

# AD域

域架构: 主从域

主机名	IP	角色
pdc.test.com	172.168.2.61	PDC
bdc.test.com	172.168.2.62	BDC
client01.test.com	172.168.2.65	client01
client02.test.com	172.168.2.66	client02

## 1. 安装PDC

### 1.1 配置网络

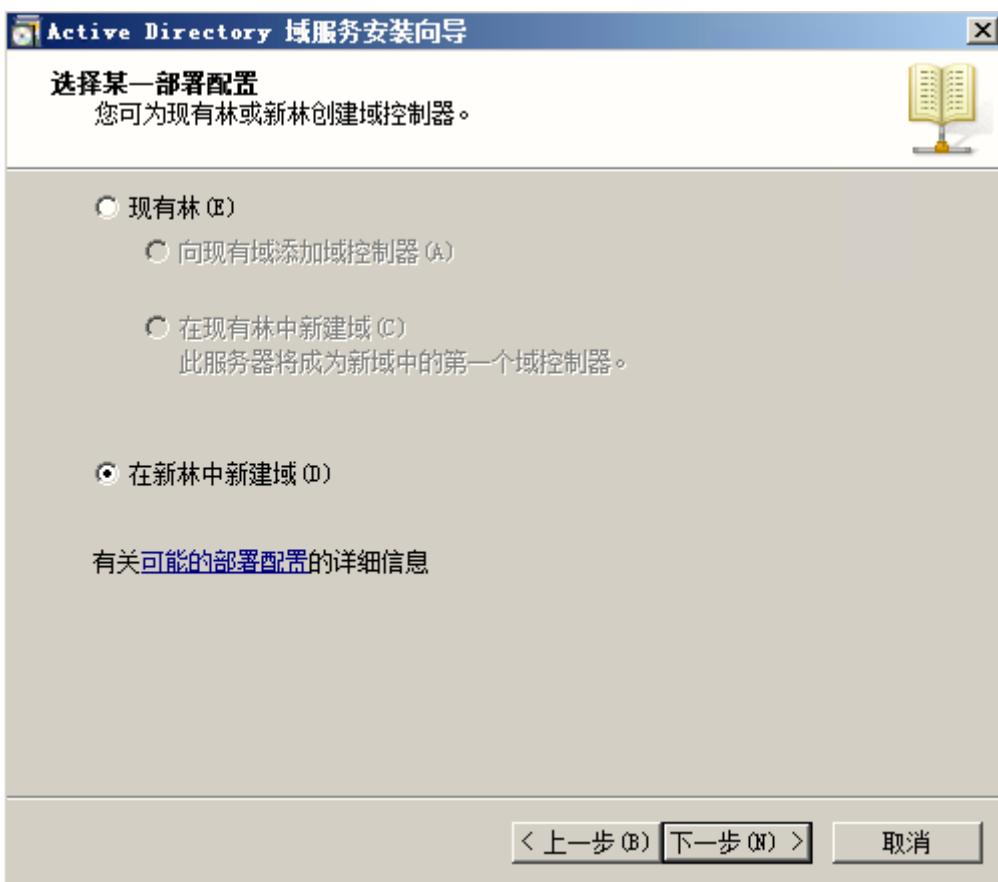
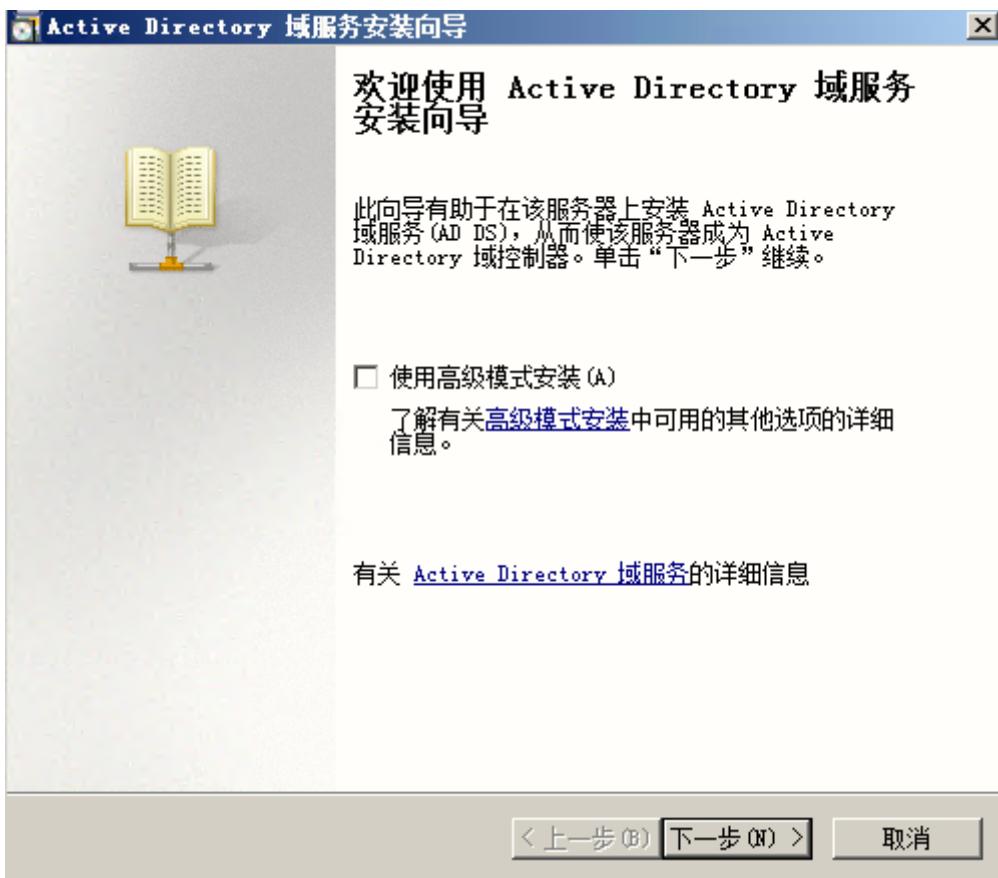
```
# 配置网络

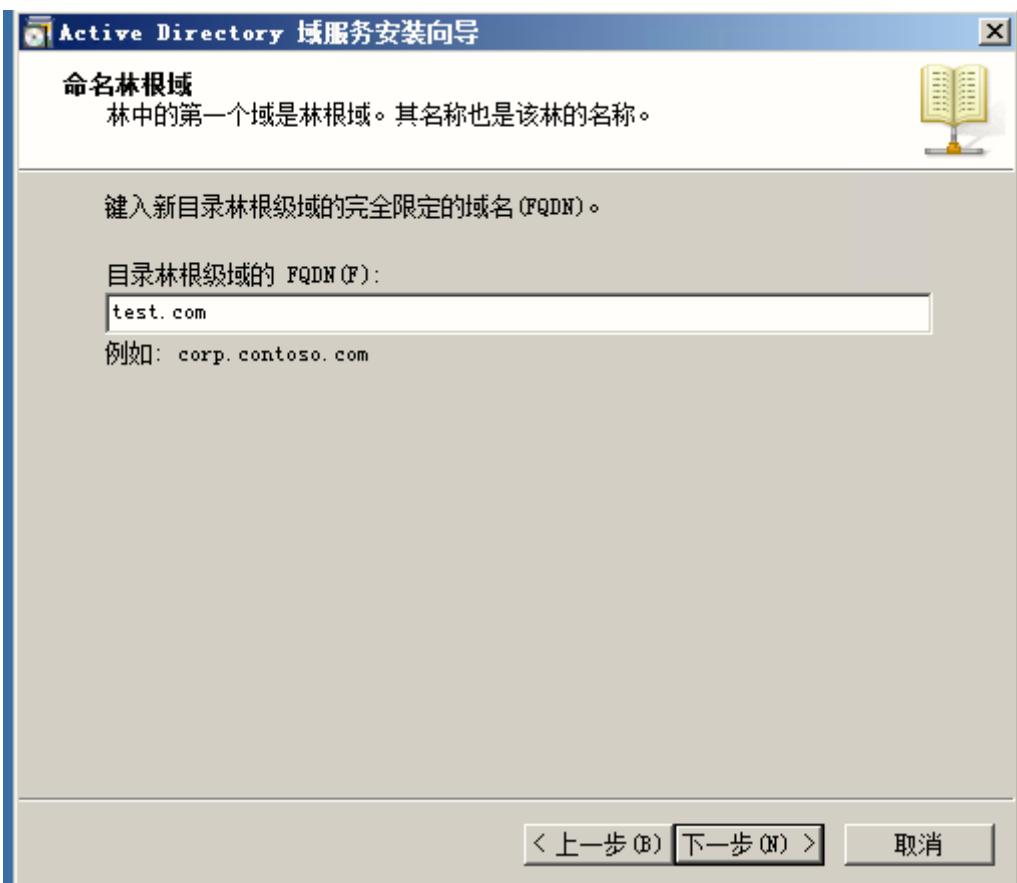
# 查看接口索引
netsh interface ip show interface
netsh interface ip set address 11 static 172.168.2.61 255.255.255.0
172.168.2.254
netsh interface ip add dnservers 11 127.0.0.1
# 启用接口
netsh interface set interface "本地连接" admin=enabled

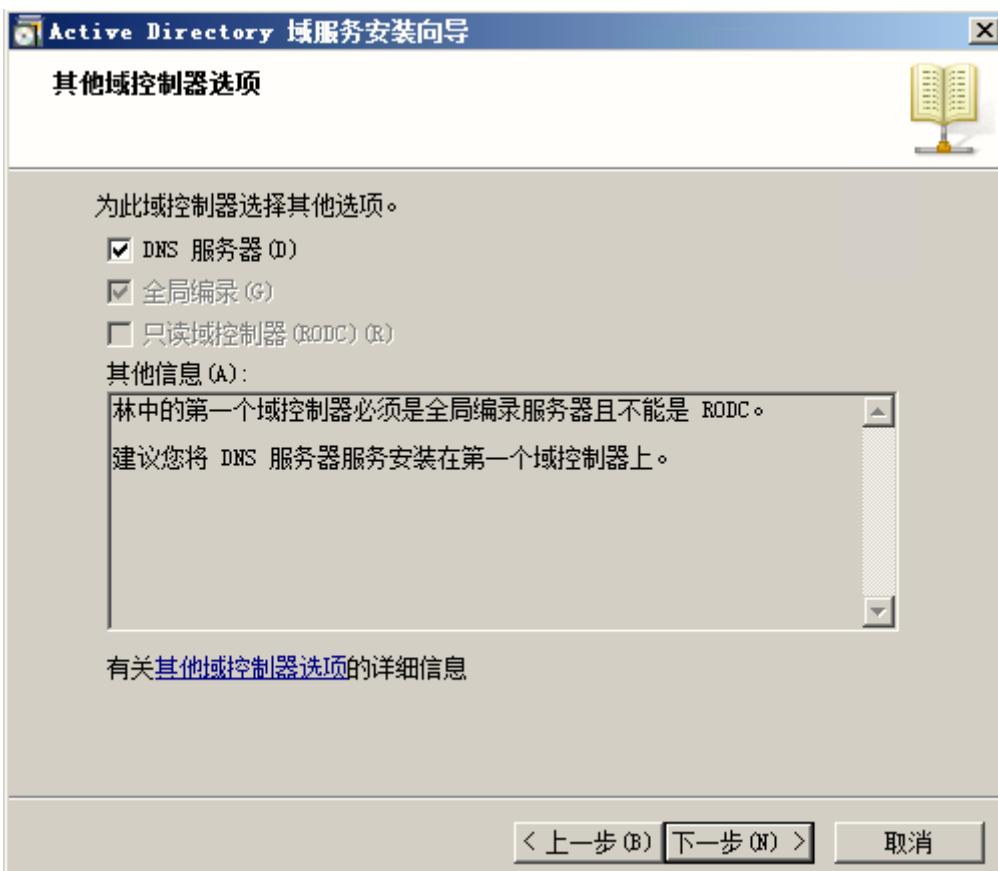
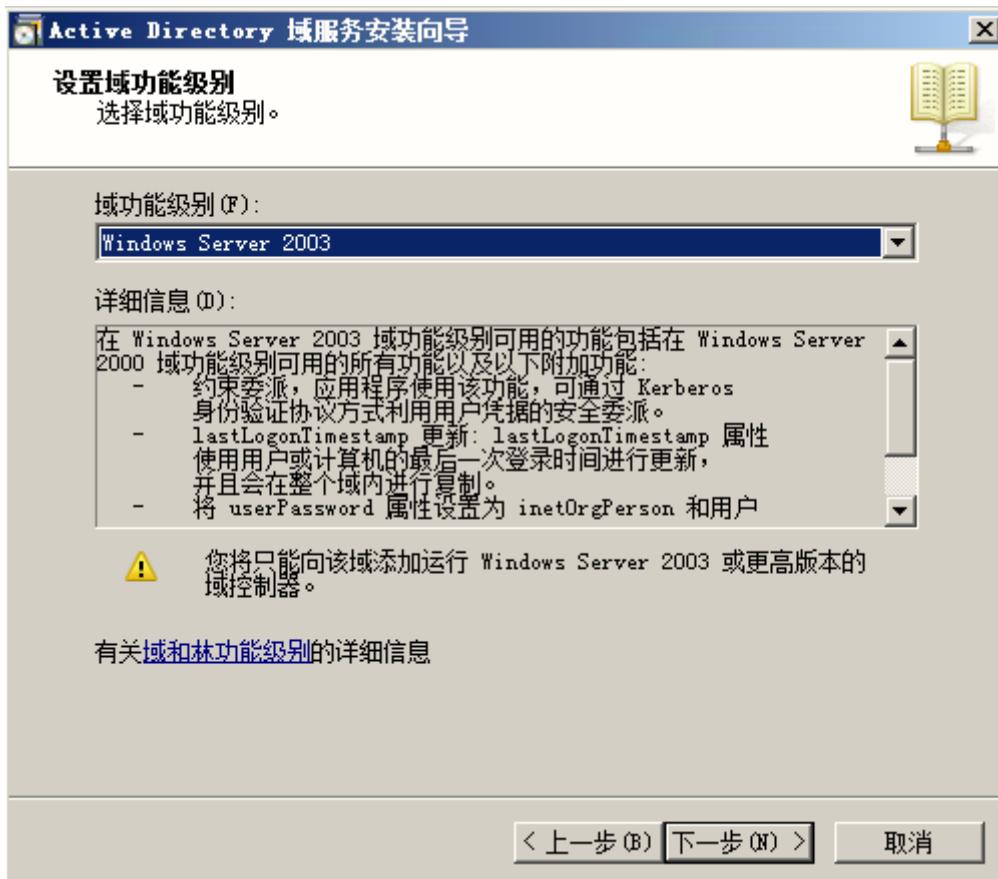
# 关闭防火墙
netsh advfirewall show domainprofile
netsh advfirewall set allprofiles state off
```

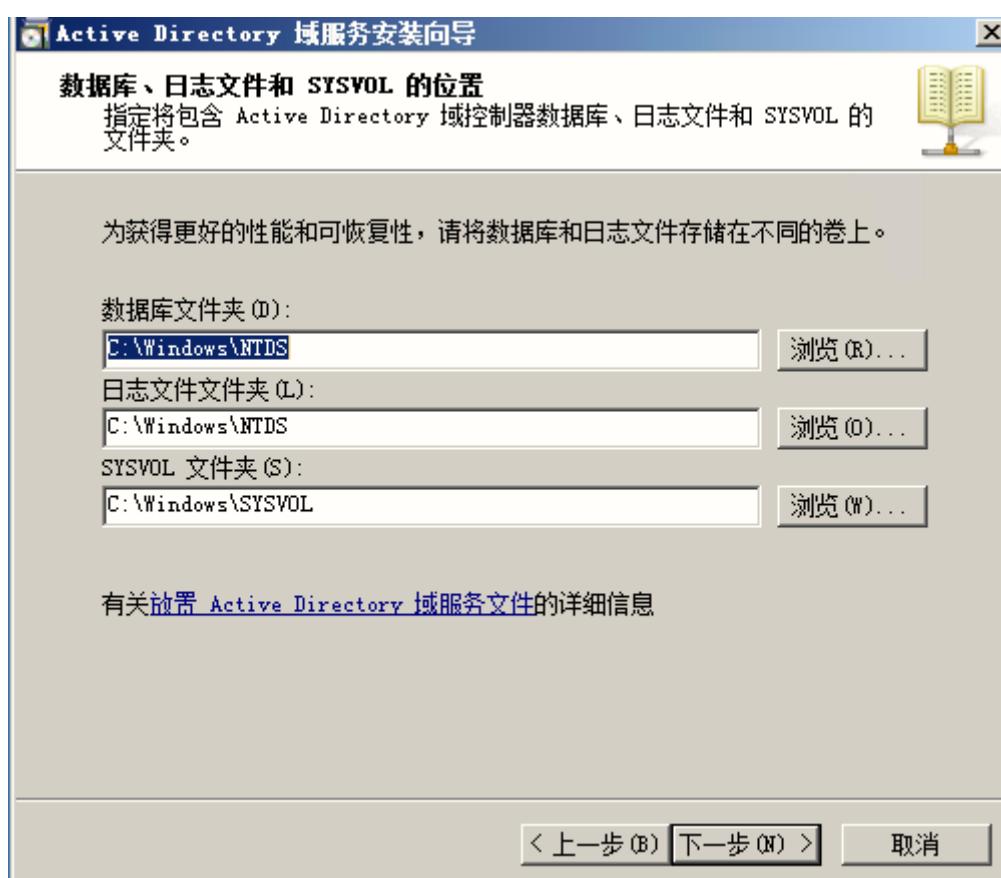
### 1.2 安装第一台域控

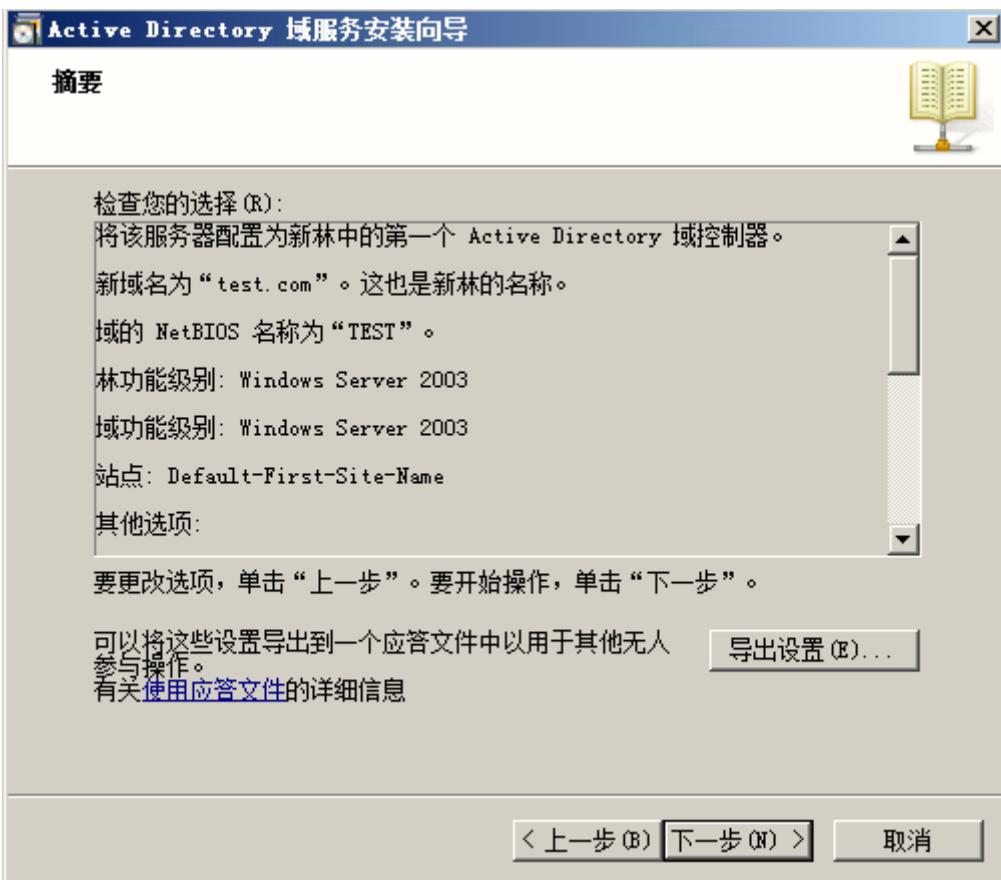
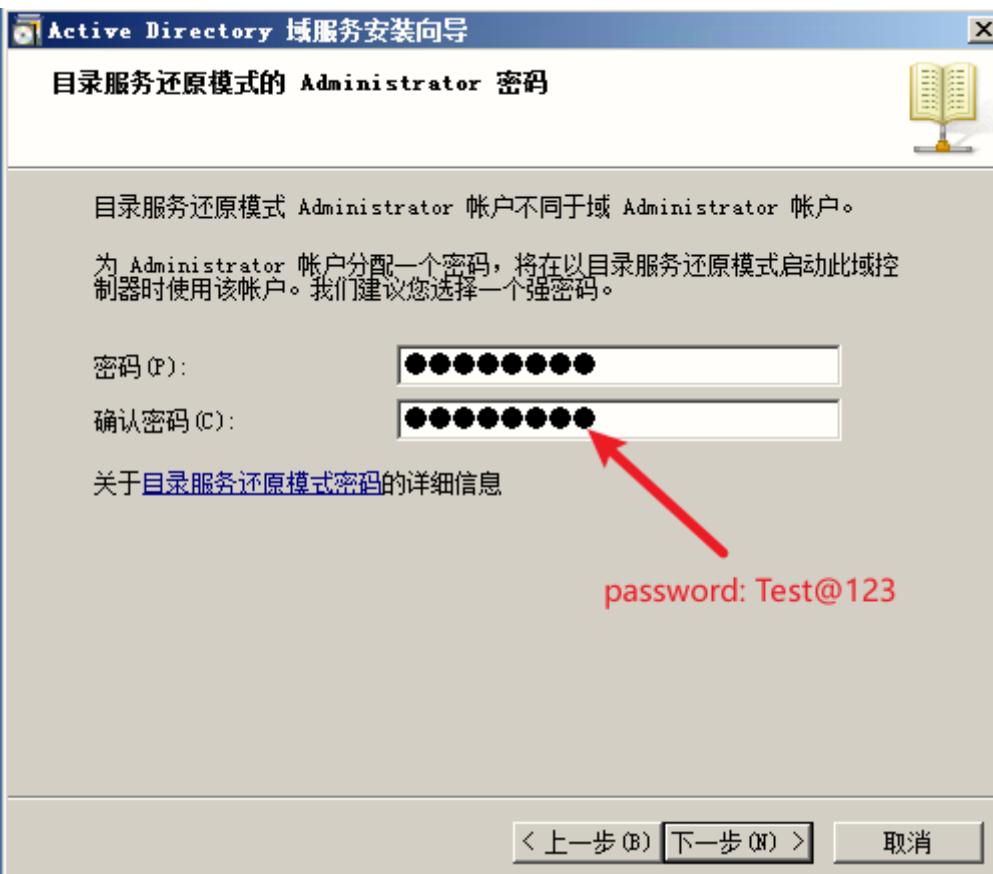
```
# 打开安装域控程序窗口
dcromo
```

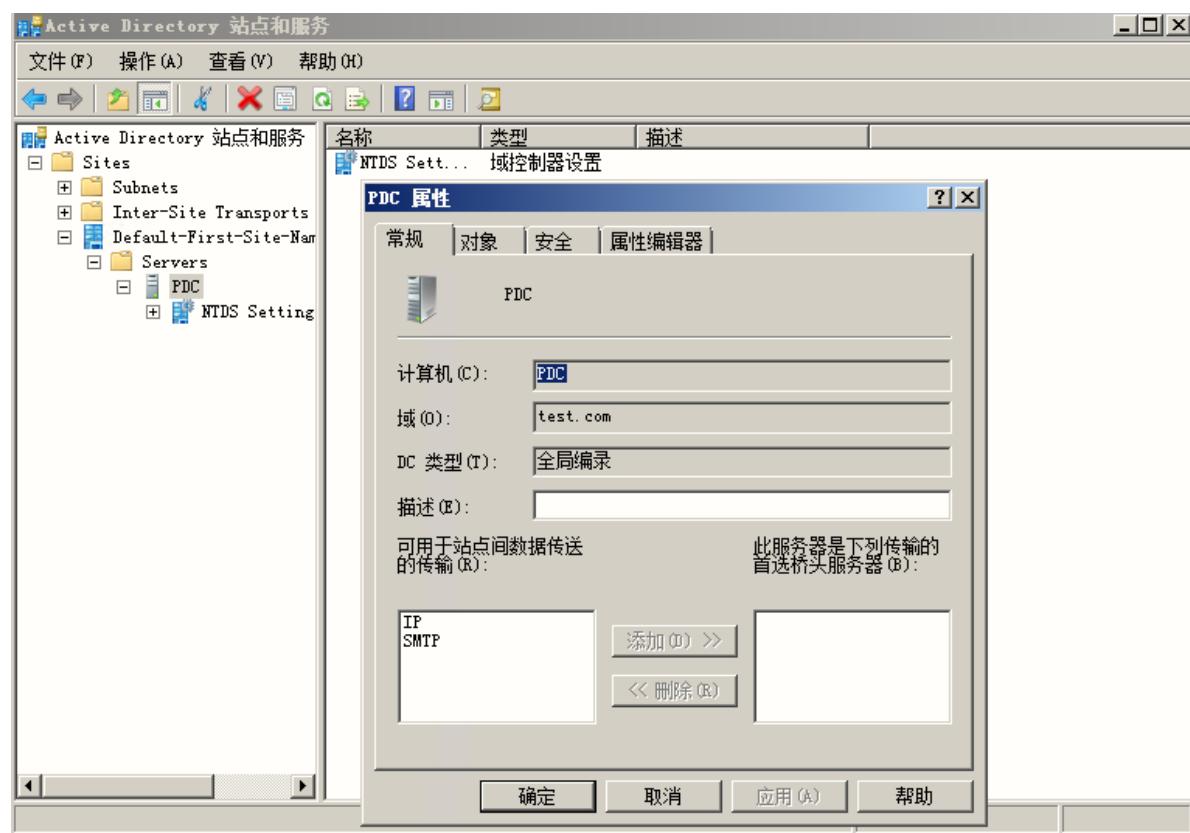
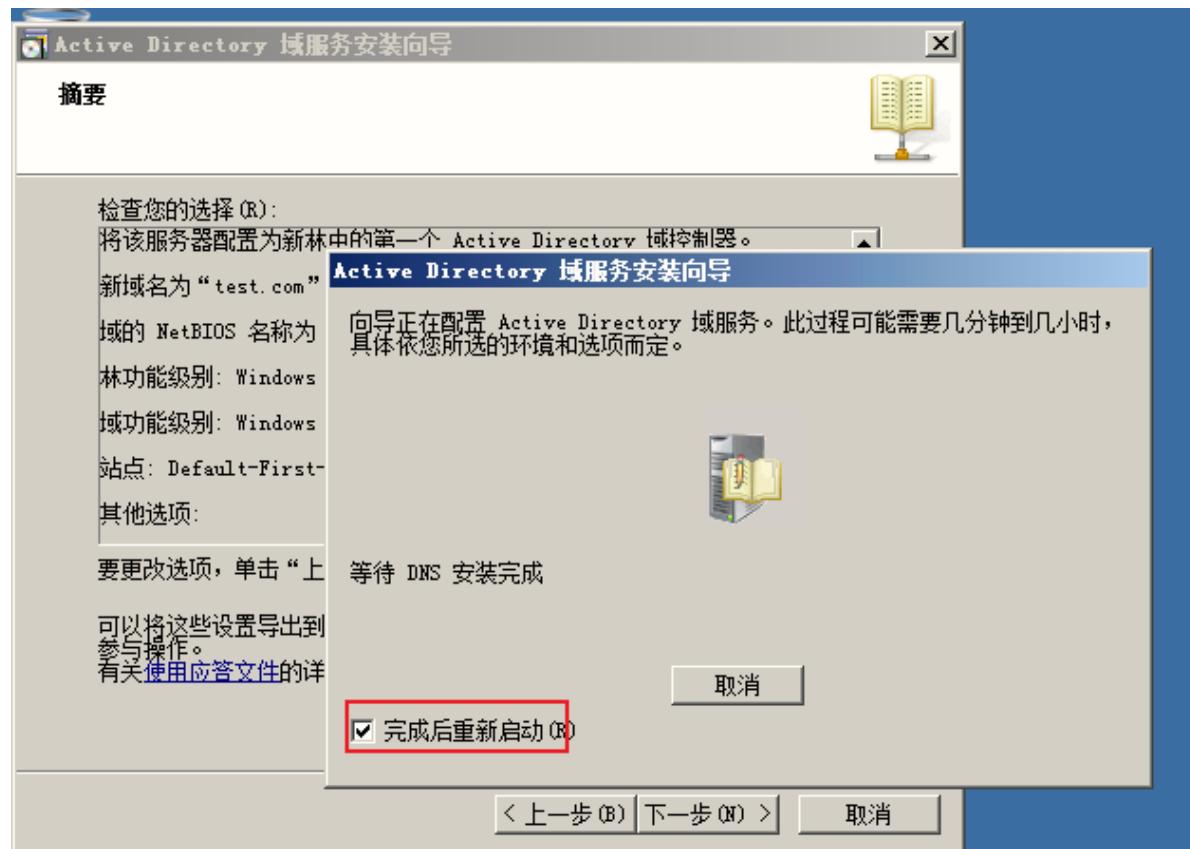


