模块 1

Windows Server 2019 的安装与基本配置

本模块主要对 Windows Server 2019 的安装与基本配置进行讲解，首先对 Windows Server 2019 的安装和基本网络信息的配置进行介绍，接着对 Windows Admin Center 的安装和使用进行说明，最后对本地安全策略配置的有效性和 Windows Server 2019 密码的恢复方法进行说明。

通过本模块的学习，读者将达到以下职业能力目标和要求：

◎ 了解 Windows Server 2019 操作系统的版本和发展历程。

◎ 掌握在虚拟机中安装 Windows Server 2019 的方法。

◎ 掌握配置 Windows Server 2019 的方法。

◎ 掌握恢复 Windows Server 2019 密码的方法。

1.1 Windows Server 2019 环境搭建

1.1.1 Windows Server 2019 介绍

Windows Server 2019 操作系统是微软公司在 2018 年 10 月 2 日发布，并于 2018 年 10 月 25 日正式商用的服务器操作系统。Windows Server 2019 相较于之前的 Windows Server 版本融合了更多云计算、大数据时代的新特性，包括更先进的安全性，广泛支持容器基础，原生支持混合云扩展，提供低成本的超融合架构，让用户在本地数据中心也能拥有接轨未来趋势的创新平台。

根据组织规模、虚拟化和数据中心的需求，微软公司将 Windows Server 2019 操作系统分为以下 3 个版本：

(1)Standard Edition(标准版)：适用于物理或最低限度虚拟化环境。

(2)Datacenter Edition(数据中心版)：适用于高虚拟化数据中心和云环境。

(3)Essentials Edition(基本版)：适用于最多 25 个用户或最多 50 台设备的小型企业。

Windows Server 2019 操作系统数据中心版独有的功能包括网络控制器、主机保护者服务(Hyper-V 主机环境)、软件定义网络和存储空间直通。

1.1.2 安装部署虚拟机

正所谓“工欲善其事，必先利其器”，要想学好 Windows 网络服务，必须有一台装有 Windows Server 操作系统的计算机，学习者也不太可能买一台计算机来单独安装 Windows Server 操作系统进行学习，所以建议使用虚拟机软件来安装 Windows Server 操作系统。本书采用的虚拟机软件是 VMware Workstation 15。

运行下载的 VMware Workstation 虚拟机软件，将会看到如图 1-1 所示的程序安装向导初始界面。

图 1-1 虚拟机程序安装向导初始界面

在 Windows 系统中，VMware Workstation 虚拟机软件的安装比较简单，在此不再赘述。安装完成后的虚拟机软件管理界面，如图 1-2 所示。

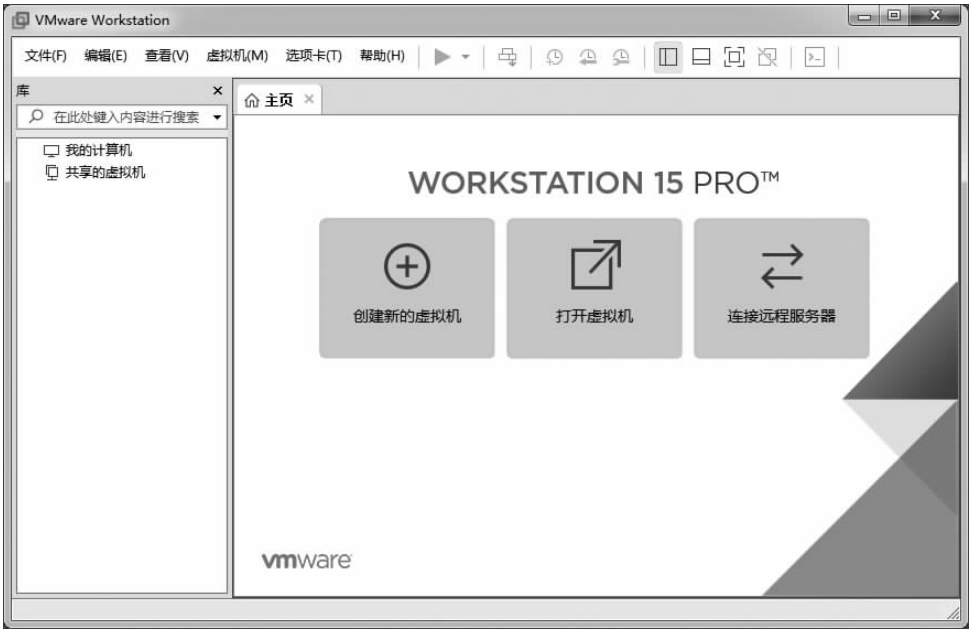

图 1-2　虚拟机软件管理界面

1.1.3　安装 Windows Server 2019

1. 下载 ISO 镜像

从 MSDN 官网(https://msdn.itellyou.cn)中找到 Windows Server 2019 的 ISO 镜像链接进行下载，如图 1-3 所示。

图 1-3　ISO 镜像文件下载

2. 创建虚拟机

在虚拟机软件管理界面中选择“创建新的虚拟机”选项，然后在弹出的“新建虚拟机向导”对话框中选中“典型(推荐)”单选按钮，如图 1-4 所示。

图 1-4　选中“典型(推荐)”单选按钮

单击“下一步”按钮，进入“安装客户机操作系统”界面，选中“安装程序光盘映像文件(iso)”单选按钮，单击“浏览”按钮，选择 ISO 文件所在路径，如图 1-5 所示。

图 1-5　选择 ISO 文件所在路径

单击“下一步”按钮，进入“选择客户机操作系统”界面，设置“客户机操作系统”的类型为“Microsoft Windows”，“版本”为“Windows Server 2016”（软件中暂无“Windows Server 2019”选项），如图 1-6 所示。

图 1-6　设置客户机操作系统

单击“下一步”按钮，进入“命名虚拟机”界面，在“虚拟机名称”文本框中输入“Windows Server 2019”，建议将“位置”设置在剩余空间比较多的物理磁盘中，如图 1-7 所示。

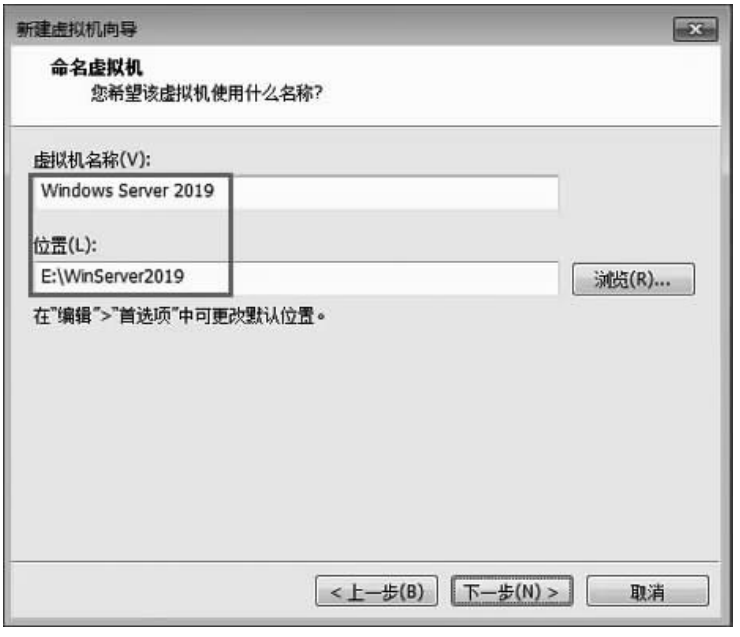

图 1-7　命名虚拟机

单击“下一步”按钮，进入“指定磁盘容量”界面，虚拟机的“最大磁盘大小(GB)”采用默认值“60.0”，选中“将虚拟磁盘存储为单个文件”单选按钮(目的是使文件不那么凌乱)，如图 1-8 所示。

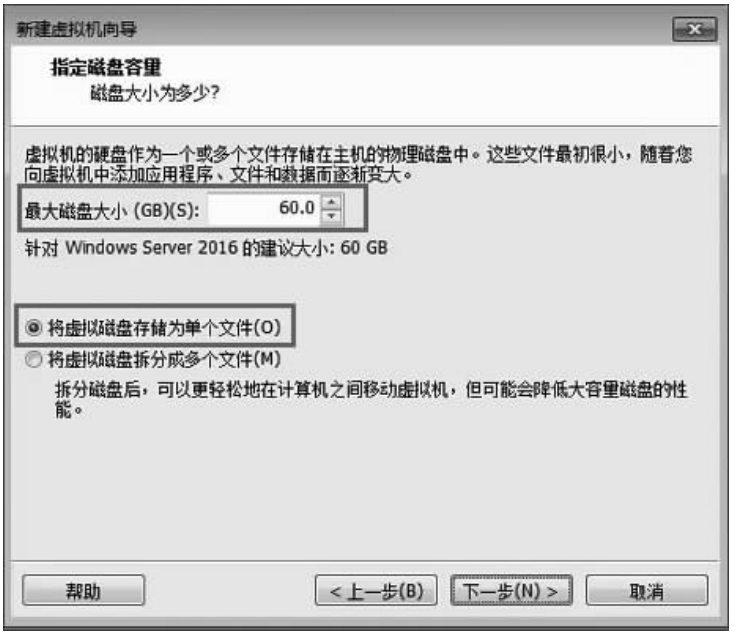

图 1-8　指定磁盘容量

单击“下一步”按钮，进入“已准备好创建虚拟机”界面(见图 1-9)，可以单击“自定义硬件”按钮，调整硬盘、内存及网络连接模式。确认配置无误，单击“完成”按钮。虚拟机配置成功后，进入如图 1-10 所示的界面。

图 1-9　“已准备好创建虚拟机”界面

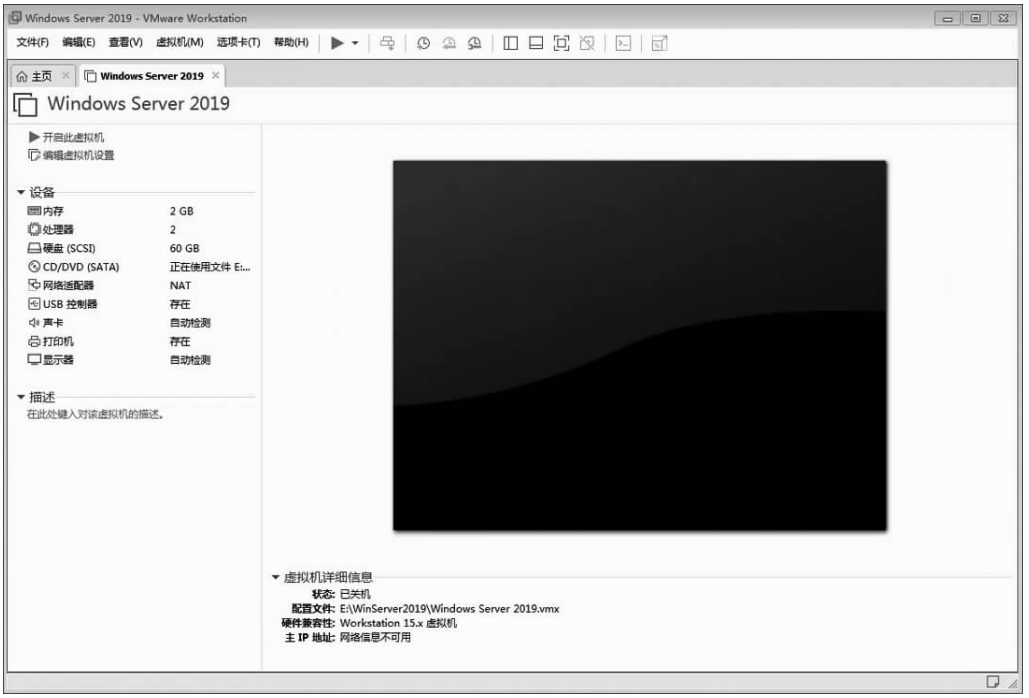

图 1-10　虚拟机配置成功后的界面

安装 Windows Server 2019 操作系统时，计算机的 CPU 需要支持虚拟化技术（virtualization technology，VT），可以在 BIOS 中开启 VT 功能，相关操作在此不再赘述。

安装 Windows Server 2019 操作系统的方法和安装 Windows Server 其他版本的操作系统大同小异。在虚拟机软件管理界面中选择“开启此虚拟机”选项，几秒后就能进入“选择要安装的操作系统”界面，如图 1-11 所示。

图 1-11　“选择要安装的操作系统”界面

选择“Windows Server 2019 Standard(桌面体验)”版有助于初学者操作与理解,单击“下一步”按钮,进行 Windows 系统文件的安装,如图 1-12 所示。

