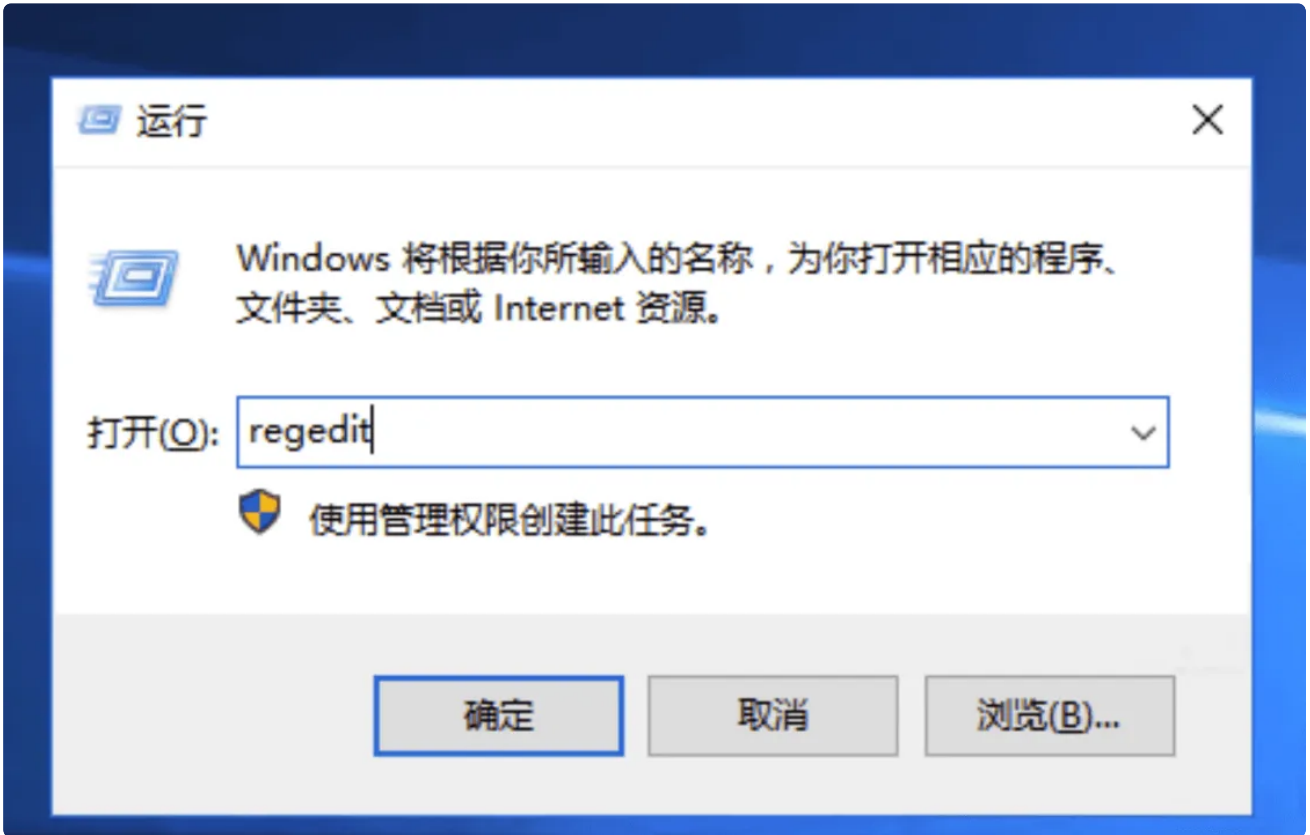


Part2

注册表

注册表保存到XXX目录

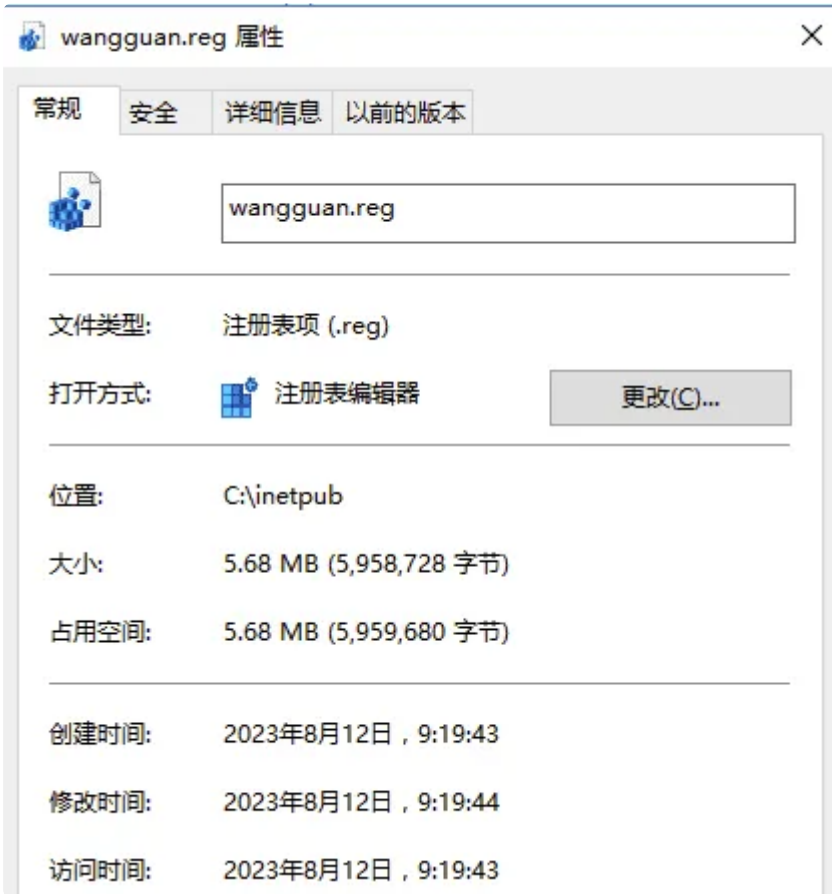
Win键+R: 调起运行窗口, 输入regedit



右键导出所需要的键



截图示例：

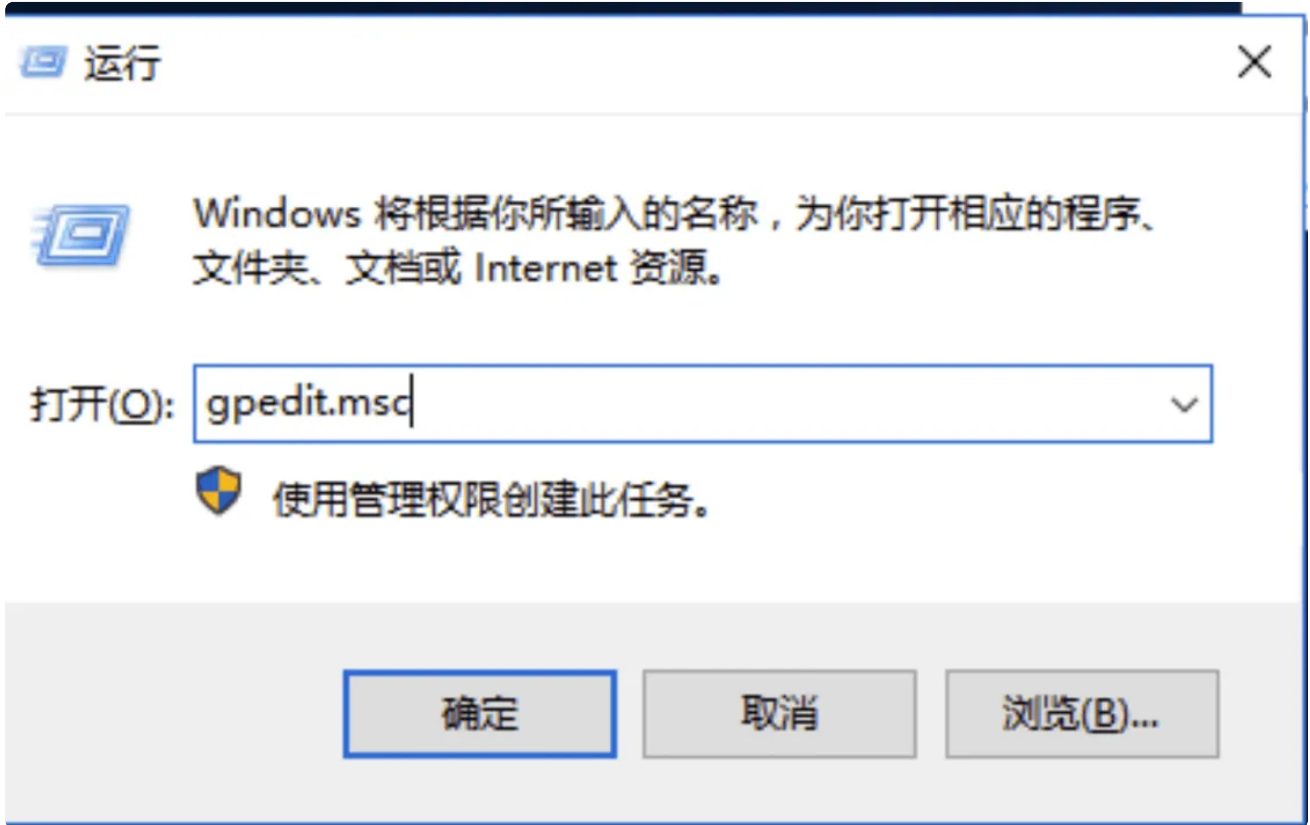


本地策略

密码策略

Windows菜单——Windows管理工具——本地安全策略
或者

Win键+R: 调起运行窗口, 输入gpedit.msc



计算机配置——Windows配置——安全设置——账户安全——密码策略

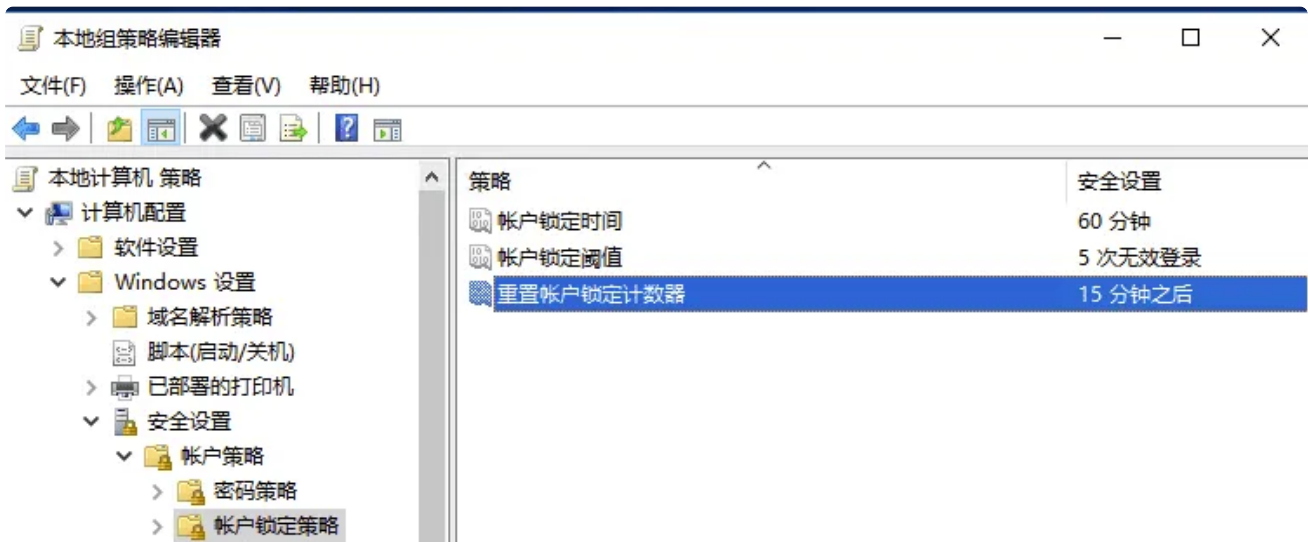


截图示例:

