1

第 1 章　Windows Server 2022 概述

Windows Server 2022 可以帮助信息部门的 IT 人员搭建功能强大的网站、应用程序服务器、高度虚拟化的云环境与容器，无论是大型、中型还是小型的企业网络，都可以利用 Windows Server 2022 的强大管理功能与安全措施来简化网站与服务器的管理、改善资源的可用性、减少成本支出、并保护企业的应用程序和数据，让 IT 人员可以更轻松有效地管理网站、应用程序服务器与云环境。

- Windows Server 2022版本
- Windows网络架构
- TCP/IP通信协议简介

1.1 Windows Server 2022版本

Windows Server 2022 提供了多种发行版本与虚拟化的环境，它分为以下三个版本：

- Windows Server Standard Edition：这是最基本的版本之一，允许搭建最多两台虚拟机。
- Windows Server Datacenter Edition：比Standard版本更高级的版本，允许搭建无限数量的虚拟机。
- Windows Server Datacenter：Azure Edition：这是功能最强的版本，专为Azure云端建立虚拟机而设计。它提供了一些额外的功能，例如**热补丁**（hot patching），支持Azure虚拟机在安装更新后不需要重新启动；还有SMB over QUIC，可以安全地通过Internet访问Azure云虚拟机内共享的文件，而无须搭建虚拟专用网（VPN）。

1.2 Windows网络架构

我们可以利用 Windows 系统来搭建网络，以便将资源共享给网络上的用户。Windows 网络架构大致可分为工作组架构（workgroup）、域架构（domain）以及包含前两者的混合架构。此外，我们还可以利用 Azure AD Connect 将域架构的目录服务 Active Directory 与云端的 Azure Active Directory 整合在一起。

工作组架构是一种分布式的管理模式，适用于小型网络。而域架构则是一种集中式的管理模式，适用于各种不同规模的网络。接下来，我们将详细说明工作组架构与域架构之间的差异。

1.2.1 工作组架构的网络

工作组是由通过网络连接在一起的多台计算机组成的（见图 1-2-1）。这些计算机可以共享其内部的文件、打印机等资源，供网络上的用户访问与使用。工作组架构的网络也被称为**对等网络**（peer-to-peer），因为网络上每台计算机的地位都是平等的，资源与管理分散在各个计算机上。工作组架构的网络具有以下三个主要特点：

- 每台Windows计算机都有一个**本地安全账户数据库**，称为Security Accounts Manager（SAM）。如果用户想要访问每台计算机内的资源，那么系统管理员则需要在每台计算机的SAM数据库内创建用户账户。例如，如果用户Peter希望访问每台计算机内的资源，管理员则需要在每台计算机的SAM数据库中创建Peter账户，并设置这些账户

的权限。在这种架构下，账户与权限管理工作相对烦琐。例如，当用户需要修改其账户密码时，就需要在每台计算机上都修改该用户账户的密码。

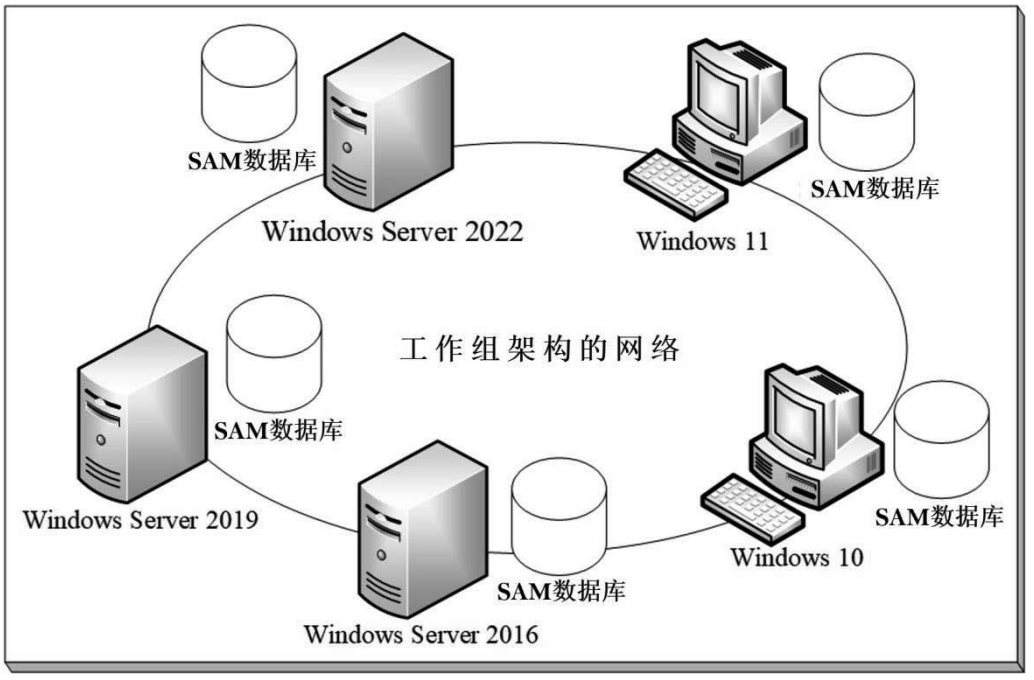


图 1-2-1

- 工作组内可以包含不同级别的计算机，例如Windows 11、Windows 10等客户端等级的计算机，也可以包含Windows Server 2022、Windows Server 2019等服务器级别的计算机。
- 如果企业内部的计算机数量不多的话，例如10台或20台计算机，那么可以选择采用工作组架构的网络。

1.2.2　域架构的网络

域也是由通过网络连接在一起的多台计算机组成的（见图 1-2-2），它们可以共享计算机内的文件、打印机等资源，供网络用户访问与使用。与工作组架构不同的是，域内的所有计算机共享一个集中式的目录数据库（directory database），其中包含整个域内所有用户的账户和相关数据。提供目录数据库的添加、删除、修改与查询等目录服务（directory service）的组件被称为 **Active Directory 域服务**（Active Directory Domain Services，AD DS）。目录数据库存储在**域控制器**（domain controller）内，而只有服务器等级的计算机才可以扮演域控制器的角色。

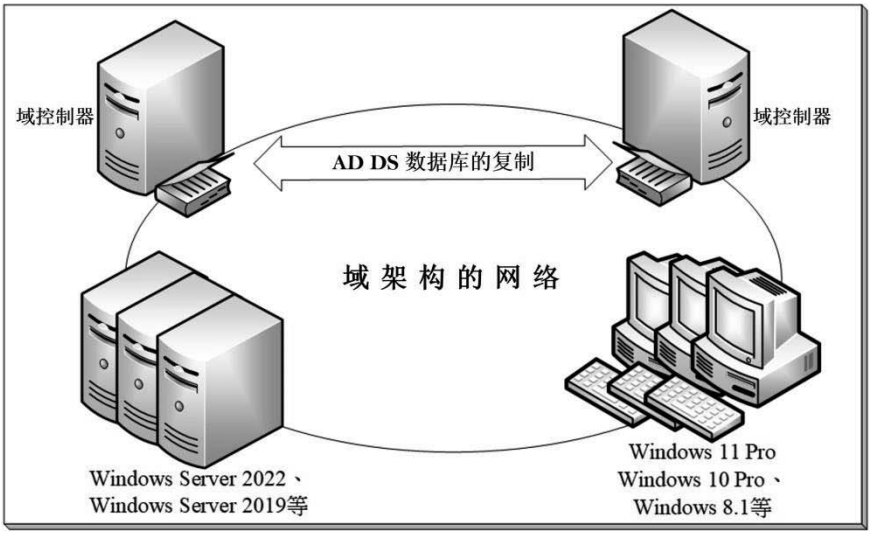


图 1-2-2

1.2.3 域中计算机的种类

域中的计算机成员如下：

- **域控制器（domain controller）**：服务器等级的计算机才可以扮演域控制器，例如Windows Server 2022 Datacenter、Windows Server 2019 Datacenter等。
  一个域内可以有多台域控制器，通常情况下它们的地位是平等的。每台域控制器都存储着一份几乎完全相同的AD DS数据库（目录数据库）。当在其中一台域控制器内新建了一个用户账户后，此账户会被存储在该台域控制器的AD DS数据库中，之后会自动被复制到其他域控制器的AD DS数据库中，这样可以确保所有域控制器中的AD DS数据库保持同步。
  当用户在域内某台计算机登录时，其中一台域控制器会根据其AD DS数据库内的账户数据来审核用户输入的账户名与密码是否正确。如果正确，用户就可以成功登录；反之，如果账户名或密码错误，则被拒绝登录。
  多台域控制器可提供容错能力，例如，如果其中一台域控制器发生故障，其他域控制器仍然可以继续提供服务。此外，多台域控制器还可以改善用户登录效率，因为它们可以共同分担审核用户登录身份（账户名与密码）的工作。
- **成员服务器（member server）**：当服务器等级的计算机加入域后，用户就可以使用AD DS内的用户账户在这些计算机上登录，否则只能使用本地用户账户来登录。这些加入域的服务器被称为**成员服务器**，它们没有AD DS，也不负责验证“域”用户的账户名与密码，而是将这些请求转发给域控制器进行审核。成员服务器可以是以下版本的Windows Server操作系统：
  - Windows Server 2022 Datacenter/Standard
  - Windows Server 2019 Datacenter/Standard

- Windows Server 2016 Datacenter/Standard

如果上述服务器没有被加入域，则它们被称为**独立服务器**（stand-alone server）或**工作组服务器**（workgroup server）。但无论是独立服务器还是成员服务器，它们都有一个**本地安全账户数据库**（SAM），系统可以用它来验证本地用户（非域用户）的身份。

- 其他比较常用的Windows计算机，例如：
  - Windows 11 Enterprise/Pro/Education
  - Windows 10 Enterprise/Pro/Education
  - Windows 8.1（8）Enterprise/Pro

当上述客户端计算机加入域后，用户就可以使用AD DS内的账户在这些计算机上登录，否则只能使用本地账户登录。

可以将 Windows Server 2022、Windows Server 2019 等独立服务器或成员服务器升级为域控制器，也可以将域控制器降级为独立服务器或成员服务器。

一些只具备基础功能的桌面版 Windows 操作系统，例如 Windows 11 Home、Windows 10 Home 无法加入域，因此只能使用本地用户账户登录。

1.3　TCP/IP通信协议简介

网络上计算机之间互相传递的信号只是一连串的“0”与“1”，这一连串的电子信号到底代表什么意义，彼此之间需要使用一套同样的规则来解释，才能够互相沟通，就好像人类用“语言”来互相沟通一样，这个计算机之间的通信规则被称为**通信协议**（protocol），而 Windows 网络依赖最深的通信协议是 TCP/IP。

TCP/IP 通信协议是目前最完整并且被广泛支持的通信协议，它让不同网络架构、不同操作系统的计算机之间可以相互通信，例如 Windows Server 2022、Windows 11、Linux 主机等。它也是 Internet 的标准通信协议，更是 AD DS 所必须采用的通信协议。

每一台连接在网络上的计算机可以被称为是一台**主机**（host），主机与主机之间的通信会涉及三个最基本的要素：**IP 地址**、**子网掩码**与**网关**。

