第5章

DNS服务器的配置和应用

域名系统(Domain Name System,DNS)服务器是现代计算机网络中应用最为广泛的一种名称解析服务,无论是 Internet 还是 Intranet 都在广泛使用。DNS 一般需要建立在相应的操作系统平台上,为基于 TCP/IP 的客户端提供名称解析服务。本章的几个实验将以 Windows Server 2016 操作系统为平台,系统介绍 DNS 服务器的安装、配置和应用方法。其中,所使用的域名为 wldhj.com。

5.1 实验 1 配置基于活动目录的第 1 台 DNS 服务器

本实验将结合 Windows Server 2016 活动目录(Active Directory)的功能和特点,介绍 DNS 服务器的配置方法。在本实验中,DNS 在安装活动目录的过程中同时安装。

5.1.1 实验概述


视频讲解

在使用 TCP/IP 的网络中,当给每台计算机(主机)分配了独立的 IP 地址后,便可以通过 IP 地址找到这台计算机并与之进行通信。但是,当网络的规模较大时,使用 IP 地址就不太方便了,所以便出现了主机名(Host Name)与 IP 地址之间的一种对应解决方案,使用形象易记的主机名而非 IP 地址进行网络的访问,这比单纯使用 IP 地址显然要方便得多。

1. 实验目的

主机名与 IP 地址之间的映射使用了解析的概念和原理,因为单独通过主机名是无法建立网络连接的,需要通过解析的过程,在主机名与 IP 地址之间建立了映射关系后,才可以使用主机名间接地通过 IP 地址建立网络连接。

主机名与 IP 地址之间的映射关系,在小型网络中多使用 HOSTS 文件完成。后来,随着网络规模的增大,为了满足不同组织的要求,实现一个可伸缩、可自定义的命名方案,国际

互联网络信息中心(Internet Network Information Center,InterNIC)制定了一套称为域名系统(DNS)的分层名字解析方案,当 DNS 用户提出 IP 地址查询请求时,就可以由 DNS 服务器中的数据库提供所需的数据。

通过本实验,在了解 DNS 工作原理和过程的基础上,掌握 Windows Server 2016 下 DNS 的安装和配置方法。

2. 实验原理

DNS 的基础是 HOSTS,DNS 最初的设计目标是"用具有层次名字空间、分布式管理、扩展的数据类型、无限制的数据库容量和具有可接受性能的轻型、快捷、分布的数据库取代笨重的集中管理的 HOSTS 文件系统"。

DNS 是一组协议和服务,它允许用户在查找网络资源时使用层次化的对用户友好的名字取代 IP 地址。当 DNS 客户端向 DNS 服务器发出 IP 地址的查询请求时,DNS 服务器可以从其数据库内寻找所需要的 IP 地址给 DNS 客户端。这种由 DNS 服务器在其数据库中找出客户端 IP 地址的过程叫作"主机名称解析"。该系统已广泛地应用到 Internet 和 Intranet 中,如果在 Internet 或 Intranet 中使用 Web 浏览器、FTP 或 Telnet 等基于 TCP/IP 的应用程序,就需要使用 DNS 的功能。

简单地讲,DNS 协议的最基本的功能是在主机名与对应的 IP 地址之间建立映射关系。例如,新浪网站的 IP 地址是 202.106.184.200,几乎所有浏览该网站的用户都是使用 www.sina.com.cn,而并非使用 IP 地址访问。

DNS 的工作任务是在计算机主机名与 IP 地址之间进行映射。DNS 工作于 OSI 参考模型的应用层,使用 TCP 和用户数据报协议(User Datagram Protocol,UDP)作为传输协议。DNS 模型相当简单:客户端向 DNS 服务器提出访问请求(如 www.sina.com.cn),DNS 服务器在收到客户端的请求后在数据库中查找相对的 IP 地址(202.106.184.200),并作出反应。如果该 DNS 服务器无法提供对应的 IP 地址(如数据库中没有该客户端主机名对应的 IP 地址),它就转给下一个它认为更好的 DNS 服务器去处理。

整个 DNS 的结构是一个类似如图 5-1 所示的分层式树状结构,该结构称为 DNS 域名空间。其中,位于树状结构最上层的是 DNS 域名空间的根(Root),Root 一般用点号(.)表示。目前 Root 由一些国际大公司(如 InterNIC)管理,由多台计算机组成的 DNS 群负责全球范围内的 DNS 解析。

紧靠在 Root 下面的是顶级域(Top-Level Domain),顶级域主要用于对 DNS 的分类管理,如 com 主要用于商业机构、edu 主要用于教育和学术研究机构、gov 主要用于政府单位、mil 主要用于国防军事单位、net 主要用于网络服务机构、org 主要用于社会团体等非营利机构等。

顶级域下面是二级域,用户一般向 ISP 申请到的就是二级域,如本例中的 wldhj.com。对于单位用户,如果网络不需要接入 Internet,则可以自定义二级域。www、mail 等网络服务一般以主机记录的方式包含在域名当中,如图 5-1 中的主机 www 和 mail 是位于 wldhj.com 中的主机记录,即 www 提供 Web 服务,而 mail 提供邮件服务,其完全限定域名(Fully Qualified Domain Name,FQDN)应该分别为 www.wldhj.com 和 mail.wldhj.com。有关主机(Host)记录的创建和使用方法将在本章的实验 3 中进行介绍。