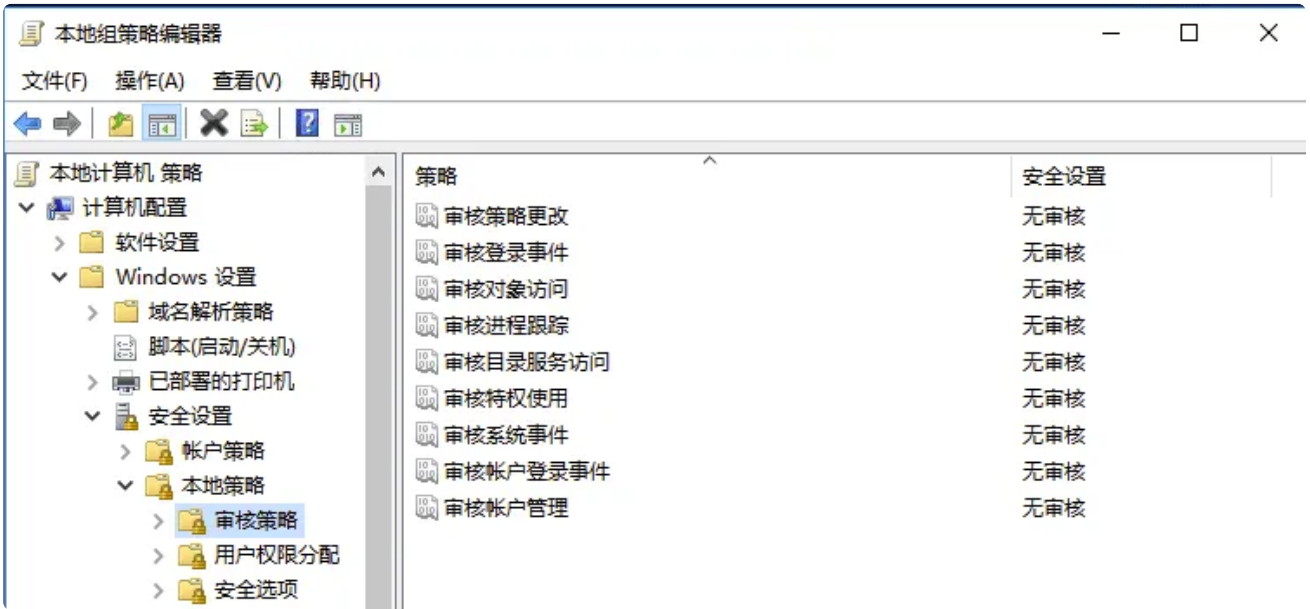
密码必须符合复杂性要求 属性



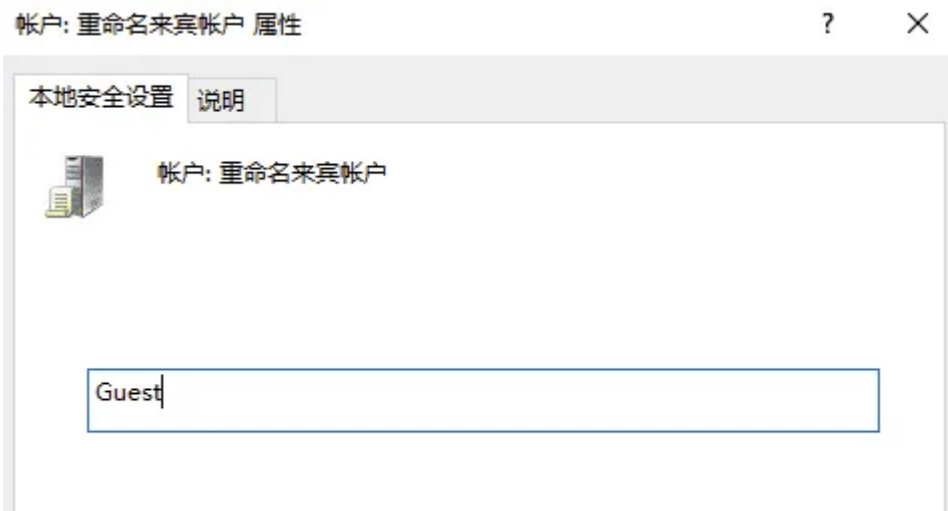
账户锁定策略



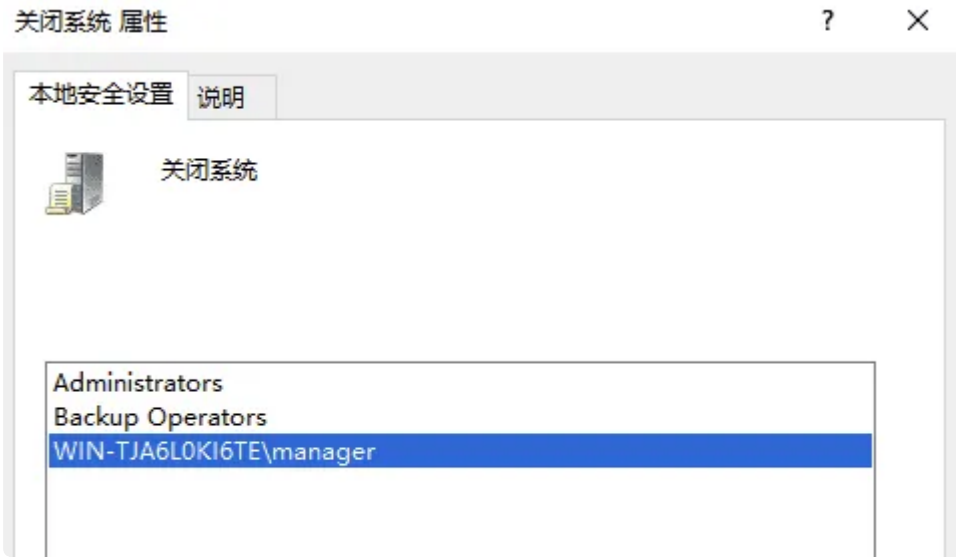
审核策略



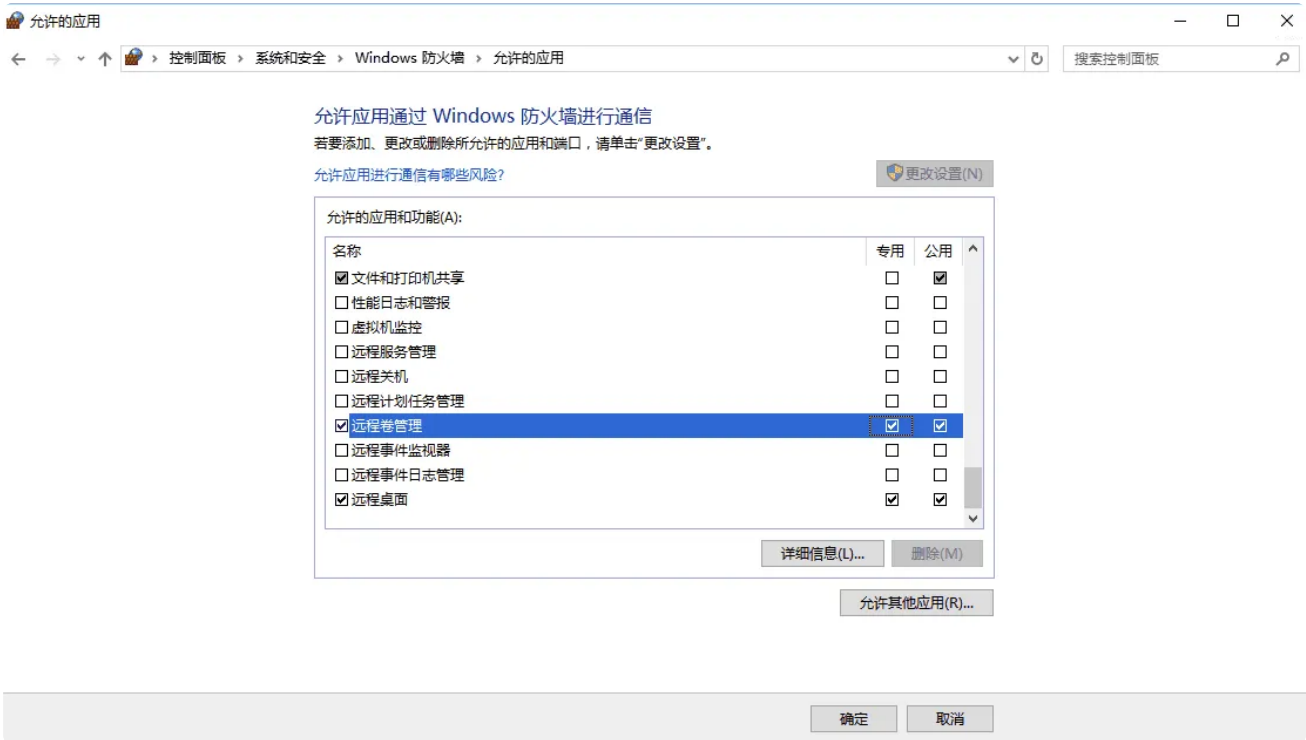
安全选项



用户权限分配



防火墙策略



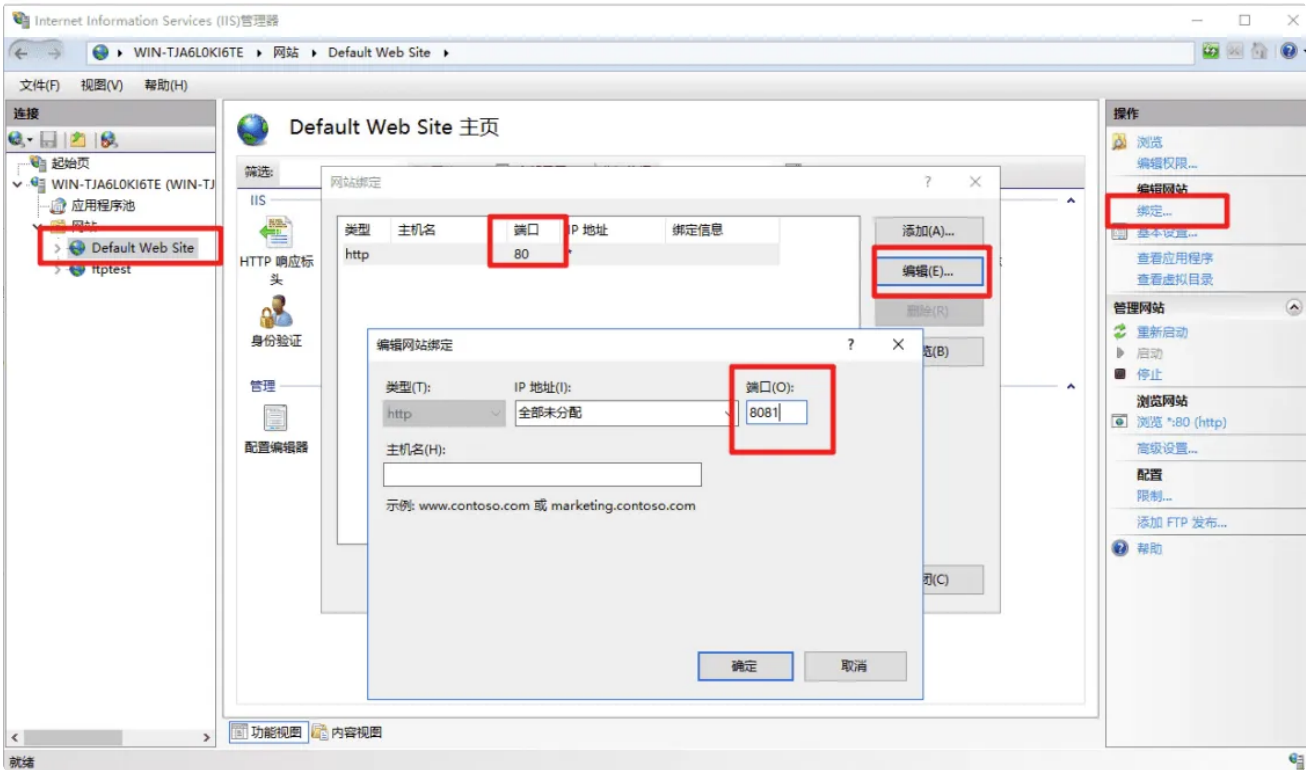
IIS

Windows管理工具——IIS管理器

服务器管理器



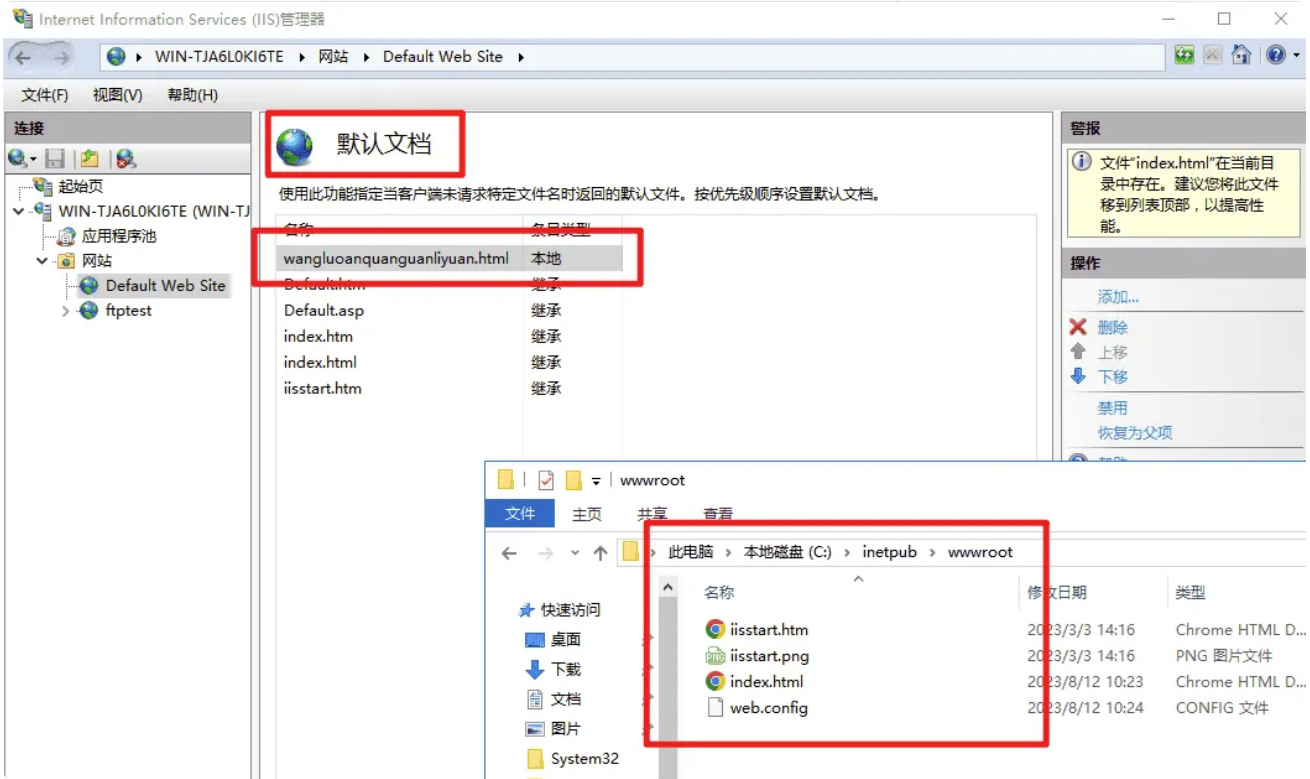
端口配置



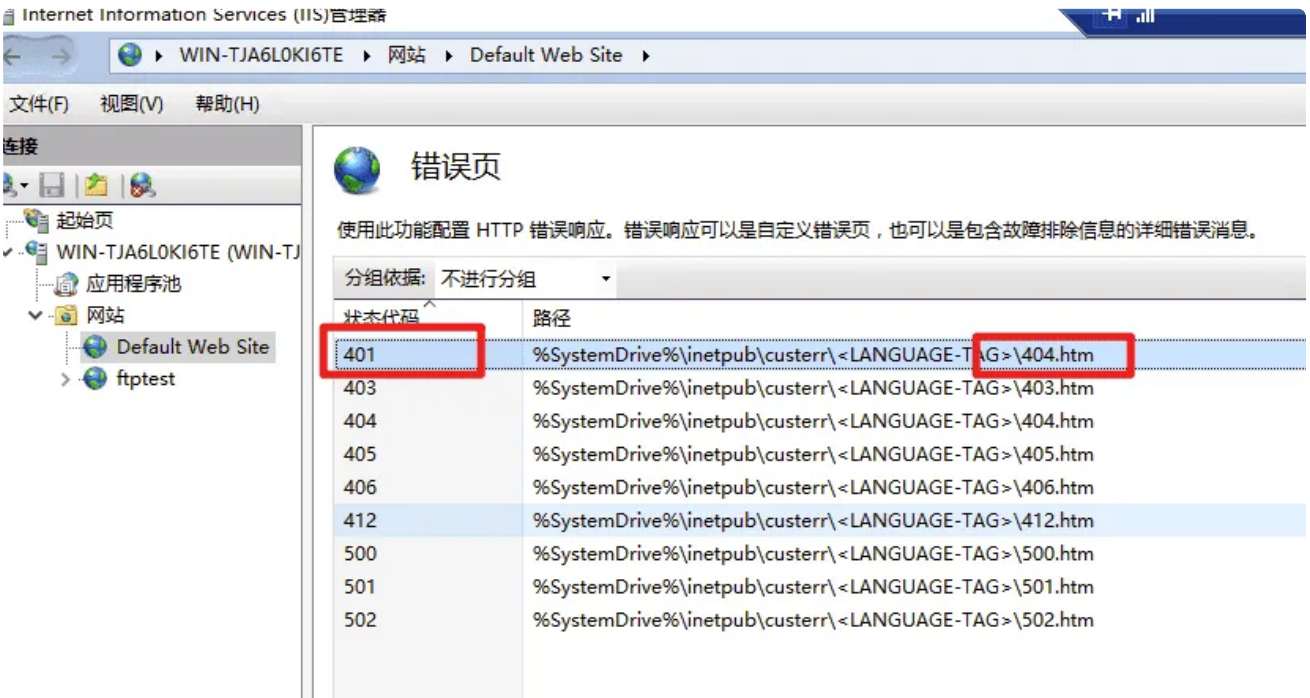
目录浏览



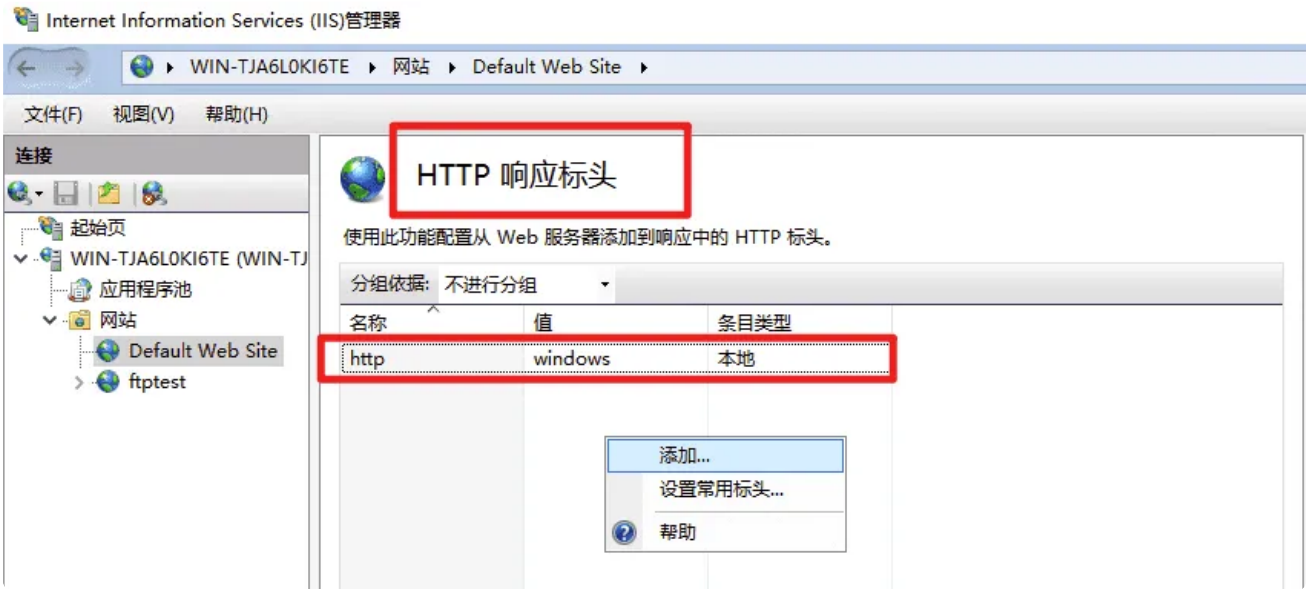
默认页面



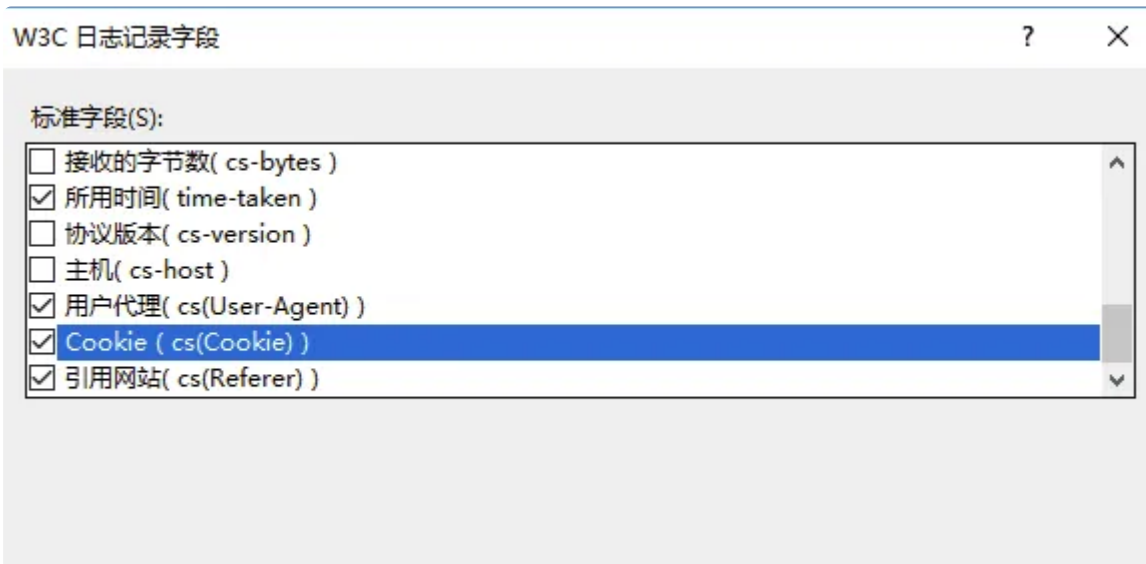
错误页面

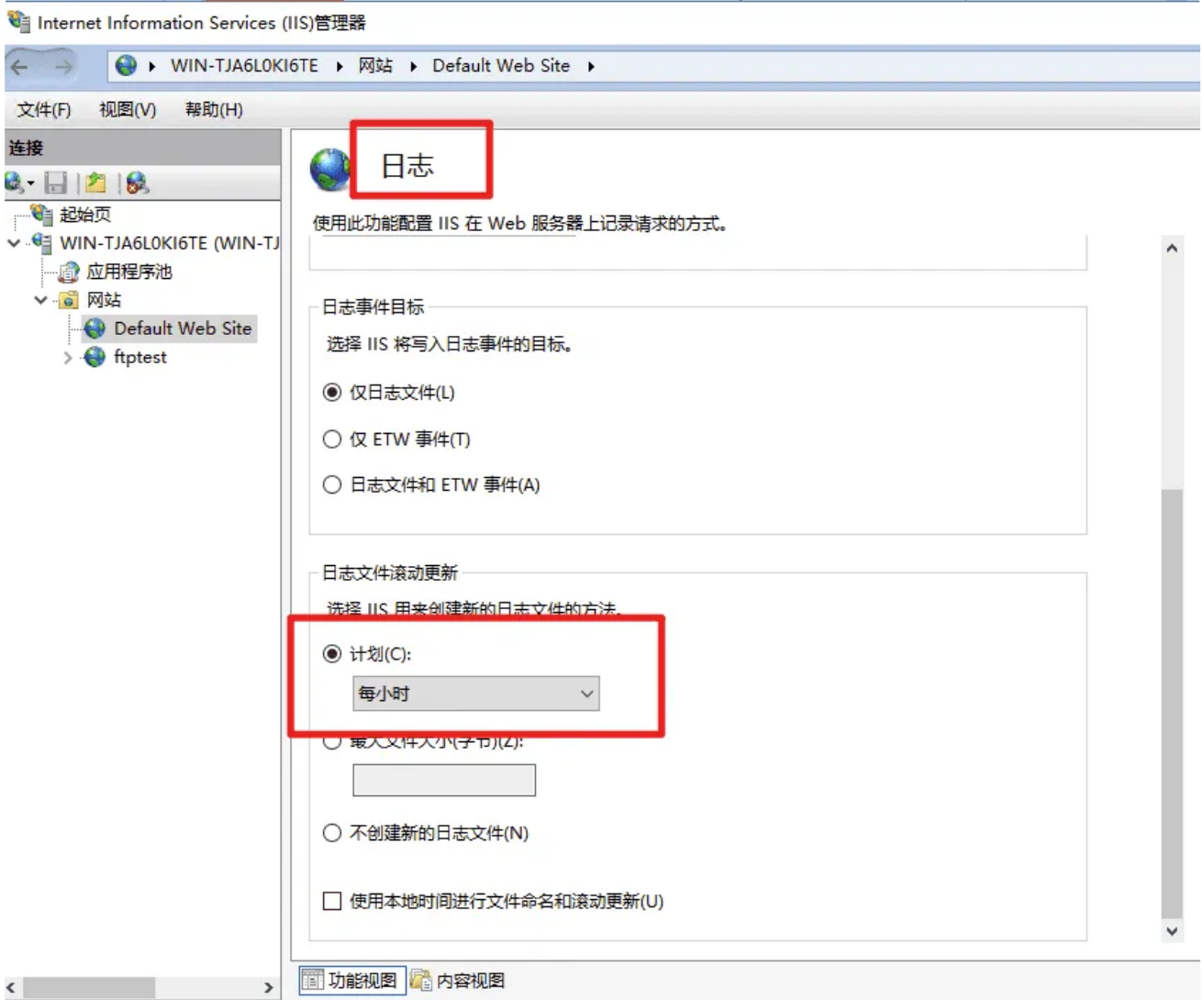


响应标头



日志滚动

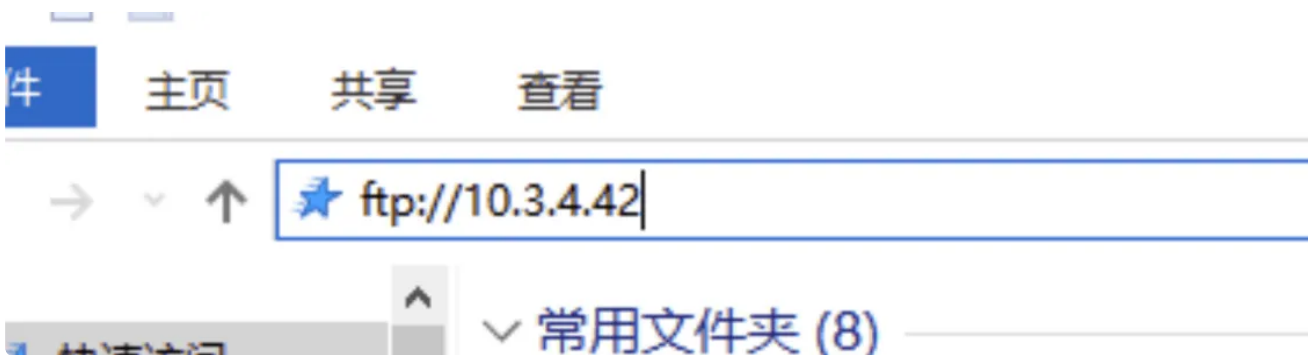





FTP

查看自己IP地址的方法:

Win键+R: 调起运行窗口, 输入cmd, 然后在cmd当中输入ipconfig, 查看10.3.4.xx的地址



身份验证

 **FTP 身份验证**

分组依据: 不进行分组

模式	状态	类型
基本身份验证	已启用	内置
匿名身份验证	已禁用	内置

请求筛选

 **FTP 请求筛选**

使用此功能可配置 FTP 服务的筛选规则。

文件扩展名 | 隐藏段 | 拒绝的 URL 序列 | 命令

文件扩展名	允许
.bak	False
.txt	True