1.3.1　IP 地址

每一台主机都有唯一的 IP 地址，就好像住家的门牌号码一样。IP 地址不但可以用来识别网络中的每一台主机，而且其地址结构中还隐含着在网络之间传送数据的路由信息。

IP 地址占用 32 位（bit），一般是以 4 个十进制数来表示，每一个数字称为一个 octet（8

位组）。octet 与 octet 之间以点（dot）隔开，例如 192.168.1.31。

此处所介绍的 IP 地址是目前使用最为广泛的 IPv4，它共占用 32 个位，Windows 系统也支持 IPv6，它共占用 128 个位（参见附录 A）。

这个 32 位的 IP 地址内包含了**网络标识符**与**主机标识符**两部分：

- **网络标识符（Network ID）**：每一个网络都有一个唯一的网络标识符，换句话说，位于相同网络内的每一台主机都拥有相同的网络标识符。
- **主机标识符（Host ID）**：相同网络内的每一台主机都有一个唯一的主机标识符。

如果该网络是直接通过路由器来连接 Internet，则需要为此网络申请网络标识符，使得整个网络内所有的主机都使用相同的网络标识符，然后再为该网络内每一台主机分配一个唯一的主机标识符，这样网络上每一台主机就都会有一个唯一的 IP 地址（网络标识符+主机标识符）。可以向 ISP（互联网服务提供商）申请网络标识符。

如果此网络并未通过路由器来连接 Internet，则可以自行选择任何一个可用的网络标识符，无需申请，但是网络内各主机的 IP 地址不能相同。

1.3.2 IP 类别

传统的 IP 地址被分为 Class A、B、C、D、E 五个类别，其中只有 Class A、B、C 三个类别的 IP 地址可供一般主机来使用（见表 1-3-1），每种类别所支持的 IP 数量都不相同，以便满足各种不同大小规模的网络需求。IP 地址共占用 4 个字节（byte），表 1-3-1 中将 IP 地址的各字节以 W.X.Y.Z 的形式来加以说明。

表 1-3-1 IP 地址的类别及形式说明

IP 地址类别	网络标识符	主机标识符	W 值可为	可支持的网络数量	每个网络可支持的主机数量
A	W	X.Y.Z	1～126	126	16 777 214
B	W.X	Y.Z	128～191	16 384	65 534
C	W.X.Y	Z	192～223	2 097 152	254

- Class A的网络，其网络标识符占用一个字节（W），W的范围为1到126，共可提供126个Class A的网络。主机标识符共占用X、Y、Z三个字节（24个位），此24个位可支持$2^{24} - 2 = 16\ 777\ 216 - 2 = 16\ 777\ 214$台主机（减2的原因是分别保留了全0和全1的地址）。
- Class B的网络，其网络标识符占用两个字节（W、X），W的范围为128到191，它可提供（191 – 128 + 1）×256 = 16 384个Class B的网络。主机标识符共占用Y、Z两个

字节，因此每个网络可支持$2^{16}-2=65\,536-2=65\,534$台主机。

- Class C的网络，其网络标识符占用三个字节（W、X、Y），W的范围为192到223，它可提供（223 – 192 + 1）×256×256 = 2 097 152个Class C的网络。主机标识符占用一个字节（Z），每个网络可支持$2^8-2=254$台主机（同样保留了全0和全1的地址）。

在设置主机的 IP 地址时请注意以下的事项：

- **网络标识符不能是127**：网络标识符127是供**环回测试**（loopback test）使用的，可用来检查网卡与驱动程序的工作是否正常。不能将它分配给主机使用。通常127.0.0.1这个IP地址用来代表主机本身。
- **每一个网络的第1个IP地址代表网络本身、最后一个IP地址代表广播地址（broadcast address），因此实际可分配给主机的IP地址将减少2个**：例如如果所申请的网络标识符为203.3.6，它共有203.3.6.0到203.3.6.255共256个IP地址，但203.3.6.0是用来代表这个网络的（因此一般会说其网络标识符为4个字节的203.3.6.0）；而203.3.6.255是保留给广播使用的（255代表广播）。例如，发送消息到203.3.6.255这个地址，表示将该消息广播给网络标识符为203.3.6.0网络内的所有主机。

图 1-3-1 为 Class C 的网络示例，其网络标识符为 192.168.1.0，图中 5 台主机的主机标识符分别为 1、2、3、21 和 22。

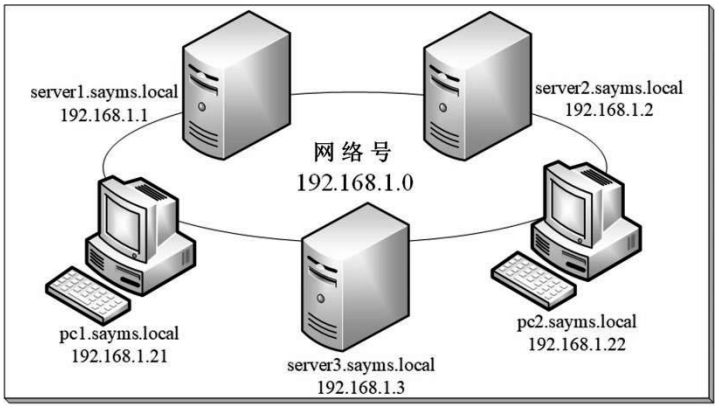


图 1-3-1

1.3.3　子网掩码

子网掩码也占用 32 位，与 IP 地址相同。当 IP 网络上两台主机通信时，它们利用子网掩码来确定双方的网络标识符，进而判断彼此是否在相同的网络内。

表 1-3-2 中为各类网络默认的子网掩码值，其中值为 1 的位用来表示网络标识符，值为 0 的位用来表示主机标识符，例如某台主机的 IP 地址为 192.168.1.3，其二进制值为 11000000.10101000.00000001.00000011，而子网掩码为 255.255.255.0，其二进制值为

11111111.11111111.11111111.00000000，则计算其网络标识符的原则是：将 IP 地址与子网掩码两个值中相对应的位进行 AND（与）逻辑运算（见图 1-3-2），所得结果 192.168.1.0 就是网络标识符。

表 1-3-2 IP 地址的类别及默认的子网掩码值

IP 地址类别	默认子网掩码（二进制）	默认子网掩码（十进制）
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

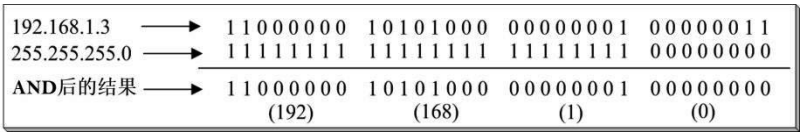


图 1-3-2

如果 A 主机的 IP 地址为 192.168.1.3、子网掩码为 255.255.255.0，B 主机的 IP 地址为 192.168.1.5、子网掩码为 255.255.255.0，则 A 主机与 B 主机的网络标识符都是 192.168.1.0，表示它们是在同一个网络内，因此可以直接相互通信，不需要借助于路由设备。

前面所叙述的 Class A、B、C 是按类别式划分的，而目前普遍采用的是无类别的 CIDR（Classless Inter-Domain Routing）划分法，它在表示 IP 地址与子网掩码时有所不同，例如网络标识符为 192.168.1.0、子网掩码为 255.255.255.0，则会使用 192.168.1.0/24 来代表此网络，其中 24 代表子网掩码中位值为 1 的数量为 24 个；同理，若网络标识符为 10.120.0.0、子网掩码为 255.255.0.0，则会使用 10.120.0.0/16 来代表此网络。

1.3.4 默认网关

当某台主机需要与同一个 IP 子网内的主机（网络标识符相同）通信时，可以直接将数据发送给该主机。但是，如果要与不同子网内的主机（网络标识符不同）进行通信，则需要先将数据发送给路由设备，再由路由设备负责发送给目标主机，即通过路由设备进行转发。一般情况下，主机只需要事先将**默认网关**指定为路由设备的 IP 地址即可。路由设备负责将数据转发给目标主机。

以图 1-3-3 为例，图中甲、乙两个网络是通过路由器来连接的。当甲网络的主机 A 要与乙网络的主机 B 通信时，由于主机 A 的 IP 地址为 192.168.1.1、子网掩码为 255.255.255.0、网络标识符为 192.168.1.0，而主机 B 的 IP 地址为 192.168.2.10、子网掩码为 255.255.255.0、网络标识符为 192.168.2.0，故主机 A 可以判断出与主机 B 是位于不同的子网内，因此会将数据发送给其默认网关，也就是 IP 地址为 192.168.1.254 的路由器，然后再由路由器负责将数

据转发给主机 B。

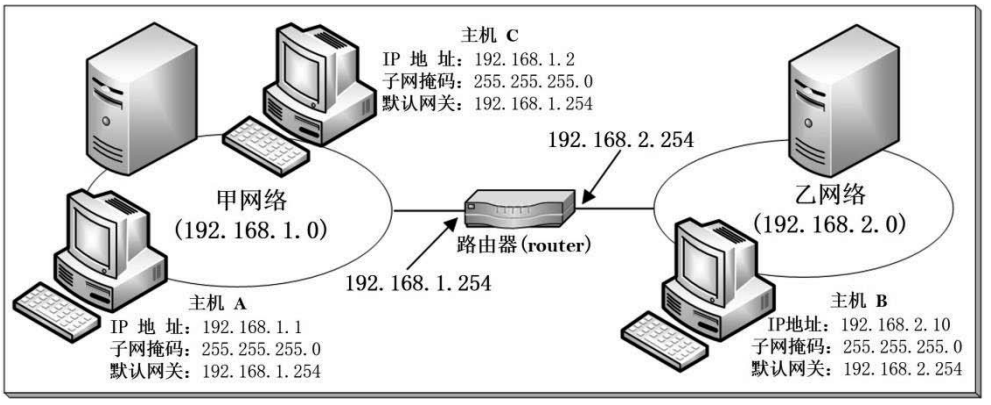


图 1-3-3

1.3.5　私有 IP 的使用

前面提到 IP 类别中的 Class A、B、C 是可供主机使用的 IP 地址。在这些 IP 地址中，有一些是被归类为**私有 IP**（private IP）（见表 1-3-3），各公司可以自行选用适合的私有 IP，而且不需要申请，因此可以节省网络建设的成本。

表 1-3-3　私有 IP 地址范围

网络标识符	子网掩码	IP 地址范围
10.0.0.0	255.0.0.0	10.0.0.1～10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1～172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1～192.168.255.254

不过私有 IP 仅限于公司内部的局域网络使用，虽然它可以让内部计算机相互通信，但是无法直接与外界计算机通信。如果需要连接外部网络并进行上网、收发电子邮件等操作，则需要使用具备网络地址转换（Network Address Translation，NAT）功能的设备，例如 IP 共享设备、宽带路由器等。这些设备能够将局域网内的私有 IP 地址转换为公共 IP 地址，从而使内部计算机能够与外界通信。

除了私有 IP 地址外，其他地址被称为**公有 IP 地址**（public IP address），例如 220.135.145.145。使用公有 IP 的计算机可以直接通过路由器与外界通信，因此这些计算机可以用于搭建商业网站，让外部用户直接访问。公有 IP 地址需要事先申请。

