第七章

Windows Server 服务器

7.1 安装 Windows Sever 2019 标准版

7.1.1 实训环境

（1）VMware Workstation。

（2）组件需求：Server 2019 Standard 版本镜像。

7.1.2 实训内容

实训目标

掌握在物理机和虚拟机上安装 Server 2019 操作系统的方法。

◆ 实训 Windows Server 系统的安装

系统的安装需求：处理器至少 1.4HZ，64 位；支持 NX 或者 DEP；支持 CMPXCHG16B/LAHF/SAHF 与 PrefethtW；内存至少 512 MB，桌面安装不得少于 2 GB；硬盘最少 32 GB（不支持 IDE 硬盘）。

安装步骤如下：

（1）开启 VMware Workstation，单击“创建新的虚拟机”按钮，如图 7.1 所示。连续单击“下一步”按钮，完成虚拟机的创建。

（2）单击创建好的虚拟机名称，右键单击，在弹出的快捷菜单中选择“设置”选项，如图 7.2 所示。

（3）在“虚拟机设置”窗口中设置安装镜像文件的路径，如图 7.3 所示。

（4）设置网卡为桥接模式，如图 7.4 所示。

（5）单击启动虚拟机，经镜像引导进入安装界面，选择要安装的语言、时间和货

币格式、键盘和输入方法，单击“下一步”按钮，如图 7.5 所示。

（6）进入 Server 2019 的安装界面，单击“现在安装”按钮，如图 7.6 所示。

图 7.1　创建新的虚拟机

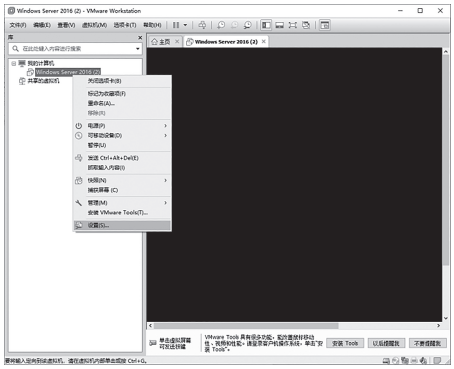

图 7.2　选择“设置”选项

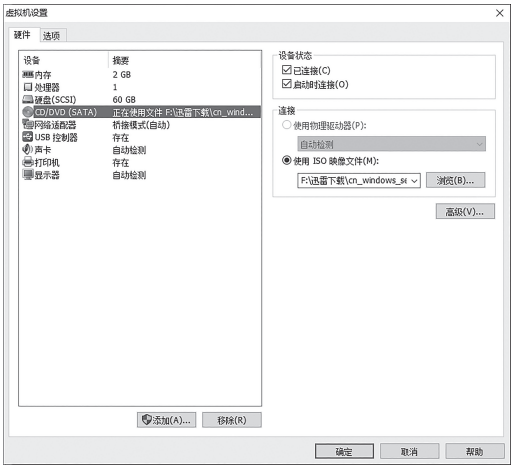

图 7.3　设置镜像文件路径

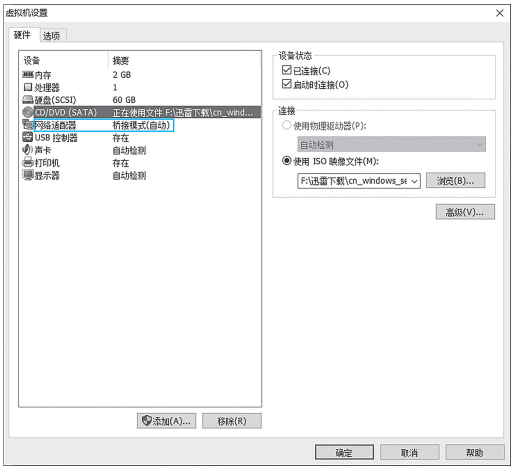

图 7.4　设置网卡为桥接模式

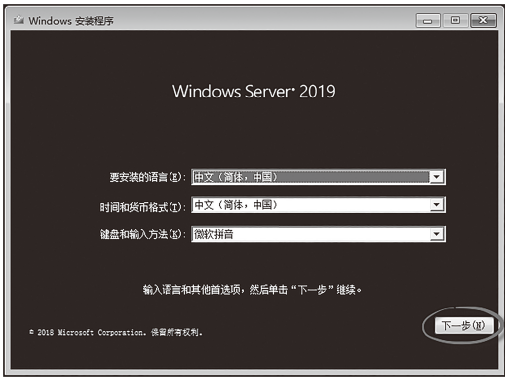

图 7.5　启动安装程序

图 7.6　准备安装

（7）输入合法的产品密钥，“-”不需要输入，单击“下一步”按钮，如图 7.7 所示。

（8）根据需求选择合适的安装方式，系统提供了两种安装方式：一种是 Server-core 安装，一种是桌面体验安装（GUI）。这里我们选择桌面体验安装，单击“下一步”按钮，如图 7.8 所示。

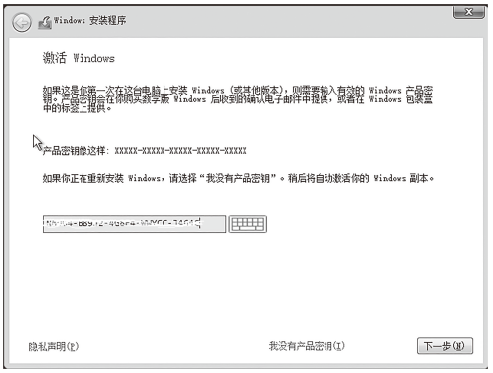

图 7.7　激活 Windows 界面

图 7.8　选择安装的操作系统

（9）单击“自定义：仅安装 Windows”，如图 7.9 所示。

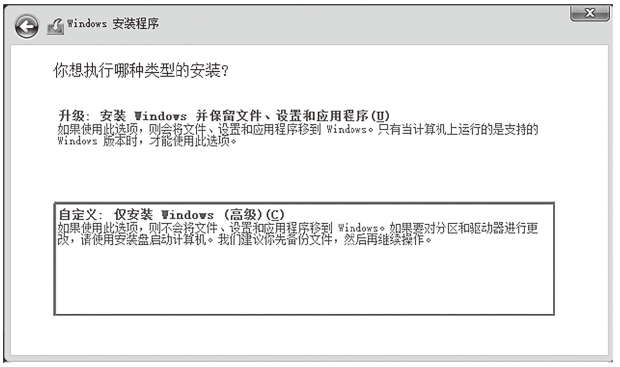

图 7.9　选择自定义安装方式

（10）默认只有一块磁盘（整块硬盘），这里需要对磁盘进行适当的分区。用鼠标单击选中磁盘，单击“新建”按钮，输入创建分区的大小，单击“下一步”按钮，如图 7.10 所示。

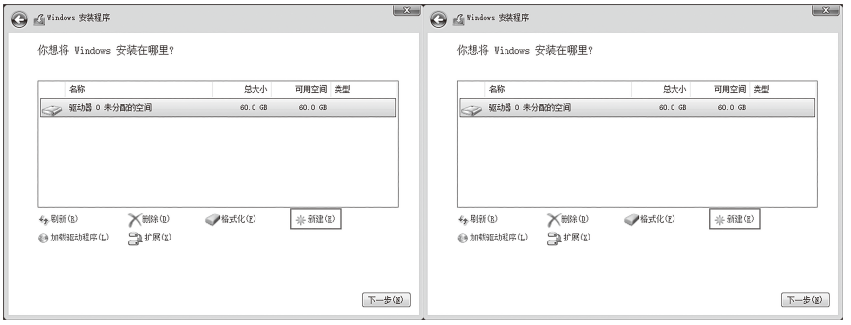

图 7.10　新建分区

（11）选中系统的安装分区，单击“下一步”按钮，进入安装进程，如图 7.11 和图 7.12 所示。

图 7.11　选择安装驱动器

图 7.12　正在安装

（12）安装完成后，系统重启，设置系统的登录密码，完成系统安装，如图 7.13 所示。

图 7.13　设置系统密码

（13）如果用的是 Server core 安装，完成安装后的界面如图 7.14 所示，选择“确定”更改管理员账户的密码，然后执行组策略更新命令，完成安装，如图 7.15 所示。

图 7.14　Server core 安装完成界面

图 7.15　安装完成后更新组策略

（14）完成系统安装

安装完成后，系统自动重启，进入登录界面，输入管理员账户的密码，即可登录系统，如图 7.16 和图 7.17 所示。

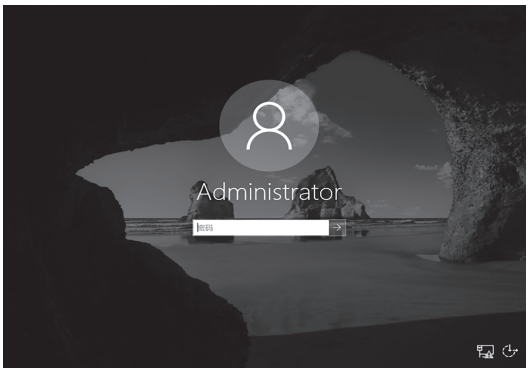

图 7.16　系统登录界面

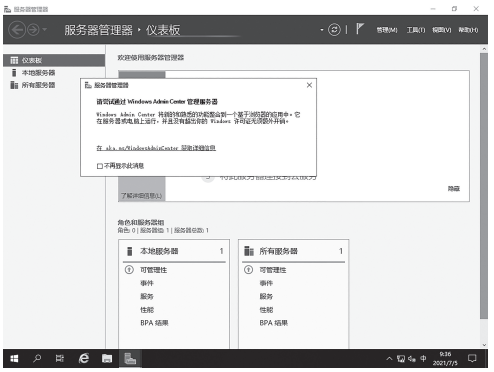

图 7.17　登录系统后的界面

（15）如果要使用 Server 2019 的 Admin Center 管理服务器，需要从 Windows 官网上下载 Windows Admin Center 组件，进行适当配置（确保管理机器可以连通服务器）即可使用。在图 7.18 中单击服务器名称，输入 administrator 的密码，即可登录成功。如图 7.19 所示。

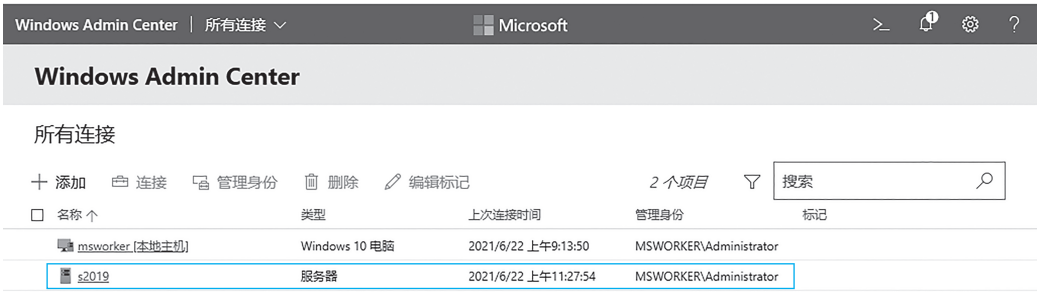

图 7.18

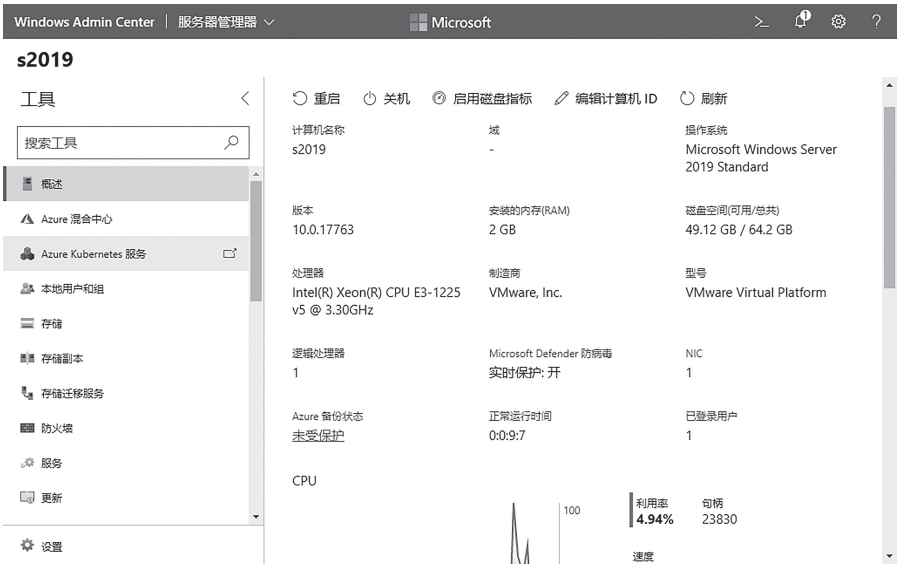

图 7.19　Admin Center 服务器管理器界面

7.2　Windows Server 2019 基本环境

每一台计算机的名称必须是唯一的，不应与网络上其他的计算机重名，虽然系统会自动设置计算机的名称，但还是建议将计算机的名称更改为容易识别的名称。每一台计算机所隶属的工作组都默认为 WORKGROUP。一台计算机的 IP 地址不能与其他计算机的 IP 地址相同，否则会造成网络互连故障，因此需要设置服务器的 IP 地址。为了确保系统的工作安全，还需要对防火墙进行适当设置，放行或者组织分类数据流，巩固系统的安全性。

7.2.1　实训环境

（1）VMware Workstation。

（2）组件需求：成功安装 Server 2019 Standard。

7.2.2　实训内容

实训目标

掌握 Windows Server 2019 的基本环境设置，以便熟悉服务器的基本管理。

◆ 实训 1　设置计算机名称和 TCP/IP 设置

为了能快速上手 Windows Server 2019 系统，从以下四个方面开始。

（1）设置计算机名称和 TCP/IP 中的 IP 地址。

（2）更改计算机名和工作组名。

（3）设置防火墙。

（4）设置环境变量。

计算机名称和 TCP/IP 设置中的 IP 地址都是用来识别计算机的，是实现计算机与其他计算机通信所必需的信息。

1. 更改计算机名称与工作组名称

（1）单击左下角的开始图标，打开服务器管理器，单击“本地服务器”选项，在“计算机名”选项卡界面中单击“更改”按钮，如图 7.20 所示。

图 7.20　单击“更改”按钮

（2）在弹出的“计算机名 / 域更改”对话框中，输入计算机名，单击“确定”按钮，如图 7.21 所示。重启系统后即完成计算机名称的修改。

（3）也可以通过 Windows Admin Center 管理服务器更改计算机的名称。打开 Windows Admin Center, 单击“添加”按钮，输入服务器的 IP 地址和管理凭据，即可登录服务器，如图 7.22 所示。