授权规则

Information Services (IIS)管理器

WIN-TJA6L0KI6TE > 网站 > ftpctest >

视图(V) 帮助(H)

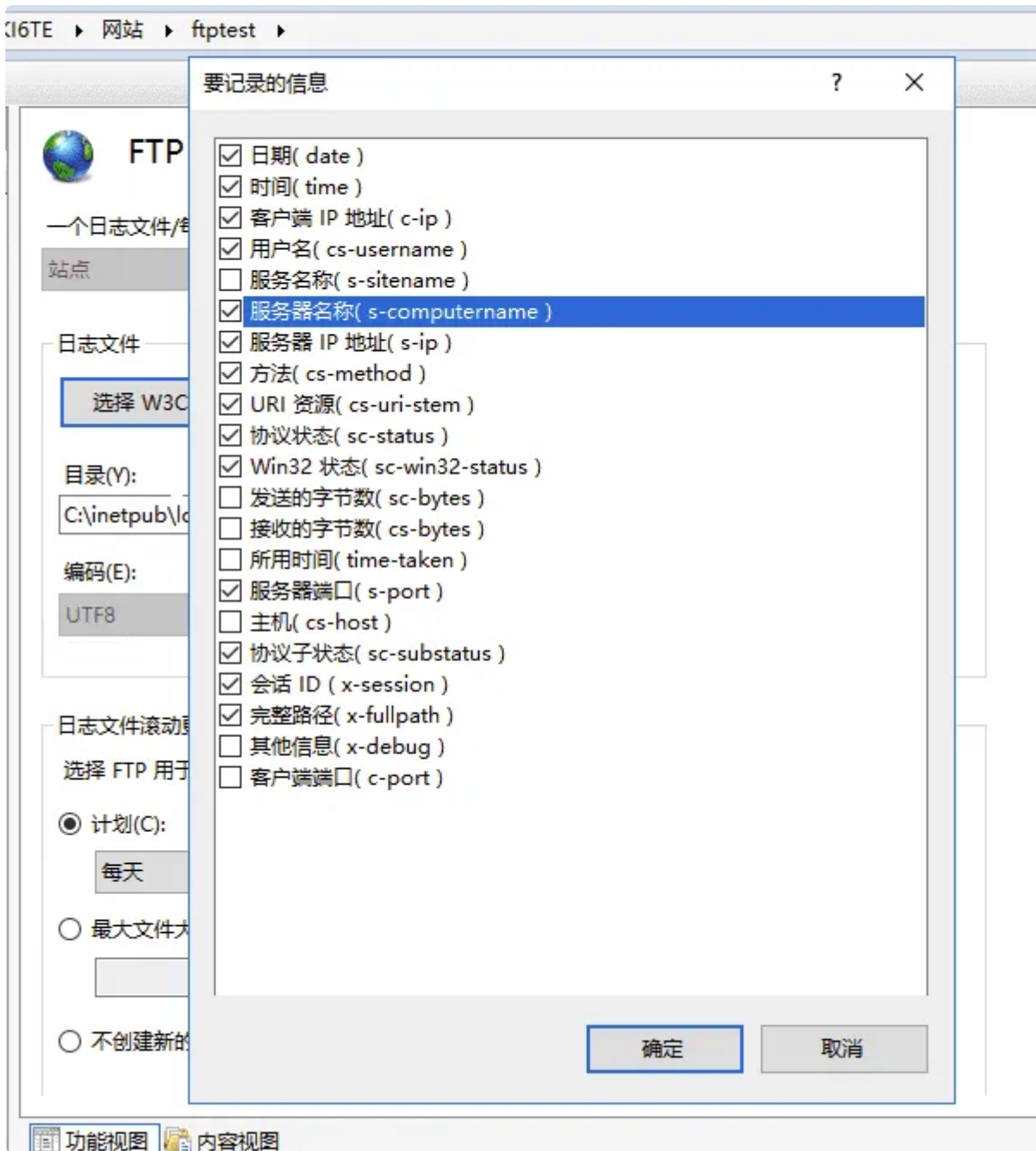
 **FTP 授权规则**

模式	用户	角色	权限
允许	所有用户		读、写
允许	manager		读取

地址限制



日志记录



SMTP



检测

首先需要开启SMTP服务器(可能会有卡死的情况, 等卡死重新开启一次即可)

然后cmd输入telnet 10.3.4.x 25

```
管理员: C:\Windows\system32\cmd.exe
```

```
Microsoft Windows [版本 10.0.14393]
(c) 2016 Microsoft Corporation。保留所有权利。

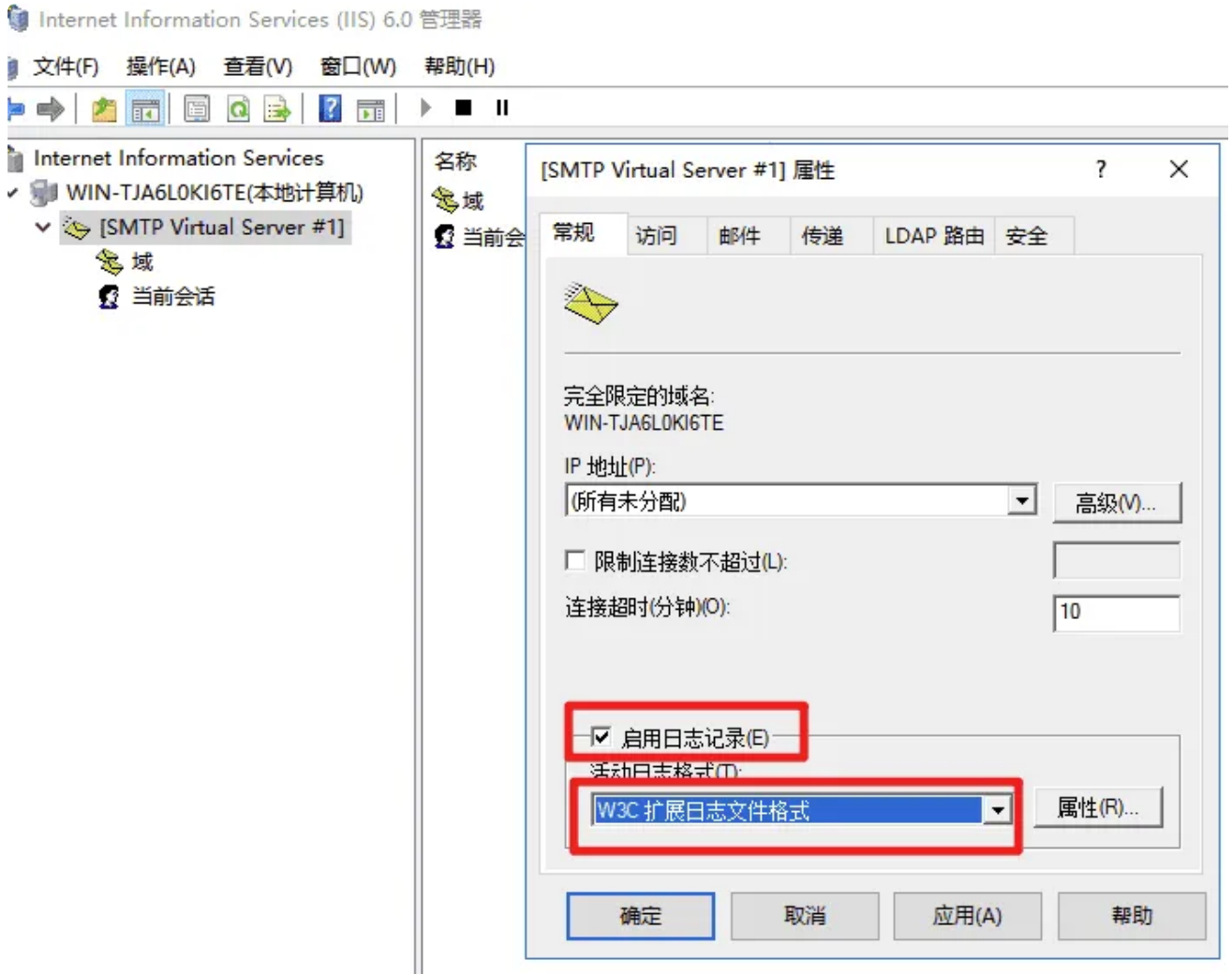
C:\Users\Administrator>telnet 10.3.4.42 25_
```

输入EHLO来检测当前SMTP服务器是否正常, 输入ehlo server也有类似效果。

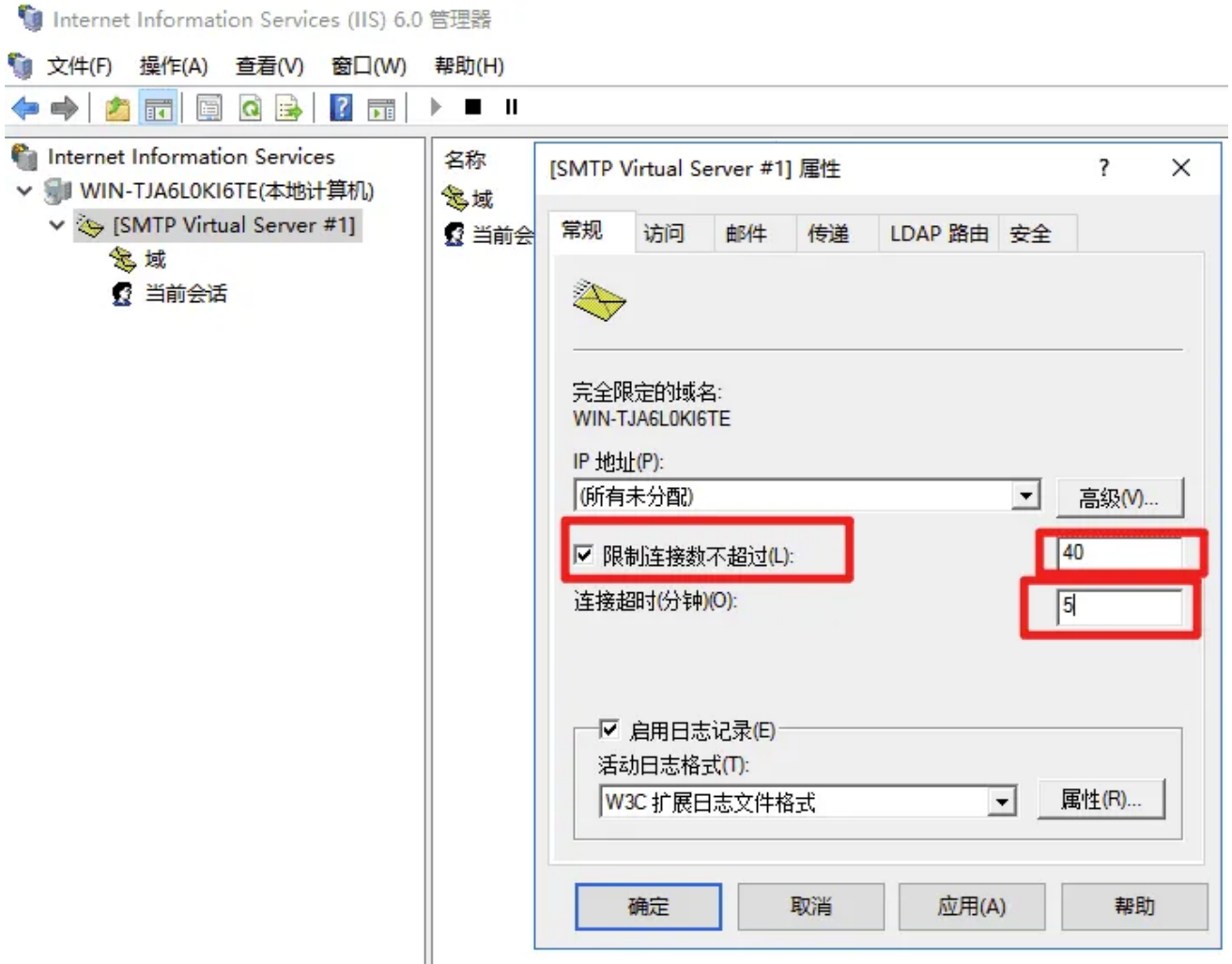
```
220 WIN-TJA6LOKI6TE Microsoft ESMTMP MAIL Service, Version: 10.0.14393.0 ready at Sat, 12
EHLO
250-WIN-TJA6LOKI6TE Hello [10.3.4.42]
250-TURN
250-SIZE 2097152
250-ETRN
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES
250-8bitmime
250-BINARYMIME
250-CHUNKING
250-VRFPY
250 OK
```