早期的 DNS 数据文件是一个平面结构的文本文件,很容易被编辑(如 WINS 和

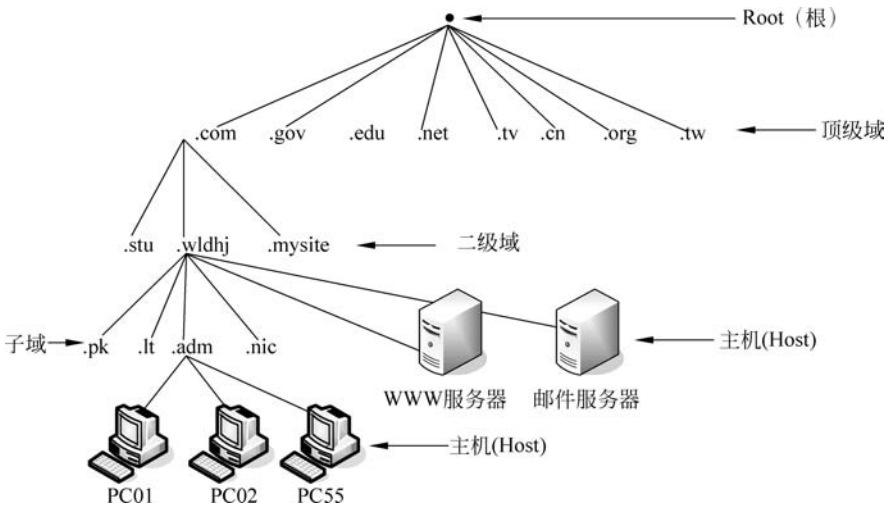

图 5-1　DNS 的分层式树状结构

HOSTS)，但不能被复制。这既不便于安全管理，也无法用其他代理方式来控制。使用活动目录(Active Directory，AD)能够克服这些局限。活动目录会将所有 DNS 区域的数据保存在自身数据库中，这样不但增加了安全性，而且便于复制。

活动目录是 Windows 服务器系列操作系统使用的目录服务，用于存放用户账户、计算机账户等网络对象的信息，可以使管理员和用户十分方便地查找和使用有关信息。由于活动目录也是通过名称空间管理信息，这与 DNS 域名的作用是相同的，而且两者具有相同的层次结构和存储区域，所以在 Windows 服务器系列操作系统中，活动目录与 DNS 进行了有机整合。一方面，活动目录的域名空间采用了 DNS 架构，域名的命名方式与 DNS 格式相同；另一方面，DNS 可以利用活动目录的同步机制，提供 DNS 数据在域内的一致性和容错能力。

在活动目录中，使用对象的概念表示用户、计算机等需要管理的数据，并通过对象的属性描述对象的特征，对象就是属性的集合。容器这个概念一般对应现实中的组织单位，用来包含各种对象，容器本身也是对象。对象与组织单位等组合在一起，构成了活动目录的层次结构。这种层次结构中的各种对象，可以用 DNS 中的域名进行命名和检索。存在层次关系的多个域构成域树，每棵域树都有自己唯一的名称空间，域树内的所有域共享一个活动目录的域服务；一棵或多棵域树组成森林。

活动目录使用目录数据库存储各种对象的数据，每个域只在目录数据库中存储域本身的数据，但由于域树内的所有域共享一个活动目录域服务(Domain Service，DS)，所以需要使用全局编录建立域树内所有域共享的 AD DS 数据库。每个域的目录数据存储在域控制器内，一个域内可以有多台域控制器，每台域控制器各自存储着一份相同的 AD DS 数据库，这份数据库在所有域控制器内都是同步的。

3. 实验内容和要求

(1) 了解 HOSTS、WINS 和 DNS 的工作特点。

(2) 了解 DNS 的分层结构。

(3) 熟悉 DNS 的工作原理。

(4) 了解 Windows Server 2016 中 DNS 的特点。

(5) 掌握 Windows Server 2016 中 DNS 的安装和配置方法。

5.1.2 实验规划

1. 实验设备

(1) VMware Workstation 软件虚拟平台。

(2) 虚拟服务器(1 台,名称为 Server1,安装 Windows Server 2016 操作系统)。

(3) 测试用 PC(2 台,安装 Windows 10 操作系统)。

(4) 实体计算机(1 台,安装 VMware Workstation 软件)。

2. 实验拓扑

实验所使用的网络拓扑如图 5-2 所示。其中,本域的域名服务器为 Server1,域名为 wldhj.com,IP 地址为 192.168.1.10; PC1 的 IP 地址为 192.168.1.11; PC2 的 IP 地址为 192.168.1.12。

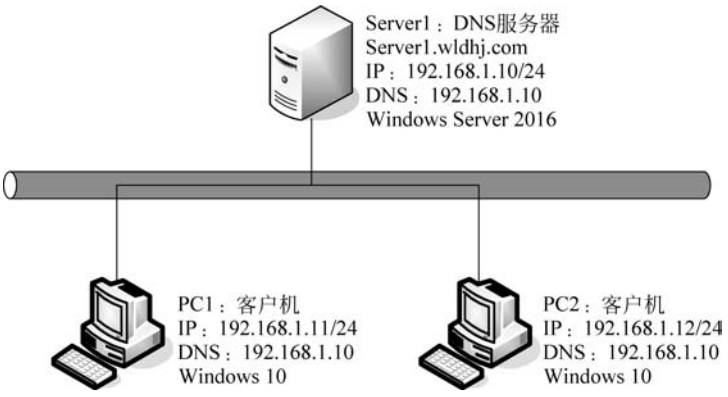

图 5-2 DNS 服务器规划

5.1.3 实验步骤

当在网络中创建第 1 个域控制器时,同时也创建了第 1 个域、第 1 个林、第 1 个站点。下面以图 5-2 为例,详细介绍第 1 台域控制器的创建方法。

1. 构建虚拟网络环境

(1) 分别为 Server1 和 PC1、PC2 安装 Windows Server 2016 和 Windows 10 操作系统。在准备好以上操作系统的 ISO 文件以及相应的 Windows 产品密钥之后,单击 VMware Workstation 的主页上的“创建新的虚拟机”选项,如图 5-3 所示。随后采用一系列的默认设置,并选择所需要安装的 ISO 文件后,就可进入安装流程,安装过程与通常情况类似,不再赘述。注意,要确保安装的操作系统已经激活。

图 5-3　使用 VMware Workstation 创建新的虚拟机

(2) 在仅主机模式(Host Only)下构建局域网。由于只需要创建一个内部互通的网络环境,所以在 Host Only 模式下构建局域网。

首先,在 VMware Workstation 菜单栏的“编辑”菜单中选择“虚拟网络编辑器”,在弹出的对话框中选择 VMnet1,这代表 Host Only 模式下的虚拟交换机,取消勾选默认选中的“使用本地 DHCP 服务将 IP 地址分配给虚拟机”,便于后续手动配置 IP 地址,如图 5-4 所示。