（4）登录后，单击“编辑计算机 ID”按钮，输入计算机名称即可，如图 7.23 所示。

图 7.21　输入计算机名

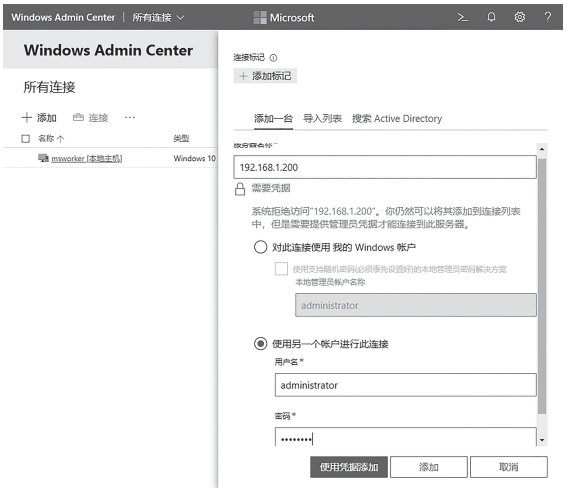

图 7.22　添加并登录服务器

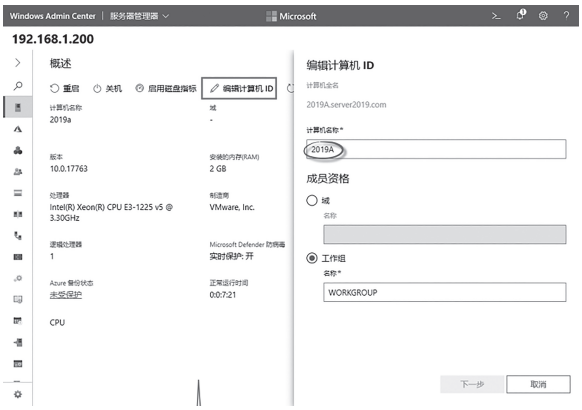

图 7.23　输入计算机名称

2. 设置 IP 地址与测试

服务器获取 IP 地址的方式有两种：一种是自动获取 IP 地址，这是系统的默认设置，计算机会向 DHCP 服务器租用 IP 地址。另一种是通过手动设置 IP 地址，这种方式会增加系统管理员的工作负担，而且手动设置 IP 地址易出错，比较适合企业内部服务器使用。

设置 IP 地址的步骤如下：

（1）打开服务器管理器，单击本地服务器右侧的“Etherneto”选项，双击“Etherneto”选项，打开“网络连接”对话框，如图 7.24 所示。

（2）右键单击网卡图标，在弹出的快捷菜单中选择“属性”选项，如图 7.25 所示。

（3）在弹出的对话框中双击“Internet 协议版本 IPv4(TCP/IPv4)”选项（见图 7.26），打开 Internet 协议版本 IPv4(TCP/IPv4) 属性对话框。

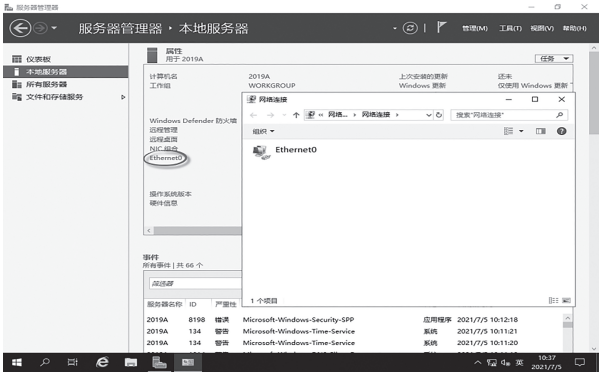

图 7.24　打开“网络连接”对话框

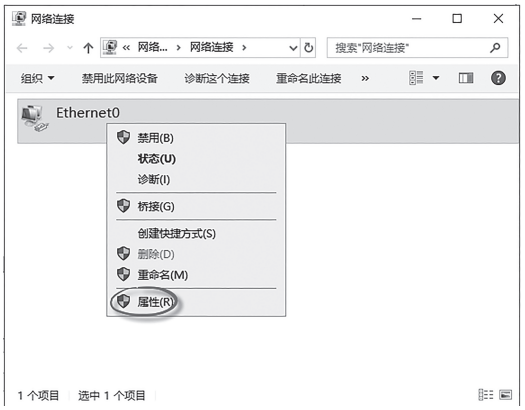

图 7.25　选择“属性”选项

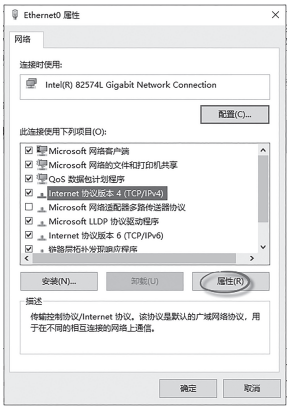

图 7.26　选择 Internet 协议版本 4(TCP/IPv4) 选项

（4）在对话框中单击“自动获得 IP 地址”单选项和“自动获得 DNS 服务器地址”单选项，单击“确定”按钮即可完成 DHCP 自动获取 IP 地址的设置，如图 7.27 所示。

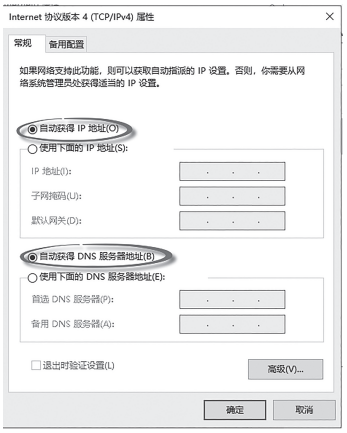

图 7.27　选择自动获取单选项

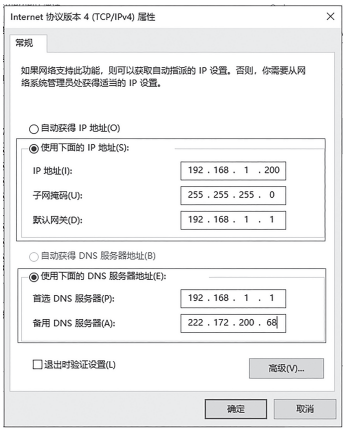

图 7.28　手动设置 IP 地址与 DNS

（5）也可以根据实际需要手动设置 IP 地址，在图 7.27 中选择“使用下面的 IP 地址”单选项和“使用下面的 DNS 服务器地址”单选项，输入 IP 地址，子网掩码和 DNS 服务器地址即可，如图 7.28 所示。

（6）也可以通过 Windows Admin Center 进行 IP 地址的设置。打开 Windows Admin Center 的服务器管理界面，选中“网络”选项，选中当前的网卡适配器，单击“设置”按钮，如图 7.29 所示。

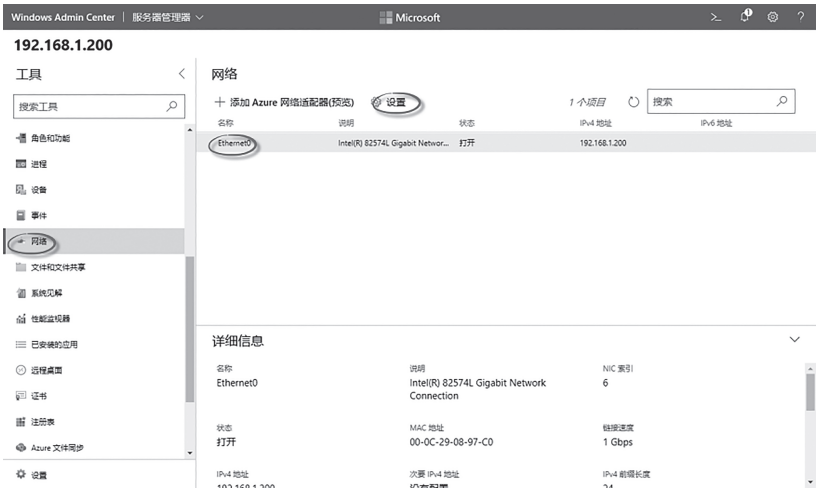

图 7.29　Windows Admin Center 中网络设置界面

（7）在弹出的对话框中进行 IP 地址与网关、DNS 服务器的设置（如果 IP 地址改变，需要重新登录 Windows Admin Center)。如图 7.30 所示。

图 7.30　设置 IP 地址

◆ 实训 2　Windows Defender 防火墙设置

Windows 内置的防火墙可以很好地保护计算机免受恶意攻击。为了增加计算机在网络内的安全性，支持对位于不用网络的计算机设置不同的防火墙规则。例如，对位于公共网络的计算机，防火墙的设置应更严格一些；对位于专业网络的计算机，其防火墙规则的设置可适当宽松些。

系统将网络分为专用网络、公共网络和域网络，而且可以自动判断计算机所在的网络位置。管理员可以根据实际需要设置网络所处的位置。

1. 网络位置设置

（1）单击左下角的图标，在开始菜单中单击“设置“图标，在打开的“设置”对话框中选择“更新和安全”选项，如图 7.31 所示。

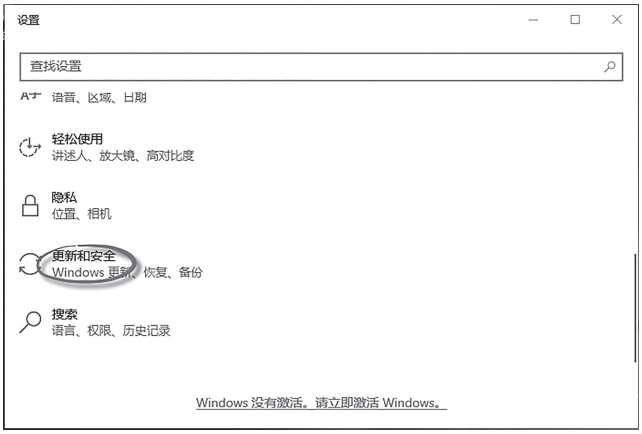

图 7.31　选择“更新与安全”选项

（2）在“设置”对话框中选中“Windows 安全中心”选项，如图 7.32 所示。

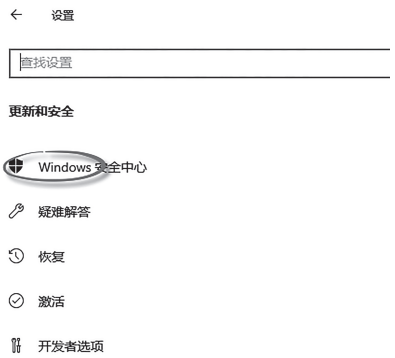

图 7.32　选择“Windows 安全中心”选项

（3）单击“防火墙和网络保护”按钮。根据需要设置网络所处的位置，如图 7.33 所示。

图 7.33　设置防火墙与网络保护

如果需要自行更改网络位置的话，也可以通过命令的方式操作。如图 7.34 所示，通过命令将网络的位置从 private（专用网络）设置为 public（公用网络）。

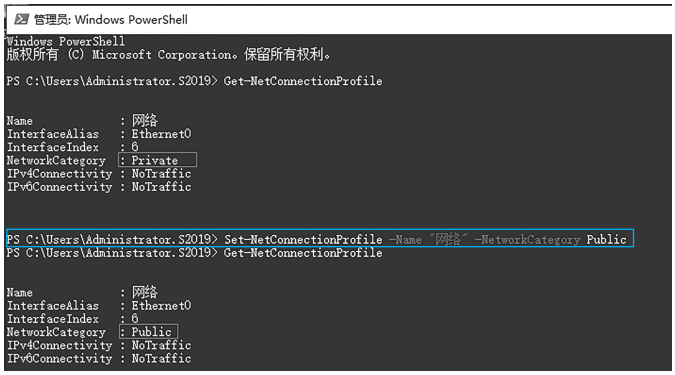

图 7.34　用命令方式更改网络位置

2. 设置防火墙的过滤规则

Windows 防火墙会阻挡绝大部分的入站连接，当然，通过简单的设置可以解除某些程序的过滤规则（阻挡或者放行）。例如，需要允许网络上的其他用户可以访问服务器上的共享文件或者实现打印机共享，可以进行以下操作。

（1）打开“控制面板”，选中“系统和安全”菜单项，在“Windows Defender 防火墙”选项下，单击“允许应用通过 Windows 防护墙”选项，如图 7.35 所示。

（2）在“允许的应用”对话框中，根据需要阻止或者放行应用，如图 7.36 所示。

3. 防火墙的高级设置

如果需要进一步配置防火墙规则，可以通过防火墙的“高级设置”功能实现，步骤如下：

（1）单击防火墙的“高级设置”选项，开启防火墙设置对话框，如图 7.37 所示。

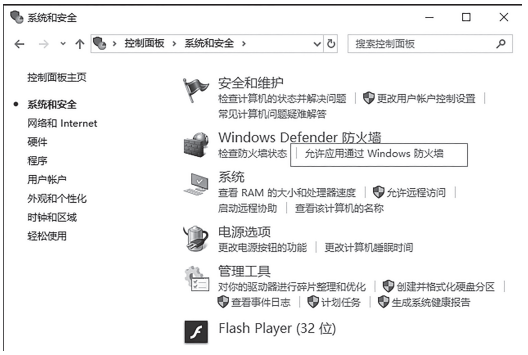

图 7.35　设置 Windows Defender 防火墙

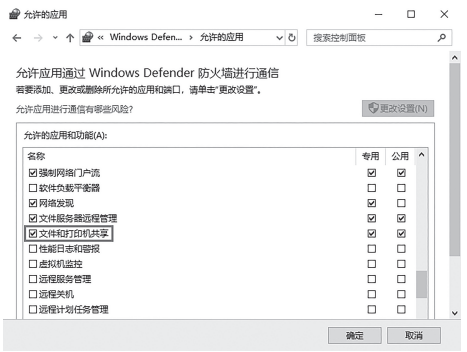

图 7.36　选择允许通过防火墙的应用

图 7.37　防火墙的高级设置界面

（2）不同的网络位置可以设置不同的 Windows Defender 防火墙规则，同时也有不同的配置文件。这些配置文件可以通过以下方式修改。

选中图 7.37 中“本地计算机上的高级安全 Windows Defender 防火墙”选项，单击鼠标右键，弹出快捷菜单，选择“属性”选项。如图 7.38 所示。弹出防火墙属性对话框，如图 7.39 所示，在此对话框中可以针对网络所处的位置设置入站和出站属性。

设置的主要选项包括：

- 阻止——阻止防火墙规则没有明确允许连接的所有连接。
- 允许——允许连接，但防火墙规则明确阻止的连接除外。
- 阻止所有连接——阻止全部连接。

（3）限定特定流量。除了全局策略外，管理员还可针对特定程序或流量实施精细化控制。例如，为防止服务器遭受 ICMP 泛洪攻击而影响正常运行，通常需配置防火墙规则，禁止外部客户端向服务器发送 Ping 请求 (ICMP 报文)。操作步骤如下：