日志记录

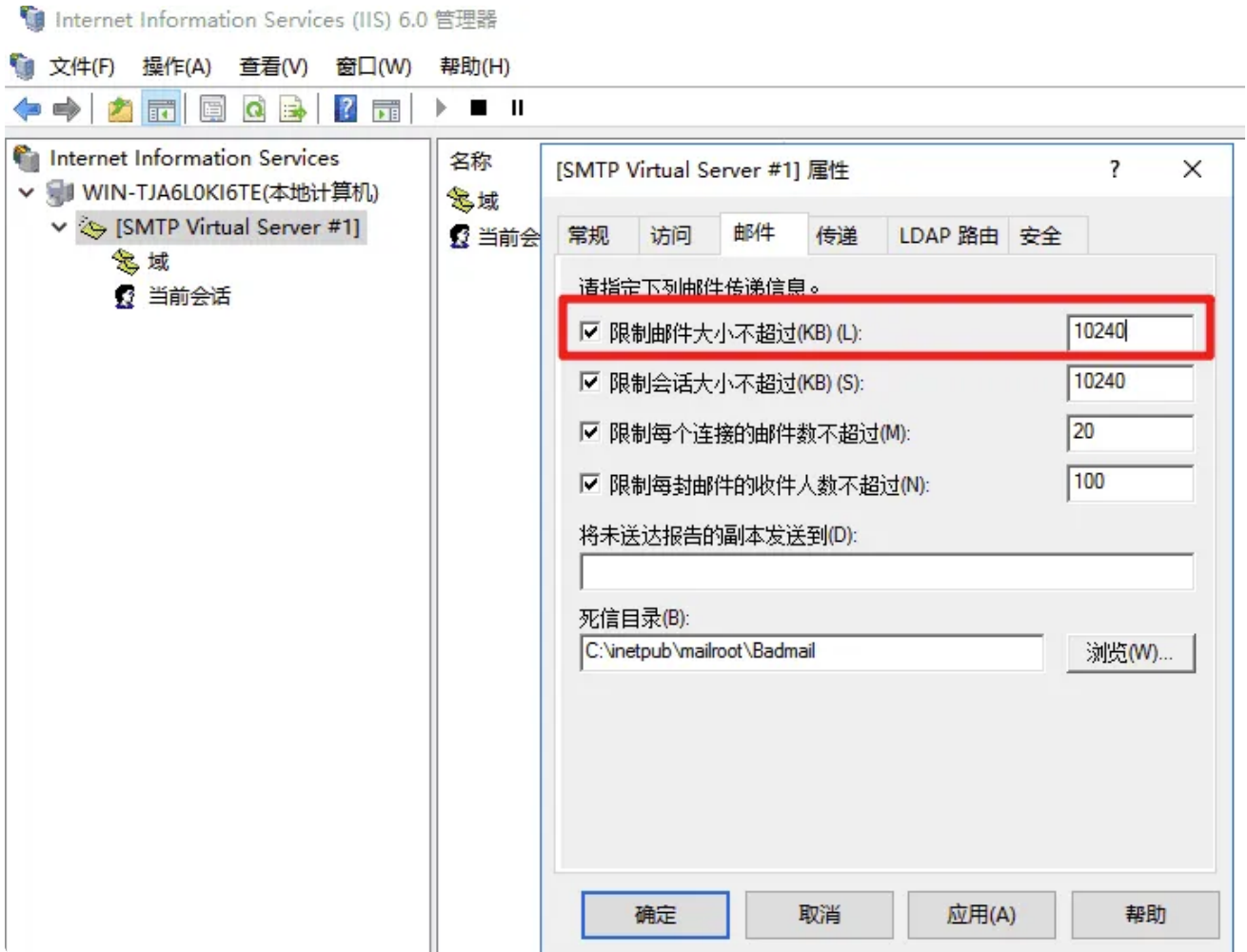
右键SMTP服务器的属性, 进行日志记录的配置



限制连接数



限制邮件大小

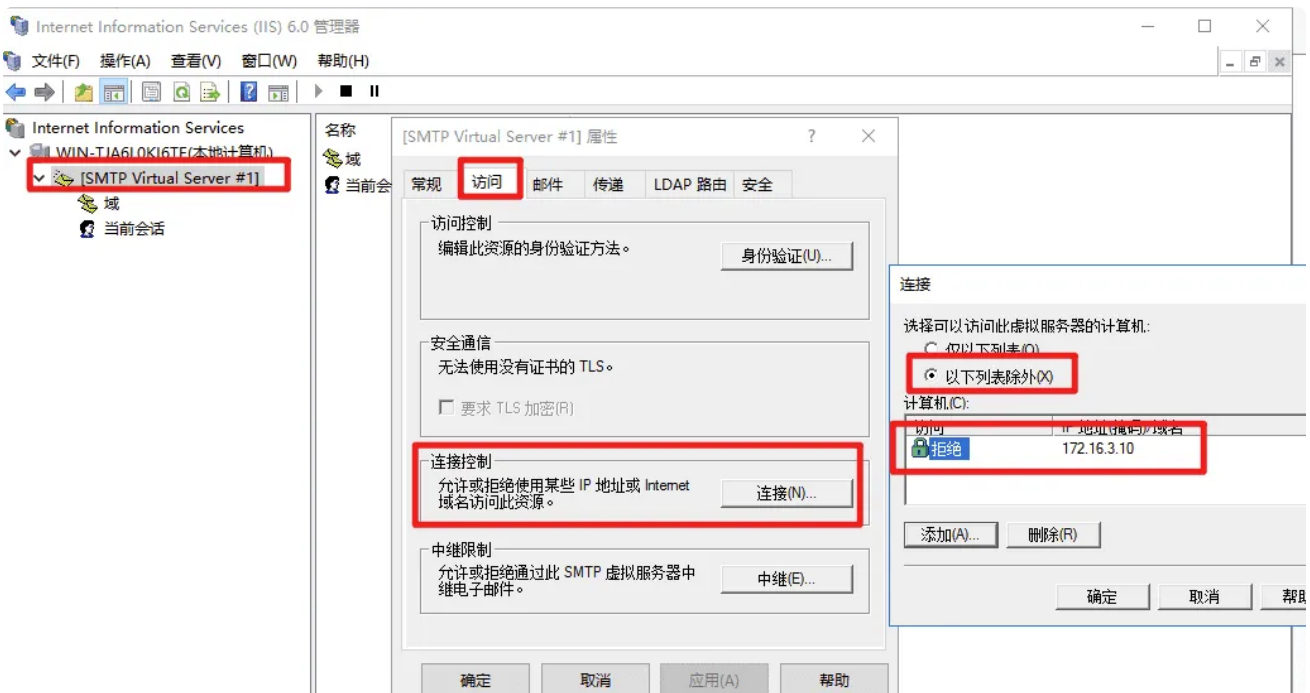


别名域

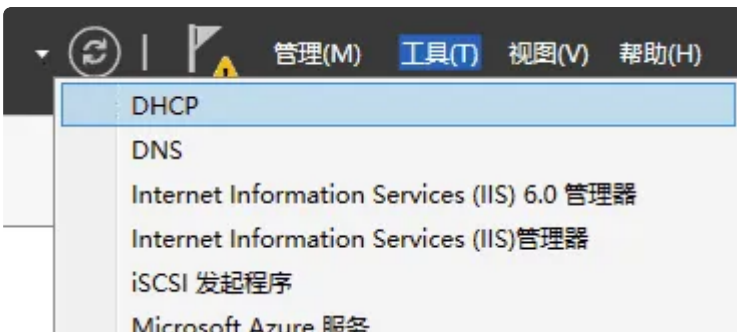




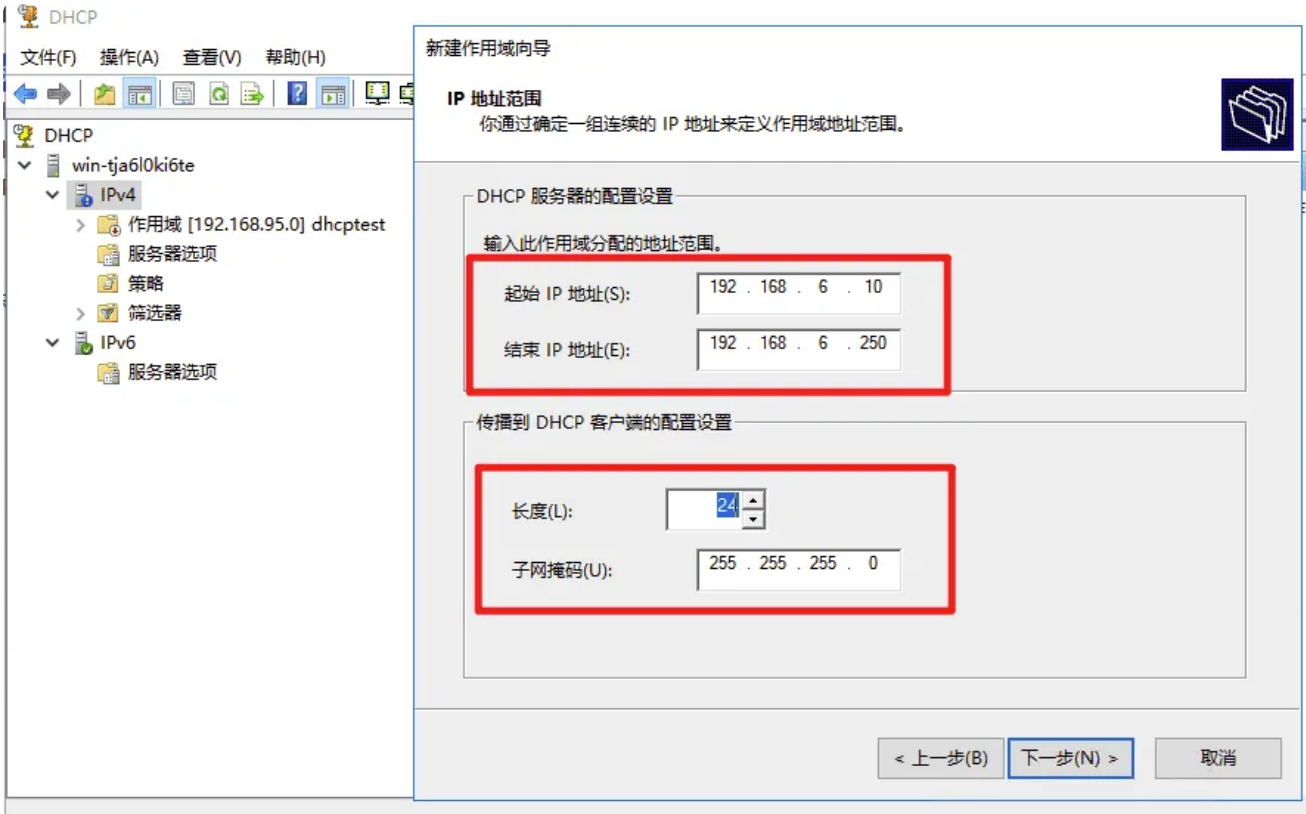
排除地址



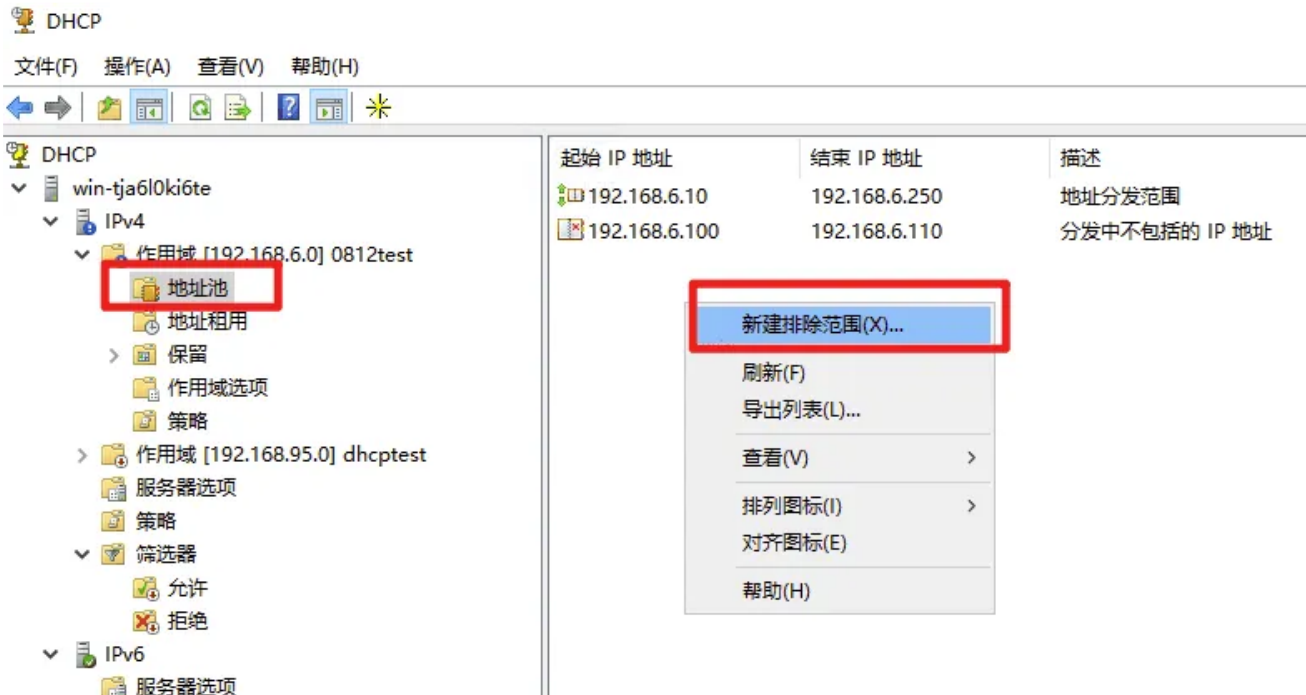
DHCP

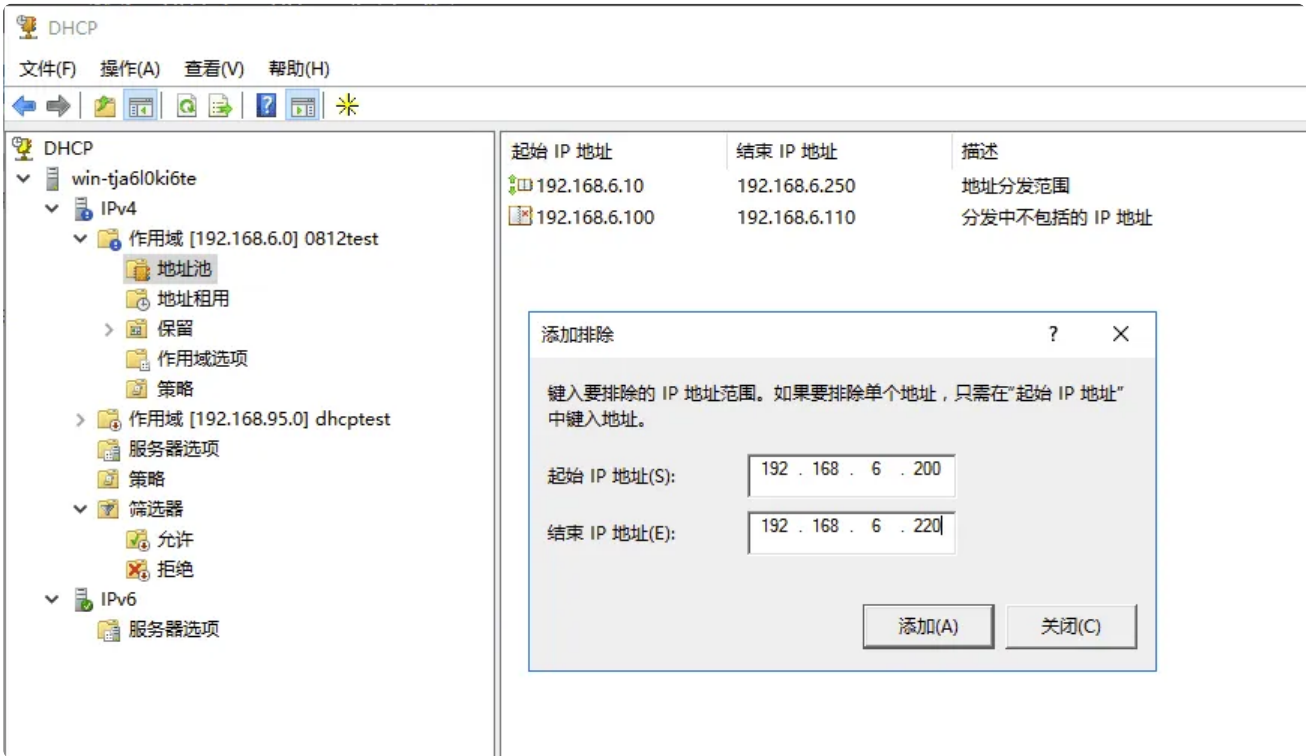


作用域

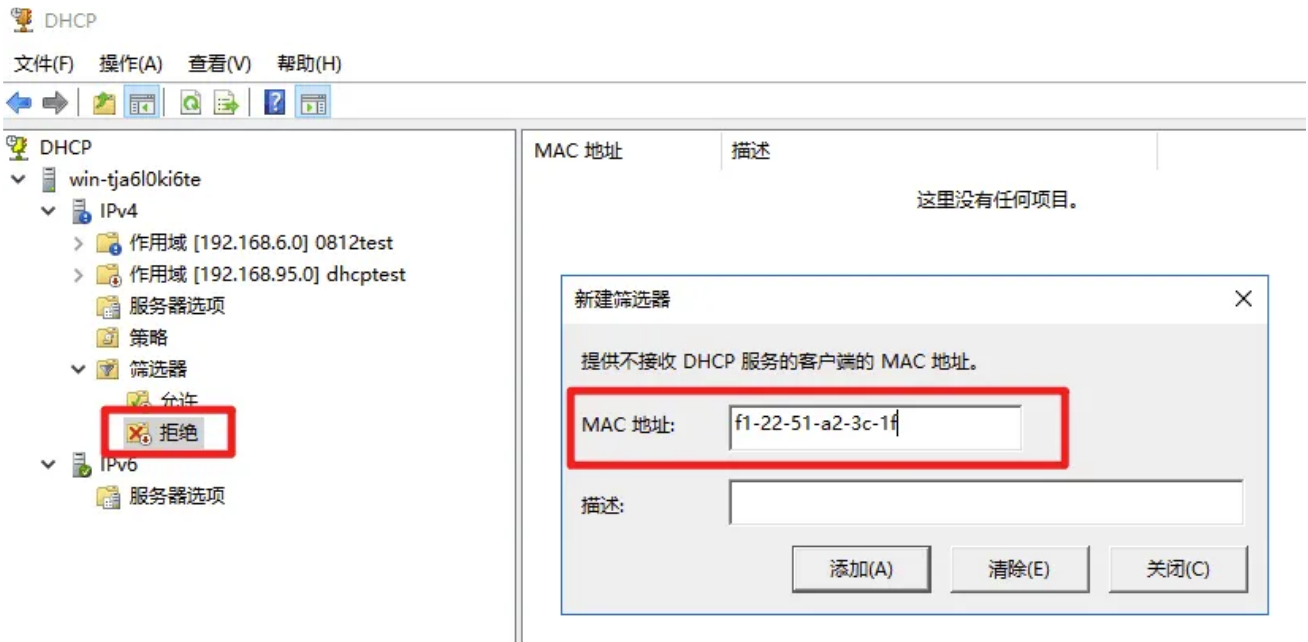


地址排除

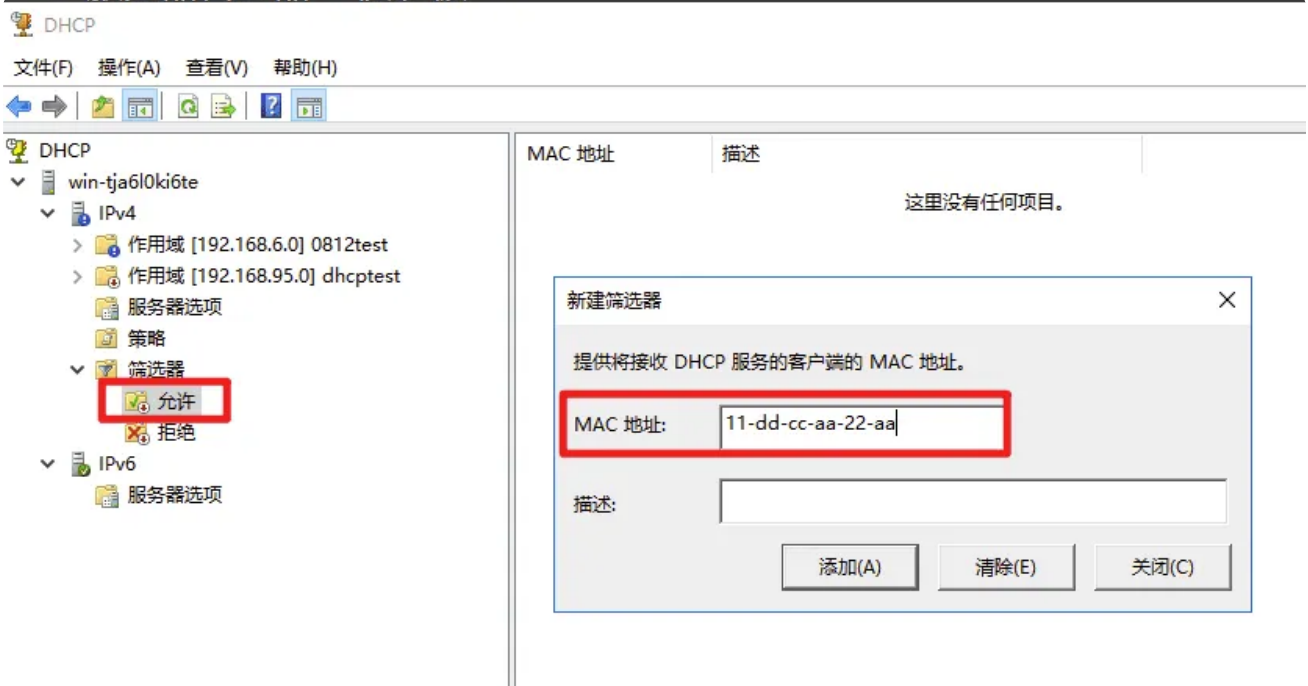




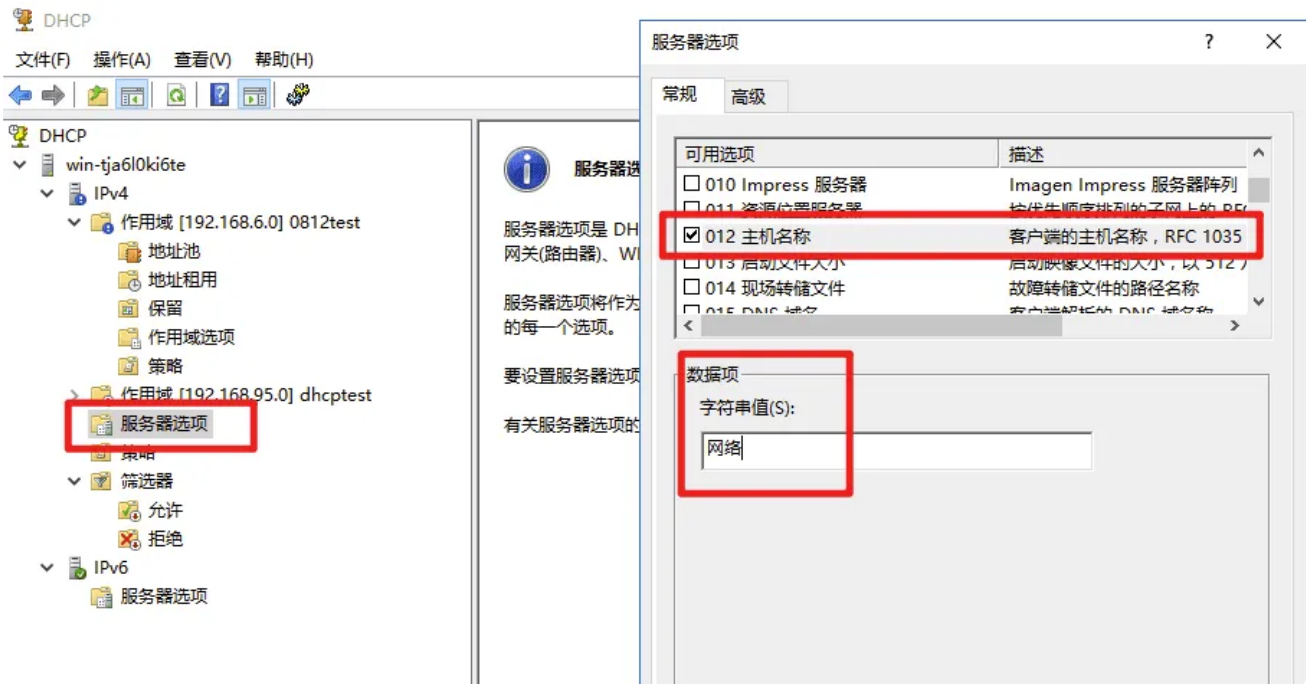
拒绝MAC地址



允许MAC地址



主机名称



保留地址

DHCP

文件(F) 操作(A) 查看(V) 帮助(H)

DHCP

- win-tja6l0ki6te
 - IPv4
 - 作用域 [192.168.6.0] 0812test
 - 地址池
 - 地址租约
 - 保留**
 - [192.168.6.123] 123321**
 - 作用域选项
 - 策略
 - 作用域 [192.168.95.0] dhcptest
 - 服务器选项
 - 策略
 - 筛选器
 - 允许
 - 拒绝
 - IPv6
 - 服务器选项

选项名	供应商	值
006 DNS 服务器	标准	223.
012 主机名称	标准	网络

新建保留

为保留客户端输入信息。

保留名称(R):

IP 地址(P):

MAC 地址(M):

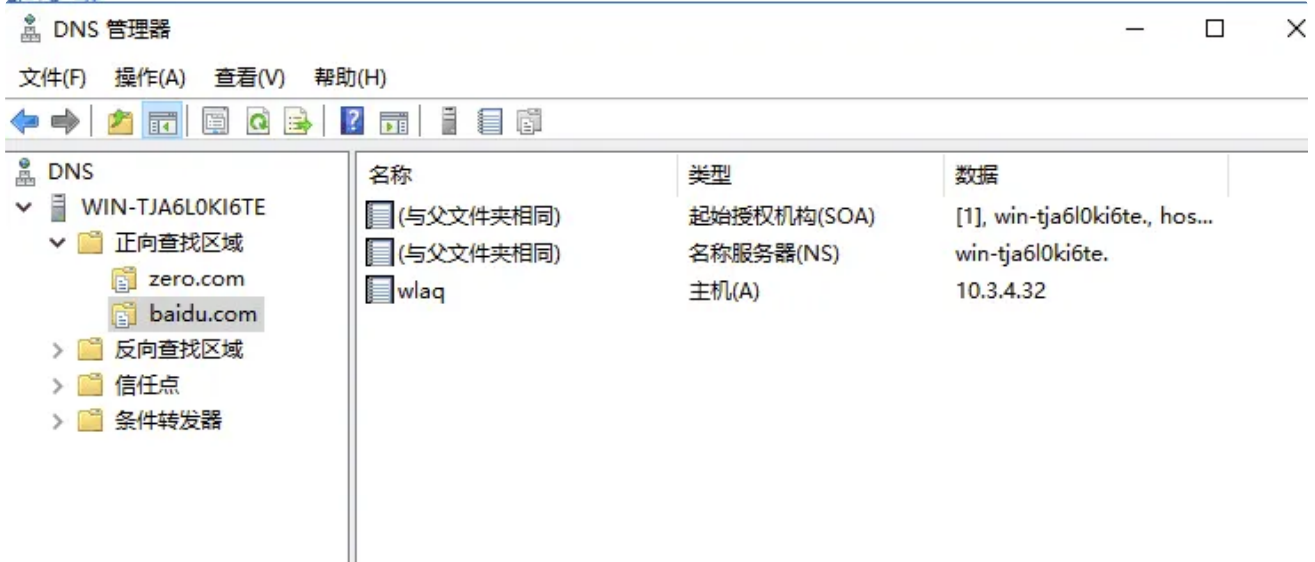
