

智能时代网络人才培养系列教材  
“互联网+”新形态一体化教材

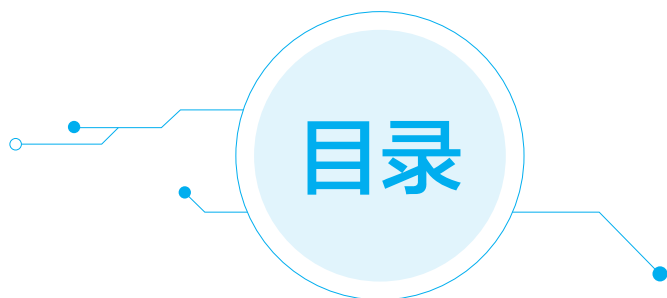
# Windows Server 操作系统项目化教程

2025版

主编◎许 媛 李辉东 李长生



北京交通大学出版社  
<http://www.bjtup.com.cn>



## 项目 1 虚拟化环境搭建与操作系统部署 001

### 1.1 了解 Windows Server 2025 002

1.1.1 系统版本 002

1.1.2 安装条件 003

### 1.2 虚拟机配置 004

1.2.1 安装 VMware Workstation  
并创建虚拟交换机 004

1.2.2 部署 Windows Server 2025  
基础映像 008

1.2.3 配置虚拟机快照与克隆 011

### 1.3 系统初始化设置 016

1.3.1 配置 IP 地址与网络连通性  
测试 016

1.3.2 初始运行 Windows Server 018

1.3.3 使用 Windows Admin Center  
远程管理 020

项目实训 024

项目评价 025

拓展阅读 025

## 项目 2 管理本地用户账户和组 027

### 2.1 规划本地用户账户 028

2.1.1 认识和使用本地用户账户 028

2.1.2 创建本地用户账户 029

2.1.3 设置本地用户账户属性与系统  
权限 030

### 2.2 管理本地用户组 031

2.2.1 认识和使用本地用户组 031

2.2.2 创建本地用户组 031

项目实训 032

项目评价 033

拓展阅读 033

## 项目 3 活动目录基础配置 035

### 3.1 初识活动目录 036

### 3.2 单域环境建设 037

3.2.1 安装 AD 域角色服务与晋升域  
控制器 037

3.2.2 创建域用户与组织单位 044

3.2.3 客户端计算机加域操作 047

### 3.3 本地安全策略与组策略 052

3.3.1 配置密码策略 052

3.3.2 部署软件分发策略 053

项目实训 059

项目评价 059

拓展阅读 059



## 项目 4 磁盘管理 061

### 4.1 了解磁盘管理 062

### 4.2 磁盘基础操作 063

#### 4.2.1 MBR 磁盘与 GPT 磁盘转换 063

#### 4.2.2 简单卷的创建与扩展 068

#### 4.2.3 存储池配置入门 070

### 4.3 存储空间应用 072

#### 4.3.1 镜像卷故障模拟 072

#### 4.3.2 磁盘配额实施 075

### 项目实训 076

### 项目评价 076

### 拓展阅读 077

## 项目 5 DNS 服务配置与优化 079

### 5.1 认识 DNS 服务 080

#### 5.1.1 DNS 服务基础 080

#### 5.1.2 DNS 服务的原理 081

### 5.2 域名解析基础 082

#### 5.2.1 配置网络环境 082

#### 5.2.2 安装 DNS 服务器角色 082

#### 5.2.3 创建正向 / 反向查找区域 083

#### 5.2.4 配置条件转发器 088

### 5.3 高可用性实现 090

#### 5.3.1 部署辅助 DNS 服务器 090

#### 5.3.2 配置 DNSSEC 基础防护 092

### 项目实训 096

### 项目评价 097

### 拓展阅读 097

## 项目 6 DHCP 服务部署与管理 099

### 6.1 认识 DHCP 服务 100

### 6.2 DHCP 服务搭建 101

#### 6.2.1 网络环境搭建 101

#### 6.2.2 安装 DHCP 服务器角色 103

#### 6.2.3 创建 IPv4 作用域并设置保留地址 104

### 项目实训 109

### 项目评价 109

### 拓展阅读 109

## 项目 7 Web 与 FTP 服务器架设 111

### 7.1 认识 Web 服务与 FTP 服务 112

### 7.2 IIS 服务部署 113

#### 7.2.1 基础环境准备 113

#### 7.2.2 安装 Web 服务器角色并创建站点 113

#### 7.2.3 配置虚拟目录与默认文档 115

#### 7.2.4 绑定域名与 HTTPS 证书 118

### 7.3 FTP 服务管理 122

#### 7.3.1 搭建匿名访问 FTP 站点 122

#### 7.3.2 实现用户隔离 FTP 124

#### 7.3.3 防火墙端口放行策略 129

### 项目实训 130

### 项目评价 130

### 拓展阅读 131

## 项目 8 远程桌面服务实现 133

8.1 认识远程桌面服务	134
8.2 安装远程桌面角色服务	136
8.3 配置会话集合	138
8.4 发布 RemoteApp 程序	140
项目实训	145
项目评价	145
拓展阅读	145

## 项目 9 VPN 服务配置 147

9.1 认识 VPN 服务	148
9.2 配置 VPN 服务	150
9.2.1 网络环境搭建	150
9.2.2 安装 VPN 服务器角色	152
9.2.3 配置 VPN 访问	153
9.2.4 创建用户并授予权限	157
9.2.5 测试	158
项目实训	160
项目评价	161
拓展阅读	161

## 项目 10 NAT 服务与端口映射 163

10.1 认识 NAT 服务	164
10.2 搭建 NAT 服务	165
10.2.1 网络环境搭建	165
10.2.2 安装路由和远程访问服务	166
10.2.3 配置 NAT 外部接口与内部网络	167
10.2.4 验证内外网通信	170
10.2.5 设置端口映射 (Web 服务发布)	170
项目实训	172
项目评价	172
拓展阅读	172

## 参考文献 174

# 项目 3 活动目录基础配置

## 项目概述

活动目录 (AD) 是 Windows Server 提供的核心目录服务, 用于集中管理企业网络中的用户、计算机、权限及资源。它通过林—树—域—组织单位的层级结构构建统一的身份认证与权限控制体系, 实现用户单点登录、跨域资源访问及组策略的集中配置。AD 以域控制器 (DC) 为核心, 存储用户账户、安全策略及网络对象属性, 并通过多域控制器间的复制机制保障高可用性。其核心功能包括统一身份验证 (如 Kerberos 协议)、细粒度权限分配 (基于 ACL 的访问控制)、自动化策略部署 (如强制密码复杂度) 及网络资源发现 (如定位域控制器或打印机)。随着混合云的发展, AD 可与 Azure AD 集成, 支持本地与云端身份同步及零信任安全架构, 成为企业 IT 管理的基石。

## 学习目标

### 知识目标

- (1) 深入理解和掌握活动目录的相关概念, 包括其层级架构、工作原理。
- (2) 全面掌握域控制器 (Domain Controller) 的作用, 了解其在活动目录环境中的核心地位。

### 能力目标

- (1) 具备独立安装域角色服务 (Domain Role Service) 的能力, 并能够顺利完成域控制器的升级操作, 确保系统的稳定性和安全性。
- (2) 能够熟练完成将计算机或设备加入域的操作, 掌握加入域的具体步骤和注意事项, 确保设备能够顺利融入企业网络环境。
- (3) 能够灵活配置组策略, 通过组策略实现对用户和计算机的集中管理, 包括设置安全策略、软件安装、脚本执行等, 提升网络管理的效率和安全性。

### 素质目标

- (1) 提升逻辑思维与规划能力, 能根据模拟企业组织架构, 合理设计组织单位、用户组及权限层级, 确保域结构清晰可维护。
- (2) 强化团队协作意识, 在多人协作管理域环境时, 能规范记录操作日志, 及时同步权限变更信息, 避免因信息脱节而引发权限冲突。



## 3.1 初识活动目录

活动目录 (AD) 是 Windows Server 的核心服务之一，本质上是一个基于 LDAP (轻型目录访问协议) 的目录服务，用于集中管理企业网络中的用户、设备、权限等资源。其核心功能包括身份验证 (如用户登录)、权限分配 (如文件访问控制)、策略管理 (如强制安全策略) 以及资源发现 (如定位网络打印机)。AD 通过结构化数据库存储对象 (如用户账户、计算机、组策略) 及其属性，支持大规模网络环境的高效管理。

### 1. 层级结构与组件

活动目录采用林 (Forest) — 树 (Tree) — 域 (Domain) — 组织单位 (OU) 的层级架构。

(1) 林：最高级别，包含一个或多个不连续的命名空间 (树)，共享统一的安全策略和信任关系。

(2) 树：由共享连续 DNS 命名空间的多个域组成 (如 domain.com、sales.domain.com)。

(3) 域：基本管理单元，包含用户、计算机等对象，通过域控制器 (Domain Controller, DC) 存储和同步 AD 数据库 (ntds.dit 文件)。

(4) 组织单位：可嵌套的容器，用于逻辑分组 (如按部门划分)，支持组策略的继承与委派管理。此外，AD 依赖全局编录 (GC) 存储林中所有对象的副本，加速跨域查询；站点 (Site) 则用于物理网络划分，优化复制流量和客户端定位。

### 2. 工作原理与协议

AD 通过多域控制器间的多主复制机制保持数据一致性，用户登录时通过 Kerberos 协议进行身份验证。关键流程包括对象创建、组策略应用、权限控制等。

(1) 对象创建：如新建用户账户时，AD 为其分配唯一安全标识符 (SID) 并存储属性 (如密码哈希)。

(2) 组策略应用：组策略通过链接到域或组织单位，在客户端登录时下发配置 (如禁用控制面板、自动安装软件)。

(3) 权限控制：基于访问控制列表 (ACL)，通过安全组或直接分配对象权限 (如某用户对文件夹的读写权限)。

相关协议包括 LDAP (查询 AD 对象)、DNS (定位域控制器)、Kerberos (认证) 及 NTLM (旧版认证协议)。

### 3. 高级功能与集成

AD 支持多种拓展场景，主要拓展场景如下。

(1) 活动目录域服务 (AD DS)：核心功能，提供域管理、信任关系和安全策略。

(2) 活动目录轻型目录服务 (AD LDS)：非域控制器版本，用于需要自定义目录结构的应用 (如独立应用程序)。

(3) 活动目录证书服务 (AD CS)：颁发和管理数字证书，支撑 HTTPS、智能卡登录等场景。

(4) 活动目录联合身份验证服务 (AD FS)：实现跨组织的单点登录 (SSO)，如访问合作伙伴的云

端应用。

此外，AD 可通过工具（如 PowerShell 或 SCOM）与第三方系统（如 Exchange Server 管理邮箱权限）集成。

#### 4. 现代演进与混合云

随着企业向云端迁移，AD 的扩展形态主要包括以下几种。

（1）Azure AD：微软云目录服务，支持混合环境（本地 AD 与 Azure 同步），提供多因素认证（MFA）、条件访问（如基于设备合规性的登录限制）及 SaaS（软件即服务）应用单点登录（如 Office 365）。

（2）AD DS 在 Azure VM 中的部署：通过虚拟机创建云域控制器，延续本地 AD 管理逻辑。

（3）IDaaS：身份即服务，Azure AD 等服务逐渐替代传统 AD 部分功能，推动企业向“无本地 AD”架构过渡。

当前，AD 的管理工具也趋向自动化（如通过 PowerShell DSC 或 Azure Policy）和可视化（如 Microsoft Entra ID 门户），适应 DevOps 与零信任安全模型的需求。

## 3.2 单域环境建设

### 3.2.1

#### 安装 AD 域角色服务与升级为域控制器

单域环境建设的网络拓扑图如图 3-1 所示。



图 3-1 单域环境建设的网络拓扑图

将 Server1 的 IP 地址设置为 192.168.10.100，将网关设置为 VMware 的虚拟网络对应的网关 IP（选择 VMware Workstation 的“编辑”→“虚拟网络编辑器”选项，选择 VMnet8 选项，单击“NAT 设置”按钮，记录弹出的“NAT 设置”对话框中的网关 IP，这里的网关 IP 为 192.168.10.254）。