图 1-12　安装 Windows 系统文件

操作系统安装进度的快慢视计算机的配置情况而定,大概持续 20 min。系统安装完成后出现的登录界面,如图 1-13 所示。

图 1-13　登 录 界 面

解锁后用安装过程中所设定的用户名及密码进行登录,进入“服务器管理器”窗口,如图 1-14 所示。

图 1-14　“服务器管理器”窗口

1.1.4　配置网络信息

1. 更改计算机名

安装完成的 Windows Server 2019 使用的是由系统随机配置的计算机名。为了更好地标识和识别服务器，应将其更改为有一定意义的名称。

单击虚拟机任务栏（或者“开始”菜单）中的“服务器管理器”按钮，打开“服务器管理器”窗口。选择“本地服务器”选项，单击“计算机名”后面的名称，弹出“系统属性”对话框。单击“更改”按钮，弹出“计算机名/域更改”对话框，在“计算机名”文本框中输入新的名称（如 WinServer2019），单击“确定”按钮，如图 1-15 所示。

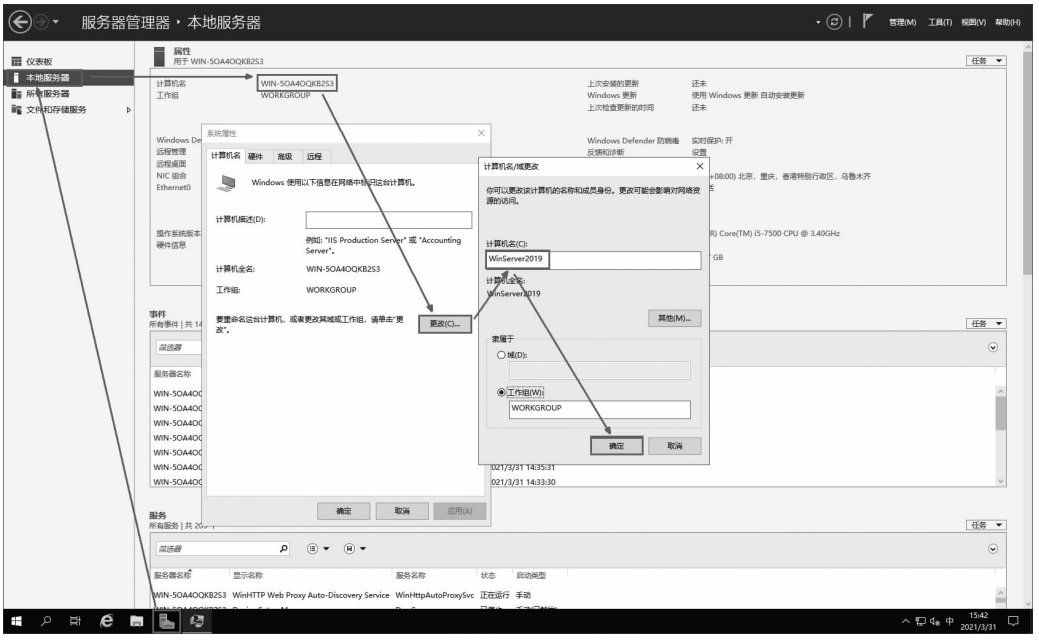

图 1-15　更改计算机名

在弹出的“重新启动计算机”提示框中单击“确定”按钮，以保证新的计算机名重启后应用更改。

2. 配置网络

1）VMware 虚拟网络编辑器

VMware Workstation 虚拟机软件提供了多种可选的网络模式，这里主要解释“桥接模式”“NAT 模式”和“仅主机模式”。系统默认采用“NAT 模式”，如图 1-16 所示。

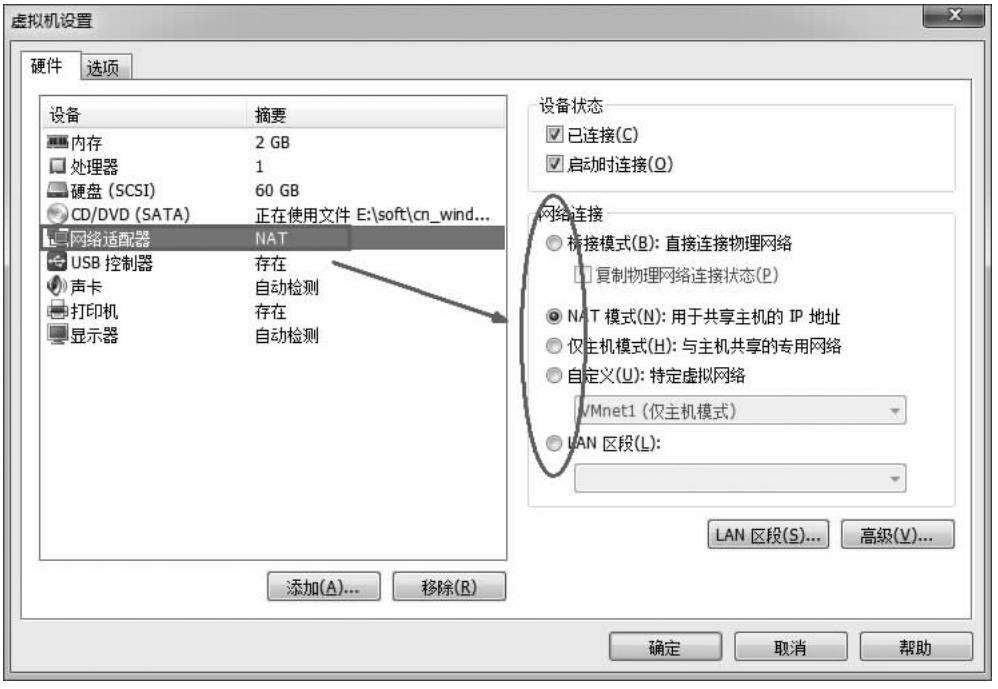

图 1-16　选择虚拟机网络模式

桥接模式就是将主机网卡与虚拟机的虚拟网卡利用虚拟网桥进行通信。在桥接的作用下，类似于把物理主机虚拟为一个交换机，所有桥接设置的虚拟机都连接到这个交换机的一个接口上，物理主机也同样插在这个交换机中。所以，所有桥接下的计算机网卡间都是交换模式，可以相互访问而不干扰。在桥接模式下，虚拟机的 IP 地址需要与主机在同一个网段内，如果需要联网，则网关和域名系统（domain name system，DNS）需要与主机网卡一致，即虚拟机对外界来说就好比独立的物理计算机。虚拟机桥接模式的网络结构如图 1-17 所示。

如果网络 IP 资源紧缺，但是用户又希望虚拟机能够联网，这时候 NAT 模式是最好的选择。NAT 模式借助虚拟 NAT 设备和虚拟动态主机配置协议（dynamic host configuration protocol，DHCP）服务器，使得虚拟机可以联网。虚拟机会将虚拟 NAT 设备和虚拟 DHCP 服务器连接到 VMnet8 虚拟交换机上，同时也会将主机上的 VMware Network Adapter VMnet8 虚拟网卡连接到 VMnet8 虚拟交换机上。虚拟网卡只是作为主机与虚拟机通信的接口，虚拟机并不是依靠 VMware Network Adapter VMnet8 虚拟网卡来联网的。虚拟机 NAT 模式的网络结构如图 1-18 所示。

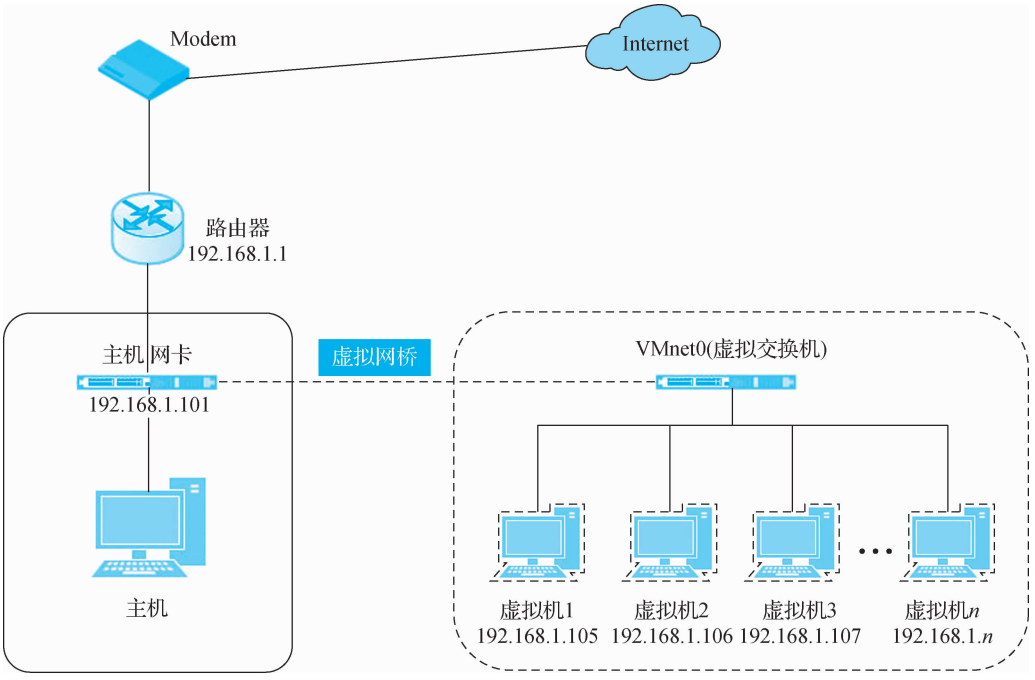

图 1-17　虚拟机桥接模式的网络结构

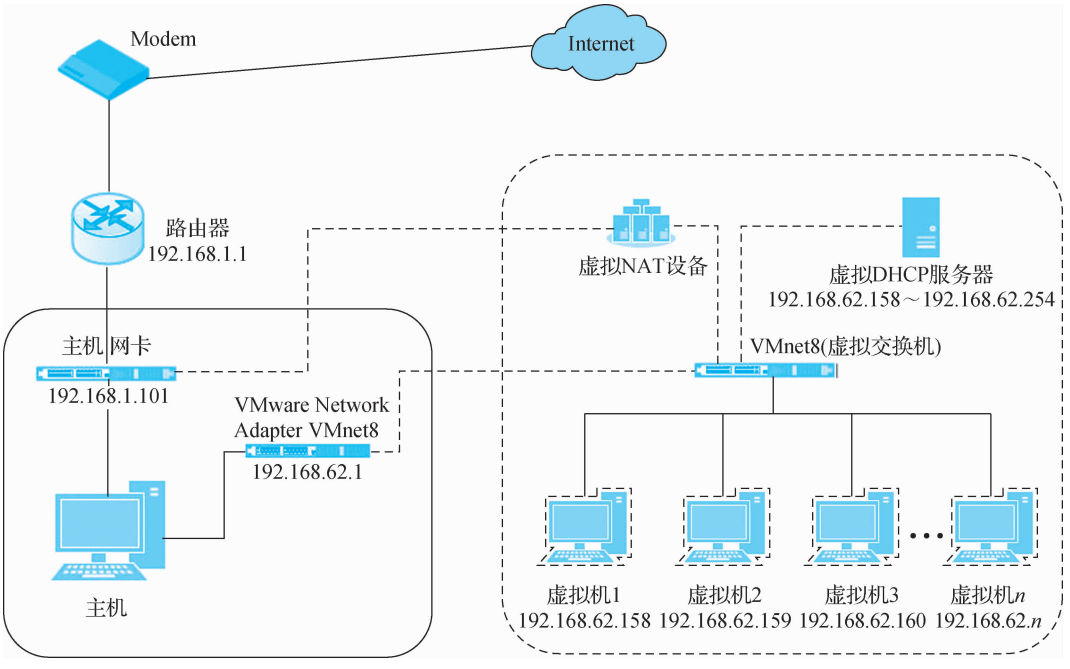

图 1-18　虚拟机 NAT 模式的网络结构

仅主机模式其实就是 NAT 模式去除了虚拟 NAT 设备，然后使用 VMware Network Adapter VMnet1 虚拟网卡连接 VMnet1 虚拟交换机来与虚拟机通信的。仅主机模式将虚

拟机与外网隔开，使得虚拟机成为一个独立的系统，只与主机相互通信。如果想要在仅主机模式下联网，可以将能联网的主机网卡共享给 VMware Network Adapter VMnet1，这样就可以实现虚拟机联网。虚拟机仅主机模式的网络结构如图 1-19 所示。

