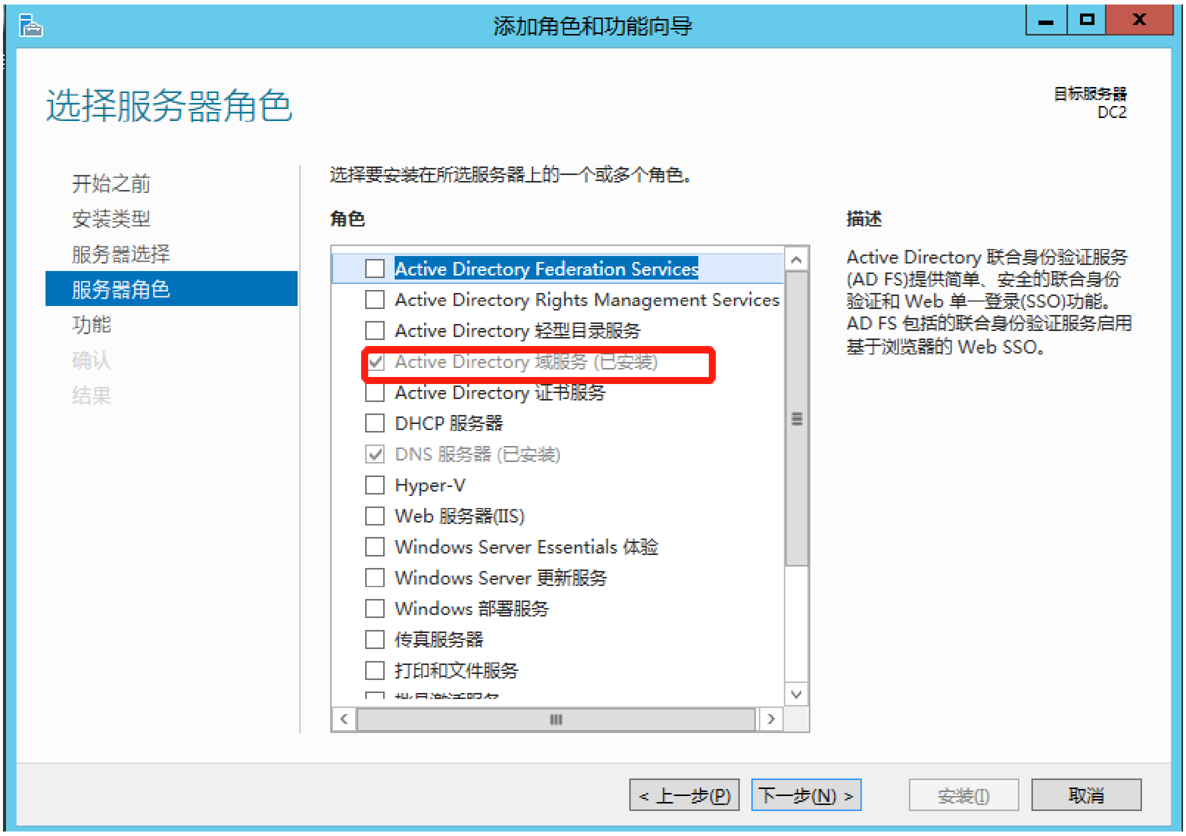
搭建和查看域信任关系

搭建域树（内部信任）

如果是复制的虚拟机请运行 `C:\Windows\System32\sysprep\sysprep.exe` 重新获取SID

1、修改计算机名和修改IP地址，DNS指向父域

2、安装 AD域服务



选择要安装在所选服务器上的一个或多个角色。

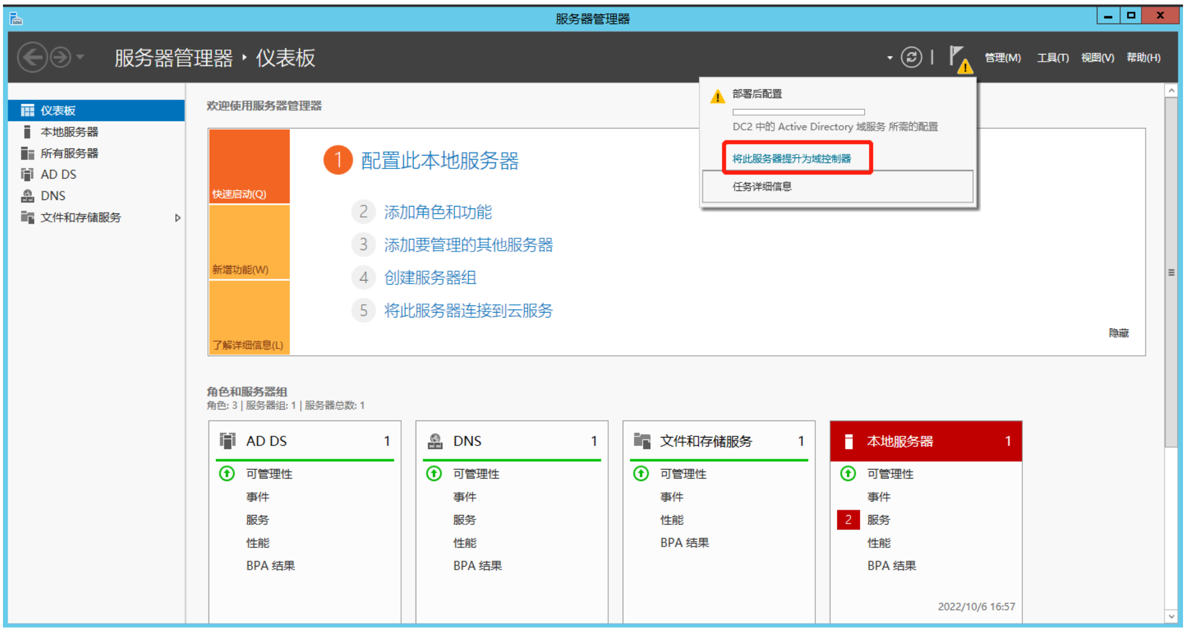
角色

- ☐ Active Directory Federation Services
- ☐ Active Directory Rights Management Services
- ☐ Active Directory 轻型目录服务
- ☑ Active Directory 域服务 (已安装)
- ☐ Active Directory 证书服务
- ☐ DHCP 服务器
- ☑ DNS 服务器 (已安装)
- ☐ Hyper-V
- ☐ Web 服务器(IIS)