以管理员身份登录 Server1，单击“开始”菜单，选择“服务器管理器”选项，在打开的“服务器管理器”窗口中单击“管理”菜单，选择“添加角色和功能”选项，打开图 3-2 所示的窗口。

持续单击“下一页”按钮，直到进入图 3-3 所示的“选择服务器角色”页面，勾选“Active Directory 域服务”复选框，在系统弹出的“添加角色和功能向导”对话框中单击“添加功能”按钮。



添加域角色  
并升级为域  
控制器



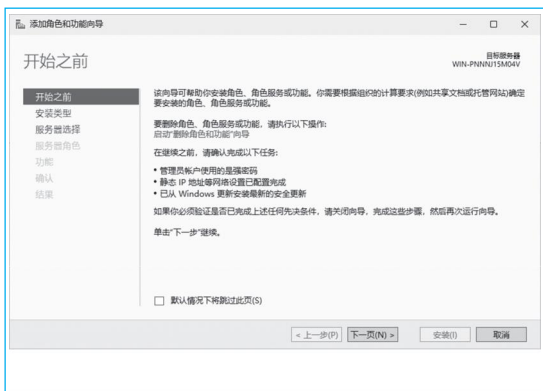


图 3-2 “开始之前” 页面

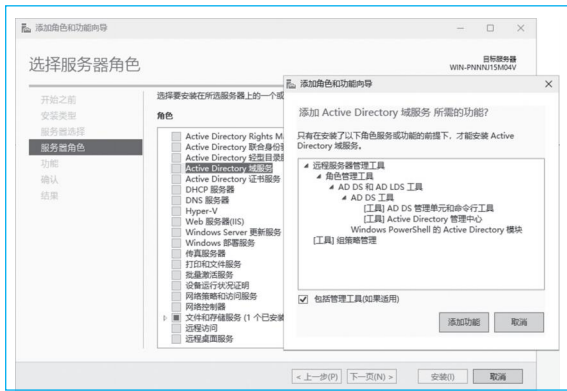


图 3-3 “选择服务器角色” 页面

持续单击“下一页”按钮，直到进入图 3-4 所示的“确认安装所选内容”页面。单击“安装”按钮开始安装，安装完成后显示图 3-5 所示的页面，提示“需要配置，已在 Server1 上安装成功”，选择“将此服务器提升为域控制器”选项，单击“关闭”按钮即可。

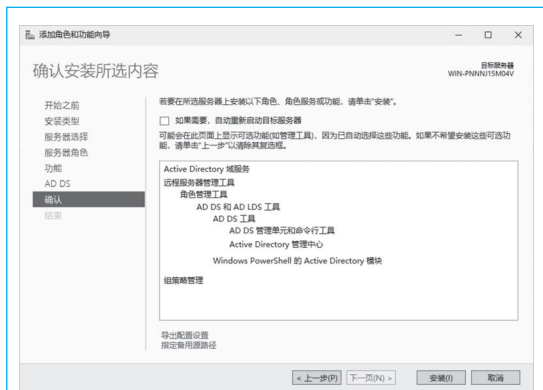


图 3-4 “确认安装所选内容” 页面

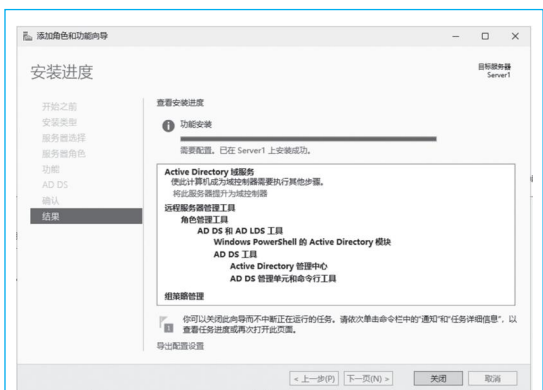


图 3-5 安装完成



若在图 3-5 所示页面中单击“关闭”按钮前未进行配置，可以在图 3-6 所示“服务器管理器·仪表板”页面上方单击旗帜图标，选择“将此服务器提升为域控制器”选项进行配置。



图 3-6 单击旗帜图标进行配置



在弹出的“Active Directory 域服务配置向导”窗口中选中“添加新林”单选按钮，并设置根域名，这里将根域名设置为 test.cn，如图 3-7 所示。

单击“下一页”按钮，进入“域控制器选项”页面，如图 3-8 所示，“林功能级别”和“域功能级别”保持默认（Windows Server 2025），设置目录服务还原模式（DSRM）密码。

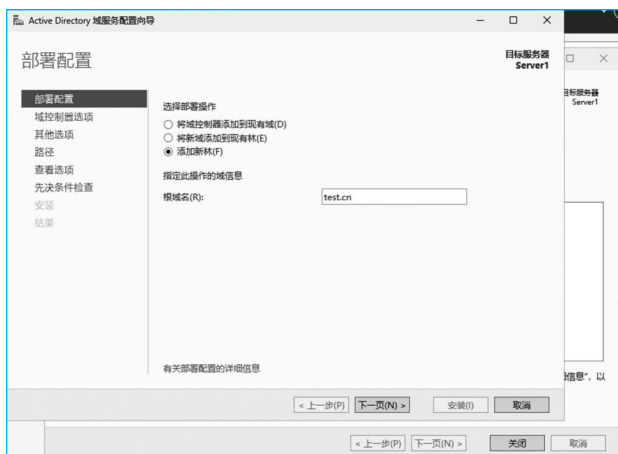


图 3-7 添加新林并设置根域名

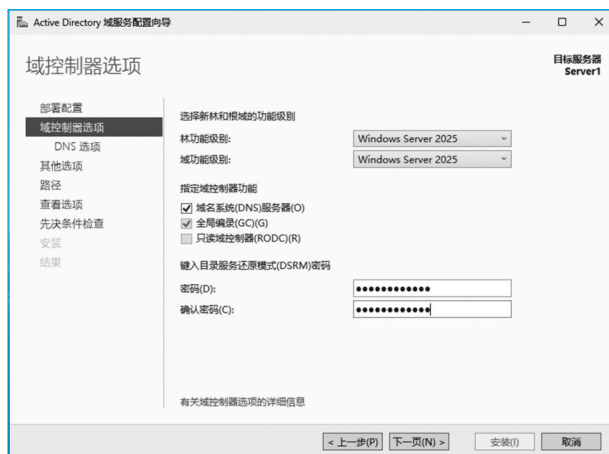


图 3-8 “域控制器选项”页面

单击“下一页”按钮，在“DNS 选项”页面（图 3-9）会提示错误，此错误不会影响后续操作，可以暂时忽略，单击“下一页”按钮。

进入“其他选项”页面，设置 NetBIOS 域名，这里保持默认，如图 3-10 所示。

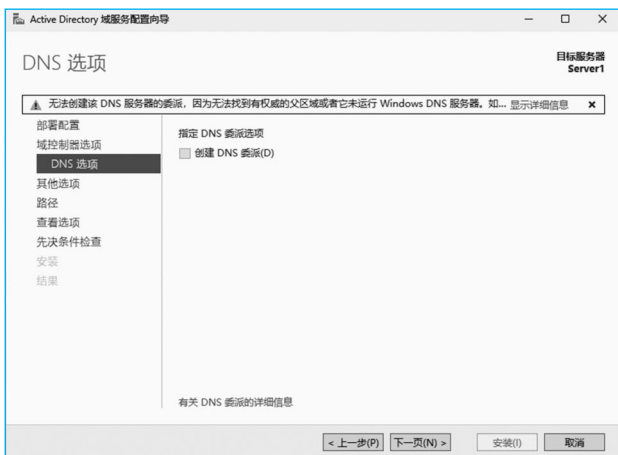


图 3-9 “DNS 选项”页面

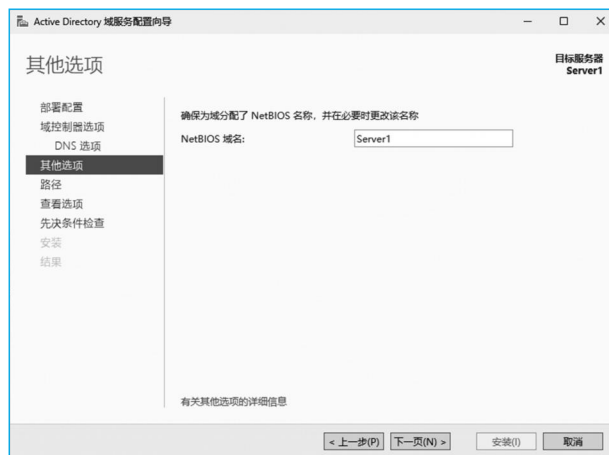


图 3-10 设置 NetBIOS 域名

单击“下一页”按钮，进入“路径”页面（图 3-11），可以在该页面设置 AD DS 数据库、日志文件和 SYSVOL 的位置，这里保持默认。

持续单击“下一页”按钮，进入“先决条件检查”页面（图 3-12），在该页面，系统会自动检查先决条件。如果检查通过，则单击“安装”按钮；如果检查不通过，则需要根据提示进行调整。单击“安装”按钮进行安装，安装完成后，系统会自动重启。