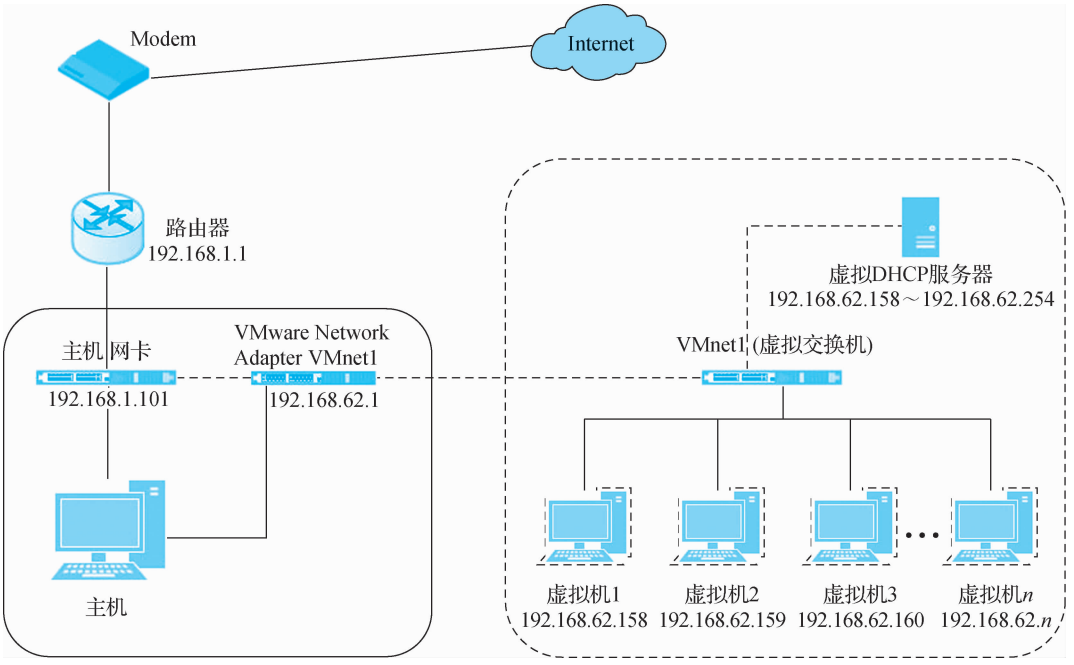

图 1-19　虚拟机仅主机模式的网络结构

在虚拟机软件管理界面中，执行“编辑”→“虚拟网络编辑器”命令，弹出“虚拟网络编辑器”对话框，可根据实际情况进行桥接模式、NAT 模式和仅主机模式相关信息（如子网 IP、子网掩码、DHCP、桥接网卡等）的设置，如图 1-20 所示。

图 1-20　设置虚拟网络编辑器

2)Windows Server 网络配置

Windows Server 2019 安装完成后,默认自动获取 IP 地址,由于服务器是为网络提供服务器的,通常需要设置其为静态 IP 地址。

单击虚拟机任务栏(或者“开始”菜单)中的“服务器管理器”按钮,打开“服务器管理器”窗口。选择“本地服务器”选项,单击“Ethernet0”后面的 IP 信息,弹出“网络连接”窗口。右击“属性”选项,弹出“Ethernet0 属性”对话框,双击“此连接使用下列项目”选项框中的“Internet 协议版本 4(TCP/IPv4)”,弹出“Internet 协议版本 4(TCP/IPv4)属性”对话框。选中“使用下面的 IP 地址”单选按钮,并输入 IP 地址(192.168.136.250)、子网掩码(255.255.255.0)和默认网关(192.168.136.2),单击“确定”按钮完成静态 IP 地址的设置,如图 1-21 所示。(注:配置的网络信息要与图 1-20 的信息匹配)

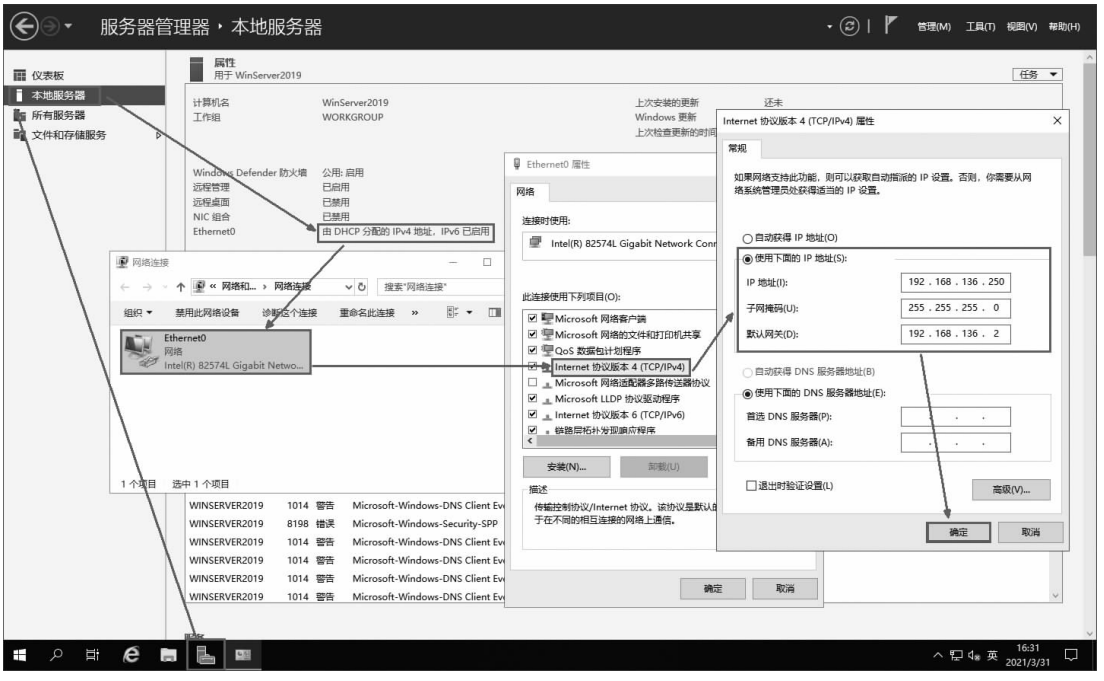

图 1-21　设置 Ethernet0 网卡的静态 IP 地址

3)高级安全 Windows Defender 防火墙

系统安装完成后,防火墙默认处于开启状态,但对于一些特殊场景可能需要进行防火墙的细化操作。

【例 1-1】　公司新安装了一台 Windows 服务器(192.168.136.250),主要实现各部门的资源共享,默认开启防火墙功能,但由于需要 ping 测试网络连通性,因此应进行额外设置。

(1)打开“高级安全 Windows Defender 防火墙”窗口。执行“开始”→“Windows 管理工具”→“高级安全 Windows Defender 防火墙”命令(或在 cmd 窗口中输入 wf.msc 命令),打开“高级安全 Windows Defender 防火墙”窗口,单击左侧目录树中的“入站规则”选项,如图 1-22 所示。

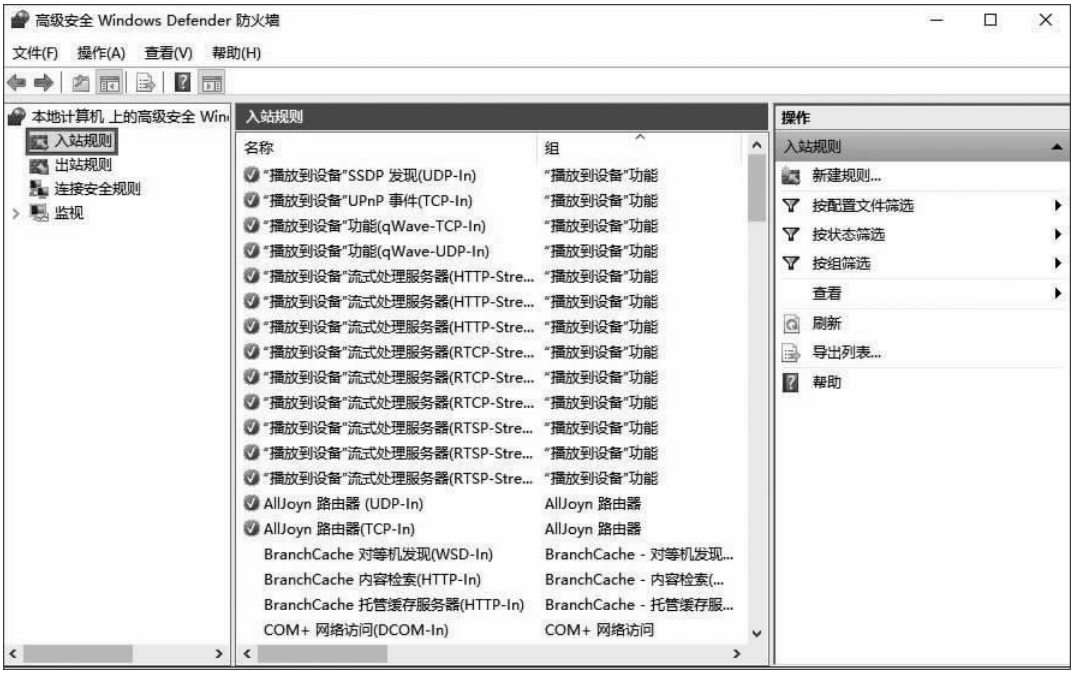

图 1-22　入 站 规 则

(2)新建规则。单击右侧“操作”列中的“新建规则”,弹出“新建入站规则向导-规则类型”对话框,选中“自定义”单选按钮,如图 1-23 所示。

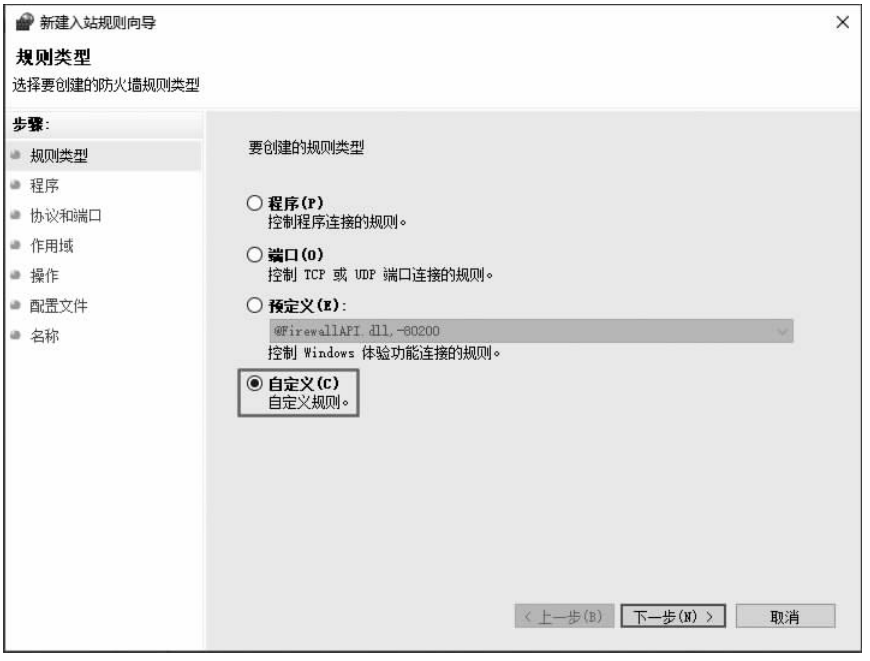

图 1-23　选中“自定义”单选按钮

单击“步骤”列中的“协议和端口”,在右侧界面中指定应用此规则的协议和端口,在“协

议类型”下拉列表框中选择“ICMPv4”，如图 1-24 所示。

图 1-24　选择协议类型

在“作用域”中指定要应用此规则的本地 IP 地址和远程 IP 地址；在“操作”中指定在连接与规则中指定的条件相匹配时要执行的操作；在“配置文件”中指定此规则应用的配置文件；在“名称”中指定此规则的名称和描述（如 ping 规则），单击“完成”按钮，使新规则生效，如图 1-25 所示。