图 5-4　Host Only 模式的配置

需要注意的是,上述配置需要具备管理员特权才能修改网络配置,此时,上述对话框右下角会出现“更改配置”按钮,单击此按钮即可进行配置。

然后,在相应虚拟机的页面上选择“编辑虚拟机设置”,将虚拟机的网络适配器属性“网络连接”设置为 Host Only 模式,如图 5-5 所示。

图 5-5 将虚拟机的“网络连接”设置为 Host Only 模式

进入每台虚拟机操作系统中的控制面板,选择“网络和 Internet”→“网络和共享中心”→“更改适配器设置”,右击 Ethernet0,在弹出的快捷菜单中选择“属性”,按图 5-2 的网络参数对每台虚拟机进行网络配置。图 5-6 所示为 Server1 的网络参数配置情况。

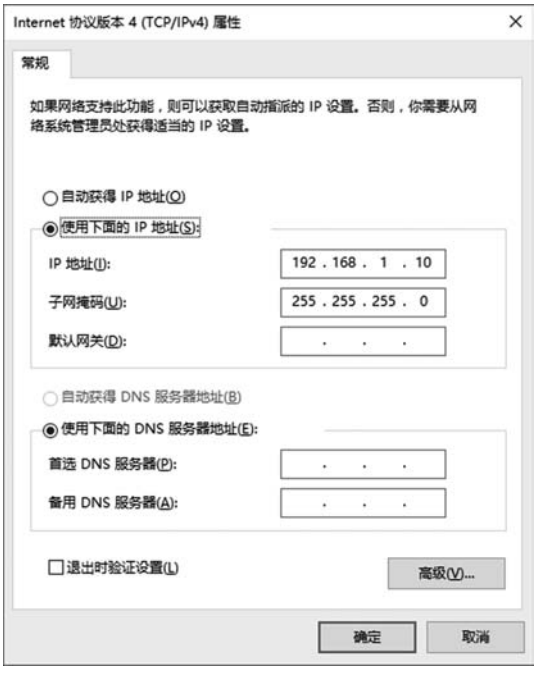

图 5-6 Server1 的网络参数配置

PC1 和 PC2 的网络参数配置类似。

（3）联通性测试。在每台虚拟机中运行 ping 命令，互相测试联通性。需要注意的是，先要保证每台虚拟机都启用文件和打印机共享，这可以在“网络设置”→“更改高级共享设置”中实现，如图 5-7 所示。

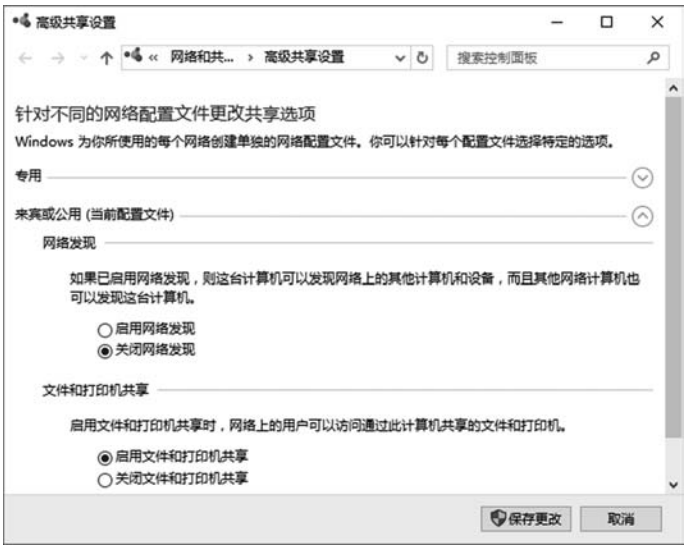

图 5-7　启用文件和打印机共享

设置完成后，就可以相互 ping 通了。

2. 通过建立网络中第 1 台域控制器的方式安装 DNS 服务器

（1）配置服务器的完整计算机名称和 DNS 指向。由于本实验使用的域名是 wldhj.com，那么在设置服务器的计算机名称之后，其完整计算机名称就是 Server1. wldhj. com。设置方法为：单击“开始”菜单按钮，选择“管理工具”→“服务器管理器”，进入服务器管理器。单击界面左侧列表中的“本地服务器”，选择“计算机名”右侧的计算机名称，单击“更改”按钮，弹出“计算机名/域更改”对话框。在该对话框中单击“其他…”按钮，在弹出对话框中的“此计算机的主 DNS 后缀”文本框中输入 wldhj. com。单击“确定”按钮，将计算机名改为 Server1，确定后按提示重启计算机，如图 5-8 所示。

然后，在 Server1 的网络参数配置中，把首选 DNS 服务器的 IP 地址配置为自己的 IP 地址，使 Server1 中的其他应用程序可通过自己这台 DNS 服务器查询 IP 地址，如图 5-9 所示。

（2）通过添加服务器角色的方式，将 Server1 升级为网络中第 1 台域控制器的同时安装 DNS 服务器。

首先，进入服务器管理器，单击界面左侧列表中的“仪表板”，在右侧选择“添加角色和功能”，如图 5-10 所示。

然后，在“添加角色和功能向导”对话框中，“开始之前”“安装类型”“服务器选择”步骤都默认单击“下一步”按钮后，勾选“服务器角色”步骤中的“Active Directory 域服务”，然后在弹出的对话框中单击“添加功能”按钮，如图 5-11 所示，随后在“功能”“确认”步骤中均默认单击“下一步”按钮，直到“确认”步骤中单击“安装”按钮。

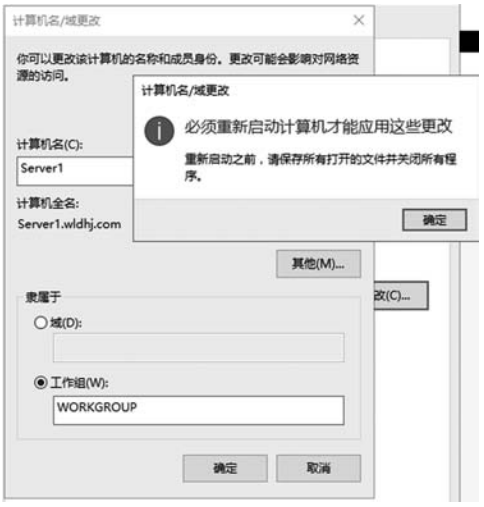

图 5-8　配置服务器的完整计算机名称

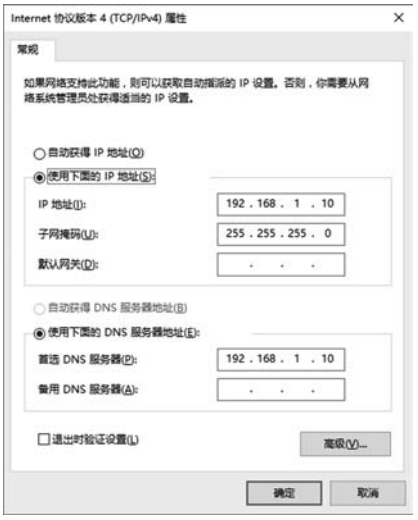

图 5-9　将 Server1 的 DNS 指向自身

图 5-10　选择“添加角色和功能”