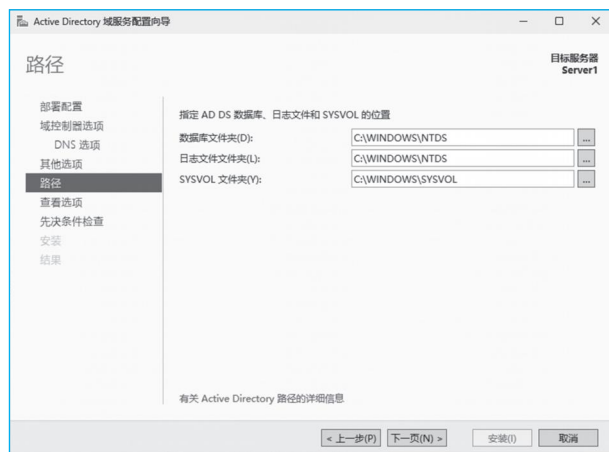


图 3-11 “路径” 页面

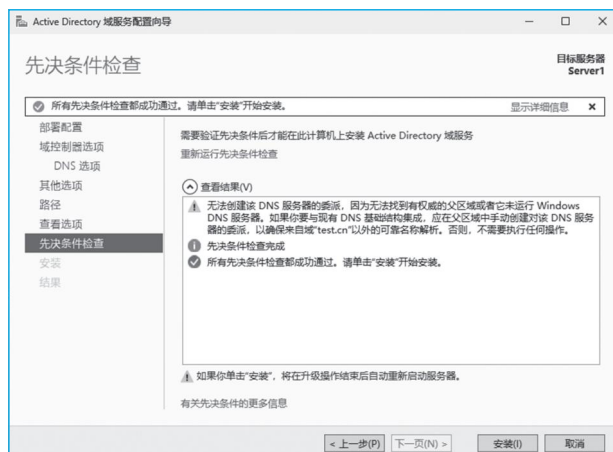


图 3-12 “先决条件检查” 页面

当服务器升级为域控制器后，必须使用域用户账户登录，如图 3-13 所示，域用户账户的格式为“用户账户 @ 域名”或“域名 \ 用户账户”。

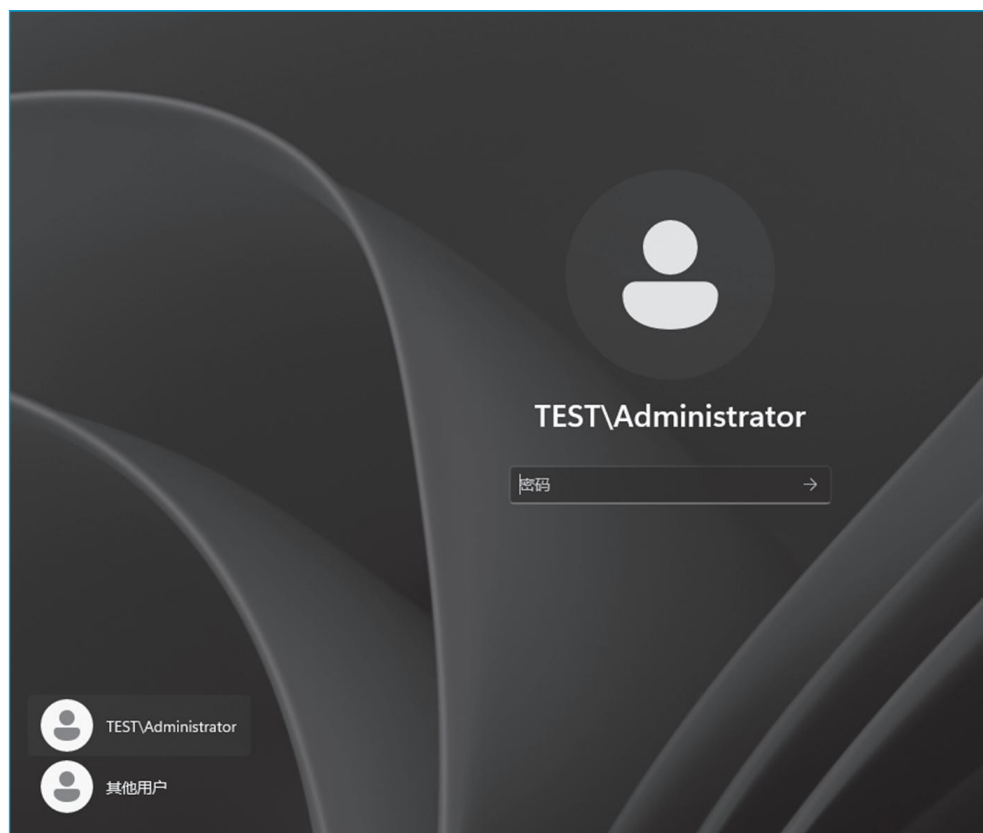


图 3-13 域用户账户登录界面

接下来验证 AD 服务器是否安装成功。

单击“开始”菜单，选择“设置”→“系统”→“系统信息”→“高级系统设置”选项，在弹出的“系统属性”对话框中选择“计算机名”选项卡，可以看到计算机全名和域均完成了修改，如图 3-14 所示。



图 3-14 计算机全名和域已修改

打开“服务器管理器”窗口，单击“工具”菜单，可以看到其中多出了与 Active Directory 相关的几个选项，如图 3-15 所示，表明该计算机已升级为域控制器。

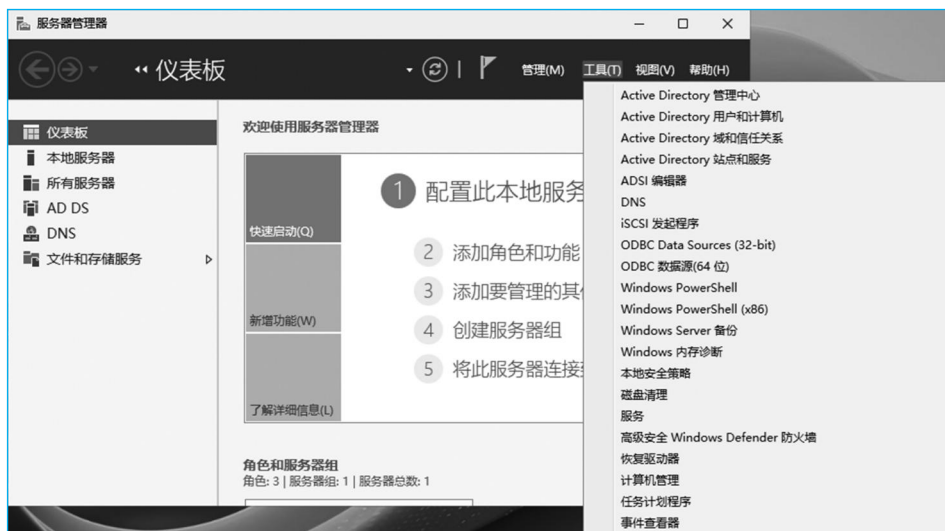


图 3-15 “工具”菜单增加与 Active Directory 相关的选项

### 知识拓展

当服务器升级为域控制器后，外部网络会断开，服务器就无法连接互联网了。这时可以设置 DNS 转发器来使服务器连接网络。

进行操作前需要为客户机 Server1 添加一个网络适配器，可以是 NAT 网络，也可以是桥接网络。



然后打开“服务器管理器”窗口，选择 DNS 选项，右侧会显示 Server1 的服务器信息，选中后右击，选择“DNS 管理器”选项，如图 3-16 所示。依次双击域名（Server1.test.cn）和“转发器”选项，如图 3-17 所示，在弹出的“Server1.test.cn 属性”对话框中可以看到新添加的网络适配器的 DNS，如图 3-18 所示。单击“编辑”按钮，添加一个公共 DNS 的 IP 地址，如 119.29.29.29 或 223.5.5.5，将下方的“在转发查询超时之前的秒数”更改为 1，如图 3-19 所示。依次单击“确定”按钮和“应用”按钮完成设置，此时即可使用 ping 命令测试网络连通性。



图 3-16 选择“DNS 管理器”选项

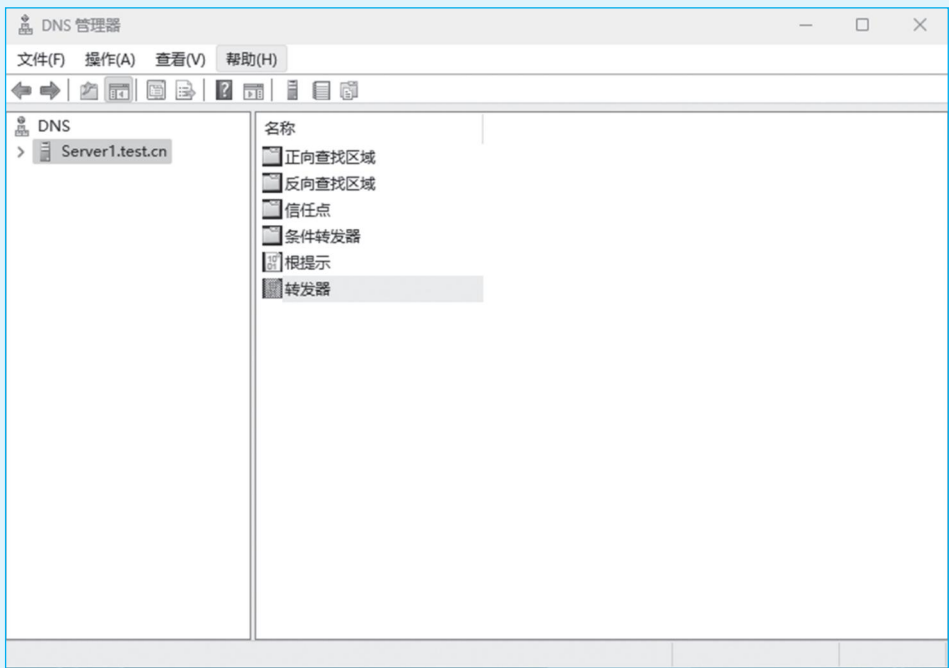


图 3-17 双击域名和“转发器”选项

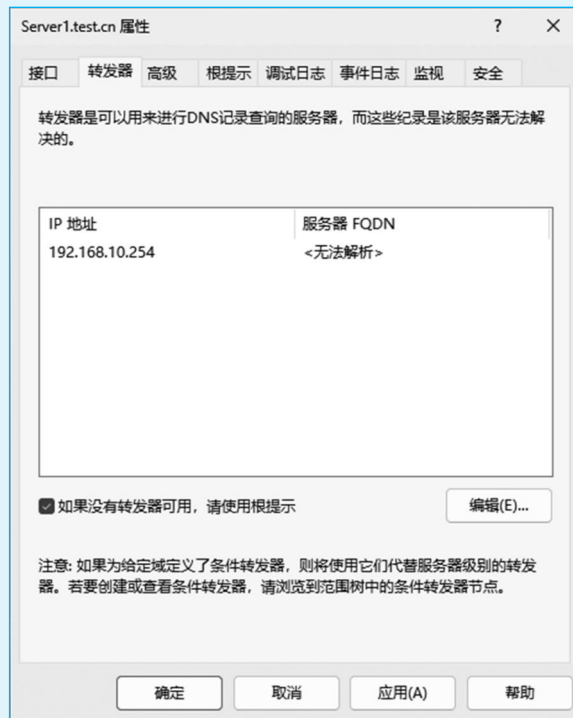


图 3-18 “Server1.test.cn 属性”对话框

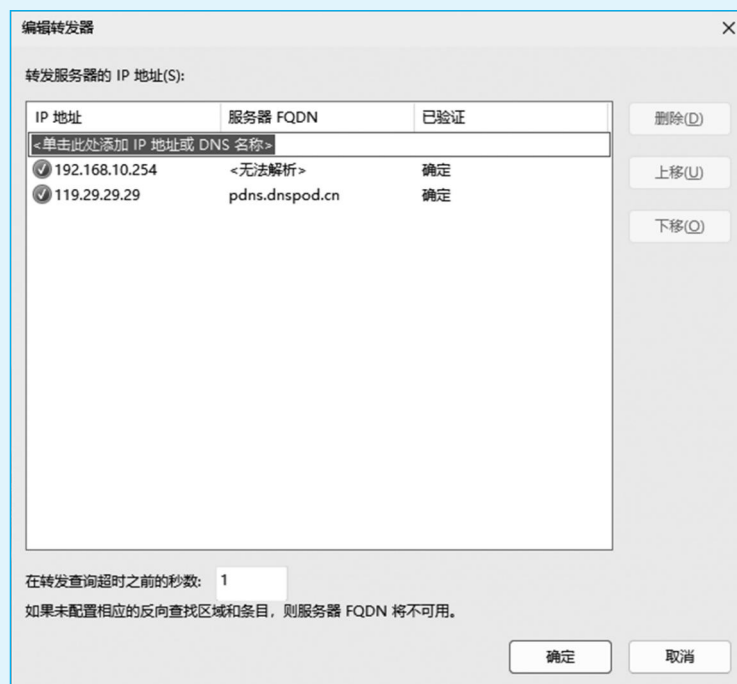


图 3-19 “编辑转发器”对话框



### 3.2.2

## 创建域用户与组织单位

### 1. 创建域用户

打开“服务器管理器”窗口，单击“工具”菜单，选择“Active Directory 用户和计算机”选项，在弹出的“Active Directory 用户和计算机”窗口中选择新用户所属的用户组（这里在 Users 用户组中新建用户），右击，选择“新建”→“用户”选项，如图 3-20 所示。

