1

第 1 章　Windows Server 2016 概述

Windows Server 2016可以帮助信息部门的IT人员来搭建功能强大的网站、应用程序服务器与高度虚拟化的云环境。大、中、小型的企业网络都可以利用Windows Server 2016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、保护企业应用程序与数据，让IT人员更轻松有效地管理网站、应用程序服务器与云环境。

- Windows Server 2016版本
- Windows网络架构
- TCP/IP通信协议简介

1.1 Windows Server 2016版本

Windows Server 2016可以提供高经济效益与高度虚拟化的环境，它分为以下三个版本：

- Datacenter Edition：适用于高度虚拟化和软件定义数据中心环境。
- Standard Edition：适用于低密度或非虚拟化的环境。
- Essentials Edition：适用于最多25个用户，最多50台设备的小型企业。

附注

Windows Server 2012 R2中所提供的Foundation版本，在Windows Server 2016中已不再提供。表1-1-1中列出Datacenter与Standard版的主要特点。

表1-1-1

版本	Datacenter	Standard
Windows Server核心功能	✓	✓
操作系统环境（OSE / Hyper-V容器）数量	无限制	2
Windows Server容器	无限制	无限制
Host Guardian Service	✓	✓
Nano Server	✓	✓
Storage Spaces Direct、Storage Replica等存储功能	✓	
Shielded Virtual Machines	✓	
网络堆栈	✓	

1.2 Windows网络架构

您可以利用Windows系统来搭建网络，以便将资源共享给网络上的用户。 Windows的网络架构大致可分为工作组架构（workgroup）、域架构（domain）与包含前两者的混合架构。您也可以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；域架构是集中式的管理模式，适用于中大型网络。下面针对工作组架构与域架构的差异来加以说明。

1.2.1 工作组架构的网络

工作组是由多台通过网络连接在一起的计算机所组成的（参见图1-2-1），它们可以将计算机内的文件、打印机等资源共享出来供网络用户来访问。

工作组网络也被称为**对等式**（peer-to-peer）网络，因为网络上每一台计算机的地位都是平等的，它们的资源与管理是分散在各个计算机上的。它的特性为：

- 每一台Windows计算机都有一个**本机安全账户数据库**，称为Security Accounts Manager（SAM）。用户如果需要访问每一台计算机内的资源，系统管理员便需要在每一台计算机的SAM数据库内建立用户账户。例如，用户Peter需要访问每一台计算机内的资源，则需要在每一台计算机的SAM数据库内建立Peter账户，并设置这些账户的权限。这种架构的账户与权限管理工作比较麻烦，例如当用户需要更改其账号密码时，就需要将该用户在每一台计算机内的账号密码都进行修改。

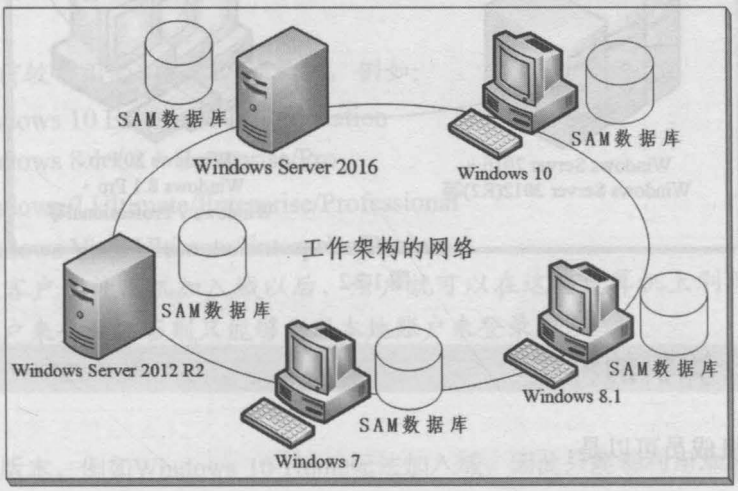

图 1-2-1

- 工作组内可以不要服务器等级的计算机（例如Windows Server 2016），也就是说即使只有Windows 10、Windows 8.1等客户端等级的计算机，也可以搭建工作组架构的网络。
- 如果企业内部计算机数量不多，例如10台或20台计算机，就可以采用工作组架构的网络。

1.2.2 域架构的网络

域也是由多台通过网络连接在一起的计算机所组成的（参见图1-2-2），它们可将计算机内的文件、打印机等资源共享出来供网络用户来访问。与工作组架构不同的是：域内所有计算机共享一个集中式的目录数据库（directory database），该目录数据库包含着整个域内所有用户的账户等相关数据。在域内提供目录服务（directory service）的组件为**Active Directory域服务**（Active Directory Domain Services，AD DS），它负责目录数据库的添加、删除、修改与查询等工作。