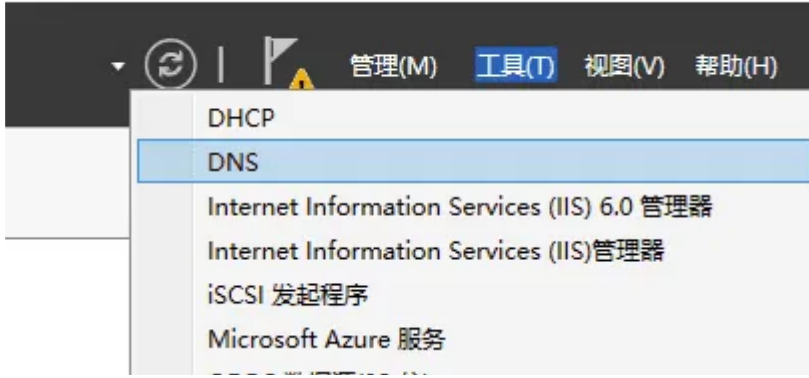
描述(E):

支持的类型

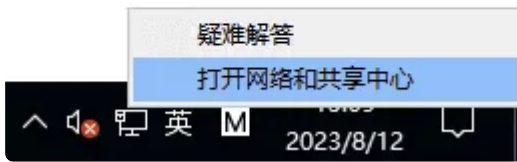
- 两者(B)
- DHCP(D)
- BOOTP(O)

DNS

正常区域、反向区域、主机、指针



“设置”以激活 Windows。



查看活动网络

网络 2
公用网络

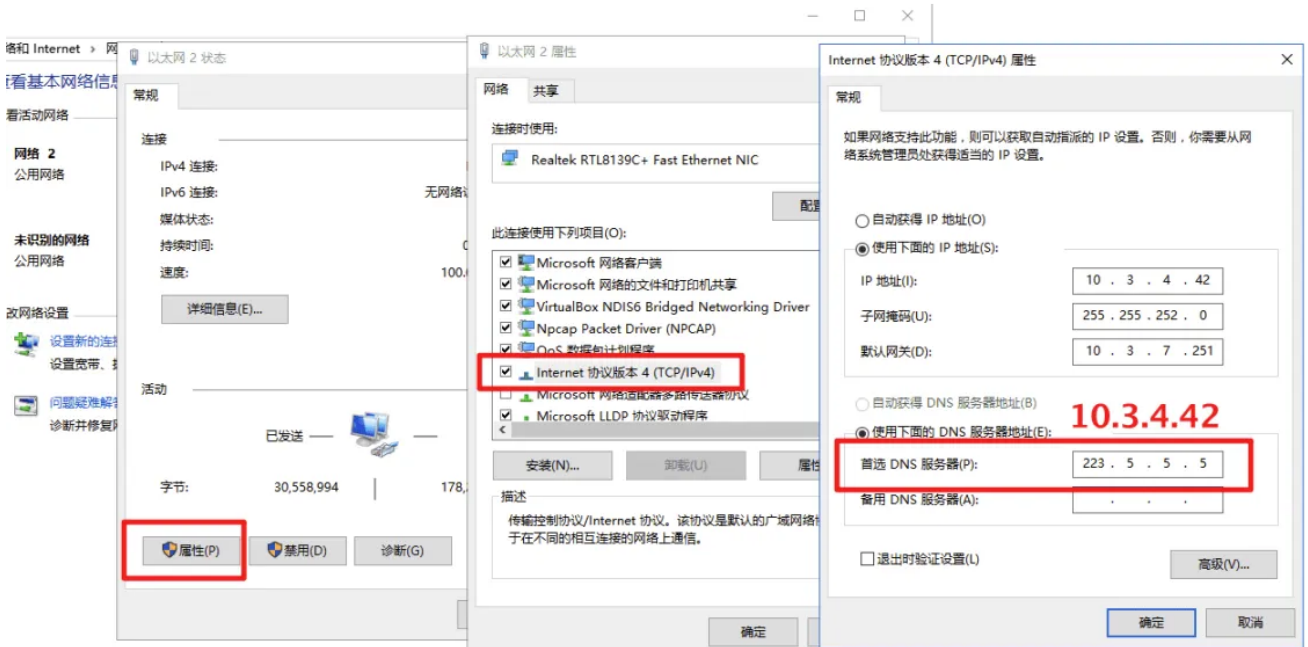
访问类型: Internet
连接: 以太网 2

未识别的网络
公用网络

访问类型: 无法连接到网络
连接: 以太网 3

更改网络设置

设置新的连接或网络
设置宽带、拨号或 VPN 连接；或设置路由器或接入点。



```
C:\Users\Administrator>nslookup wlaq.baidu.com
服务器: UnKnown
Address: 10.3.4.42

名称: wlaq.baidu.com
Address: 10.3.4.42
```

刷新dns

```
C:\Users\Administrator>ipconfig /flushdns
Windows IP 配置
已成功刷新 DNS 解析缓存。
C:\Users\Administrator>
```



hello world

反向区域

要标识反向查找区域，请键入网络 ID 或区域名称。

网络 ID(E):

10 .3 .4 .

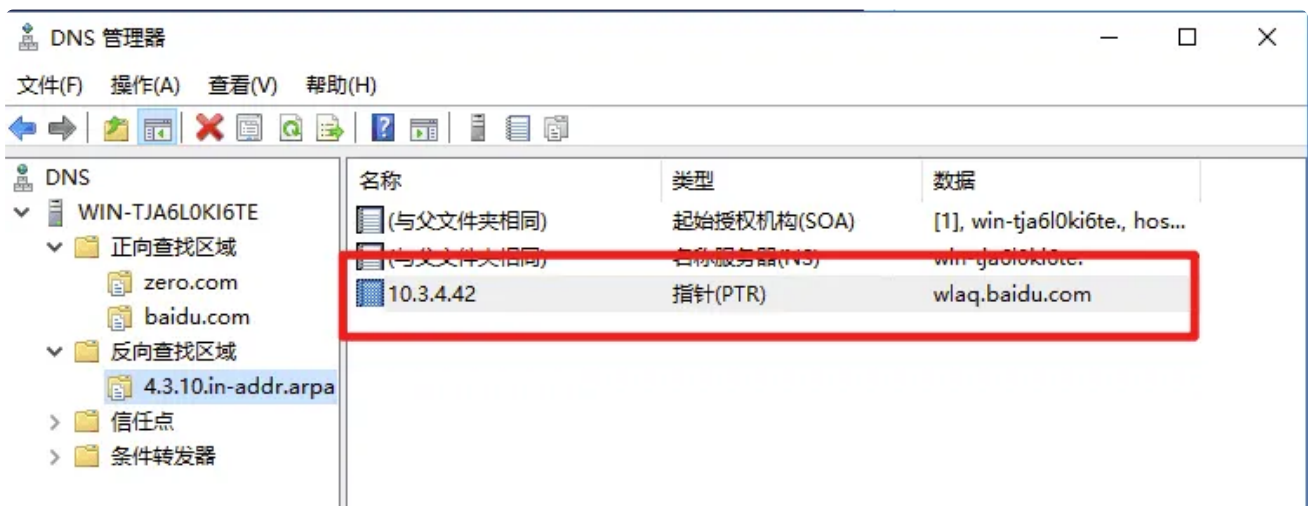
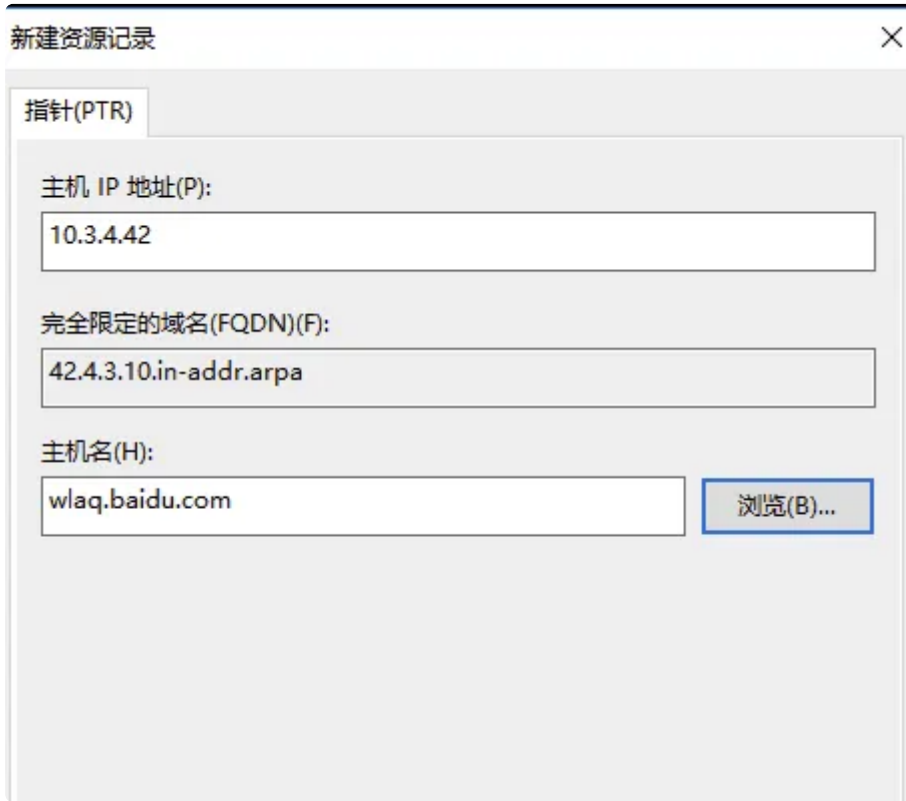
网络 ID 是属于该区域 IP 地址的部分。用正常(不是反向的)顺序输入网络

如果在网络 ID 中使用了一个零，它会出现在区域名称中。例如，网络 ID 10.in-addr.arpa 区域，网络 ID 10.0 会创建 0.10.in-addr.arpa 区域。

