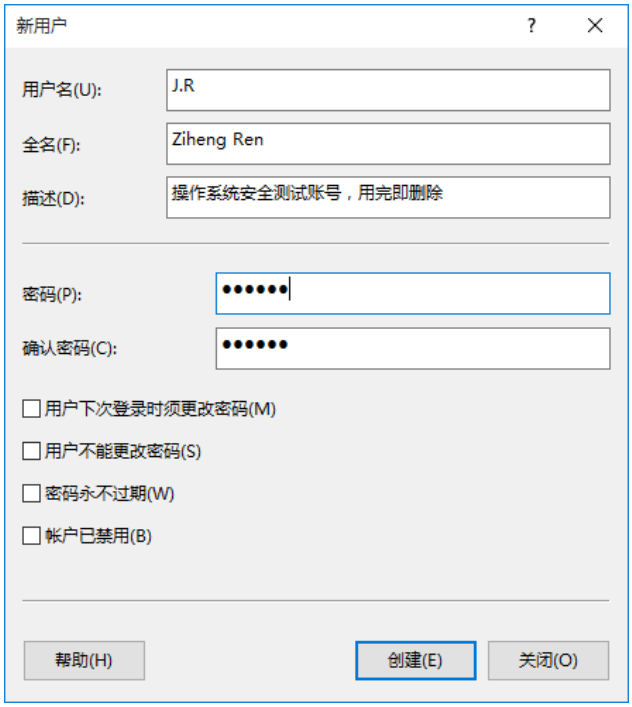
4.1.1 配置本地安全策略

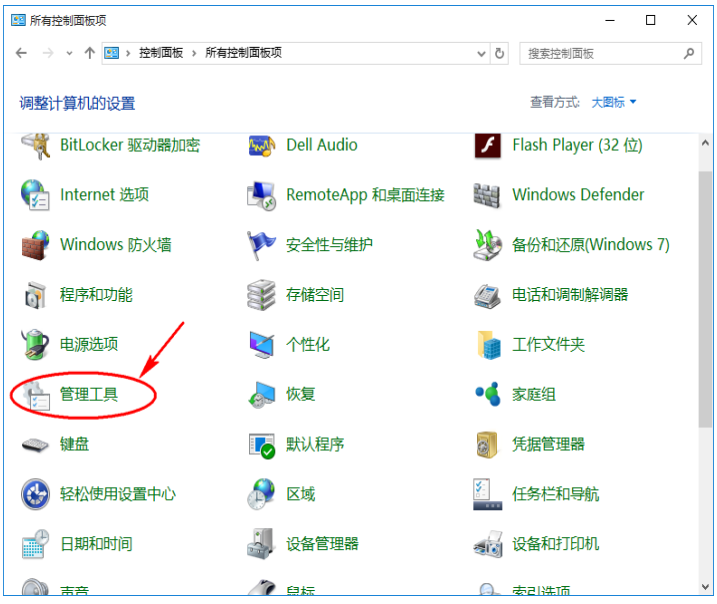
1.右击桌面上的“此电脑”，进入“计算机管理”界面。

2. 依次展开“系统工具”→“本地用户和组”→“用户”。



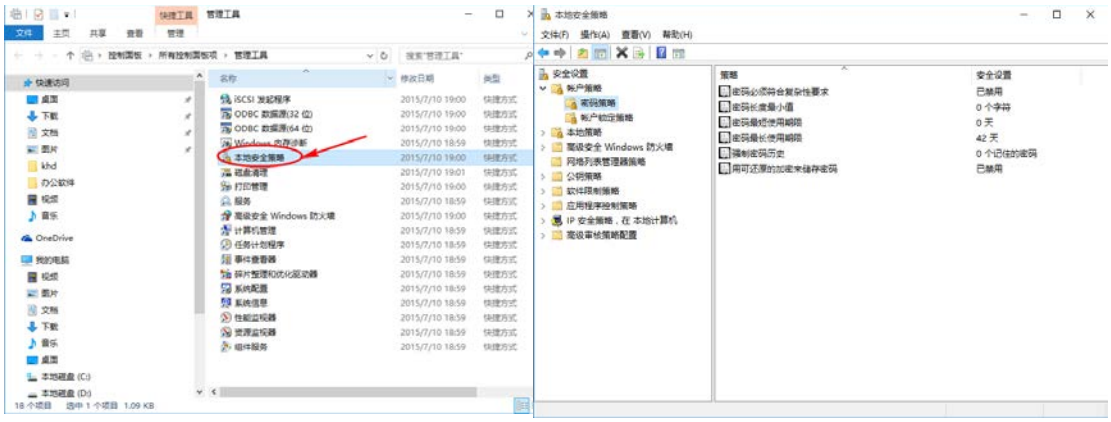
3. 新建一个用户。注意下方的设置。





4. 进入“控制面板”，找到“管理工具”。

5. 双击“本地安全策略”。并展开“账户策略”。

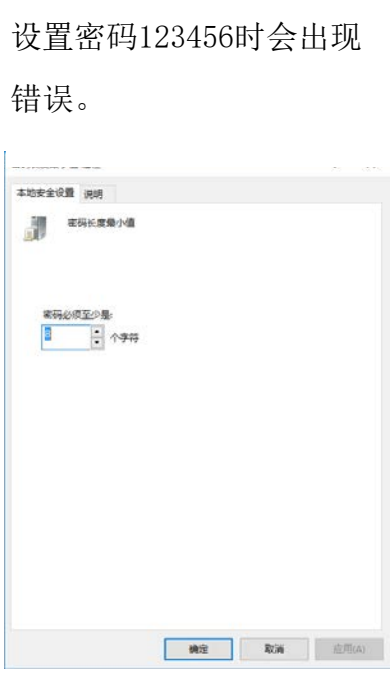