- ☐ Windows Server Essentials 体验
- ☐ Windows Server 更新服务
- ☐ Windows 部署服务
- ☐ 传真服务器
- ☐ 打印和文件服务
- ☐ 批量激活服务

描述

Active Directory 联合身份验证服务(AD FS)提供简单、安全的联合身份验证和 Web 单一登录(SSO)功能。AD FS 包括的联合身份验证服务启用基于浏览器的 Web SSO。

3、升级为域控



部署后配置

DC2 中的 Active Directory 域服务 所需的配置

将此服务器提升为域控制器

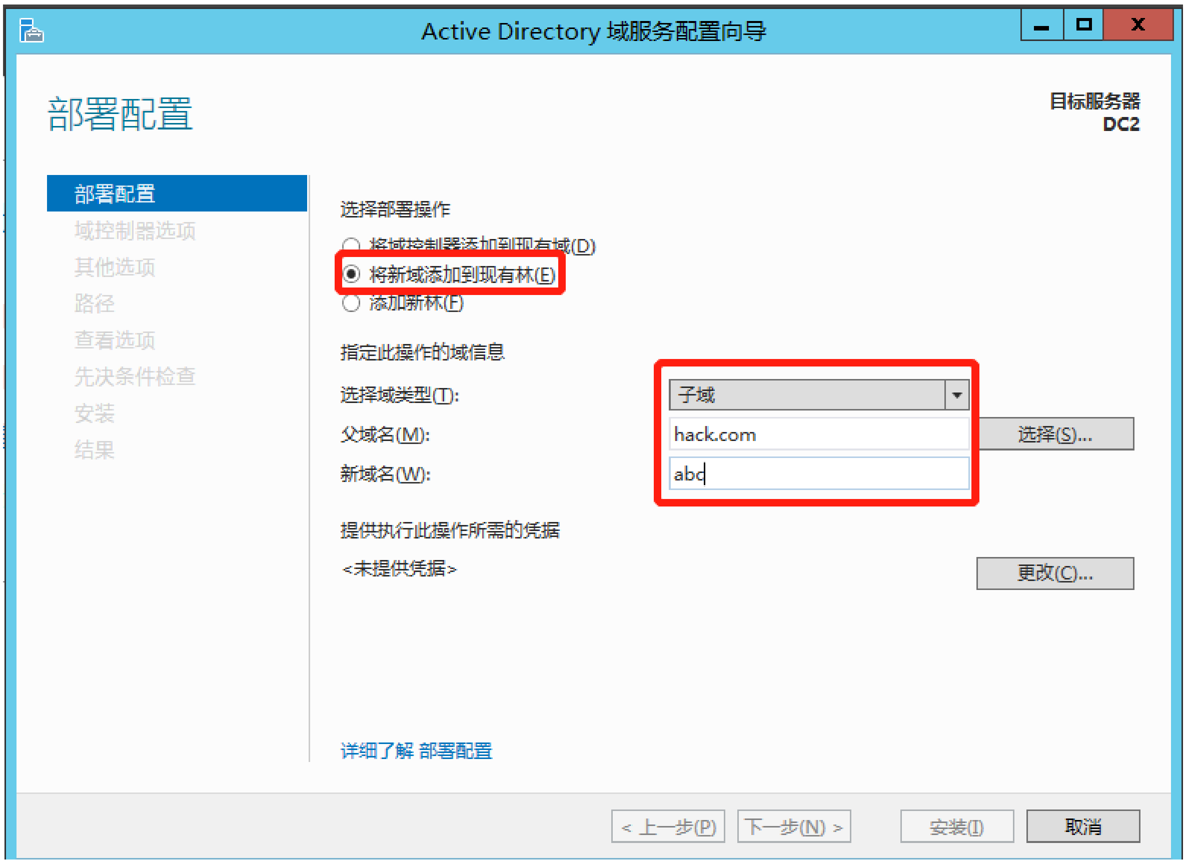
任务详细信息

角色和服务器组

角色: 3 | 服务器组: 1 | 服务器总数: 1

2022/10/6 16:57

4、添加到现有林



Active Directory 域服务配置向导

部署配置

目标服务器
DC2

选择部署操作

○ 将域控制器添加到现有域(D)

● 将新域添加到现有林(E)

○ 添加新林(F)