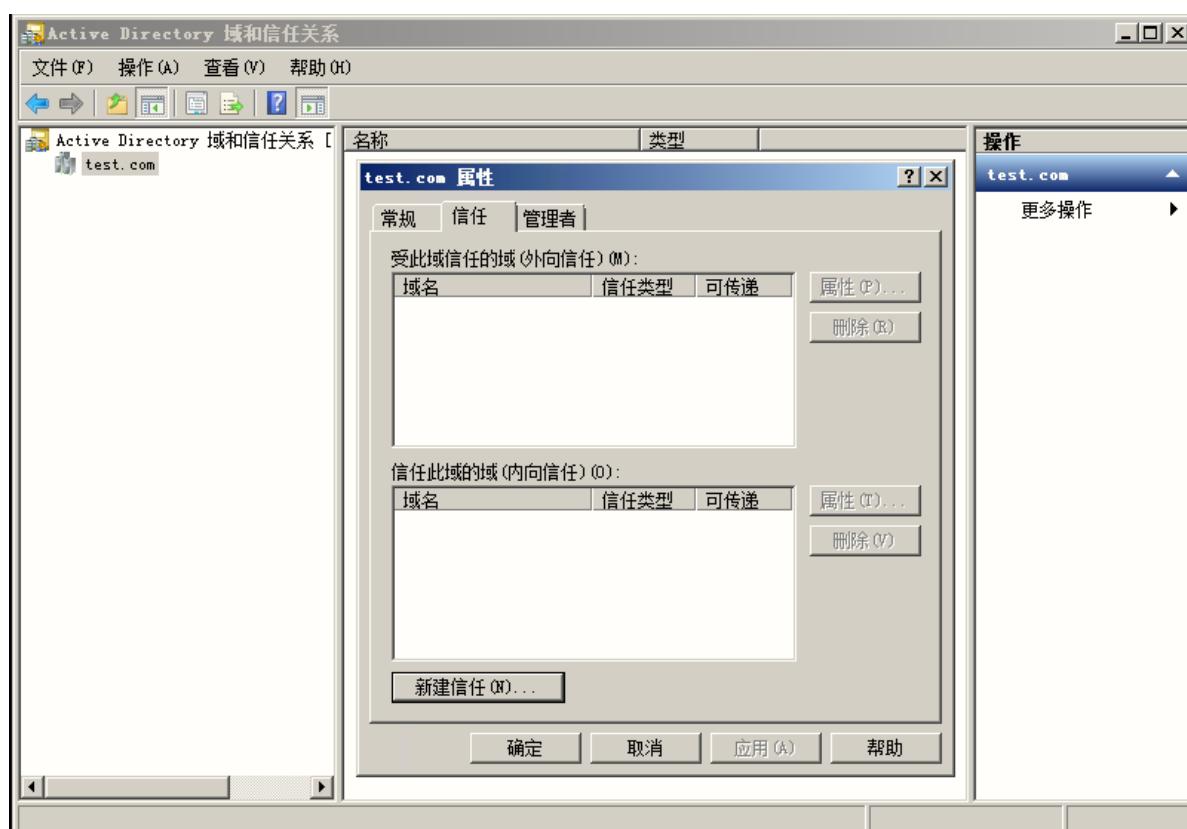
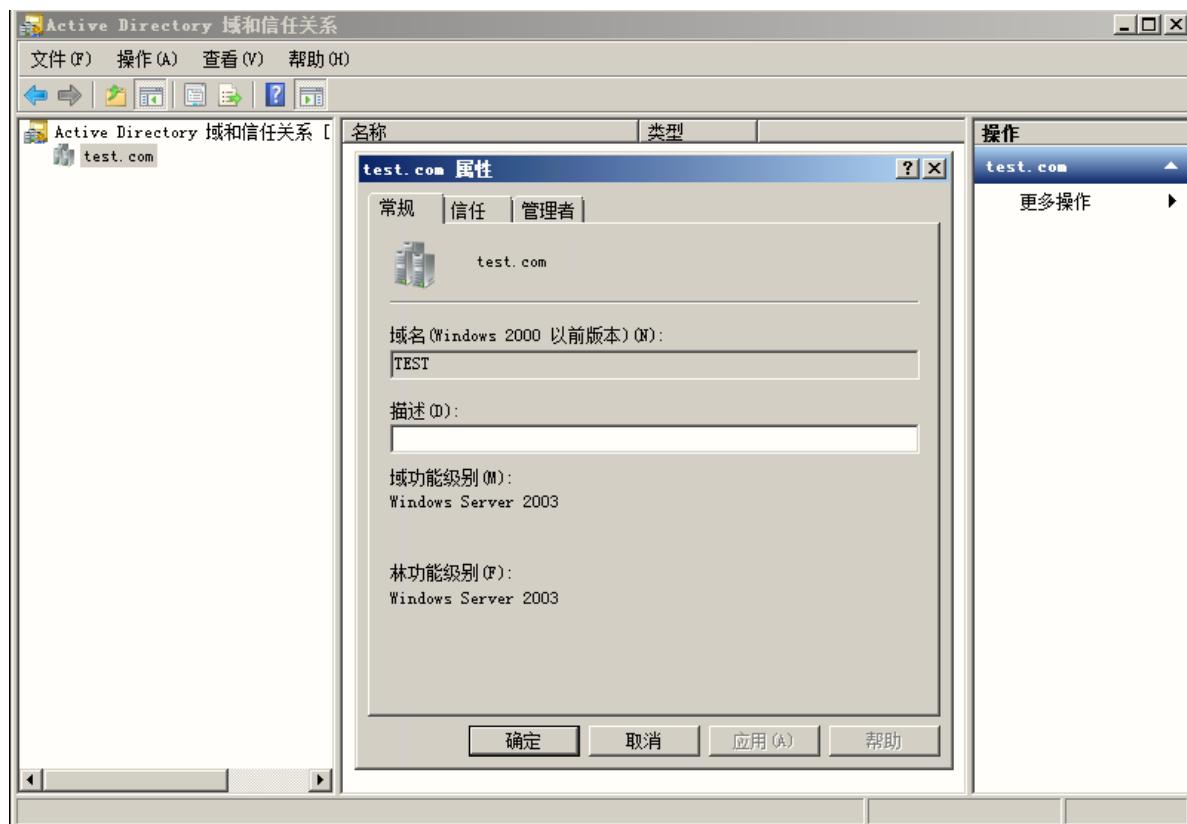


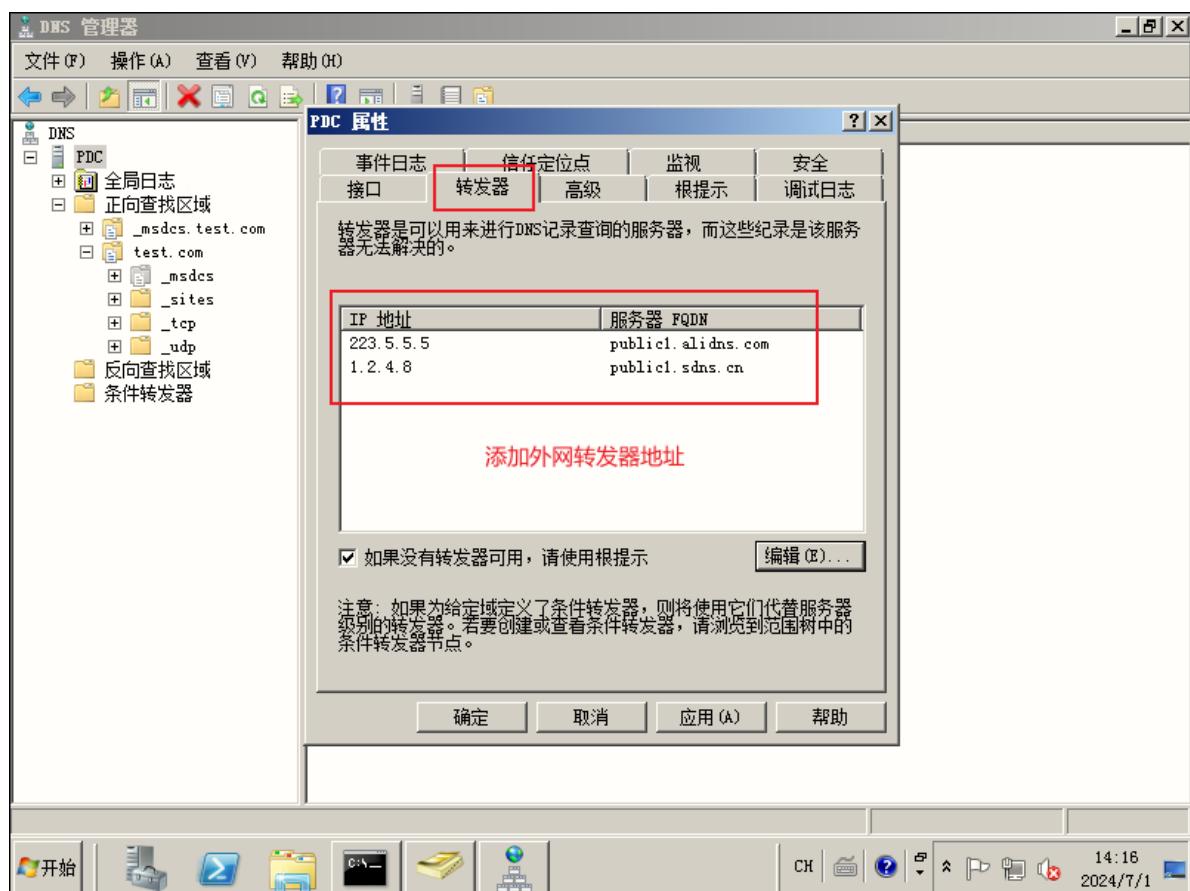
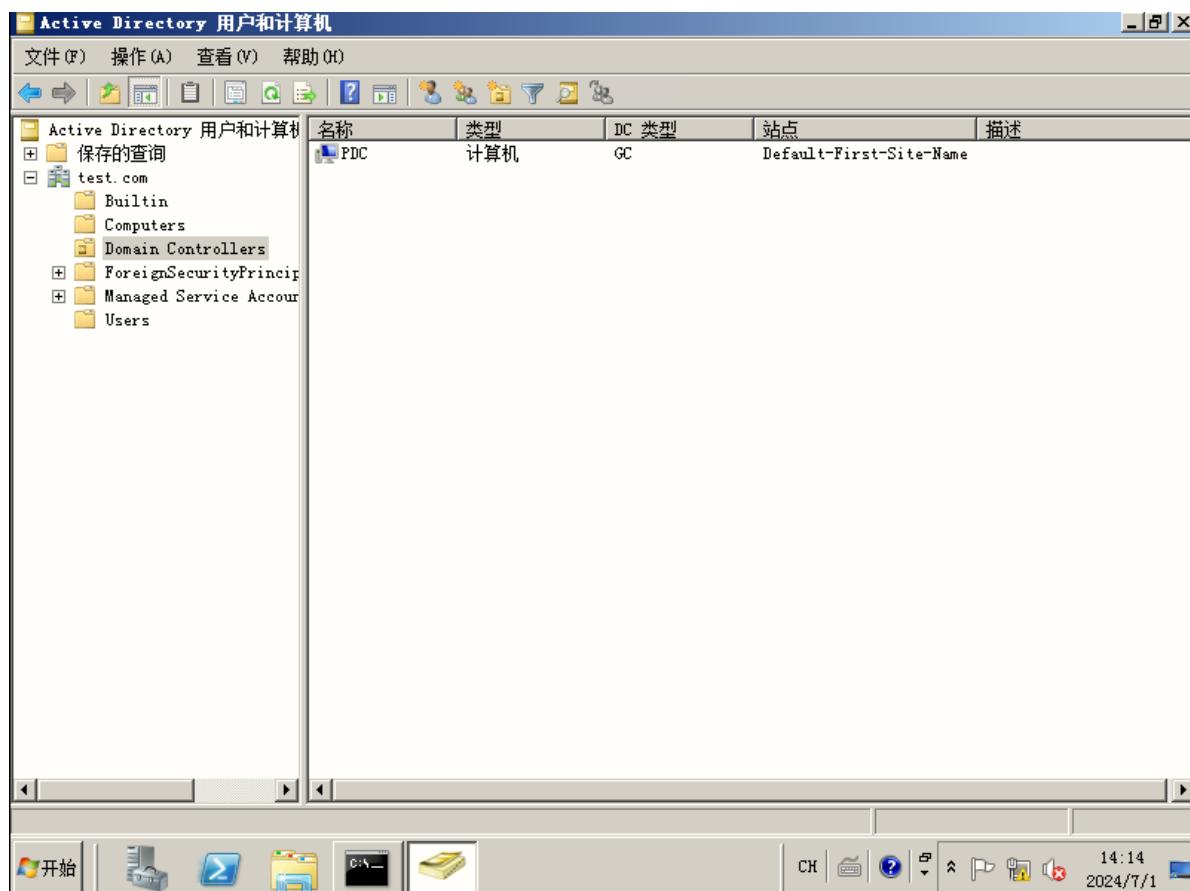