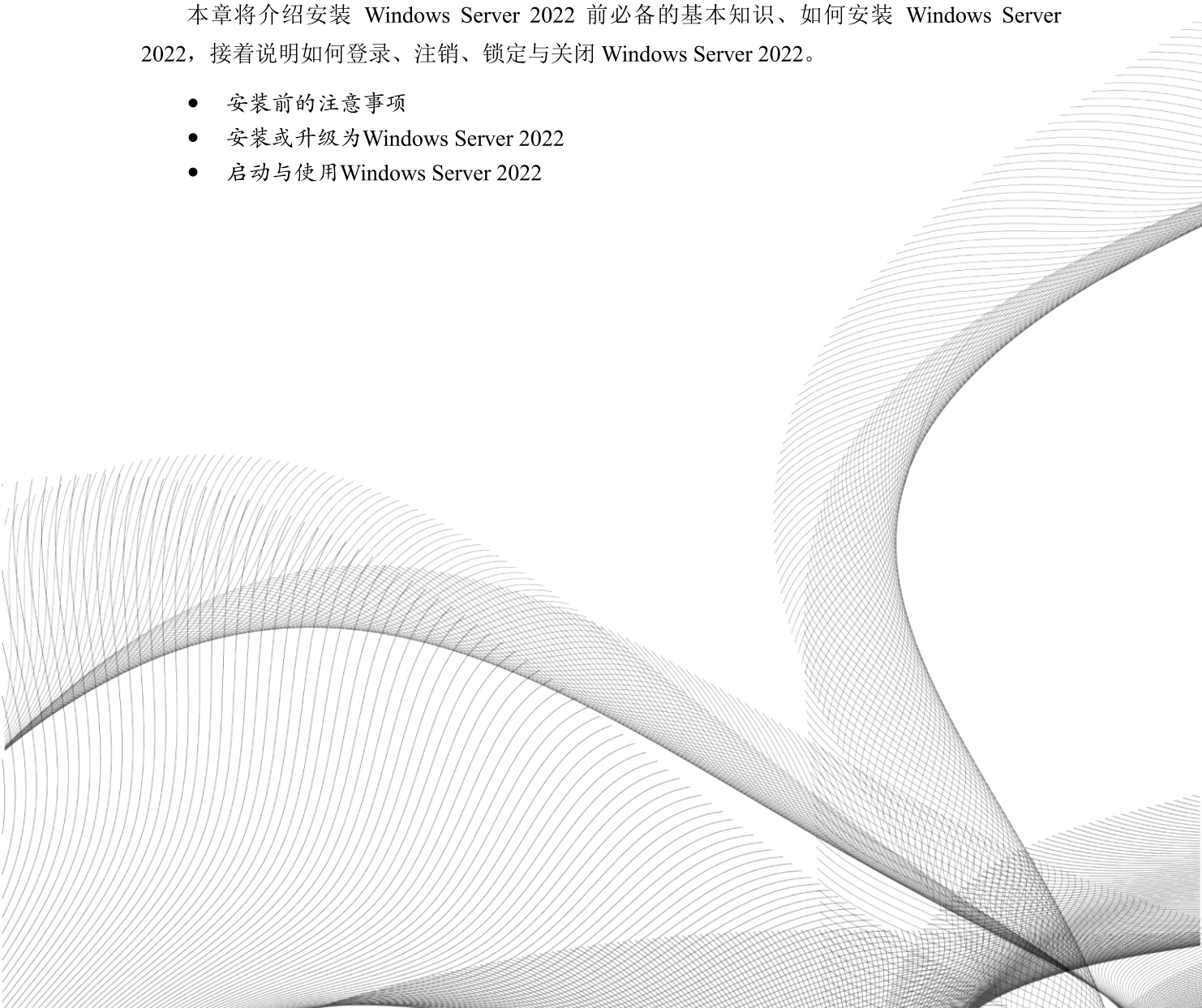
当 Windows 计算机的 IP 地址设置采用自动获取的方式，但因某些原因无法获取到 IP 地址，该计算机会通过自动专用 IP 地址（Automatic Private IP Addressing，APIPA）机制为自己分配一个临时 IP 地址，该 IP 地址的网络标识符为 169.254.0.0，例如 169.254.49.31。但该 IP 地址只能够用于与同一网络内的其他 IP 地址（即 169.254.x.x 格式）的计算机通信。

2

第 2 章　安装 Windows Server 2022

本章将介绍安装 Windows Server 2022 前必备的基本知识、如何安装 Windows Server 2022，接着说明如何登录、注销、锁定与关闭 Windows Server 2022。

- 安装前的注意事项
- 安装或升级为Windows Server 2022
- 启动与使用Windows Server 2022



2.1　安装前的注意事项

2.1.1　Windows Server 2022 的安装选择

Windows Server 2022 提供三种安装选择：

- **包含桌面体验的服务器**：它会安装标准的图形用户界面，并支持所有的服务与工具。由于包含图形用户界面（GUI），因此用户可以通过友好的窗口与管理工具来管理服务器。
- **Server Core**：它可以降低管理需求、减少硬盘容量占用以及减少被攻击面。由于Server Core没有窗口管理界面，只能使用Windows PowerShell、**命令提示符**（command prompt）或通过远程计算机来管理此服务器。有的服务在**Server Core**中并不支持，因此除非有图形化界面或特殊服务的需求，否则使用Server Core是微软**建议**的选项。
  另外，为了提高应用程序的兼容性，让某些具有交互性操作需求的应用程序可以正常在Server Core环境下运行，微软提供了一个名为**Server Core应用程序兼容性FOD**（Feature-on-Demand，可选安装）的功能，它也支持一些图形界面的管理工具。
- **Nano Server**：类似于Server Core，但明显较小，适用于云环境，没有本地登录功能。Windows Server 2022仅在容器（container）内支持Nano Server。

2.1.2　Windows Server 2022 的系统需求

如果要在计算机内安装并使用 Windows Server 2022，此计算机的硬件配置需符合表 2-1-1 所示的基本需求。需要特别说明的事，以下说明同时适用于**包含桌面体验的服务器、Server Core 与 Nano Server**）。

表 2-1-1　安装 Windows Server 2000 的硬件配置需求

组件	需求（附注）
处理器（CPU）	最少 1.4GHz、64 位；支持 NX 与 DEP；支持 CMPXCHG16B、LAHF/SAHF 与 PREFETCHW；支持 SLAT（EPT 或 NPT）
内存（RAM）	最少 2GB（包含桌面体验的服务器，建议用 ECC 内存）
硬盘	最少 32GB，不支持 IDE 硬盘（PATA 硬盘）

① 实际需求根据计算机设置、所安装的应用程序、所扮演的角色以及所安装的功能数量的多少而可能需要增加。

② 本书中的许多示例需要使用多台计算机来练习，此时可以利用 Windows Server 2022 内置的 Hyper-V 来搭建虚拟的测试网络与计算机（详见第 5 章）。

可以到微软网站上下载 coreinfo.exe 程序（假设存储到 C:\coreinfo），然后选中左下角的**开始**图标⊞，再右击➲Windows PowerShell（管理员），➲切换到 C:\coreinfo 目录，➲输入.**coreinfo** 命令来查看计算机的 CPU 是否支持表 2-1-1 中所列功能。例如，从图 2-1-1 中可以看出计算机支持 64 位与 NX，而从图 2-1-2 中可以看出支持 CMPXCHG16B(CX16)与 LAHF/SAHF。

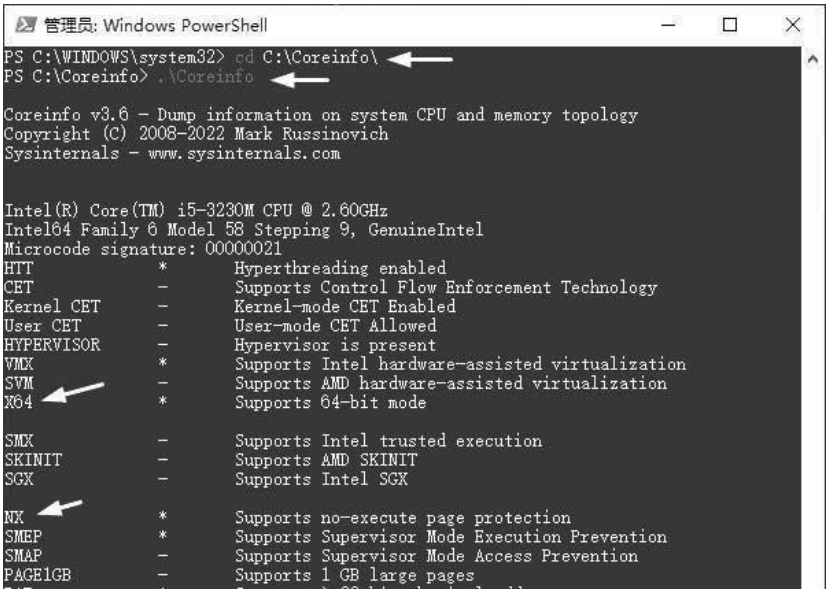


图 2-1-1

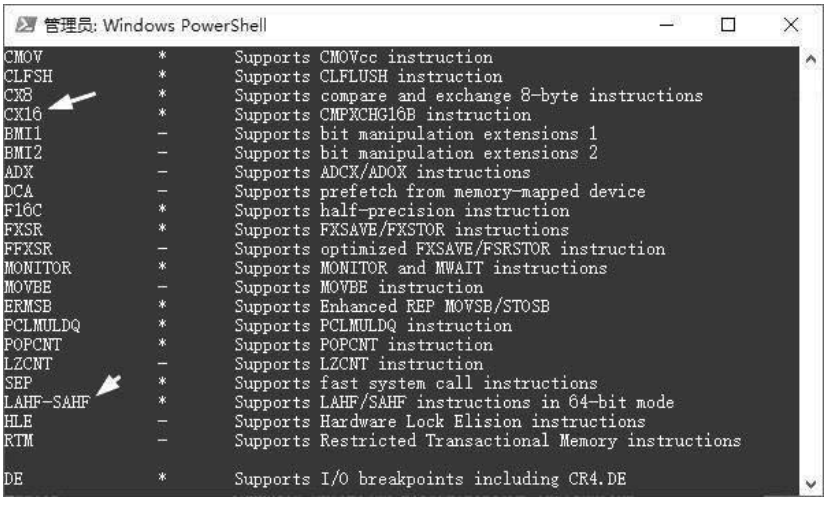


图 2-1-2

从图 2-1-3 中可以看出支持 PREFETCHW，从图 2-1-4 中执行**.\coreinfo/v（当前系统为 64 位时执行.\coreinfo64 /v）**的结果可以看出支持 SLAT。