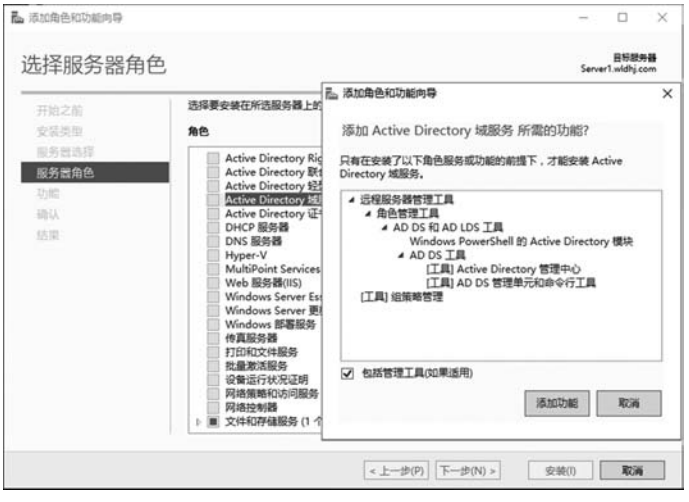

图 5-11　安装 Active Directory 域服务

在完成安装后的界面上，选择“将此服务器提升为域控制器”，如图 5-12 所示。

图 5-12　将服务器提升为域控制器

接下来，在“部署配置”页面中选择“添加新林”，并设置根域名为 wldhj.com，如图 5-13 所示。

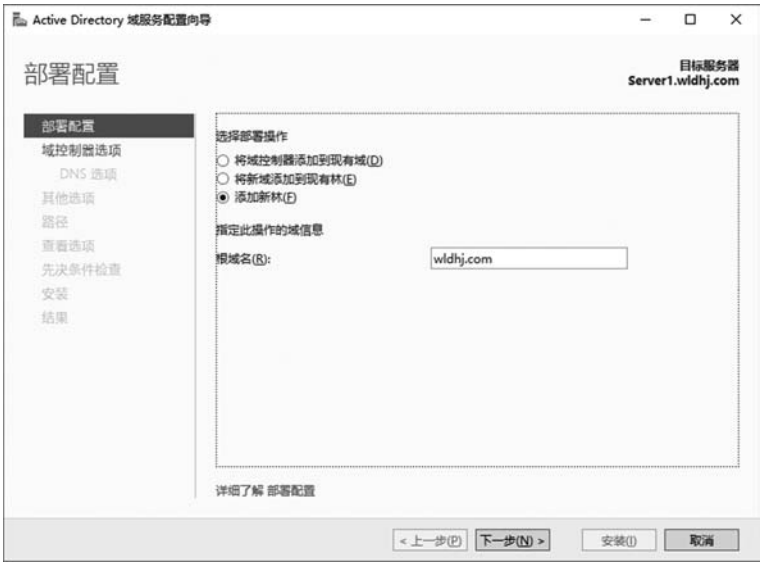

图 5-13　添加新林，并设置根域名

然后，在“域控制器选项”页面中设置“输入目录服务还原模式(DSRM)密码”，如图 5-14 所示。需要注意的是，密码必须至少 7 个字符，至少包含 A～Z、a～z、0～9、非字母字符等 4 组字符中的 3 组。

忽略“DNS 选项”中出现的警告(当前不会有影响)并单击“下一步”按钮，在“其他选项”中会自动设置一个 NetBIOS 域名(当前应该为 wldhj，有时可能会等待一会儿才会出现)，然

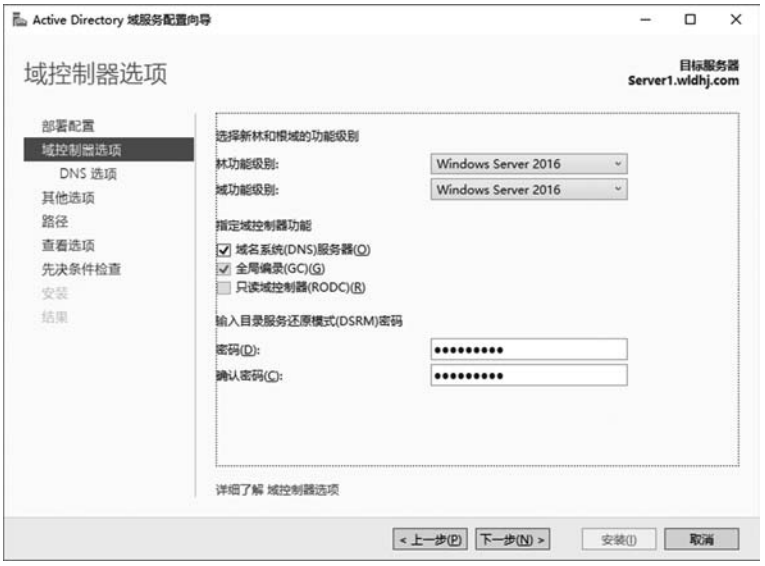

图 5-14　设置“输入目录服务还原模式(DSRM)密码”

后单击“下一步”按钮设置数据库文件夹(用来存储活动目录数据库)、日志文件夹(用于存储活动目录的变化日志)、SYSVOL 文件夹(用于存储域共享文件)的路径。若计算机内有多块硬盘,可将数据库与日志文件夹分别设置到不同硬盘上,在保证工作效率的同时,提高活动目录数据库的修复能力。这里使用默认位置,如图 5-15 所示。