① 在“高级安全 Windows Defender 防火墙”界面中，单击左侧的 " 入站规则 " 选项。

图 7.38　选择“属性”选项

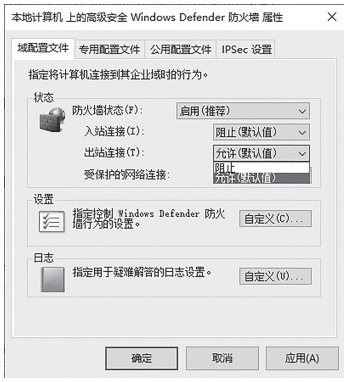

图 7.39　防火墙属性配置窗口

② 在规则列表中找到并选中“文件和打印机共享 (回显请求 - ICMPv4-In)”条目双击，打开属性对话框，如图 7.40 所示。

③ 在“常规”选项卡中选中“阻止连接”单选按钮，最后单击“确定”按钮保存设置。

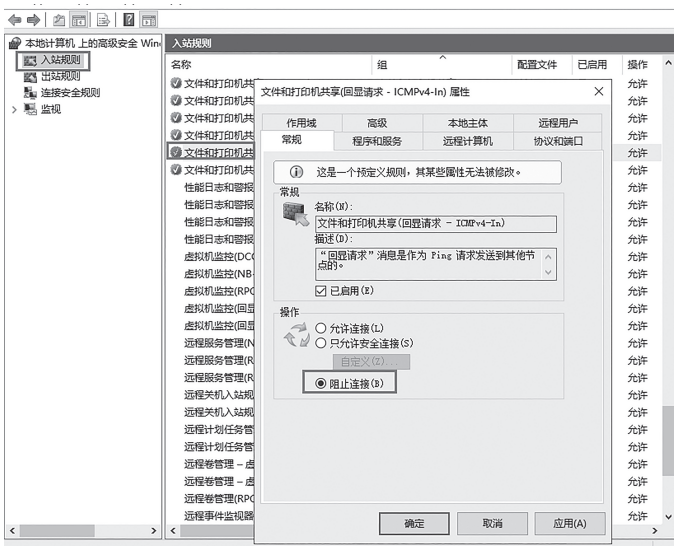

图 7.40　设置某个入站规则的操作属性

需要注意的是，禁用 Ping 功能仅阻断向服务器的探测请求，不会影响服务器提供其他正常的网络服务。

（4）开放特定端口服务。若需对外提供特定网络服务，管理员可根据业务需求手动开放相应的端口。例如，若要使用基于 TCP 协议的 8888 端口部署 Web 服务，需创建一条新的入站规则允许该端口通信。操作步骤如下：

① 在左侧导航栏选择“入站规则”选项，在右侧“操作”面板中单击“新建规则...”操作，如图 7.41 所示。

图 7.41　新建规则

② 弹出“新建入站规则向导”对话框，在该对话框中勾选“端口”单选项，单击“下一步”按钮，如图 7.42 所示。

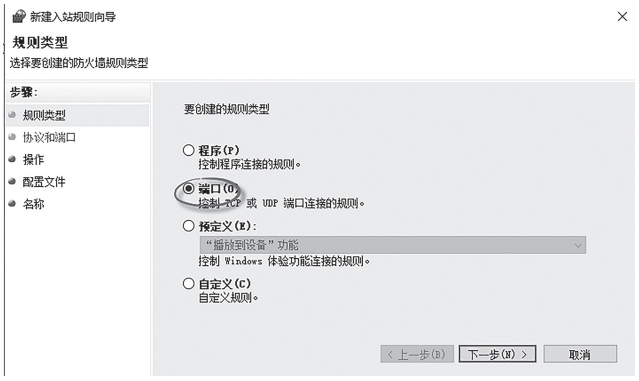

图 7.42　设置规则类型

③ 在“新建入站规则向导”对话框中，按照图 7.43 所示设置协议和端口，单击“下一步”按钮继续下一步“操作”设置，设为“允许连接”，完成设置。

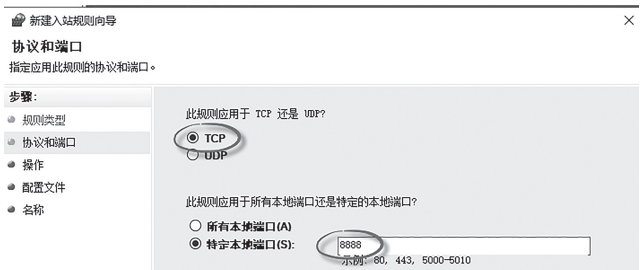

图 7.43　设置规则的协议和端口

7.2.3　环境变量的管理

Windows 环境变量是操作系统用于配置运行环境的关键参数，直接影响计算机中程序的执行路径、文件查找机制及分配内存分配策略等行为方式。环境变量分为系统环境变量和用户环境变量两种：系统环境变量作用于登录系统的所有用户，即所有

用户的工作环境都会加载这些变量值。这类变量仅允许具有管理员权限的系统用户管理和维护。用户环境变量仅影响当前登录系统的特定用户，其设置不会影响其他用户。

1. 查看系统环境变量

要查看系统环境变量，必须使用管理员身份登录系统，运行 cmd.exe 进入命令行界面，输入 set 命令进行查询，如图 7.44 所示。

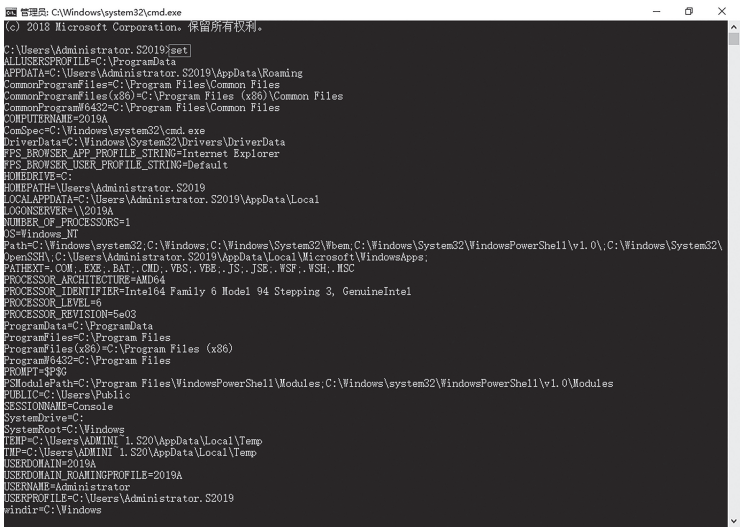

图 7.44　查看系统环境变量

2. 修改环境变量

若需修改环境变量，在图形化界面中可按以下步骤操作。

（1）右键单击“此电脑”图标，在弹出的快捷菜单中选择“属性”选项，如图 7.45 所示选项。

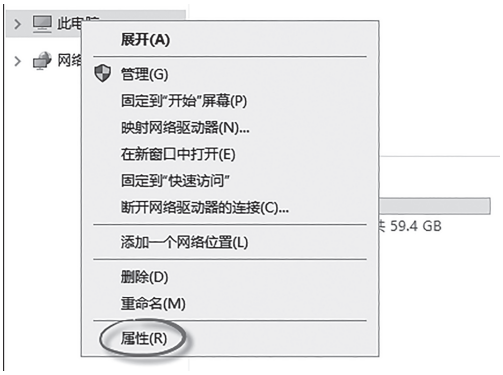

图 7.45　选择“属性”选项

（2）在打开的“系统”对话框中选中“高级系统设置”选项，如图 7.46 所示。

图 7.46　选择“高级系统设置”选项

（3）在打开的“系统属性”对话框中，单击“环境变量”按钮（见图 7.47），进入“环境变量”设置对话框，如图 7.48 所示。在此窗口界面中，可以新建、编辑、删除环境变量。

图 7.47　“系统属性”对话框

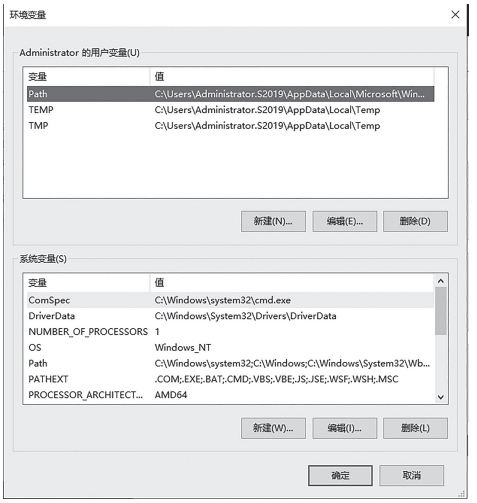

图 7.48　“环境变量”设置对话框

3. 创建和修改环境变量实例

通过适当修改环境变量，实现 JSP 动态网站的环境设置（确保安装 JSP 和 Tomcat 组件）。

（1）按图 7.49 所示的步骤操作，打开“环境变量”对话框。

（2）创建一个名称为“JAVA_HOME”的环境变量，设置变量值为第二步安装 JDK 的路径。为避免手工输入出现差错，可以打开 JDK 所在的文件夹，将文件夹的位置信息直接复制过来，如图 7.50 所示。

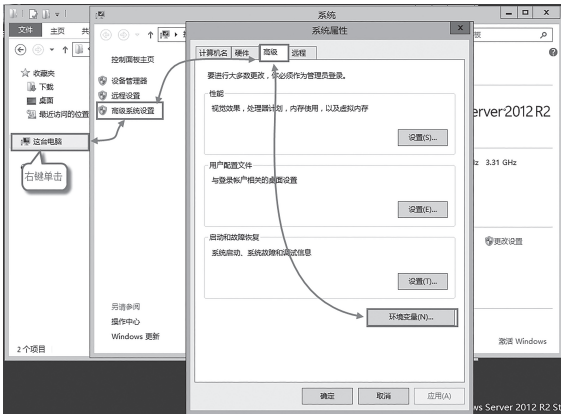

图 7.49　打开环境变量对话框操作

（3）将复制的内容粘贴在变量值一栏中，单击“确定”按钮，如图 7.51 所示。

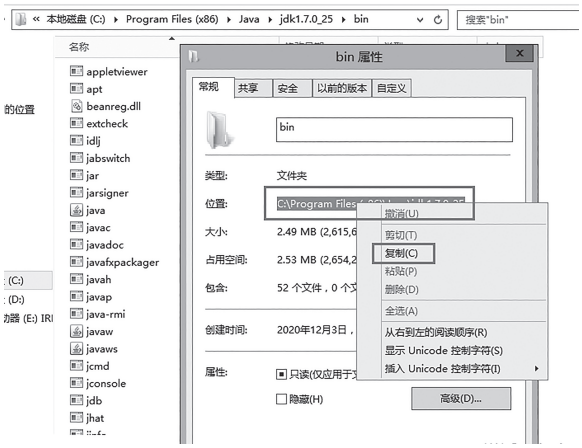

图 7.50　复制路径

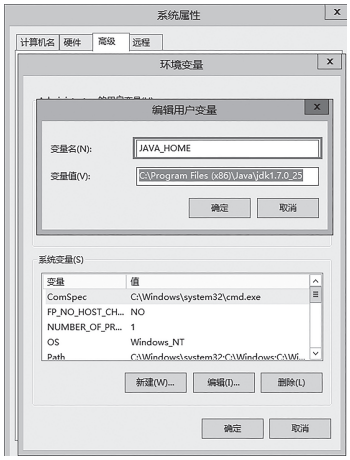

图 7.51　创建环境变量 JAVA_HOME

（4）再创建一个名称为“PATH”的变量，变量值设置如图 7.52 所示。

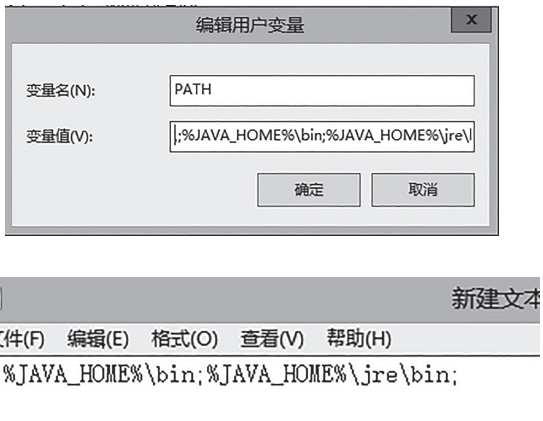

图 7.52　创建和设置 PATH 变量

（5）在命令行模式下查看 JDK 的版本，如图 7.53 所示。

```
PS C:\Users\Administrator> java -version
java version "1.7.0_25"
Java(TM) SE Runtime Environment (build 1.7.0_25-b17)
Java HotSpot(TM) Client VM (build 23.25-b01, mixed mode, sharing)
PS C:\Users\Administrator> _
```

图 7.53　查看 JDK 版本

（6）安装 Apache Tomcat 组件。直接双击安装包文件，在安装界面中连续单击“next”按钮即可。如图 7.54 和图 7.55 所示。

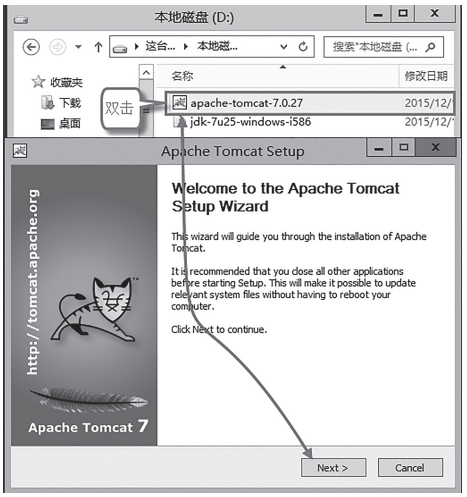

图 7.54　安装 Apache Tomcat

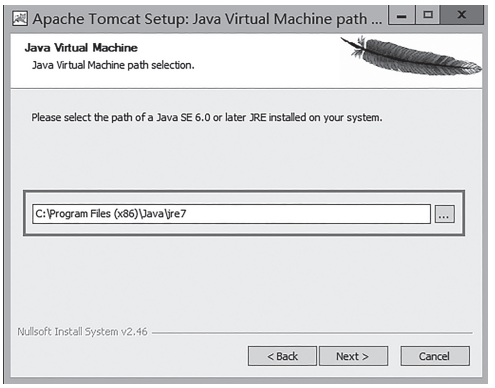

图 7.55　设置安装路径

（7）安装完成后，启动 Web 浏览器，在地址栏中输入 http://localhost:8080 或者将 localhost 替换为本机的 IP 地址，访问 Tomcat 的默认主页，以验证服务是否正常运行。Tomcat 默认监听 8080 端口，界面如图 7.56 所示。