在弹出的“新建对象 - 用户”对话框中输入相关信息，其中“名”和“用户登录名”为必填项，完成后如图 3-21 所示。

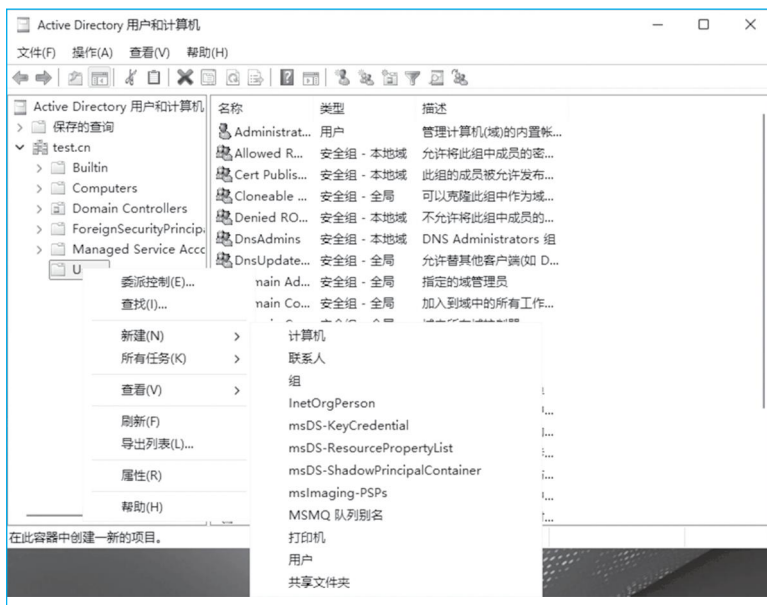


图 3-20 新建用户

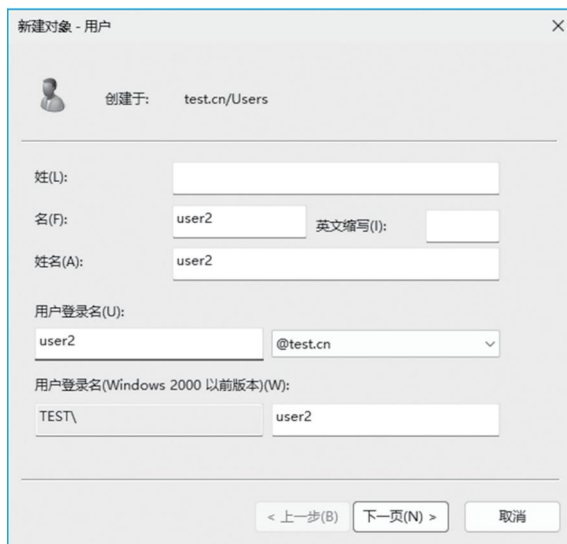


图 3-21 “新建对象 - 用户”对话框

单击“下一页”按钮，按照提示设置新建用户的密码，如图 3-22 所示，并取消勾选“用户下次登录时须更改密码”复选框。再单击“下一页”按钮可以查看新建用户的信息（图 3-23），单击“完成”按钮完成设置。

A screenshot of the 'New Object - User' dialog box in Windows Server. The 'Created by' field shows 'test.cn/school'. There are two password input fields: 'Password (P):' and 'Confirm Password (C):', both filled with dots. Below the password fields are four unchecked checkboxes: 'User must change password at next logon (M)', 'User cannot change password (S)', 'Password never expires (W)', and 'Account is disabled (O)'. At the bottom are three buttons: '< Back (B)', 'Next (N) >', and 'Cancel'. A mouse cursor is hovering over the 'Next (N) >' button.

图 3-22 设置密码



注意

经测试，Windows Server 2025 Datacenter 24H2 在新建用户时需要取消勾选“用户下次登录时须更改密码”复选框，否则使用新建的域用户时无法登录服务器，也无法修改密码。

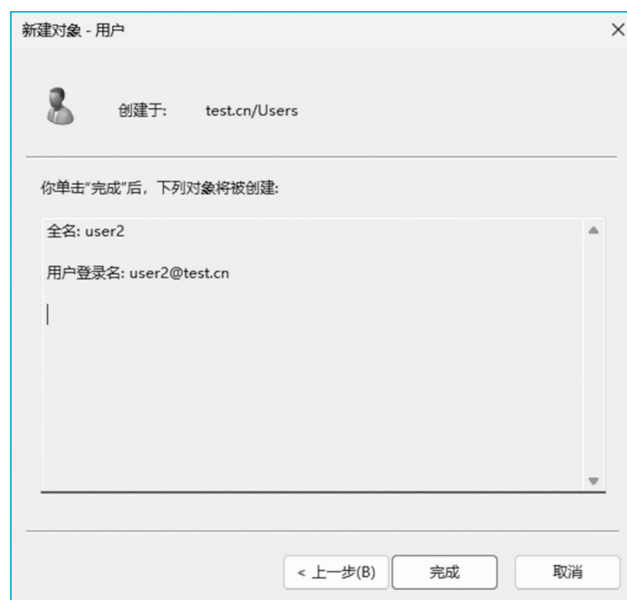
A screenshot of the 'New Object - User' dialog box in Windows Server, showing the 'Next' step. The 'Created by' field shows 'test.cn/Users'. Below the header, it says '你单击“完成”后，下列对象将被创建：' (After you click 'Finish', the following objects will be created:). There are two text boxes: 'Full name: user2' and 'User logon name: user2@test.cn'. At the bottom are three buttons: '< Back (B)', 'Finish', and 'Cancel'.

图 3-23 新建用户的信息





## 2. 创建组织单位

打开“服务器管理器”窗口，单击“工具”菜单，选择“Active Directory 用户和计算机”选项，在弹出的“Active Directory 用户和计算机”窗口中右击域名（test.cn），选择“新建”→“组织单位”选项，如图 3-24 所示。

在弹出的“新建对象 - 组织单位”对话框中输入组织单位的名称，如图 3-25 所示。

单击“确定”按钮即可完成新建，如图 3-26 所示。

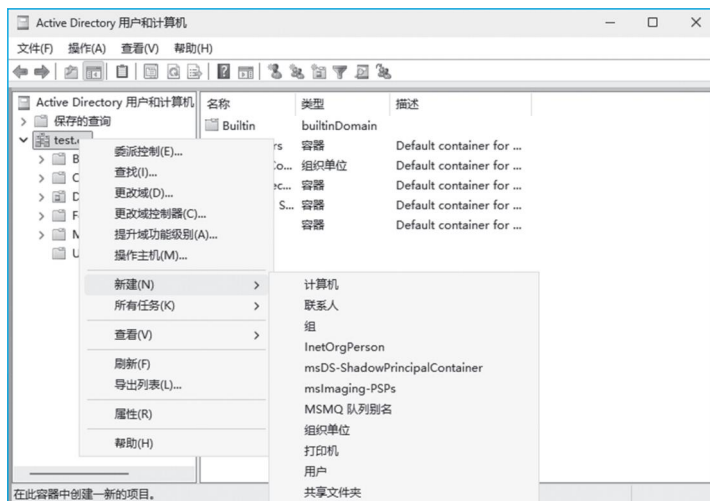


图 3-24 新建组织单位

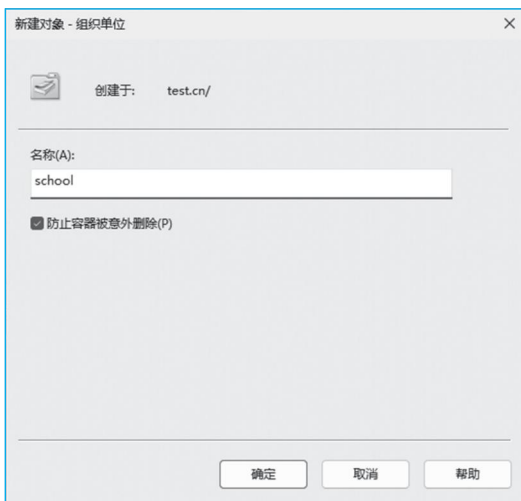


图 3-25 输入组织单位的名称

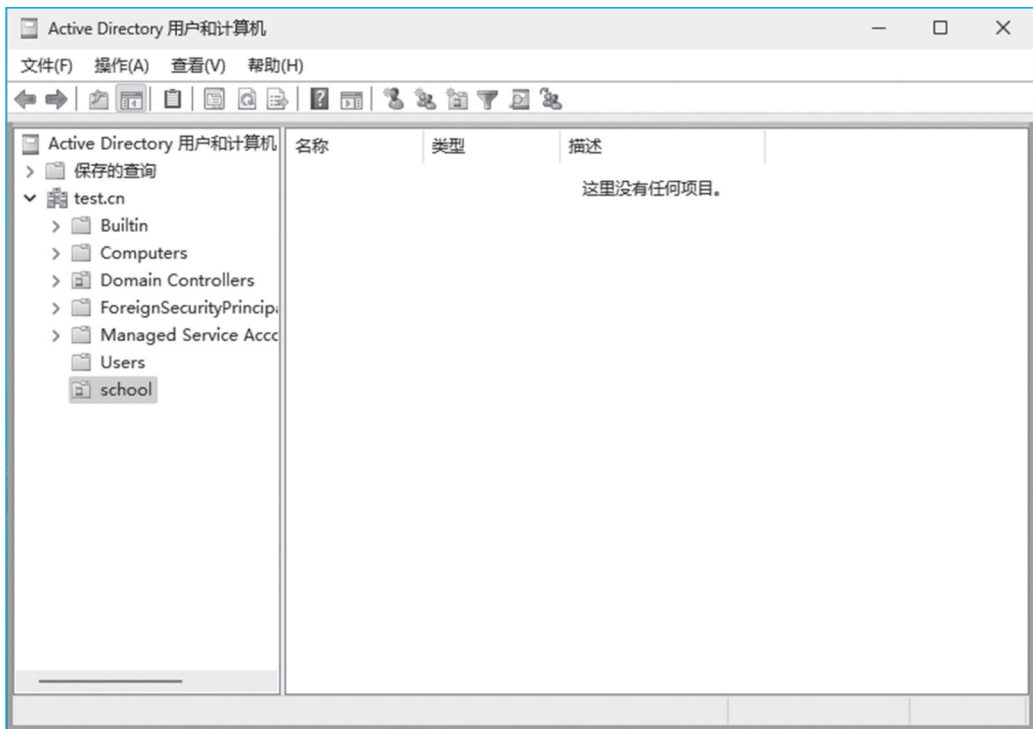


图 3-26 新建完成

## 知识拓展

按照默认选项添加的组织单位是不能随意删除的（默认勾选“防止对象被意外删除”复选框），如需删除，需先取消勾选该复选框。

首先在“Active Directory 用户和计算机”窗口中的空白处右击，选择“查看”→“高级功能”选项，如图 3-27 所示。

选择要删除的组织单位，如 school，右击并选择“属性”选项，在弹出的“school 属性”对话框的“对象”选项卡中，如图 3-28 所示，取消勾选“防止对象被意外删除”复选框，单击“确定”按钮完成，此时 school 组织单位即可被正常删除。

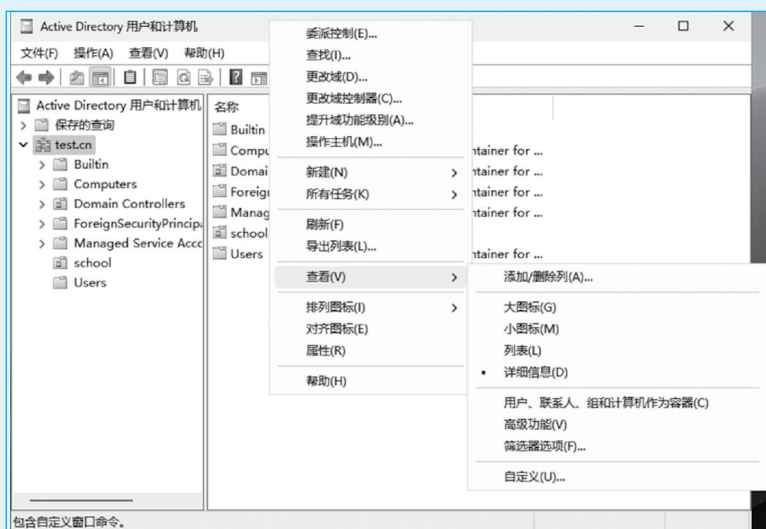


图 3-27 查看高级功能



图 3-28 “school 属性”对话框的“对象”选项卡

## 3.2.3

## 客户端计算机加域操作

启动另一台服务器 Server2，将 Server2 的 IP 地址设置为 192.168.10.200，子网掩码设置为 255.255.255.0，网关设置为 192.168.10.254，DNS 设置为 192.168.10.100（指向域控制器）。



注意

此时的 Server1 和 Server2 虚拟机均处于 VMware 的 NAT 网络模式下。

单击“开始”菜单，选择“设置”→“系统”→“系统信息”选项，在弹出的“系统属性”对话框中选择“计算机名”选项卡，单击“更改”按钮，将计算机名更改为 Server2，选中“隶属于”下的“域”单选按钮，输入“test.cn”，单击“确定”按钮，如图 3-29 所示。



加入域操作



图 3-29 更改计算机名及加入域

在弹出的“Windows 安全中心”对话框（图 3-30）中输入 Server 的域账户及密码，单击“确定”按钮，加入成功会弹出提示（图 3-31）。



图 3-30 “Windows 安全中心”对话框



图 3-31 成功加入 test.cn 域提示

## 知识拓展

在 Windows 系统中，域名和用户名不区分大小写。例如，TEST 域和 test 域是同一个域，administrator 和 Administrator 是同一个用户。