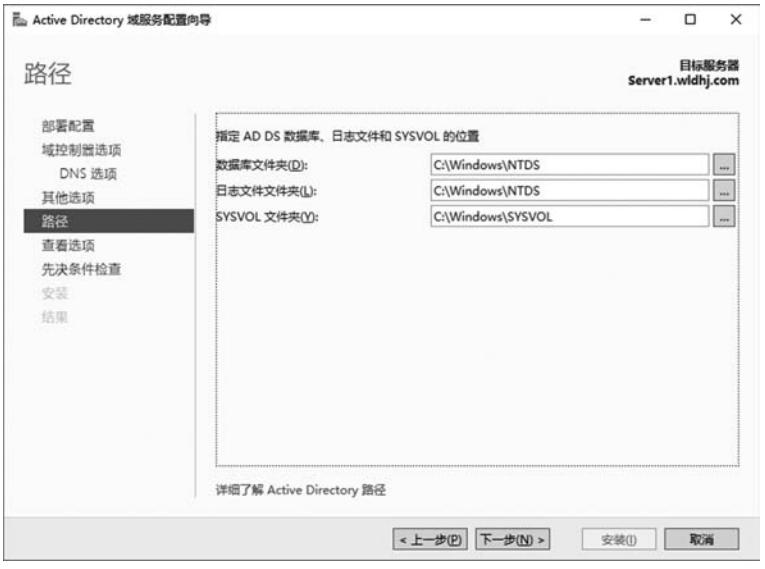

图 5-15　配置相关路径

单击“下一步”按钮,就可在“查看选项”中检查前面的配置情况,然后进入“先决条件检查”。在此检查过程中,最容易出现的问题是本地 administrator 账户密码不符合要求,这是因为相应账户的密码没有设置,或者设置不符合要求,这时需要为本地 administrator 账户设置或修改密码,然后单击“重新运行先决条件检查”再次执行检查即可,如图 5-16 所示,然

后单击“安装”按钮。

图 5-16　先决条件检查

安装完成后，就会自动重启计算机，此后活动目录和 DNS 就会开始工作。

5.1.4　结果验证

在安装和配置完 Windows Server 2016 域服务器后，需要对域服务器的各项设置和运行情况进行检查。

1. 检查 DNS 服务器内的记录

在 Windows Server 2016 上安装了活动目录后，域控制器会将自己登记到 DNS 服务器内，这样其他的计算机就可以通过 DNS 服务器查找这个域控制器。所以，当 Windows Server 2016 升级为域控制器后，首先要检查 DNS 服务器内是否已经有这些域控制器的数据。

单击“开始”菜单→“Windows 管理工具”→DNS，打开如图 5-17 所示的“DNS 管理器”对话框。

其中，在“正向查找区域”下方应该有一个已经创建的名为 wldhj.com 的区域，它可以让 Windows Server 2016 域 wldhj.com 中的成员将其数据登记到本区域中。右侧列表框显示了域控制器 Server1.wldhj.com 已经将其主机名称(Server1)与 IP 地址(192.168.1.10)登记到 DNS 服务器中。

另外，图 5-17 右侧列表框中还有_tcp、_udp 等记录，这说明域控制器已经将其与活动目录有关的数据登记到 DNS 服务器内。例如，单击_tcp 记录，将打开如图 5-18 所示的对话框。其中，数据类型为 SRV 的_ldap 记录表示 Server1.wldhj.com 已将其扮演域控制器角色的信息登记到 DNS 服务器中。从_gc 记录可以看出，“全局编录”的角色由 Server1.wldhj.com 来扮演。

图 5-17 DNS 中已经登记的域控制器信息

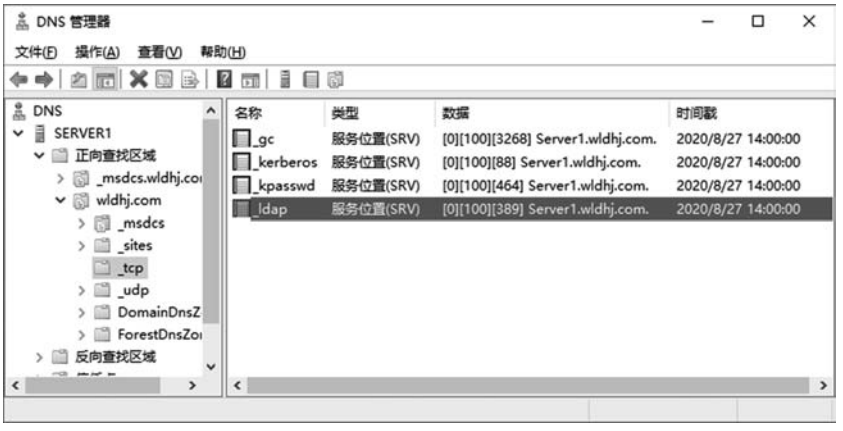

图 5-18 查看_tcp 记录的相关信息

2. 检查 DNS 解析功能

通过 DNS 进行域名解析时,在 DNS 客户端必须指定 DNS 服务器的 IP 地址,以便告诉 DNS 客户端在何处去完成域名解析过程。下面以 Windows 10 客户端为例介绍其设置方法。

(1) 在 PC1 或 PC2 进入“控制面板”,单击“网络和 Internet”→“网络连接”,打开如图 5-19 所示窗口。

(2) 右击 Ethernet0 图标,在弹出的快捷菜单中选择“属性”,打开“本地连接属性”对话框。

(3) 在对话框“此连接使用下列选定的组件”列表框中选择已安装的“Internet 协议(TCP/IP)”选项,然后单击“属性”按钮,出现如图 5-20 所示的对话框。在“首选 DNS 服务器”文本框中输入 DNS 服务器的 IP 地址,如果网络中还有其他的 DNS 服务器,在“备用 DNS 服务器”文本框中输入这台备用 DNS 服务器的 IP 地址。

(4) 通过以上的设置后,DNS 客户端会依次向 DNS 服务器进行查询。这时可以在命令行窗口中 ping 服务器的完全限定域名 FQDN(如 Server1. wldhj. com),如果 DNS 服务器和客户端的配置正确,将出现如图 5-21 所示的结果。