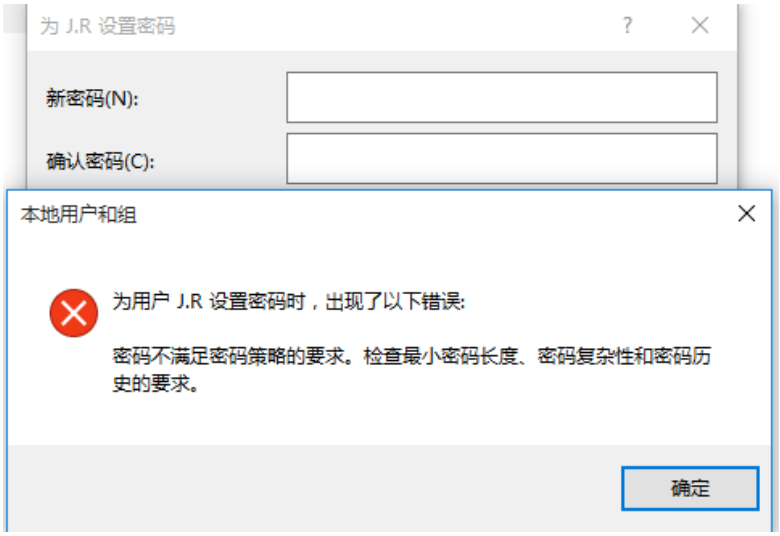
① 密码策略

i. 对“密码必须符合复杂性要求”，选择“已启用”。

这意味着创建和更改密码时至少有六个字符长，至少包含英文大写字母、小写字母、10个基本数字、非字母字符中的三种，不能包含用户的账户名，不能包含用户姓名中超过两个连续字符的部分。

启用后，试图对新用户 J.R 设置密码123456时会出现错误。





ii.对“密码长度最小值”，设置为≥8位。

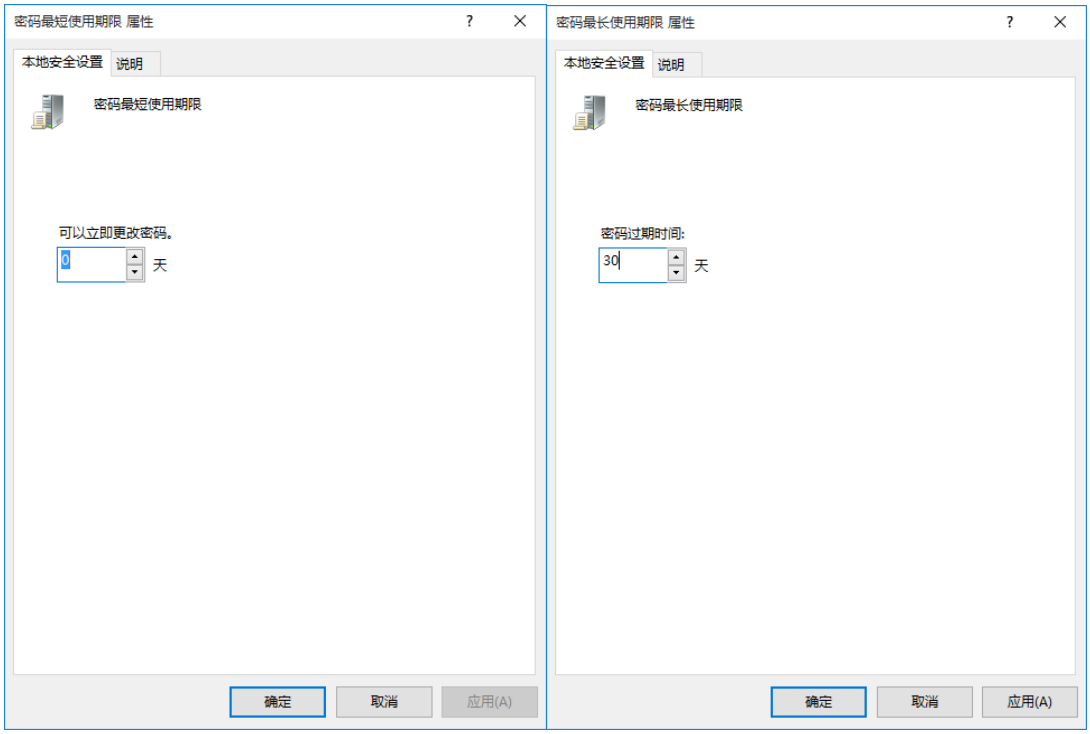
启用后，试图对新用户 J.R 设置密码1234567时会发生错误，错误信息同6.