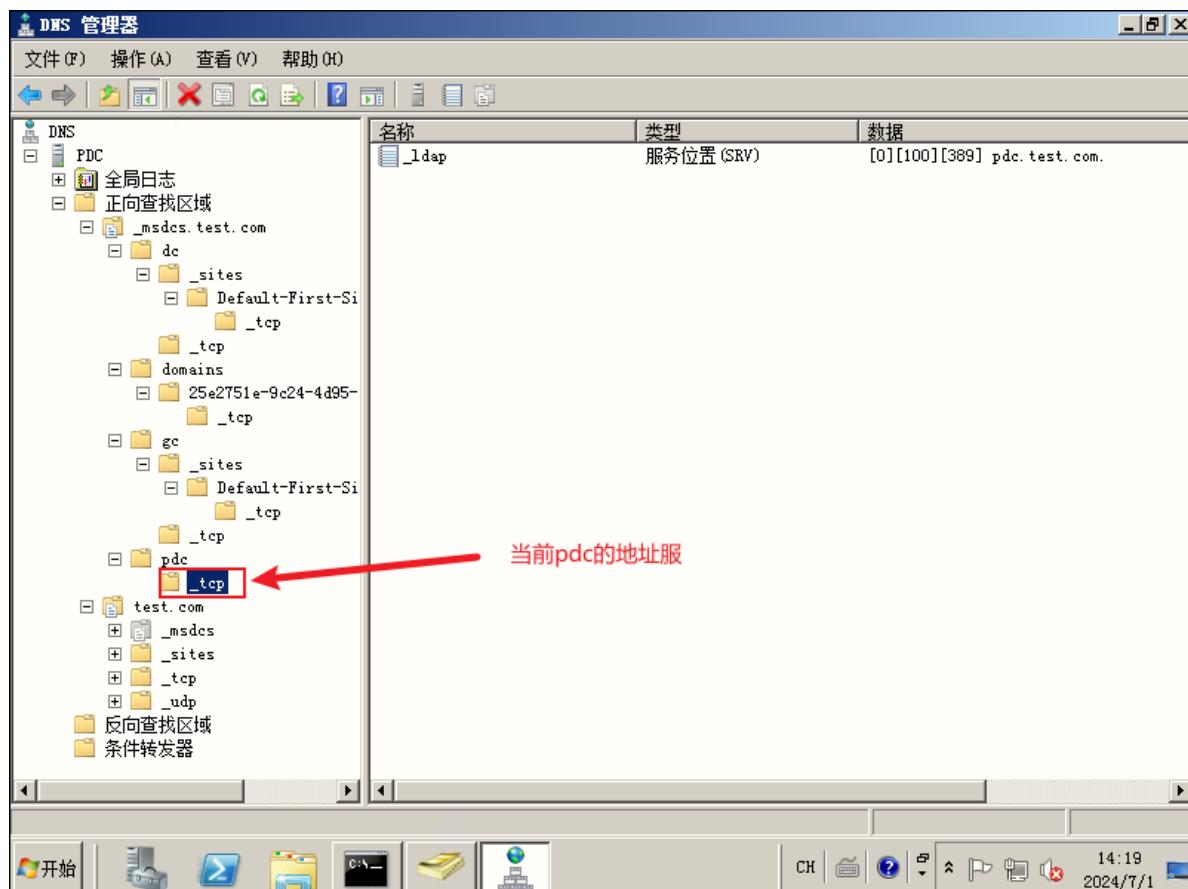




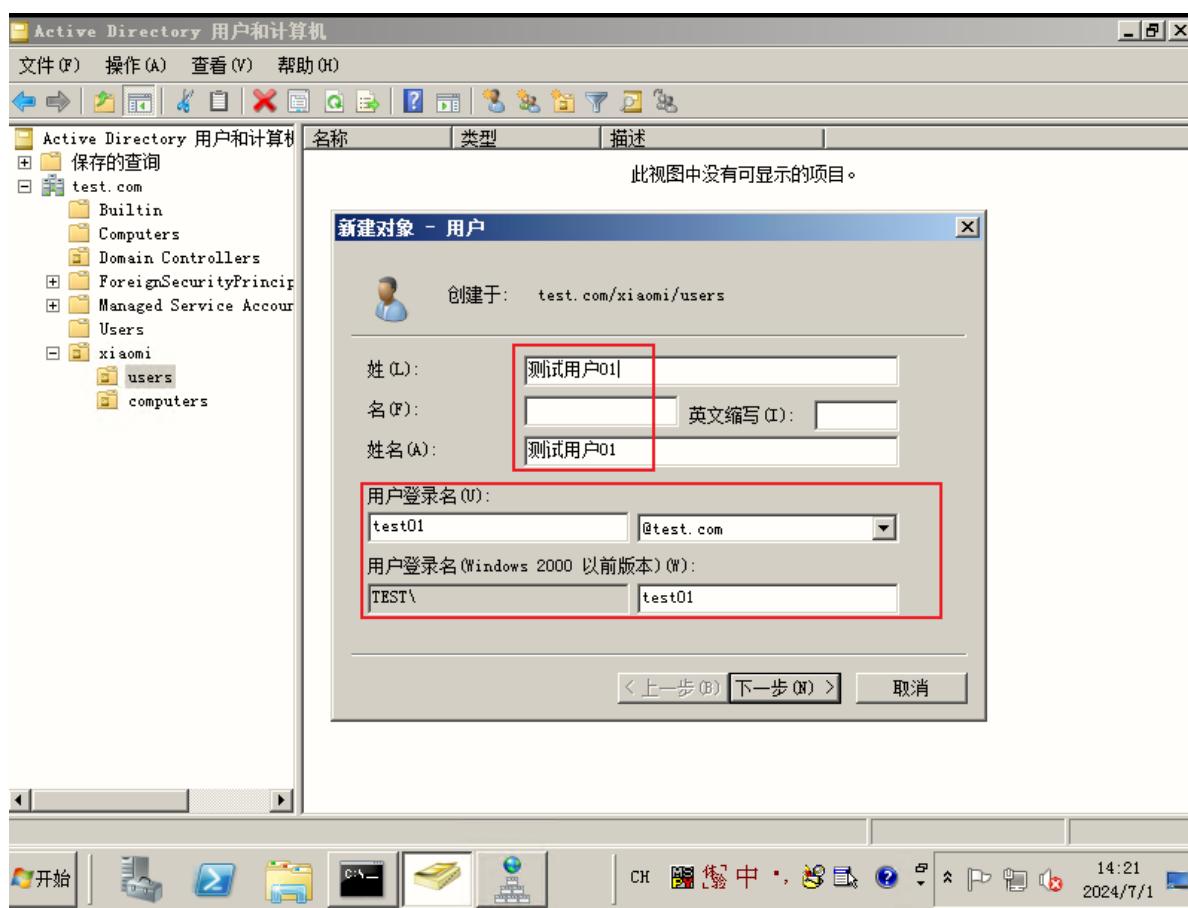


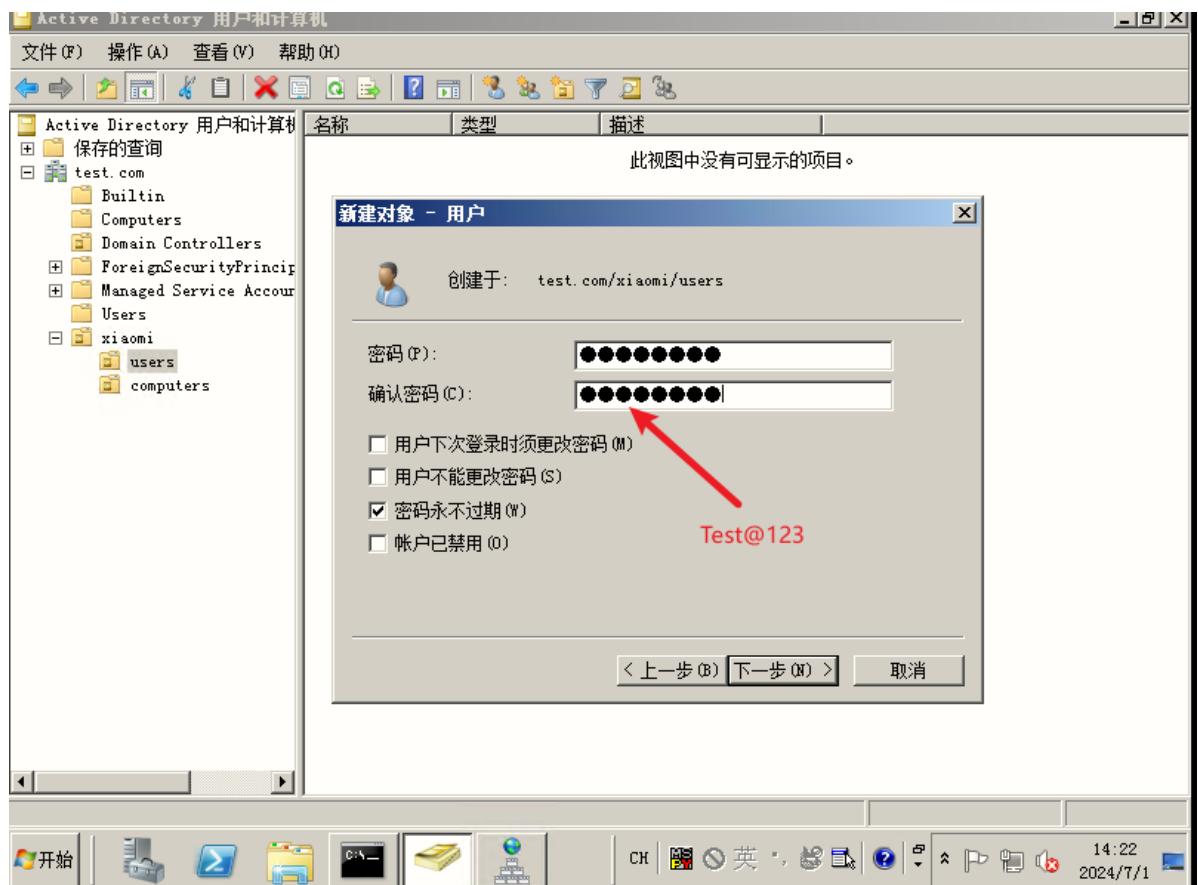






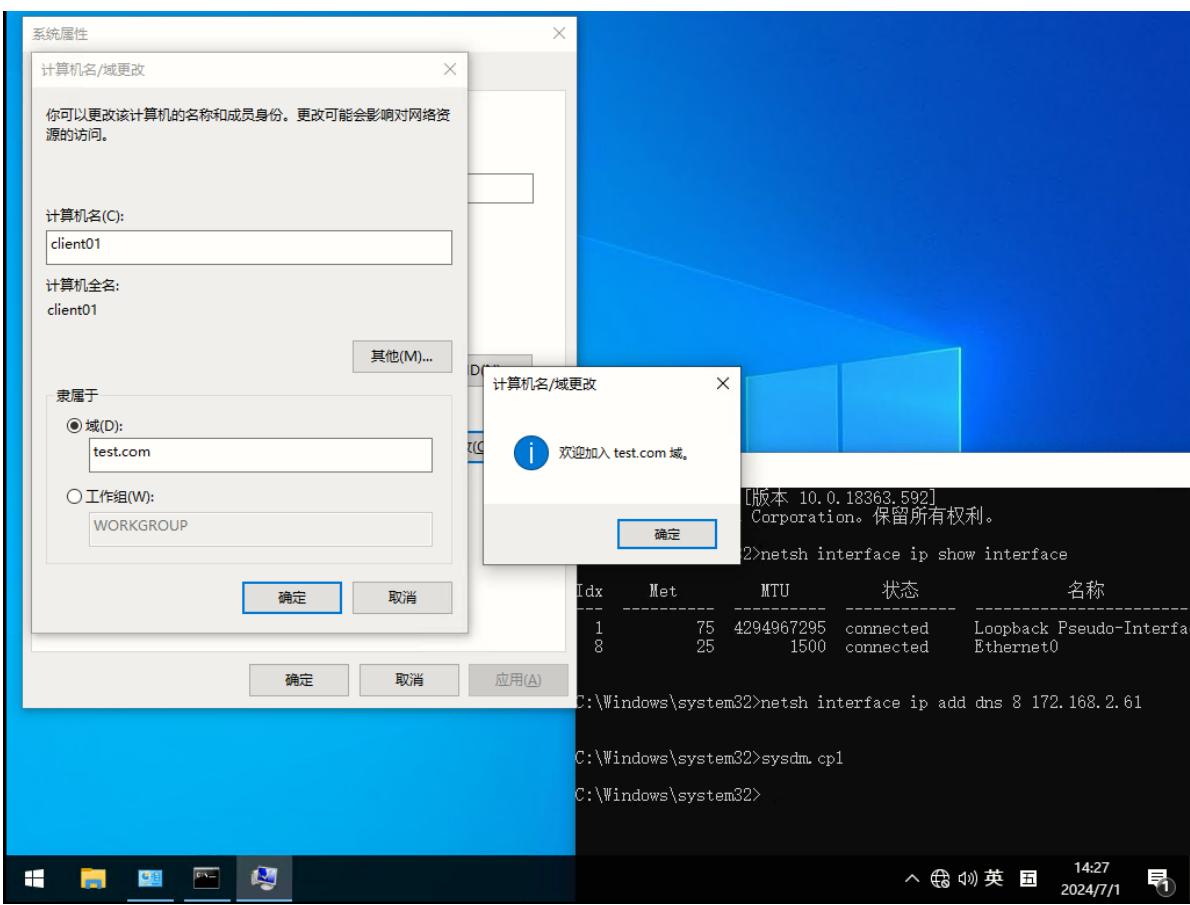
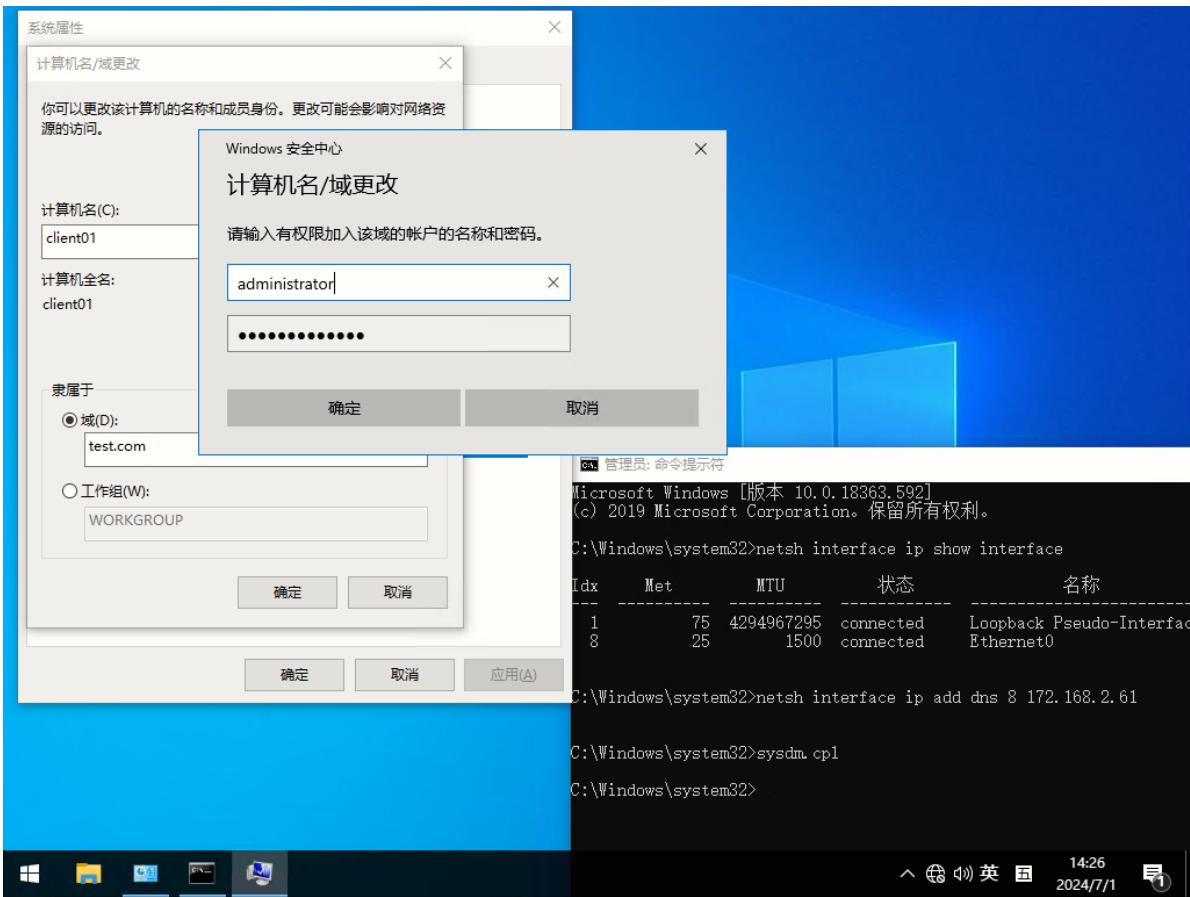
### 1.3 创建普通域用户



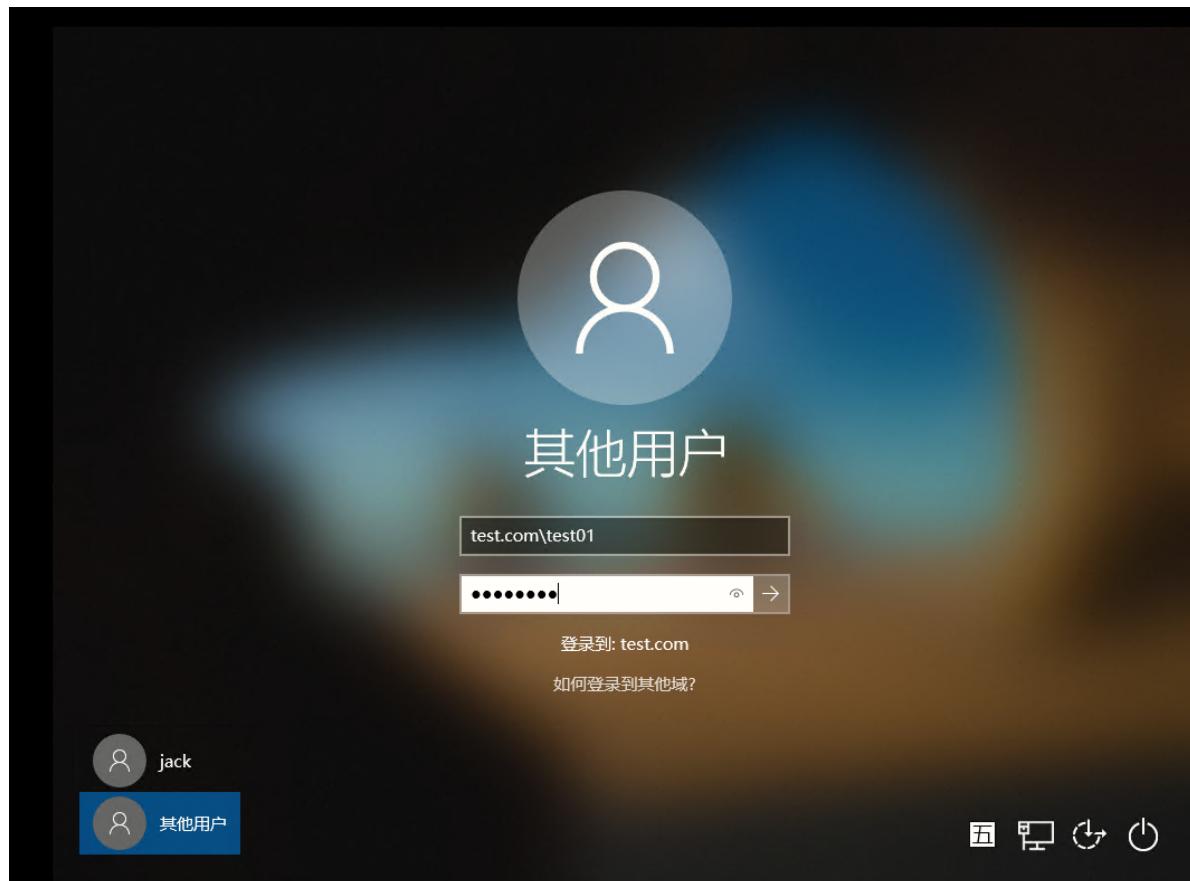


## 2. 客户端01

### 2.1 配置网络并加域



## 2.2 登录域用户并测试dns



```
C:\Windows\system32\cmd.exe
获得域“test.com”中 DC 的列表(从“\\pdc.test.com”中)。
pdc.test.com [PDC] [DS] 站点: Default-First-Site-Name
此命令成功完成

C:\Users\test01>whomia
“whomia”不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\Users\test01>whoami
test\test01

C:\Users\test01>hostname
client01

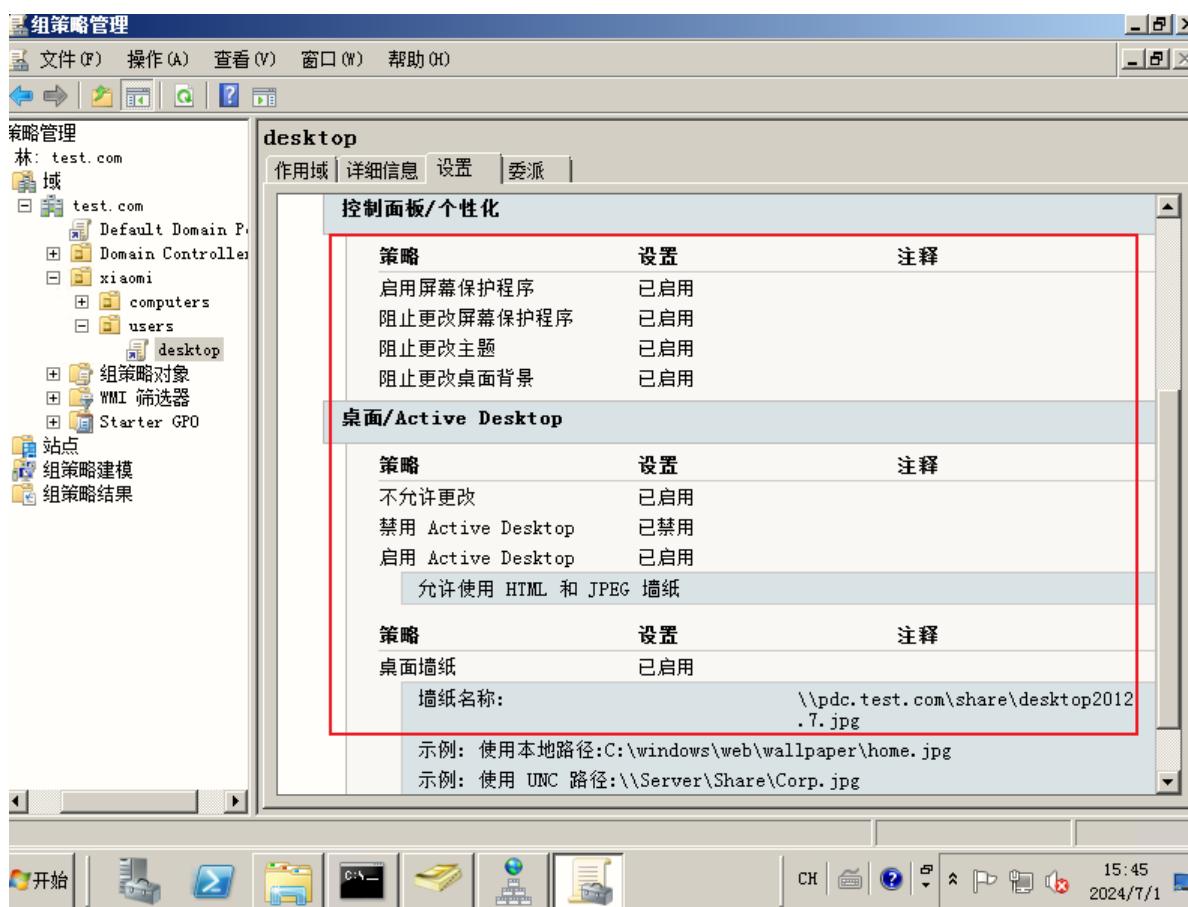
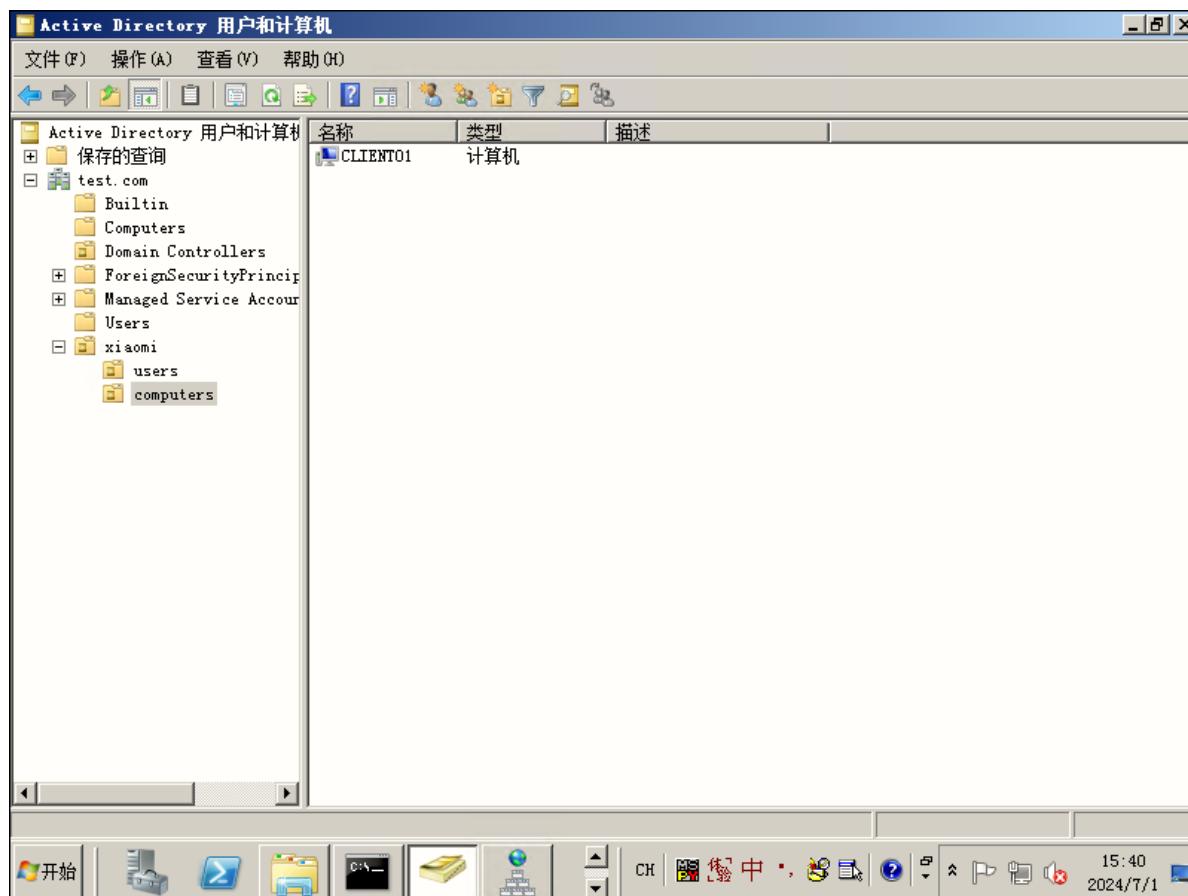
C:\Users\test01>nltest /dclist:test.com
获得域“test.com”中 DC 的列表(从“\\pdc.test.com”中)。
pdc.test.com [PDC] [DS] 站点: Default-First-Site-Name
此命令成功完成

C:\Users\test01>ping -n 1 pdc.test.com
正在 Ping pdc.test.com [172.168.2.61] 具有 32 字节的数据:
来自 172.168.2.61 的回复: 字节=32 时间<1ms TTL=128

172.168.2.61 的 Ping 统计信息:
数据包: 已发送 = 1, 已接收 = 1, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\test01>
```

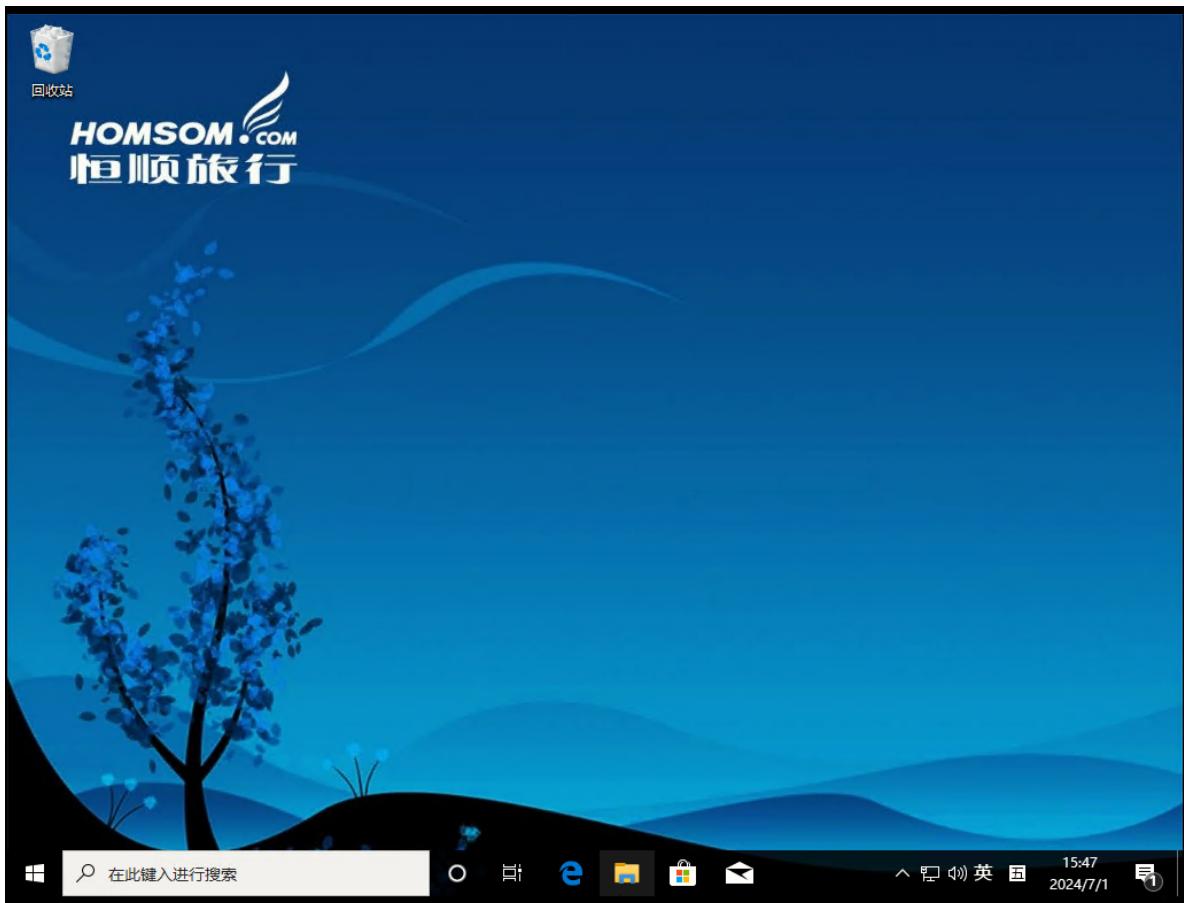
## 2.3 PDC配置组策略



## 2.4 客户端01验证组策略

### 强制刷新组策略并重启

```
gpupdate /force  
shutdown -r -t 0
```



## 3. 安装BDC

### 3.1 配置网络

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ipconfig /all

Windows IP 配置

主机名 . . . . . : bdc
主 DNS 后缀 . . . . . :
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否

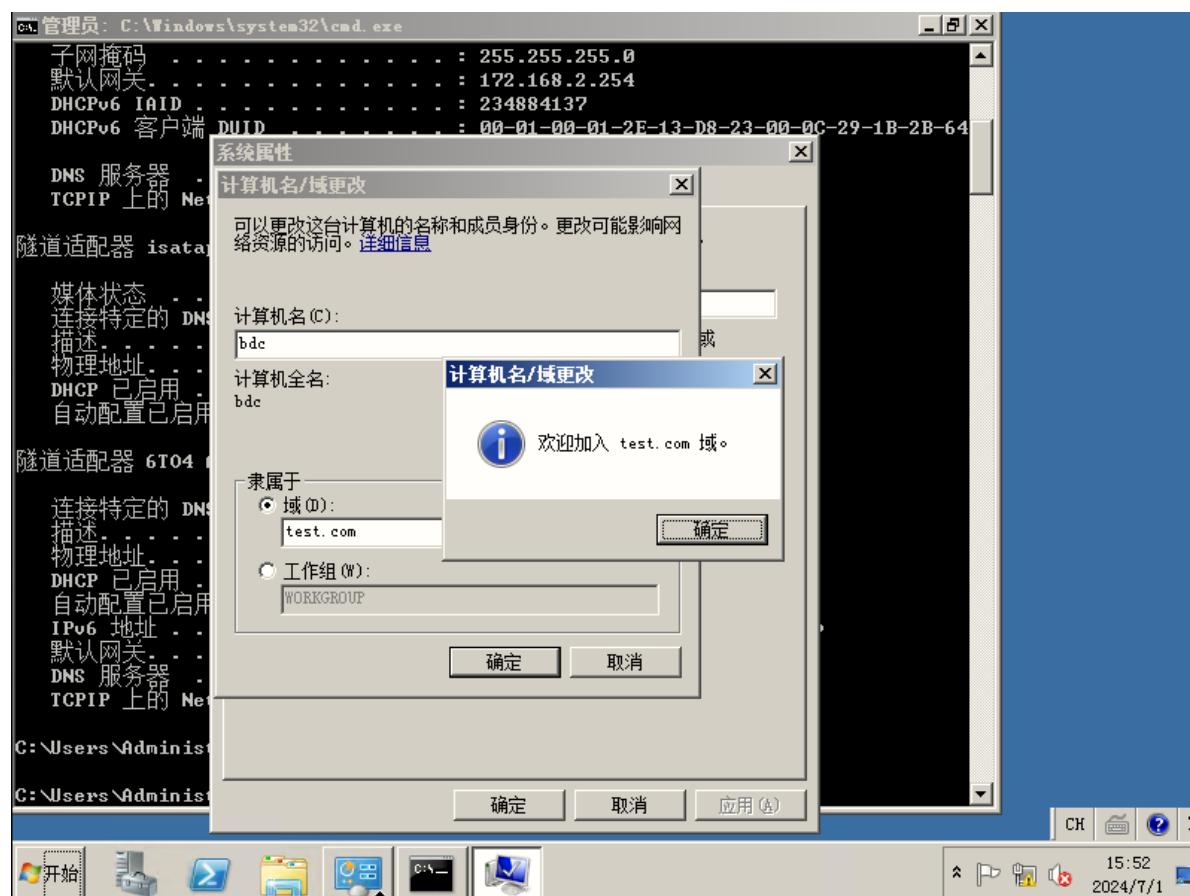
以太网适配器 本地连接:

连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Intel(R) PRO/1000 MT Network Connection
物理地址 . . . . . : 00-0C-29-84-D5-3A
DHCP 已启用 . . . . . : 否
自动配置已启用 . . . . . : 是
本地链接 IPv6 地址 . . . . . : fe80::3815:b965:72a7:7d25%11<首选>
IPv4 地址 . . . . . : 172.168.2.62<首选>
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 172.168.2.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2E-13-D8-23-00-0C-29-1B-2B-64