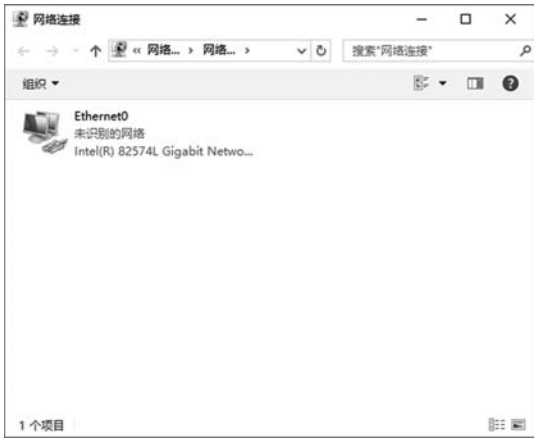

图 5-19　“网络连接”窗口

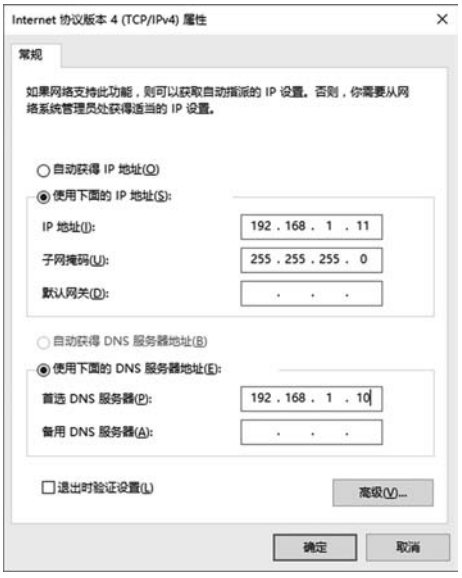

图 5-20　设置“首选 DNS 服务器”

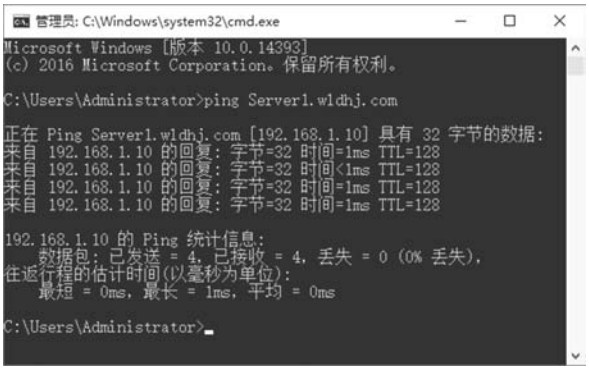

图 5-21　ping Server1. wldhj. com 的返回结果

5.2　实验 2　配置基于活动目录的其他 DNS 服务器


视频讲解

在本章实验 1 中，介绍了网络中第 1 台 DNS 服务器的安装和配置方法。出于安全考虑，对于实际运行的 DNS 服务器，一般需要提供至少一台备份 DNS 服务器，当一台 DNS 服务器出现故障时，其他的 DNS 服务器可以继续提供域名解析服务。在 Windows Server 2016 中，为同一域名创建的多台 DNS 服务器之间没有主次之分，所有 DNS 服务器中的数据都是同步更新的。本实验介绍第 2 台域名服务器的安装和配置方法。

5.2.1　实验概述

基于活动目录，一个域内可以有多台域控制器，共同分担审核用户登录身份（就是验证

账户和密码)的负担,这可以提高登录效率,而且还能在某台域控制器发生故障时,继续由其他正常的域控制器为客户端提供 DNS 域名解析等服务。

1. 实验目的

在掌握了网络中第 1 台基于活动目录的域名服务器安装方法的基础上,以第 2 台域名服务器的安装为例,学习其他域名服务器的安装和配置方法。通过本实验,在掌握多域名服务器具体组建方法的同时,熟悉网络域名系统的安全配置措施和策略。

2. 实验原理

活动目录是 Windows Server 系列操作系统使用的目录服务,它存放着有关网络对象的数据,使管理员和用户可以十分方便地进行查找和使用域中的网络对象的信息。活动目录使用 DNS,两者具有相同的层次结构和存储区域。

早期的 DNS 数据文件是一个平面结构的文本文件,很容易被编辑(如 WINS 和 HOSTS),但它却不能被复制。这既不便于安全管理,也无法用其他代理方式来控制。在创建了活动目录后,所有这些局限将不会存在。活动目录会将所有的 DNS 区域的数据保存在自身的数据库中,这样不但增加了安全性,而且便于复制。

当网络中同时安装和配置了多台域名服务器时,各域名服务器之间会通过活动目录实现 DNS 数据同步,这样就保证了当其中一台域名服务器出现故障时不影响域名的解析服务。

3. 实验内容和要求

(1) 了解多 DNS 服务器的工作特点。

(2) 了解 Windows Server 2016 活动目录中 DNS 数据库的同步方法。

(3) 在安装和配置第 1 台 DNS 服务器的基础上掌握其他 DNS 服务器的安装和配置方法。

5.2.2 实验规划

1. 实验设备

(1) VMware Workstation 软件虚拟平台。

(2) 虚拟服务器(2 台,名称分别为 Server1 和 Server2,安装 Windows Server 2016 操作系统)。

(3) 测试用 PC(2 台,安装 Windows 10 操作系统)。

(4) 实体计算机(1 台,安装 VMware Workstation 软件)。

2. 实验拓扑

实验所使用的网络拓扑是在实验 1 的基础上,添加一台虚拟服务器,如图 5-22 所示。其中,本域名服务器 Server1 的域名为 wldhj.com,IP 地址为 192.168.1.10,Server2 的 IP 地址为 192.168.1.20,PC1 的 IP 地址为 192.168.1.11,PC2 的 IP 地址为 192.168.1.12。

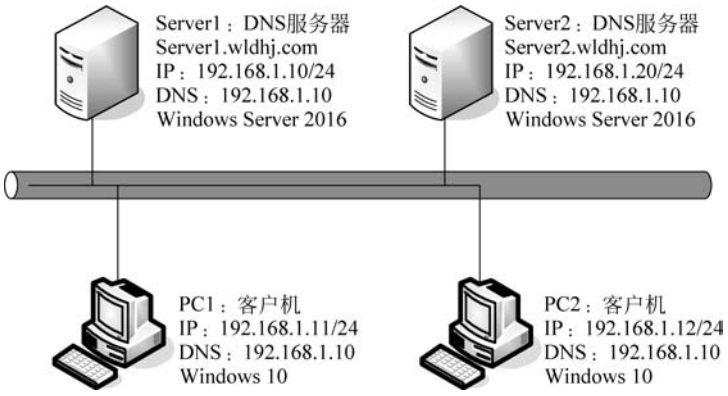

图 5-22　多 DNS 服务器的实验网络拓扑

5.2.3　实验步骤

下面首先将一台运行 Windows Server 2016 的计算机(Server2)加入实验 1 的网络拓扑中,然后再将其升级为域控制器,并加到现有域中。

1. 新建一台 Windows Server 2016 虚拟机并将其加入网络拓扑中

创建新虚拟机,并配置其网络参数,并加入现有网络中,其过程与本章实验 1 相同,不再赘述。

2. 将新加入的虚拟机升级为域控制器并加入现有域

(1) 配置服务器的完整计算机名称和 DNS 指向。由于本实验使用的域名是 wldhj.com,那么在设置服务器的计算机名称之后,其完整计算机名称就是 Server2. wldhj. com。设置方法与本章实验 1 相同(只是将计算机名改为 Server2),然后,将此虚拟机的网络设置的 DNS 也设置为 192. 168. 1. 10。这部分与实验 1 的内容一样。