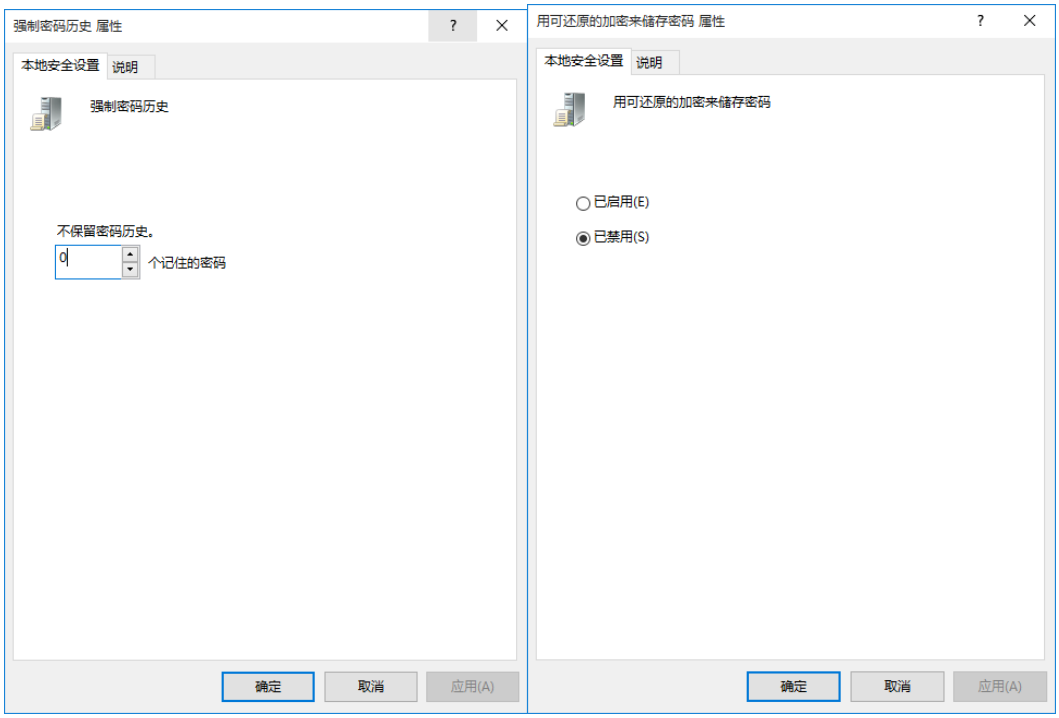
iii.对“密码最短使用期限”，保留默认设置（0天）。

iiii.对“密码最长使用期限”，设置为30天。

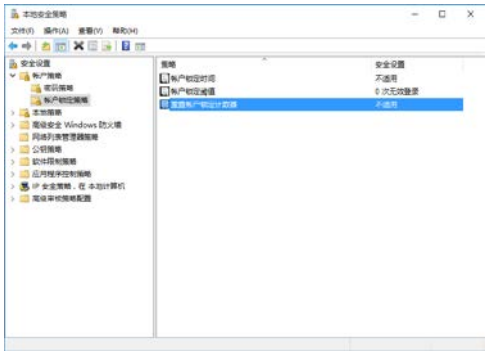
v.对“强制密码历史”，保持默认设置（0个）。

vi.对“用可还原的加密来储存密码”，保持默认设置（已禁用）。





② 账户锁定策略