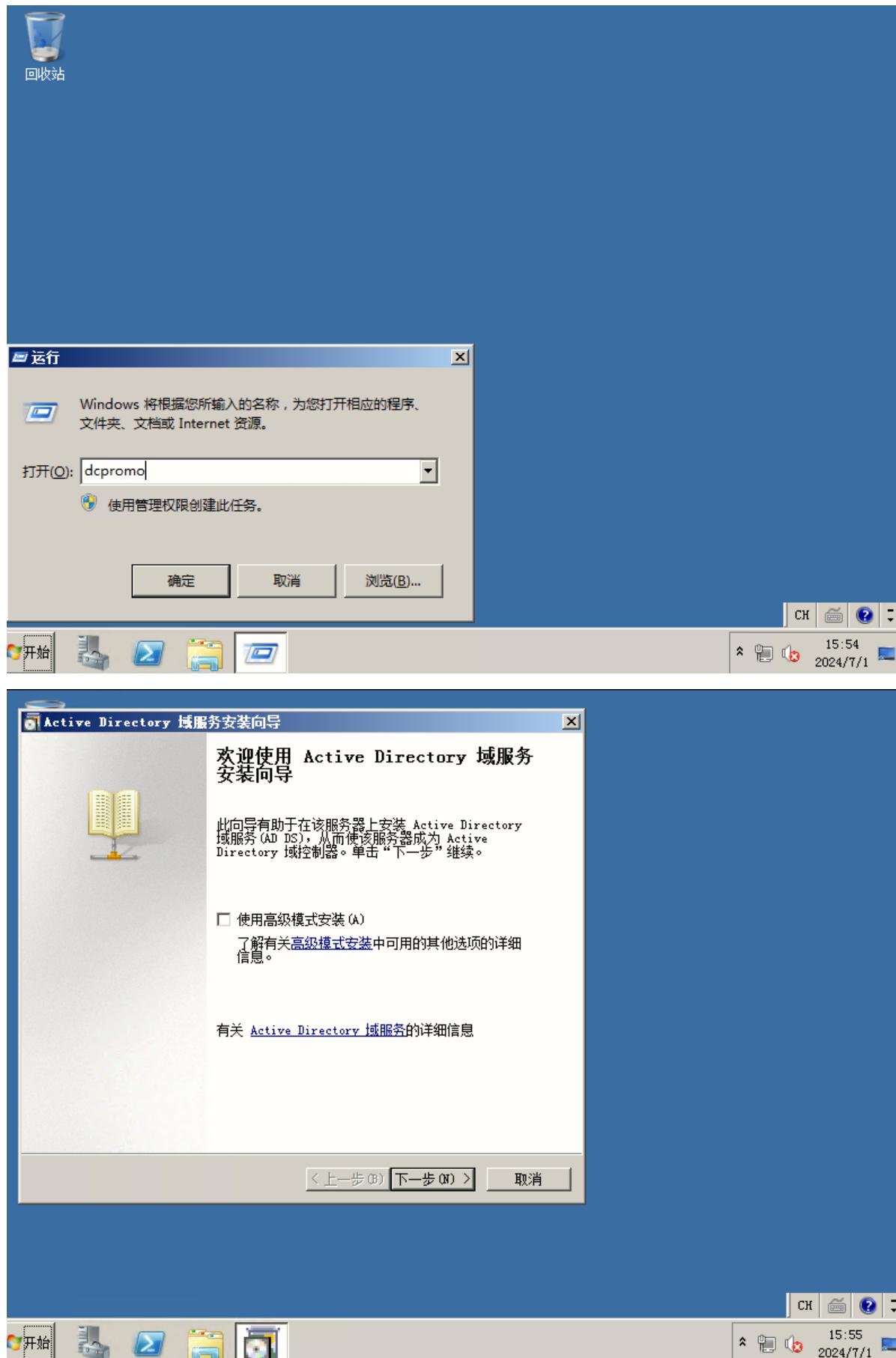
DNS 服务器 . . . . . : 172.168.2.61
TCPIP 上的 NetBIOS . . . . . : 已启用

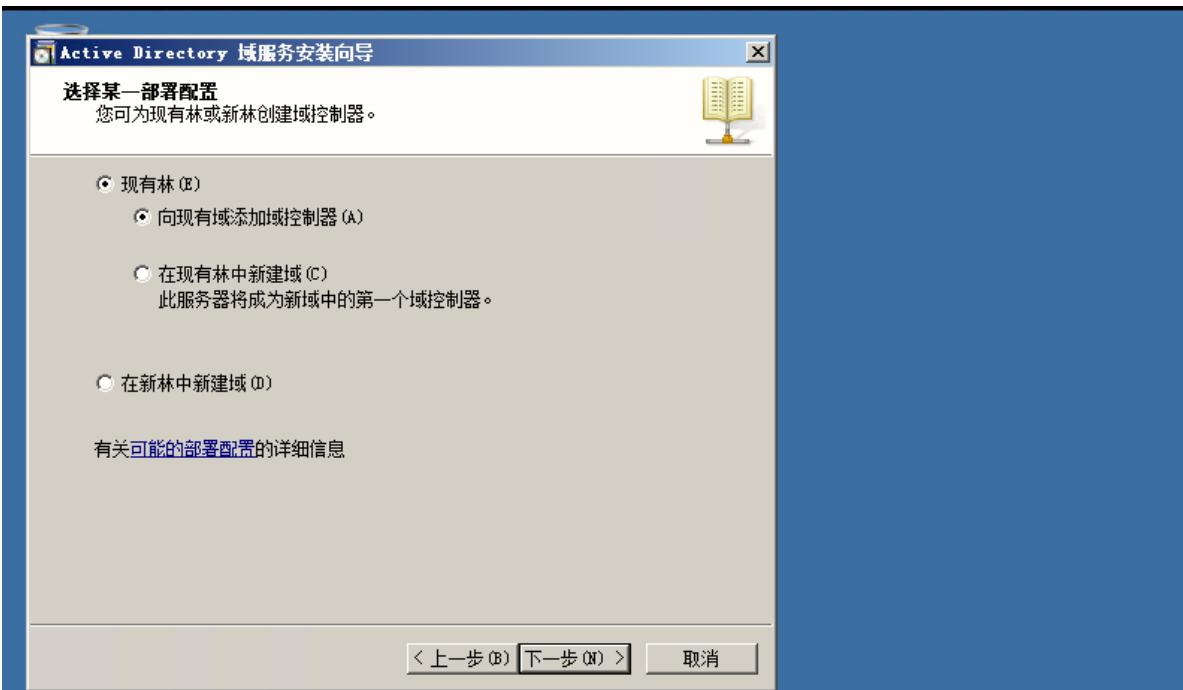
隧道适配器 isatap.{6D66A533-42BC-4BF5-8497-879821853EB8}:

媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
```



### 3.2 安装第二台域控，为BDC角色





The screenshot shows the 'Network Credentials' step of the Active Directory Domain Services Installation Wizard. It has two main sections:

- Network Credentials:** A note says: '指定将在其上执行安装的林的名称, 以及具有执行安装所需的足够权限的帐户凭据。' (Specify the name of the forest on which the installation will be performed, and the account credentials with sufficient permissions to perform the installation.) Below is a text input field containing 'test.com'.
- Windows Security:** A note says: '请指定用于执行安装的帐户凭据:' (Specify the account credentials to be used for performing the installation.) It shows a user selection dialog with 'administrator' in the username field and '\*\*\*\*\*' in the password field. The 'Domain' dropdown is set to 'test.com'. A red box highlights the 'administrator' field in the Windows Security dialog.

Below the network credentials section is a note: '键入位于计划安装此域控制器的林中任何域的名称 (T):' (Enter the name of any domain in the forest where the domain controller will be installed). A red box highlights the 'test.com' entry in the text input field.

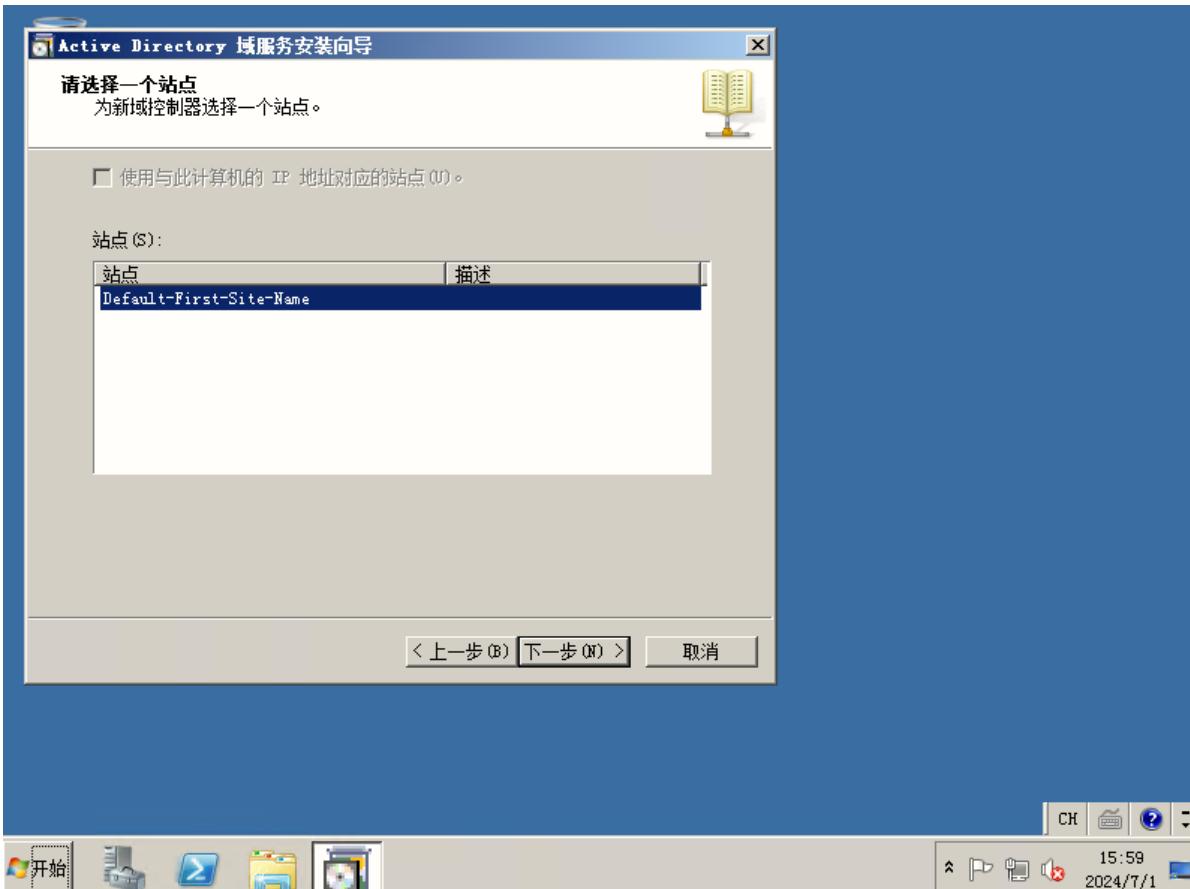
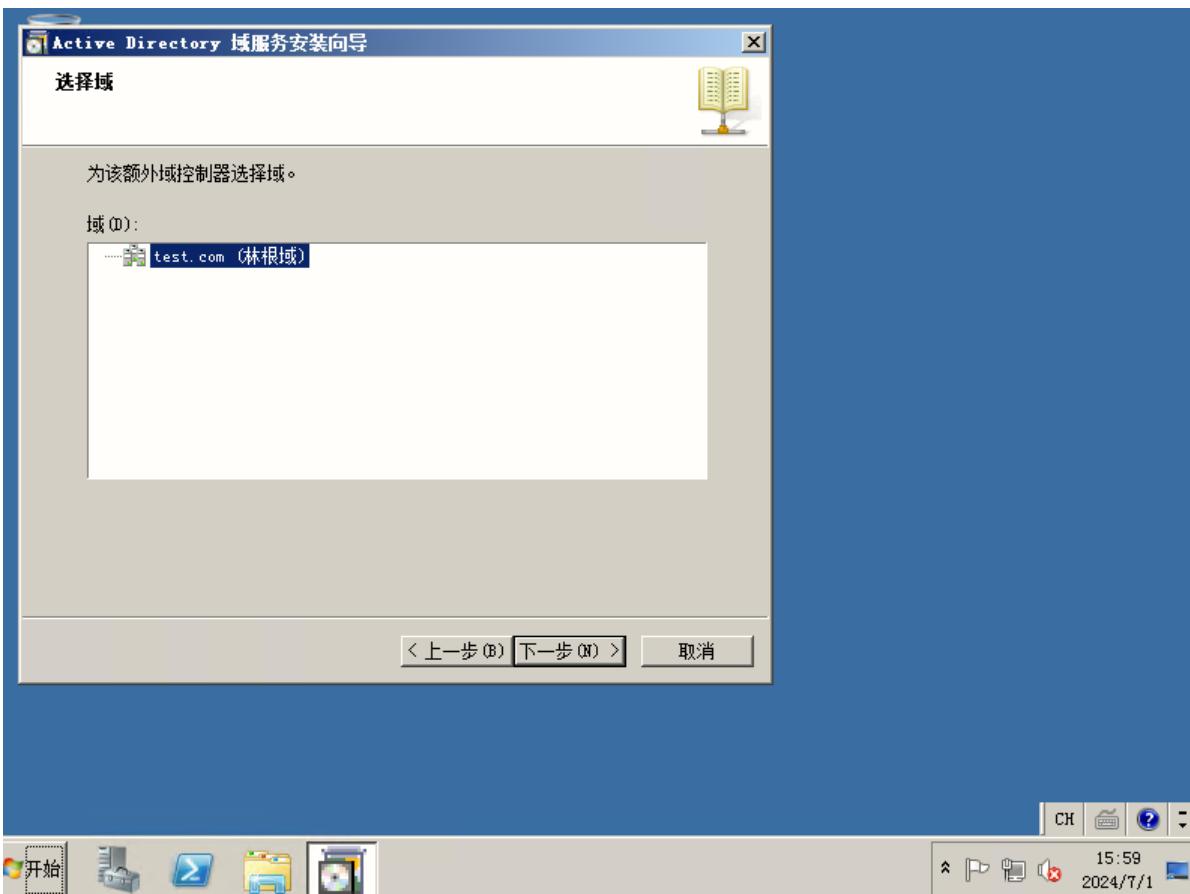
Under the Windows Security dialog, there is a note: '请指定用于执行安装的帐户凭据:' (Specify the account credentials to be used for performing the installation). It lists two options:

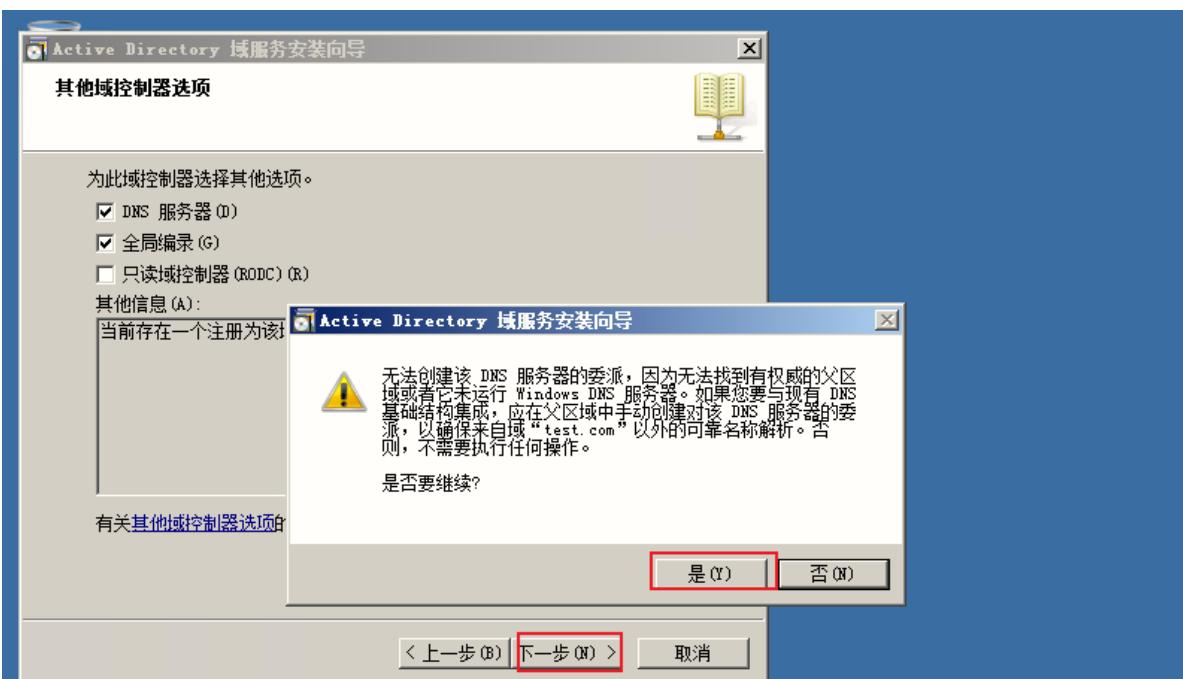
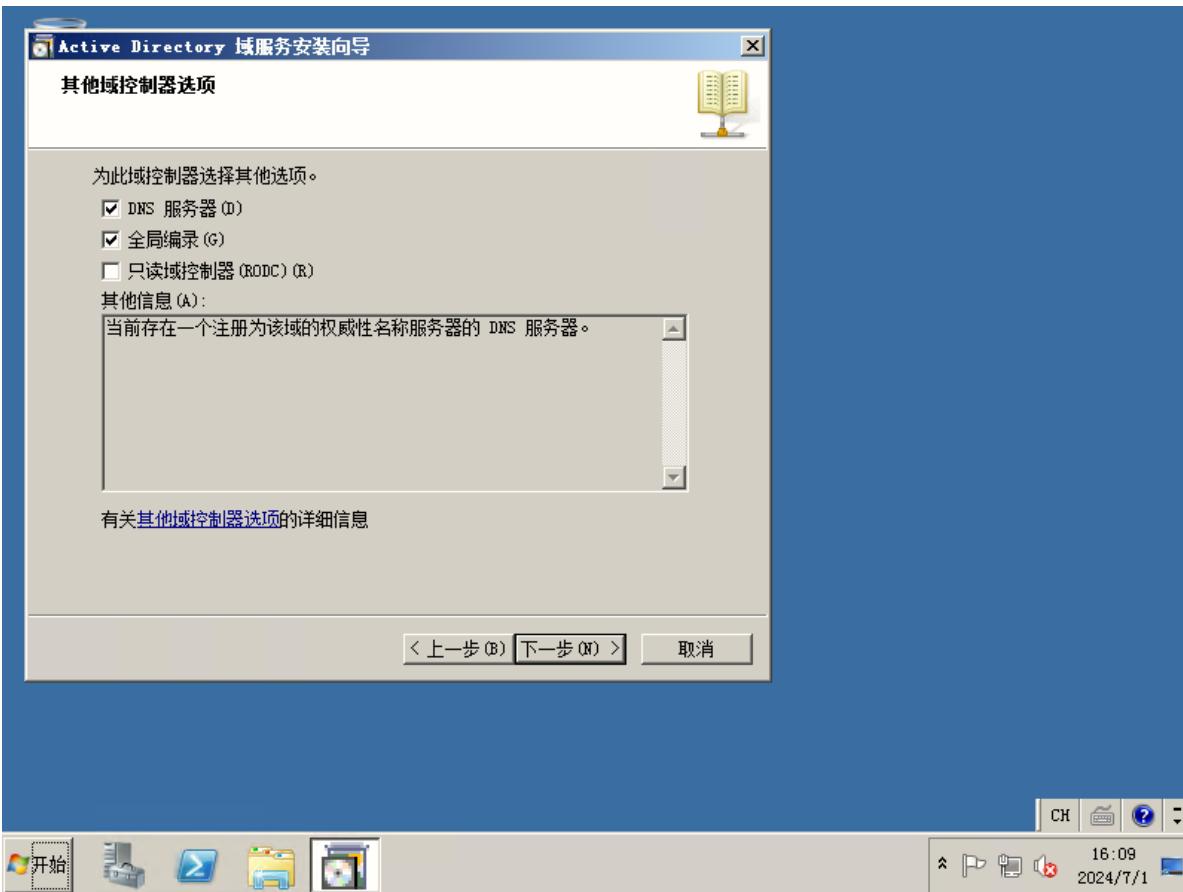
- 我的当前登录凭据 (BDC\Administrator) (C) (My current logon credentials (BDC\Administrator))
- 备用凭据 (A) (Backup credentials) (A)

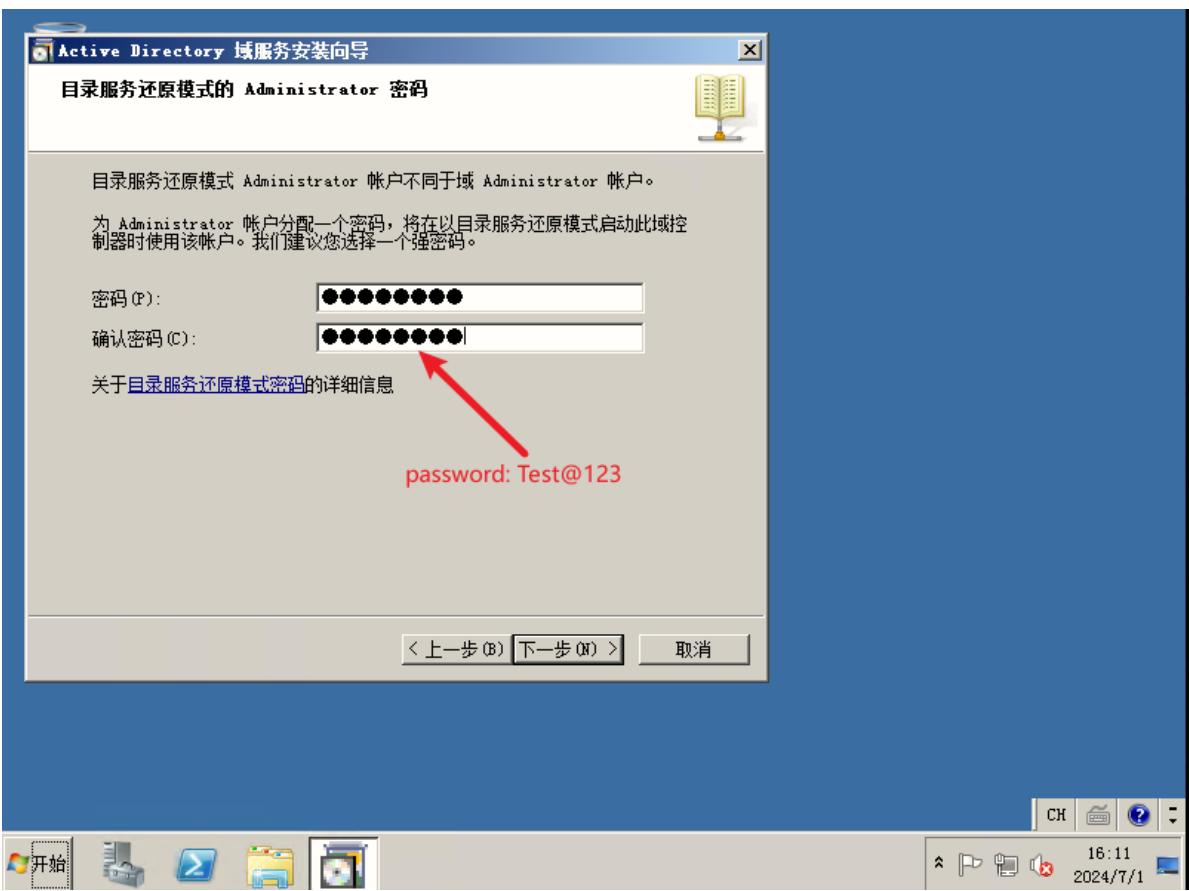
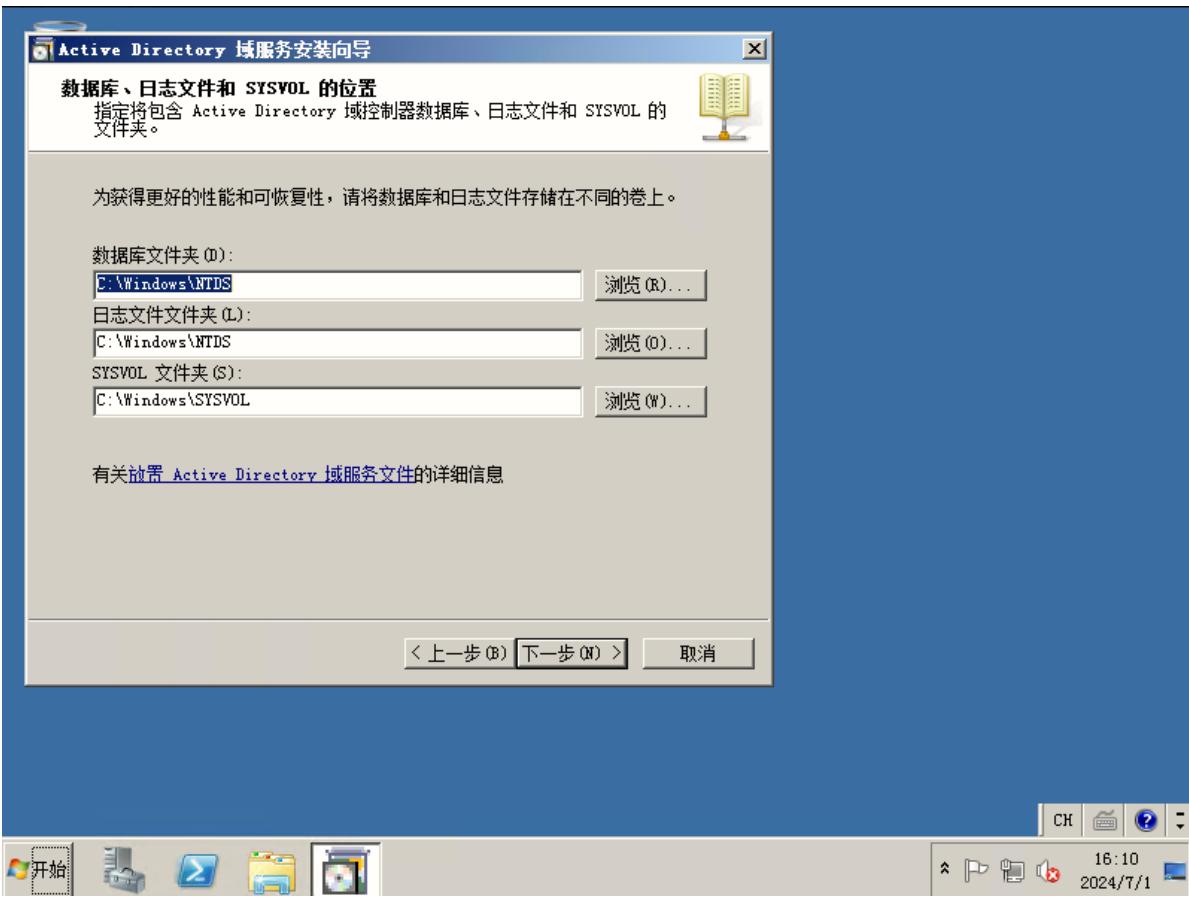
A warning message in a red box states: '因为当前用户凭据是该计算机的本地凭据, 所以无法选择。需要一组域凭据。' (Because the current user credentials are local to this computer, they cannot be selected. A group of domain credentials is required.)

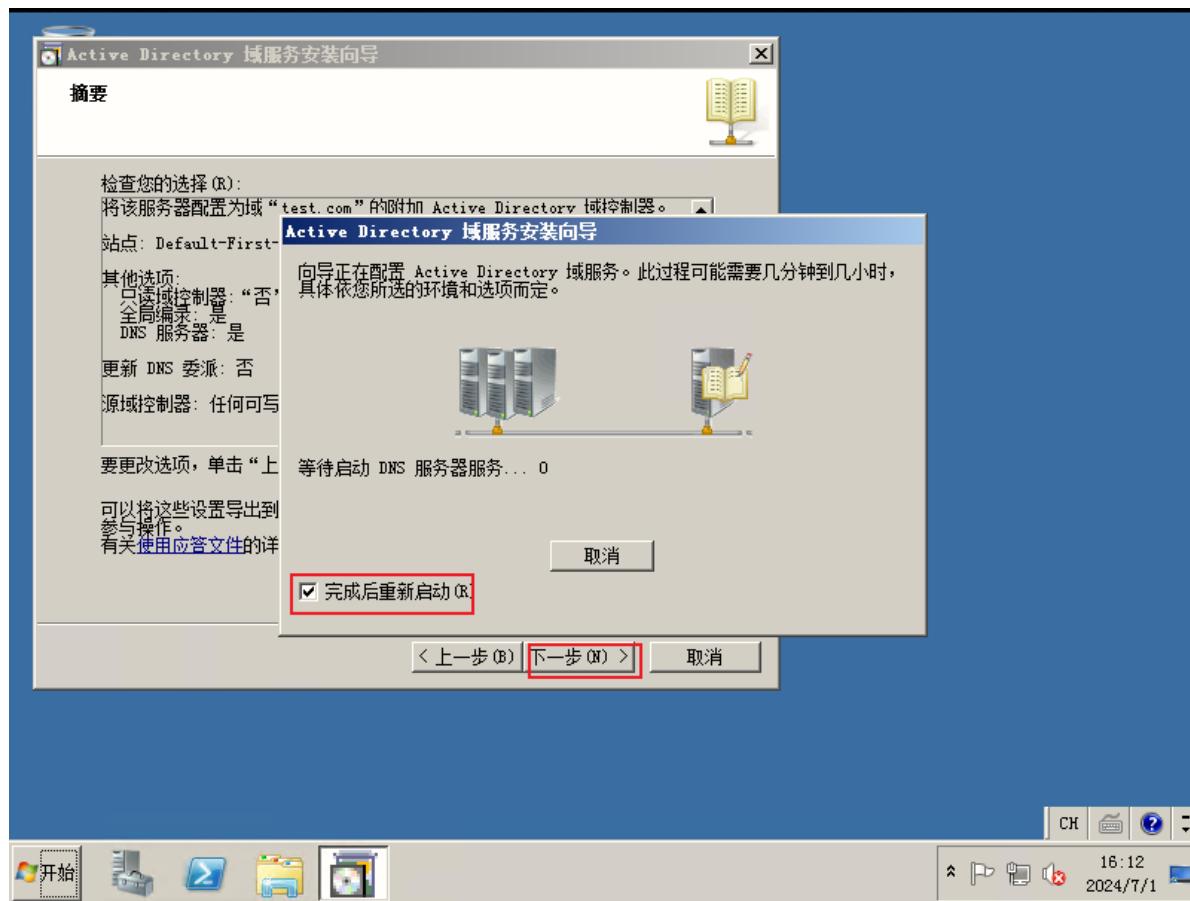
At the bottom are buttons: < 上一步 (B) (Previous Step), 下一步 (N) > (Next Step), and 取消 (Cancel).











### 3.3 登录并配置BDC