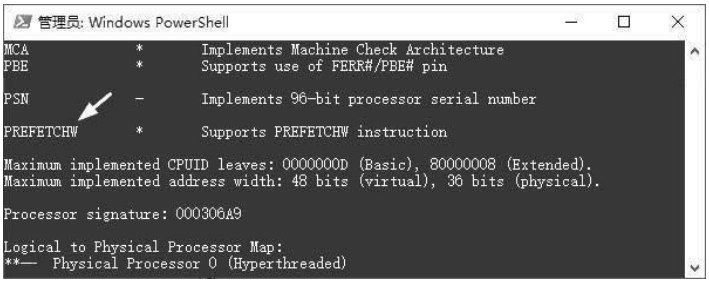


图 2-1-3

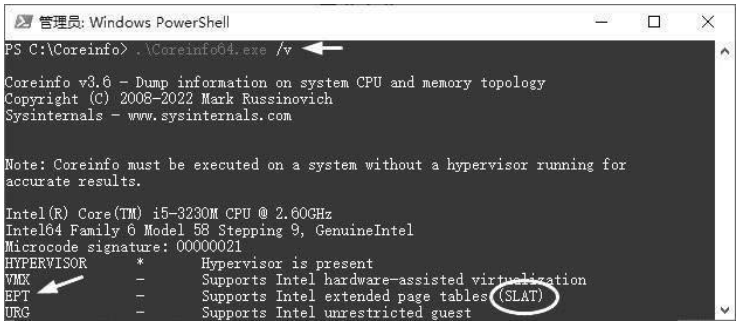


图 2-1-4

2.1.3　选择磁盘分区

在磁盘（硬盘）具备存储数据的能力之前，需要将其分割成一个或数个磁盘分区（partition），每个磁盘分区都是一个独立的存储单位。在安装过程中选择要安装 Windows Server 2022 的磁盘分区（以下假设为 MBR 磁盘，详见第 10 章）：

- 如果磁盘并未经过分区（例如全新磁盘），如图2-1-5左图所示，则可以将整个磁盘视为一个磁盘分区，并选择将Windows Server 2022安装到此分区（会被安装到**Windows**文件夹内）。不过，因为安装程序会自动建立一个系统保留分区（详细内容见第10章），因此最终的结果如图2-1-5右图所示。

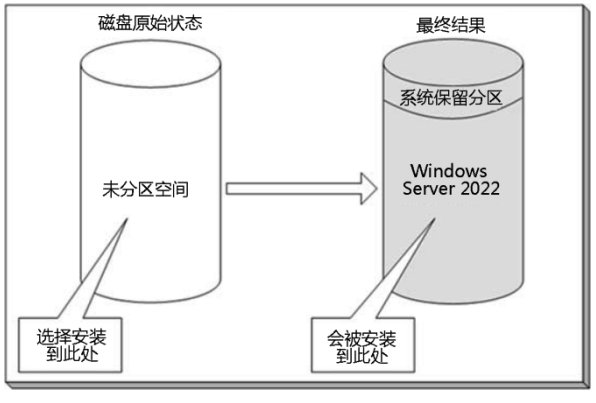


图 2-1-5

- 可以将一个未分区磁盘的部分空间划分出一个磁盘分区，然后将Windows Server 2022安装到此分区。不过安装程序还会自动建立一个系统保留分区，如图2-1-6所示。图中最终结果中，剩余未分区的空间可以用作数据存储分区或安装另外一套操作系统。

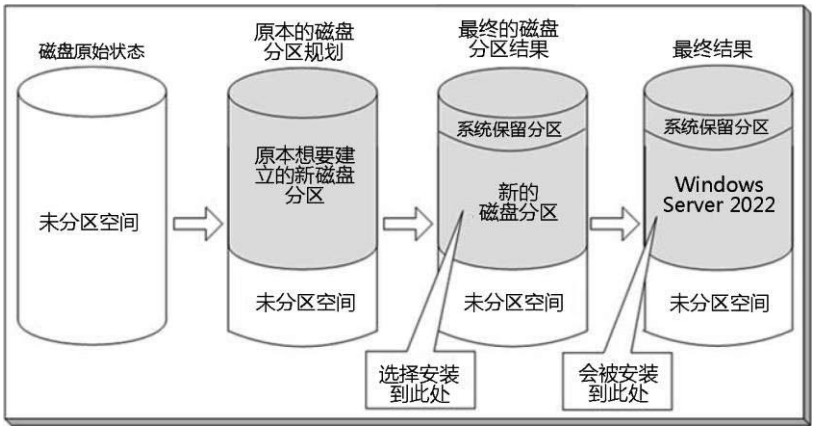


图 2-1-6

- 当磁盘分区内已经安装了其他操作系统时，例如Windows Server 2019，如果要将Windows Server 2022安装到此分区，则可以进行如下操作（见图2-1-7）：
  - **对旧版 Windows 系统升级**：此时旧版系统会被 Windows Server 2022 取代，同时原来大部分的系统配置会被保留在 Windows Server 2022 系统内，一般的数据文件（非操作系统文件）也会被保留。
  - **不对旧版 Windows 系统升级**：此磁盘分区内原有文件会被保留，虽然旧版系统已经无法使用，不过此系统所在的文件夹（一般是 Windows）会被移动到 Windows.old 文件夹内。而新的 Windows Server 2022 会被安装到此磁盘分区的 Windows 文件夹内。

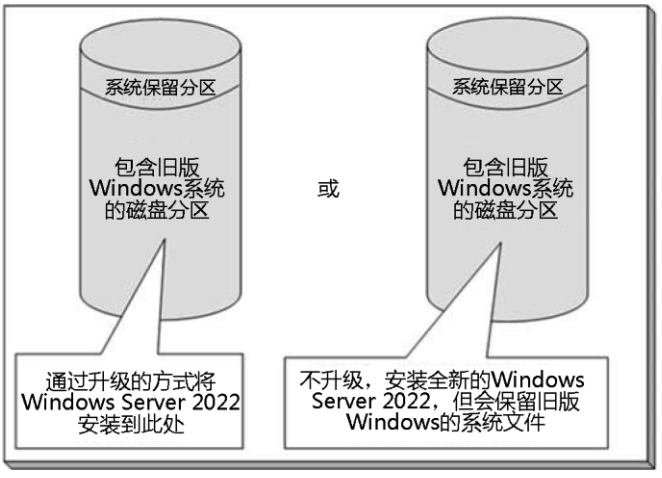


图 2-1-7

如果在安装过程中将现有磁盘分区删除或格式化，则该分区内的现有数据都将丢失。

- 虽然磁盘内已经安装了其他Windows系统，不过如果该磁盘内尚有其他未分区空间，则可以将Windows Server 2022安装到此未分区空间的Windows文件夹内，如图2-1-8所示。此方式在启动计算机时，可选择Windows Server 2022或原有的其他Windows系统，这就是所谓的**多重引导**（multiboot）设置。

磁盘分区需要被格式化成适当的文件系统后，才能在其中安装操作系统与存储数据。常见的文件系统包含 NTFS、ReFS、FAT32、FAT 与 exFAT 等。需要注意的是，Windows Server 2022 只能安装到 NTFS 格式的磁盘内，其他格式的磁盘只能用来存储数据。

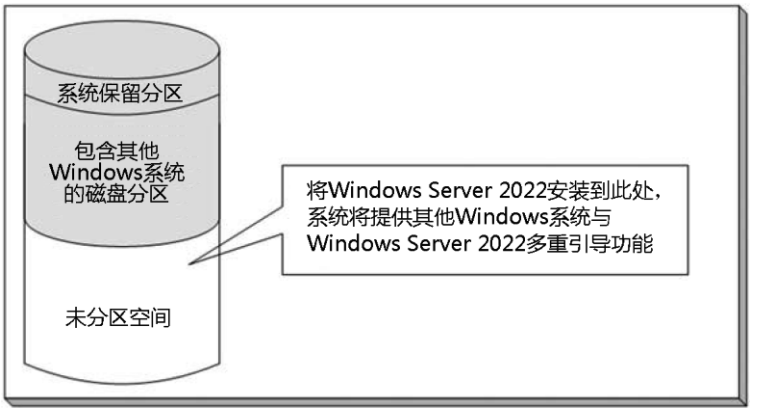


图 2-1-8

2.2　安装或升级为Windows Server 2022

可以选择全新安装 Windows Server 2022 或将现有的旧版本 Windows 系统升级（以下主要是针对具备图形界面的“桌面体验的服务器”来说明）。

- **全新安装**：利用包含Windows Server 2022安装文件的可启动U盘（或DVD）来启动计算机并执行U盘内的安装程序。如果磁盘内已经有旧版Windows系统，则也可以先启动此系统，然后插入U盘来执行其中的安装程序；也可以直接执行Windows Server 2022 ISO文件内的安装程序。
- **将现有的旧版Windows操作系统升级**：先启动旧版本的Windows系统，然后插入包含Windows Server 2022安装文件的U盘（或DVD）来执行其中的安装程序；也可以直接执行Windows Server 2022 ISO文件内的安装程序。

2.2.1 使用 U 盘启动计算机与安装

这种安装方式只能进行全新安装，无法进行升级安装。首先准备好包含 Windows Server 2022 安装文件的可启动 U 盘（或 DVD），然后依照以下步骤来安装 Windows Server 2022。

可以上网找工具程序来制作包含 Windows Server 2022 安装文件的可启动 U 盘，例如 Rufus、Windows USB/DVD Download Tool 等。

STEP 1 将 Windows Server 2022 安装文件的可启动 U 盘插入计算机的 USB 插槽。

STEP 2 将计算机的 BIOS 设置改为从 USB 来启动计算机，重新启动计算机后就会执行 U 盘内的安装程序（开启计算机的电源后，按 Delete 键或 F2 键可进入 BIOS 设置界面，然后选择从 U 盘启动计算机）。

STEP 3 在图 2-2-1 的界面中直接单击下一页按钮后单击现在安装按钮。

图 2-2-1

STEP 4 在激活 Microsoft Server 操作系统设置界面，输入产品密钥后单击下一页按钮，或是单击**我没有产品密钥来试用此产品**。

STEP 5 在图 2-2-2 中选择要安装的版本后单击下一页按钮（此处我们选择 Windows Server 2022 Datacenter（Desktop Experience））。

STEP 6 在**适用的声明和许可条款**界面中勾选**我接受 Microsoft 软件许可条款**后单击下一页按钮。

STEP 7 在图 2-2-3 中单击**自定义：仅安装 Microsoft Server 操作系统（advanced(C)）**。

图 2-2-2

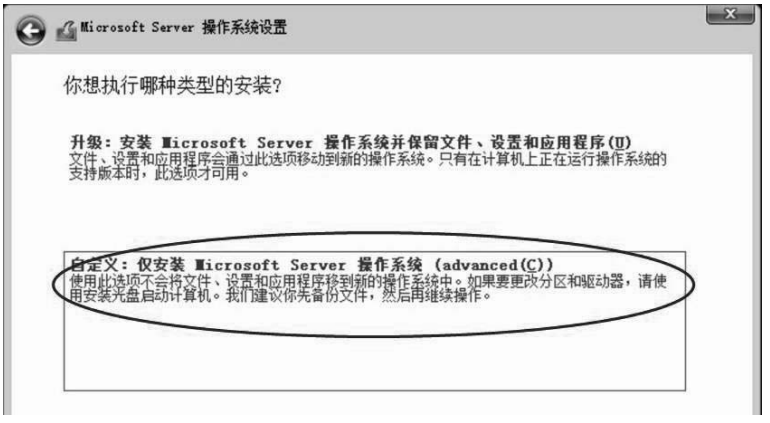


图 2-2-3

STEP 8　在**操作系统的安装位置**界面中直接单击下一页按钮以便开始安装 Windows Server 2022。

如果需要安装厂商提供的驱动程序才能访问磁盘，请在安装界面中单击**加载驱动程序**；若单击**新建**，可以建立主分区；单击**格式化**、**删除**，则会执行对现有磁盘分区的格式化或删除。