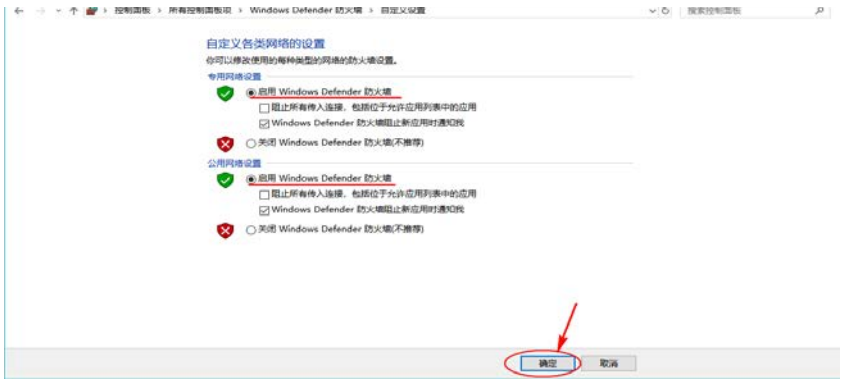
全部保持默认设置。

4.1.2 开启防火墙

1.进入“控制面板”，找到“Windows Defender 防火墙”。

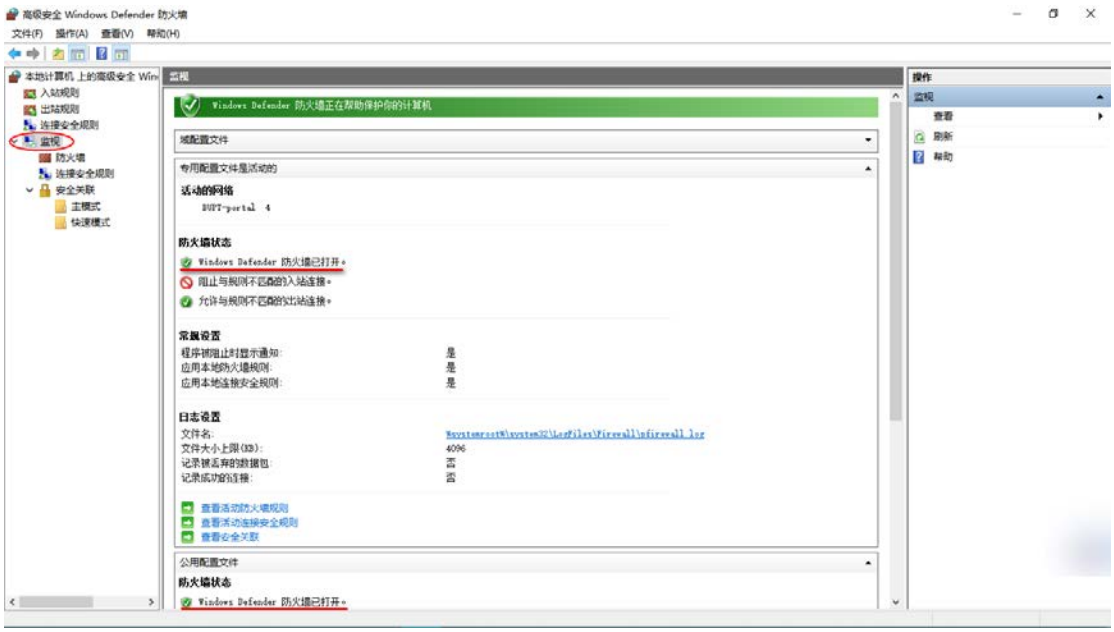
2. 点击左侧的“启用或关闭 Windows 防火墙”。

3. 确认“专用网络设置”和“公用网络设置”中都选中“启用 Windows Defender 防火墙”。