```
管理员: C:\Windows\system32\cmd.exe

C:\Users\Administrator>nlist /dclist:test.com
获得域“test.com”中 DC 的列表<从“\\bdc.test.com”中>。
  BDC.test.com [DS] 站点: Default-First-Site-Name
  pdc.test.com [PDC] [DS] 站点: Default-First-Site-Name
此命令成功完成

C:\Users\Administrator>whoami
test\administrator

C:\Users\Administrator>hostname
bdc

C:\Users\Administrator>ipconfig /all

Windows IP 配置

  主机名 . . . . . : bdc
  主 DNS 后缀 . . . . . : test.com
  节点类型 . . . . . : 混合
  IP 路由已启用 . . . . . : 否
  WINS 代理已启用 . . . . . : 否
  DNS 后缀搜索列表 . . . . . : test.com

以太网适配器 本地连接:

  连接特定的 DNS 后缀 . . . . . :
  描述 . . . . . : Intel(R) PRO/1000 MT Network Connection
  物理地址 . . . . . : 00-0C-29-84-D5-3A
  DHCP 已启用 . . . . . : 否
  自动配置已启用 . . . . . : 是
```

```
管理员: C:\Windows\system32\cmd.exe
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
DNS 后缀搜索列表 . . . . . : test.com

以太网适配器 本地连接:

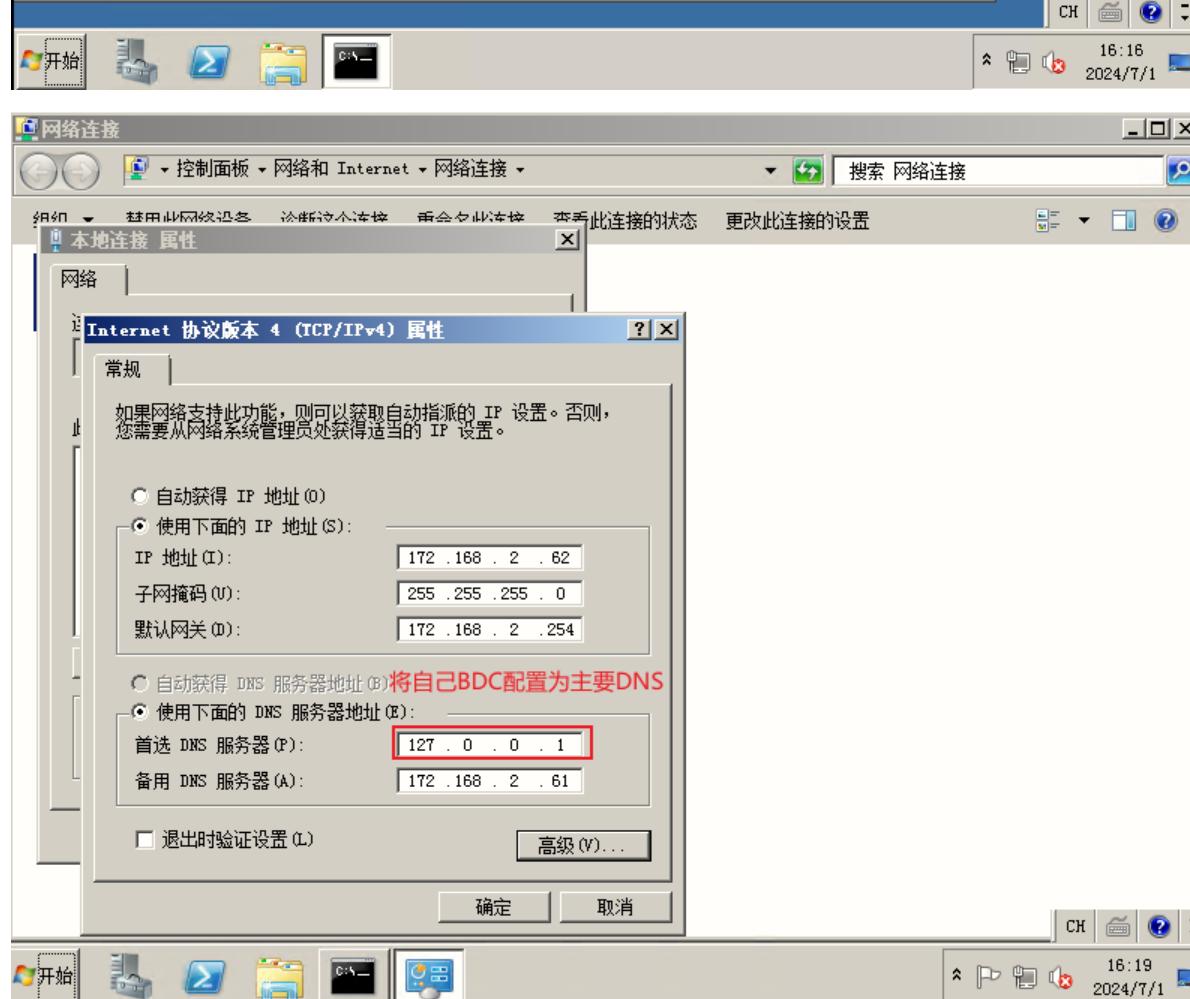
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Intel(R) PRO/1000 MT Network Connection
物理地址 . . . . . : 00-0C-29-84-D5-3A
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是
本地链接 IPv6 地址 . . . . . : fe80::3815:b965:72a7:7d25%11<首选>
IPv4 地址 . . . . . : 172.168.2.62<首选>
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 172.168.2.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2E-13-D8-23-00-0C-29-1B-2B-64

DNS 服务器 . . . . . : ::1
172.168.2.61
127.0.0.1

TCPIP 上的 NetBIOS . . . . . : 已启用

隧道适配器 isatap.{6D66A533-42BC-4BF5-8497-879821853EB8}:

媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Microsoft ISATAP Adapter
物理地址 . . . . . : 00-00-00-00-00-00-00-E0
DHCP 已启用 . . . . . : 否
自动配置已启用 . . . . . : 是
```



```

管理员: C:\Windows\system32\cmd.exe
主机名 . . . . . : bdc
主 DNS 后缀 . . . . . : test.com
节点类型 . . . . . : 混合
IP 路由已启用 . . . . . : 否
WINS 代理已启用 . . . . . : 否
DNS 后缀搜索列表 . . . . . : test.com

以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . : Intel(R) PRO/1000 MT Network Connection
描述 . . . . . : Intel(R) PRO/1000 MT Network Connection
物理地址 . . . . . : 00-0C-29-84-D5-3A
DHCP 已启用 . . . . . : 否
自动配置已启用 . . . . . : 是
本地链接 IPv6 地址 . . . . . : fe80::3815:b965:72a7:7d25%11<首选>
IPv4 地址 . . . . . : 172.168.2.62<首选>
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 172.168.2.254
DHCPv6 IAID . . . . . : 234884137
DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2E-13-D8-23-00-0C-29-1B-2B-64

DNS 服务器 . . . . . : ::1
127.0.0.1
172.168.2.61
TCPIP 上的 NetBIOS . . . . . : 已启用

隧道适配器 isatap.{6D66A533-42BC-4BF5-8497-879821853EB8}:
媒体状态 . . . . . : 媒体已断开
连接特定的 DNS 后缀 . . . . . :
描述 . . . . . : Microsoft ISATAP Adapter
物理地址 . . . . . : 00-00-00-00-00-00-E0

```

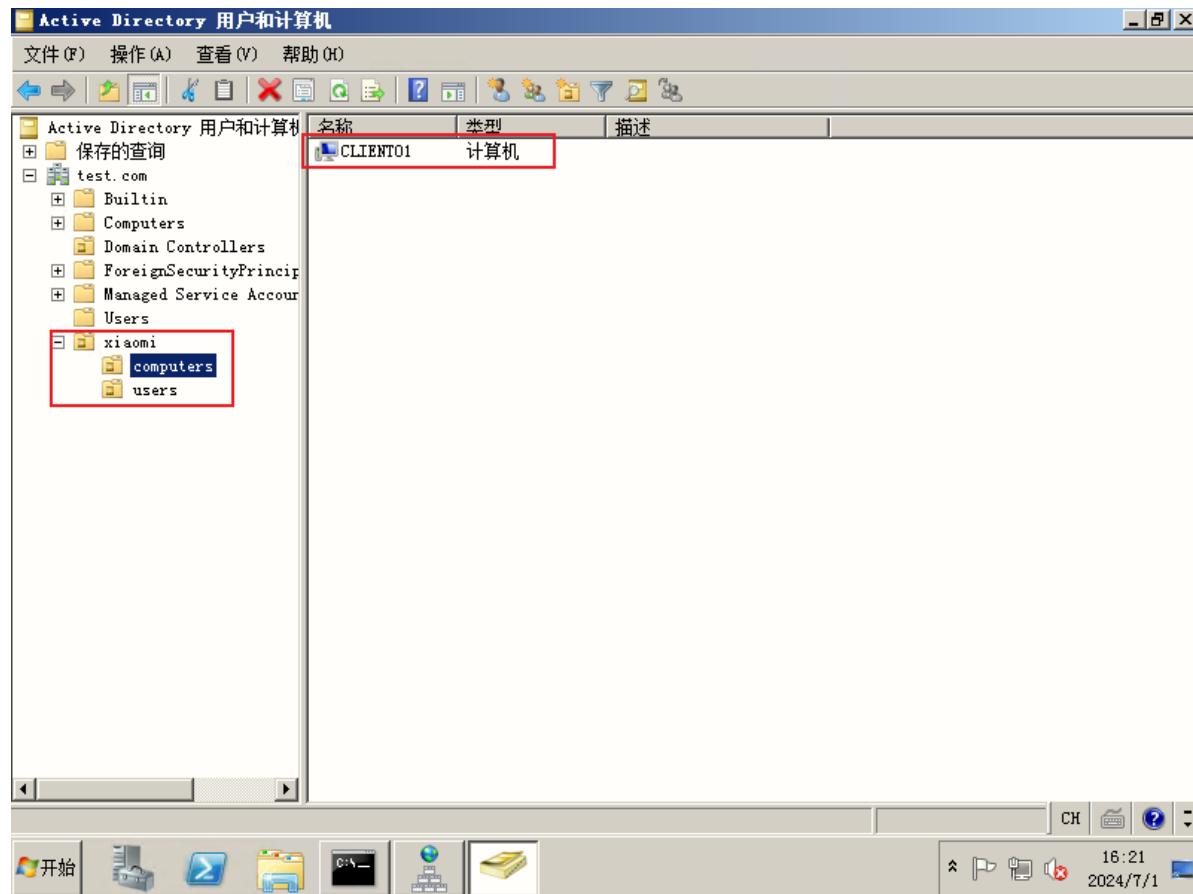
### 3.4 查看BDC跟PDC同步的状态

#### DNS

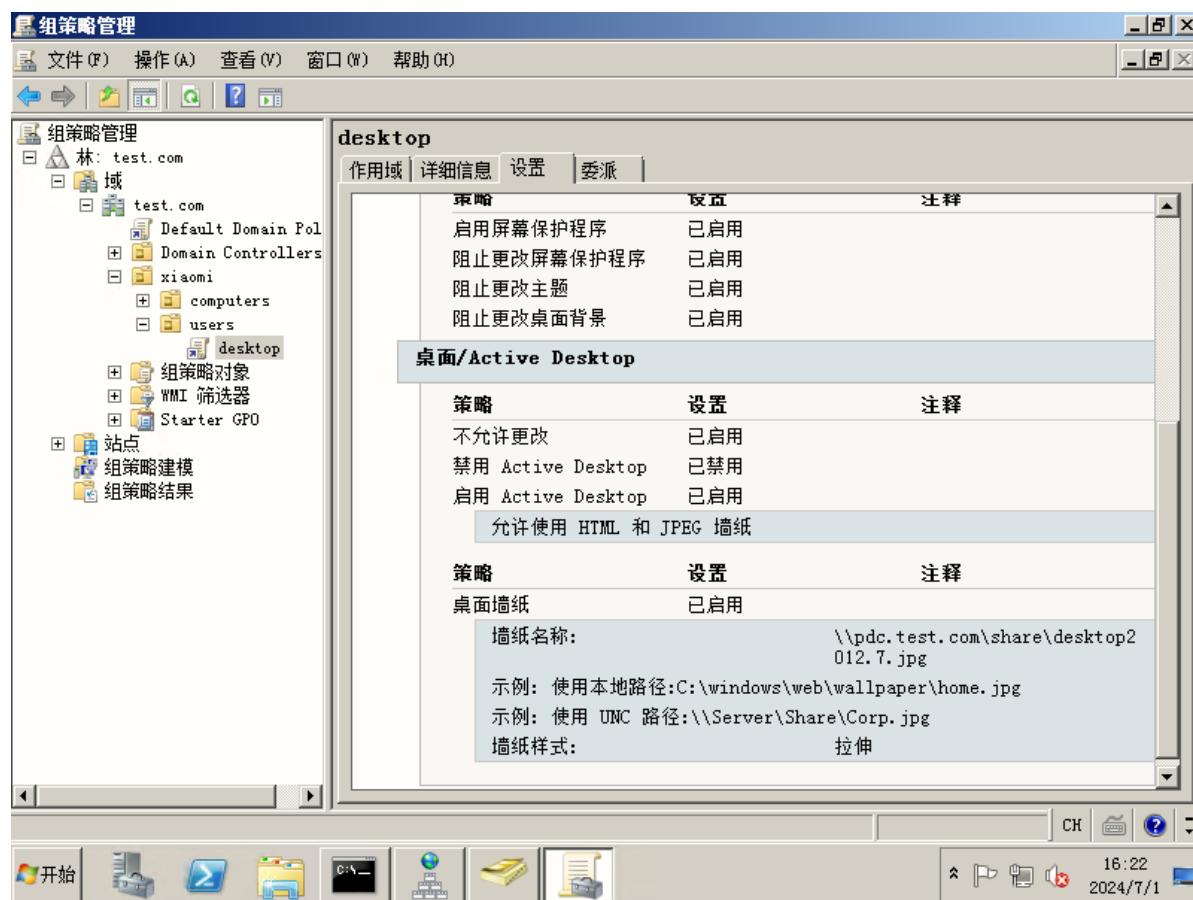
**DNS 管理器**

名称	类型	数据	时间戳
_msdc	起始授权机构 (SOA)	[52], bdc.test.com, ...	静态
_sites	名称服务器 (NS)	bdc.test.com.	静态
_tcp	名称服务器 (NS)	pdc.test.com.	静态
_udp	主机 (A)	172.168.2.62	2024/7/1 16:00:00
DomainDnsZones	主机 (A)	172.168.2.61	2024/7/1 14:00:00
ForestDnsZones	IPv6 主机 (AAAA)	2002:ac8:023e:0000:0... 2002:ac8:023d:0000:0...	2024/7/1 16:00:00 2024/7/1 14:00:00
(与父文件夹相同)	IPv6 主机 (AAAA)	2002:ac8:023e:0000:0... 2002:ac8:023d:0000:0...	2024/7/1 14:00:00 2024/7/1 14:00:00
(与父文件夹相同)	主机 (A)	172.168.2.62	2024/7/1 16:00:00
(与父文件夹相同)	主机 (A)	172.168.2.61	2024/7/1 14:00:00
(与父文件夹相同)	IPv6 主机 (AAAA)	2002:ac8:023e:0000:0... 2002:ac8:023d:0000:0...	2024/7/1 16:00:00 2024/7/1 14:00:00
bdc	主机 (A)	172.168.2.62	静态
bdc	IPv6 主机 (AAAA)	2002:ac8:023e:0000:0... 2002:ac8:023d:0000:0...	2024/7/1 14:00:00 静态
client01	主机 (A)	172.168.2.65	2024/7/1 14:00:00
pdc	主机 (A)	172.168.2.61	静态

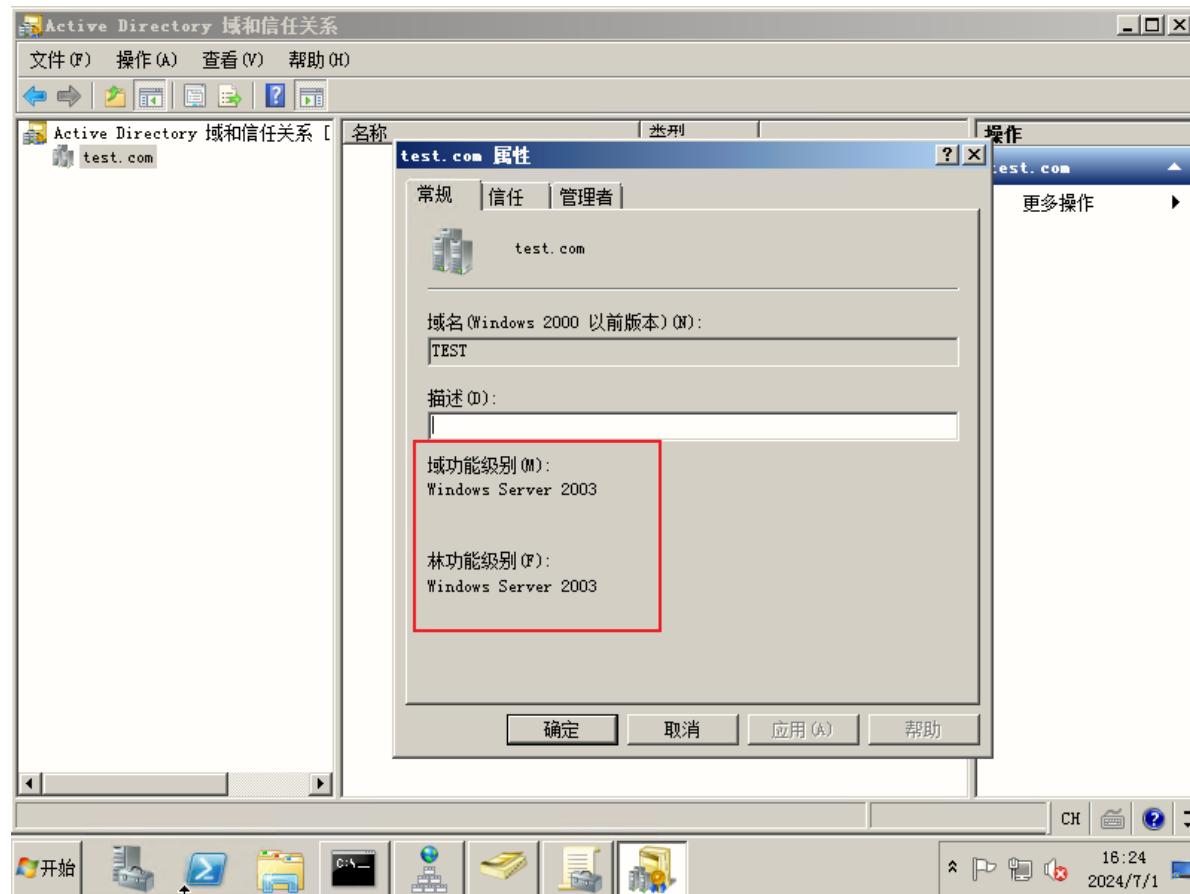
## 域对象



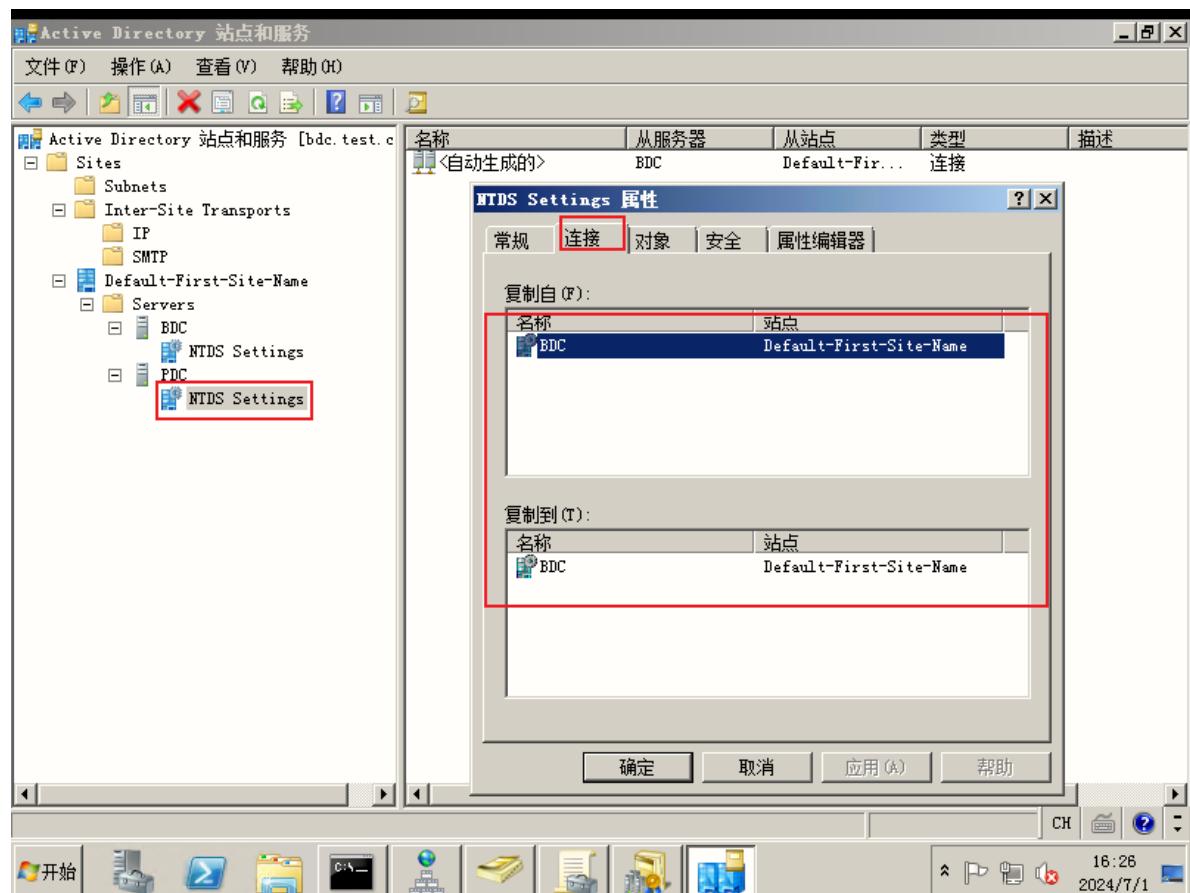
## 组策略

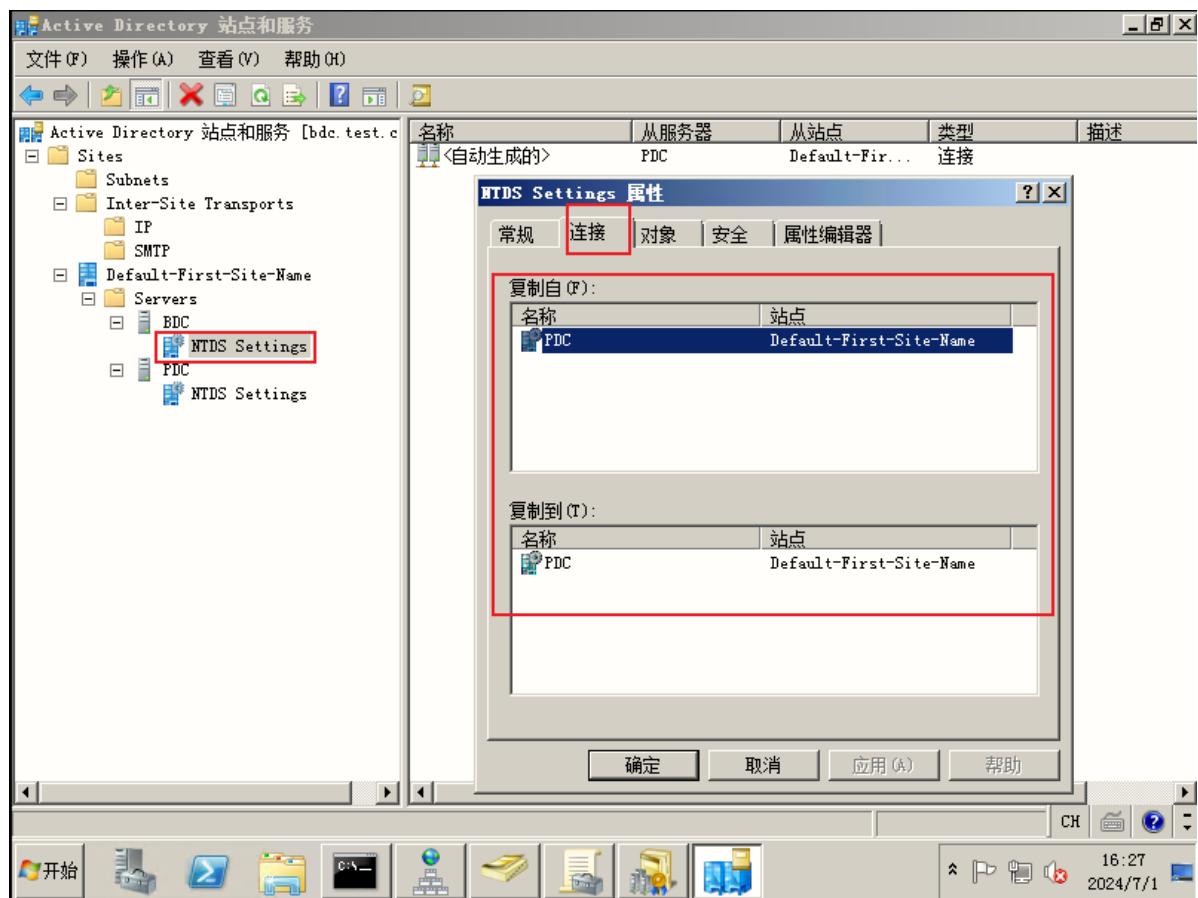


## 域和信任关系



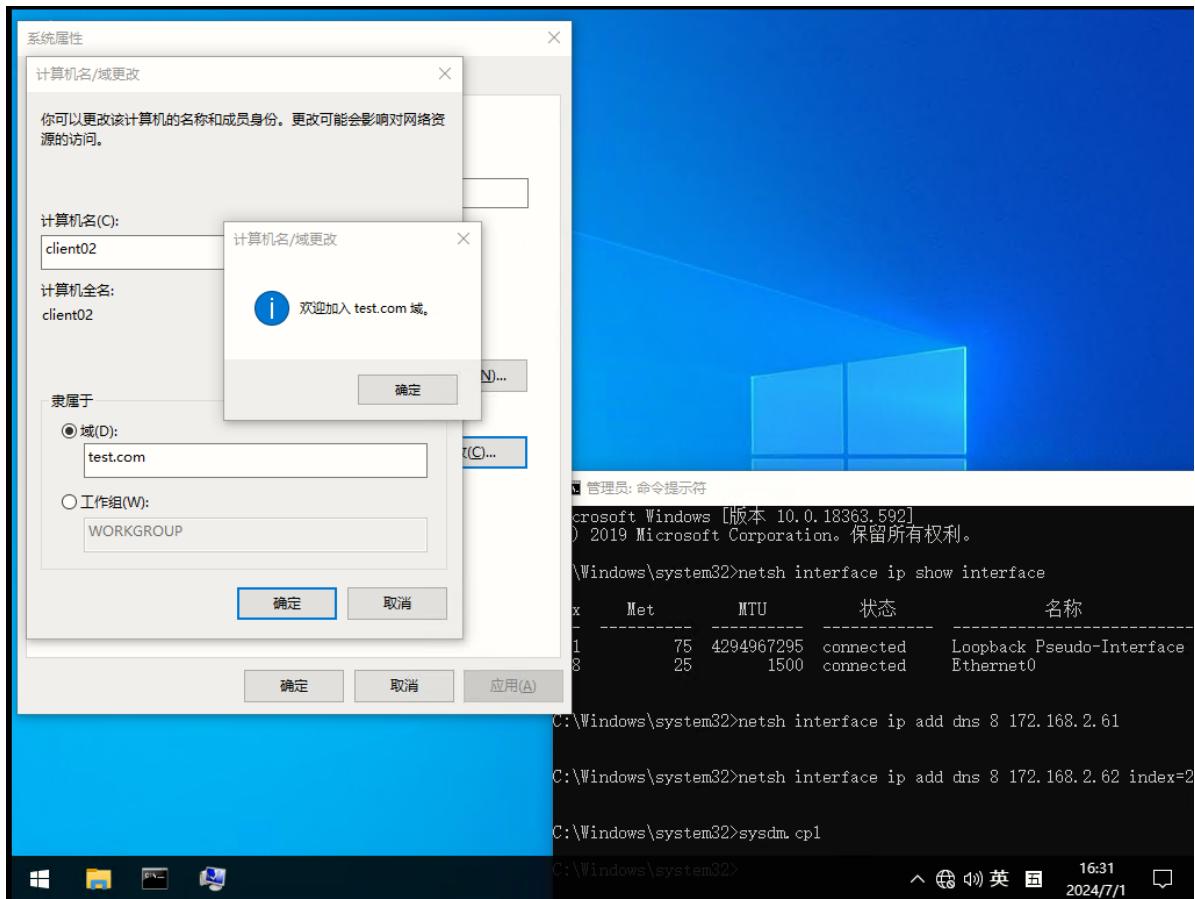
## 站点和服务





## 4. 客户端02

### 4.1 配置网络并加域



## 4.2 在BDC上创建普通域用户

Active Directory 用户和计算机

文件(F) 操作(O) 查看(V) 帮助(H)

名称 类型 描述

测试用户01 用户

测试用户02 用户

保存的查询

test.com

Builtin

Computers

Domain Controllers

ForeignSecurityPrincipals

Managed Service Accounts

Users

xiaomi

computers

users

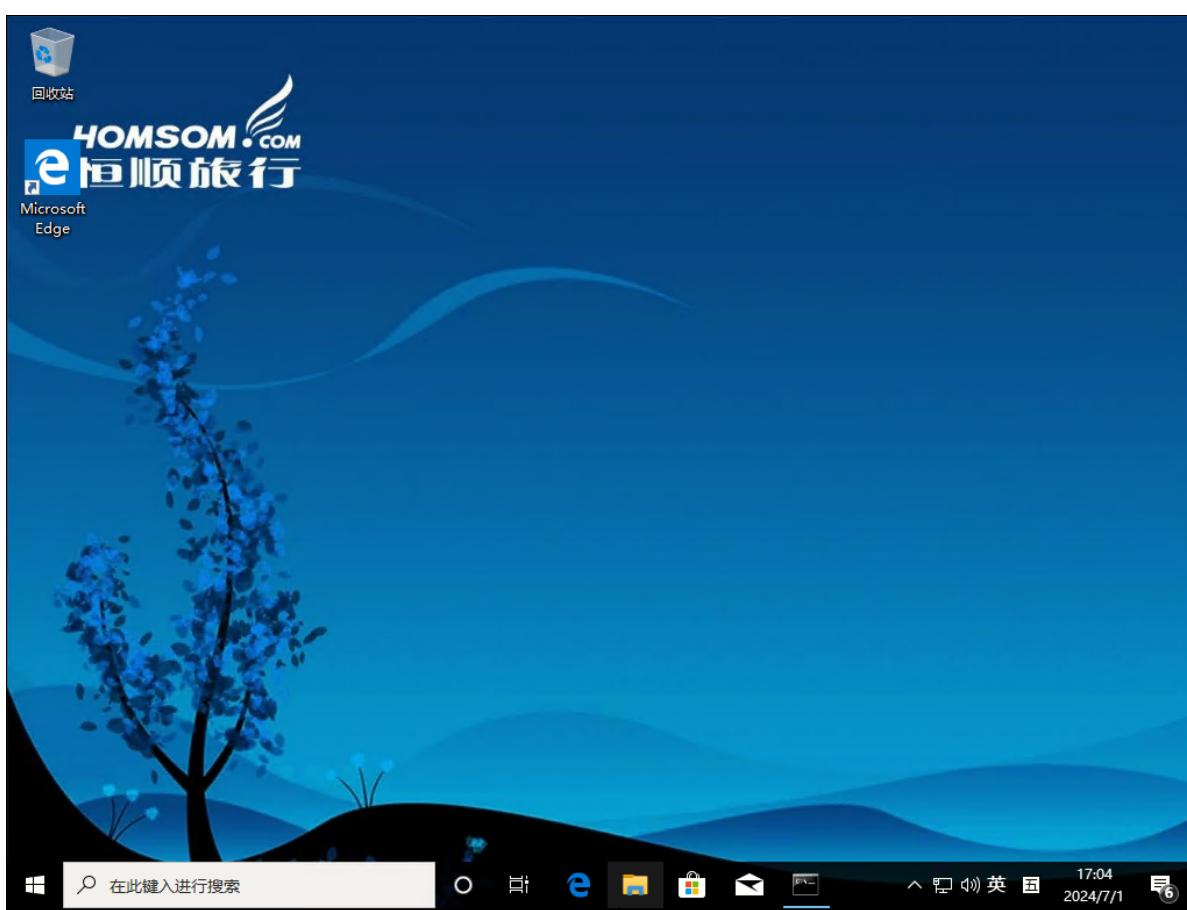
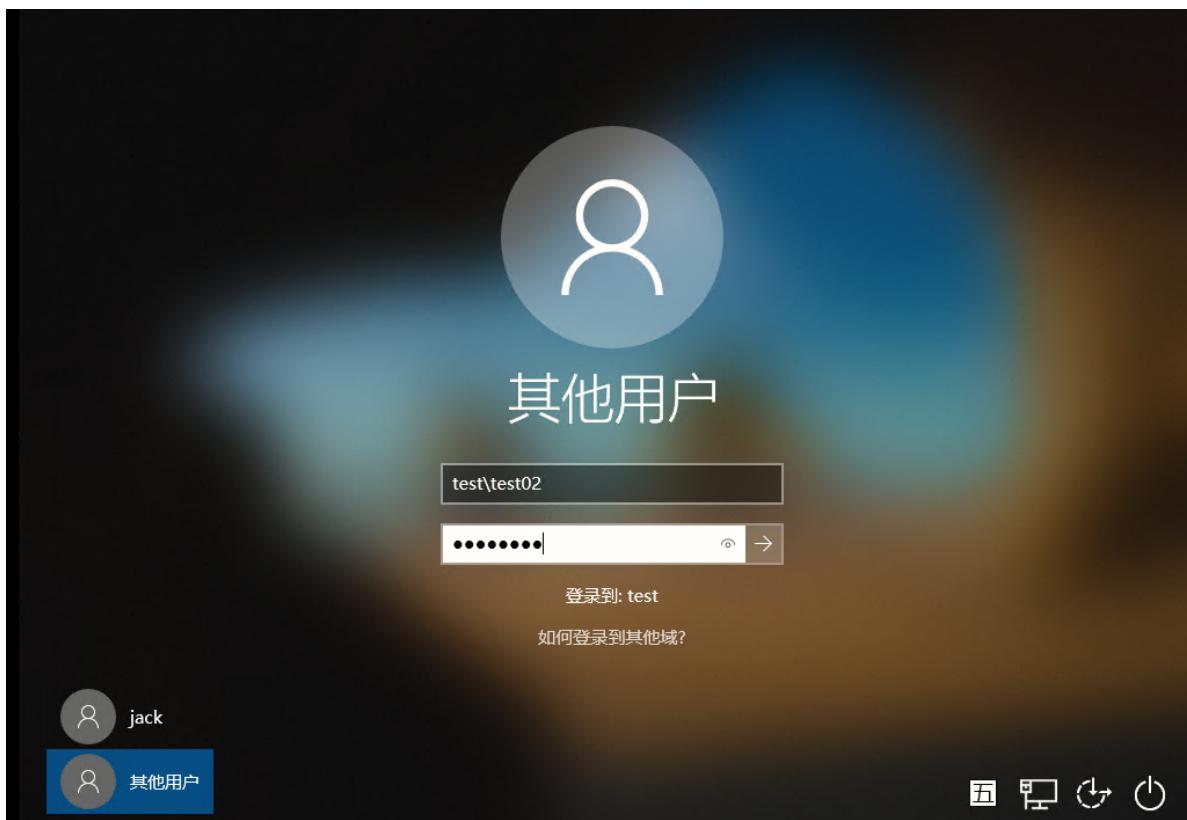
测试用户02并将"client02"计算机加入到computers OU中

CH MS 中 ?

开始

16:32 2024/7/1

## 4.3 登录域用户并测试dns