反向查找区域名称(V):

4.3.10.in-addr.arpa





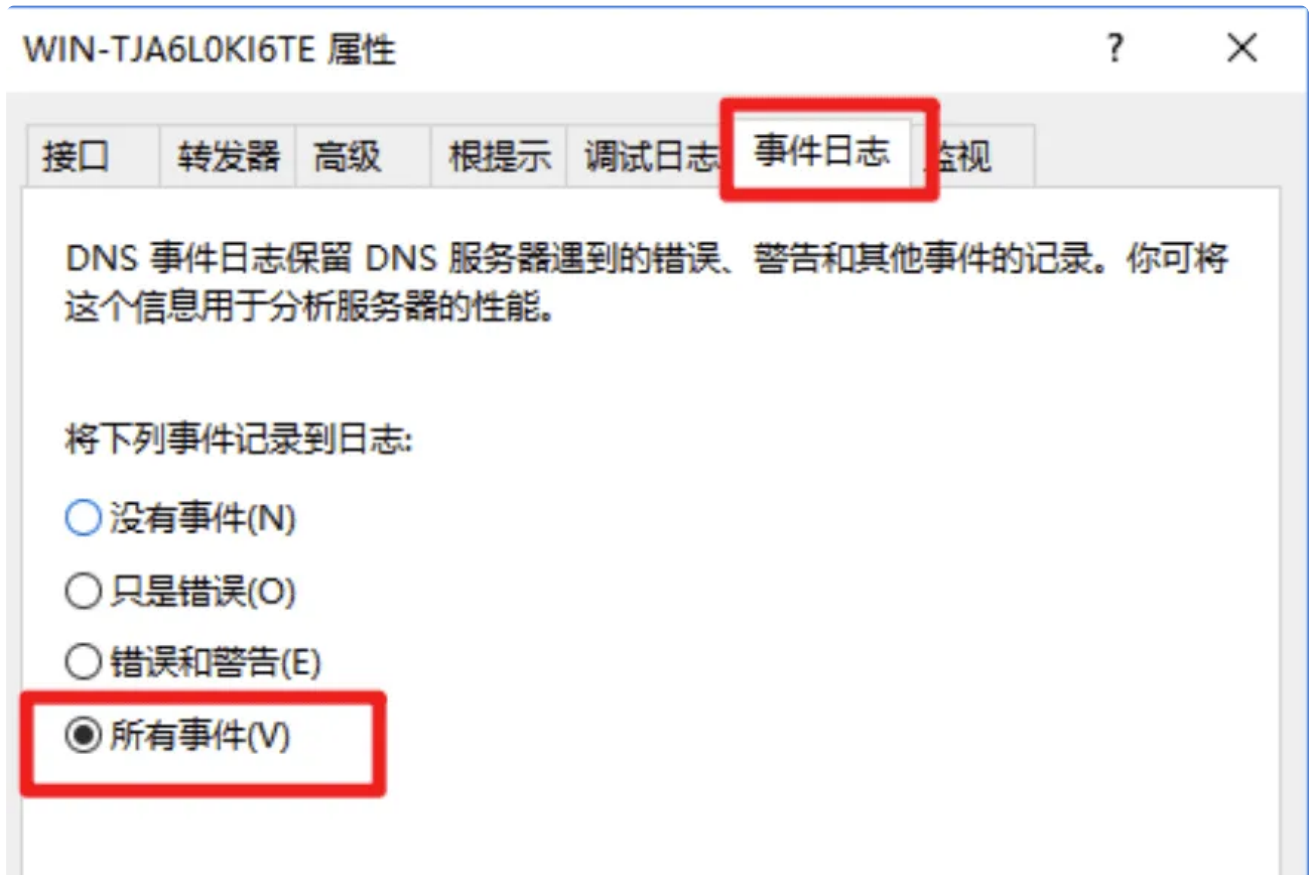
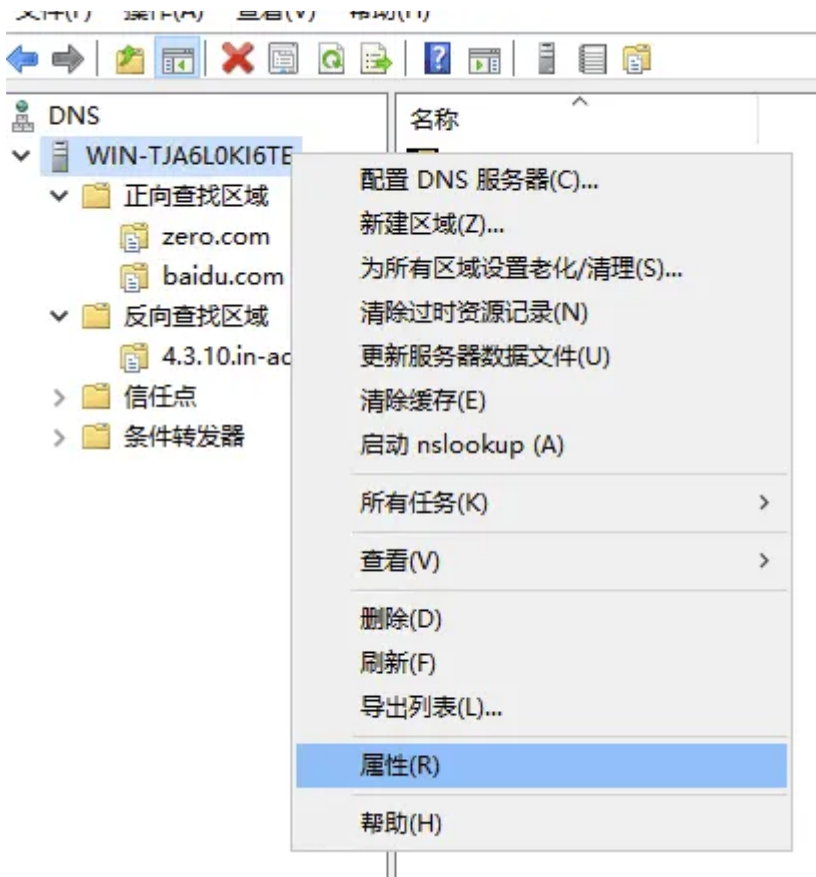
```
C:\Users\Administrator>nslookup 10.3.4.42
服务器: UnKnown
Address: 10.3.4.42

*** UnKnown 找不到 10.3.4.42: Non-existent domain
```

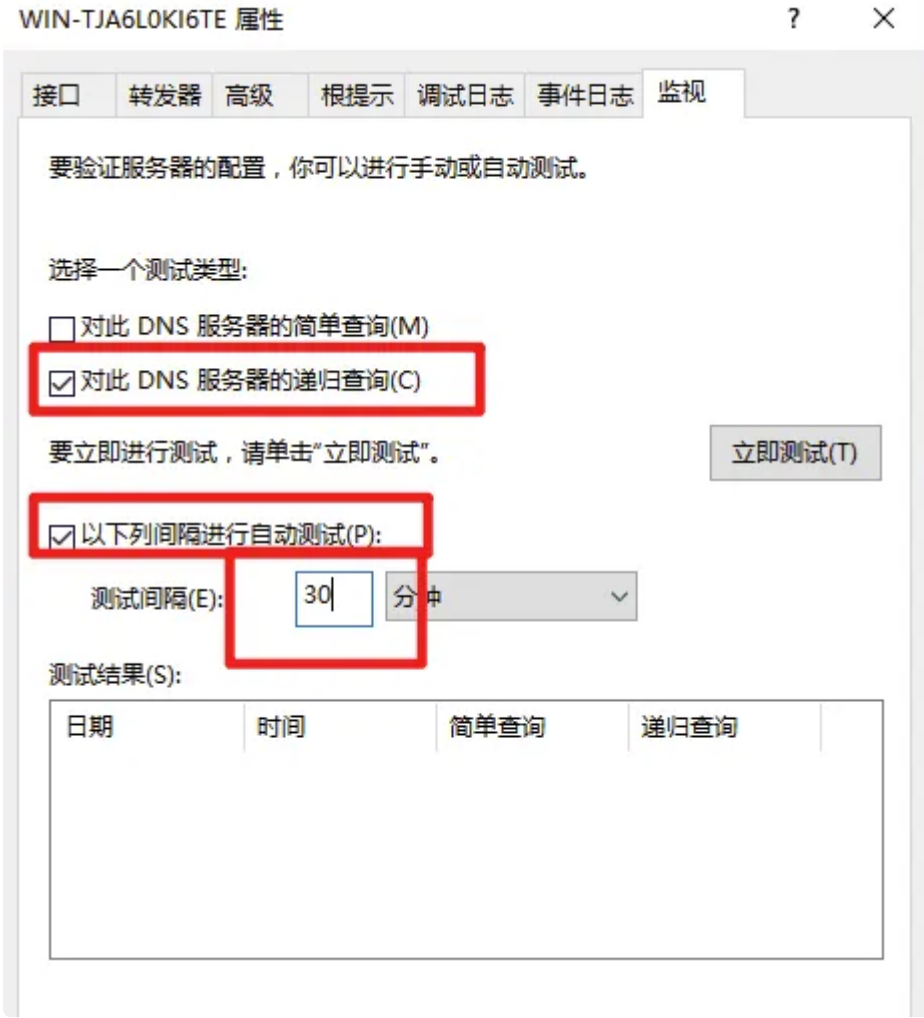
```
C:\Users\Administrator>nslookup 10.3.4.42
服务器: wlaq.baidu.com
Address: 10.3.4.42

名称: wlaq.baidu.com
Address: 10.3.4.42
```

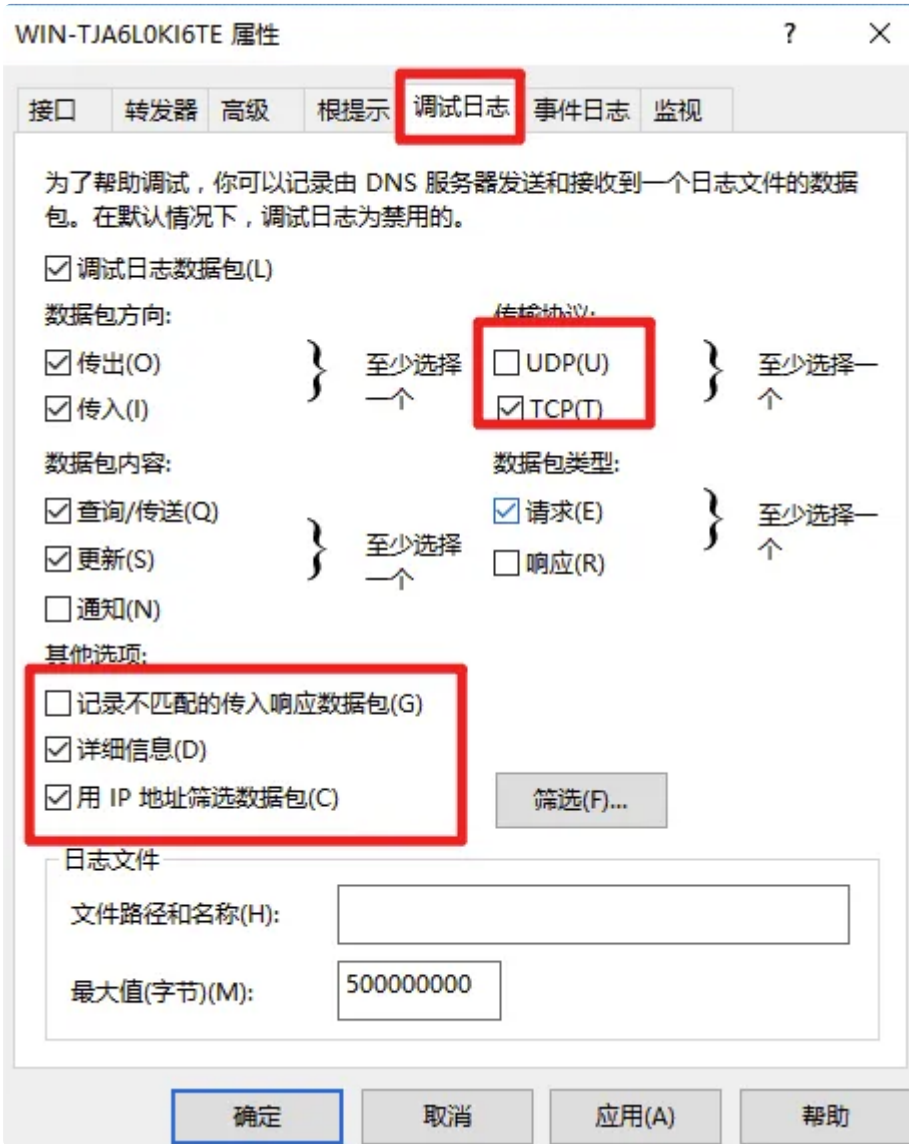
事件日志



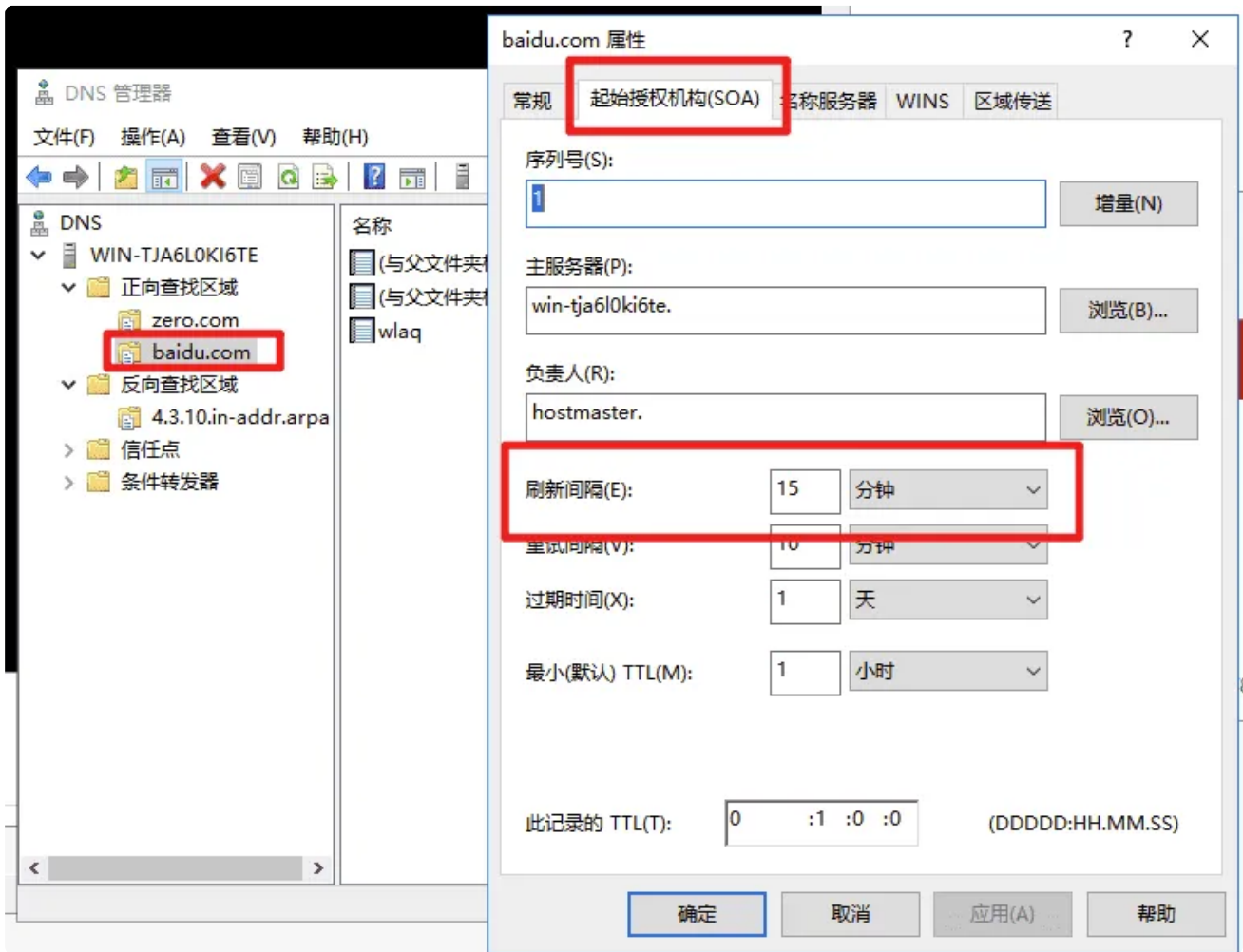
监视



调试日志



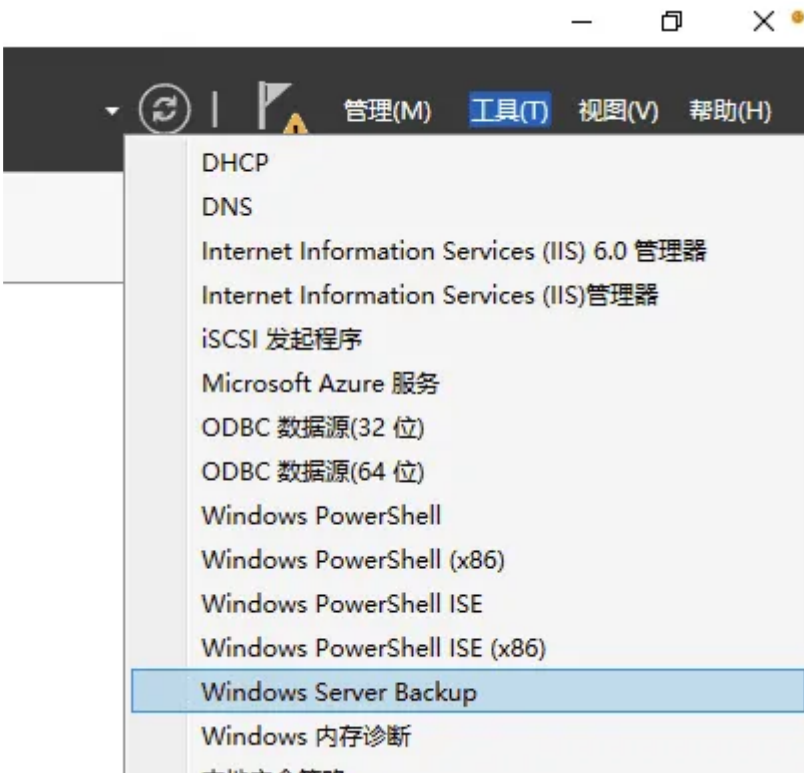
刷新间隔



自动清理



backup



备份、恢复

操作

- 本地备份
- 备份计划...
- 一次性备份...
- 恢复...
- 配置性能设置...
- 查看
- 帮助

以保护你的数据。

备份计划向导

指定备份时间

开始

- 选择备份配置
- 指定备份时间
- 指定目标类型
- 确认
- 摘要

你希望以什么频率及何时运行备份?