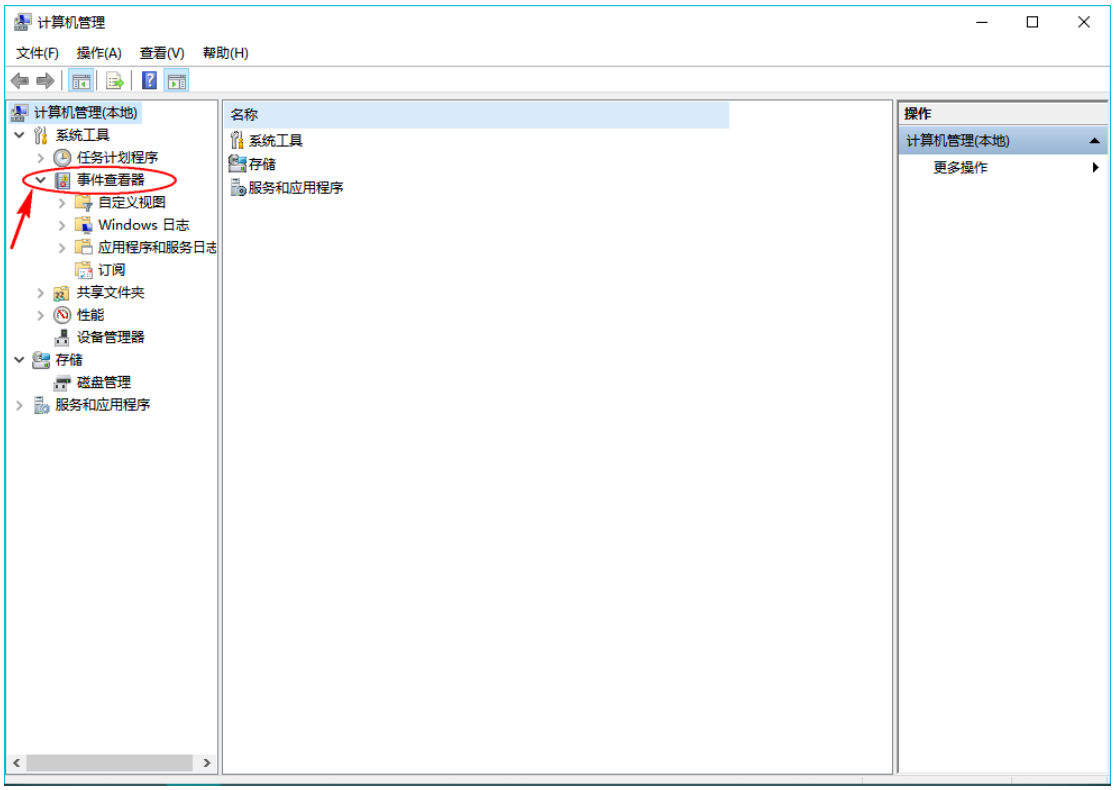
4. 可以进入“高级设置”，进一步验证防火墙有无开启。

点击第二步的“高级设置”以进入。

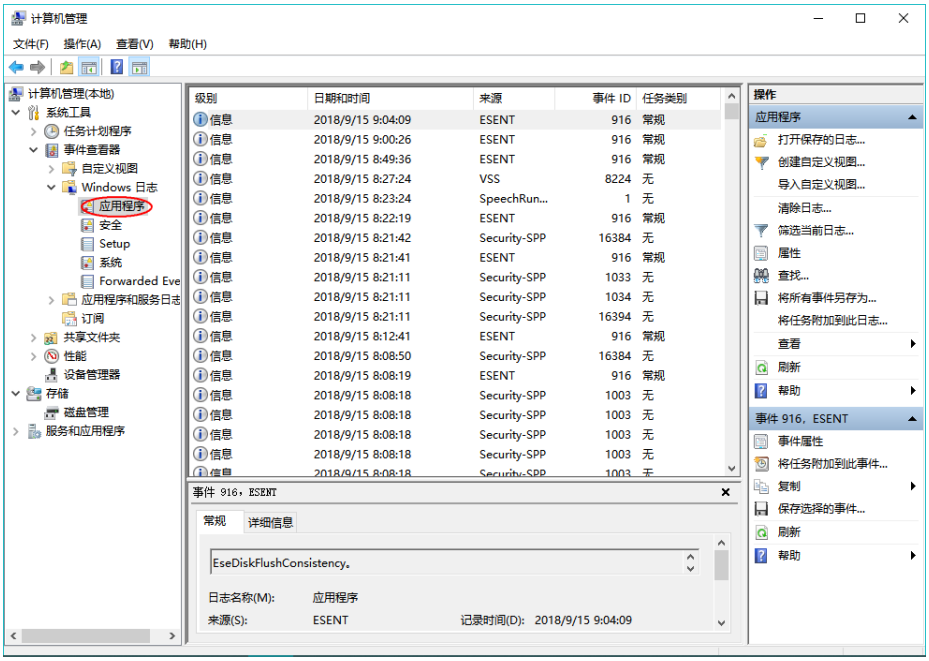


4.1.3 审核 Windows 日志

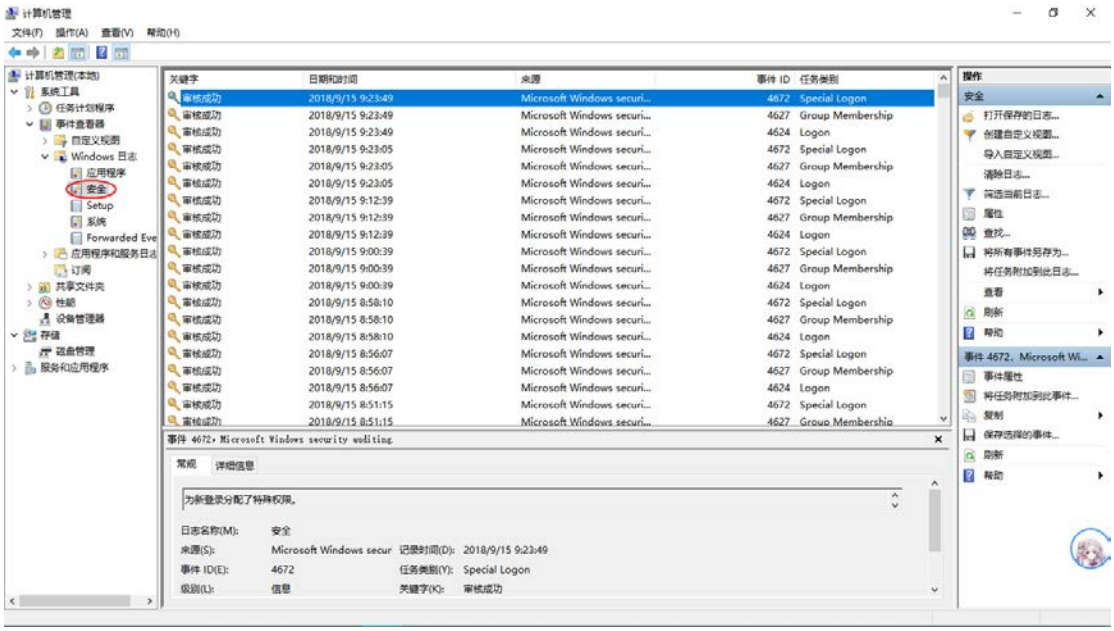
1. 右击桌面上的“此电脑”，进入“计算机管理”界面。