指定此操作的域信息

选择域类型(T): 子域

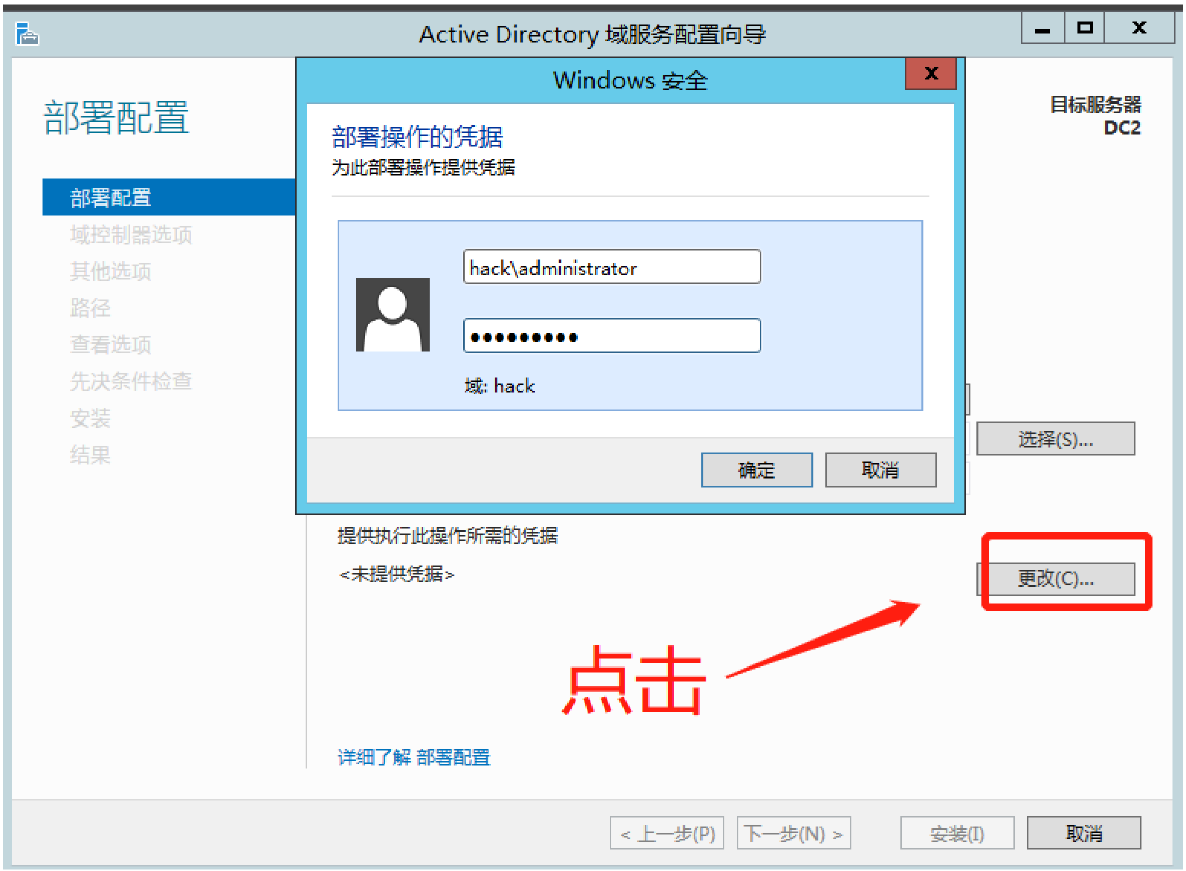
父域名(M): hack.com

新域名(W): abc

提供执行此操作所需的凭据

<未提供凭据>

5、提供父域的账号密码



Active Directory 域服务配置向导

Windows 安全

部署操作的凭据

为此部署操作提供凭据

hack\administrator

●●●●●●●●●●

域: hack

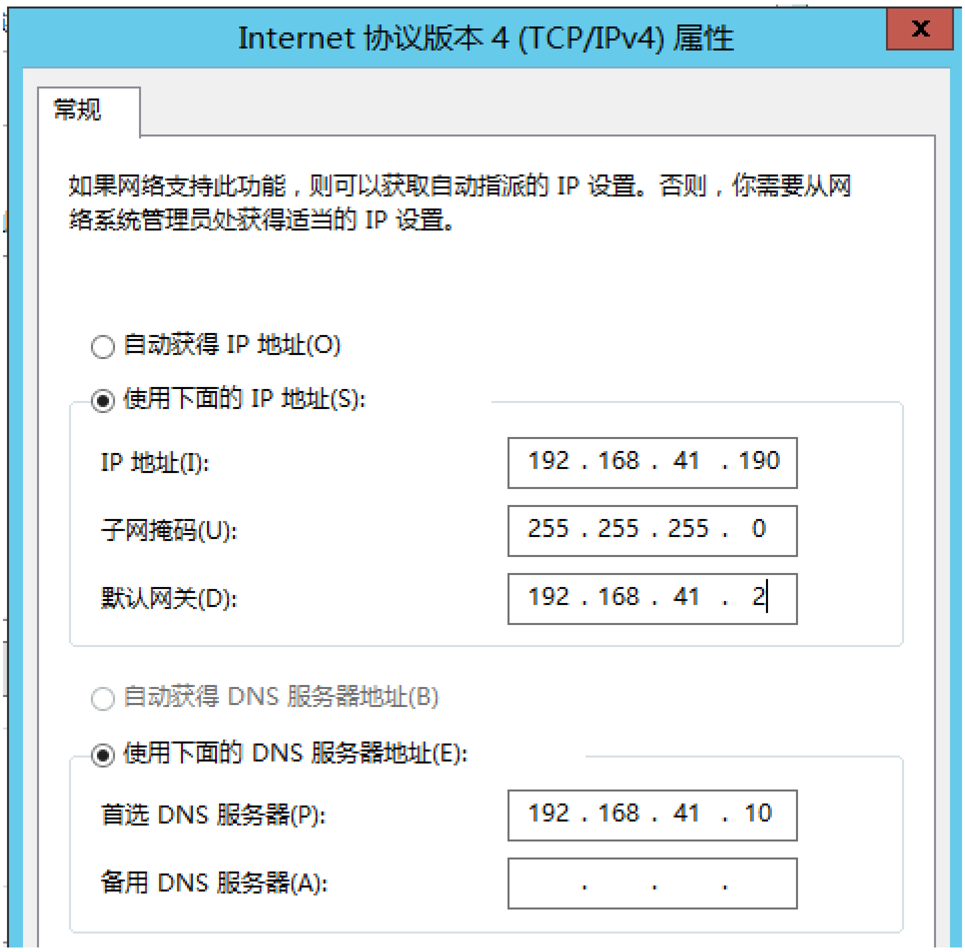
提供执行此操作所需的凭据

<未提供凭据>

6、正常安装直到结束

搭建域森林（外部信任）

1、修改计算机名和修改IP地址，DNS指向根域