2.2.2　在现有的 Windows 系统内安装

这种安装方式既可以用来升级安装，也可以用来全新安装，不过主要是用来升级安装，因此以下说明以升级安装为主。请准备好包含 Windows Server 2022 安装文件的 ISO 文件或可启动 U 盘（或 DVD），然后按照以下步骤来安装 Windows Server 2022。

STEP 1 启动现有的 Windows 系统、登录。

STEP 2 插入包含 Windows Server 2022 安装文件的 U 盘（或 DVD），让系统自动执行 U 盘内的安装程序；也可以手动直接执行 ISO 文件内的安装程序 **setup.exe**。

STEP 3 接下来的步骤与前面利用 U 盘来启动计算机以及安装操作系统类似，此处不再赘述。

2.3 启动与使用Windows Server 2022

2.3.1 启动与登录

安装完成后会自动重新启动。在第一次启动 Windows Server 2022 时，会出现如图 2-3-1 所示的页面来要求设置系统管理员 Administrator 的密码（单击密码右侧图标可显示所输入的密码），设置好后单击完成按钮。

图 2-3-1

用户的密码默认需至少 6 个字符、不可包含用户账户名称或全名，还有至少要包含 A～Z、a～z、0～9、特殊字符（例如!、$、#、%）等 4 组字符中的 3 组，例如 12abAB 是一个有效的密码，而 123456 则是无效的密码。

接下来请按照图 2-3-2 的要求按 Ctrl+Alt+Delete 组合键（先按 Ctrl+Alt 组合键不放，再按 Delete 键），接着在图 2-3-3 的界面中输入系统管理员（Administrator）的密码，最后按 Enter 键登录（sign in）。登录成功后会出现如图 2-3-4 所示的**服务器管理器**界面。

图 2-3-2

图 2-3-3

图 2-3-4

① 可以利用**服务器管理器**来管理系统；图 2-3-4 中提示了可以通过浏览器的管理工具**Windows Admin Center**。

② 如果已经关闭**服务器管理器**，可以通过单击左下角**开始**图标⊞➲服务器管理器来重新打开。

③ 也可以通过自定义的**微软管理控制台**（Microsoft Management Console，MMC）来管理系统，具体步骤是：按⊞+R键➲输入 **MMC**➲单击确定按钮➲选择**文件**菜单➲添加/删除管理单元➲在列表中选择所需的工具。

2.3.2 锁定、注销与关机

如果暂时不想使用此计算机，但又不能将此计算机关闭，可以选择锁定或注销。单击左下角的**开始**图标⊞，然后单击图 2-3-5 中代表用户账户的人头图标：

- **锁定**：锁定期间所有的应用程序都仍然会继续执行。如果要解除锁定，以便继续使用此计算机，需要重新输入密码。
- **注销**：注销会结束当前正在运行的应用程序。之后如果要继续使用此计算机，必须重新登录。

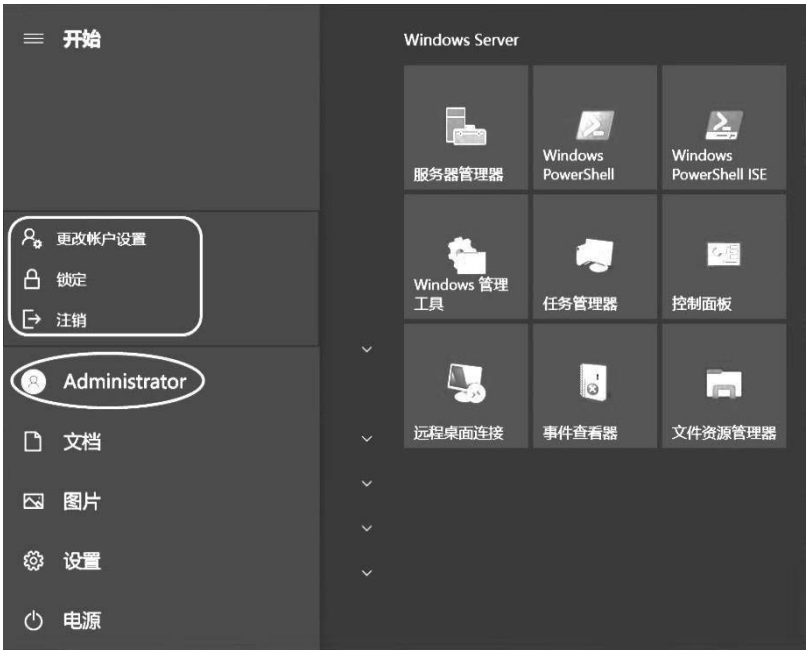


图 2-3-5

如果要关闭计算机或重新启动计算机，则单击左下角的**开始**图标⊞➲单击选**关机**或**重启**，如图 2-3-6 所示。

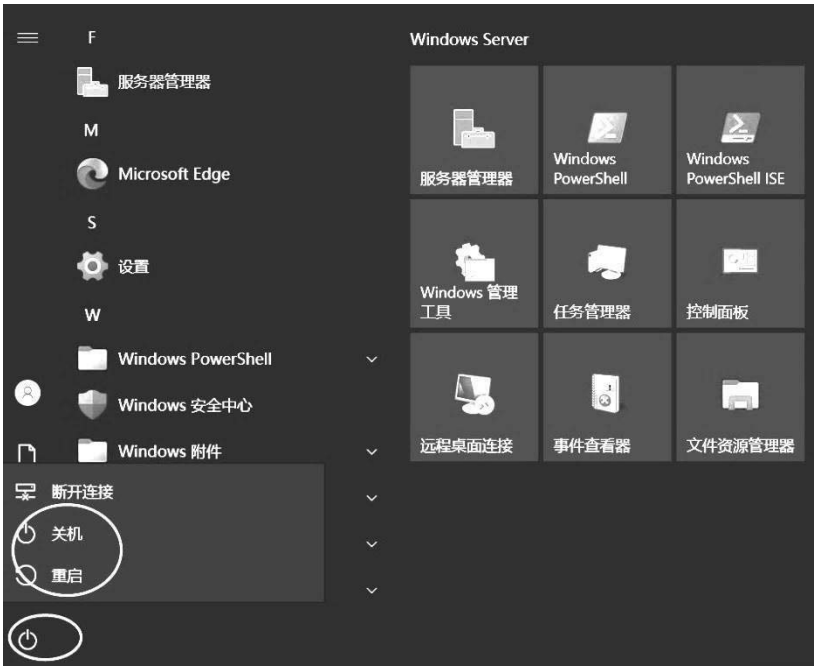


图 2-3-6

也可以直接按 Ctrl+Alt+Delete 组合键，然后在图 2-3-7 所示的界面选择**锁定**、**注销**等功能，或单击右下角的**关机**图标。

图 2-3-7

3

第 3 章　Windows Server 2022 基本环境

本章将介绍如何设置 Windows Server 2022 的基本环境，以便熟悉并掌握基本的服务器管理能力。

- 屏幕的显示设置
- 计算机名称与TCP/IP设置
- 安装Windows Admin Center
- 连接Internet与启用Windows系统
- Windows Defender 防火墙与网络位置
- 环境变量的管理
- 其他的环境设置

3.1　屏幕的显示设置

通过对显示设置做适当的调整，可以让显示器得到最佳的显示效果，提高观看屏幕的舒适度，保护眼睛。

屏幕上所显示的字符由一个一个点所组成，这些点被称为**像素**（pixel）。我们可以自行调整水平与垂直的显示点数，例如水平 1920 点、垂直 1080 点，此时我们将其称为“分辨率为 1920×1080”，分辨率越高，画面越细腻，影像与对象的清晰度越佳。每一个**像素**所能够显示的颜色多寡，取决于使用多少位（bit）来显示 1 个**像素**。例如，若用 16 位来显示 1 个**像素**，那么 1 个**像素**可以有 2^{16} =65 536 种颜色；同理，32 位可以有 2^{32} = 4 294 967 296 种颜色。

如果要调整显示分辨率或文字的大小等设置，具体的步骤为：右击桌面空白处➲显示设置➲然后通过图 3-1-1 所示的选项。如果要同时修改屏幕分辨率、显示颜色与屏幕更新频率，则可以单击图 3-1-1 下方的**高级显示设置**➲显示器 1 的显示适配器属性。

图 3-1-1

3.2　计算机名与TCP/IP设置

计算机名与 TCP/IP 的 IP 地址都是用来识别计算机的信息，它们是计算机之间相互通信

所需要的基本信息。

3.2.1 更改计算机名与工作组名

每一台计算机的计算机名必须是唯一的，不应该与网络上其他计算机重复。虽然系统会自动设置计算机名，不过建议将此计算机名改为易于识别的名称。每一台计算机所隶属的工作组名称默认都是 WORKGROUP。更改计算机名或工作组名的方法如下所示。

STEP 1 单击左下角的**开始**图标⊞➲服务器管理器（先关闭关于 Windows Admin Center 的说明窗口）➲单击图 3-2-1 中**本地服务器**右侧由系统自动设置的计算机名➲单击前景图的更改按钮。

图 3-2-1

Windows 11、Windows 10 更改计算机名的方法为：选中左下角的**开始**图标（或⊞），再右击➲系统➲重命名这台计算机。

STEP 2 更改图 3-2-2 中的**计算机名**后单击确定按钮（图中并未更改**工作组**名），按照提示重新启动计算机后，这些更改才会生效。

图 3-2-2

3.2.2　TCP/IP 的设置与测试

一台计算机如果要与网络上其他计算机通信，还需要有适当的 TCP/IP 设置值，例如正确的 IP 地址。一台计算机取得 IP 地址的方式有两种：

- **自动获取IP地址**：这是默认设置，此时计算机会自动向DHCP服务器租用IP地址，这台服务器可能是一台计算机，也可能是一台具备DHCP服务器功能的代理服务器（NAT）、宽带路由器、无线基站等。
  如果找不到DHCP服务器，此计算机会采用Automatic Private IP Addressing（APIPA）机制自动为自己分配一个符合169.254.0.0/16格式的IP地址。不过，此时此计算机仅能够与同一个网络内也是使用169.254.0.0/16格式的计算机通信。
- **手动设置IP地址**：这种方式会增加系统管理员的负担，而且手动设置容易出错，适合于需要固定IP地址的企业内部服务器使用。