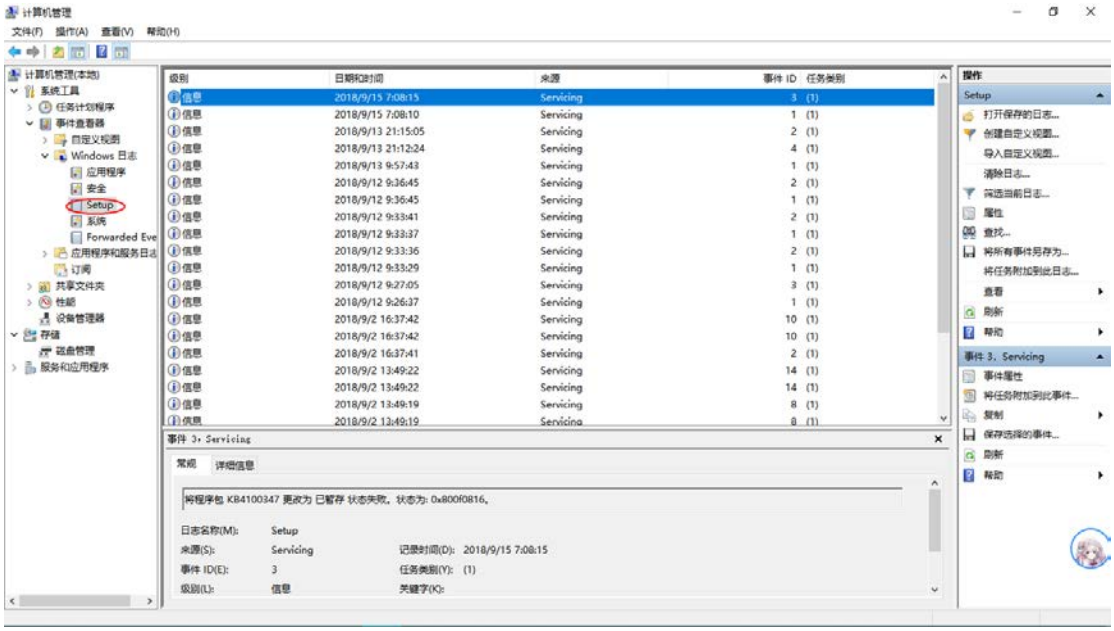
2. 依次展开“系统工具”→“事件查看器”→“Windows 日志”。



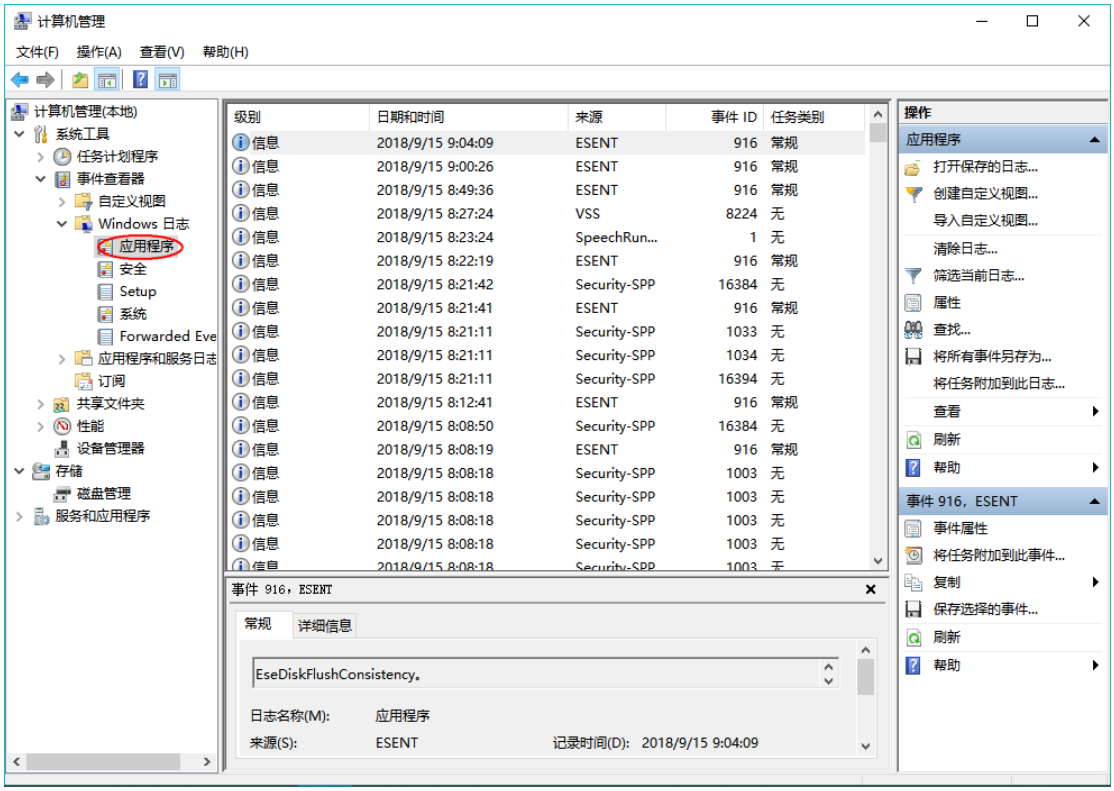
3. 还可以查看“安全”，“应用程序”，“Setup”中的信息。**其中都可以发现，正常状况下，日志中“信息”记录的占比应该很大，偶尔存在少量的“错误”和“警告”记录。“安全”中，大部分都是“审核成功”记录。**