```
C:\Windows\system32\cmd.exe
Microsoft Windows [版本 10.0.18363.592]
(c) 2019 Microsoft Corporation。保留所有权利。

C:\Users\test02>n1test /dcList:test.com
获得域“test.com”中 DC 的列表(从“\\pdc.test.com”中)。
pdc.test.com [PDC] [DS] 站点: Default-First-Site-Name
      BDC.test.com [DS] 站点: Default-First-Site-Name
此命令成功完成

C:\Users\test02>hostname
client02

C:\Users\test02>whoami
test\test02

C:\Users\test02>ipconfig /all

Windows IP 配置

    主机名 . . . . . : client02
    主 DNS 后缀 . . . . . : test.com
    节点类型 . . . . . : 混合
    IP 路由已启用 . . . . . : 否
    WINS 代理已启用 . . . . . : 否
    DNS 后缀搜索列表 . . . . . : test.com

以太网适配器 Ethernet0:

    连接特定的 DNS 后缀 . . . . . :
        描述 . . . . . : Intel(R) 82574L Gigabit Network Connection
        物理地址 . . . . . : 00-0C-29-19-11-B5
        DHCP 已启用 . . . . . : 否
        自动配置已启用 . . . . . : 是
        本地链接 IPv6 地址 . . . . . : fe80::64ce:ba70:7c05:3c4c%8(首选)
        IPv4 地址 . . . . . : 172.168.2.66(首选)
        子网掩码 . . . . . : 255.255.255.0
        默认网关 . . . . . : 172.168.2.254
        DHCPv6 IAID . . . . . : 100666409
        DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2E-13-DC-95-00-0C-29-19-11-B5
        DNS 服务器 . . . . . : 172.168.2.61
                                         172.168.2.62
        TCPIP 上的 NetBIOS . . . . . : 已启用

C:\Users\test02>
```

## 5. 模拟PDC故障，BDC升级为PDC-灾难恢复-方式一

### 5.1 模拟PDC故障

将PDC关机



BDC已经无法ping通PDC了，表示PDC已经关机了

```
Administrator: C:\Windows\system32\cmd.exe
连接特定的 DNS 后缀 . . . . . : Microsoft 6to4 Adapter
描述 . . . . . : 00-00-00-00-00-00-E0
物理地址 . . . . . : 不
DHCP 已启用 . . . . . : 是
自动配置已启用 . . . . . : 是
IPv6 地址 . . . . . : 2002:aca8:23e::aca8:23e<首选>
默认网关 . . . . . : 2002:c058:6301::c058:6301
DNS 服务器 . . . . . : ::1
127.0.0.1
172.168.2.61
TCPIP 上的 NetBIOS . . . . . : 已禁用

C:\Users\Administrator>
C:\Users\Administrator>firewall.cpl
C:\Users\Administrator>hostname
bdc
C:\Users\Administrator>ping 172.168.2.61

正在 Ping 172.168.2.61 具有 32 字节的数据:
来自 172.168.2.62 的回复: 无法访问目标主机。
来自 172.168.2.62 的回复: 无法访问目标主机。
来自 172.168.2.62 的回复: 无法访问目标主机。
来自 172.168.2.62 的回复: 无法访问目标主机。

172.168.2.61 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 <0% 丢失>,
```

右侧任务栏显示了时间轴（Timeline）窗口，展示了从2024年7月1日14:00:00到16:00:00的静态事件。

系统托盘显示时间为17:32，日期为2024年7月1日。

## 5.2 BDC升级为PDC

```
管理员: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 © 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>netdom query fsmo
架构主机          pdc.test.com
域命名主机        pdc.test.com
PDC               pdc.test.com
RID 池管理器      pdc.test.com
结构主机          pdc.test.com
命令成功完成。

C:\Users\Administrator>nltest /dclist:test.com
获得域“test.com”中 DC 的列表(从“\\bdc.test.com”中)。
  BDC.test.com [DS] 站点: Default-First-Site-Name
  pdc.test.com [PDC] [DS] 站点: Default-First-Site-Name
此命令成功完成

C:\Users\Administrator>hostname
bdc

C:\Users\Administrator>ipconfig /all

Windows IP 配置

  主机名 . . . . . : bdc
  主 DNS 后缀 . . . . . : test.com
  节点类型 . . . . . : 混合
  IP 路由已启用 . . . . . : 否
  WINS 代理已启用 . . . . . : 否
  DNS 后缀搜索列表 . . . . . : test.com
```

```
管理员: C:\Windows\system32\cmd.exe
  主机名 . . . . . : bdc
  主 DNS 后缀 . . . . . : test.com
  节点类型 . . . . . : 混合
  IP 路由已启用 . . . . . : 否
  WINS 代理已启用 . . . . . : 否
  DNS 后缀搜索列表 . . . . . : test.com

以太网适配器 本地连接:

  连接特定的 DNS 后缀 . . . . . :
  描述 . . . . . : Intel(R) PRO/1000 MT Network Connection
  物理地址 . . . . . : 00-0C-29-84-D5-3A
  DHCP 已启用 . . . . . : 否
  自动配置已启用 . . . . . : 是
  本地链接 IPv6 地址 . . . . . : fe80::3815:b965:72a7:7d25%11<首选>
  IPv4 地址 . . . . . : 172.168.2.62<首选>
  子网掩码 . . . . . : 255.255.255.0
  默认网关 . . . . . : 172.168.2.254
  DHCPv6 IAID . . . . . : 234884137
  DHCPv6 客户端 DUID . . . . . : 00-01-00-01-2E-13-D8-23-00-0C-29-1B-2B-64

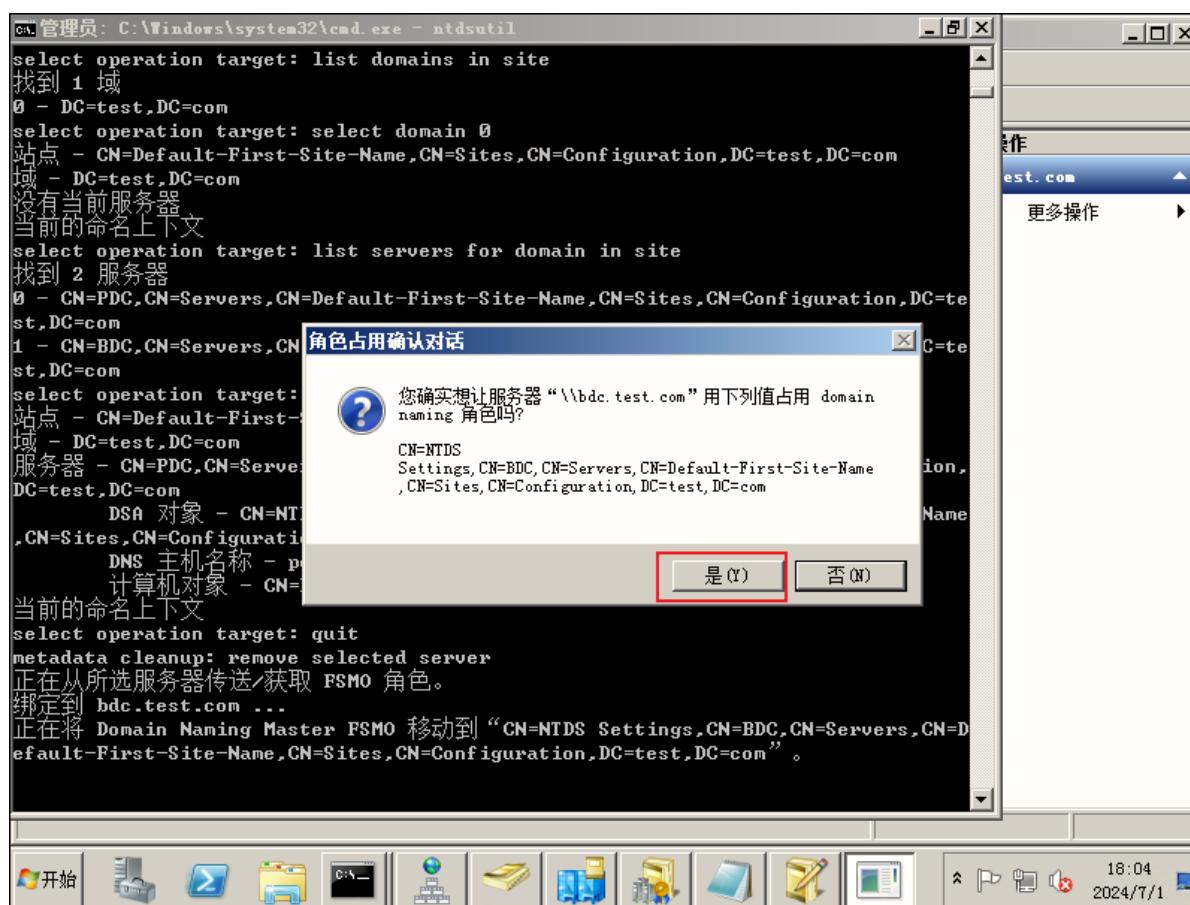
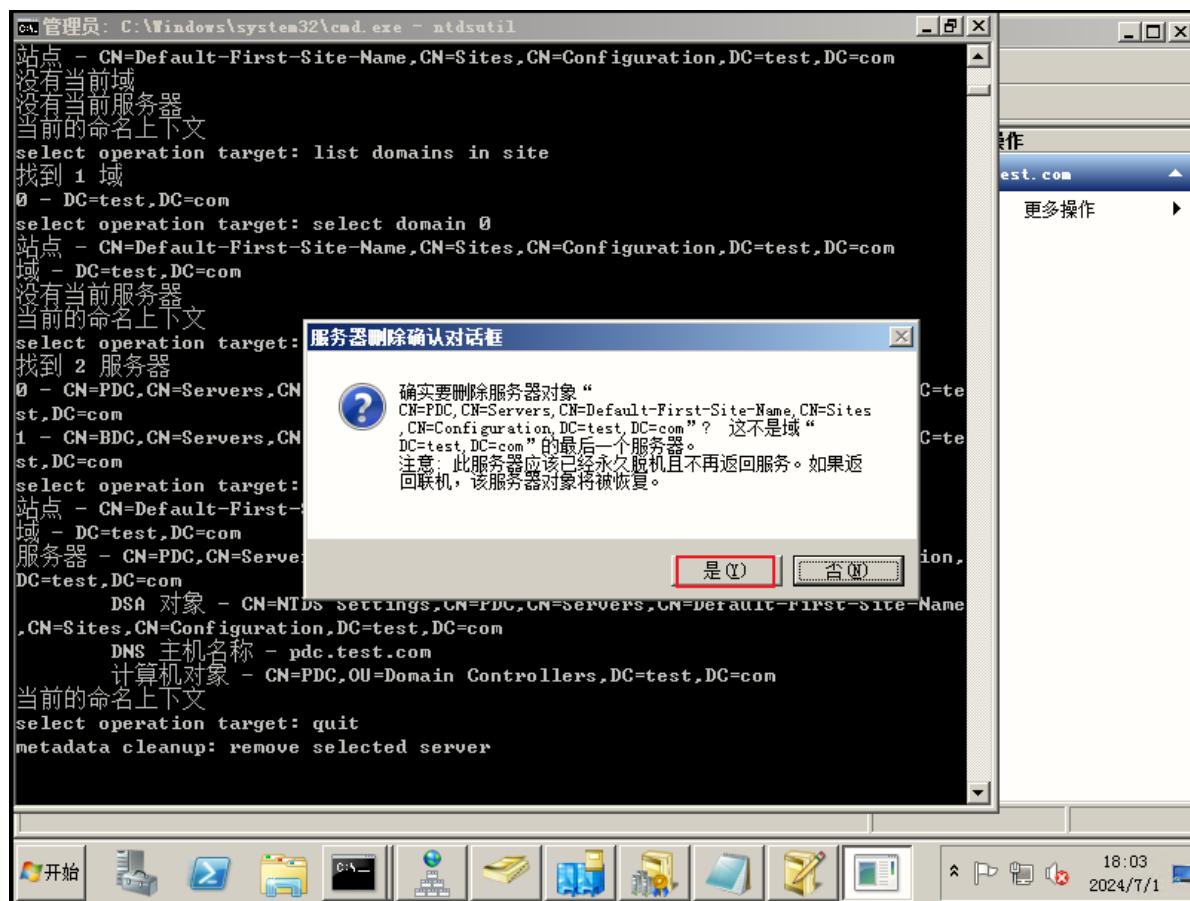
  DNS 服务器 . . . . . : ::1
                           127.0.0.1
                           172.168.2.61
  TCPIP 上的 NetBIOS . . . . . : 已启用