Internet 协议版本 4 (TCP/IPv4) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

○ 自动获得 IP 地址(O)

● 使用下面的 IP 地址(S):

IP 地址(I): 192 . 168 . 41 . 190

子网掩码(U): 255 . 255 . 255 . 0

默认网关(D): 192 . 168 . 41 . 2

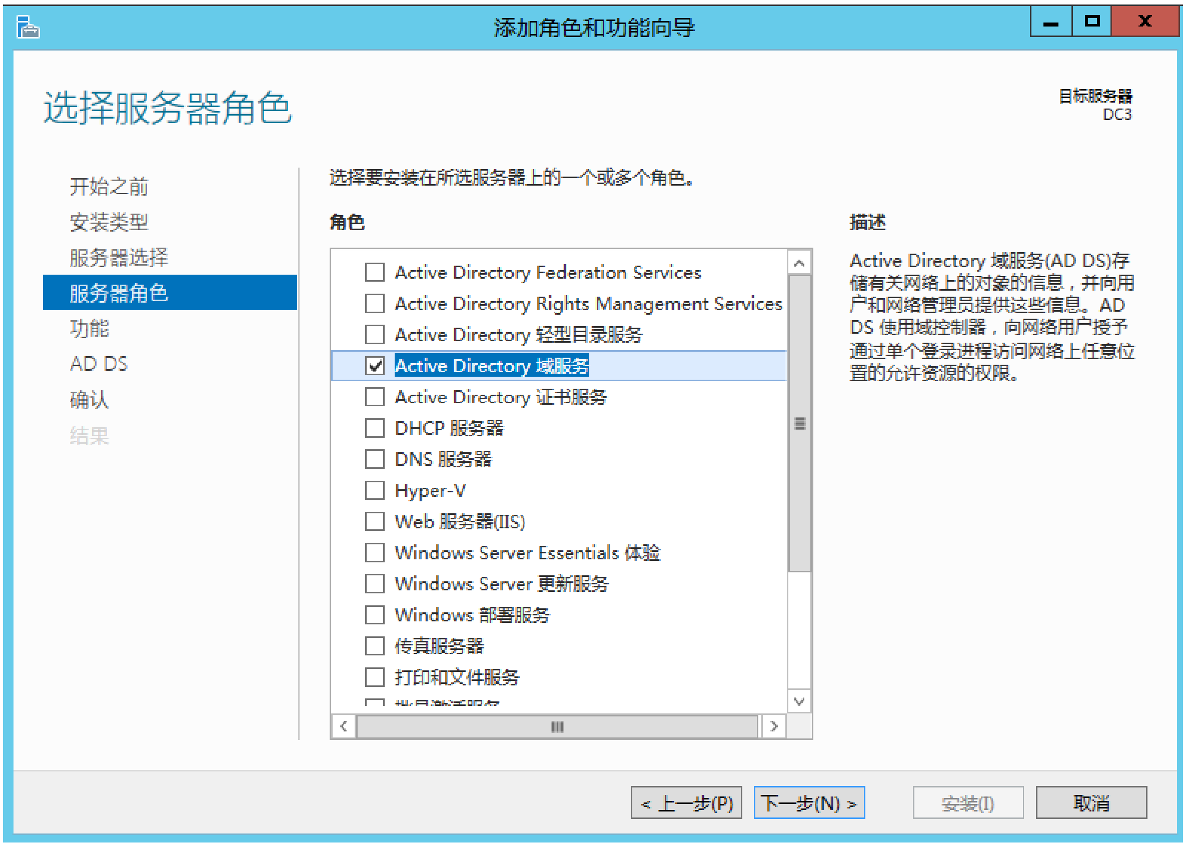
○ 自动获得 DNS 服务器地址(B)

● 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): 192 . 168 . 41 . 10

备用 DNS 服务器(A): . . .