“安全”，其中记录的内容可能与授权相关。



“Setup”，可能与 Windows 自动更新有关。



“应用程序”，可能与系统中非自带的程序有关。

4.2 问题分析

4.2.1 Windows 日志审核

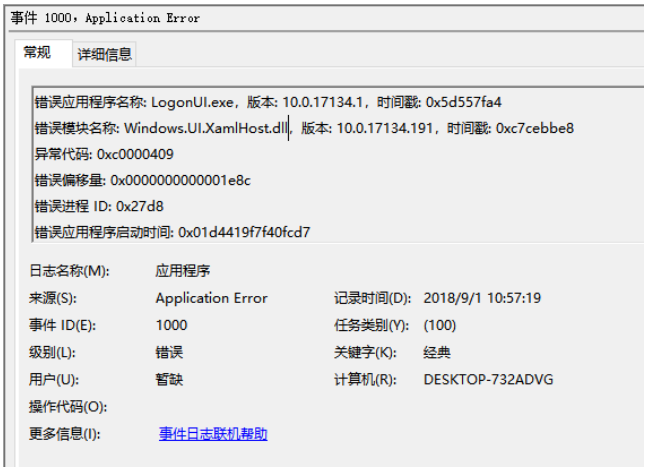
发生在自己电脑上的部分异常的分析

1.“系统”部分的一个异常分析

正常状况下，日志中“信息”记录的占比应该很大，偶尔存在少量的“错误”和“警告”记录。但在我的电脑上，我发现在9月1日上午约11点的“应用程序”记录中，出现了一个“错误”紧接着一个“信息”的异常。

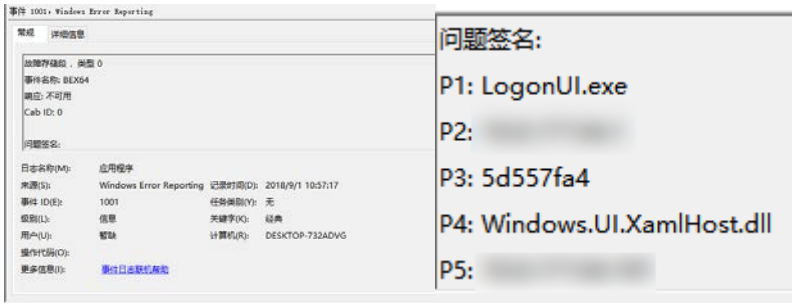
级别	日期和时间	来源	事件 ID	任务类别
信息	2018/9/1 10:57:15	Windows E...	1001	无
错误	2018/9/1 10:57:15	Application...	1000	(100)
信息	2018/9/1 10:57:15	Windows E...	1001	无
错误	2018/9/1 10:57:16	Application...	1000	(100)
信息	2018/9/1 10:57:16	Windows E...	1001	无
错误	2018/9/1 10:57:16	Application...	1000	(100)
信息	2018/9/1 10:57:16	Windows E...	1001	无
错误	2018/9/1 10:57:17	Application...	1000	(100)
信息	2018/9/1 10:57:17	Windows E...	1001	无
错误	2018/9/1 10:57:17	Application...	1000	(100)
信息	2018/9/1 10:57:17	Windows E...	1001	无
错误	2018/9/1 10:57:18	Application...	1000	(100)
信息	2018/9/1 10:57:18	Windows E...	1001	无
错误	2018/9/1 10:57:18	Application...	1000	(100)
信息	2018/9/1 10:57:19	Windows E...	1001	无
错误	2018/9/1 10:57:19	Application...	1000	(100)
信息	2018/9/1 10:57:19	Windows E...	1001	无
错误	2018/9/1 10:57:19	Application...	1000	(100)
信息	2018/9/1 10:57:20	Windows E...	1001	无
错误	2018/9/1 10:57:20	Application...	1000	(100)
信息	2018/9/1 10:57:20	Windows E...	1001	无
错误	2018/9/1 10:57:20	Application...	1000	(100)