每日一次(O)

选择时间(E): 21:00

每日多次(M)

单击可用的时间, 然后单击“添加”将其添加到备份计划。

可用时间: 计划时间:

0:00
0:30
1:00
1:30
2:00
2:30
3:00
3:30
4:00
4:30

添加(A) >

< 删除(R)

21:00

< 上一步(P) 下一步(N) > 完成(F) 取消

一次性备份向导

备份进度

备份选项

- 选择备份配置
- 选择要备份的项
- 指定目标类型
- 选择备份目标
- 确认
- 备份进度

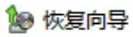
状态: 已完成。

状态详细信息

备份位置: F:

传输的数据: 1 KB

项目	状态	传输的数据
新加卷 (E:)	已完成。	1 KB/1 KB



恢复进度

开始

选择备份日期

选择恢复类型

选择要恢复的项目

指定恢复选项

确认

恢复进度

文件恢复进度:

状态: 已完成。

恢复详细信息(R):

项目	目标	状态	传输的数据
E:\Test.txt	C:\Users\Administrator\Desktop\	已完成。	1 KB/1 KB

若要关闭向导, 请单击“关闭”- 恢复操作将在后台继续运行。若要查看此操作的进度, 请从 Windows Server Backup 控制台打开正在进行的备份消息。

备份方式

本地备份

- 备份计划...
- 一次性备份...
- 恢复
- 配置性能设置...**
- 查看
- 帮助

优化备份性能

如果备份包含整卷, 则可以通过选择下列设置之一管理以后的性能。如果备份仅包含系统状态、文件或文件夹, 则不适用这些设置。

普通备份性能(N)
创建备份的时间与要备份的数据大小成正比。

快速备份性能(F)
通过只跟踪上次备份和当前备份之间的更改来提高备份速度。这可能会降低备份中包含的卷上的磁盘吞吐量。对于执行密集使用磁盘操作的服务器, 不建议使用此选项。

自定义(U)
如果你拥有某些密集使用磁盘操作的卷, 则分别配置每个卷。

卷	备份选项
系统保留	完整备份
新加卷 (F:)	完整备份
本地磁盘 (C:)	完整备份
新加卷 (E:)	完整备份
	增量备份

确定(O) 取消(C)

系统管理

CMD添加用户、用户组、修改密码、删除用户

```
C:\Users\Administrator>net user hzwg /add
命令成功完成。

C:\Users\Administrator>net user hzwg 123456
命令成功完成。

C:\Users\Administrator>net localgroup zhangzhou /add
命令成功完成。

C:\Users\Administrator>net localgroup zhangzhou hzwg /add
命令成功完成。

C:\Users\Administrator>net user hzwg /del
命令成功完成。

C:\Users\Administrator>net localgroup zhangzhou /del
命令成功完成。
```

添加用户 hzwg

修改 hzwg 的密码为 123456

添加用户组 zhangzhou

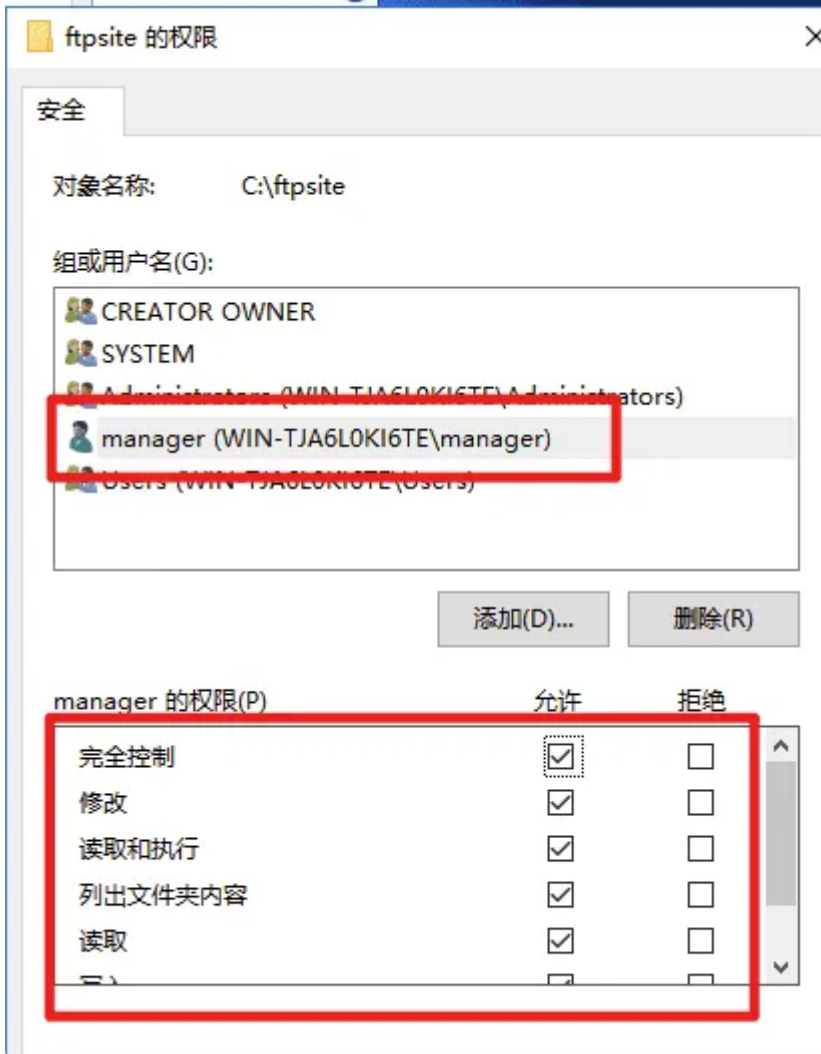
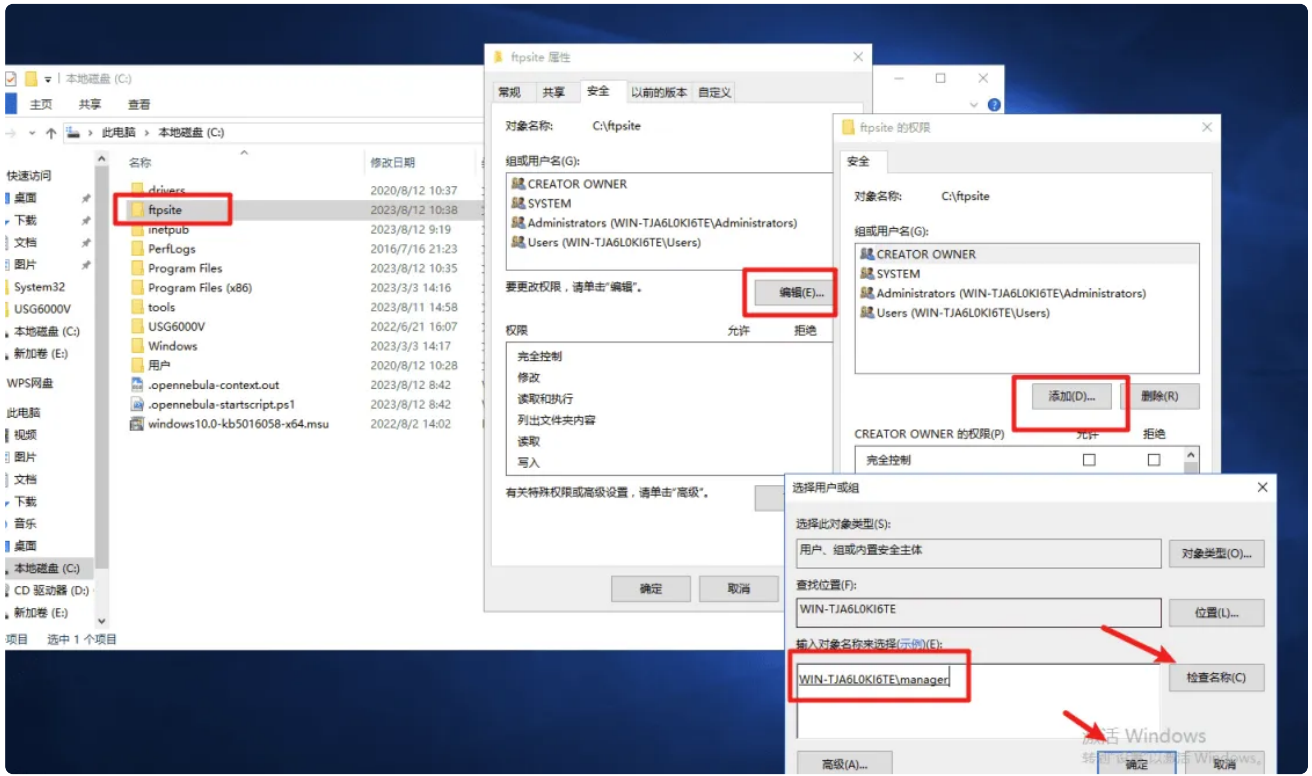
将 hzwg 添加到 zhangzhou 组

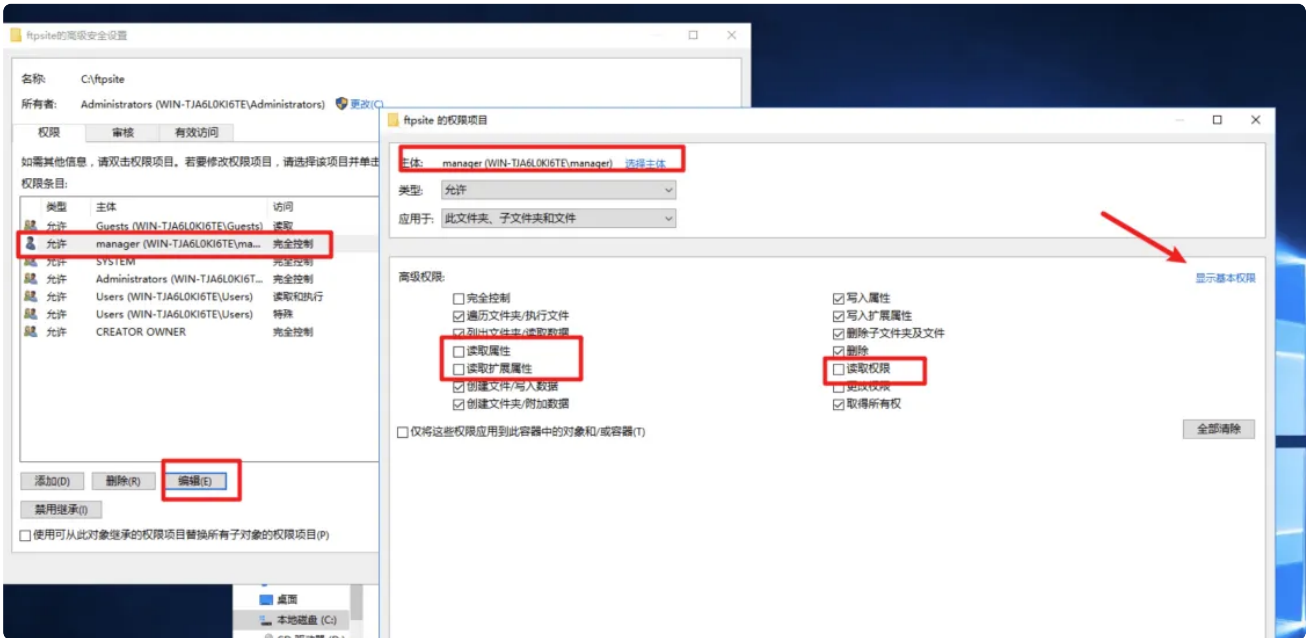
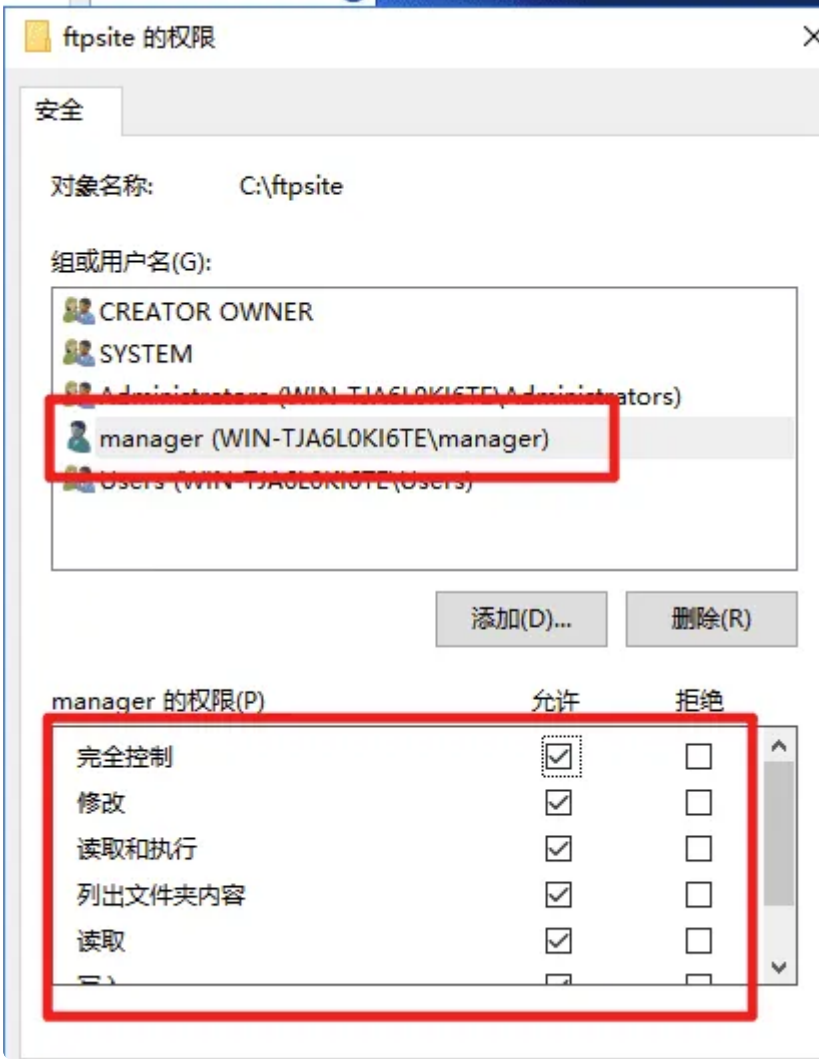
删除 hzwg

删除 zhangzhou 组

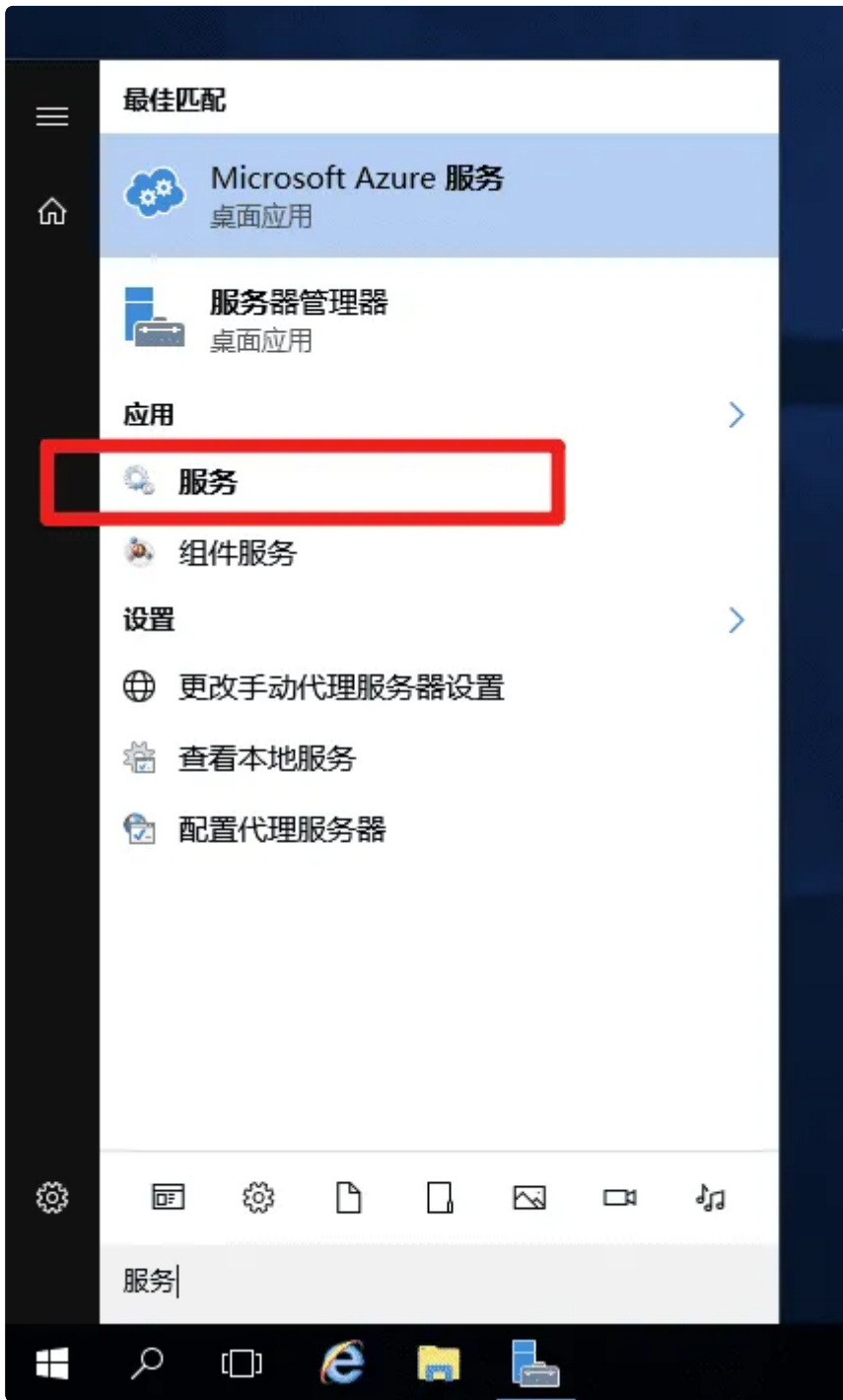
```
1 C:\Users\Administrator> net user hzwg /add
2 命令成功完成。
3
4
5 C:\Users\Administrator> net user hzwg 123456
6 命令成功完成。
7
8
9 C:\Users\Administrator> net localgroup zhangzhou /add
10 命令成功完成。
11
12
13 C:\Users\Administrator> net localgroup zhangzhou hzwg /add
14 命令成功完成。
15
16
17 C:\Users\Administrator> net user hzwg /del
18 命令成功完成。
19
20
21 C:\Users\Administrator> net localgroup zhangzhou /del
22 命令成功完成。
```