2、安装 AD域服务



添加角色和功能向导

选择服务器角色

目标服务器
DC3

选择要安装在所选服务器上的一个或多个角色。

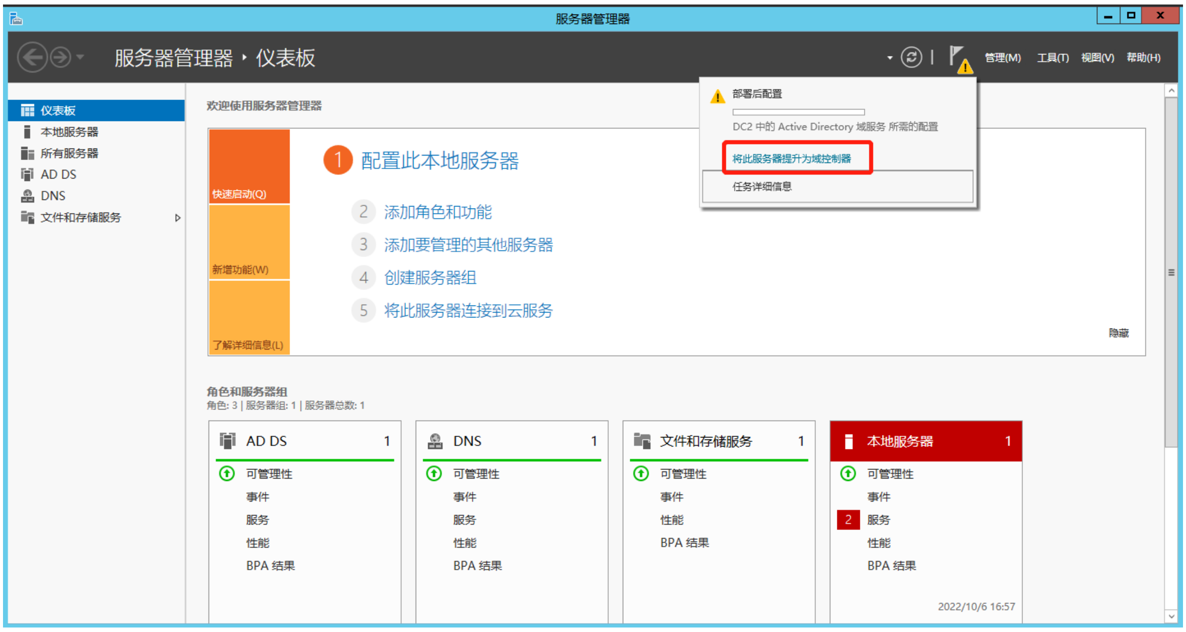
角色

□ Active Directory Federation Services
□ Active Directory Rights Management Services
□ Active Directory 轻型目录服务
☑ Active Directory 域服务
□ Active Directory 证书服务
□ DHCP 服务器
□ DNS 服务器
□ Hyper-V
□ Web 服务器(IIS)
□ Windows Server Essentials 体验
□ Windows Server 更新服务
□ Windows 部署服务
□ 传真服务器
□ 打印和文件服务

描述

Active Directory 域服务(AD DS)存储有关网络上的对象的信息，并向用户和网络管理员提供这些信息。AD DS 使用域控制器，向网络用户授予通过单个登录进程访问网络上任意位置的允许资源的权限。