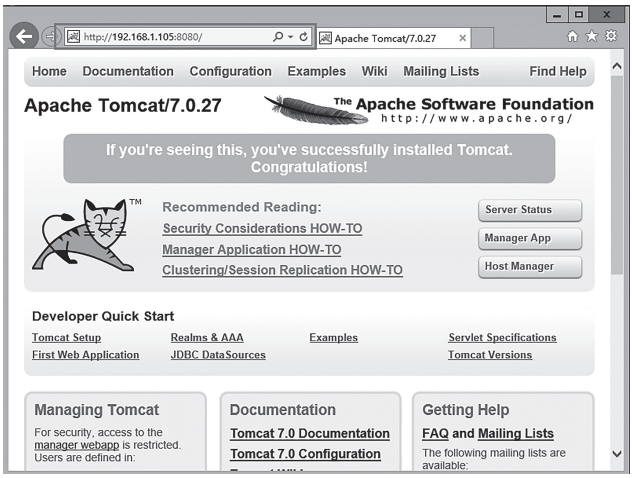

图 7.56　Tomcat 的默认主页

（8）若要修改 Tomcat 的默认端口，需编辑位于安装目录中的 server.xml 文件。该文件位于安装目录下的 conf 子文件夹中，即 Tomcat 的安装路径 \Program Files (x86)\Apache Software Foundation\Tomcat 7.0\conf\ 中。找到 server.xml 文件，用记事本程序打开该文件，如图 7.57 所示。

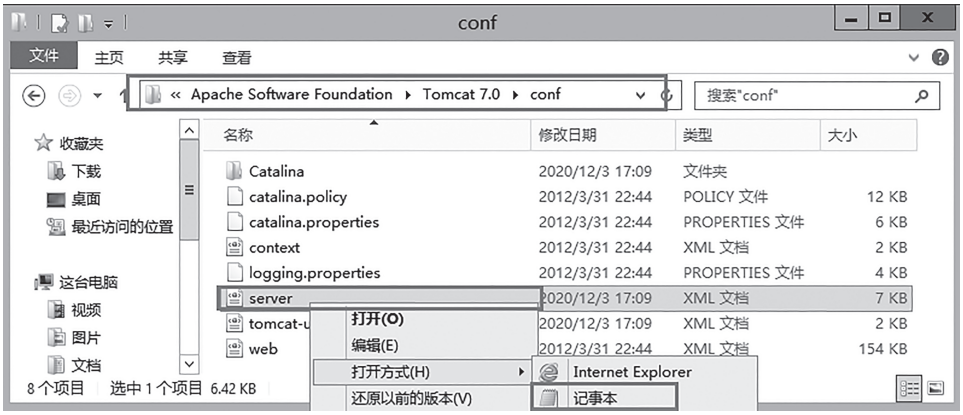

图 7.57　用记事本打开 server.xml 文件

（9）在 server.xml 文件中，按 Ctrl+ F 组合键打开“查找”对话框，输入 8080 进行搜索，通常会找到三处 8080 端口配置项（分别是 HTTP 连接器端口、AJP 连接器端口、重定向端口）。一般情况下，只需修改第二处和第三处出现的 8080（视具体版本而定），将其改为所需 要的端口号即可。例如，将服务端口号修改为 8888，修改前后对比如图 7.58 和图 7.59 所示。

图 7.58　查找 8080 端口

（10）修改端口后，必须重启 Tomcat 服务才能使新端口生效。重启 Tomcat 服务分为 2 步：先停止服务，再启动服务。

- 停止服务：在命令模式下输入 shutdown 命令，如图 7.60 所示。

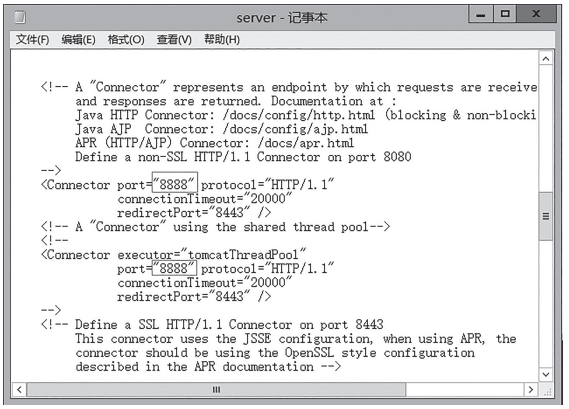

图 7.59　修改为 8888 端口

图 7.60　停止 Tomcat 服务

● 启动服务：在命令模式下运行 Tomcat 7.exe 程序，如图 7.61 所示。

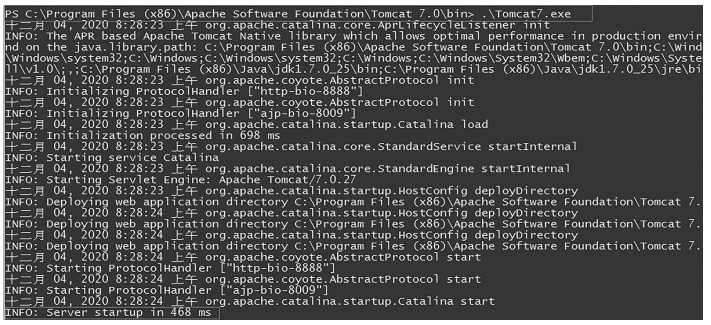

图 7.61　启动 Tomcat 服务

（11）打开浏览器进行验证，在地址栏中输入 http://192.168.1.105:8888/, 显示界面如图 7.62 所示。

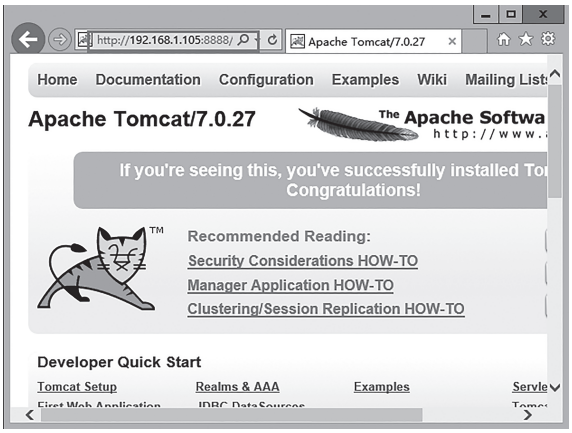

图 7.62　修改端口后的 Tomcat 默认主页

7.3 本地用户和用户组

用户在访问计算机系统前必须登录操作系统，这一过程要求用户提供有效的账户名称及对应的登录密码。在 Windows Server 操作系统中，不同类型的用户（组）所拥有的管理权限往往不同。Windows Server 操作系统采用分层用户权限管理模式：管理员账户（名称为 Administrator）拥有最高权限，所有用户账户及用户组的权限，均需由具备管理员权限的账户进行统一分配与管理。用户的操作权限与其所属的账户组紧密关联。科学、有效的用户权限分配策略，不仅能够保障系统安全，还能显著降低网络管理的复杂度。

7.3.1 实训环境

（1）利用 VMware Workstation 安装好的 Windows Server 2019 操作系统，且系统能够正常登录。

（2）组件需求：VMware Workstation，Windows Admin Center。

7.3.2 实训内容

实训目标

（1）掌握在服务器上添加本地用户和本地用户组。

（2）掌握对本地用户和本地用户组的管理。

◆ 实训 1　本地用户的管理

1. 新建本地用户账户

这里采用 Windows Admin Center 环境实现对本地用户的管理，步骤如下：

（1）开启 Windows Admin Center，成功登录系统后，单击“本地用户和组”选项，如图 7.63 所示。

图 7.63　打开“本地用户和组”界面

（2）单击“新建用户”按钮，在“添加新用户”对话框中输入“名称”，设置用户密码，用户的密码必须符合系统用户密码复杂性要求，如图 7.64 所示。

图 7.64　输入新用户信息

（3）添加用户后，在用户列表中会显示出已经创建的本地用户，如图 7.65 所示。

图 7.65　添加用户成功

2. 删除本地用户

如果要删除用户，可以在“本地用户和组”对话框中选中需要删除的用户，单击“删除用户”按钮即可，如图 7.66 所示。

图 7.66　删除用户操作

3. 编辑本地用户

如果需要更改用户名称或密码，可以在“本地用户和组”对话框中单击“…”

按钮，然后在下拉菜单中选择“更改密码”或者“编辑用户”进行操作即可。如图 7.67 所示。

图 7.67　编辑用户操作

◆ 实训 2　本地用户组的管理

1. 添加本地用户组

（1）单击左侧的“本地用户和组”选项，选择“组”选项，如图 7.68 所示。

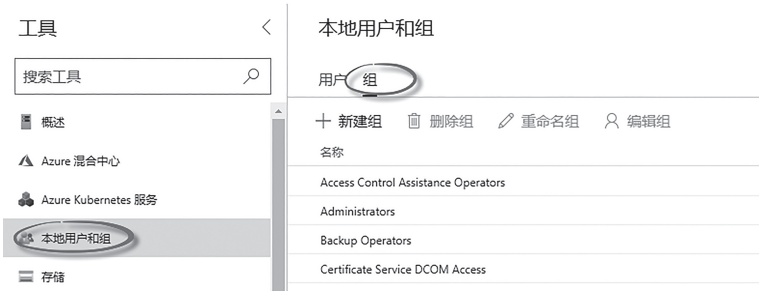

图 7.68　选择“组”选项

（2）单击“新建组”，在“添加新组”对话框中输入组的名称，说明信息是可选项，单击“添加”按钮即可，如图 7.69 所示。

图 7.69　添加新组

（3）要将用户添加到用户组中，需先选中用户，再单击“管理成员资格”按钮，在右侧选中组“group1”，即将用户 user1 加入到组 group1 中了，如图 7.70 所示。

图 7.70　将用户添加到用户组中

2. 删除本地用户组

如果需要删除本地用户组，可以打开“本地用户和组”界面，选中需要删除的组，单击“删除组”按钮即可，如图 7.71 所示。

图 7.71　删除组

7.4　建立 Active Directory 域

域是 Windows 网络操作系统与 Internet 的逻辑组织单元，在 Windows 网络环境中，域也是安全边界。域管理员仅能管理本域内部，跨域管理需经显式授权；每个域均有独立的安全策略以及与其他域的安全信任关系。

域的核心机制在于对计算机加入网络进行集中控制。域控制器（DC）维护着包含本域账户、密码及所属计算机信息的数据库。当计算机接入网络时，域控制器将验证该计算机是否属于本域、用户登录账号是否存在及密码是否正确。任一验证失败均会导致登录被拒，此时，用户只能以对等网方式访问共享资源，从而限制其对服务器上受保护资源的访问，有效保障了网络安全。

将计算机加入域，仅实现与服务器的网络可见远远不够，需由网络管理员进行相

应设置，将计算机加入到域中，才能实现资源的集中共享与统一管控的目标。

7.4.1 实训环境

（1）VMware Workstation 安装的 Windows Server 2019 操作系统，且系统能够正常登录。

（2）组件需求：Active Directory 域服务 DNS 服务。

7.4.2 实训内容

实训目标

（1）掌握建立域服务的方法。

（2）掌握将计算机加入域和脱离域的方法。

（3）掌握管理域用户账户和域组账户的方法，以及删除域的方法。

◆ 实训 1　建立第一台域控制器

将 7.3 节中安装的服务器升级为一台域控制器，设计域名为 S19.com，服务器的主机名为 DC，使用本服务器作为域的 DNS 服务器。升级为域控制器后，服务器的主机名自动变为 DC.S19.COM。

操作步骤如下：

（1）打开服务器管理器，单击仪表板中的“添加角色和功能”按钮，如图 7.72 所示。

图 7.72　添加角色和功能

（2）进入“添加角色和功能向导”界面，三次单击“下一步”按钮后，进入

图 7.73 所示的界面，勾选“Active Directory 域服务”复选项，单击“下一步”按钮。

图 7.73　勾选“Active Directory 域服务”选项

（3）持续两次单击“下一步”按钮，进入到如图 7.74 所示的界面，单击“安装”按钮，开始安装域服务。

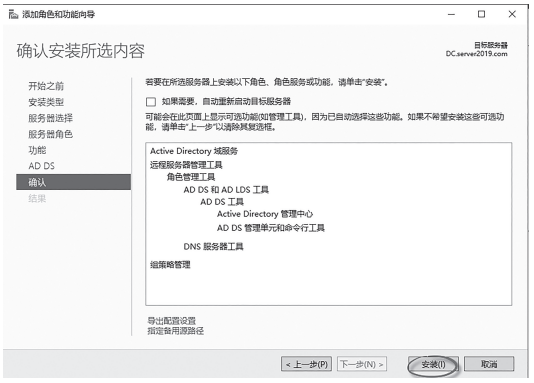

图 7.74　“确认安装所选内容”界面

（4）安装完成后，单击“将此服务器提升为域控制器”链接按钮，开始配置域服务，如图 7.75 所示。

图 7.75　将此服务器提升为域控制器操作

（5）打开如图 7.76 所示的“Active Directory 域服务配置向导”界面，选择“添加到新林”单选项，在根域名输入框中输入域名 S19.COM，单击“下一步”按钮。

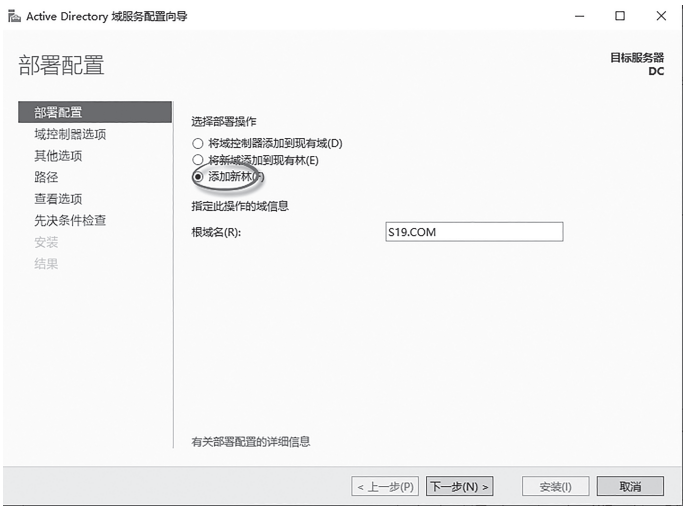

图 7.76　配置域林和根域名

（6）进入“域控制器选项”界面，在“林功能级别”和“域功能级别”中选择 Windows Sever 2016（这里最高级别即为 Windows Server 2016），输入目录服务器还原模式密码。密码的复杂性至少需要 7 位，且必须符合复杂性要求。单击“下一步”按钮，如图 7.77 所示。