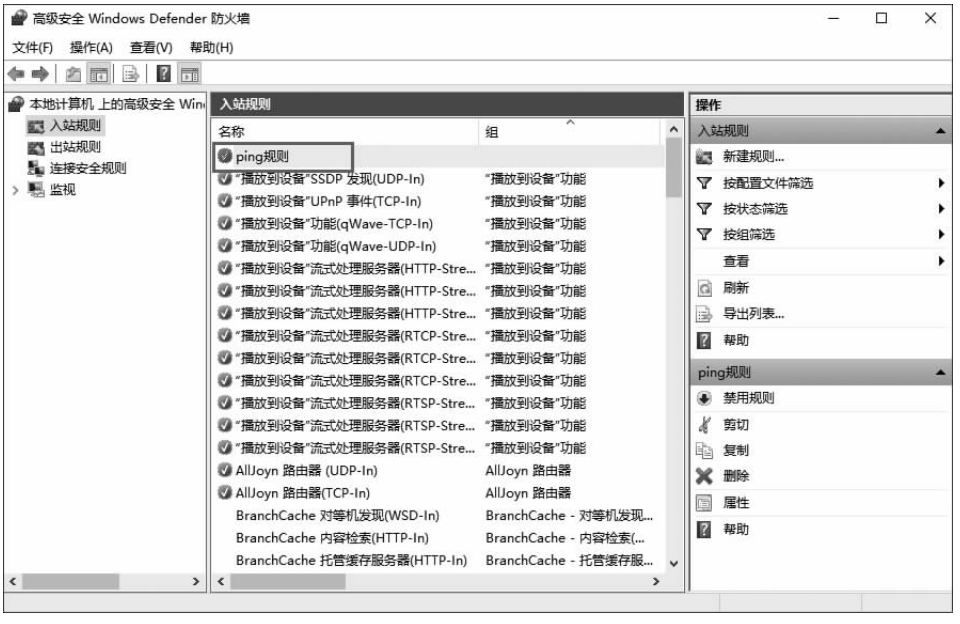

图 1-25　新建 ping 规则

（3）ping 测试。启用 ping 规则与禁用 ping 规则的测试结果如图 1-26 所示。

图 1-26　启用与禁用 ping 规则的测试效果

1.2　运维新利器——Windows Admin Center

1.2.1　了解 Windows Admin Center

Windows Admin Center 是本地部署的基于浏览器的应用，用于管理 Windows 服务器、群集、超融合基础设施和 Windows 10 电脑。它不会在 Windows 之外产生额外费用，并可以在生产中使用，其界面如图 1-27 所示。

图 1-27　Windows Admin Center 的 Web 控制台界面

1. Windows Admin Center 场景用途

(1)简化服务器管理。5 min 内即可完成安装并立即在环境中管理服务器,无须其他配置。

(2)与混合解决方案结合。可与 Azure 集成,选择性地将本地服务器与相关云服务相连。

(3)简化超融合管理。简化 Azure Stack HCI 或 Windows Server 超融合群集的管理,使用简化工作负载创建和管理 VM、存储空间直通卷和软件定义网络等。

Windows Admin Center 是“内部”管理工具[如服务器管理器和微软管理控制台(microsoft management console,MMC)]的现代演进版,通过在 Windows Server 或已加入域的 Windows 10 上安装的 Windows Admin Center 网关来管理 Windows Server 2019、Windows Server 2016、Windows Server 2012 R2、Windows Server 2012、Windows 10、Azure Stack HCI 等。该网关通过使用远程 PowerShell 管理服务器,并通过 WinRM 管理 WMI。

2. 下载 Windows Admin Center

Windows Admin Center 可以进入微软官网进行下载,其他途径亦可。

Windows Admin Center 软件是 msi 格式的,下载后双击即可安装,监听端口可根据实际情况修改(默认 443 端口),如图 1-28 所示。

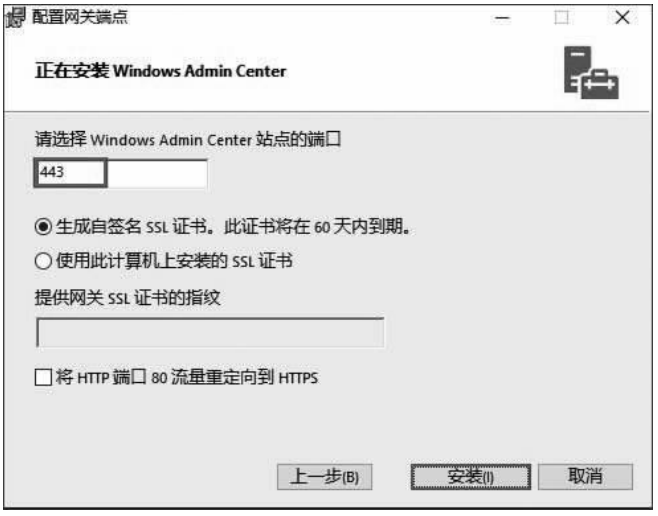

图 1-28　安装 Windows Admin Center 并设置监听端口

3. 浏览器登录 Windows Admin Center

安装完成后,从远程计算机打开 Web 浏览器,输入安装程序最后一步提供的统一资源定位器(uniform resource locator,URL),如“https://<Your-WindowsServer-IP>:443”,并输入具有管理员权限的用户名和密码,如图 1-29 所示。

> **注意:**登录前需要设置防火墙放行监听端口的流量,可能需要多次输入用户名和密码。

图 1-29　以 Web 方式登录 Windows Admin Center

1.2.2　创建本地用户与组

Windows Server 2019 支持两种用户账户：本地账户和域账户。本地账户只能登录到一台特定的计算机上，并访问其资源；域账户可以登录到域上，并获得访问网络的权限。

1. 命名约定

(1)账户名必须唯一：本地账户必须在本地计算机上唯一。

(2)账户名不能包含以下字符：?、+、*、<、>、=、"、;、:、,、/、\、[、]、|。

(3)账户名最长不能超过 20 个字符。

2. 密码原则

(1)账户密码最少由 8 个字符组成。

(2)密码由大小写字母、数字和特殊符号(如 !、$、#、?)混合组成。

(3)密码不能太简单，以防被他人猜出。

(4)给 Administrator 账户设置一个密码，以防他人随便使用该账户。

Windows 为每个账户提供了名称，目的是方便用户记忆、输入和使用。系统内部使用安全标识符(security identifier，SID)来识别用户身份，每个用户账户都对应一个唯一的由系统自动生成的安全标识符。当删除一个用户账户后，重新创建名称相同的账户并不能获得先前账户的权利，因为系统指派权利、授权资源访问权限等都需要使用 SID。用户可以在登录后通过“whoami/logonid”命令查询当前用户账户的 SID。

【例 1-2】　通过 Windows Admin Center 的 Web 控制台创建、管理、维护本地用户和组。

(1)创建本地用户 user01。进入 Web 控制台界面，选择左侧列表中的“本地用户和组”

选项，进入“本地用户和组”管理界面，此时可以进行用户和组的操作，如图 1-30 所示。

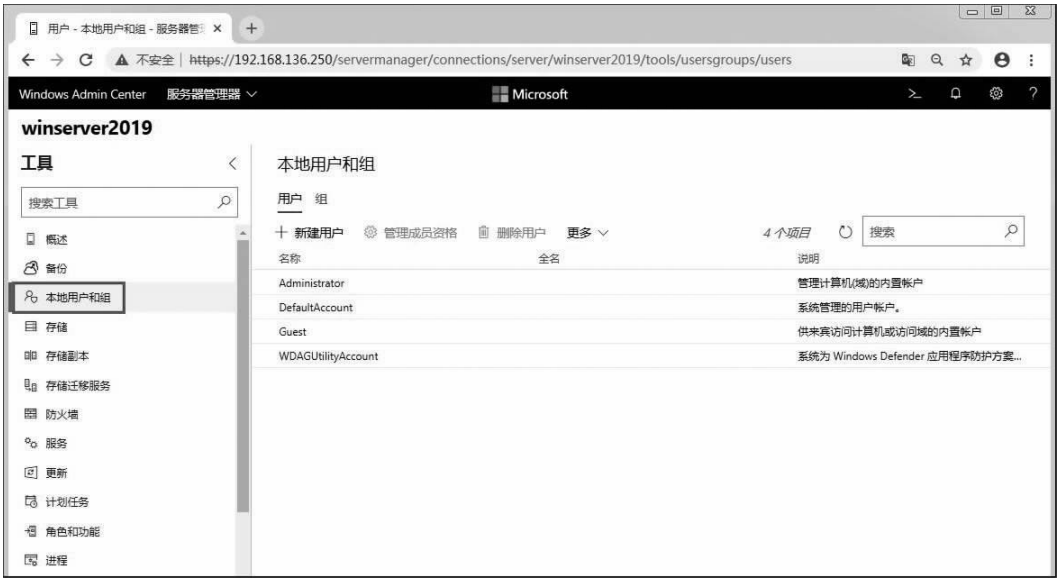

图 1-30　“本地用户和组”管理界面

选择“用户”选项卡下的“新建用户”选项，在打开的“添加新用户”界面中输入 user01 的相关信息，如图 1-31 所示。

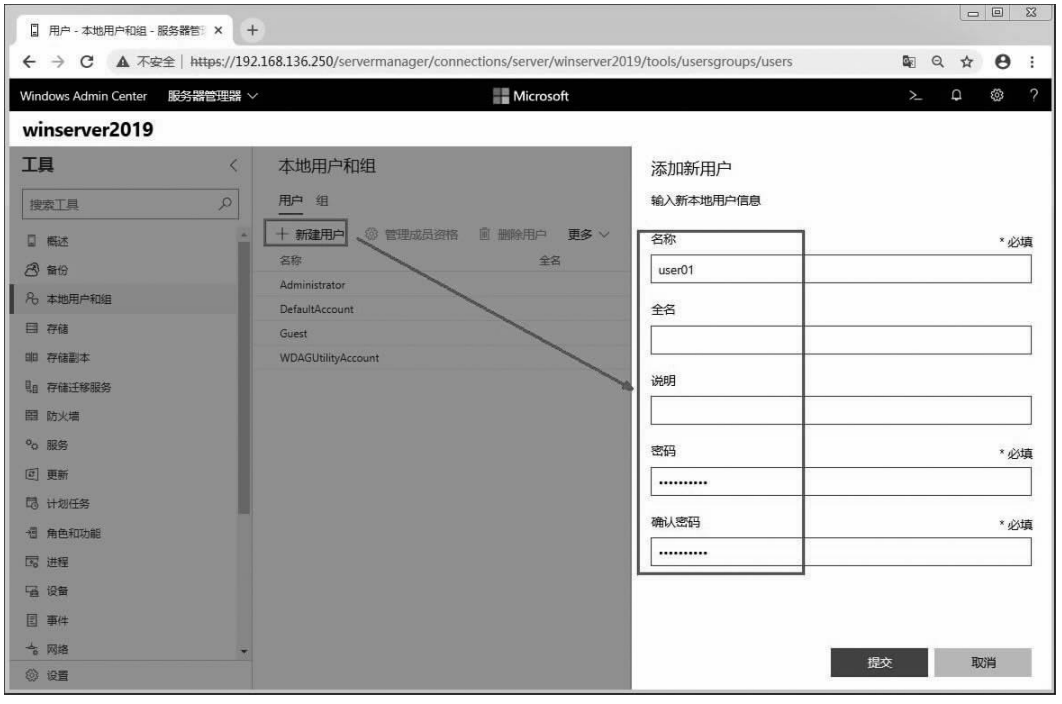

图 1-31　添加新用户 user01

(2)创建本地组 group01。选择“组”选项卡下的“新建组”选项，在打开的“添加新组”界

面中输入 group01 的相关信息，如图 1-32 所示。

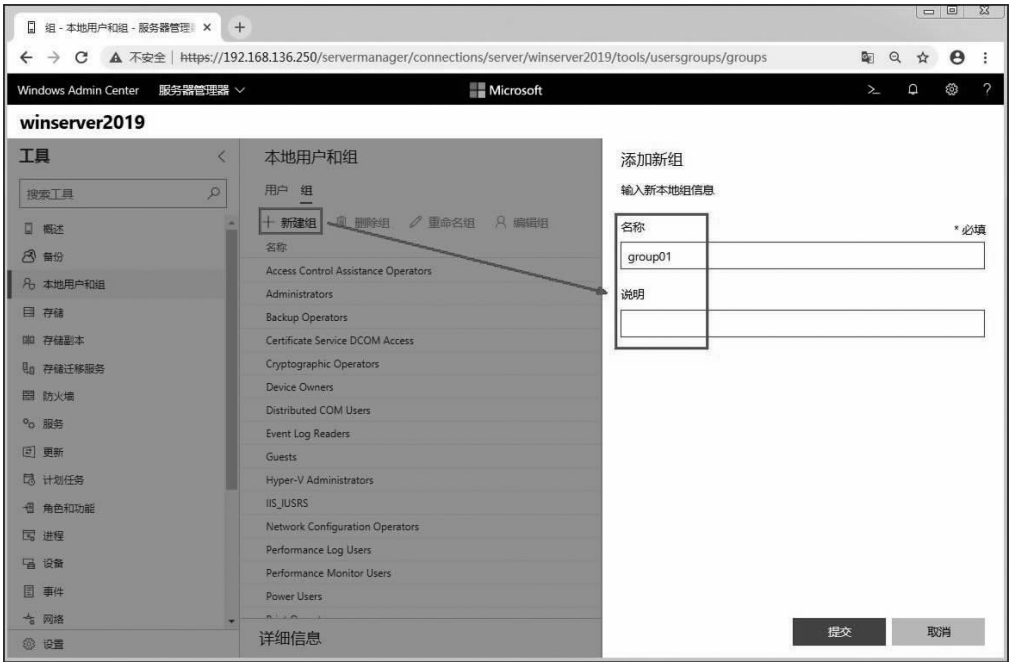

图 1-32　添加新组 group01

(3)将用户 user01 添加到组 group01 中。在“用户”选项卡中，先在“名称”列表中选择“user01”选项，然后选择“管理成员资格”选项，在打开的“管理成员资格”界面中选中“group01”复选框，如图 1-33 所示。