查看“错误”信息，发现*均是*由 LogonUI.exe 文件中的错误模块 Windows.UI.XamlHost.dll 引起。其异常代码为0xc0000409，为系统文件被异常破坏或删除的异常代码。回忆起当天上午的操作，我为了更换系统登陆时的背景，替



换掉了 Windows.UI.Logon.pri 文件，然而没有注意到跨 Windows 版本的问题（当天系统刚经过一次更新），新的文件在启动时没有通过验证，导致再次登陆系统时，登录界面无法显示，当时没有意识到，便反复重启，这一过程也记录下来了。

查看紧接着的“信息”，为“故障存储段异常”，里面的内容，尤其是“问题签名”部分，一定程度上证明了我上面的判断和异常解读。（P2和 P5为文件版本）



2. setup 部分的一个异常分析

来源：WUSA

分析：错误码为2149842967，经查询为补丁安装出现错误的代码。观察提示内容发现可能是一个 Windows8相关补丁 KB2999226安装失败，我的系统是 Win10，此错误基本上可以忽略。

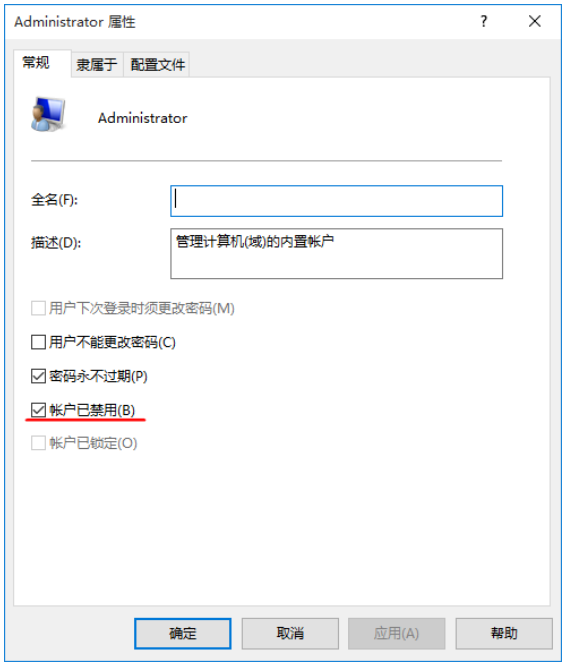
4.2.2 本地安全策略配置

一、密码最短/最长使用期限无效？

很可能在创建用户时勾选了“用户不能更改密码”。

另外，如果勾选了“密码永不过期”，则密码最长使用期限会无效。

二、为什么会把 Administrator 账户禁用？



在学校的机子上做实验时，发现 Administrator 账户是禁用的，这可能是因为**系统默认的 Administrator 权限过大**，用户登录后可能会做出一些危害系统安全的操作。但是，系统必须要有一个可以修改密码权限的用户账户，为了确保正常使用，系统管理员会再创建一个账号，给它赋予足够的权限，而把原来的账户禁用掉。另外一个原因是默认管理员目标很大，容易被攻击，一旦被拿下，对于整个操作系统安全危害很大，而且系统管理员的口令问题经常被忽视，禁用掉这个账户，可以把 Administrator 账户从登陆界面隐藏掉，防止用户利用。

也可能是**官方安全策略**的原因：Win10系统**默认都是以微软账户或者是本地账户进入系统的**，如果想要使用管理员账户，就要登录 Administrator 的账号了，但一般情况下都是用不到的。

在 Win10专业版中，可以通过进入“本地用户与组”，在 Administrator 账户页面中勾选“账户已禁用”来取消默认管理员账户；家庭版中，可以进入命令行，输入 net user administrator /active:no 来禁用管理员账户。

有点危险的是，这个 Administrator 账户默认状态下没有密码！（可能是安

装系统过程中没有设置）

三、我为什么这样配置自己的安全策略？

在前面设置安全策略时，我主要进行了密码策略的设置。我认为最重要的是启用密码复杂性，因为它决定了用户密码的质量，强制性让用户设立较复杂的密码，从密码的制定下手。其次是禁用了“可还原的加密”，此项功能对于个人用户毫无必要，是一项可能的安全隐患。剩下的设置项主要针对用户使用密码的习惯，设置了密码最长可用一个月，是综合考虑了安全性和用户方便性需求的结果，一个密码“打天下”，一旦泄露，很容易全盘皆崩。

之所以没有在锁定策略进行设置，是因为考虑到这是对个人电脑的安全配置，使用者只会有自己一个人，不涉及到多个用户账户的问题，且若设定了锁定，还要进入安全模式或管理员账户进行解锁，十分麻烦。如果是在域中，就需要在这里设置一些东西了。