(2) 通过添加服务器角色的方式,将 Server2 升级为网络中域控制器,同时也就安装了 DNS 服务器。

首先,进入服务器管理器,单击“仪表板”→“添加角色和功能”。然后,在“添加角色和功能向导”对话框中,“开始之前”“安装类型”“服务器选择”步骤都默认单击“下一步”按钮,在“服务器角色”步骤中勾选“Active Directory 域服务”,然后在弹出的对话框中单击“添加功能”按钮。随后在“功能”“确认”步骤中均默认单击“下一步”按钮,直到“确认”步骤中单击“安装”按钮。在完成安装后的界面上,选择“将此服务器提升为域控制器”。

接下来,需要将当前的域控制器添加到现有域,这一步是与本章实验 1 中不同的地方,如图 5-23 所示。在选择“将域控制器添加到现有域”后,填写为本章实验 1 中建立的域 wldhj. com。此处也可单击“选择”按钮,以选择已有的域,如图 5-23 所示。但这要保证前一台 DNS 服务器正常工作,否则就会出现无法连接到相应域的 Active Directory 控制器的问题。

确定后,单击“更改”按钮,输入实验 1 中的建立的域控制器 Server1 的管理员账户和密码,如图 5-24 所示。

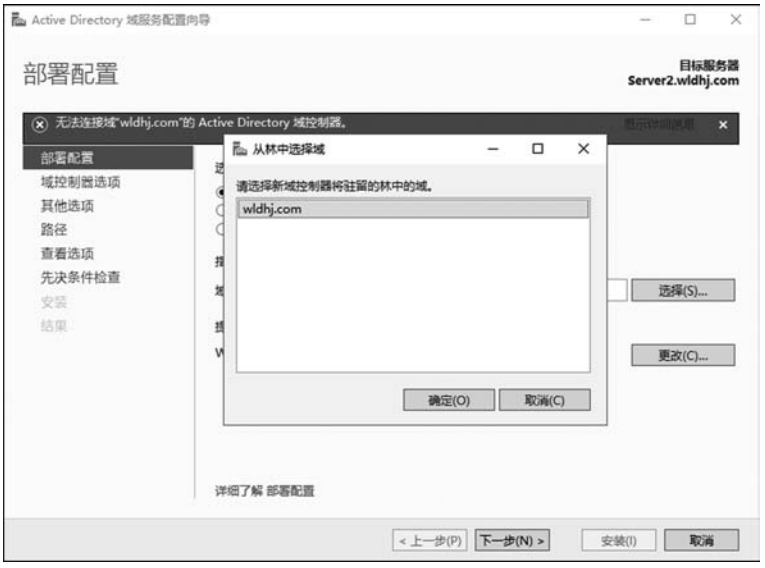

图 5-23　选择现有域

图 5-24　将域控制器添加到现有域

然后,在"域控制器选项"中设置目录服务还原模式(DSRM)密码,如图 5-25 所示。需要注意的是,密码必须至少有 7 个字符,至少包含 A～Z、a～z、0～9、非字母字符等 4 组字符中的 3 组。

忽略"DNS 选项"中出现的警告(当前不会有影响)后,在"其他选项"中会要求选择复制 Active Directory 的域控制器,这里可以选择"任何域控制器",也可以选择 Server1. wldhj. com,如图 5-26 所示。