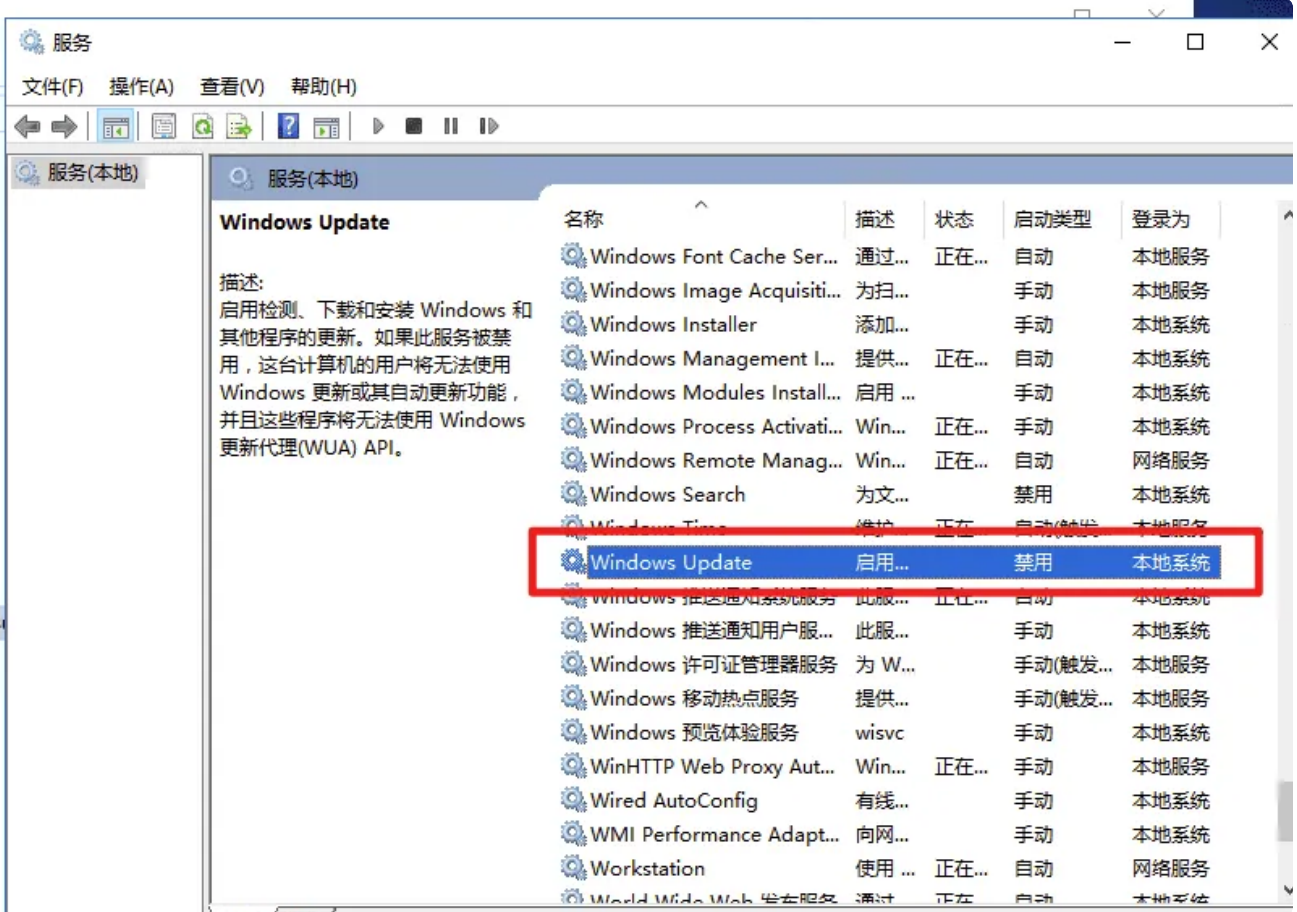
用户文件权限、高级权限





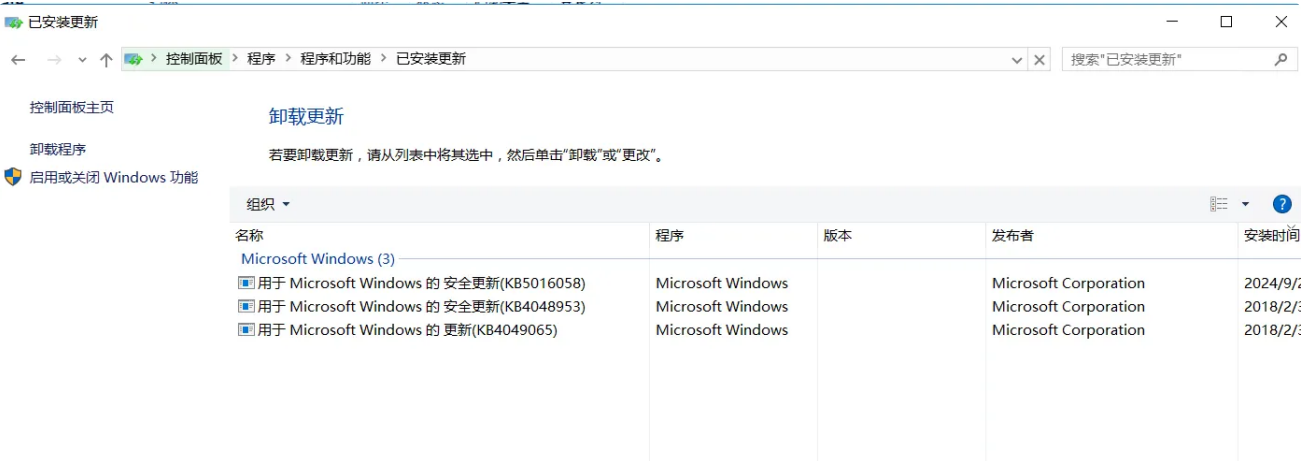
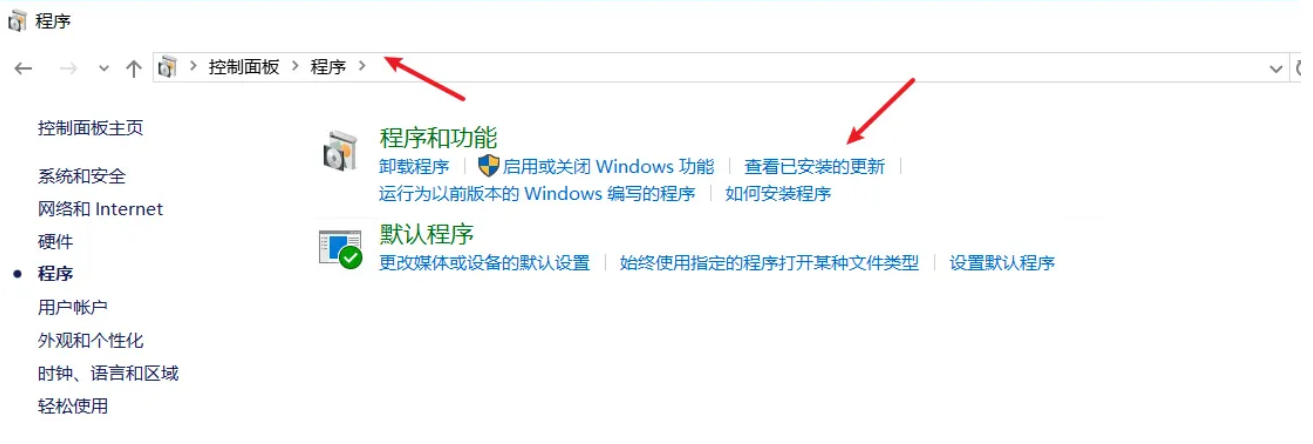
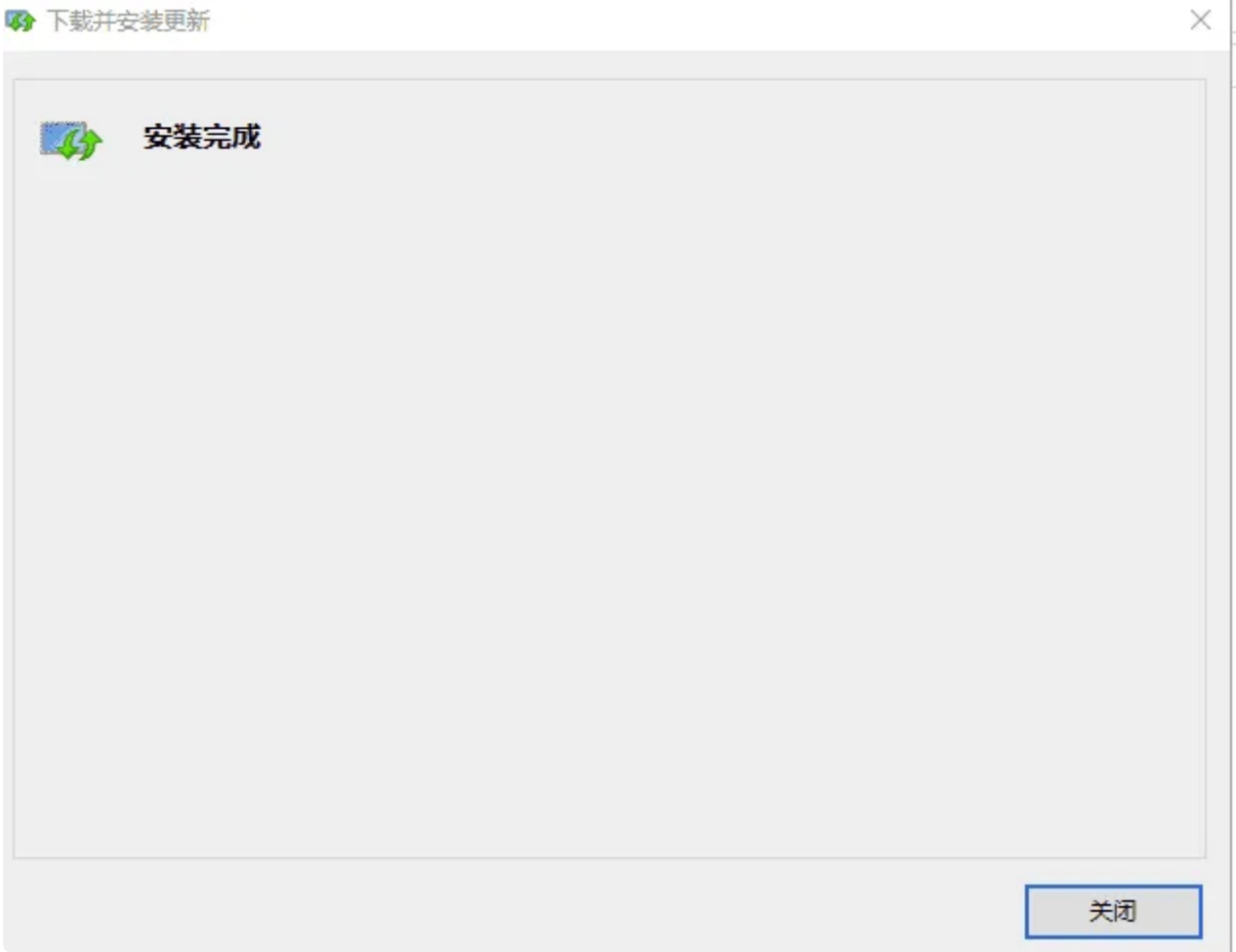
安装补丁



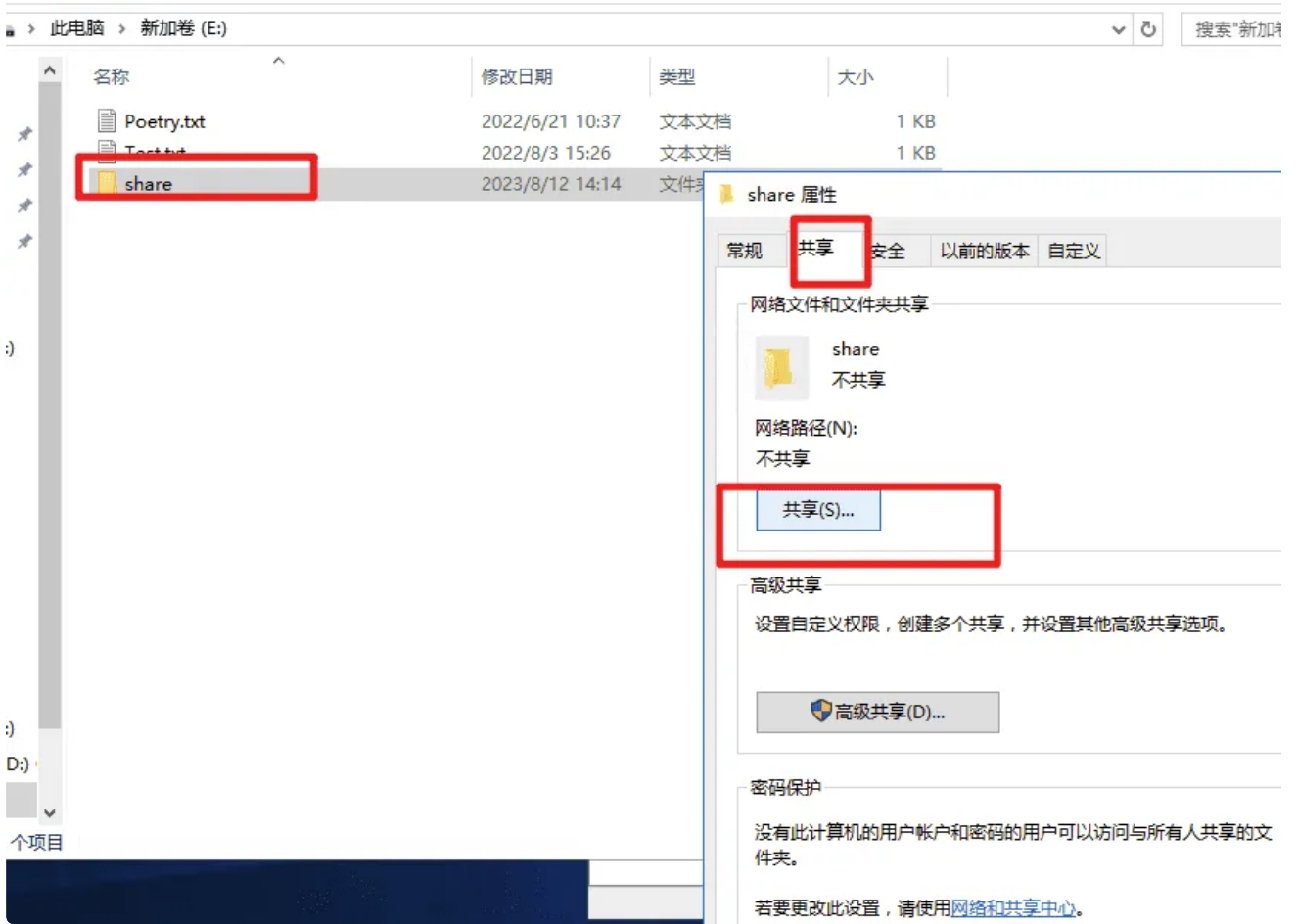


取消禁用，启动服务，然后再安装更新包





文件SMB共享



文件隐藏、只读

guest 属性

常规 共享 安全 以前的版本 自定义

guest

类型: 文件夹

位置: E:\share

大小: 0 字节

占用空间: 0 字节

包含: 0 个文件, 0 个文件夹

创建时间: 2023年8月12日, 14:18:39

属性: 只读(仅应用于文件夹中的文件)(R)

隐藏(H) 高级(D)...

qqq 属性

常规 共享 安全 以前的版本 自定义

qqq

类型: 文件夹

位置: E:\

大小: 0 字节

占用空间: 0 字节

包含: 0 个文件, 0 个文件夹

创建时间: 2023年8月12日, 14:30:39

属性: 只读(仅应用于文件夹中的文件)(R)

隐藏(H) 高级(D)...

火绒信任区、压缩包扫描、系统加固



以下文件已经被信任，已被认为是安全的；如果发生误报，您也可以在此加入信任

文件 网址

路径

类型

Q

C:\Users\Administrator\Desktop\whitelist\

文件夹

设置

常规设置

基础设置

查杀设置

软件升级

病毒防护

系统防护

网络防护

全盘查杀配置

深度查杀压缩包中的木马病毒，并跳过大于 10 MB的压缩包 (20M-9999M)

仅扫描 指定扩展名文件 例如：.exe;.doc;.txt;.zip

扫描网络驱动器

病毒处理方式

询问我

自动处理

火绒扫描

病毒类型



共发现风险项目1个，建议立即处理

全部忽略 立即处理

风险项目

状态

C:\tools\安全自...

代码混淆器 VirTool/Obfuscator.fq

风险详情

病毒类型：代码混淆器 (VirTool/Obfuscator.fq)

病毒描述：通过代码变形、反跟踪、反虚拟机等技术手段，专门被病毒用来与安全软件进行技术对抗的恶意代码类型。

风险路径：C:\tools\安全自检工具.exe

处理建议：立即处理

打开文件路径

信任文件

MD5计算

```
C:\tools>certutil -hashfile 安全自检工具.exe md5
MD5 哈希(文件 安全自检工具.exe):
99342a4b5ce806ef4ab2a6d89ba8e99e
CertUtil: -hashfile 命令成功完成。
```

certutil -hashfile 文件名 md5