注意

克隆后的虚拟机的 SID 与源虚拟机的 SID 相同，两个 SID 相同的计算机在加入同一个域时会出现错误，如图 3-32 所示。如果 Server2 是 Server1 在提升为域控制器前克隆的，则需要在加入 test.cn 域之前修改 Server2 的 SID。



重置克隆虚拟机的 SID

图 3-32 SID 相同导致的错误

搜索并打开 command Prompt (可以在“开始”菜单旁的搜索框中搜索, 也可以按“Ctrl+R”组合键打开“运行”对话框, 输入“cmd”并按 Enter 键), 输入“whoami/user”命令, 系统会返回用户名和 SID。此时输入“cd c:\windows\system32\sysprep”命令, 在弹出的“系统准备工具 3.14”对话框中勾选“通用”复选框, “系统清理操作”保持默认选项, 如图 3-33 所示, 单击“确定”按钮完成设置。

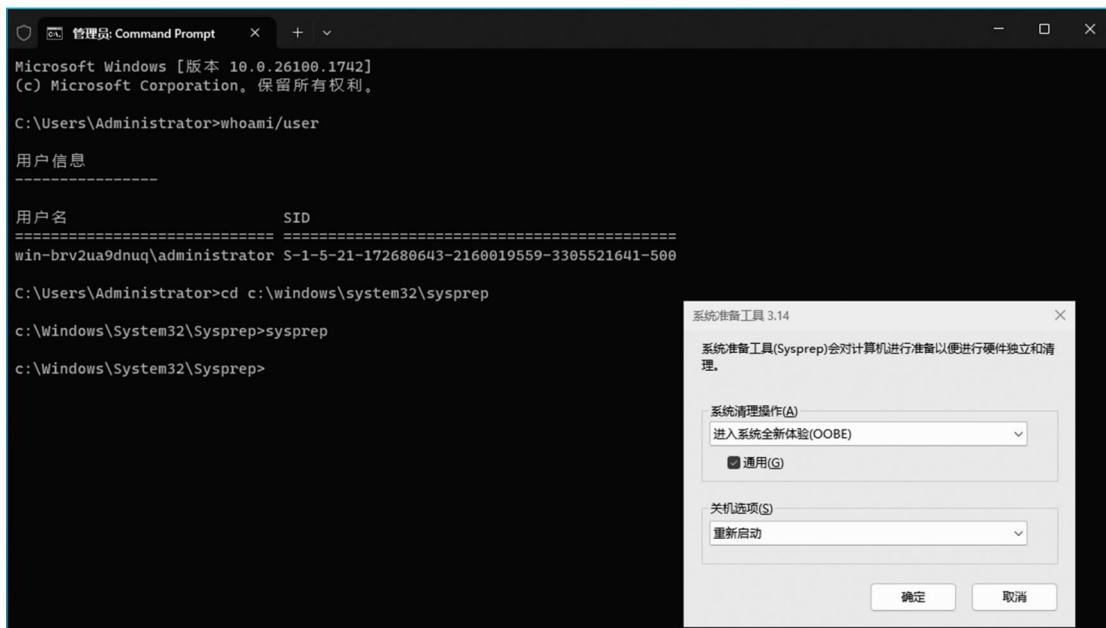


图 3-33 “系统准备工具 3.14”对话框



系统弹出“Sysprep 正在工作...”对话框(图 3-34),操作完成后,系统会自动重启计算机。

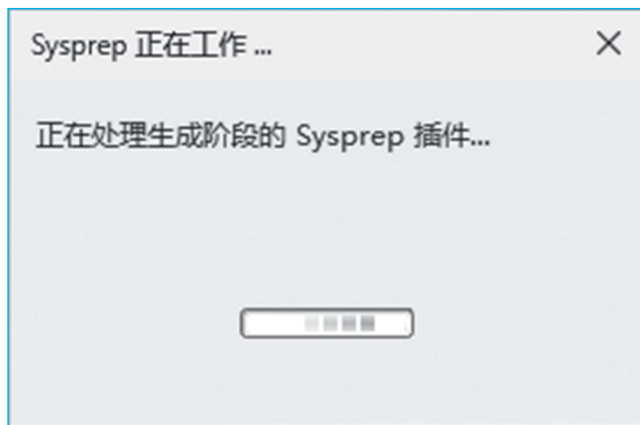


图 3-34 “Sysprep 正在工作”对话框

计算机重启后需要重新设置或确认相关信息,如图 3-35 所示。

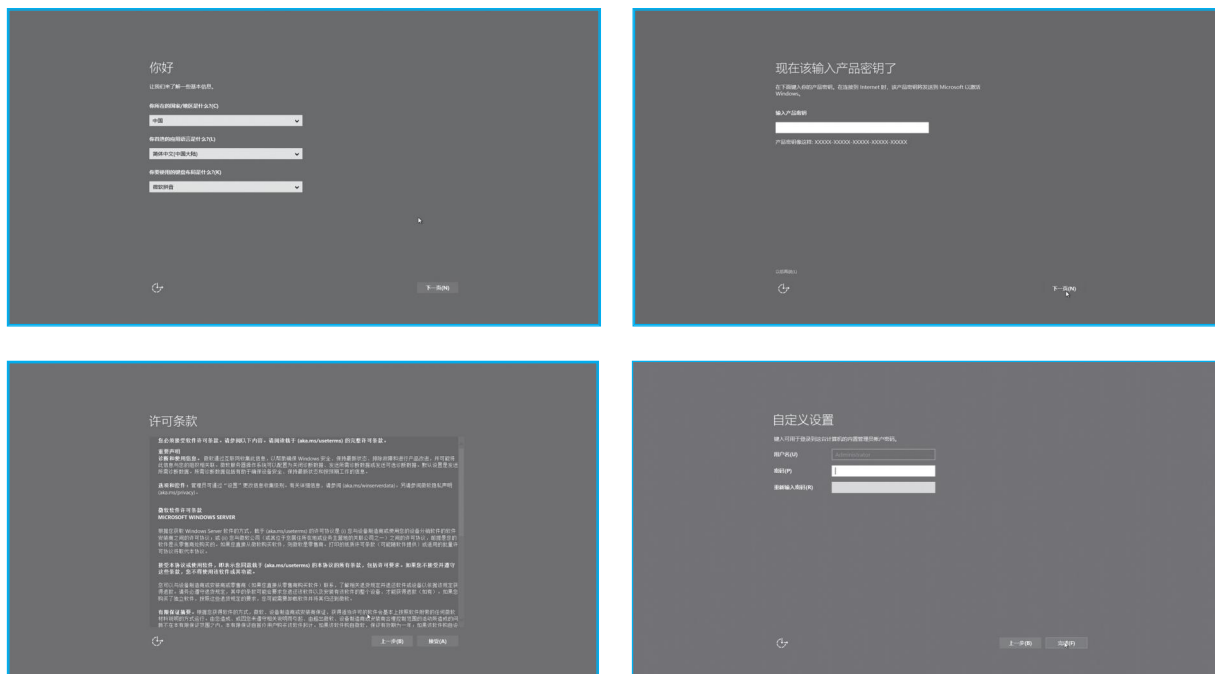


图 3-35 计算机重启后重新设置或确认相关信息

完成后再次输入“whoami/user”命令查询 SID,与图 3-33 进行对比,可以发现 SID 发生了变化,如图 3-36 所示。

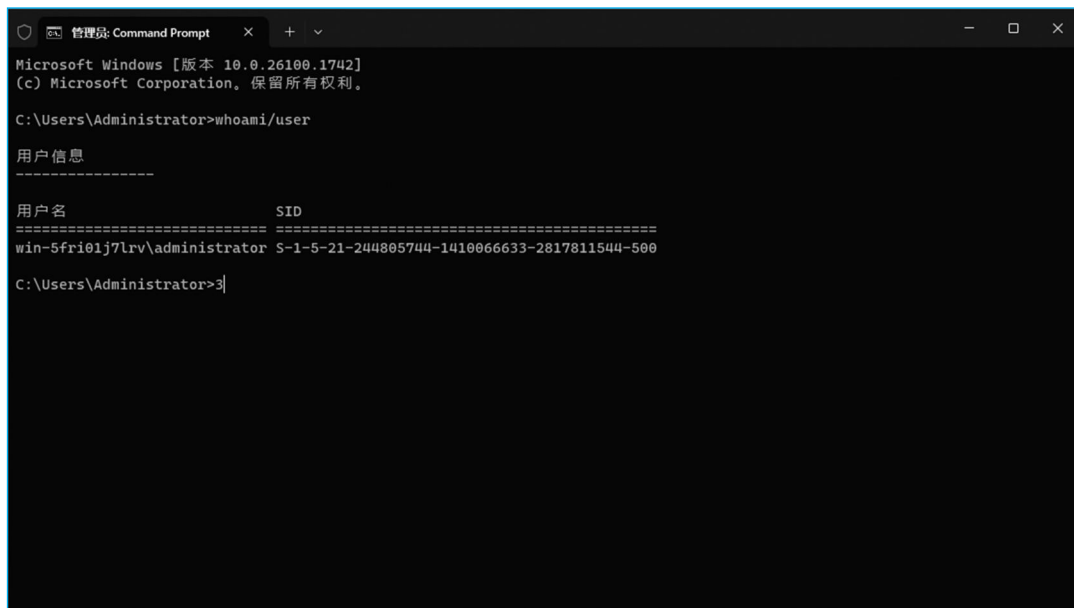


图 3-36 更改后的 SID

成功加入 test.cn 域后，在 Server 的“服务器管理器”窗口中，单击“工具”菜单，选择“Active Directory 用户和计算机”选项，在弹出的“Active Directory 用户和计算机”窗口中选择 Computers 选项即可看到刚刚加入 test.cn 域的 Server2，如图 3-37 所示。

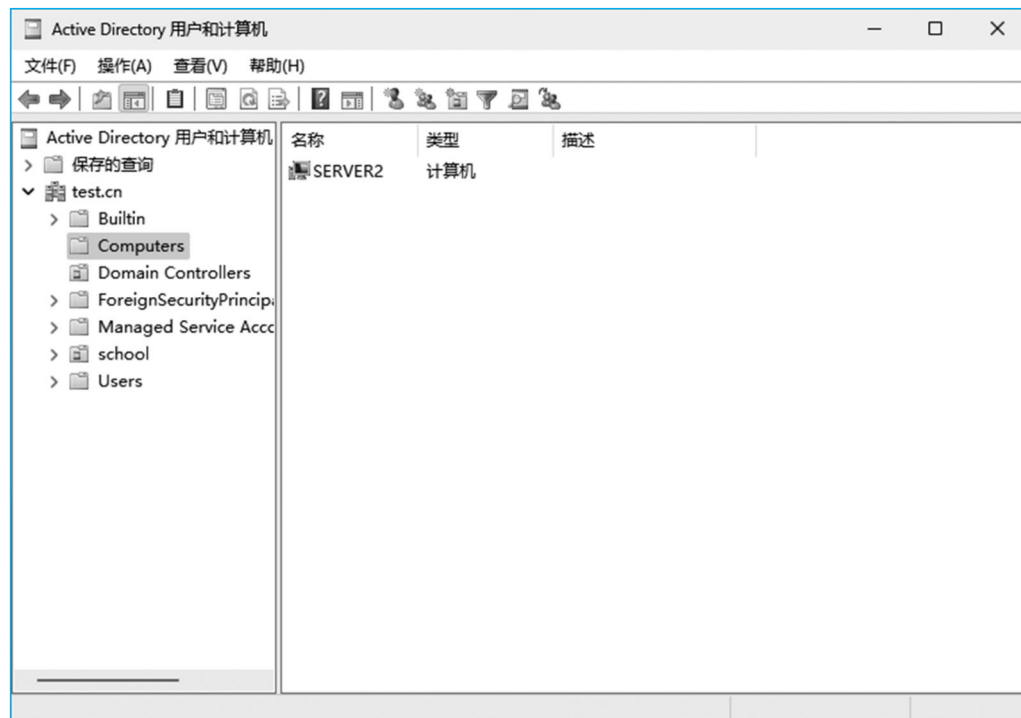


图 3-37 刚刚加入 test.cn 的 Server2



## 3.3

## 本地安全策略与组策略

### 3.3.1

### 配置密码策略

#### 知识拓展

本地安全策略是 Windows 系统中用于配置和管理计算机安全设置的核心工具，主要面向管理员控制访问权限与风险防护。通过账户策略（如密码复杂度、账户锁定规则）、审核策略（记录登录行为与系统事件）、用户权限分配（限制特殊权限）及安全选项（禁用匿名共享等），强化系统防护并满足合规需求。