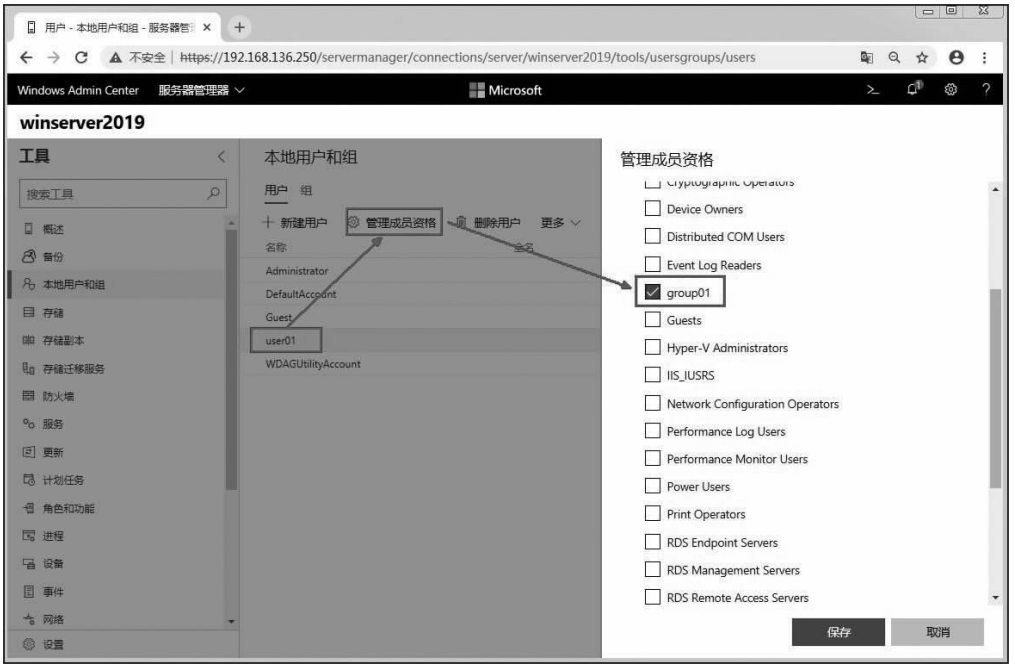

图 1-33　选中“group01”复选框

（4）删除用户 user01 和组 group01。在“用户”选项卡中，先在“名称”列表中选择“user01”选项，然后选择“删除用户”选项，在弹出的“删除用户”提示框中单击“是”按钮，完成用户 user01 的删除，如图 1-34 所示。

图 1-34　删除用户 user01

在“组”选项卡中，先在“名称”列表中选择“group01”选项，然后选择“删除组”选项，在弹出的“删除组”提示框中单击“是”按钮，完成组 group01 的删除，如图 1-35 所示。

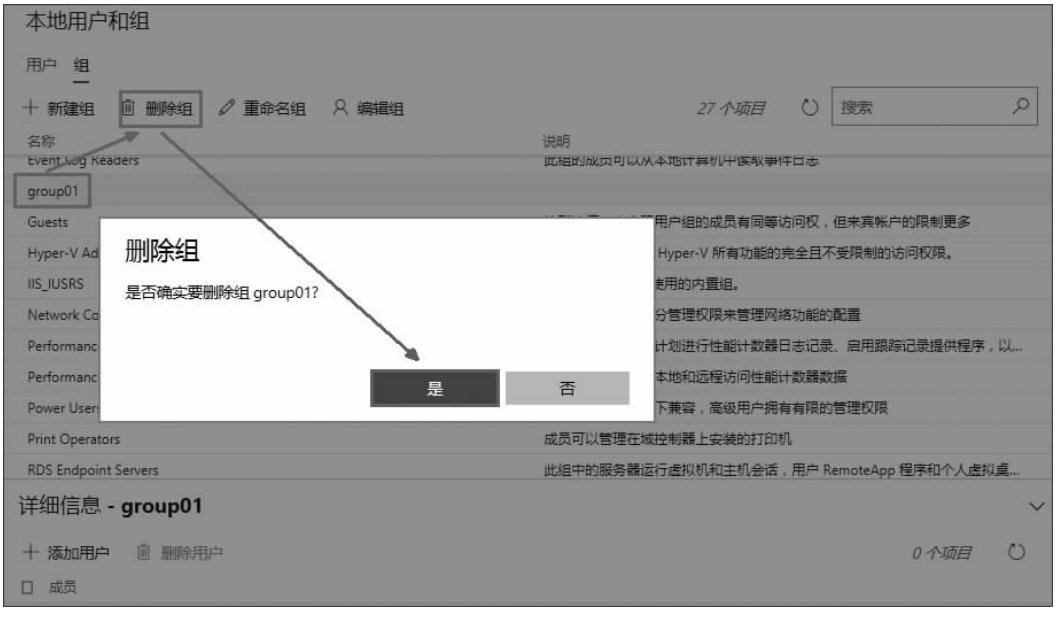

图 1-35　删除组 group01

1.2.3 共享文件夹的管理

在 Windows Server 2019 中，要共享文件夹必须满足下列条件：

(1)默认情况下，只有 Administrators 组成员能够共享文件夹，Administrators 组成员可共享 NTFS 分区下的任何文件夹。

(2)用户共享的文件夹，要求用户必须对该文件夹拥有完全控制权限。

【例 1-3】 通过命令方式添加账户、创建共享文件夹并设置共享、设置访问共享。

(1)添加账户。在服务端打开 cmd 窗口，输入以下命令：

```
net user zs Password1! /add      //添加账户 zs 并设置密码
net user ls Password1! /add      //添加账户 ls 并设置密码
```

(2)创建共享文件夹并设置共享。在服务端 C 盘创建共享文件夹，输入以下命令：

```
cd c:/                    //切换到 C 盘根目录
mkdir Share1;Share2       //创建文件夹
net share ShareZs = C:/Share1 /grant:zs,full /users:3
                          //设置共享名为 ShareZs 的文件实际路径为 C:/Share1，授权 zs
                            用户有读写权限，同时访问共享资源的数量限制为 3
net share ShareLs = C:/Share2 /grant:ls,read /unlimited /remark:"ShareLs"
                          //设置共享名为 ShareLs 的文件实际路径为 C:/Share2，授
                            权 ls 用户只有读取权限，指定同时访问共享资源的数量
                            不受限制，并添加资源注释为“ShareLs”
```

(3)设置访问共享。通过客户端设置访问共享的操作如下。

①通过账户名“zs”、密码“Password1!”将 ShareZs 共享文件链接到本地。在客户端打开 cmd 窗口，输入以下命令(注意防火墙的干扰)：

```
net use \\192.168.136.250\ShareZs "Password1!" /user:zs
echo “test” > test.txt                          //创建内容为“test”的 test.txt 文档
copy test.txt \\192.168.136.250\ShareZs         //上传文件到共享目录中
copy \\192.168.136.250\ShareZs\test.txt down.txt
                                                //下载文件到本地目录中
net use \\192.168.136.250\ShareZs /delete /y
                                                //删除共享资源链接
```

②通过账户名“ls”、密码“Password1!”将 ShareLs 共享文件映射到本地并分配盘符 H。在客户端打开 cmd 窗口，输入以下命令(注意防火墙的干扰)：

```
net use h: \\192.168.136.250\ShareLs "Password1!" /user:ls
echo “test-up” > testup.txt          //创建内容为“test-up”的 testup.txt 文档
copy testup.txt H:                   //上传失败，权限拒绝
net use * /delete /y                 //删除全部链接
```

1.3　本地安全策略

本地安全策略是计算机的一项重要工作，在没有活动目录集中管理的情况下，本地管理员必须对计算机进行设置以确保其安全。例如，限制用户设置密码、通过账户策略设置账户安全性、通过锁定账户策略避免他人登录计算机、指派用户权限等。

1.3.1　账户策略

在 Windows 操作系统中，账户策略包含两个子集：

(1)密码策略。对于域或本地用户账户，密码策略决定密码的设置，如强制性和期限。

(2)账户锁定策略。对于域或本地用户账户，账户锁定策略决定系统锁定账户的时间，以及锁定谁的账户。

【例 1-4】　为保证账户的安全，公司需要对新安装的 Windows 服务器(192. 168. 136. 250)进行密码策略和账户锁定策略的设置。

(1)打开“本地安全策略”窗口。执行“开始”→“Windows 管理工具”→“本地安全策略”命令(或在 cmd 窗口中输入 secpol. msc 命令)，打开“本地安全策略”窗口，单击左侧目录树中的“账户策略”前面的 > 图标，打开其选项列表，如图 1-36 所示。