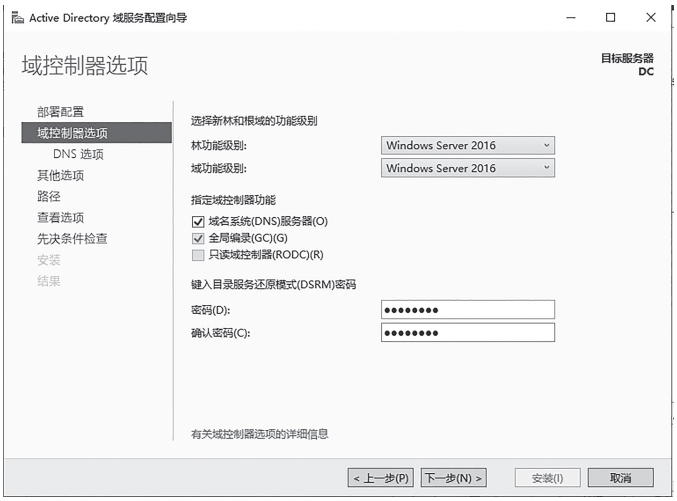

图 7.77　设置域控制器选项

（7）连续单击“下一步”按钮，进入“先决条件检查”界面，显示“所有先决条件检查都成功通过，请单击“安装”开始安装。此时单击“安装”按钮即可进行域环境配置，如图 7.78 所示。安装完成后，设备自动重启，完成第一台域控制器的配置。

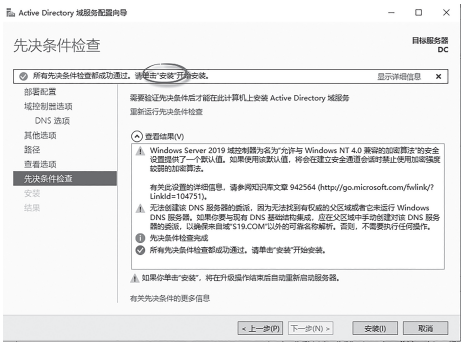

图 7.78 “先决条件检查”界面

（8）设备重启后，单击服务选项卡的“本地服务器”，查看域控制器的配置情况，如图 7.79 所示。

图 7.79 重启后查看本地服务器的配置

◆ 实训 2 将服务器 Server 2012 加入域

要求将 Server 2012 的 DNS 服务器地址指向域控制器，保证路由可通，同时关闭与控制器之间的防火墙。操作步骤如下：

（1）进入服务器管理界面，“本地服务器”选项，单击计算机名“S2012”，打开“系统属性”对话框，如图 7.80 所示。

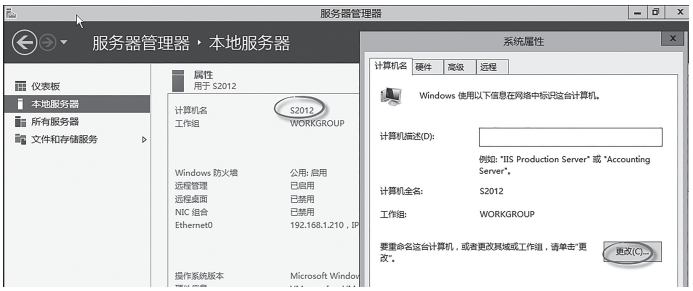

图 7.80 打开“系统属性”对话框

（2）单击图 7.80 中的“更改”按钮，在打开的“计算机名 / 域更改”对话框的

“隶属于”栏，单击“域”单选框，并输入将要加入的根域名称，单击“确定”按钮，如图 7.81 所示。

图 7.81　设置隶属于的域名

（3）在打开的“Windows 安全”对话框中，输入域管理员账户的名称和密码，单击“确定”按钮，如图 7.82 所示。

（4）如果用户名和密码正确，DNS 服务器的实施没有问题，系统会提示成功加入域的信息，如图 7.83 所示。加入域后，系统需要重启才能完成加入域的配置。

图 7.82　输入域管理员账户和密码

图 7.83　成功提示框

（5）在域控器上查看，打开服务器管理器，选择“AD DS”选项，右键单击服务器名称，在弹出的快捷菜单中选择“Active Directory 用户和计算机”选项，如图 7.84 所示。

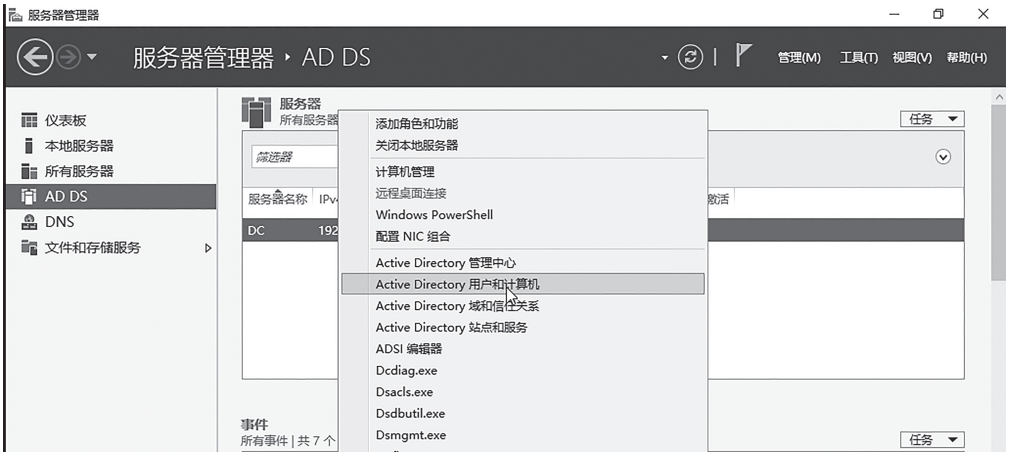

图 7.84　查看 Active Directory 用户和计算机

（6）选择 S19.com 下的“computer”选项，在右侧可以看到已经加入域的主机名称，如图 7.85 所示。

图 7.85　查看域中包含的计算机

◆ 实训 3　使用组策略管理用户工作环境

组策略是系统管理员管理与控制用户工作环境的一种机制，通过该机制，管理员既能确保用户拥有符合要求的工作环境，又能实施必要的操作限制。这样不仅优化了用户体验，也大大减轻了系统管理员的管理负担。

在域中可以针对站点、域、组织单位（OU）来设置组策略。

组策略包含了“计算机配置”和“用户配置”两部分：计算机配置可以控制域内计算机的环境，用户配置可以控制组织单位（OU）内用户的工作环境。

下面举例说明组策略的运用方法。在 Windows Server 中设置组策略时，开放防火墙的 TCP/8080 端口，这样加入域的计算机就会开放该端口。操作步骤如下：

（1）打开管理工具，单击“组策略管理”选项，如图 7.86 所示。

图 7.86　打开组策略管理

（2）在“组策略管理”界面中，展开组策略管理器，右键单击“Default Domain Policy”选项，在快捷菜单中选择“编辑”选项，如图 7.87 所示。

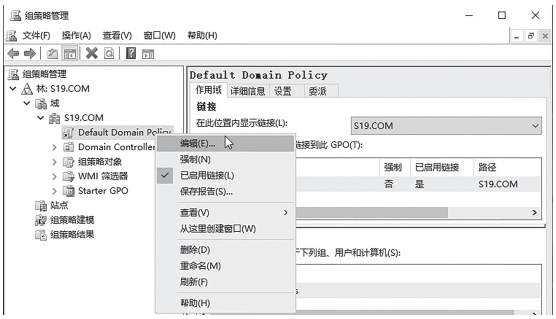

图 7.87　选择“编辑”选项

（3）在“组策略管理编辑器”界面中，选择“Windows 设置”→“安全设置”→“高级安全 Windows Defender 防火墙”→“高级安全 Windows Defender 防火墙 -LDA”→“入站规则”，右键单击，在快捷菜单中选择“新建规则”选项新建一个入站规则，如图 7.88 所示。

图 7.88　新建一条入站规则

（4）选择“端口”单选项，如图 7.89 所示。

图 7.89　选择端口

（5）在“协议和端口”步骤中选中“TCP”单选项，特定本地端口输入 8080，单击“下一步”按钮直至完成配置，如图 7.90 所示。

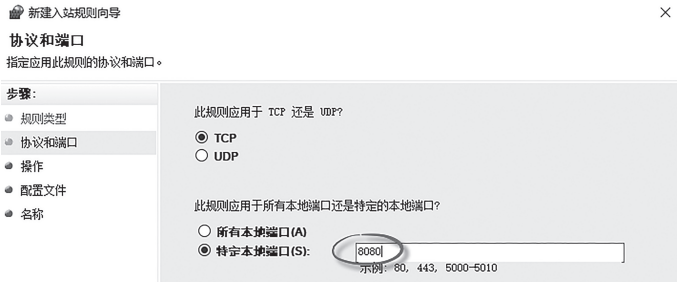

图 7.90　设置协议和端口号

这样，加入域的计算机就会开放该端口。

7.5　文件权限与文件共享

文件共享是主机及多用户计算机系统的核心功能。随着互联网的发展，基于文件传送协议（file transfer protocol,FTP）的文件传输系统得到了广泛应用。FTP 允许用户访问（读取或写入）服务器上的共享资源，此类访问通常需通过服务器端配置的专用凭据进行身份验证，以确保数据安全。

7.5.1　实训环境

（1）VMware Workstation 安装的 Windows Server 2019 操作系统，且系统能够正

常登录。

（2）组件需求：VMware Workstation，Windows Admin Center。

7.5.2 实训内容

实训目标

掌握文件共享权限的设置和对文件共享的设置。

◆ 实训 1　文件权限设置

用户必须对磁盘内的文件或文件夹拥有特定的权限后，才可以访问和使用这些文件资源。文件权限可以分为基本权限和特殊权限：基本权限可以满足常规的使用需求，而特殊权限可以更加精细地控制和分配文件权限。

基本文件权限包括：读取、写入、读取和执行、修改、完全控制。

基本文件夹权限包括：读取、写入、列出文件夹内容、读取和执行、修改、完全控制。

1. 基本文件权限和文件夹权限的设置

系统会为新建的文件和文件夹自动设置默认权限。例如，在 C:\ 下新建一个名称为 document 的文件夹，然后右键单击该文件夹，在快捷菜单中选择“属性”选项，在打开的属性对话框中单击“安全”选项卡，可以看到该文件夹的组或用户名以及用户所拥有的权限，如图 7.91 所示。设置文件共享权限的操作步骤如下：

（1）创建一个名为 user1 的用户，右键单击 document 文件夹，选择“属性”选项，如图 7.92 所示。

（2）在“共享”选项卡界面中单击“共享”按钮，如图 7.93 所示。

（3）右键单击用户名产 user1，在弹出的对话框中按照需求设置文件的权限，如图 7.94 所示。

（4）如果需要设置为不继承父文件夹权限，

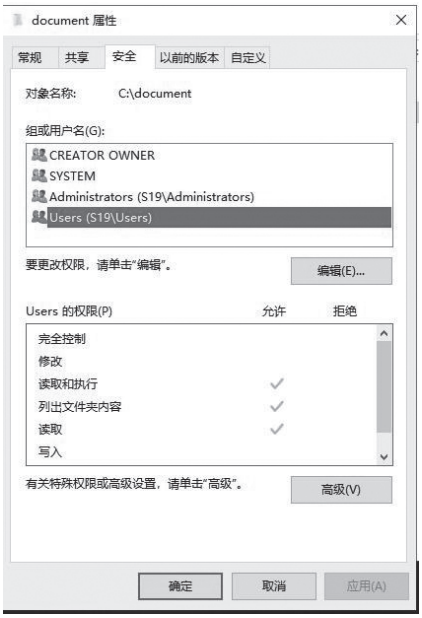

图 7.91　文件夹属性对话框

右键单击文件夹 --- 属性 --- 高级，单击“启用继承”，设置为“禁用继承”即可。如图 7.95 所示。

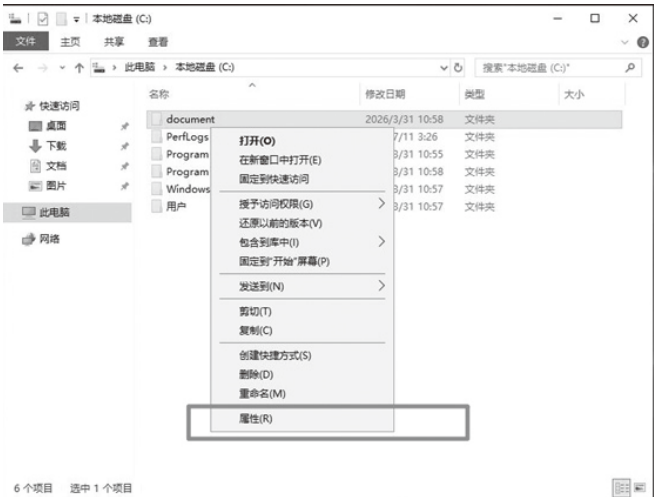

图 7.92　选择“属性”选项

图 7.93　单击“共享”按钮

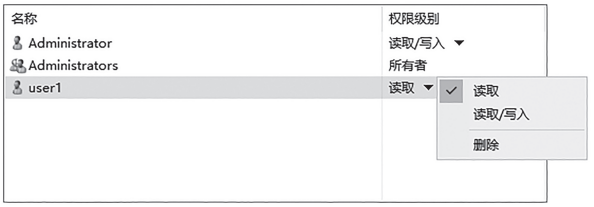

图 7.94　设置用户 user1 的权限

图 7.95　设置为“禁用继承”

2. 特殊权限的分配

基本权限有时无法满足对使用者的更精细的控制，因此需要使用特殊权限来进行

更加精细的权限分配，以满足各种不同的需求。操作步骤如下：

（1）在图 7.95 中开启权限继承，再单击“编辑”按钮，如图 7.96 所示。

图 7.96　执行编辑操作

（2）进入如图 7.97 所示的界面，在此界面中可以根据需求设置特定的权限。

图 7.97　设置特定的权限

◆ 实训 2　磁盘配额

文件共享的最大问题是用户对共享空间的使用，不可能让共享用户无限制的使用磁盘空间，这样会造成极大的资源分配问题。为避免个别用户占用大量的磁盘空间，需要对用户进行磁盘配额限制。操作步骤如下：