在域架构的网络内，这个目录数据库是存储在**域控制器**（domain controller）内的，而只

有服务器等级的计算机才可以扮演域控制器的角色。

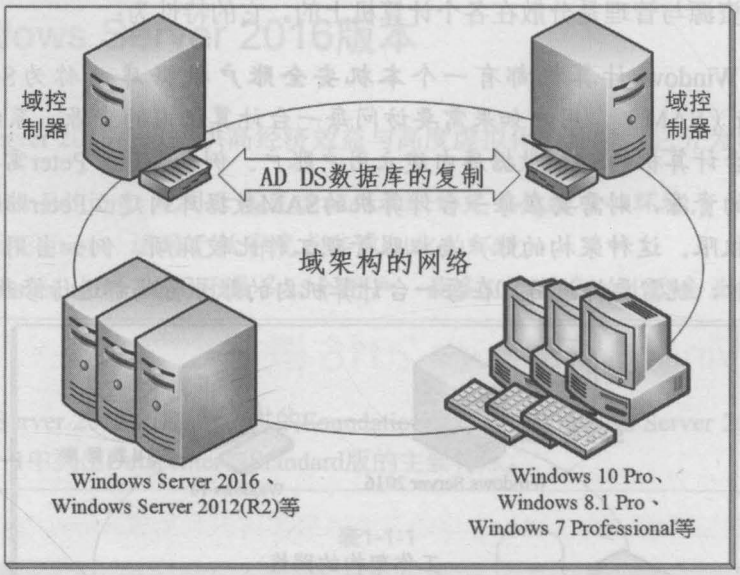

图 1-2-2

1.2.3 域中计算机的种类

域内的计算机成员可以是：

- **域控制器（domain controller）**：需服务器等级的计算机才可扮演域控制器的角色，例如Windows Server 2016 Datacenter、Windows Server 2012 R2 Datacenter等，但并非所有服务器等级的计算机都可扮演域控制器，例如Windows Web Server 2008 R2便无法成为域控制器。

  一个域内可以有多台域控制器，而在大部分情况下，每台域控制器的地位都是平等的，它们各自存储着一份几乎完全相同的AD DS数据库（目录数据库）。当您在其中一台域控制器内新增了一个用户账户后，此账户是被建立在这台域控制器的AD DS数据库中的，之后这份数据会自动被复制到其他域控制器的AD DS数据库内。这个复制动作可确保所有域控制器内的AD DS数据库都能够同步（synchronize），也就是拥有相同数据。

  当用户在域内某台计算机登录时，会由其中一台域控制器根据其AD DS数据库内的账户数据来审核用户所输入的账户与密码是否正确，如果是正确的，用户就可以成功登录，反之将被拒绝登录。

  多台域控制器还可提供容错功能，例如其中一台域控制器故障了，此时仍然能够由其他域控制器来继续提供服务。它也可改善用户登录效率，因为多台域控制器可分担审核用户登录身份（账户名称与密码）的工作。

- **成员服务器（member server）**：当服务器等级的计算机加入域后，用户就可以在这

些计算机上利用Active Directory内的用户账户来登录，否则只能够利用本地用户账户登录。这些加入域的服务器被称为**成员服务器**，成员服务器中没有Active Directory数据，它们也不负责审核域用户的账户名称与密码。成员服务器可以是：

- Windows Server 2016 Datacenter/Standard/Essentials
- Windows Server 2012（R2）Datacenter/Standard
- Windows Server 2008（R2）Datacenter/Enterprise/Standard

若上述服务器并没有被加入域，则它们被称为**独立服务器**（stand-alone server）或**工作组服务器**（workgroup server）。不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），系统可以用它来审核本地用户（非域用户）的身份。

- 其他目前较常用的Windows计算机，例如：
  - Windows 10 Enterprise/Pro/Education
  - Windows 8.1（8）Enterprise/Pro
  - Windows 7 Ultimate/Enterprise/Professional
  - Windows Vista Ultimate/Enterprise/Business

  当上述客户端计算机加入域以后，用户就可以在这些计算机上利用Active Directory内的账户来登录，否则只能够利用本地账户来登录。

注意

1. 较低的版本，例如Windows 10 Home无法加入域，因此只能够利用本地用户账户来登录。
2. 若Windows 10客户端有加入云端Azure Active Directory域，则可以利用Azure Active Directory内的账户来登录。