1. 设置 IP 地址

STEP 1　打开**服务器管理器**➲单击图 3-2-3 中**本地服务器**右侧**以太网**的设置值➲双击图中的**以太网**。

STEP 2　在图 3-2-4 中单击**属性**按钮➲Internet 协议版本 4（TCP/IPv4）➲属性。

STEP 3　在图 3-2-5 中设置 IP 地址、子网掩码、默认网关与首选 DNS 服务器等。设置完成后依次单击确定按钮和关闭按钮来结束设置。

- **IP地址**：可按照计算机所在的网络环境进行设置，或按照图进行设置。
- **子网掩码**：请按照计算机所在的网络环境来设置，如果IP地址设置成图中的192.168.8.1，则可以输入255.255.255.0，或在IP地址输入完成后直接按Tab键，系统会自动填入子网掩码的默认值。

- **默认网关**：位于内部局域网的计算机若要通过路由器或代理服务器（NAT）来连接Internet，此处请输入路由器或代理服务器的局域网IP地址（LAN IP地址），假设是192.168.8.254，否则保留空白即可。
- **首选DNS服务器**：位于内部局域网的计算机若要上网，此处请输入DNS服务器的IP地址，它可以是企业自行搭建的DNS服务器、Internet上任一台可提供服务的DNS服务器（例如图中是Google的DNS服务器IP地址8.8.8.8）或代理服务器的局域网IP地址（LAN IP地址）等。
- **备用DNS服务器**：如果首选DNS服务器故障且没有响应，则会自动改用此处的DNS服务器。

图 3-2-3

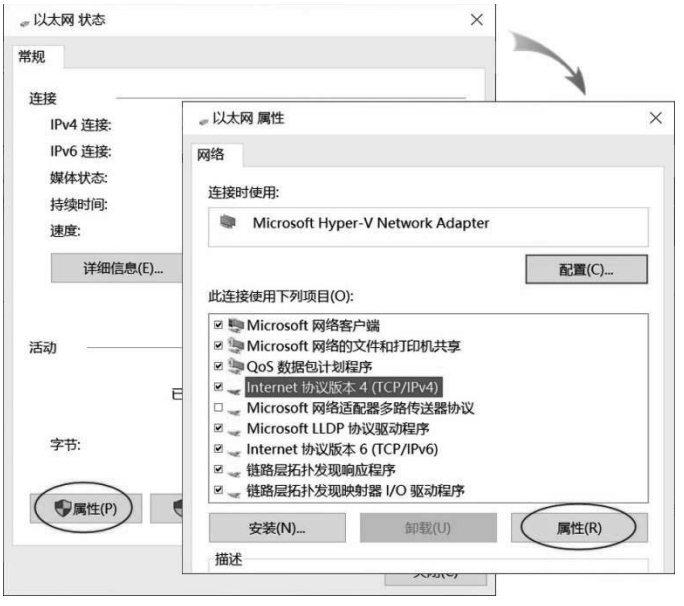


图 3-2-4

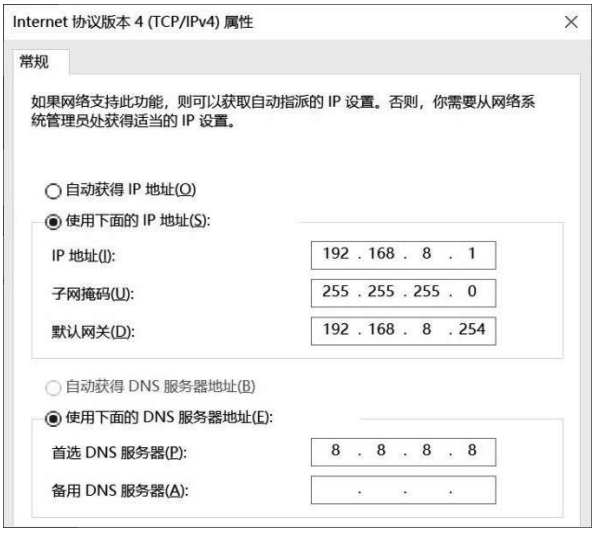


图 3-2-5

2. 查看 IP 地址的设置值

如果 IP 地址是自动获取的，我们可能想要知道所租用的 IP 设置值是什么？即使 IP 地址是手动设置的，所设置的 IP 地址也不一定就是可用的 IP 地址，例如 IP 地址已经被其他计算机先占用了。这时，我们可以通过图 3-2-6 的**服务器管理器**来查看 IP 地址的设置值（此例中为 192.168.8.1）。

图 3-2-6

若要查看更详细的信息，单击图 3-2-6 中圈起来的部分➲双击**以太网**➲单击**详细信息**按钮➲，就可看到 IP 地址的详细设置值（见图 3-2-7），从图中还可以看到网卡的物理地址（MAC address）为 00-15-5D-79-B0-00。

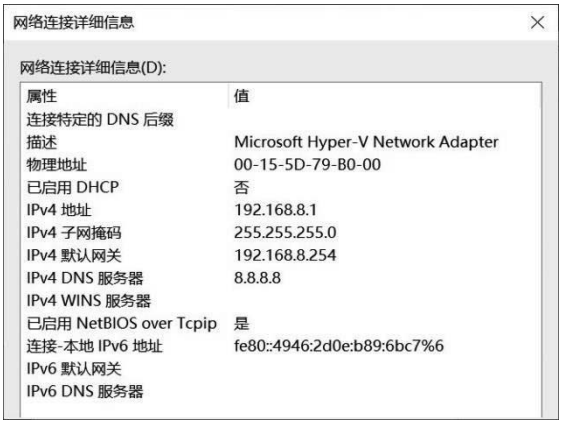


图 3-2-7

① 如果 IP 地址与同一网络内另一台计算机的 IP 地址相同（或冲突），且该计算机先启动了，则系统会另外分配 169.254.0.0/16 格式的 IP 地址给当前计算机使用，且在图 3-2-6 中圈起来处会显示**多个 IPv4 地址**信息（单击该处可查看细节）。

② 也可以单击左下角的**开始**图标⊞➲Windows PowerShell，然后执行 **ipconfig** 或 **ipconfig /all** 来查看 IP 地址设置值（如果 IP 地址发生冲突，则表示另一台计算机已经使用了此 IP 地址，且目前使用的 IP 地址为**自动设置 IPv4 地址**字段的 IP 地址。

3. 使用 Ping 命令来排错

可以使用 Ping 命令来检测网络问题与找出不正确的设置。单击左下方的**开始**图标⊞➲Windows PowerShell，然后执行：

- **环回测试（loopback test）**：也就是执行**ping 127.0.0.1**命令，它可以检测本地计算机的网卡硬件与TCP/IP驱动程序是否可以正常接收、发送TCP/IP数据包。如果正常，会出现类似图3-2-8的回复界面（自动测试4次）。

图 3-2-8

- 测试与同一个网络内其他计算机是否可以正常通信。例如，若另一台计算机的IP地址为192.168.8.2，此时请输入**ping 192.168.8.2**，如果可以正常通信，则应该会有如图3-2-9所示的回复，不过因为其他计算机的**Windows Defender防火墙**默认已经开启，

它会阻止此数据包，因此可能会出现如图3-2-10所示的**请求超时**的界面。

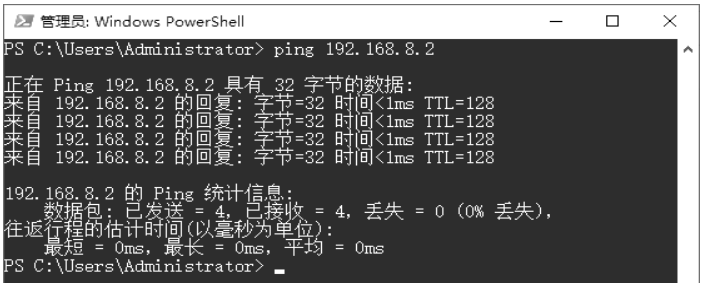


图 3-2-9

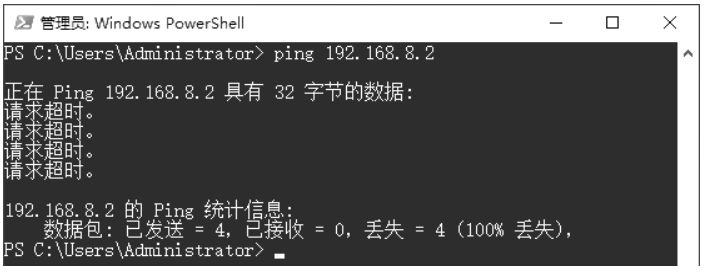


图 3-2-10

- Ping默认网关的IP地址。它可以检测当前计算机是否能够与默认网关正常通信，只有与默认网关正常通信之后才可以通过默认网关来与其他网络的计算机通信。

3.3　安装Windows Admin Center

除了**服务器管理器**之外，现在又添加了一个浏览器界面的管理工具——Windows Admin Center。在启动**服务器管理器**时，会有一个该管理工具的使用提示（见图 3-3-1）。可以通过单击图中的链接来下载与安装该工具。

图 3-3-1

通过 Microsoft Edge 下载 Windows Admin Center，下载完成后采用默认值安装即可。安装完成后可以到 Windows 计算机（Windows 11）上打开浏览器（支持 Microsoft Edge 与 Google Chrome），然后输入 **https://服务器的名称或 IP 地址/**，例如 **https://192.168.8.1/**（如果出现此网站不安全的提示信息，可以不加理会，继续单击**高级➲继续访问 192.168.8.1（不安全）**）。接着输入用户账号（例如 Administrator）与密码，单击需要管理的服务器（例如 server1）…，然后便可以如图 3-3-2 所示来管理服务器 server1，例如可以通过界面右上方的**编辑计算机 ID** 来更改计算机名、工作组名等。

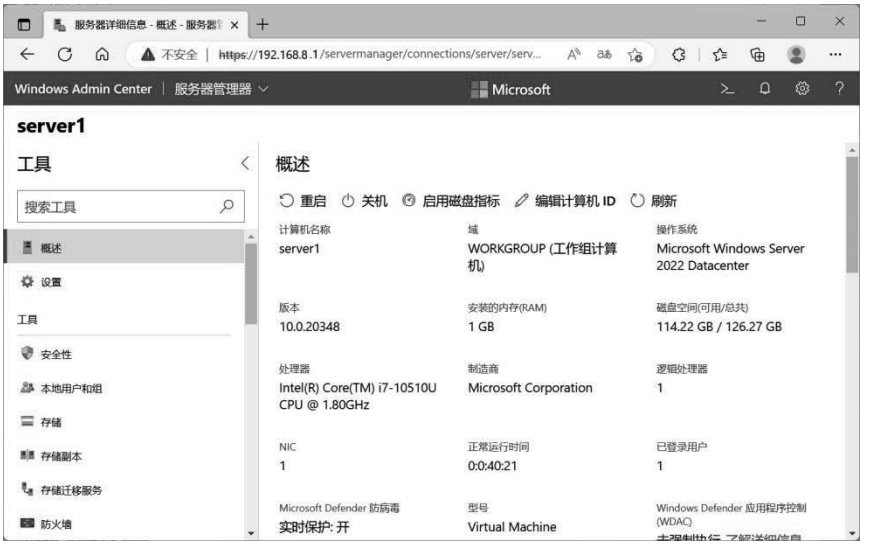


图 3-3-2

3.4 连接Internet与激活Windows系统

Windows Server 2022 安装完成后，需执行激活程序以获得完整的功能。然而，为了执行激活操作，计算机需要先连接到 Internet。

3.4.1 连接 Internet

计算机需要通过以下几种方式来连接 Internet：

- 通过路由器或NAT上网：如果计算机位于企业内部局域网并且通过路由器或NAT来连接Internet，则需将其**默认网关**指定到路由器或NAT的IP地址（参考图3-2-5）。还需要在**首选DNS服务器**处，输入企业内部DNS服务器的IP地址或Internet上任何一台处于工作状态的DNS服务器的IP地址。
- 通过代理服务器上网：需要指定代理服务器，选中左下角的**开始**图标⊞，右击➲运行➲输入control后，单击 确定 按钮➲网络和Internet➲Internet选项➲单击**连接**选项卡下的