（1）单击磁盘，选择“属性”选项，在属性对话框中单击“配额”选项卡，在图 7.98 所示的界面中按照需求设置配额参数。

（2）使用一个客户端远程登录共享文件夹，在该文件夹内进行多次文件复制，当空间达到预警时，系统会发出提示警报信息，如图 7.99 所示。

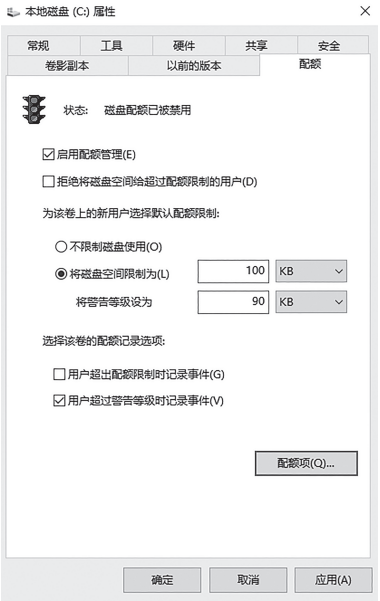

图 7.98　设置配额限制

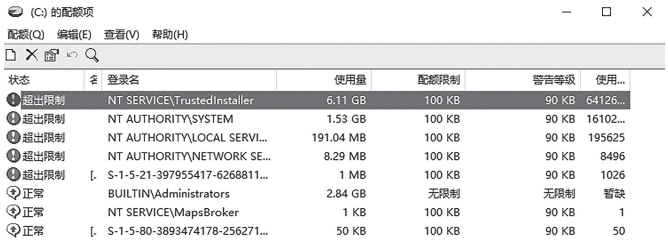

图 7.99　提示警报信息

7.6　NTP 服务器

NTP 是网络时间协议（network time protocol），它是用来同步网络中各个计算机的时间的协议。在计算机网络世界中，时间非常重要，如系统中常见的证书，每一个证书都是有时限的，当时间超过了限额，证书便失效；再如，在进行群集服务时，每一台服务器的时间必须是一致的。

7.6.1　实训环境

（1）VMware Workstation 安装的 Windows Server 2019 操作系统，且系统能够正常登录。

（2）组件需求：VMware Workstation NTP。

7.6.2 实训内容

实训目标

（1）掌握 NTP 服务的配置方法。

（2）掌握 Windows 客户端和 Linux 客户端使用 NTP 服务器同步时间的配置方法。

◆ 实训 1　配置服务器的 NTP 服务

在 Windows Server 2019 上安装 AD DS 组件，将服务器提升为域控制器，之后关闭防火墙，开启 Windows Server 2019 的 NTP 服务。作为 NTP 服务器，为加入域的客户端提供时钟同步。操作步骤如下：

（1）在命令行界面中，输入组策略管理的命令，打开组策略管理器，展开“计算机配置”项，选择“管理模版”→“系统”→“Windows 时间服务”→“时间提供程序”，在“时间提供程序”栏目中，选择“启用 Windows NTP 服务器”选项，如图 7.100 所示。

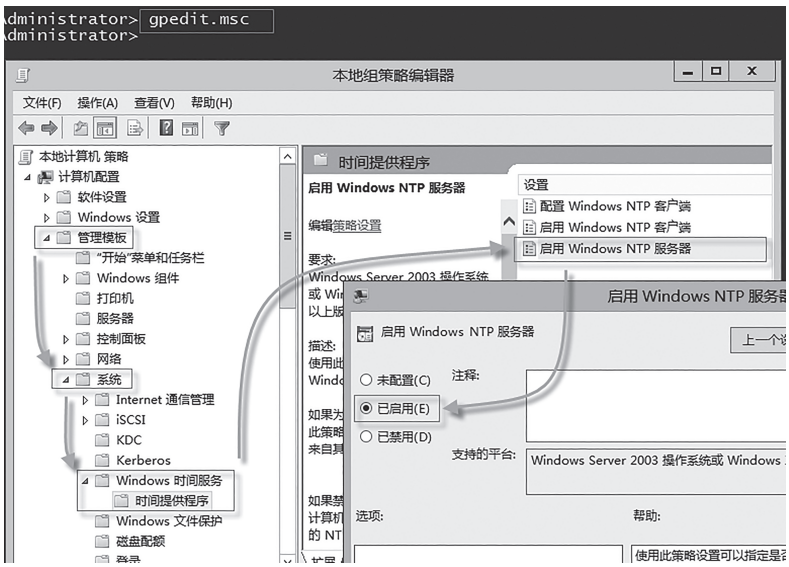

图 7.100　启用 Windows NTP 服务器

（2）设置完成后，对防火墙进行适当配置放行 NTP 数据端口，或者关闭防火墙，

这台 Windows Server 2019 服务器就成为了一台时间服务器。

（3）在服务器上开启注册表编辑器，打开“运行”对话框，输入“regedit”命令，如图 7.101 所示。

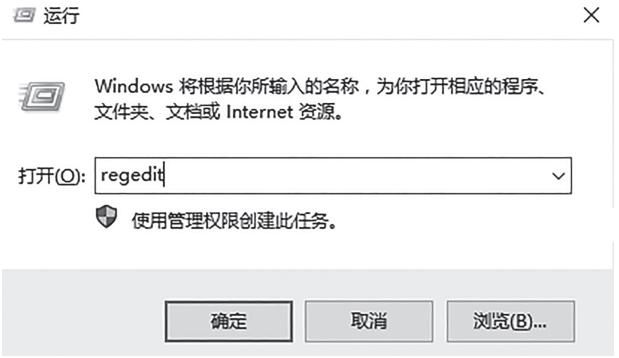

图 7.101　打开注册表编辑器

（4）在注册表编辑器中，连续展开“HKEY_LOCAL_MACHINE”→“SYSTEM”→“currentcontrolset”→“services”→“W32Time”→“Parameters”项，将 type 项的值设置为 NTP（系统缺省设置为 NTP），如图 7.102 所示。

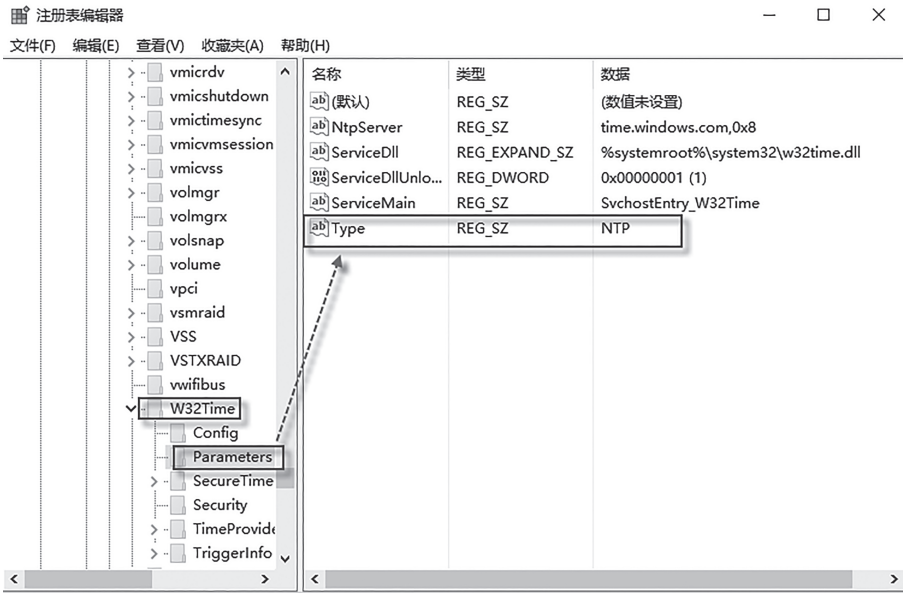

图 7.102　设置 Parameters 的 Type 值

（5）在注册表编辑器中找到，连续展开“HKEY_LOCAL_MACHINE”→“SYSTEM”→“currentcontrolset”→“services”→“W32Time”→“config”项，在右侧双击“AnnouceFlags”值打开“编辑 DWORD（32 位）值”对话框，将数值修改为 5，如图 7.103 所示。

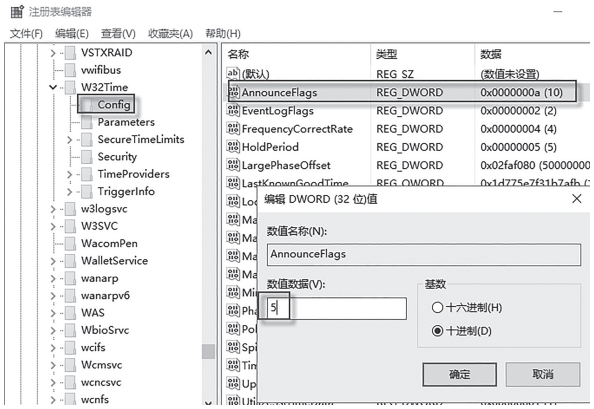

图 7.103　修改 AnnouceFlags 的值

（6）在注册表编辑器中，连续展开“HKEY_LOCAL_MACHINE”→“SYSTEM”→“currentcontrolset”→“services”→“W32Time”→“TimeProviders”→“NtpServer”项，在右侧双击“Enabled”值，在打开的编辑对话框中将数值修改为 1，如图 7.104 所示。

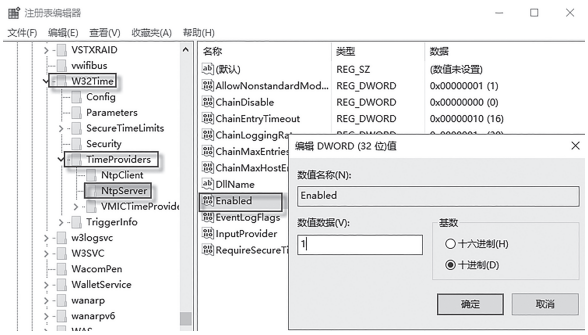

图 7.104　修改 Enabled 的值

（7）打开命令行界面，输入“services.msc”命令，开启服务管理，如图 7.105 所示。

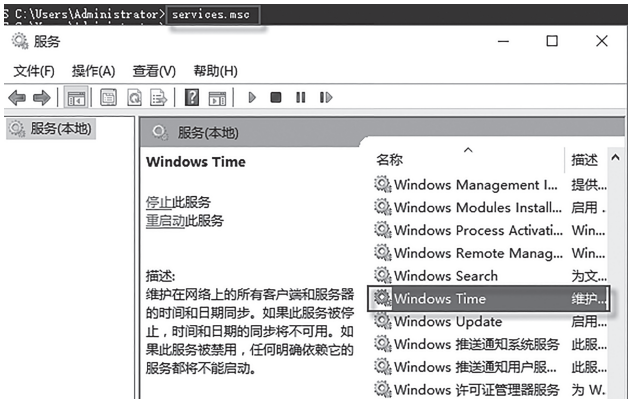

图 7.105　开启 Windows Time 服务

（8）找到 Windows Time，双击后打开 Windows Time 的属性对话框，设置启动类型为“自动”，然后单击“启动”按钮启动服务，如图 7.106 和图 7.107 所示。

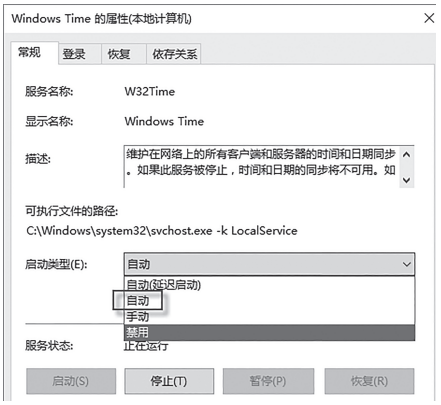

图 7.106　设置启动类型

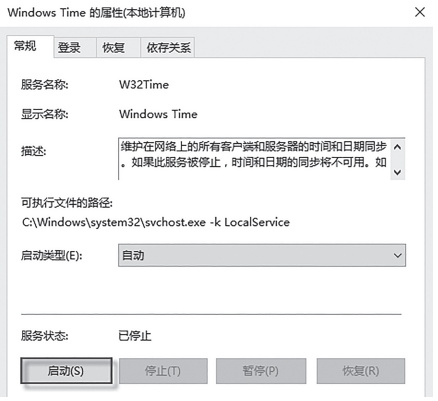

图 7.107　启动 Windows Time 服务

（9）在服务管理中，选中 Windows Time，单击“重启此服务”链接按钮，如图 6.108 所示。

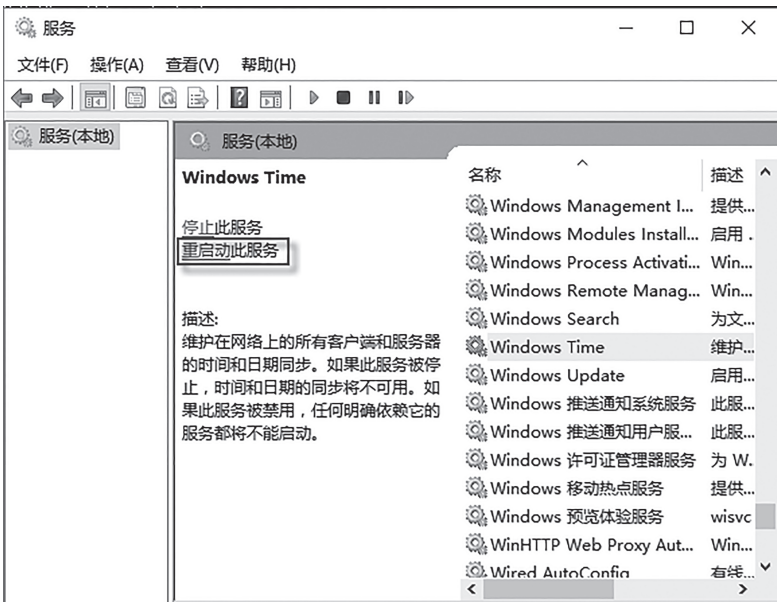

图 7.108　重启动 Windows Time 服务

（10）如果域控制器和 Linux 都需要从另外的 NTP 服务器进行时钟同步，则还需要在 Windows Server 2019 的“时间提供程序”栏目中选择“配置 Windows NTP 客户端”和“启用 Windows NTP 客户端”。例如，如果 Windows Sever 2019 和 Linux 都需要从 192.168.1.200/24 这台服务器上进行时钟同步，那么在 Windows Server 2019 上要做如下的配置，如图 7.109 和图 7.110 所示。