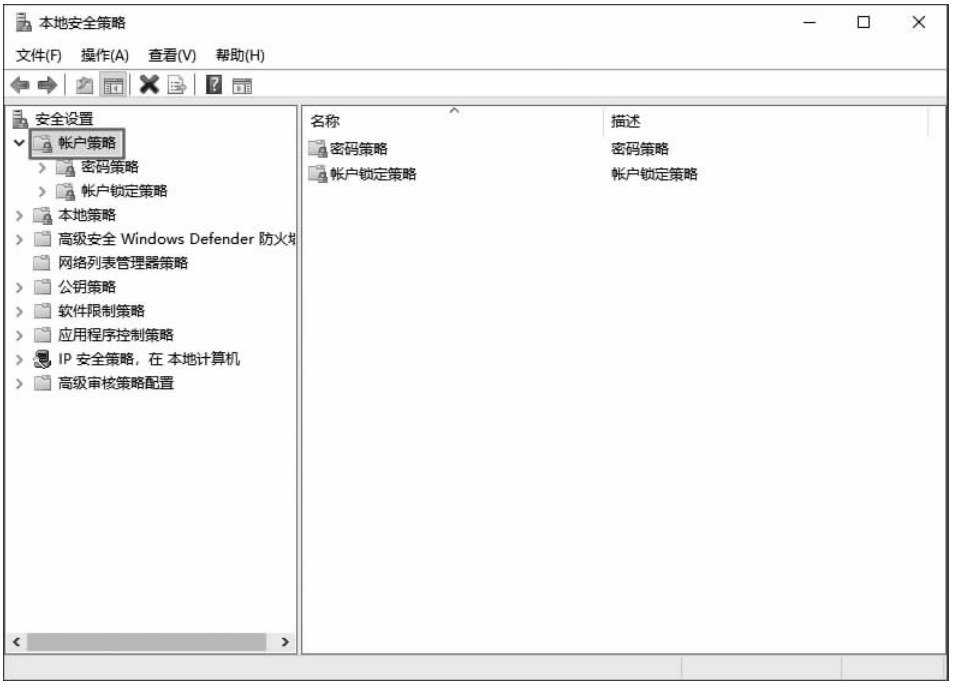

图 1-36　打开“账户策略”下的选项列表

(2)设置“密码策略”。选择“账户策略”下的“密码策略”选项,并按照图 1-37 所示设置密码策略。

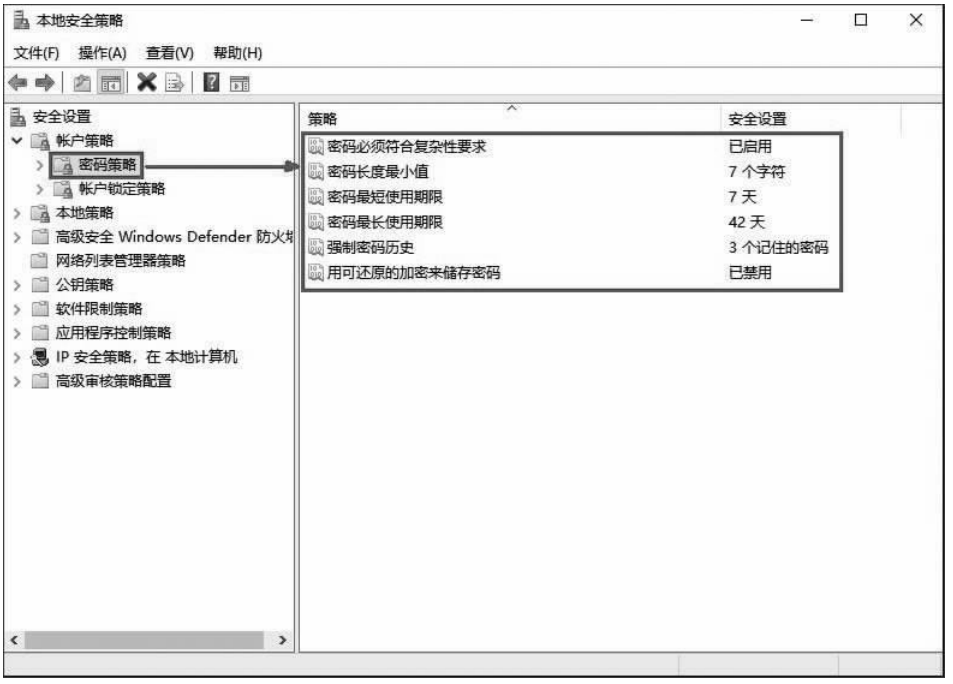

图 1-37 设置密码策略

①密码必须符合复杂性要求。此项安全设置用于确定密码是否必须符合复杂性要求。如果启用此策略,则密码必须符合下列最低要求:

a. 不能包含用户的账户名,不能包含用户姓名中超过两个连续字符的部分。

b. 至少有 6 个字符长。

c. 包含以下 4 类字符中的 3 类字符:英文大写字母(A 到 Z),英文小写字母(a 到 z),10 个基本数字(0 到 9),非字母字符(如!、$、#、%)。

d. 在更改或创建密码时执行复杂性要求。

②密码长度最小值。此项安全设置用于确定用户账户密码包含的最少字符数,可以将值设置为 1～20 个字符;或者将字符数设置为 0,从而确定不需要密码。

③密码最短使用期限。此项安全设置用于确定在用户更改某个密码之前必须使用该密码一段时间(以天为单位),可以将该值设置为 1～998 天,如果设置为 0,则允许立即更改密码。

④密码最长使用期限。此项安全设置用于确定在系统要求用户更改某个密码之前可以使用该密码的期限(以天为单位),可以设置密码在 1～999 天后到期,如果设置天数为 0,则密码将永不过期。如果“密码最长使用期限”为 1～999 天,则“密码最短使用期限”必须小于“密码最长使用期限”。如果将“密码最长使用期限”设置为 0,则可以将“密码最短使用期限”设置为 0～998 天。

注意：“密码最长使用期限”的默认值为 42 天，较为安全的操作是将密码设置为 30～90 天后过期。这样，攻击者用来破解用户密码以及访问网络资源的时间就会受到限制。

⑤强制密码历史。此项安全设置用于确定再次使用某个旧密码之前必须与某个用户账户关联的唯一新密码数。该值必须为 0～24 个密码。此策略使管理员能够通过确保旧密码不被连续重新使用来增强安全性。

如果希望“强制密码历史”有效，则需要将“密码最短使用期限”设置为大于 0 的值。如果没有设置“密码最短使用期限”，则用户可以循环选择密码，直到获得期望的旧密码。默认设置没有遵从此建议，以便管理员能够为用户指定密码，然后要求用户在登录时更改管理员定义的密码。如果将“强制密码历史”设置为 0，则用户不必选择新密码。因此，默认情况下将“强制密码历史”设置为 1。

⑥用可还原的加密来储存密码。此项设置为某些应用程序提供支持，这些应用程序使用的协议需要用户密码来进行身份验证。用可还原的加密来储存密码与储存纯文本密码在本质上是相同的。因此，除非应用程序需求比保护密码信息更重要，否则绝不要启用此项设置。

(3)设置“账户锁定策略”。为防止其他人无数次猜测计算机上的用户账户密码，可以选择“账户策略”下的“账户锁定策略”选项，并按照图 1-38 所示设置账户锁定策略。

图 1-38　设置账户锁定策略

①账户锁定时间。此项安全设置用于确定锁定账户在自动解锁之前保持锁定的分钟数。“账户锁定时间”可设置为 0～99 999 min。如果将“账户锁定时间”设置为 0，则账户将一直被锁定，直到管理员明确解除对它的锁定。

注意：只有指定了“账户锁定阈值”，“账户锁定时间”的设置才有意义。

②账户锁定阈值。此项安全设置用于确定导致用户账户被锁定的登录尝试失败的次数。在管理员重置锁定账户或账户锁定时间期满之前，无法使用该锁定账户。可以将“账户锁定阈值”设置为 0～999 次；如果将值设置为 0，则永远不会锁定账户。

在使用“Ctrl＋Alt＋Del”组合键或受密码保护的屏幕保护程序锁定的工作站或成员服务器上的密码尝试失败将计为登录尝试失败。

③重置账户锁定计数器。此项安全设置用于确定在某次登录尝试失败之后将登录尝试失败计数器重置为 0 次错误登录尝试之前需要的时间。“重置账户锁定计数器”的可用范围为 1～99 999 min。

如果定义了“账户锁定阈值”，则“账户锁定时间”的值必须大于或等于“重置账户锁定计数器”的值。

注意：只有指定了“账户锁定阈值”，“重置账户锁定计数器”的设置才有意义。

1.3.2 本地策略

账户策略只用于控制登录过程，要控制用户登录之后的操作，需要使用本地策略。本地策略包含以下三个子集：

(1)审核策略：用于观察用户在干什么，审查与用户管理有关的事件。

(2)用户权限分配：用于确定用户和计算机的权限，应用于用户或组。

(3)安全选项：用于用户对计算机配置安全措施，应用于计算机。

【例 1-5】 公司有台新安装的 Windows 服务器(192.168.136.250)，为保证信息的安全性，需要审核特定用户对文件夹失败的访问。

(1)打开“本地安全策略”窗口，单击左侧目录树中的“本地策略”前面的›图标。

(2)设置“审核策略”。选择“本地策略”下的“审核策略”选项，并按照图 1-39 所示，双击“审核对象访问”，在弹出的“审核对象访问 属性”对话框中选中“失败”复选框，单击“确定”按钮。

(3)在资源上设置审核策略。

①在 C 盘中创建一个测试文件夹 test，并右击选择“属性”选项，在弹出的“test 属性”对话框中选择“安全”选项卡，单击“高级”按钮，弹出“test 的高级安全设置”窗口，如图 1-40 所示。

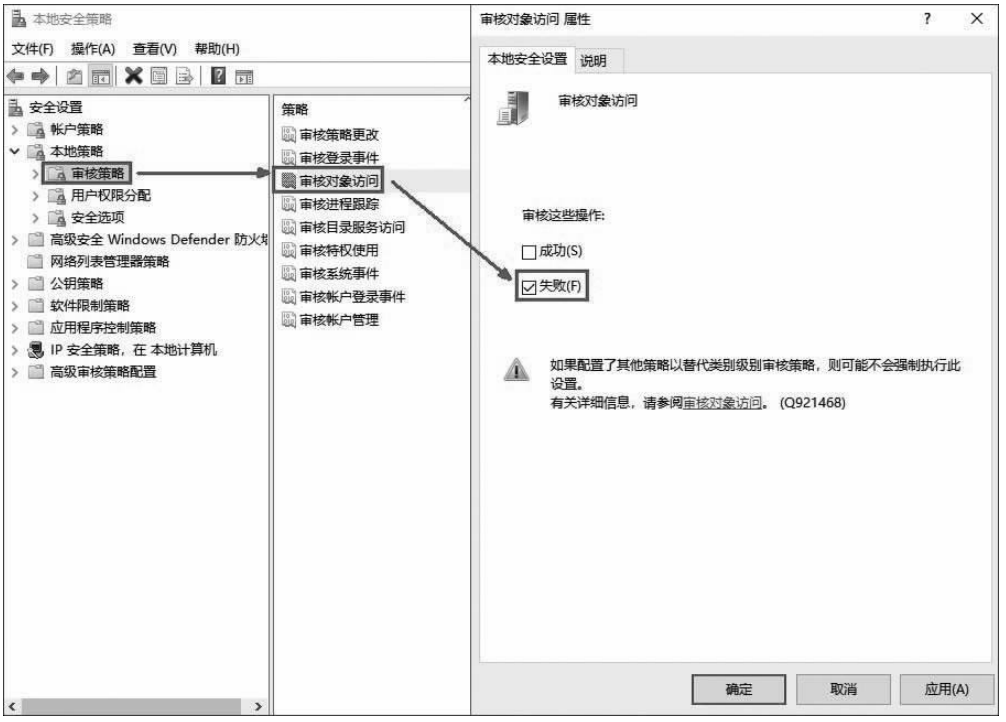

图 1-39　设置“审核策略”

图 1-40　“test 的高级安全设置”窗口

②单击“审核”选项卡中的“添加”按钮，打开“test 的审核项目”窗口，如图 1-41 所示。

图 1-41 “test 的审核项目”窗口

③单击“选择主体”超链接，弹出“选择用户或组”对话框，在“输入要选择的对象名称”对话框中输入“Administrator”，单击“检查名称”按钮，最后单击“确定”按钮，如图 1-42 所示。

图 1-42 选 择 用 户

④在“test 的审核项目”窗口的“类型”下拉列表框中选择“失败”选项，根据实际情况选择“应用于”下拉列表框中的选项和“基本权限”选项组中的复选项，单击“确定”按钮完成设置，如图 1-43 所示。

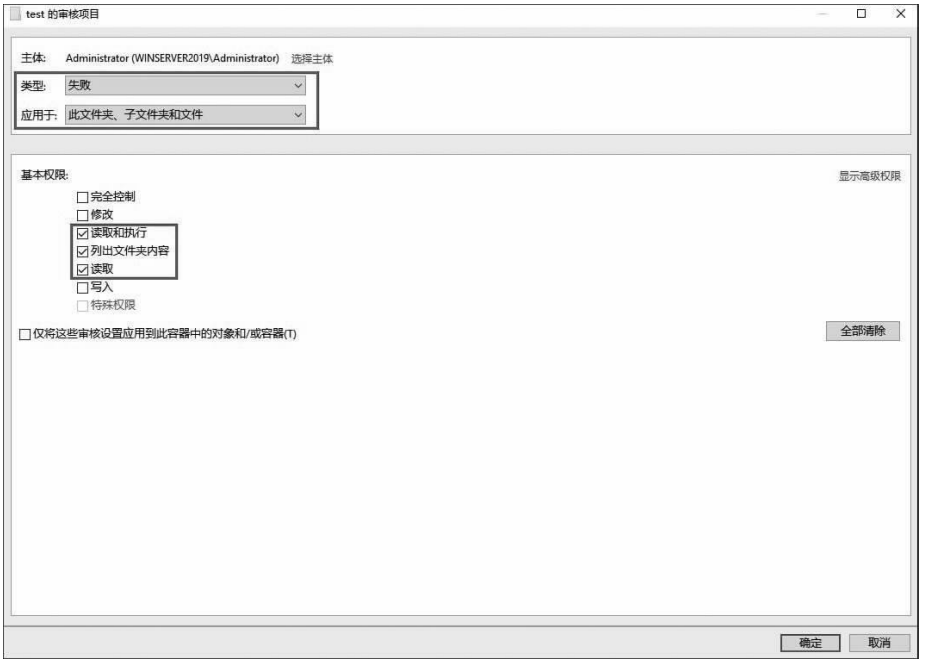

图 1-43　设置 test 的审核项目类型及权限

(4)在资源上设置权限。

①在“test 的高级安全设置”窗口中,单击“权限”选项卡中的“添加”按钮,打开“test 的权限项目”窗口,单击“选择主体”超链接,弹出“选择用户或组”对话框,在“输入要选择的对象名称”对话框中输入“Administrator”,单击“检查名称”按钮,最后单击“确定”按钮,再进行“类型”“应用于”和“基本权限”的设置,如图 1-44 所示。