打开“服务器管理器”窗口，单击“工具”菜单，选择“本地安全策略”选项，如图 3-38 所示。在弹出的“本地安全策略”窗口左侧导航栏中选择“安全设置”→“账户策略”→“密码策略”选项，可以双击想要修改的策略，按要求进行修改。这里双击“最小密码长度审核”选项，将“新密码长度小于以下值时记录审核事件”修改为 8 字符，如图 3-39 所示，单击“确定”按钮完成设置。

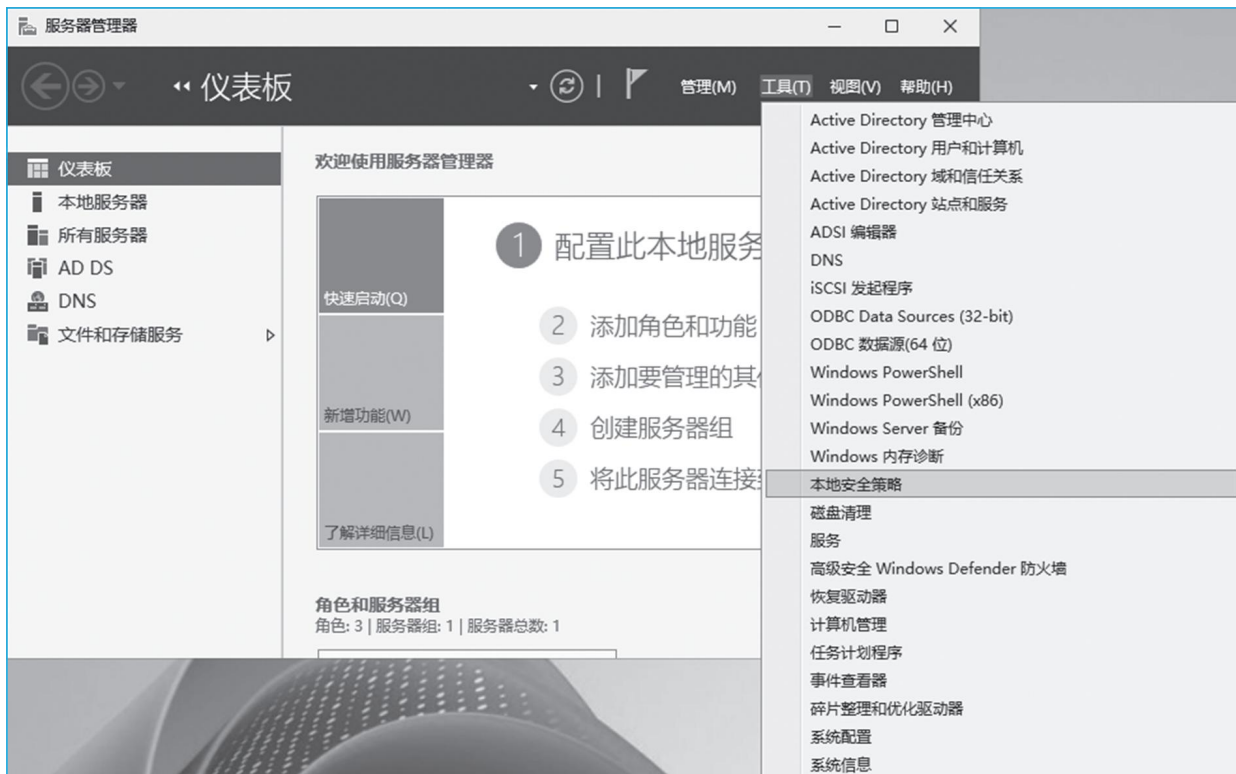


图 3-38 选择“本地安全策略”选项



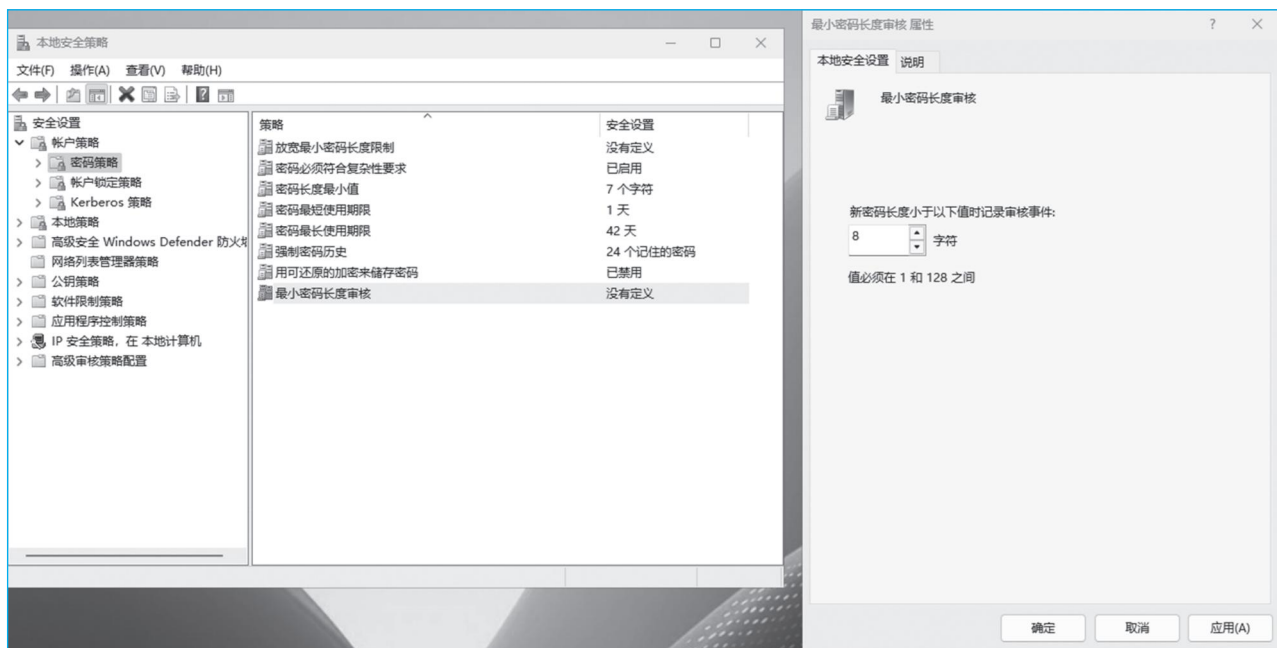


图 3-39 设置最小密码长度审核

## 3.3.2



## 部署软件分发策略

## 知识拓展

组策略是 Windows 系统中的一种管理工具，主要用于集中管理和配置网络中的用户和计算机设置。通过组策略，管理员可以设置针对特定用户组或计算机组的统一策略，例如，限制软件安装、控制网络访问权限、部署系统更新或配置安全选项等。它基于 AD 域服务实现，以组策略对象（GPO）的形式关联到站点、域或组织单位（OU），从而自动化运行设置的组策略，提升管理效率并保障系统安全性。

在部署软件分发策略前，需要准备分发的软件安装文件，只支持 msi 格式的安装文件，这里使用 7-Zip 的安装文件。

在 C 盘创建一个 share 文件夹，将 7-Zip 的安装文件放在该文件夹中。右击 share 文件夹，选择“属性”选项，如图 3-40 所示。

在弹出的“share 属性”对话框中单击“高级共享”按钮，在弹出的“高级共享”对话框中勾选“共享此文件夹”复选框，单击“权限”按钮，在弹出的“share 的权限”对话框中确认 Everyone 用户组拥有读取权限，如图 3-41 所示。依次单击三个对话框中的“确定”按钮，完成文件夹的共享。



配置软件分发策略

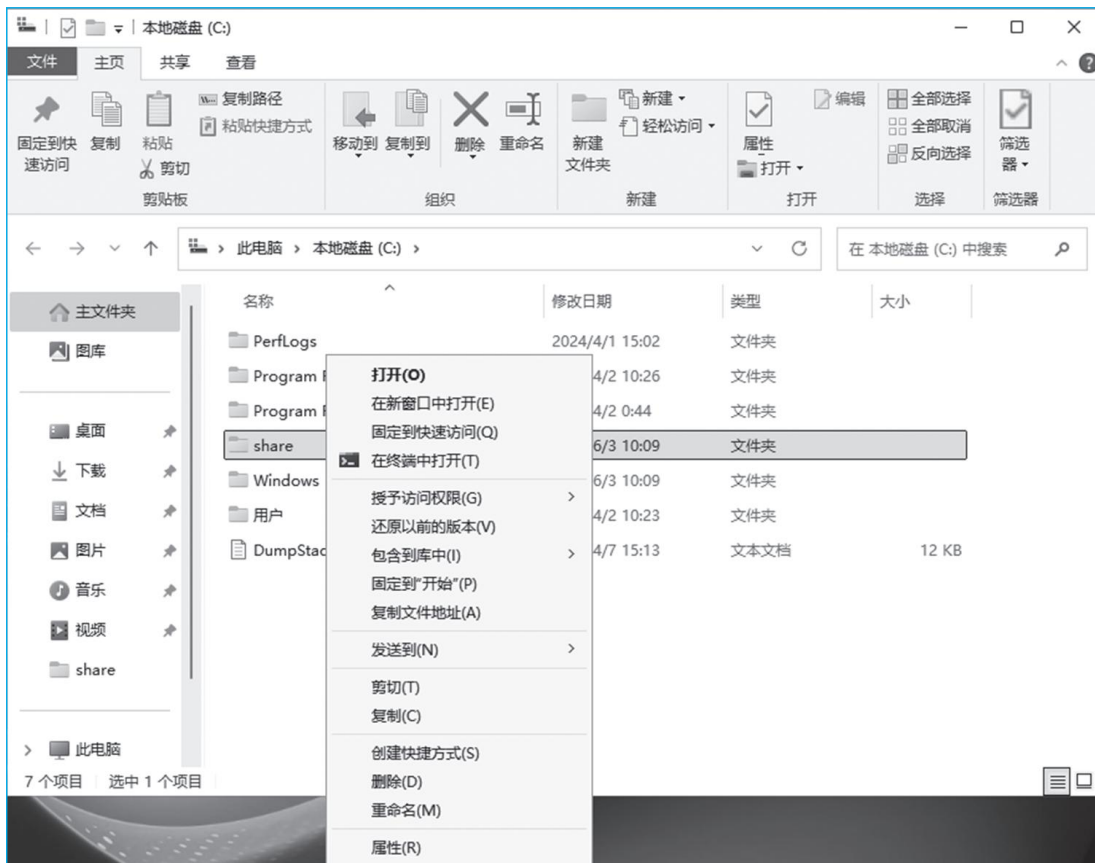


图 3-40 选择“属性”选项

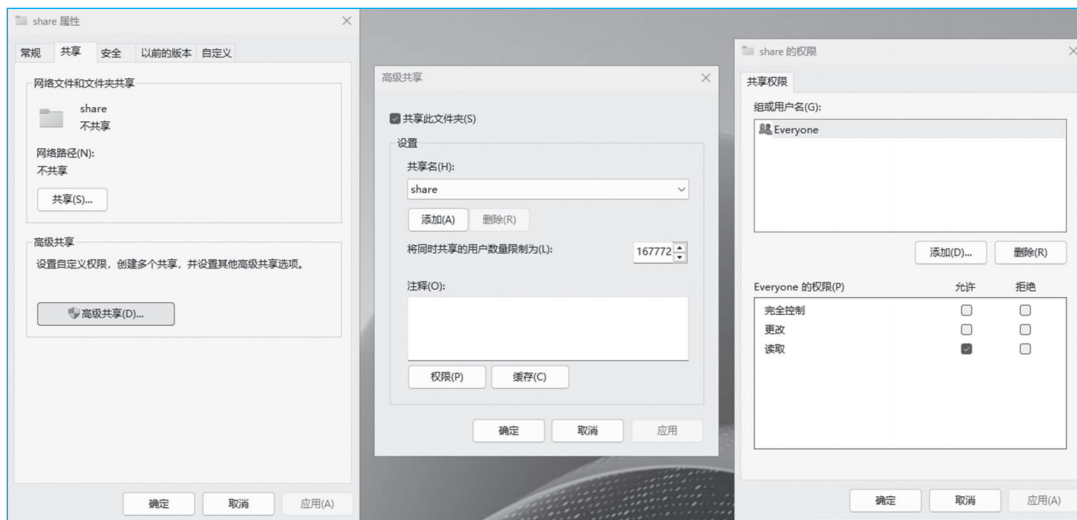


图 3-41 完成文件夹的共享

文件夹共享完成后，记录共享文件夹的网络路径。这里共享文件夹的网络路径为“\\SERVER1\share”，如图 3-42 所示。

打开“服务器管理器”窗口，单击“工具”菜单，选择“Active Directory 用户和计算机”选项。在弹出的“Active Directory 用户和计算机”窗口中新建 school 组织单位，并在 school 组织单位中创建