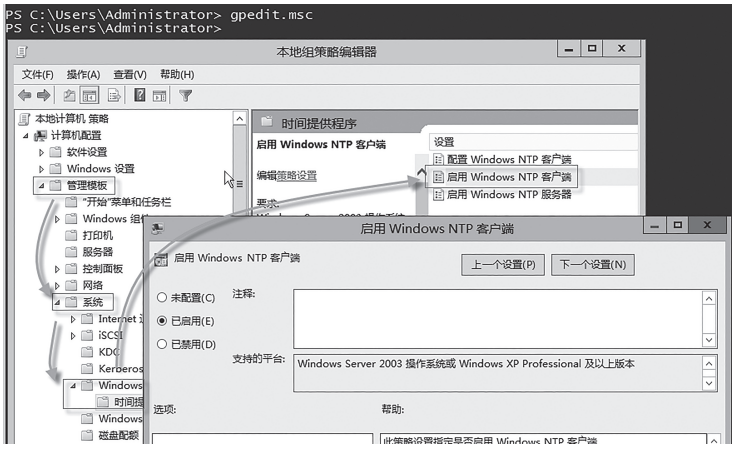

图 7.109　启用 Windows NTP 客户端

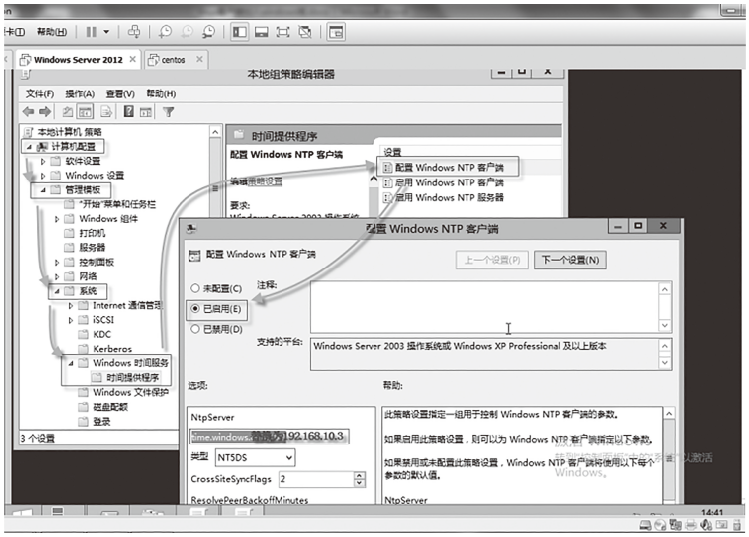

图 7.110　配置 Windows NTP 客户端

◆ 实训 2　Linux 客户端通过 NTP 服务器同步时间

Linux 客户端通过 NTP 服务器实现时间同步的操作步骤如下：

（1）修改域格式的主机名称为 centosA.jnds.net，IP 地址为 192.168.1.2/24，DNS 服务器为 192.168.1.10（DNS1=192.168.1.10），并关闭防火墙和 selinux，修改 /etc/reslove 文件，命令及显示结果如下：

```
[root@centosA ~]# cat /etc/resolv.conf
Search S19.com      ------ 在 S19.COM 域中查询
nameserver 192.168.1.10 ---- 指定域控制器（DNS 服务器的地址）
```

（2）修改时区，命令及显示结果如下：

```
[root@centosA ~]# timedatectl set-timezone Asia/Shanghai
[root@centosA ~]# timedatectl
      Local time: Sun 2021-05-02 22:54:19 CST
  Universal time: Sun 2021-05-02 14:54:19 UTC
        RTC time: Sun 2021-05-02 15:10:07
       Time zone: Asia/Shanghai (CST, +0800)
     NTP enabled: yes
NTP synchronized: no
 RTC in local TZ: no
      DST active: n/a
```

（3）安装 Chrony，将 NTP 服务器的地址指向域控制器（域控制器承担 NTP 服务器的角色），然后进行时钟同步，命令及显示结果如下：

```
[root@centosA ~]# cat /etc/chrony.conf
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (http://www.pool.ntp.org/join.html).
server 192.168.1.200 iburst    ---- 指向 NTP 服务器
# Record the rate at which the system clock gains/losses time.
driftfile /var/lib/chrony/drift
。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。。

[root@centosA ~]# chronyc sourcestats -v    ----- 进行时钟同步
210 Number of sources = 1
                             .- Number of sample points in measurement set.
                            /    .- Number of residual runs with same sign.
                           |    /    .- Length of measurement set (time).
                           |   |    /      .- Est. clock freq error (ppm).
                           |   |   |      /           .- Est. error in freq.
                           |   |   |     |           /         .- Est. offset.
                           |   |   |     |          |          |   On the -.
                           |   |   |     |          |          |   samples.\
                           |   |   |     |          |          |            |
Name/IP Address     NP  NR  Span  Frequency  Freq Skew  Offset  Std Dev
======================================================================
============
192.168.10.200        9   4   518     +9.087     34.849  +28315s   2916us
```

◆ 实训 3　Windows 客户端通过 NTP 服务器同步时间

Windows 客户端通过 NTP 服务同步时间的操作步骤如下：

（1）打开客户端的时间设置对话框，选择“Internet 时间”选项卡，单击“更改设置”按钮，如图 7.111 所示。

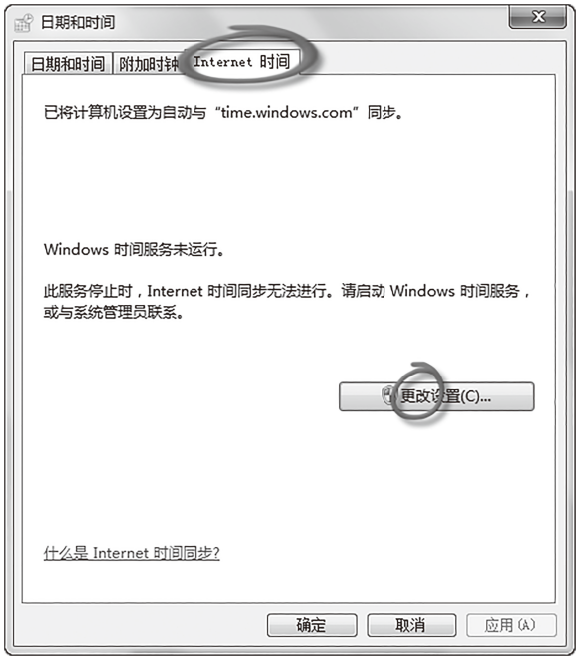

图 7.111　更改 Internet 时间设置

（2）在服务器栏输入 NTP 服务器的 IP 地址（也可以是域名），单击“立即更新”按钮，如图 7.112 所示。

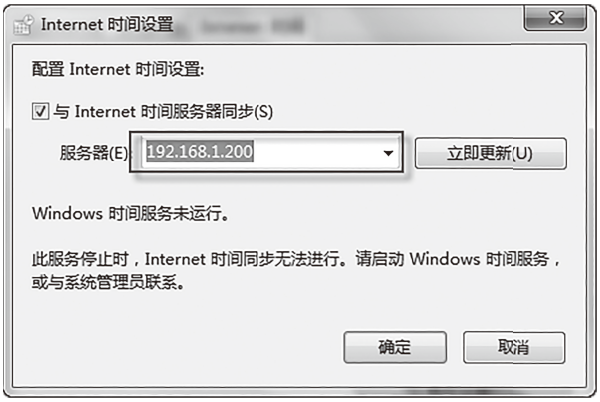

图 7.112　设置服务器地址

（3）如果配置没有问题，系统会提示时间更新成功，如图 7.113 所示。

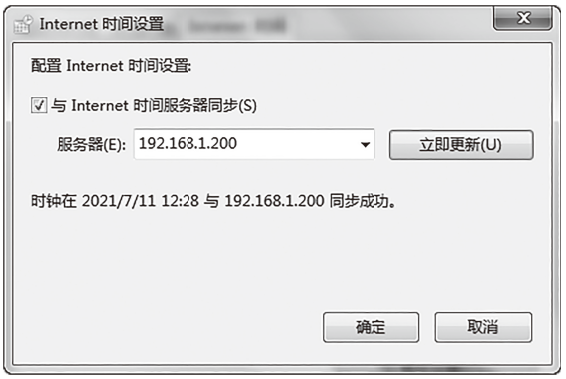

图 7.113　时间同步成功提示

7.7 DHCP 服务器

DHCP（动态主机配置协议）的前身是 BOOTP 协议，是基于 UDP 协议的局域网协议，主要使用 67（服务端）和 68（客户端）端口通信。DHCP 通常部署于局域网环境，用于集中管理和自动分配 IP 地址，使客户端能够动态获取 IP 地址、网关及 DNS 等网络参数。简言之，DHCP 能够自动为内网设备分配网络配置信息，而无须手动输入或登录账号认证。

7.7.1　实训环境

（1）VMware Workstation 安装的 Windows Server 2019 操作系统，且系统能够正常登录。

（2）组件需求：VMware Workstation DHCP Server Windows 部署服务。

7.7.2　实训内容

实训目标

（1）了解 DHCP 的原理，掌握 DHCP 的配置方法。

（2）掌握无人值守系统安装的配置方法。

◆ 实训 1　DHCP 分服务器的授权

DHCP 服务器安装好后，并不能立刻为 DHCP 客户端提供 DHCP 服务，还必须经过授权，未经过授权的 DHCP 服务器将无法将 IP 地址出租给客户端。为 DHCP 服务器授权的操作步骤如下：

（1）在“服务器角色”界面中勾选“DHCP 服务器”多选项，点击“下一步”按钮，如图 7.114 所示。

图 7.114　勾选“DHCP 服务器”多选项

（2）连续两次单击“下一步”按钮，在“确认”界面中单击“安装”按钮，开始安装组件，如图 7.115 和图 7.116 所示。

图 7.115　确认安装所选内容界面

图 7.116　安装过程

（3）安装完成后，单击“完成 DHCP 配置”链接按钮，如图 6.117 所示。

图 7.117　安装完成进行配置

（4）打开“描述”界面，单击“下一步”按钮，如图 7.118 所示。

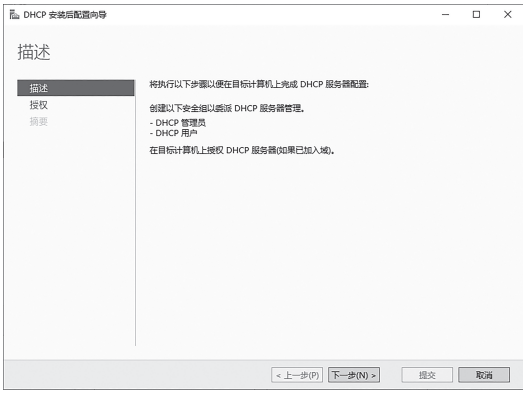

图 7.118　“描述”界面

（5）进入“授权”界面，在该界面中选择“使用以下用户凭据”单选项，用户名默认为域管理员账户，单击“下一步”按钮，如图 7.119 所示。

图 7.119　指定授权用户

（6）单击“下一步”按钮，完成 DHCP 服务器的授权，显示界面如图 7.120 所示。

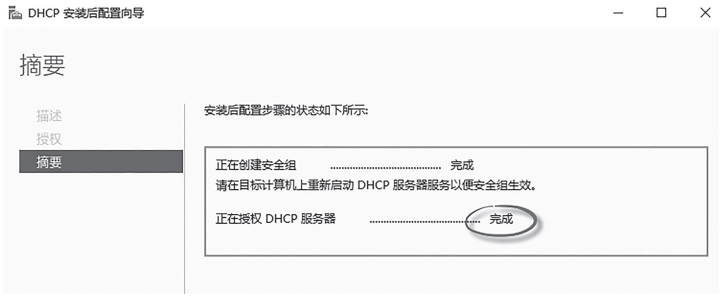

图 7.120　授权配置完成

◆ 实训 2　DHCP 作用域的配置

DHCP 作用域的配置步骤如下：

（1）在服务器管理器中选择“DHCP”选项，在右侧对话框中右键单击服务器名称，在弹出的快捷菜单中选择“DHCP 管理器”选项，如图 7.121 所示。

图 7.121　选择“DHCP 管理器”选项

（2）在打开的“DHCP”窗口中展开名称为“DC.S19.COM”的服务器，右键单击“IPv4”选项，在弹出的右键菜单中选择“新建作用域”选项，如图 7.122 所示。