局域网设置按钮➲输入企业内部的代理服务器的主机名或IP地址、端口号（图3-4-1中仅是示例）。如果代理服务器支持Web Proxy Autodiscovery Protocol（WPAD），则还可以勾选**自动检测设置**。

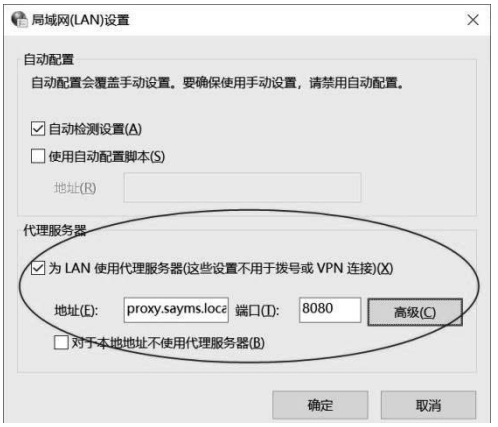


图 3-4-1

- 通过ADSL或VDSL上网：如果想要通过ADSL或VDSL非固定式上网，需要创建一个连接来连接ISP（如中国电信）与上网：选中右下方任务栏的**网络**图标并右击➲打开网络和Internet设置➲网络和共享中心➲单击**设置新的连接或网络**➲单击**连接到**Internet后单击下一步按钮➲单击**宽带（PPPoE）**➲输入用来连接ISP的账号与密码，然后单击连接按钮就可以连接ISP与上网。

3.4.2　激活 Windows Server 2022

Windows Server 2022 安装完成后需执行激活程序，否则有些用户个性化功能无法使用，例如无法更改背景、颜色等。激活 Windows Server 2022 的方法，打开**服务器管理器**➲通过单击**本地服务器**右侧的**产品 ID** 处的状态值（目前是**未激活**，见图 3-4-2）来输入产品密钥与激活。

图 3-4-2

3.5 Windows Defender防火墙与网络位置

内置的 **Windows Defender 防火墙**可以保护计算机，避免遭受恶意软件的攻击。

3.5.1 网络位置

系统将网络位置分为**专用网络**、**公用网络**与**域网络**，并且可以自动识别计算机所在的网络位置。例如，加入域的计算机的网络位置会自动被设置为**域网络**。我们可以通过单击左下角的**开始**图标➲**设置**图标➲更新和安全（Windows 11 为**隐私和安全性**）➲Windows 安全中心➲防火墙和网络保护来查看网络位置。如图 3-5-1 所示的**使用中**字样，表示此计算机所在的网络位置为**公用网络**。

为了提高计算机在网络内的安全性，因此要为位于不同网络位置的计算机设置不同的防火墙规则。例如，位于公用网络的计算机，其防火墙的设置较为严格，而位于专用网络的计算机的防火墙则较为宽松。

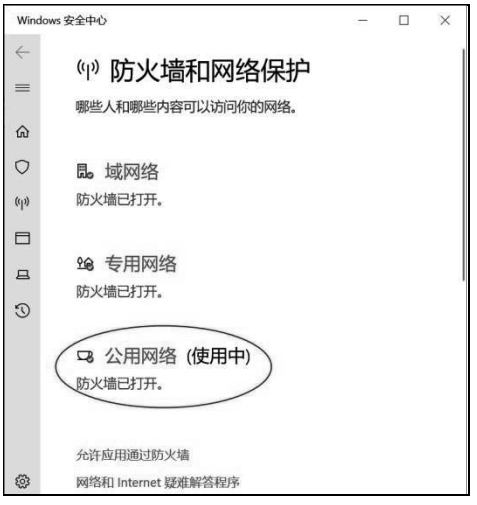


图 3-5-1

如果要自行更改网络位置，例如要将网络位置从**公用网络**修改为**专用网络**，可以单击左下角的**开始**图标➲Windows PowerShell（Windows 11 为 **Windows 终端**），然后先执行以下命令来取得网络名称（见图 3-5-2），例如通常是**网络**：

```
Get-NetConnectionProfile
```

接着再执行以下命令来将此网络的设置变更为 Private：

```
Set-NetConnectionProfile -Name "网络" -NetworkCategory Private
```

系统默认已经针对每一个网络设置来启用 **Windows Defender 防火墙**，它会阻止其他计

算机来与这台计算机的相关通信。若要更改设置，则可以单击图 3-5-1 中的**域网络**、**专用网**或**公用网络**来进行相应的更改。

图 3-5-2

3.5.2　解除对某些程序的阻止

Windows Defender 防火墙在默认情况下会阻止传入连接，不过可以通过单击图 3-5-1 下方的**允许应用通过防火墙**来解除对某些程序的阻止，例如如果要允许网络上其他用户来访问当前计算机内的共享文件与打印机，则需要勾选图 3-5-3 中**文件和打印机共享**，并且可以分别设置**专用网络**与**公用网络**（若此计算机已经加入网域，则还会有**域网络**可供选择）。

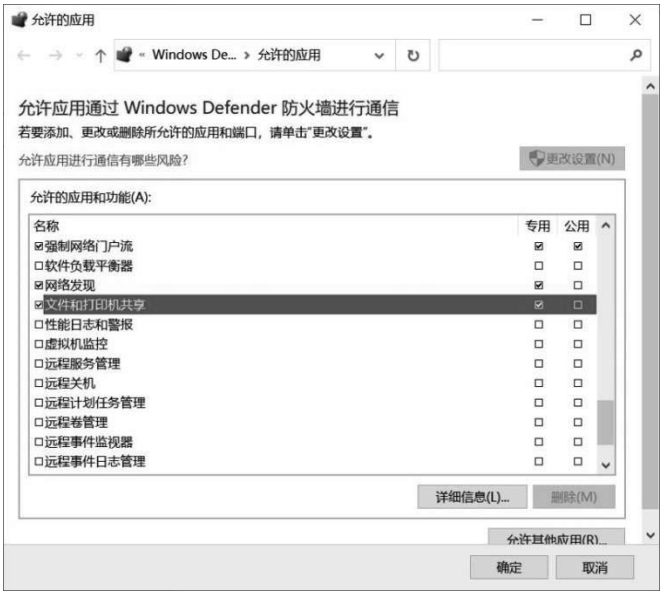


图 3-5-3

3.5.3　Windows Defender 防火墙的高级安全设置

如果要进一步设置防火墙规则，可以通过**高级安全 Windows Defender 防火墙**：单击图 3-5-1 中的**高级设置**，之后可由图 3-5-4 左侧看出它可以同时针对入站与出站连接来分别设置

访问规则（图中的**入站规则**与**出站规则**）。

图 3-5-4

不同的网络位置可以有不同的 Windows Defender **防火墙**规则设置，同时也有不同的配置文件，而这些配置文件可通过以下的方法来更改，选中图 3-5-4 左侧的**本地计算机上的高级安全 Windows Defender 防火墙**，右击➲属性，如图 3-5-5 所示，图中针对域、专用与公用网络位置的入站与出站连接分别有不同设置值，这些设置值包含：

- **阻止（默认值）**：阻止防火墙规则没有明确允许连接的所有连接。
- **阻止所有连接**：阻止全部连接，无论是否有防火墙规则明确允许的连接。
- **允许**：允许连接，但有防火墙规则明确阻止的连接除外。

图 3-5-5

可以针对特定程序或流量来开放或阻止。例如，防火墙默认是启用的，因此网络上其他用户无法利用 Ping 命令来与当前的计算机通信。如果要开放，可通过**高级安全 Windows**

Defender 防火墙的**入站规则**来开放 ICMP Echo Request 数据包：单击图 3-5-4 左侧的**入站规则**➲单击中间下方的**文件和打印机共享（回显请求 – ICMPv4-In）**➲勾选**已启用**（见图 3-5-6）。

图 3-5-6

如果要开放的服务或应用程序未列在列表中，可在此处通过新建规则来开放。例如，如果此计算机是 Web 服务器，则需要让其他用户来连接此网站，可通过单击图 3-5-7 中**新建规则**来建立一个开放端口号码为 80 的规则。如果安装了系统内置的“Web 服务器（IIS）”，则系统会自动新建规则来开放端口 80。

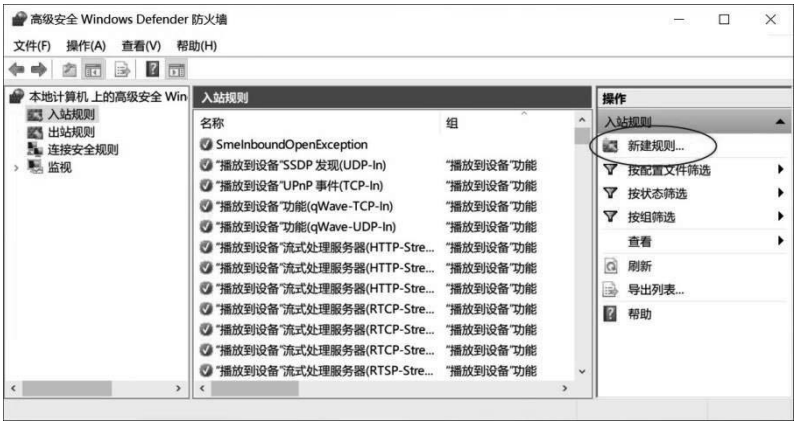


图 3-5-7

3.6　环境变量的管理

环境变量（environment variable）会影响计算机如何执行程序、查找文件、分配内存空间等工作方式。

3.6.1 查看现有的环境变量

可以通过单击左下角的**开始**图标⊞➲Windows PowerShell➲执行 **dir env:**或 **Get-Childitem env:** 命令，来查看现有的环境变量，如图 3-6-1 所示。图中每一行都有一个环境变量，左边 Name 为环境变量名称，右边 Value 为环境变量值。例如，通过环境变量 COMPUTERNAME 和 USERNAME，我们可以分别得知此计算机的计算机名称为 SERVER1、登录的用户为 Administrator。