user2 用户，如图 3-43 所示。



图 3-42 共享文件夹的网络路径

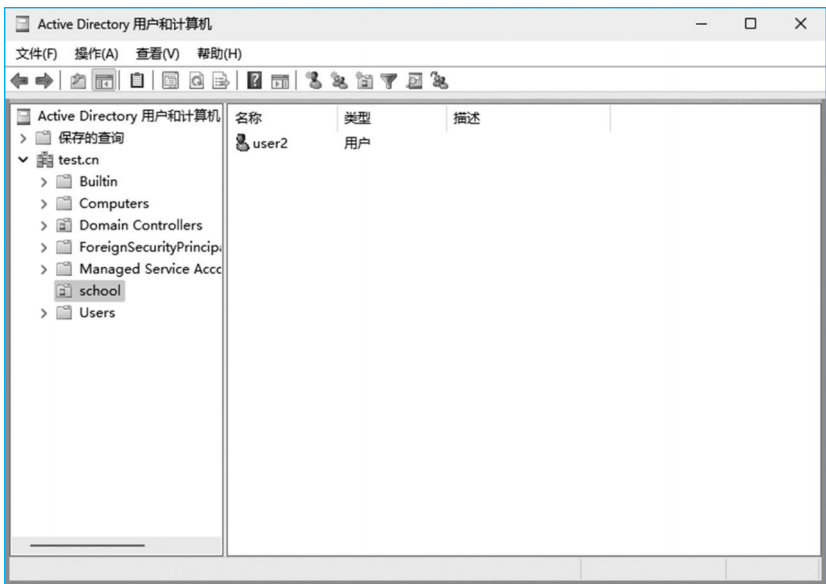


图 3-43 school 组织单位及 user2 用户

打开“服务器管理器”窗口，单击“工具”菜单，选择“组策略管理”选项，在弹出的“组策略管理”窗口左侧导航栏中选择“林：test.cn”→“域”→test.cn→school 选项，右击，选择“在这个域中创建 GPO 并在此处链接”选项，如图 3-44 所示。

在弹出的“新建 GPO”对话框中设置名称，如图 3-45 所示，单击“确定”按钮完成新建。

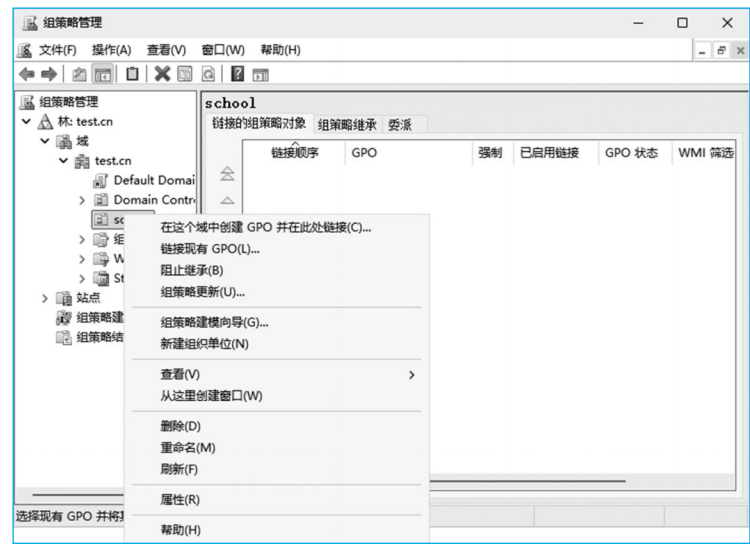


图 3-44 新建 GPO

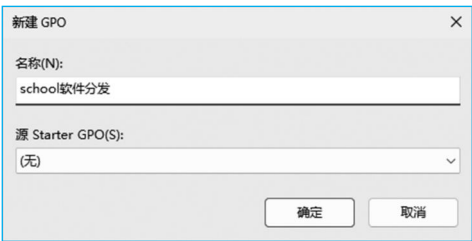


图 3-45 “新建 GPO”对话框

在“组策略管理”窗口左侧导航栏中选择“school 软件分发”选项（刚刚新建的 GPO），右击，选择“编辑”选项，如图 3-46 所示。

在弹出的“组策略管理编辑器”窗口左侧导航栏中选择“用户配置”→“策略”→“软件设置”→“软件安装”选项，右击，选择“新建”→“数据包”选项，如图 3-47 所示。

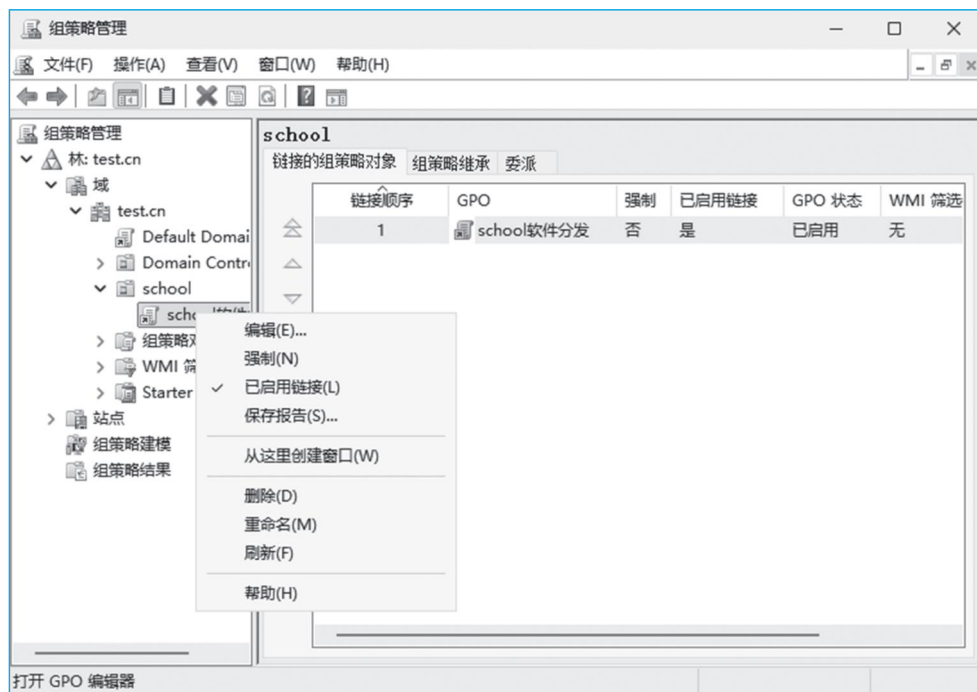


图 3-46 选择“编辑”选项

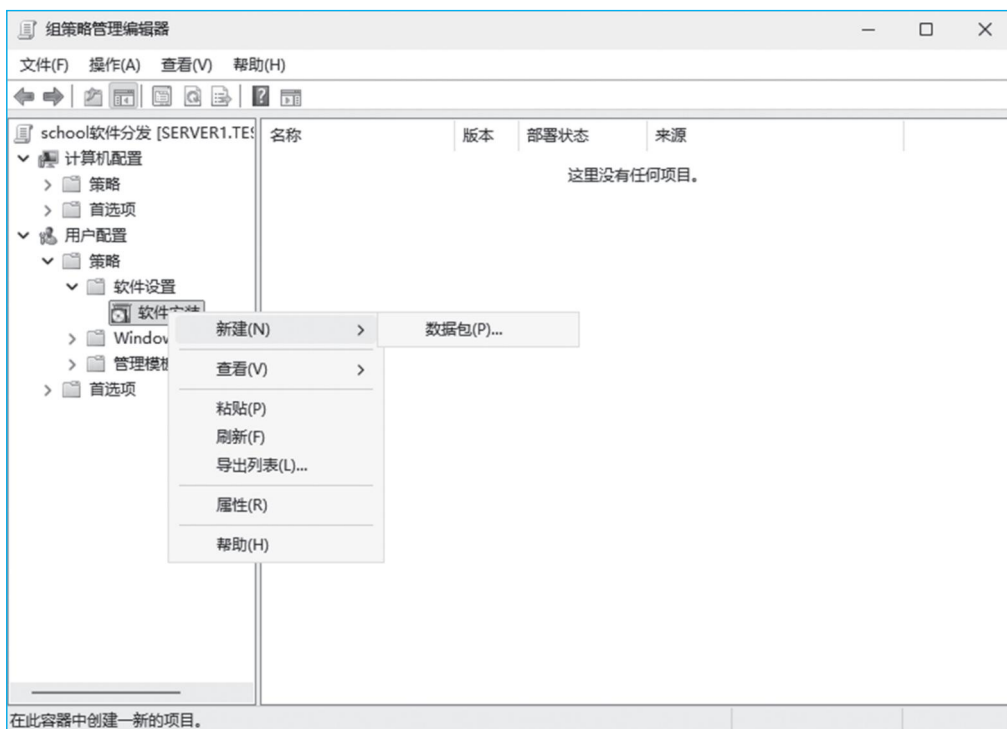


图 3-47 新建数据包

系统弹出“打开”窗口，在地址栏输入共享文件夹的网络路径（\\Server1\share）并按 Enter 键，选择 7-Zip 安装文件，如图 3-48 所示，单击“打开”按钮。

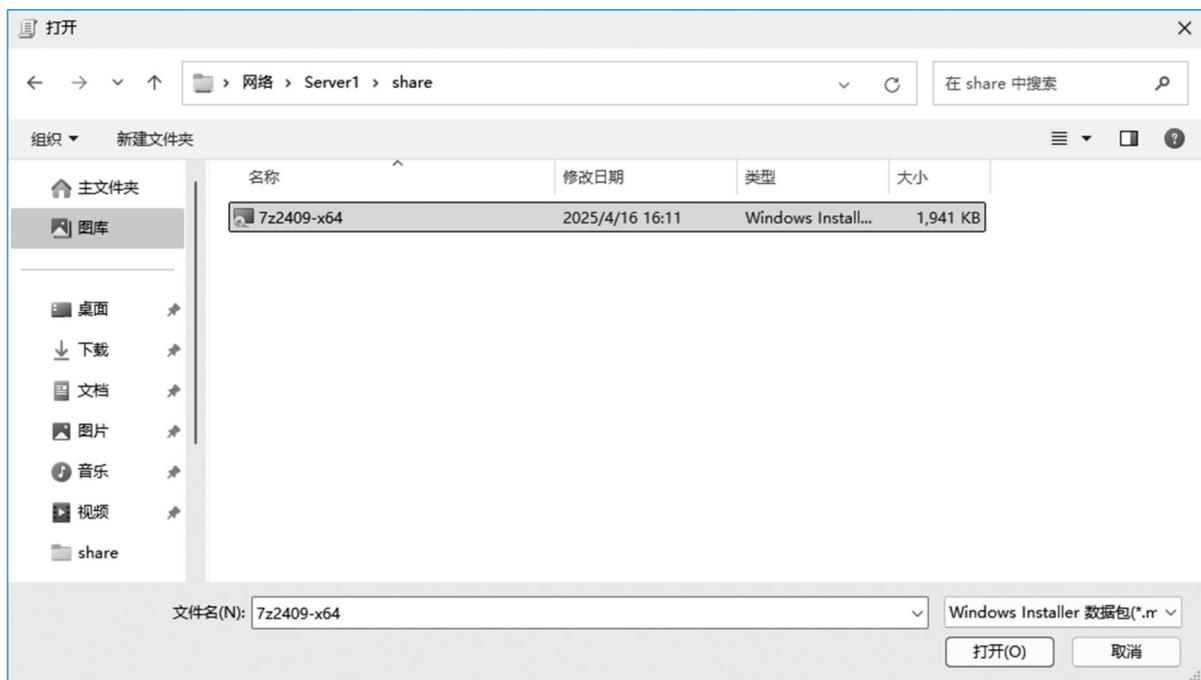


图 3-48 选择 7-Zip 安装文件

在弹出的“部署软件”对话框中选中“已分配”单选按钮，如图 3-49 所示，单击“确定”按钮。在“组策略管理编辑器”窗口中选择新建好的数据包，右击，选择“属性”选项，如图 3-50 所示。