3、升级为域控



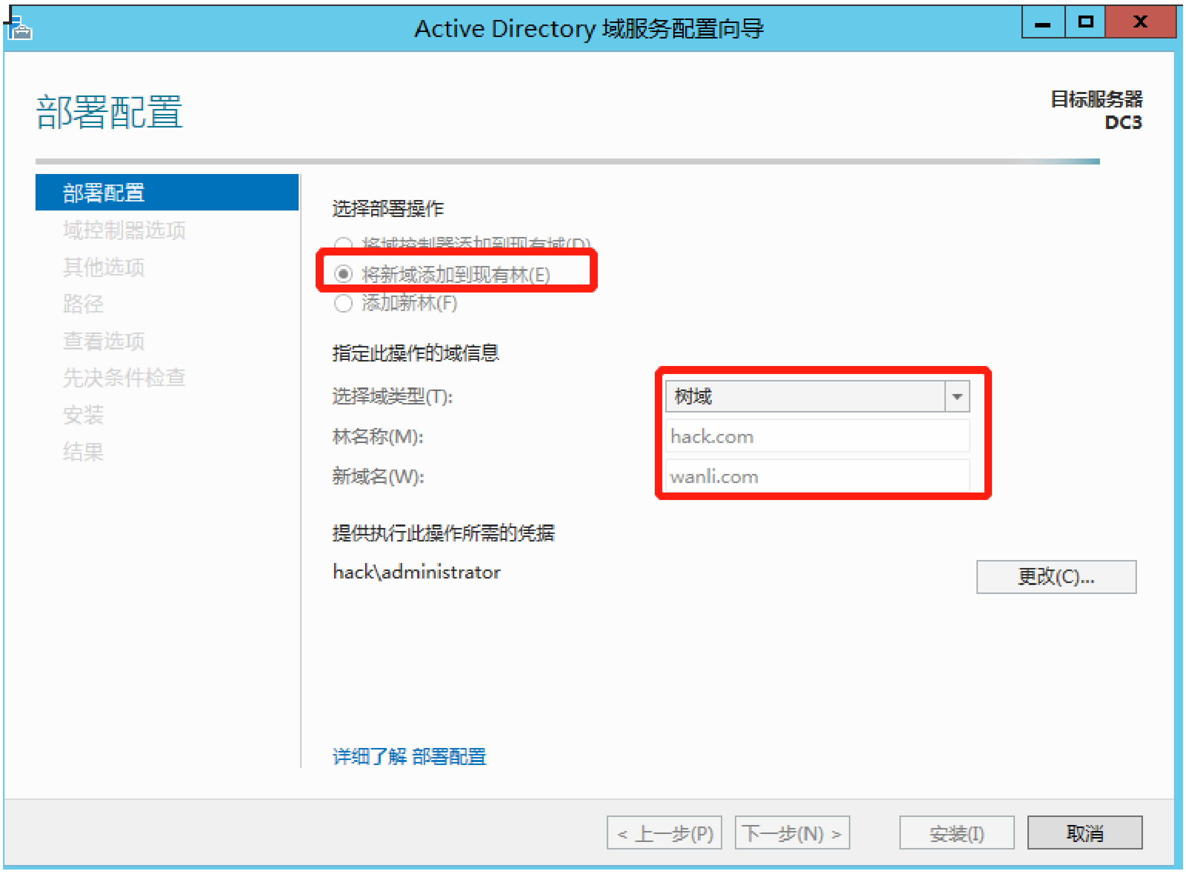
部署后配置

DC2 中的 Active Directory 域服务 所需的配置

将此服务器提升为域控制器

任务详细信息

4、添加到现有林



部署配置

目标服务器
DC3

选择部署操作

○ 将域控制器添加到现有域(D)

● 将新域添加到现有林(E)

○ 添加新林(F)

指定此操作的域信息

选择域类型(T): 树域

林名称(M): hack.com

新域名(W): wanli.com

提供执行此操作所需的凭据

hack\administrator

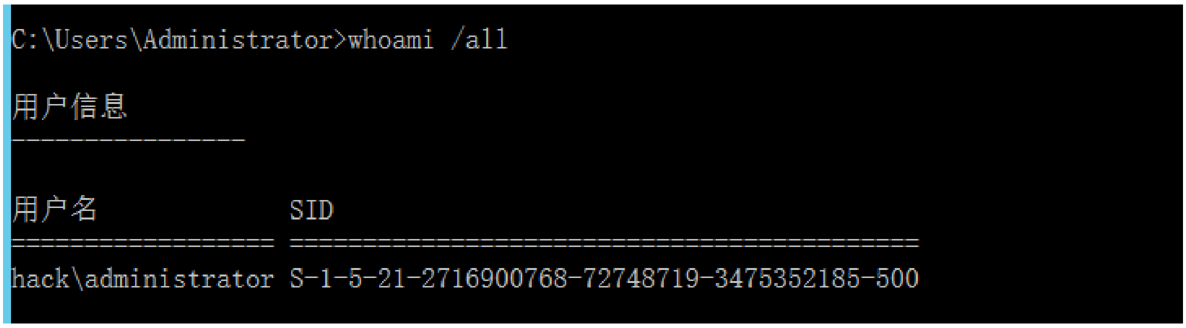
5、正常安全即可

获取域信息

在域中，Enterprise Admins组（出现在林中的根域中）的成员具有对目录林中所有域的完全控制权限。在默认情况下，该组包含林中所有域控制器上具有Administrators权限的成员

查看当前域中计算机的权限

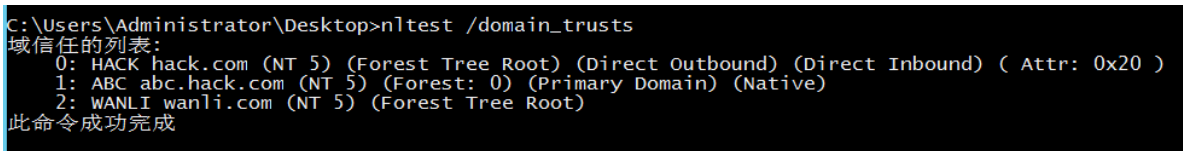
```
whoami /all
```



```
C:\Users\Administrator>whoami /all

用户信息
----------------

用户名             SID
================== =============================================
hack\administrator S-1-5-21-2716900768-72748719-3475352185-500
```