您可以将Windows Server 2016、Windows Server 2012 R2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。

1.3 TCP/IP通信协议简介

网络上计算机与计算机之间或计算机与网络设备之间，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，需要彼此之间通过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，这个计算机之间的沟通规则被称为**通信协议**（protocol）。Windows系统支持多种的通信协议，其中的TCP/IP是Windows网络依赖最深的通信协议。

TCP/IP通信协议是目前最完整、被支持范围最为广泛的通信协议，它让不同网络架构、不同操作系统的计算机之间可以相互沟通，例如Windows Server 2016、Windows 10、Linux主

机等。它也是Internet的标准通信协议，更是Active Directory Domain Services（AD DS）所必须采用的通信协议。

在TCP/IP网络上，每一台连接在网络上的计算机（设备）都被称为是一台**主机**（host），而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**IP路由器（默认网关）**。

1.3.1 IP地址

每一台主机都有唯一的IP地址（其功能就好像是家里的门牌号码），IP地址不但可以被用来辨识每一台主机，其中也隐含着如何在网络间传送数据的路由信息。

IP地址占用32个位（bit），一般是以4个十进制数来表示，每一个数字称为一个“8位二进制数”（octet）。“8位二进制数”（octet与octet）之间以点（dot）隔开，例如192.168.1.31。

> **附注**
>
> 此处所介绍的IP地址是目前使用最为广泛的IPv4，共占用32位，Windows 系统也支持新版的IPv6。

这个32位的IP地址内包含**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）**：相同网络内的每台主机都有一个唯一的主机标识符。

若此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，整个网络内所有主机都使用这个网络标识符，然后再赋予此网络内每一台主机一个唯一的主机标识符，因此网络上每一台主机都会有一个唯一的IP地址（网络标识符+主机标识符）。您可以向ISP（因特网服务提供商）申请网络标识符。

若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，不用申请，但是网络内各主机的IP地址不可相同。

1.3.2 IP地址分类

传统的IP地址被分为A、B、C、D、E五大类别，其中只有A、B、C三个类别的IP地址可供一般主机来使用（参见表1-3-1），每种类别所支持的IP数量都不相同，以便满足各种不同规模的网络需求。

IP地址共占用4个字节（byte），表中将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

- A类IP地址适合于超大型网络，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A类的网络标识符。
  主机标识符共占用X、Y、Z三个字节（24位），这24位可支持（2^{24}）–2=16 777 216–2=16 777 214台主机（减2的原因后述）。
- B类IP地址适合于中、大型网络，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B类网络。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。
- C类IP地址适合于小型网络，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C类网络。主机标识符只占用一个字节（Z），因此每个网络可支持（2^{8}）– 2 = 254台主机。

在设置主机的IP地址时请注意以下事项：

- **网络标识符不可以是127**：网络标识符127是供**回路测试**（loopback test）使用的，可用来检查网卡与驱动程序是否正常工作。不能将它分配给主机使用。一般来说，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地址将少2个**：例如若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的256个IP地址，但203.3.6.0是用来代表这个网络的（因此我们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是保留给广播用途的（255代表广播），例如若发送信息到203.3.6.255这个地址，表示将信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C类网络示例，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与22。

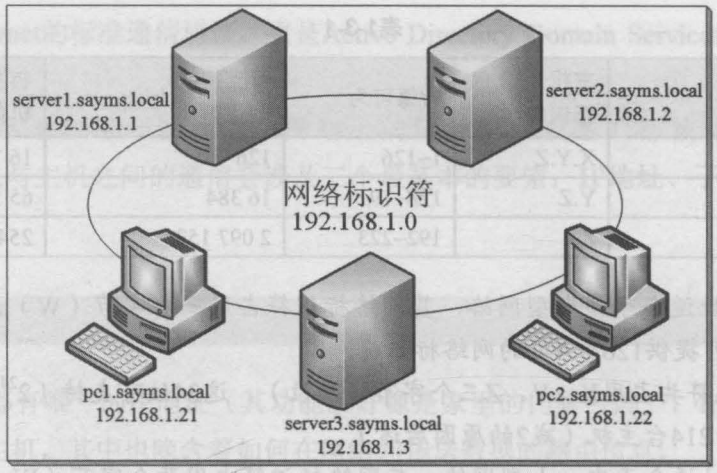

图 1-3-1

1.3.3 子网掩码

子网掩码也占用32位，当IP网络上两台主机在相互通信时，它们利用子网掩码来得知双方的网络标识符，进而得知彼此是否在相同网络内。

表1-3-2中为各类别IP地址默认的子网掩码值，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，例如若某台主机的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做AND逻辑运算（参见图1-3-2），所得出来的结果192.168.1.0就是网络标识符。