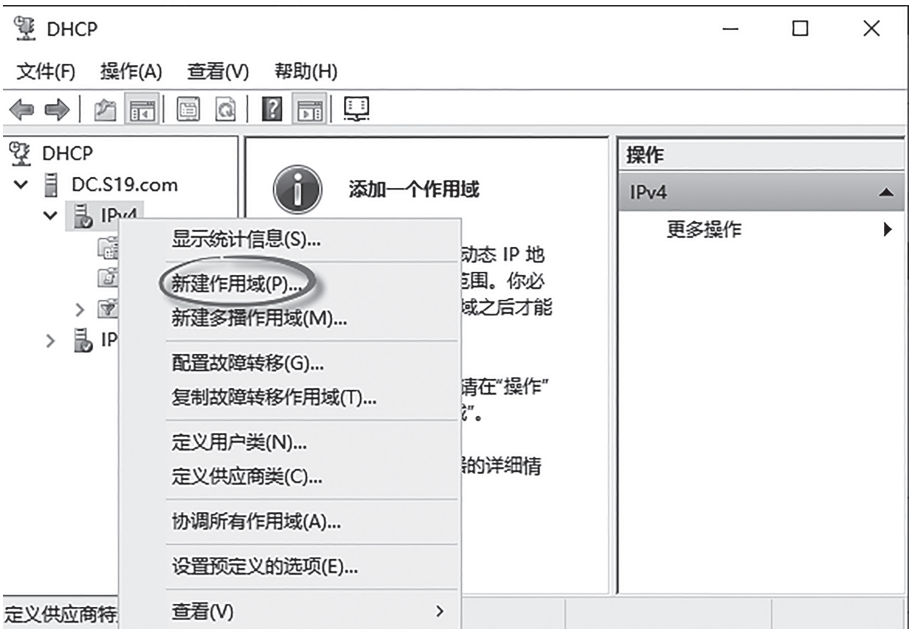

图 7.122　选择“新建作用域”选项

（3）在“新建作用域向导”对话框中输入作用域的名称，单击“下一步”按钮，如图 7.123 所示。

（4）在对话框中输入起始 IP 地址，注意需要排除网关地址，并设置子网掩码的长度，再单击“下一步”按钮，如图 7.124 所示。

图 7.123　设置作用域名称

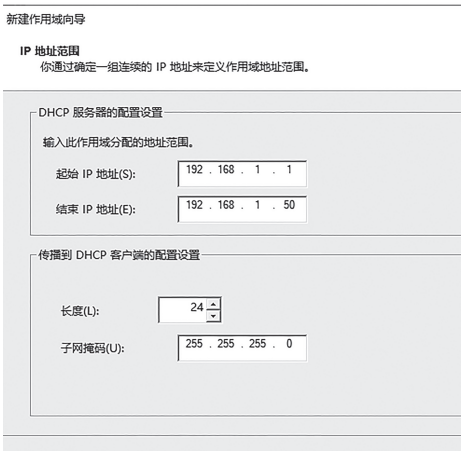

图 7.124　设置起始 IP 地址和子网掩码长度

（5）按照需求添加需要排除的 IP 地址范围，单击“下一步”按钮，如图 7.125 所示。

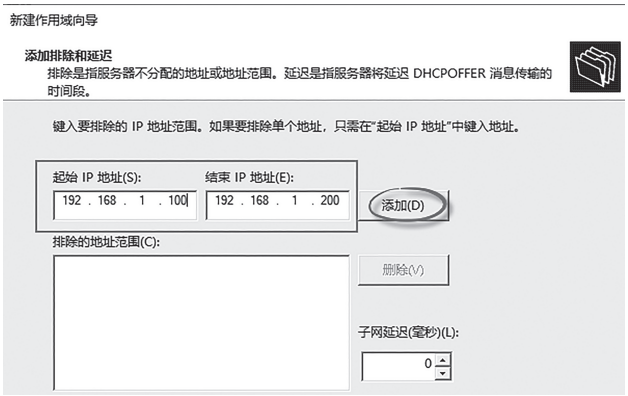

图 7.125　设置需要排除的 IP 地址范围

（6）设置合适的租用期限，再单击“下一步”按钮，如图 7.126 所示。

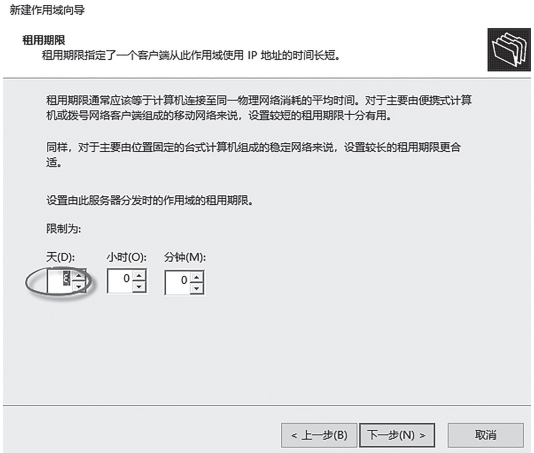

图 7.126　设置租用期限

（7）启用以上几步的配置，选择“是，我想现在配置这些选项”选项，单击“下一步”按钮，如图 7.127 所示。

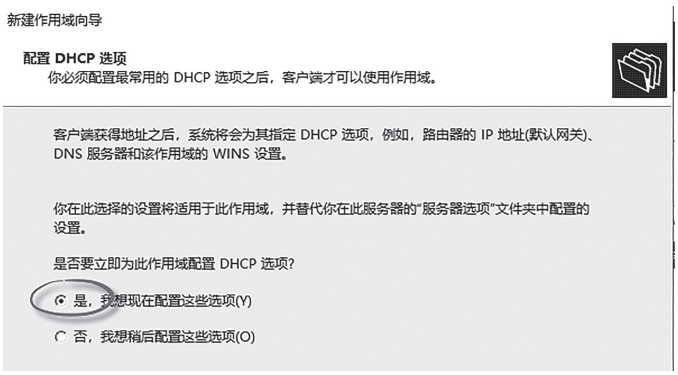

图 7.127　配置 DHCP 选项

（8）配置好 DNS 服务器的名称和 IP 地址，单击“下一步”按钮，如图 7.128 所示。

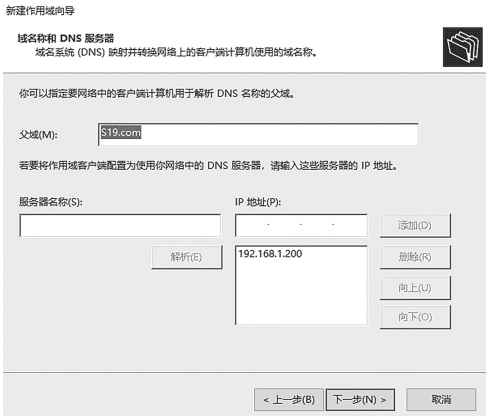

图 7.128　配置服务器名称和 IP 地址

（9）选择“是，我想现在激活此作用域”激活上述所配置的作用域，单击“下一步”按钮，再单击“完成”按钮，即完成作用域的配置，如图 7.129 和图 7.130 所示。

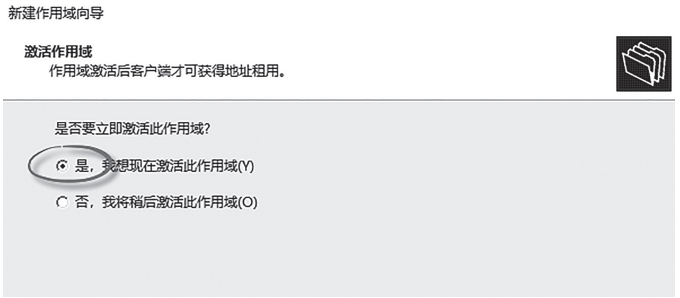

图 7.129　选择激活作用域选项

图 7.130　完成新建作用域

（10）展开 DHCP 服务器，查看已经配置的作用域选项，如图 7.131 所示。

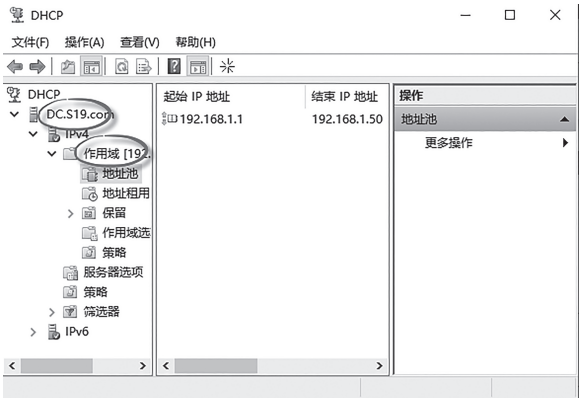

图 7.131　查看 DHCP 的作用域

（11）在 DHCP 客户端上设置 IP 地址和 DNS 服务器的地址，让 DHCP 自动获取，DHCP 服务器会将地址租用给 DHCP 客户端，如图 7.132 和图 7.133 所示。

图 7.132　显示网络连接详细信息

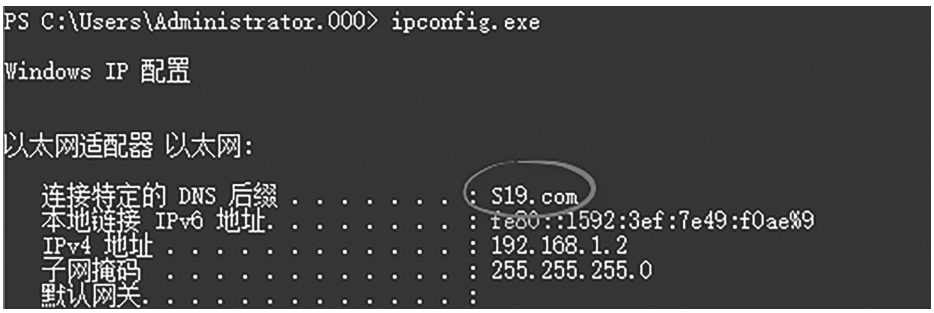

图 7.133　查看网络配置信息

7.8 DNS 服务器配置

DNS（domain name system，域名系统）是因特网上一个用于实现域名与 IP 地址相互映射的分布式数据库。它使用户能够通过域名方便地访问互联网，而无须记住机器直接可读的数字 IP 地址串。通过域名获取其对应 IP 地址的过程叫作域名解析（或主机名解析）。DNS 协议基于 UDP 协议运行，使用 53 号端口。

7.8.1 实训环境

（1）VMware Workstation 安装 Windows Server 2019 操作系统。

（2）组件需求：VMware Workstation DNS。

7.8.2 实训内容

实训目标

（1）了解 DNS 的概念。

（2）掌握主 DNS 的配置。

（3）掌握辅助 DNS 的配置。

◆ 实训　DNS 服务器的配置

由于之前已经安装了 Active Directory 服务组件，DNS 服务组件已一并安装，下面进行 DNS 服务器的配置，操作步骤如下：

（1）进入服务器管理器界面，单击左侧的“DNS”选项，在右侧的对话框中右键单击服务器名称，在弹出的菜单中选择“DNS 管理器”选项，如图 7.134 所示。

图 7.134　选择“DNS 管理器”选项

（2）打开“DNS 管理器”窗口，展开后选中根域名称，可以看到正向区域已经创建，如图 7.135 所示。

图 7.135　DNS 管理器窗口

（3）选中根域名称，右键单击“反向查找区域”选项，在弹出的快捷菜单中选择“新建区域”选项，如图 7.136 所示。

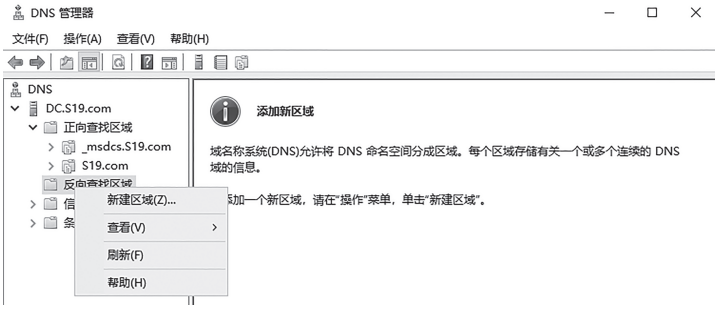

图 7.136　选择“新建区域”选项

（4）在反向查找区域的“网络 ID”栏目下输入 DNS 服务器所在的 IP 地址，单击“下一步”按钮，如图 7.137 所示。

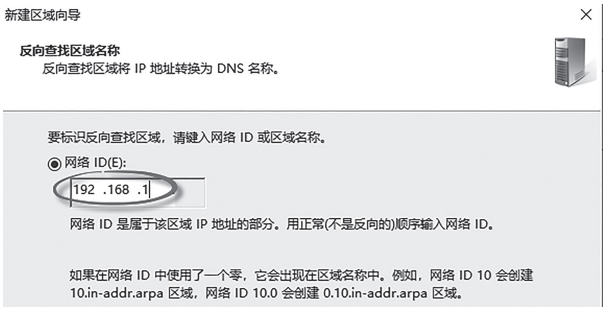

图 7.137　输入网络 ID

（5）在“动态更新”对话框中选择“不允许动态更新”单选项，单击“完成”按钮，即可创建反向查找区域，如图 7.138 所示。

图 7.138　选择“不允许动态更新”单选项

（6）选中 DNS 域名，在右侧对话框中单击右键，在弹出的快捷菜单中选择“新建主机（A 或 AAAA）”选项，创建主机记录，如图 7.139 所示。

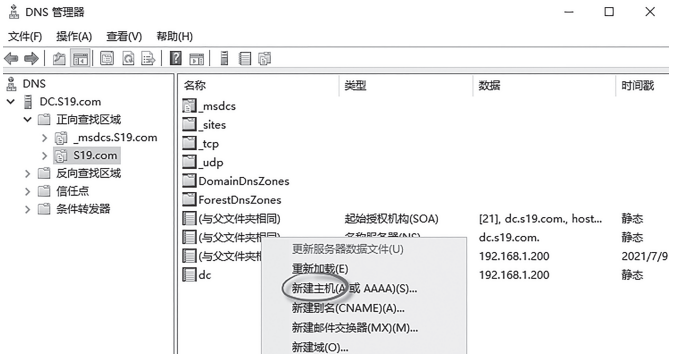

图 7.139　新建主机（A 或 AAAA）操作

（7）在“新建主机”对话框中输入主机名和 IP 地址，单击“添加主机”按钮（见图 7.140），即可添加一条主机记录，成功后显示如图 7.141 所示的提示信息。之后再添加 3 条主机记录。

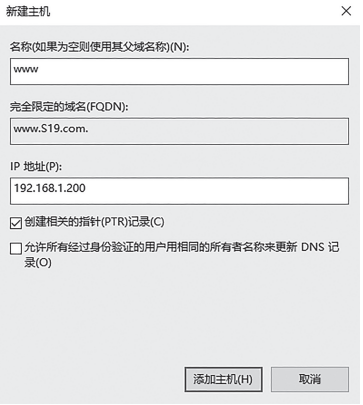

图 7.140　添加主机记录

图 7.141　添加成功提示

（8）查询已经创建的主机记录。展开“正向查找区域”，单击根域名称，在右侧可以看到新添加的 4 条主机记录，如图 7.142 所示。

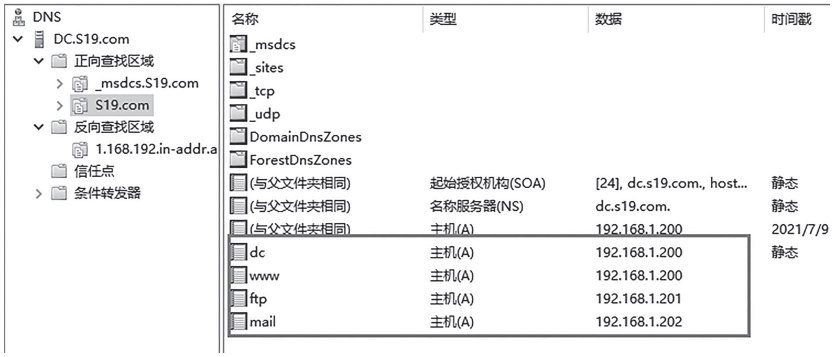

图 7.142　查看新建的主机记录

（9）同样，展开“反向查找区域”，单击根域名称，在右侧可以看到新添加的查询方向 PTR 指针记录，如图 7.143 所示。

图 7.143　查看反向查找记录

（10）在客户端命令模式下执行 nslookup 命令，可以查看 DNS 服务器的详细信息。需要注意的是，在执行 nslookup 命令前，需先将 DNS 服务器的 IP 地址指向

DNS 服务器，关闭防火墙。若防火墙处于开启状态，须放行 DNS 服务端口（TCP/UDP 53）；随后执行主机名解析测试，结果如图 7.144 所示。

```
PS C:\Users> nslookup.exe
默认服务器:  www.s19.com
Address:  192.168.1.200

> www.s19.com
服务器:  www.s19.com
Address:  192.168.1.200

名称:    www.s19.com
Address:  192.168.1.200

> ftp.s19.com
服务器:  www.s19.com
Address:  192.168.1.200

名称:    ftp.s19.com
Address:  192.168.1.201

> mail.s19.com
服务器:  www.s19.com
Address:  192.168.1.200

名称:    mail.s19.com
Address:  192.168.1.202
```

图 7.144　用命令查看 DNS 详细信息

（11）此外，利用 nslookup 命令也可查询 DNS 中类型为 SOA（起始授权机构）及 PTR（指针）的记录，具体操作与结果如图 7.145 所示。

```
PS C:\Users> nslookup.exe -type=soa s19.com
服务器:  www.s19.com
Address:  192.168.1.200

s19.com
        primary name server = dc.s19.com
        responsible mail addr = hostmaster.s19.com
        serial  = 30
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
dc.s19.com      internet address = 192.168.1.200
PS C:\Users> nslookup.exe -type=ptr s19.com
服务器:  www.s19.com
Address:  192.168.1.200

s19.com
        primary name server = dc.s19.com
        responsible mail addr = hostmaster.s19.com
        serial  = 30
        refresh = 900 (15 mins)
        retry   = 600 (10 mins)
        expire  = 86400 (1 day)
        default TTL = 3600 (1 hour)
```

图 7.145　用命令查看 DNS 中 SOA 与 PTR 记录