使用lg工具获取域的相关信息

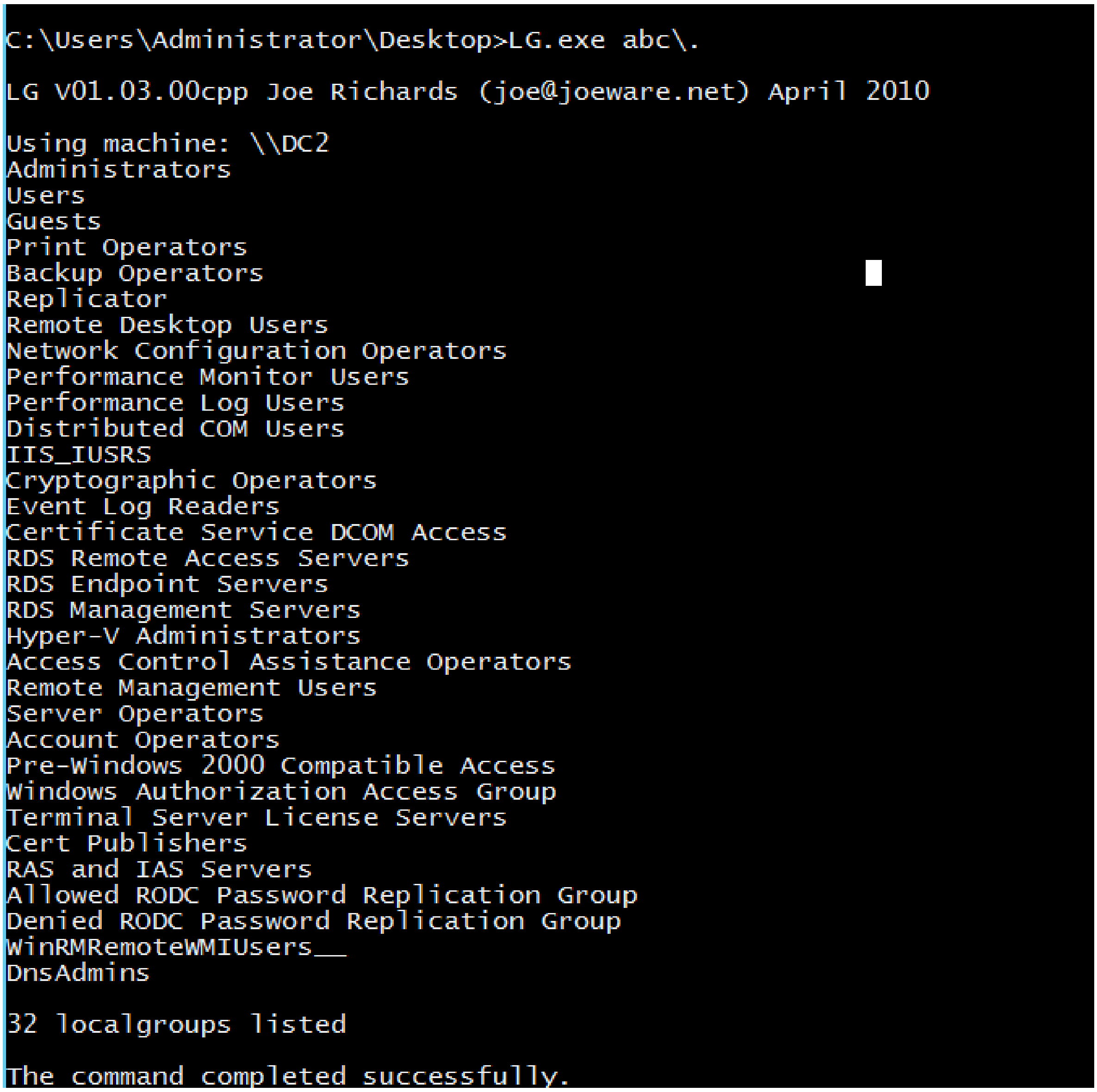
查看域信任关系



```
C:\Users\Administrator\Desktop>nltest /domain_trusts
域信任的列表:
    0: HACK hack.com (NT 5) (Forest Tree Root) (Direct Outbound) (Direct Inbound) ( Attr: 0x20 )
    1: ABC abc.hack.com (NT 5) (Forest: 0) (Primary Domain) (Native)
    2: WANLI wanli.com (NT 5) (Forest Tree Root)
此命令成功完成
```

获取当前域中的用户组

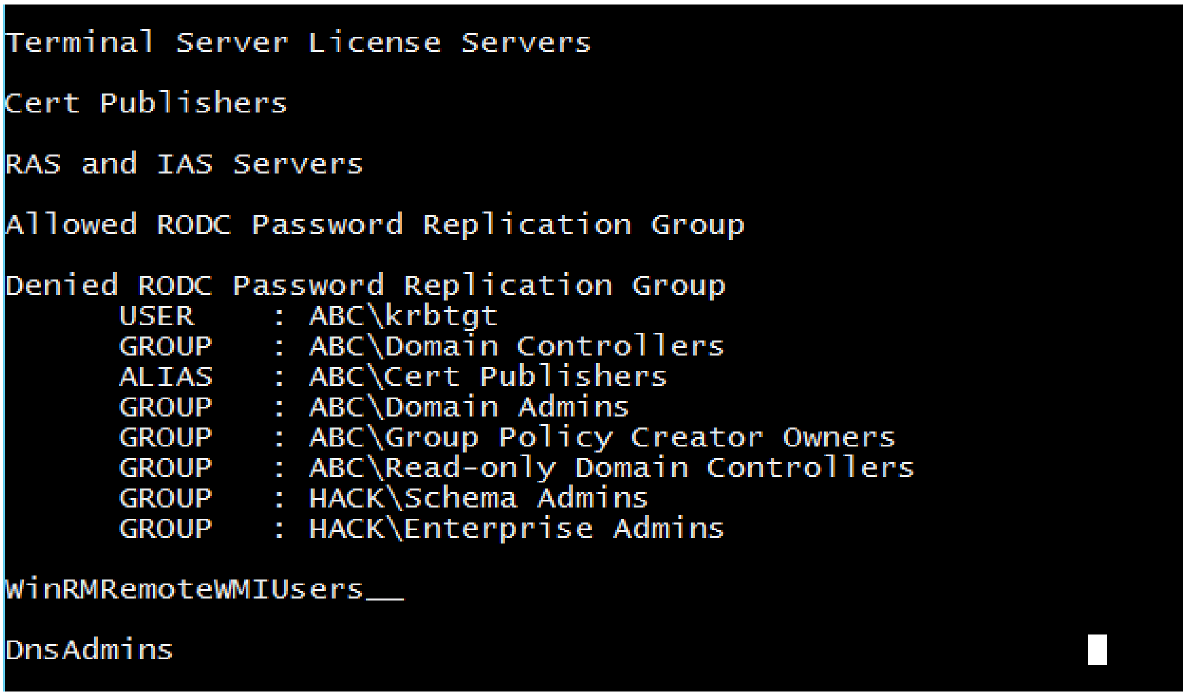
```
LG.exe 域名\.
```



```
C:\Users\Administrator\Desktop>LG.exe abc\.

LG V01.03.00cpp Joe Richards (joe@joeware.net) April 2010

Using machine: \\DC2
Administrators
Users
Guests
Print Operators
Backup Operators
Replicator
Remote Desktop Users
Network Configuration Operators
Performance Monitor Users
Performance Log Users
Distributed COM Users
IIS_IUSRS
Cryptographic Operators
Event Log Readers
Certificate Service DCOM Access
RDS Remote Access Servers
RDS Endpoint Servers
RDS Management Servers
Hyper-V Administrators
Access Control Assistance Operators
Remote Management Users
Server Operators
Account Operators
Pre-Windows 2000 Compatible Access
Windows Authorization Access Group
Terminal Server License Servers
Cert Publishers
RAS and IAS Servers
Allowed RODC Password Replication Group
Denied RODC Password Replication Group
WinRMRemoteWMIUsers__
DnsAdmins

32 localgroups listed

The command completed successfully.
```