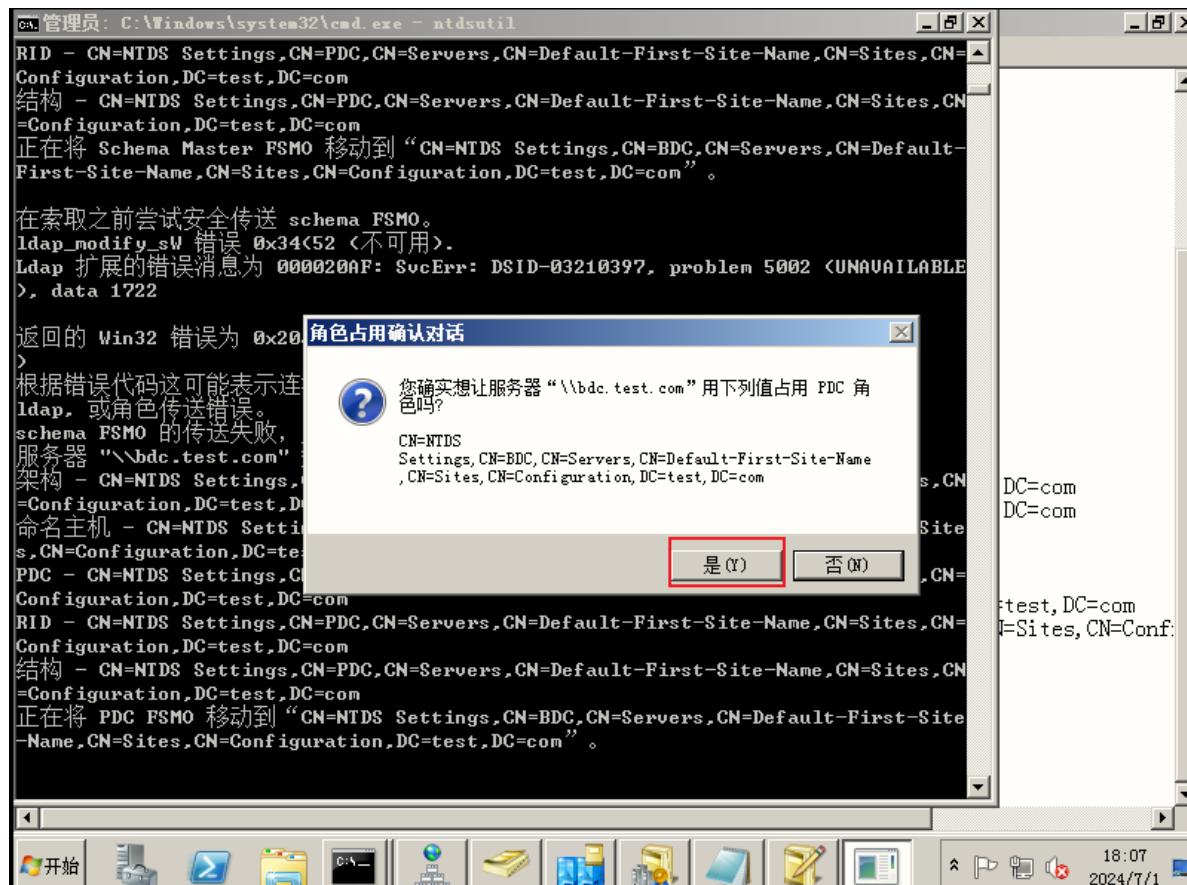
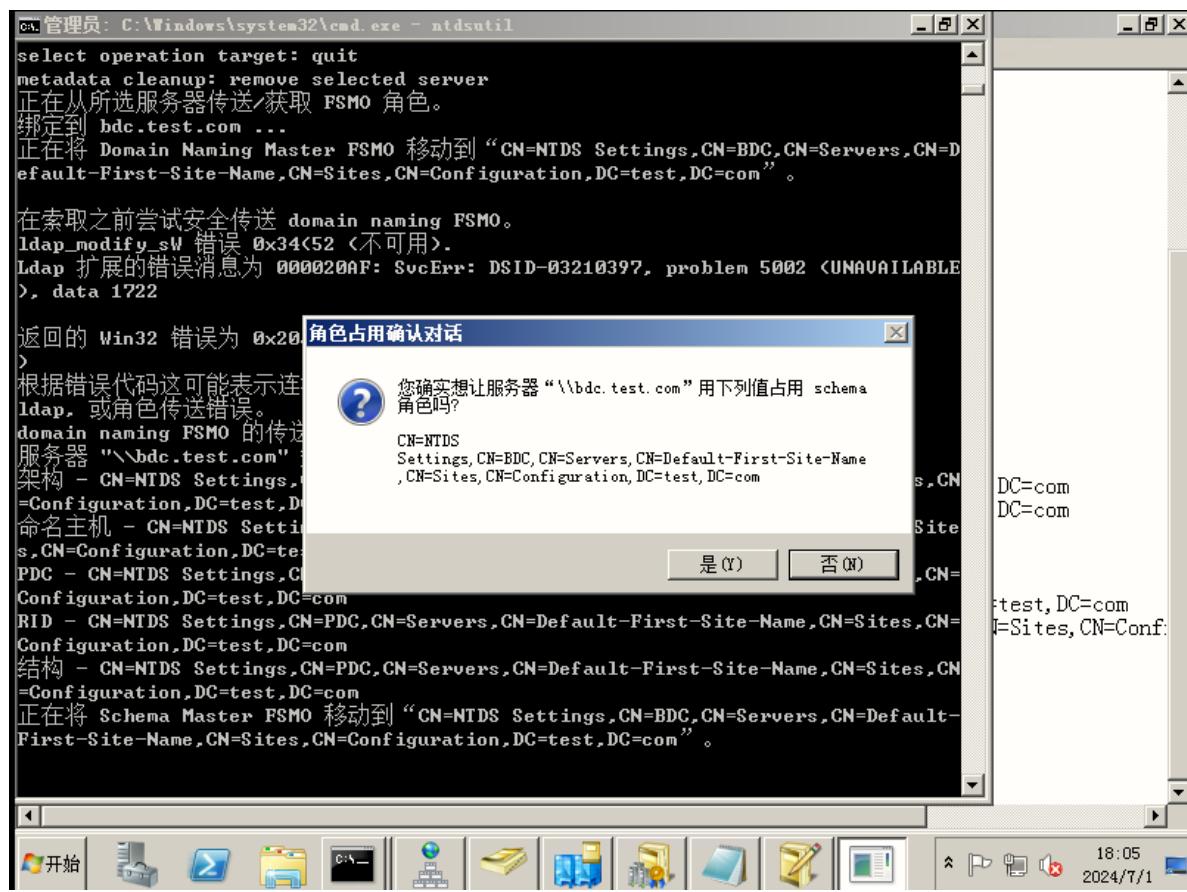
隧道适配器 isatap.{6D66A533-42BC-4BF5-8497-879821853EB8}:

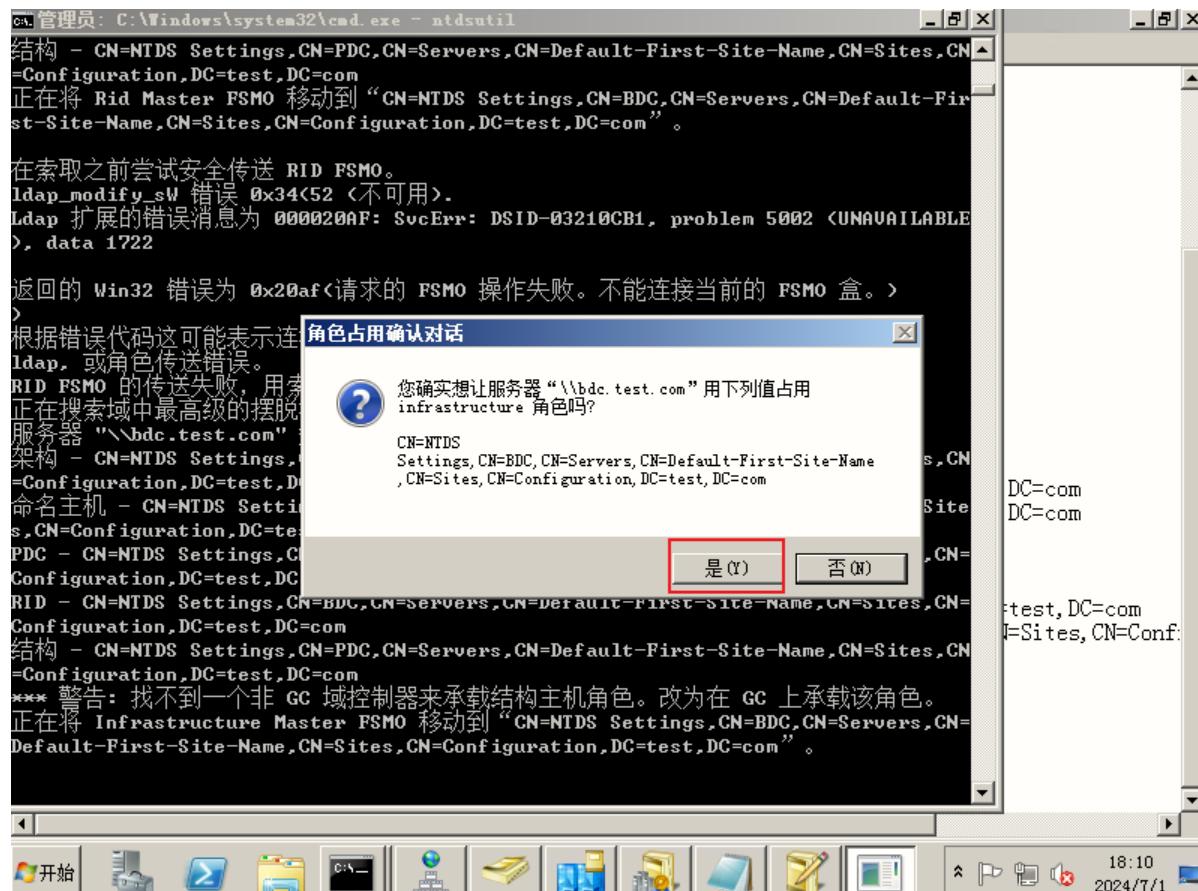
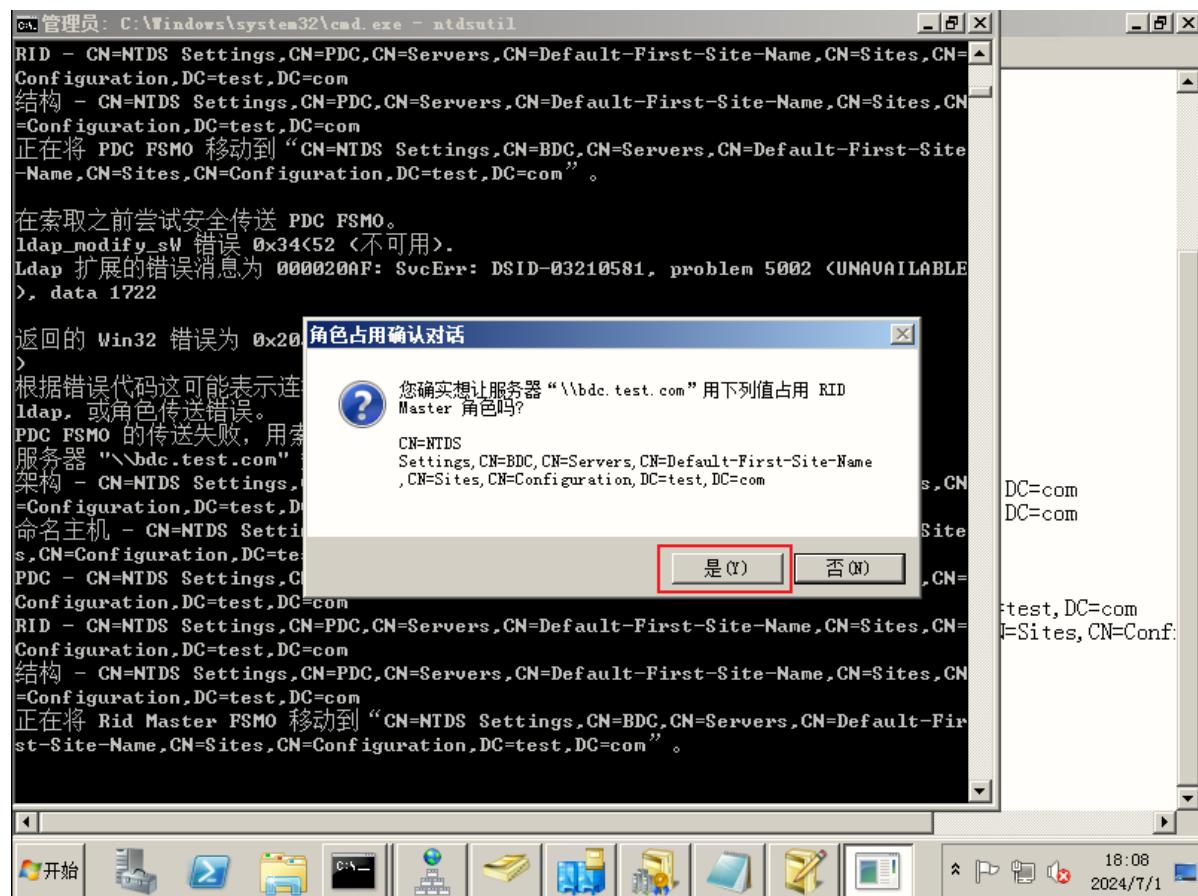
  媒体状态 . . . . . : 媒体已断开
  连接特定的 DNS 后缀 . . . . . :
  描述 . . . . . : Microsoft ISATAP Adapter
```

## 清除元数据，抢夺五大角色

```
C:\Users\Administrator>ntdsutil
ntdsutil: metadata cleanup
metadata cleanup: select operation target
select operation target: connections
server connections: connect to domain test.com
绑定到 \\bdc.test.com ...
用本登录的用户的凭证连接 \\bdc.test.com。
server connections: quit
select operation target: list sites
找到 1 站点
0 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com
select operation target: select site 0
站点 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com
没有当前域
没有当前服务器
当前的命名上下文
select operation target: list domains in site
找到 1 域
0 - DC=test,DC=com
select operation target: select domain 0
站点 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com
域 - DC=test,DC=com
没有当前服务器
当前的命名上下文
select operation target: list servers for domain in site
找到 2 服务器
0 - CN=PDC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=com
1 - CN=BDC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=com
select operation target: select server 0
站点 - CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com
域 - DC=test,DC=com
服务器 - CN=PDC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=com
    DSA 对象 - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-
Name,CN=Sites,CN=Configuration,DC=test,DC=com
    DNS 主机名称 - pdc.test.com
    计算机对象 - CN=PDC,OU=Domain Controllers,DC=test,DC=com
当前的命名上下文
select operation target: quit
metadata cleanup: remove selected server
```







```
C:\Users\Administrator>netdom query fsmo
架构主机          bdc.test.com
域命名主机        bdc.test.com
PDC              bdc.test.com
RID 池管理器      bdc.test.com
结构主机          bdc.test.com
命令成功完成。

C:\Users\Administrator>hostname
bdc

C:\Users\Administrator>nltest /dclist:test.com
获得域“test.com”中 DC 的列表(从“\\bdc.test.com”中)。
BDC.test.com [PDC] [DS] 站点: Default-First-Site-Name
此命令成功完成

C:\Users\Administrator>ipconfig
Windows IP 配置

以太网适配器 本地连接:
连接特定的 DNS 后缀 . . . . . : fe80::3815:b965:72a7:7d25%11
本地链接 IPv6 地址 . . . . . : fe80::3815:b965:72a7:7d25%11
IPv4 地址 . . . . . : 172.168.2.62
子网掩码 . . . . . : 255.255.255.0
默认网关 . . . . . : 172.168.2.254

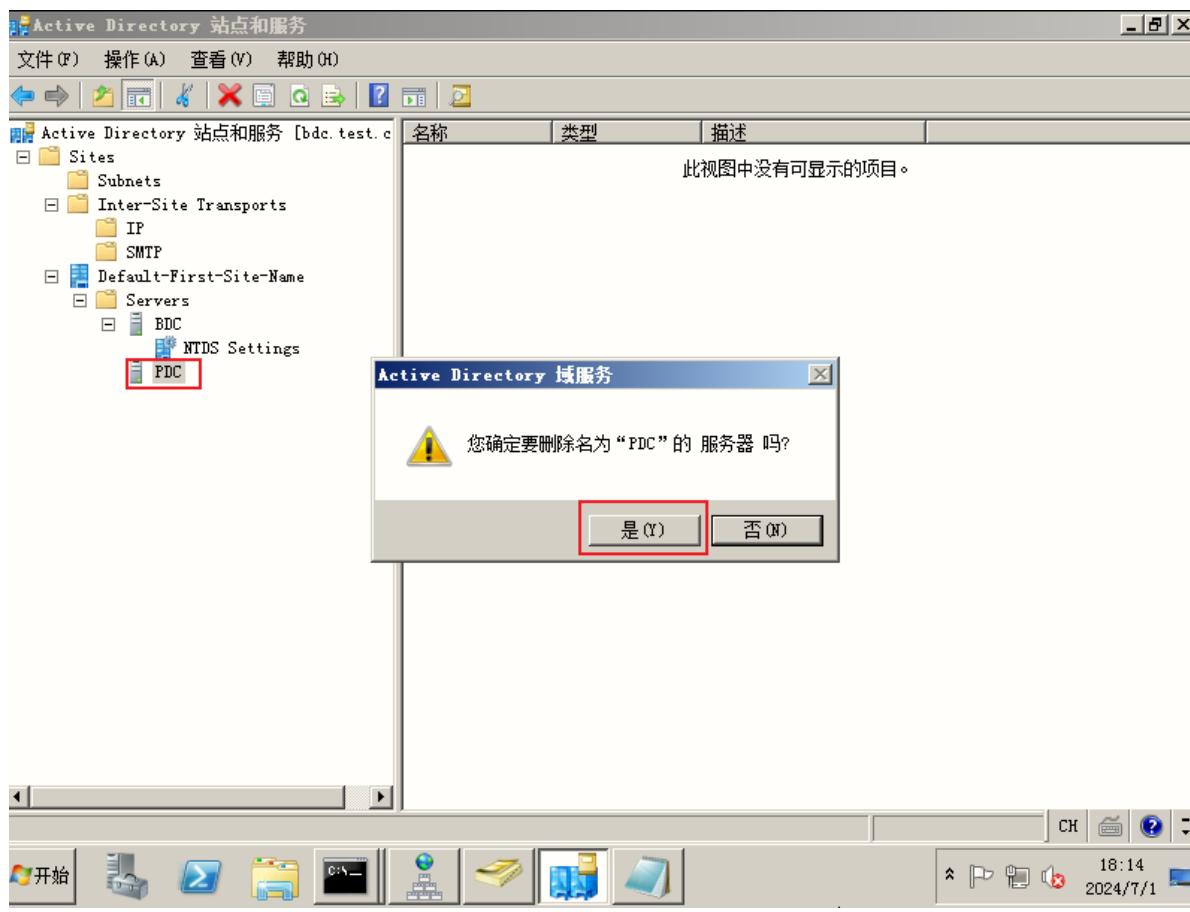
隧道适配器 isatap.{6D66A533-42BC-4BF5-8497-879821853EB8}:

```

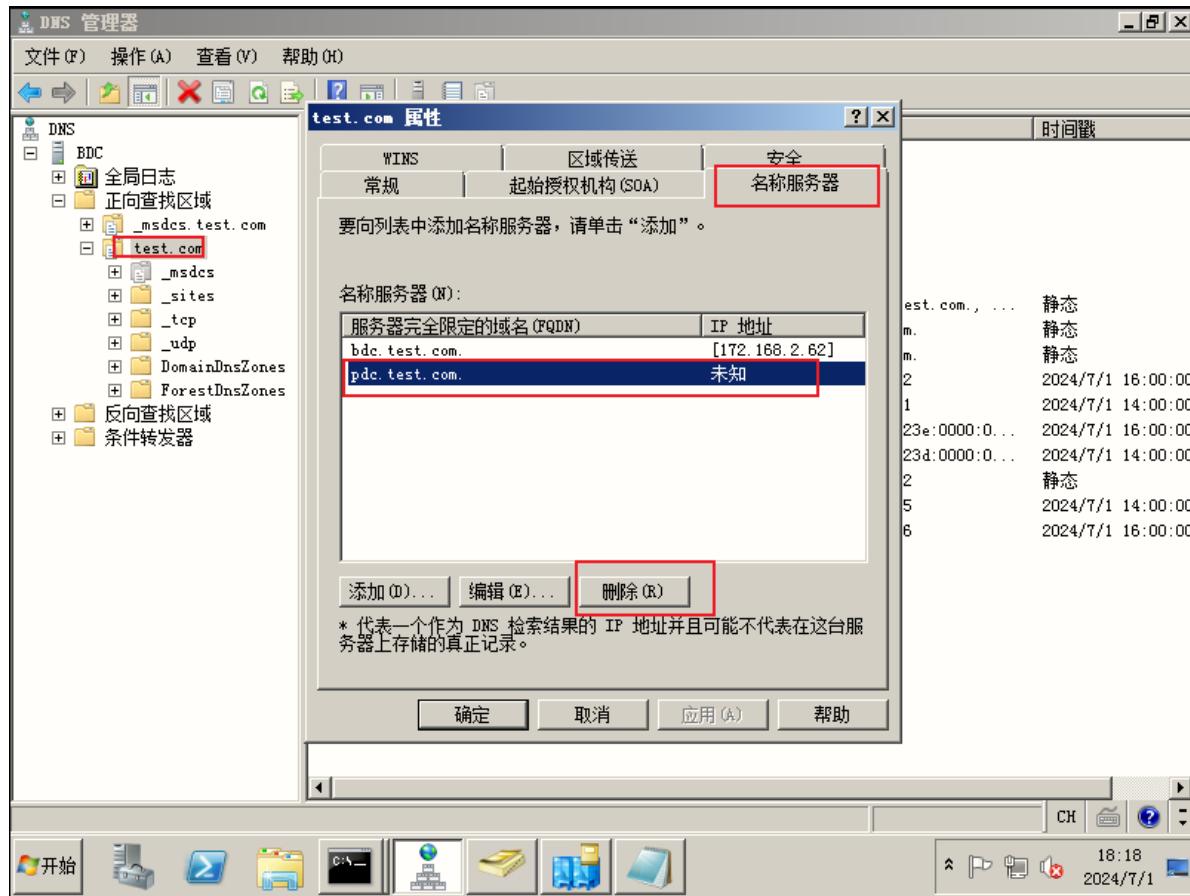
The screenshot shows a Windows Command Prompt window with several network configuration commands and their outputs. The commands include netdom query fsmo, hostname, nltest /dclist:test.com, and ipconfig. The ipconfig output details the local connection configuration, including IPv4 and IPv6 addresses, subnet mask, and default gateway. The taskbar at the bottom shows various icons and the system clock.

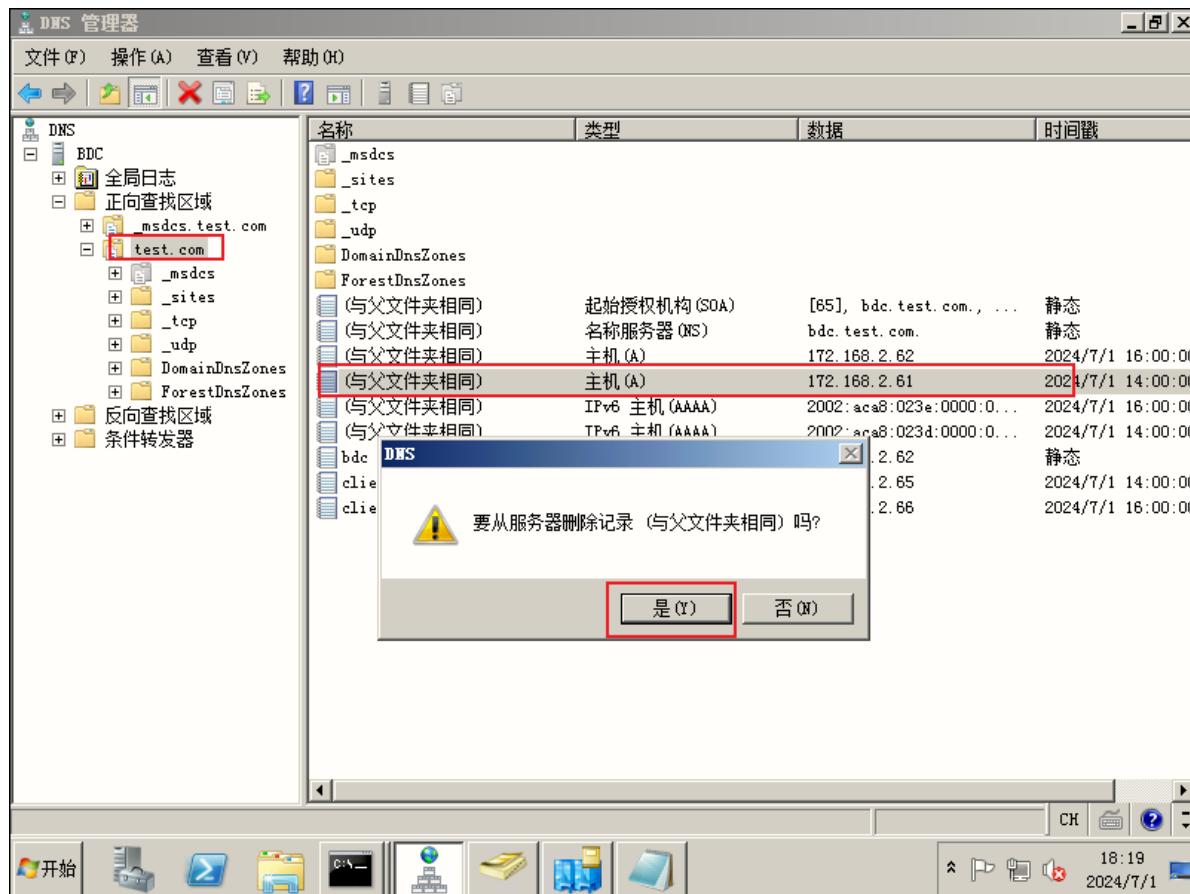
## 5.3 删除PDC无用相关资源

站点和服务



## DNS





## 5.4 客户端查看当前PDC主机

### 客户端01

```
C:\Windows\system32\cmd.exe
C:\Users\test01>ipconfig
Windows IP 配置

以太网适配器 Ethernet0:
连接特定的 DNS 后缀 . . . . . : fe80::f42c:e4b5:f1c5:bd6%8
本地链接 IPv6 地址 . . . . . : 172.168.2.65
IPv4 地址 . . . . . : 255.255.255.0
子网掩码 . . . . . : 172.168.2.254
默认网关. . . . . : 172.168.2.254

C:\Users\test01>hostname
client01

C:\Users\test01>whoami
test\test01

C:\Users\test01>nlist /dclist:test.com
获得域“test.com”中 DC 的列表(从“\\bdc.test.com”中)。
BDC.test.com [PDC] [DS] 站点: Default-First-Site-Name
此命令成功完成

C:\Users\test01>
```

### 客户端02

```
C:\Users\test02>ipconfig
Windows IP 配置

以太网适配器 Ethernet0:

连接特定的 DNS 后缀 . . . . . : 
本地链接 IPv6 地址 . . . . . : fe80::64ce:ba70:7c05:3c4c%8
IPv4 地址 . . . . . : 172.168.2.66
子网掩码 . . . . . : 255.255.255.0
默认网关. . . . . : 172.168.2.254