表1-3-2

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

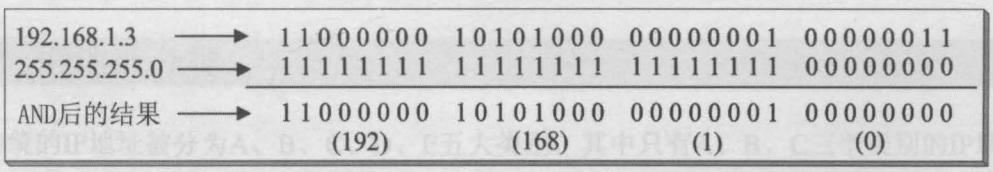

图 1-3-2

若主机A的IP地址为192.168.1.3、子网掩码为255.255.255.0，主机B的IP地址为

192.168.1.5、子网掩码为255.255.255.0，因此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，因此可直接相互通信，不需要借助于路由器（可参阅系列著作：**Windows Server 2016网络管理与架站**）。

注意

前面所叙述的 A、B、C类IP地址为类别式的划分方式，不过目前最普遍采用的却是无类别的CIDR（Classless Inter-Domain Routing）划分方式，这种方式在表示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，则一般我们会利用192.168.1.0/24来代表此网络，其中的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，则一般我们会利用10.120.0.0/16来代表此网络。

1.3.4 默认网关

主机A若要与同一个IP子网内的主机B通信（网络标识符相同），可以直接将数据发送给主机B；但是若要与不同子网内的主机C通信的话（网络标识符不同），就需要先将数据发送给路由器，再由路由器负责发送给主机C。一般主机若要通过路由器来转发数据的话，只要事先将其**默认网关**指定到路由器的IP地址即可。

以图1-3-3为例，甲、乙两个网络是通过路由器来连接的。当甲网络的主机A需要与乙网络的主机C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C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，因此主机A可以判断出主机C是位于不同的子网内，会将数据发送给默认网关，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其发送到主机C。

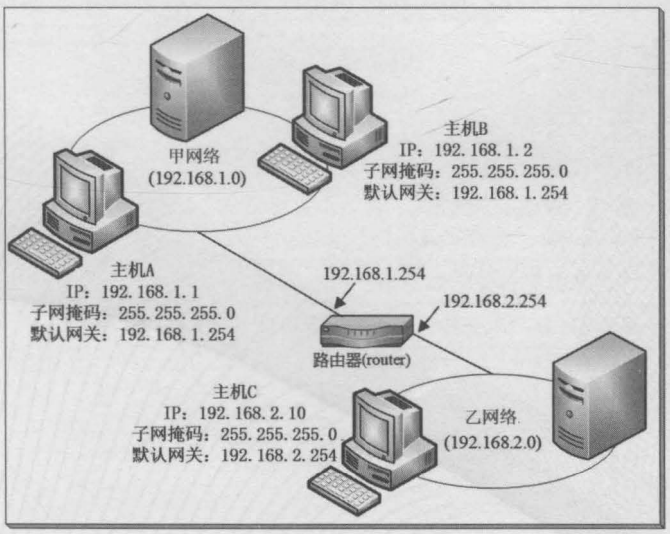

图 1-3-3

1.3.5 私有IP的使用

前面提到IP类别中的A、B、C类是可供主机使用的IP地址。在这些IP地址中，有一些被归类为**私有IP**（private IP，参见表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成本。

表1-3-3

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只能够在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，但是无法直接与外部计算机通信。使用私有IP的计算机若要对外上网、收发电子邮件，则需要通过具备Network Address Translation（NAT）功能的设备，例如IP共享器、宽带路由器等。另一本书《**Windows Server 2016网络管理与架站**》中有NAT的详细说明。

其他不属于私有IP的地址被称为**公有IP**（public IP），例如220.135.145.145。使用公有IP的计算机可以通过路由器来直接对外通信，因此在这些计算机上可以搭建商业网站，让外部用户直接连接此商业网站。这些公有IP必须事先申请。

如果Windows Server 2016计算机的IP地址设置是采用自动获取的方式，但是却因故无法获取IP地址，那么此时该计算机会通过Automatic Private IP Addressing（APIPA）机制来为自己设置一个网络标识符为169.254.0.0的临时IP地址，例如169.254.49.31，不过只能够利用它来与同一个网络内IP地址也是169.254.x.x格式的计算机通信。