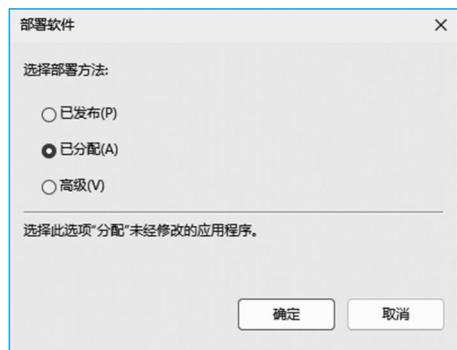


图 3-49 “部署软件”对话框

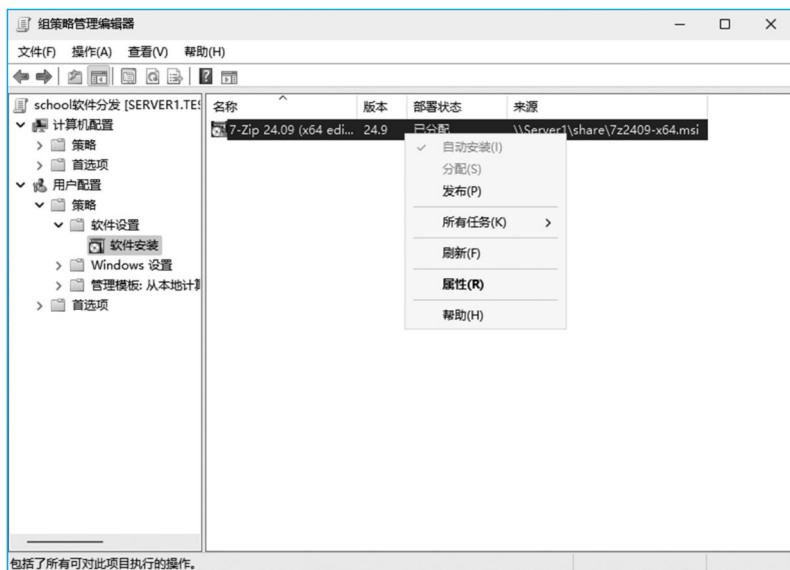


图 3-50 选择“属性”选项

在弹出的“7-Zip 24.09 (x64 edition) 属性”对话框中选择“部署”选项卡，勾选“在登录时安装此应用程序”复选框，如图 3-51 所示，单击“确定”按钮。

按“Win+R”组合键打开“运行”对话框，输入“cmd”并按 Enter 键。在弹出的命令行窗口中输入“gpupdate /force”并按 Enter 键对组策略进行强制更新，如图 3-52 所示。



注意

组策略在设置完成后并非立即更新，系统会按照特定逻辑更新。为了方便后续的测试，这里使用了强制更新命令对组策略进行更新。



图 3-51 勾选“在登录时安装此应用程序”复选框

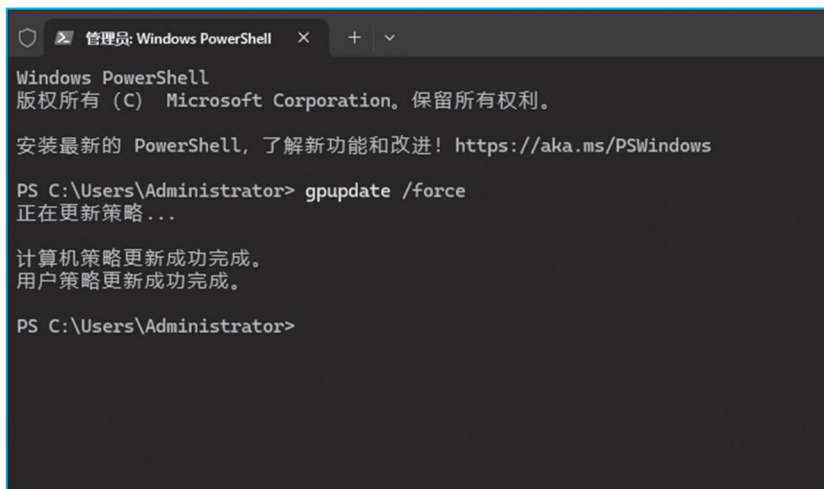


图 3-52 更新组策略

使用创建好的 user2 用户登录 Server2 虚拟机，在登录界面可以看到正在安装托管软件的提示，如图 3-53 所示。

登录后等待片刻，单击“开始”菜单即可看到安装好的 7-Zip 软件，如图 3-54 所示。

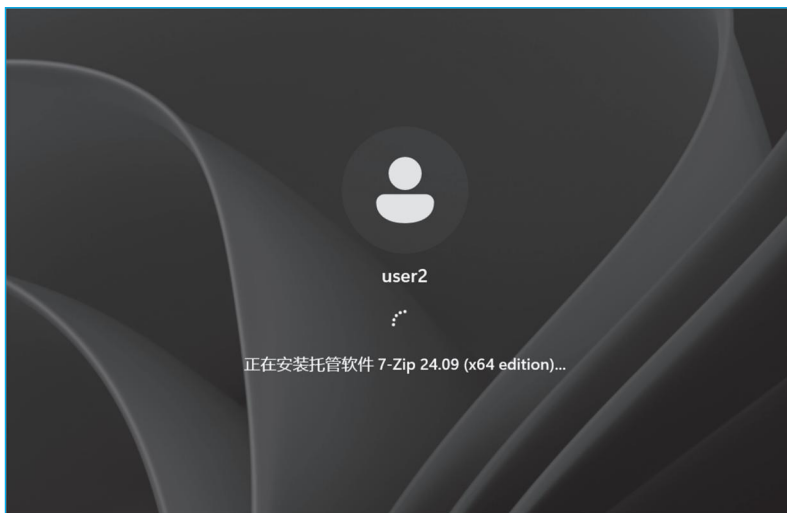


图 3-53 正在安装托管软件的提示

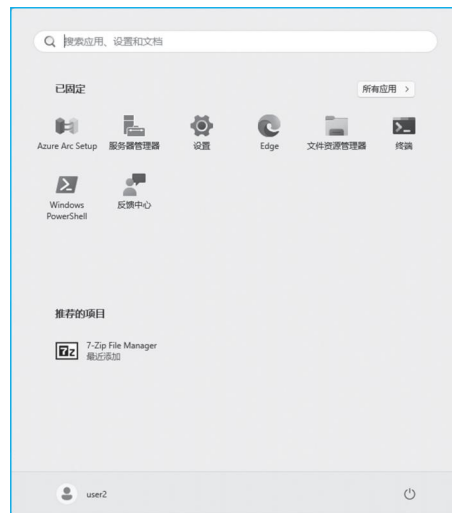


图 3-54 7-Zip 软件已安装

[项目实训]

升级为域控制器并部署软件分发策略

1. 项目环境
- 现有一台 Windows Server 2025 服务器（虚拟机），主机名为 Server1，还有一台 Windows 11 计算机（虚拟机），主机名为 win11-1。目前两台虚拟机只进行了系统初始化。
2. 实训要求
- (1) 将 Server1 升级为域控制器。

(2) 将 win11-1 加入 Server1 所在的域中。

(3) 创建组织单位和域用户。

(4) 为新建的组织单位部署软件分发策略（部署的软件自选）。

(5) 测试部署的软件分发策略能否正常运行。

[项目评价]

评价内容	学生自评	小组互评	教师评价
能够将 Server1 升级为域控制器	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
能够将 win11-1 加入域中	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
能够创建组织单位和域用户	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆
能够部署软件分发策略	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆

[拓展阅读]

AI 与操作系统深度融合将改变交互方式，提升智能化水平

2024 年 12 月 18 日，第十五届新华网教育论坛“新质生产力”人才创新培养分论坛在北京举办。首场圆桌对话环节，由天津大学人工智能学院讲席教授、卓越工程师学院执行院长作为主持人，对话鸿蒙系统创始人、深开鸿首席执行官（以下简称专家）等嘉宾，围绕“人工智能浪潮对就业的影响及应对策略”展开讨论。

近年来，人工智能等技术的迅猛发展，在生成式人工智能引领下，全球对新一代人工智能的关注度再次攀升。

专家认为，人工智能发展势不可挡，将对各行各业产生深远影响，但人工智能至少在未来二三十年不太可能完全替代人。专家认为，“应该理性看待人工智能等技术手段，技术本身只是工具，关键在于我们如何使用这些工具来解决问题。”

专家用鸿蒙操作系统举例，他表示，鸿蒙操作系统是一个颇具革新性的技术成果。鸿蒙操作系统与传统操作系统相比，有着两大显著区别。首先，鸿蒙系统几乎能够装载在所有类型的设备上，这打破了设备间沟通与协调的壁垒。在数字化、信息化进程中，“烟囱”问题一直困扰着各领域，即不同系统、





设备之间难以实现互通互联。而鸿蒙系统的这一特性，为设备间的无缝协同提供了可能，从而大大提高整体效率。其次，鸿蒙系统在设备协同工作时，能够作为一个统一的系统，为未来所有的 AI 应用提供高质量的数据。“我们构建的开源鸿蒙系统，能够赋能各种设备，将它们场景化地连接成一张感知网络。这张网络能够实时、准确、完备地将物理世界的所有变化以统一的数据格式表征出来，与 AI 模型实现自洽，从而进一步提升 AI 的智能化水平。”

此外，专家表示，他还在致力于推动 AI 与操作系统深度融合。“我相信，未来 AI 对人类影响最大的领域之一，将是改变我们与物理世界、数字世界的交互方式。这种改变将使人工智能真正普及到每个人、每个单位、每个组织。通过 AI 与操作系统的充分融合，我们在使用设备的过程中，AI 的能力将自然而然地发挥作用，而不再仅仅是操作系统上的一个应用。这种深度融合将为我们带来更加便捷、智能的生活体验。”

“人类社会的发展始终伴随着替代前进的过程，例如，汽车替代马车，农业机械替代传统农耕。”对于技术的发展，专家认为人们过度强调了 AI 替代人类的可能性，“我们应该更加关注如何利用技术解决实际问题，而不是盲目追求各种概念。”他建议，当新技术出现时，如果发现它不能解决行业问题，可以忽略它；但如果能解决问题，就应该积极采纳，既不要忽视，也不要神化。“我们应实事求是地对待新技术，既看到其优点，也承认其局限性。”

尽管 AI 大模型的数量在不断增加，但高质量模型仍然相对稀缺。专家表示，高质量模型稀缺，源于缺乏优质数据。他用炒菜来比喻，“就如同炒菜需要好的原料，数据质量决定技术成果。”他认为，产业界和学界应冷静看待技术，重实际应用。“技术应解决过去难题或简化复杂问题。”

（资料来源：新华网，2024-12-19）