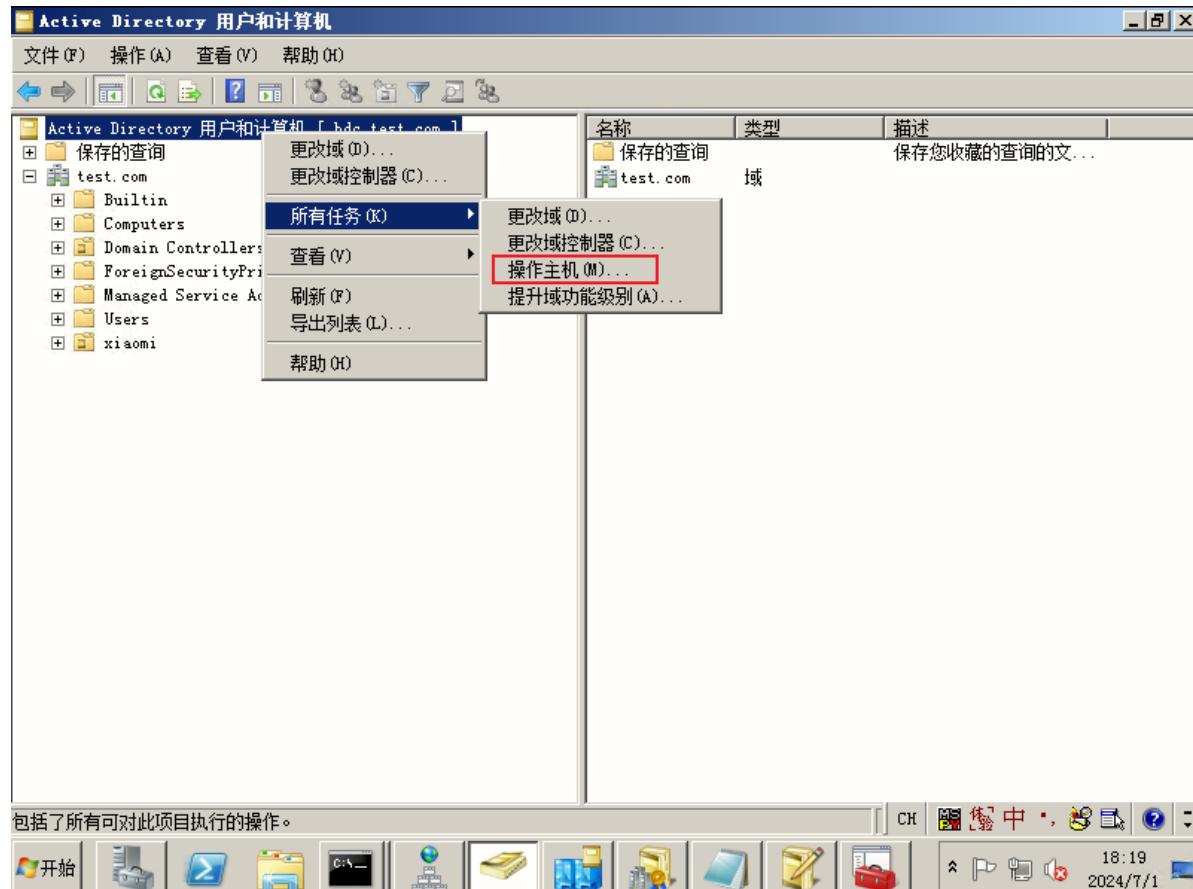
C:\Users\test02>hostname
client02

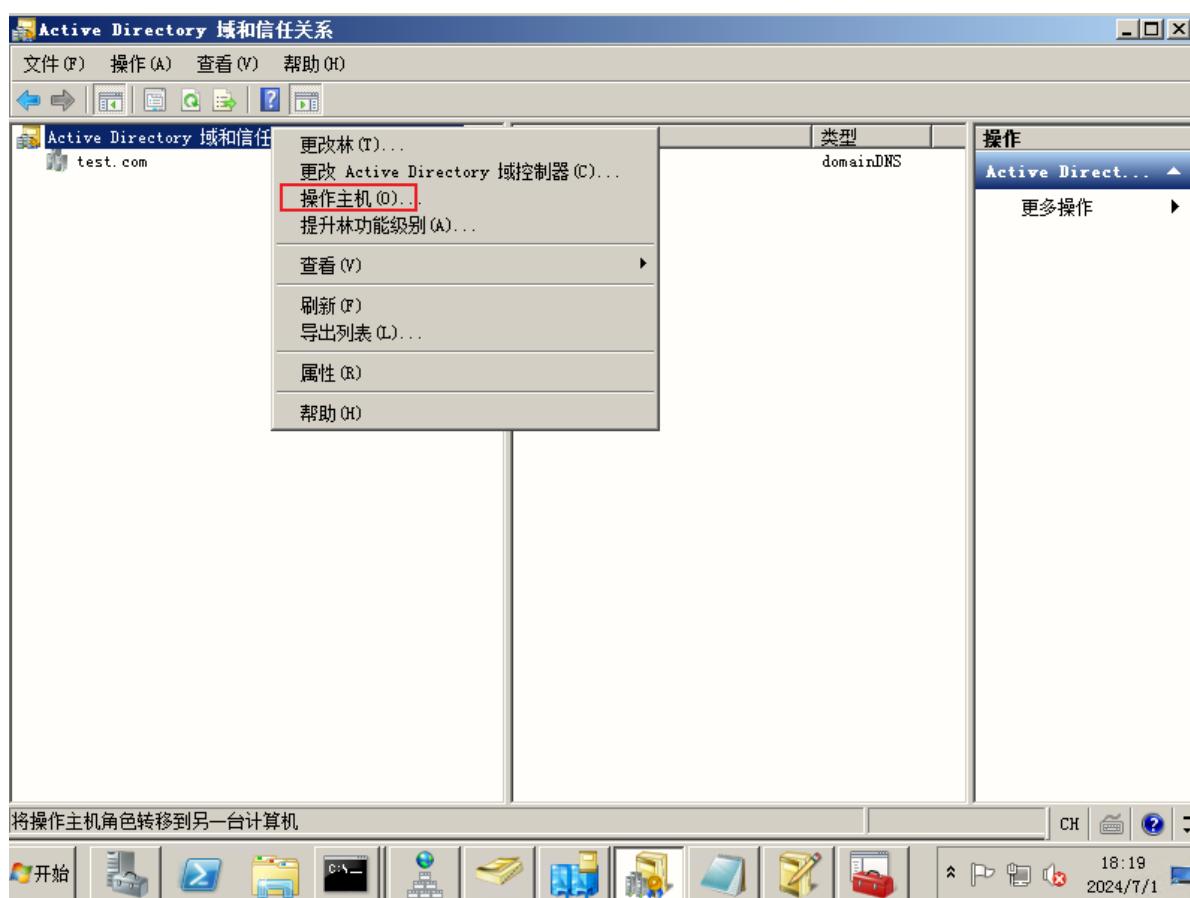
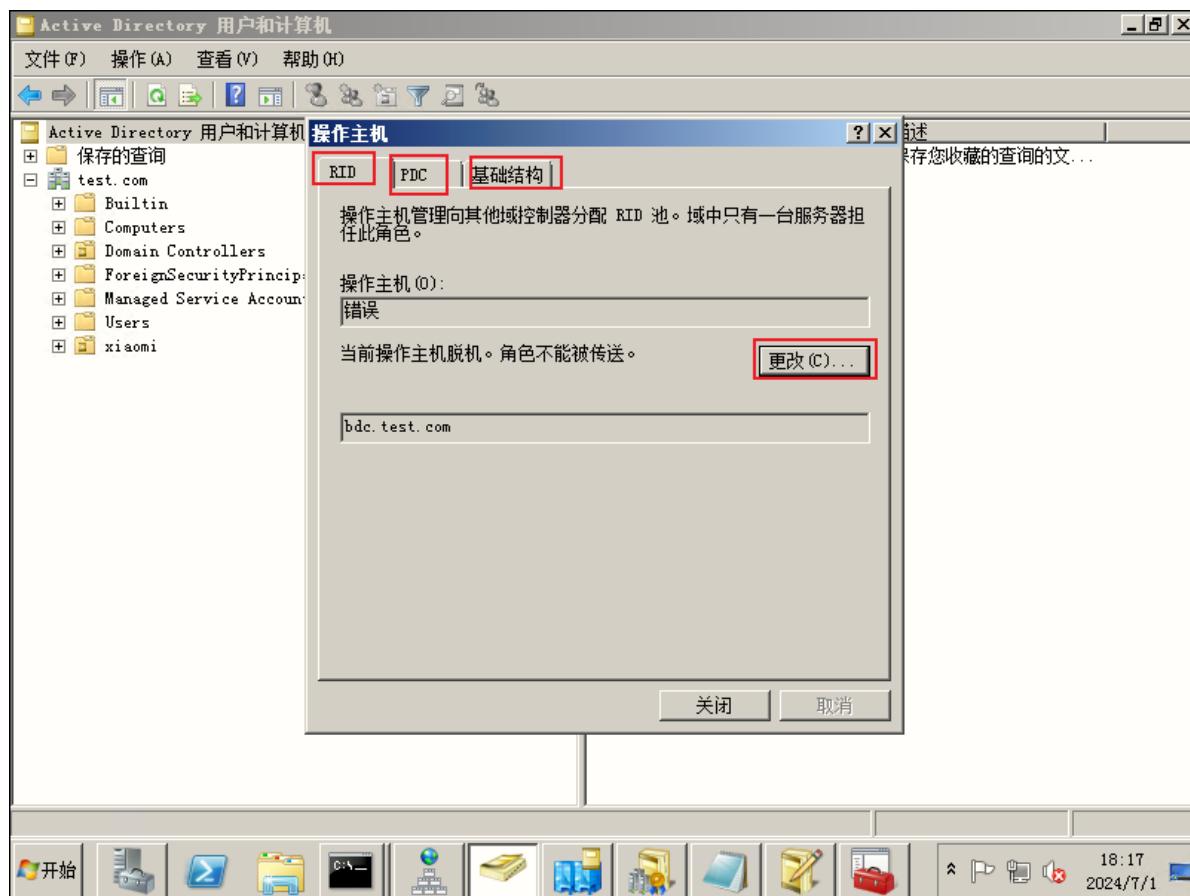
C:\Users\test02>whoami
test\test02

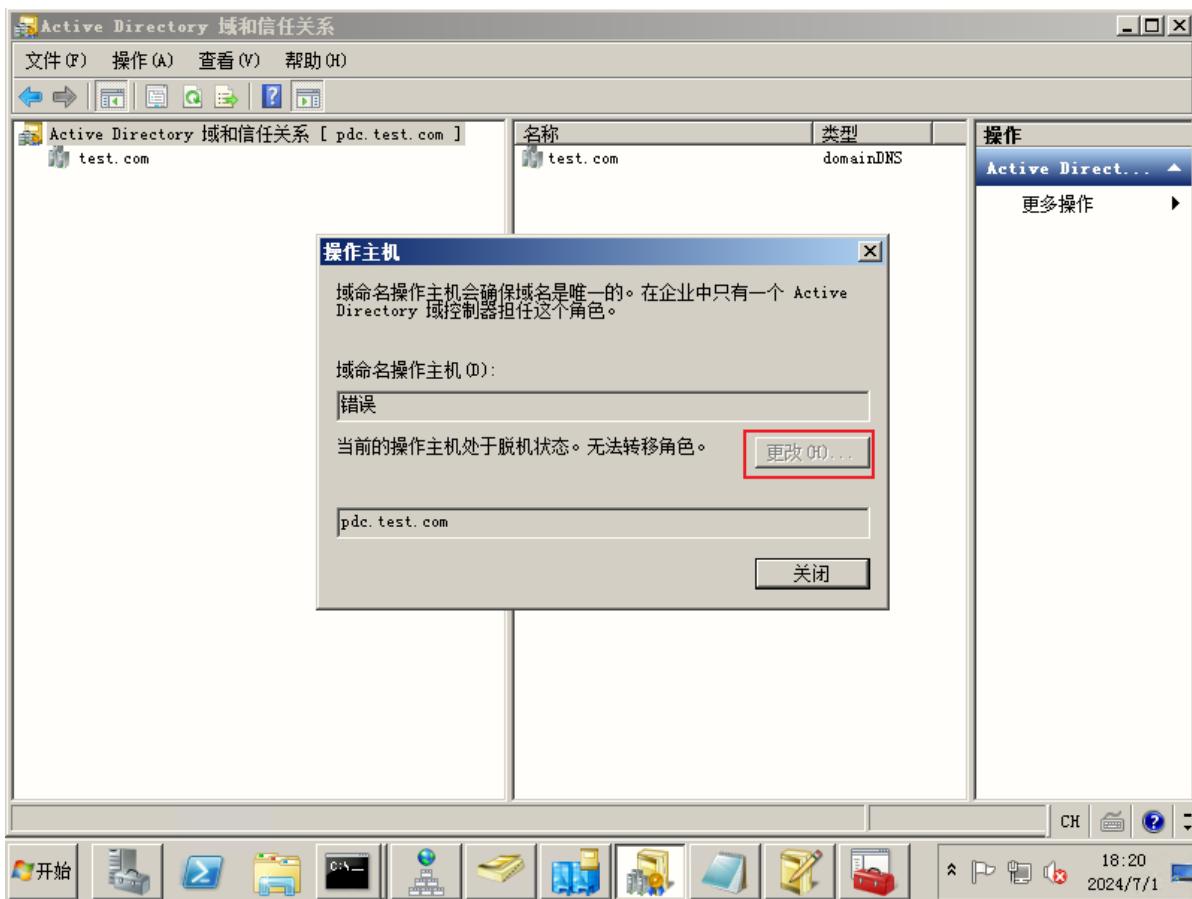
C:\Users\test02>nltest /dclist:test.com
获得域“test.com”中 DC 的列表(从“\\bdc.test.com”中)。
    BDC.test.com [PDC] [DS] 站点: Default-First-Site-Name
此命令成功完成
```

## 6. 手动转移五大角色

### 6.1 GUI方式转移

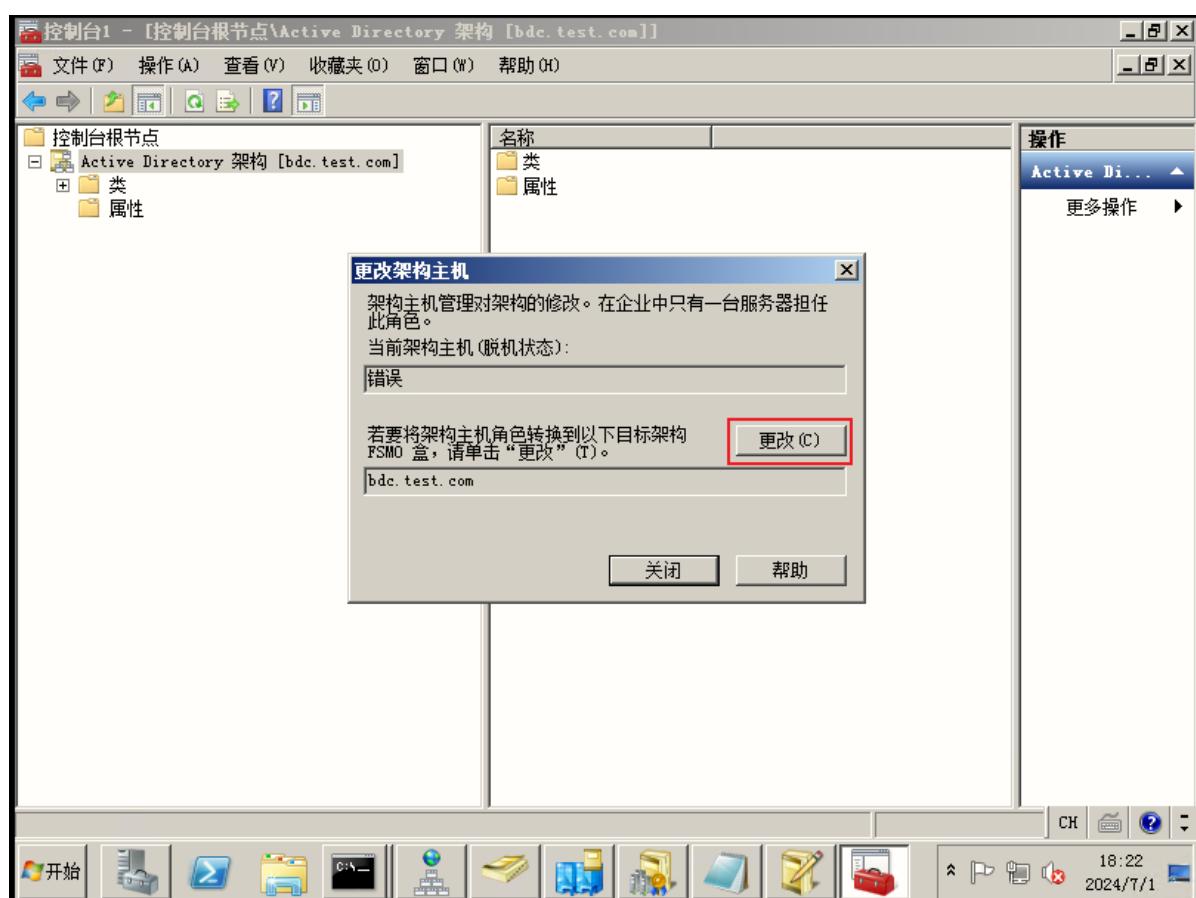
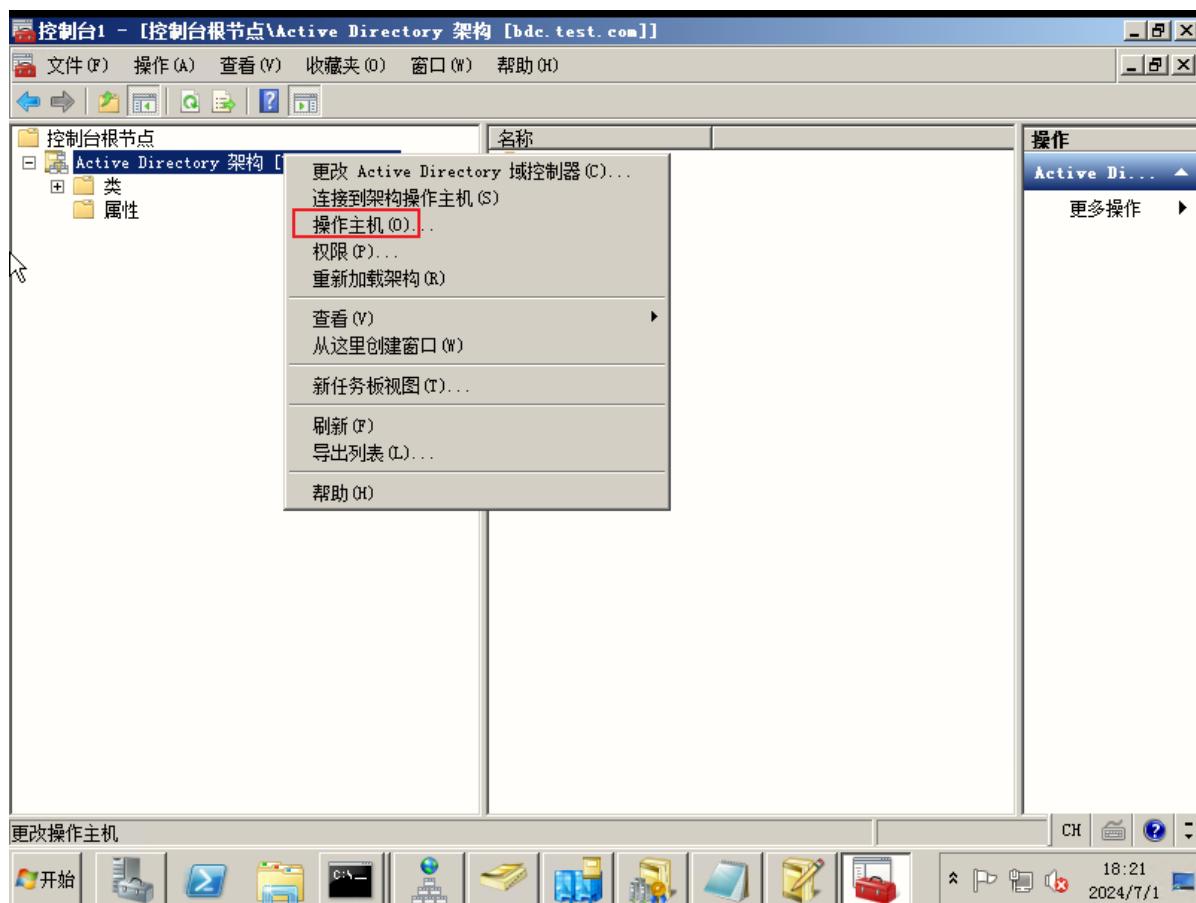






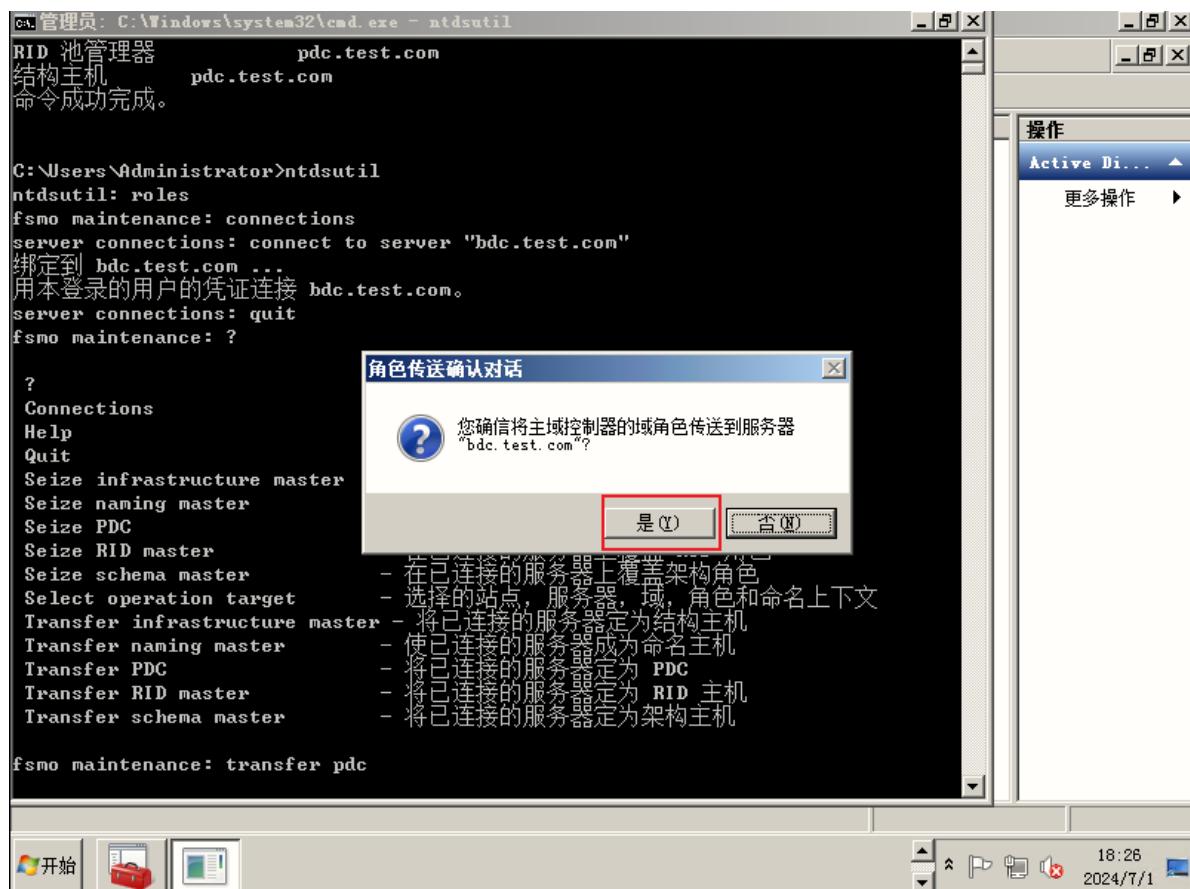
### 注册"Active Directory架构"图形化界面

```
管理员: C:\Windows\system32\cmd.exe
C:\Users\Administrator>regsvr32 schmmgmt.dll
C:\Users\Administrator>mmc
C:\Users\Administrator>
```



## 6.2 CLI方式转移

```
# 需要转移五大角色 PDC、RID master、schema master、naming master、infrastructure
master
# 以下为转移pdc为例
C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server "bdc.test.com"
绑定到 bdc.test.com ...
用本登录的用户的凭证连接 bdc.test.com。
server connections: quit
fsmo maintenance: transfer pdc
```



```
ldap_modify_sw 错误 0x34(52 (不可用)).
Ldap 扩展的错误消息为 000020AF: SvcErr: DSID-03210581, problem 5002 (UNAVAILABLE
), data 1722
```

返回的 Win32 错误为 0x20af(请求的 FSMO 操作失败。不能连接当前的 FSMO 盒。)

)

根据错误代码这可能表示连接

ldap, 或角色传递错误。

服务器 "bdc.test.com" 知道有关 5 作用

架构 - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com

命名主机 - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Site S,CN=Configuration,DC=test,DC=com

PDC - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=test,DC=com

RID - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=

```
Configuration,DC=test,DC=com
结构 - CN=NTDS Settings,CN=PDC,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN
=Configuration,DC=test,DC=com
fsmo maintenance:
```

错误原因：因为PDC已经关机不在线，所以转移不成功，PDC不变，如图

```
C:\Users\Administrator>netdom query fsmo
架构主机          pdc.test.com
域命名主机        pdc.test.com
PDC               pdc.test.com
RID 池管理器      pdc.test.com
结构主机          pdc.test.com
命令成功完成。
```

## 7. 手动抢夺五大角色-灾难恢复-方式二

方式一删除不干净，用此方式二次删除，可以抢夺五大角色

```
C:\Users\Administrator>ntdsutil
ntdsutil: roles
fsmo maintenance: connections
server connections: connect to server "bdc.test.com"
绑定到 bdc.test.com ...
用本登录的用户的凭证连接 bdc.test.com。
server connections: quit

# 占用 RID 主机角色
seize RID master
# 占用 PDC 模拟器角色
seize PDC
# 占用结构主机角色
seize infrastructure master
# 占用域命名主机角色
seize domain naming master
# 占用架构主机角色
seize schema master
```

此方式抢夺五大角色后，重启机器如果提示此域不存在，原因是其它域控服务器DNS地址未填写新PDC服务器的IP地址，所以造成通信交互失败