图 1-44　设置 test 的权限项目

②设置完成后，以对应的账户登录系统并双击 test 文件夹，弹出“你当前无权访问该文件夹”提示框，如图 1-45 所示。

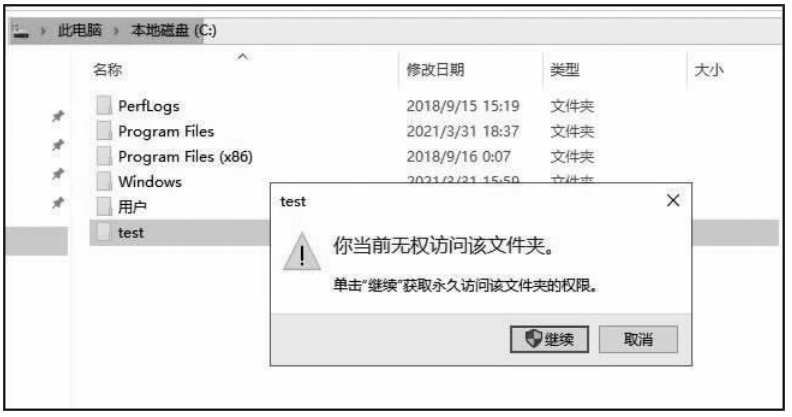

图 1-45　访 问 失 败

(5)查看审核日志。

①执行“开始”→“Windows 管理工具”→“事件查看器”命令(或在 cmd 窗口中输入 eventvwr. msc 命令)，打开“事件查看器”窗口，单击左侧目录树中的“Windows 日志”前面的 › 图标，打开其选项列表，如图 1-46 所示。

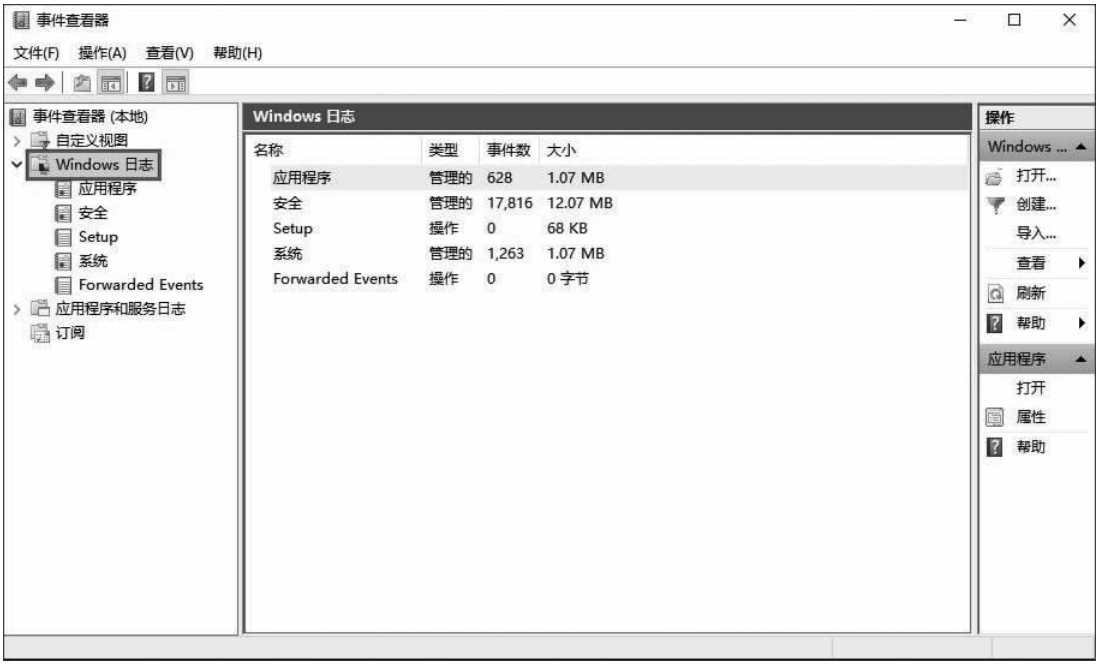

图 1-46　打开“Windows 日志”下的选项列表

②选择“Windows 日志”下的“安全”选项，可以看到 Administrator 用户访问 C:\test 文件夹“审核失败”信息，如图 1-47 所示。

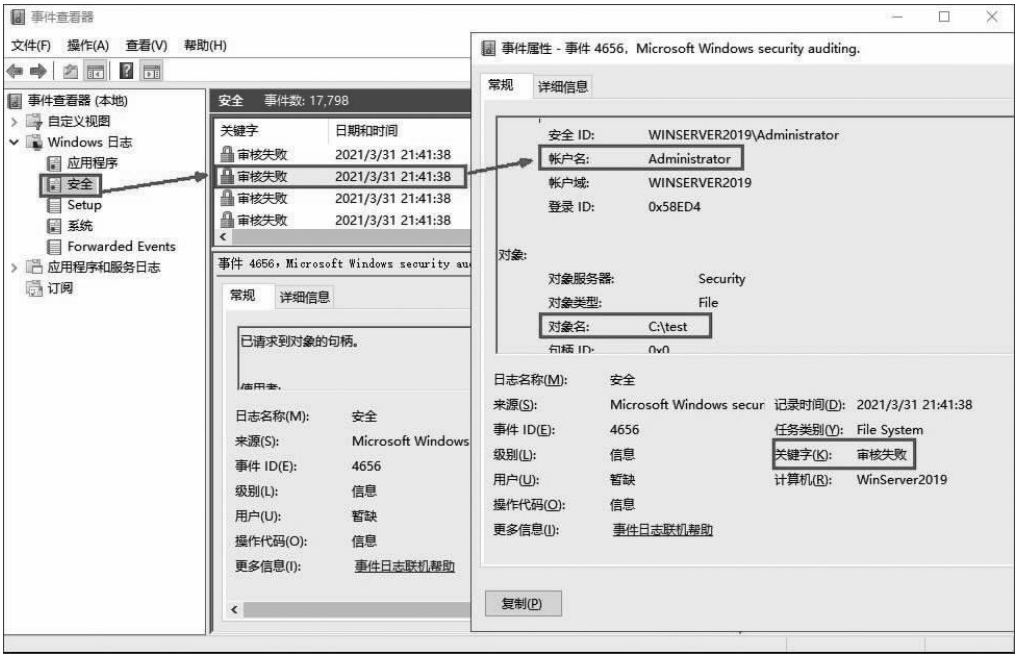

图 1-47　查看审核日志

【例 1-6】　为保证信息的安全性，公司需要对新安装的 Windows 服务器(192.168.136.250)设置拒绝 Administrator 用户从网络访问服务器资源。

(1)打开“本地安全策略”窗口，单击左侧目录树中的“本地策略”前面的›图标。

(2)设置“用户权限分配”。选择“本地策略”下的“用户权限分配”选项，并按照图 1-48 所示，双击“拒绝从网络访问这台计算机”选项，在弹出的“拒绝从网络访问这台计算机 属性”对话框中单击“添加用户或组”按钮来进行用户或组的设置，最后单击“确定”按钮。

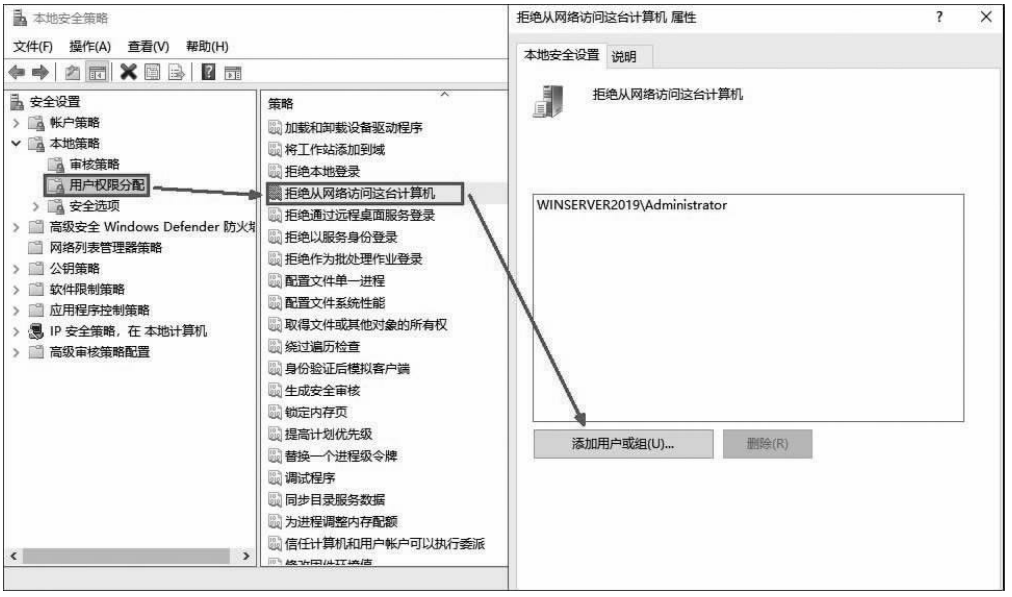

图 1-48　设置“拒绝从网络访问这台计算机”的属性

(3)创建共享文件夹 share,并进行相应的设置,如图 1-49 所示。

图 1-49　设置共享文件夹 share

(4)通过网络访问服务器共享资源。在同网段的客户端机器上访问 Windows 服务器(192.168.136.250)的共享资源,输入资源地址“\\192.168.136.250\share”,以及用户名和密码,弹出拒绝访问服务器共享文件资源的提示框,如图 1-50 所示。

图 1-50　拒绝访问服务器共享文件资源的提示框

【例 1-7】　公司有台新安装的 Windows 服务器(192.168.136.250),默认登录时,按“Ctrl+Alt+Delete”组合键,将显示所有的用户名。为保证服务器的相对安全性,需要设置服务器不显示登录的用户名。

(1)打开“本地安全策略”窗口,单击左侧目录树中的“本地策略”前面的›图标。

（2）设置“安全选项”。选择“本地策略”下的“安全选项”，并按照图 1-51 和图 1-52 所示，双击“交互式登录：不显示上次登录” 和“交互式登录：登录时不显示用户名”，在弹出的对话框中选中“已启用”单选按钮，最后单击“确定”按钮完成设置。