获取远程机器的本地用户组

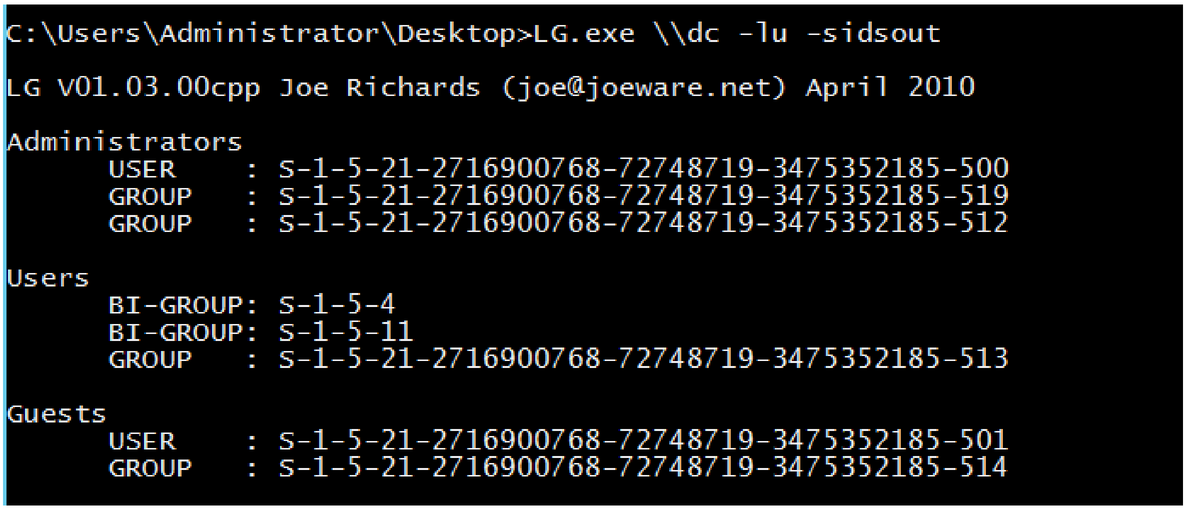
```
LG.exe \\计算机名 -lu
```



```
Terminal Server License Servers

Cert Publishers

RAS and IAS Servers

Allowed RODC Password Replication Group

Denied RODC Password Replication Group
      USER     : ABC\krbtgt
      GROUP    : ABC\Domain Controllers
      ALIAS    : ABC\Cert Publishers
      GROUP    : ABC\Domain Admins
      GROUP    : ABC\Group Policy Creator Owners
      GROUP    : ABC\Read-only Domain Controllers
      GROUP    : HACK\Schema Admins
      GROUP    : HACK\Enterprise Admins

WinRMRemoteWMIUsers__

DnsAdmins
```

获取远程系统中的用户SID

```
LG.exe \\计算机名 -lu -sidsout
```



```
C:\Users\Administrator\Desktop>LG.exe \\dc -lu -sidsout

LG V01.03.00cpp Joe Richards (joe@joeware.net) April 2010

Administrators
      USER     : S-1-5-21-2716900768-72748719-3475352185-500
      GROUP    : S-1-5-21-2716900768-72748719-3475352185-519
      GROUP    : S-1-5-21-2716900768-72748719-3475352185-512

Users
      BI-GROUP: S-1-5-4
      BI-GROUP: S-1-5-11
      GROUP    : S-1-5-21-2716900768-72748719-3475352185-513

Guests
      USER     : S-1-5-21-2716900768-72748719-3475352185-501
      GROUP    : S-1-5-21-2716900768-72748719-3475352185-514
```