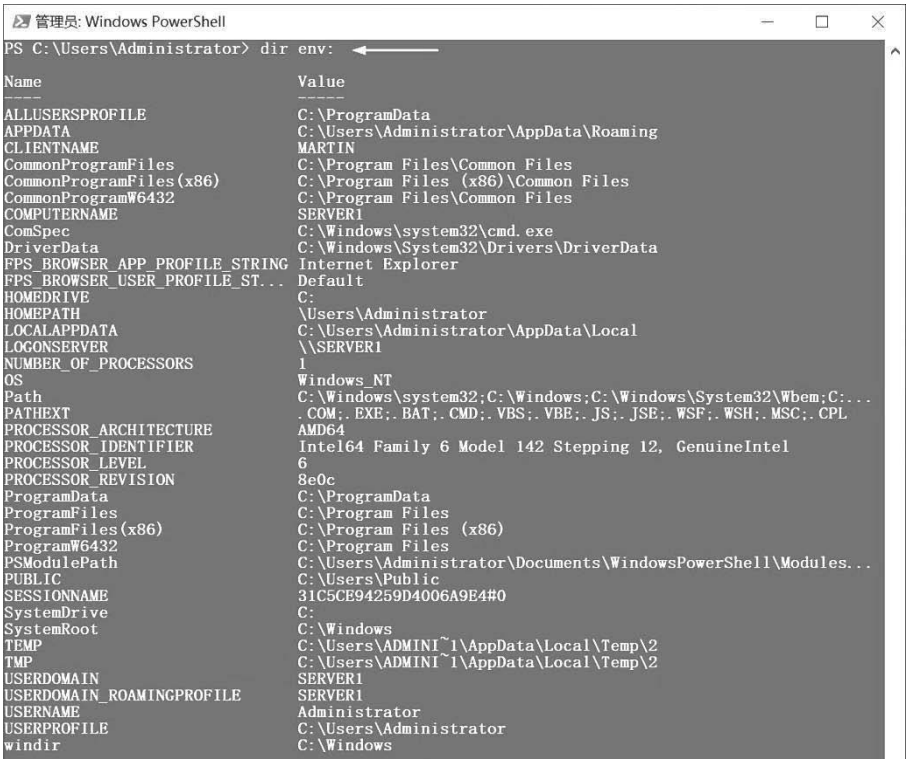


图 3-6-1

也可以按⊞+ R 键➲执行 cmd 来打开**命令提示符**窗口，然后通过 **SET** 命令来查看环境变量。

3.6.2 更改环境变量

环境变量分为以下两类：

- **系统变量**：它会被应用到每一个在此计算机登录的用户，也就是所有用户的工作环境内都会有这些变量。只有具备系统管理员权限的用户，才有权利更改系统变量。建议不要随便修改此处的变量，以免影响系统的正常工作环境。
- **用户变量**：每一个用户可以拥有自己专属的用户变量，这些变量只会被应用到该用

户，不会影响到其他用户。

如果要更改环境变量，选中左下角的**开始**图标⊞，再右击➲系统➲单击右侧的**高级系统设置**➲单击环境变量按钮，然后通过图 3-6-2 所示的窗口来修改，图中上、下半部分别为用户变量区域（此处是 Administrator）与系统变量区域。

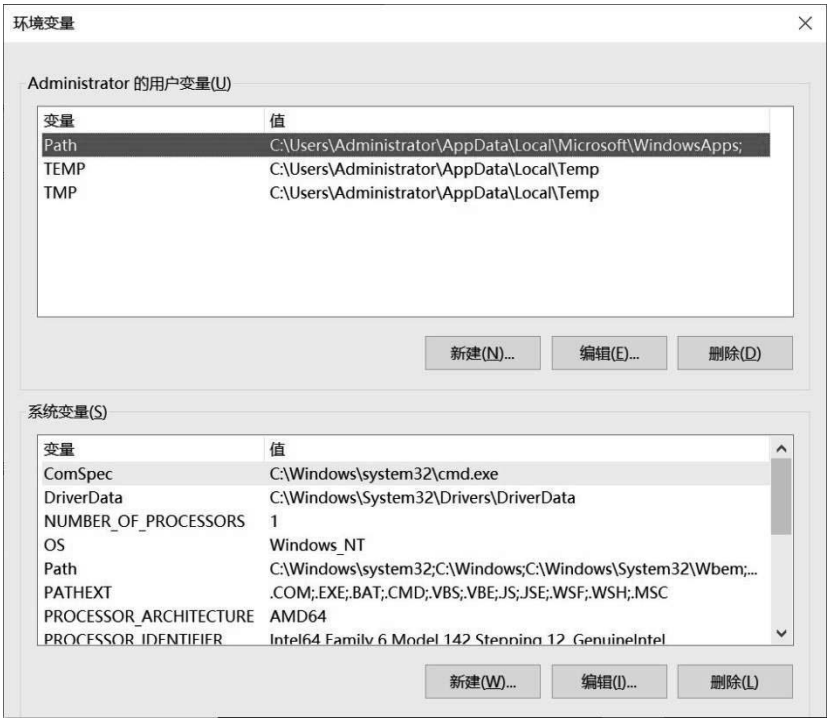


图 3-6-2

计算机在应用环境变量时，会先应用系统变量，再应用用户变量。如果这两个区域内都有相同变量，则以用户变量优先。例如，系统变量区域内有一个变量 TEST=SYS，用户变量列表内也有一个变量 TEST=USER，则最后的结果是 TEST=USER。

变量 PATH 是一个例外：用户变量区域中的 PATH 变量会被附加在系统变量区域中的 PATH 变量之后。例如，系统变量区域内的 PATH= C:\WINDOWS\system32，用户变量区域内的 PATH= C:\Tools，则最后的结果为 PATH=C:\WINDOWS\system32；C:\Tools（系统在查找可执行文件时，是根据 PATH 的文件夹路径，按路径的先后顺序来查找文件）。

3.6.3　环境变量的使用

在 Windows PowerShell 中使用环境变量，可在环境变量前加上**$env:**，例如图 3-6-3 中的**$env:username** 代表当前登录的用户账户名（Administrator）。

图 3-6-3

3.7 其他的环境设置

3.7.1 硬件设备的管理

系统支持 Plug and Play（PnP，即插即用）功能，它会自动检测新安装的设备（例如网卡）并安装其所需的驱动程序。如果新硬件设备无法被自动检测到，则可以尝试单击左下角的**开始**图标⊞➲**设置**图标⚙➲设备➲添加蓝牙和其他设备，以添加设备。

也可以通过单击左下角的**开始**图标⊞➲Windows 管理工具➲计算机管理➲**设备管理器**来管理设备。

还可以在**设备管理器**界面中选中服务器名称，右击➲扫描检测硬件改动来扫描是否有新安装的设备；也可以选中某设备再右击来将该设备禁用或卸载。

在更新某设备的驱动程序后，如果发现此新驱动程序无法正常工作时，可以将之前正常的驱动程序再安装回来，此功能称为**回退驱动程序**（driver rollback）。其操作步骤为：在**设备管理器**界面中选中该设备后右击➲属性➲**驱动程序**选项卡下的回退驱动程序按钮，如图 3-7-1 所示。

图 3-7-1

驱动程序经过签名后，可以确保要安装的驱动程序是安全的。当安装驱动程序时，如果该驱动程序未经过签名、数字签名无法被验证是否有效或驱动程序内容被篡改过，系统会显示警告信息。建议不要安装未经过签名或数字签名无法被验证是否有效的驱动程序，除非确认该驱动程序确实来自发行厂商。

3.7.2　虚拟内存

当计算机的物理内存（RAM）不足时，系统会通过将部分硬盘（磁盘）空间虚拟成内存的方式来提供更多内存给应用程序或服务。系统会建立一个名为 pagefile.sys 的文件作为虚拟内存的存储空间，此文件也被称为**页面文件**。

因为虚拟内存是通过硬盘来提供的，如果硬盘是普通传统硬盘，因其访问速度比内存慢很多，因此若经常发生内存不足的情况，建议给系统安装更多的内存，以免计算机运行效率被硬盘拖慢。

虚拟内存的设置过程，选中左下角的**开始**图标⊞，再右击➲系统➲高级系统设置➲单击**性能**处的设置按钮➲**高级**选项卡➲单击更改按钮，如图 3-7-2 所示。

图 3-7-2

系统默认会自动管理所有磁盘的页面文件，并将文件保存在 Windows 系统安装磁盘的根文件夹中，例如 C：\盘中。页面文件大小有初始大小与最大值，初始大小容量用完后，系统会自动扩大，但不会超过最大值。我们也可以自行设置页面文件大小，或将页面文件同时建立在多个物理磁盘内以提高页面文件的工作效率。

页面文件 pagefile.sys 是受保护的系统文件。想要查看它，操作步骤为：单击**文件资源管理器**图标➲单击上方**查看**菜单➲单击右侧**选项**图标➲**查看**选项卡➲点选**显示隐藏的文件、文件夹和磁盘驱动器**，取消勾选**隐藏受保护的操作系统文件**。之后在 C：\盘下才看得到它（见图 3-7-3）。

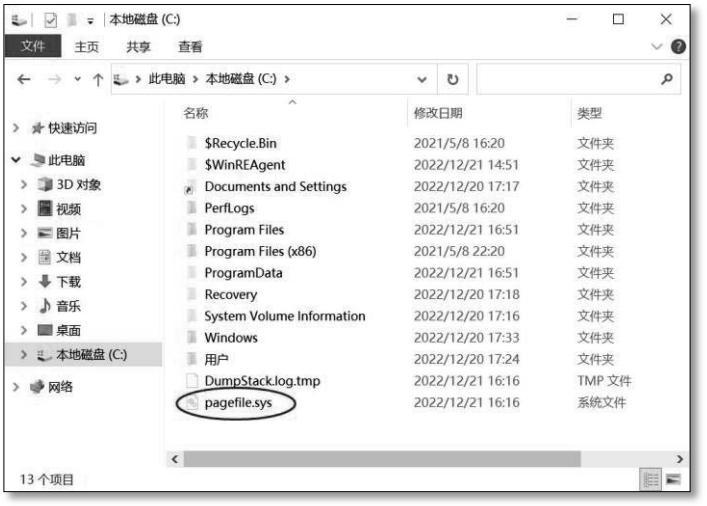


图 3-7-3

① 如果计算机拥有多个显示端口，则可以连接多个显示器来扩大工作桌面，具体的设置方法为：选中桌面空白处后右击➲显示设置。

② 可以通过**任务管理器**来查看或管理计算机内的应用程序、性能、用户与服务等，而打开**任务管理器**的方法为：按 Ctrl+Alt+Delete 组合键➲任务管理器，或右击下方的任务栏➲任务管理器。

③ 为确保计算机的安全性并拥有良好效能，请定期更新系统，定期更新系统的方法为：单击左下角的**开始**图标➲单击**设置**图标➲更新和安全➲Windows 更新。

④ 传统磁盘（HDD）使用一段时间后，存储在磁盘内的文件可能会零零散散的分布在磁盘内，从而影响到磁盘的访问效率，因此建议定期整理磁盘，定期整理方法为：打开**文件资源管理器**➲选中任一磁盘后右击➲属性➲单击**工具**选项卡下的优化按钮，然后选择要整理的磁盘，可以先通过单击分析按钮来了解该磁盘分散的程度，然后通过单击优化按钮来整理磁盘。固态磁盘（SSD）不需要执行整理操作，但也可以执行检查工作，其途径与上述步骤相同。