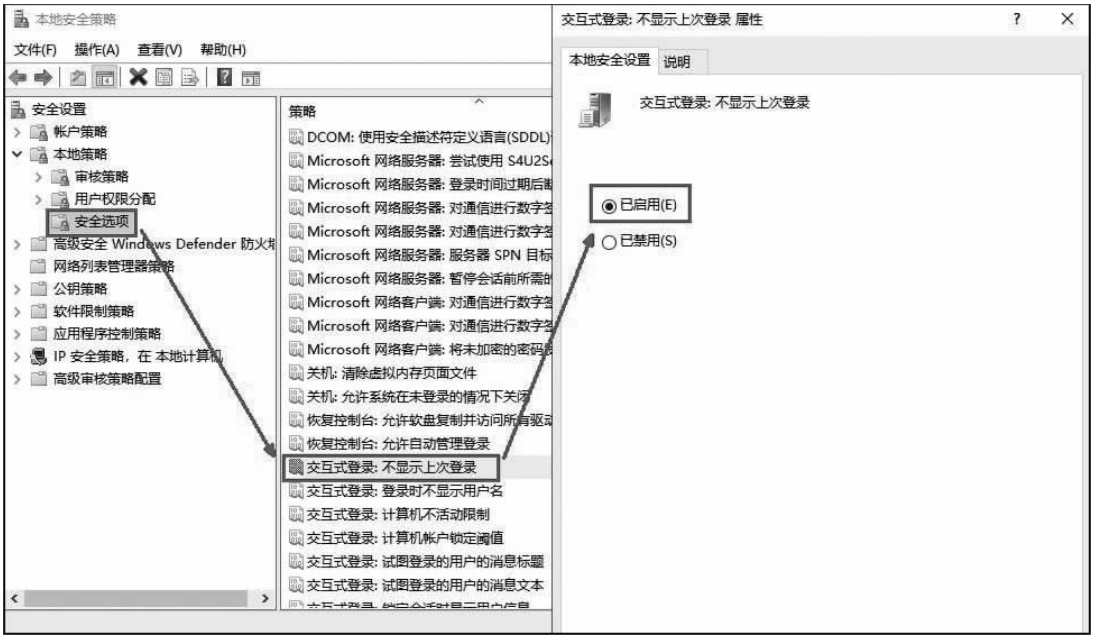

图 1-51　设置“不显示上次登录”的属性

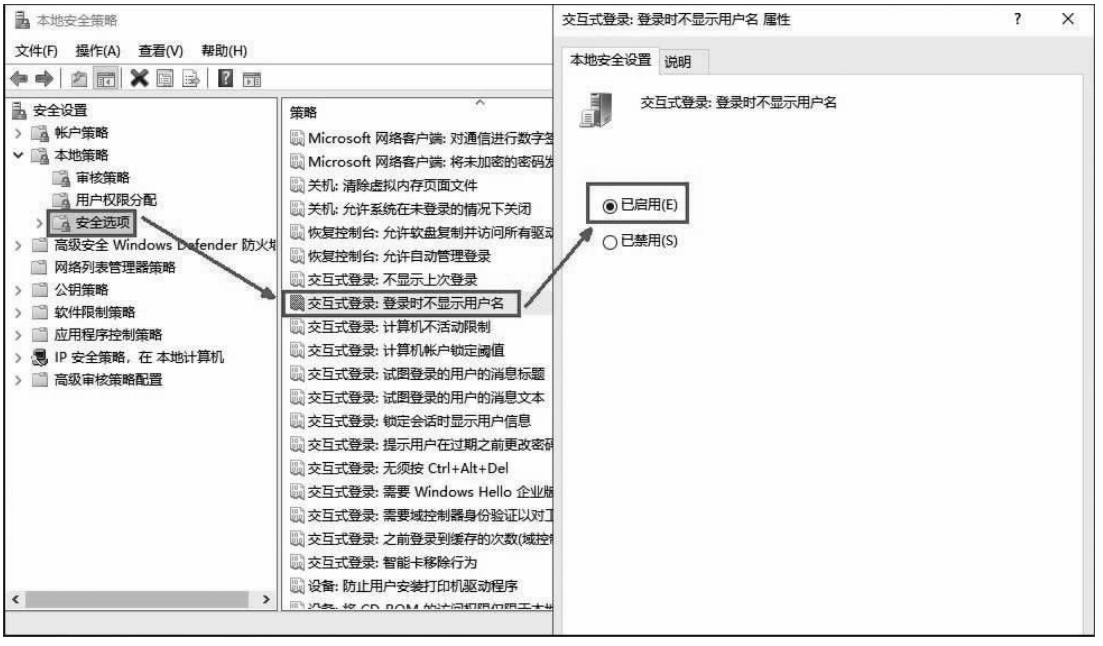

图 1-52　设置“登录时不显示用户名”的属性

(3)重启服务器,登录时将不会显示该计算机上的所有用户名,如图 1-53 所示。

图 1-53　不显示登录名

以上例子只是抛砖引玉,更多的本地安全策略设置,请查阅微软公司官方资料。

1.4　恢复 Windows Server 2019 密码

Windows 系统的 Administrator 账户是非常重要的一个账户,也是权限最大的一个账户,如果忘记了 Administrator 账户密码,可以通过一些方法来重置密码。

【例 1-8】　公司有台 Windows 服务器(192. 168. 136. 250),由于人员工作交接不到位,导致密码不得而知,无法进入系统进行管理,现在需要对 Administrator 账户密码进行恢复。

(1)加载 Windows 服务器对应的 ISO 映像文件,如图 1-54 所示。

图 1-54　加载 ISO 映像文件

(2)设置从 CDROM 启动系统,如图 1-55 所示。

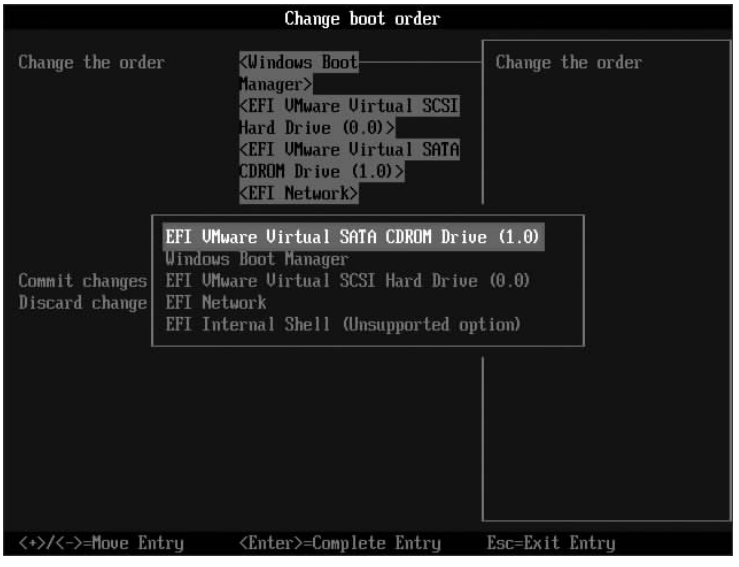

图 1-55　设置系统的启动程序

(3)启动系统后,在“Windows 安装程序”界面中按“Shift+F10”组合键,弹出 cmd 窗口,如图 1-56 所示。

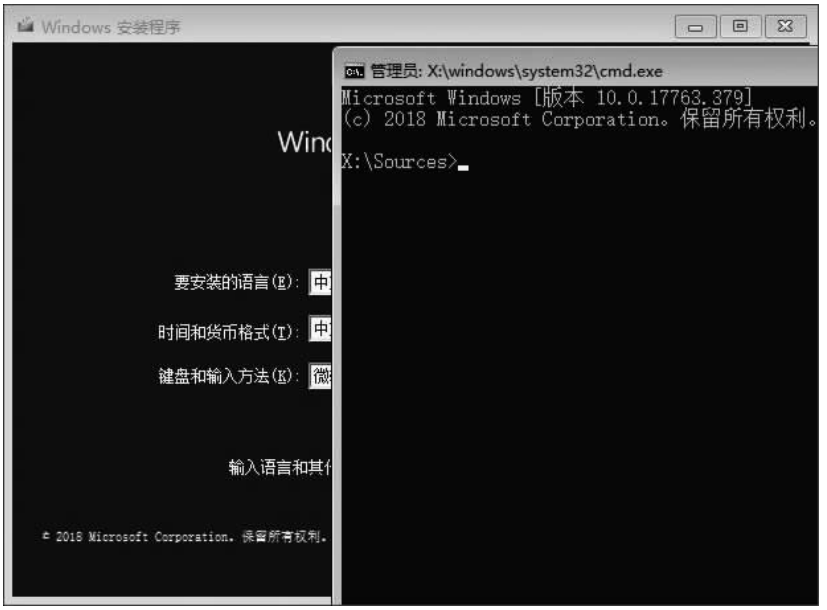

图 1-56 cmd 窗口

(4)输入命令,如图 1-57 所示。

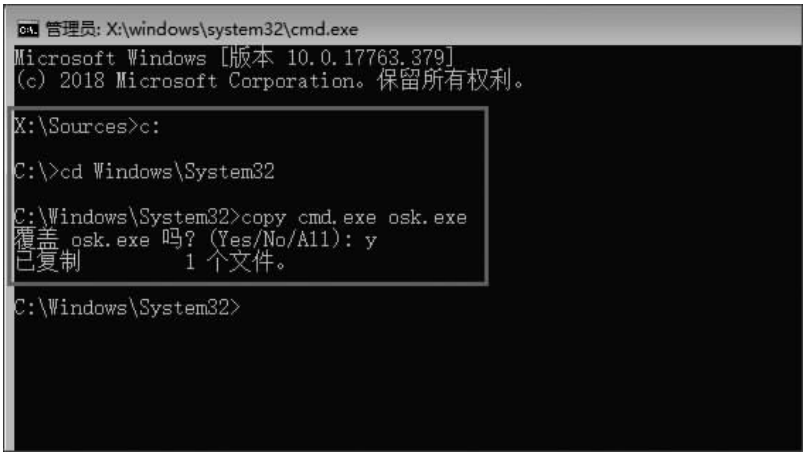

图 1-57 在 cmd 窗口中输入命令

```
c:                          //切换到系统 C 盘
cd Windows\System32         //切换到 Windows 目录下的 System32 目录
copy cmd.exe osk.exe        //复制 cmd.exe 程序覆盖命名 osk.exe
```

(5)参照步骤(2)设置系统从硬盘启动,单击系统开机界面右下角的“轻松使用”按钮,在打开的列表中选择“屏幕键盘”选项,如图 1-58 所示。

图 1-58　选择“屏幕键盘”选项

（6）在打开的 cmd 窗口中运行命令“net user Administrator Password!!”，进行 Administrator 账户密码的修改，如图 1-59 所示。

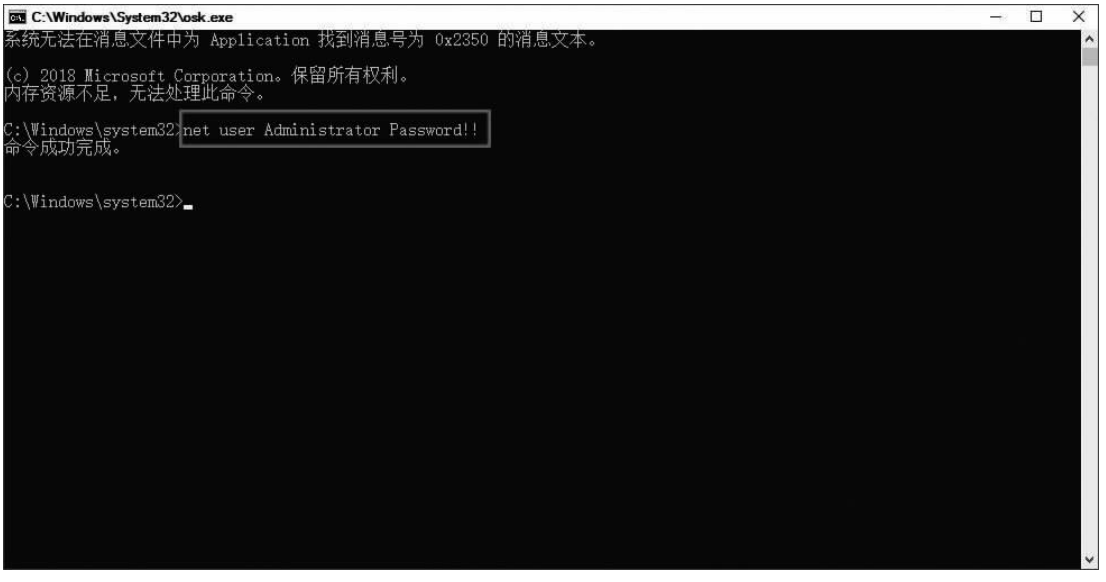

图 1-59　修改 Administrator 账户密码

（7）利用修改的密码登录系统进行测试，如图 1-60 所示。

图 1-60　成功登录系统

1.5　Windows Server 2019 的安装与基本配置实训

1. 实训目的

(1)掌握虚拟机(VMware Workstation/VirtualBox 等)的安装及使用方法。

(2)掌握 Windows Server 2012/2016/2019 操作系统的安装与启动。

(3)掌握主机名/IP 地址等网络信息配置的方法。

(4)能运用 Windows Admin Center 进行本地用户与组、共享文件夹的管理。

(5)能根据需求进行本地安全策略和防火墙的设置。

(6)掌握恢复 Windows Server 账户密码的方法。

2. 实训内容

(1)根据现有的虚拟机软件,安装 VMware Workstation/VirtualBox 软件。

(2)安装 Windows Server 服务器(系统内存推荐 2 GB,但应根据自己的物理设备进行调整)。

(3)虚拟机中网络采用默认方式,暂不更改,仅将网卡启用。

(4)添加账户 XXX 和组 YYY,采用多种方法(如命令、图形法)创建用户和组。其中,XXX 表示姓名的拼音,YYY 表示学号。

(5)安装 Windows Admin Center 软件,并进行本地用户与组的管理(删除组 YYY)。

(6)配置防火墙的出站规则,使得服务器不能 ping 通 IP 地址 8.8.8.8。

(7)设置本地安全策略。

①为普通用户配置密码策略,该策略要求密码为长度最小 9 位数的复杂性密码。

②当 3 次无效尝试密码后,锁定账户 5 min。

③对账户登录事件进行失败审核。

④允许 XXX 用户关闭计算机和重启计算机。

⑤拒绝 XXX 用户从网络访问该服务器。

⑥设置服务器不显示登录的用户名。

⑦修改来宾账户名为 Guest。

(8)恢复 Windows Server 服务器密码。

3. 实训要求

(1)按实训内容完成相应的操作("文字+截图"方式)。

(2)总结实训心得与体会。