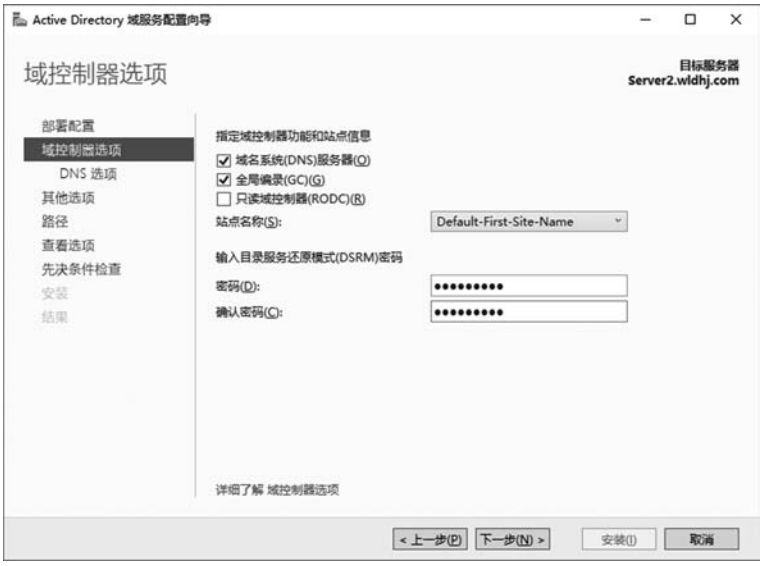

图 5-25　设置目录服务还原模式(DSRM)密码

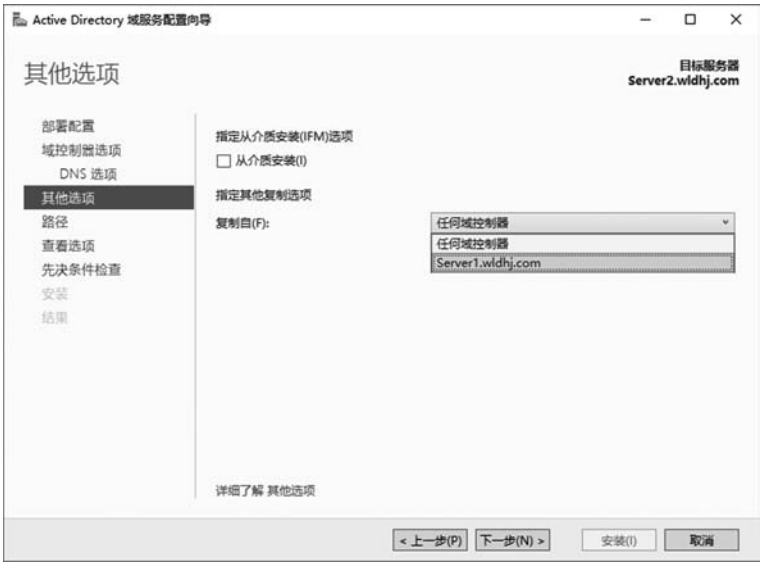

图 5-26　选择复制 Active Directory 的域控制器

然后单击“下一步”按钮，设置数据库文件夹、日志文件夹、SYSVOL 文件夹的路径。若计算机内有多块硬盘，可将数据库与日志文件夹分别设置到不同硬盘上，如图 5-27 所示。

在“查看选项”中，可检查前面的配置情况，然后进入“先决条件检查”，若顺利通过检查，如图 5-28 所示，就可单击“安装”按钮。系统开始安装 Active Directory，并与第 1 台域控制器进行数据同步。

安装完成后，必须重新启动计算机。当重新启动计算机后，该服务器将成为已有域(wldhj.com)中的一员。而且，Windows Server 2016 域控制器没有主域和备份域之分，凡加入同一域的计算机，不管加入顺序的先后，在身份和功能上都是平等的。

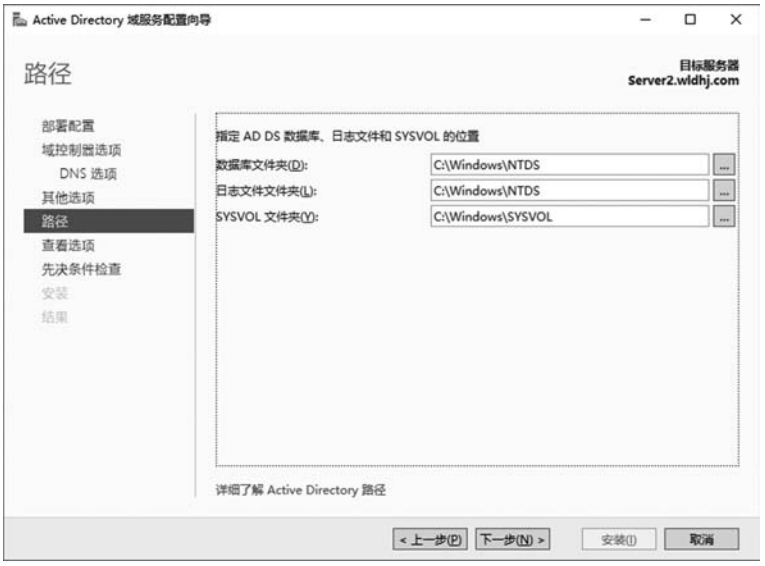

图 5-27 配置相关路径

图 5-28 通过"先决条件检查"

5.2.4 结果验证

首先，检查 Server2 的 DNS 服务器内的记录。单击"开始"菜单→"Windows 管理工具"→DNS，进入 DNS 管理器，如图 5-29 所示。

其中，在"正向查找区域"下应该有一个已经创建的名为 wldhj.com 的区域，它可以让 Windows Server 2016 域 wldhj.com 中的成员将其数据登记到本区域中。右侧列表框显示域控制器 Server1.wldhj.com 已经将其主机名称(Server1)与 IP 地址(192.168.1.10)登记

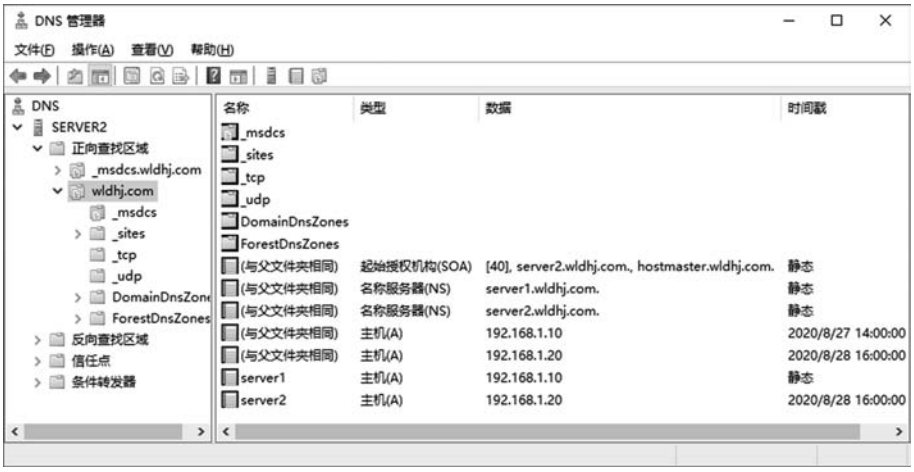

图 5-29　DNS 中已经登记的域控制器信息

到 DNS 服务器中。同时，域控制器 Server2. wldhj. com 也已经将其主机名称(Server2)与 IP 地址(192. 168. 1. 20)登记到 DNS 服务器中。

然后，检查 Server1 的 DNS 服务器内的记录，也是如此。

由于网络中已同时具有两台 DNS 服务器，这时可在客户端 PC 上将“首选 DNS 服务器”设置为第 1 台 DNS 服务器的 IP 地址 192. 168. 1. 10，将“备用 DNS 服务器”设置为第 2 台 DNS 服务器的 IP 地址 192. 168. 1. 20。这样，当其中任何一台 DNS 服务器出现故障(可人为断开网线进行测试)时，网络同样能够提供域名解析。具体的验证方法在随后的实验中将进一步证实。

5.3　实验 3　配置 DNS 服务器的反向查找区域


视频讲解

DNS 是计算机网络中解决主机名称与 IP 地址之间映射的一种方式。在本章前面的实验中，当在 Windows Server 2016 中安装了 DNS 后，系统会自动创建“正向查找”，即通过 DNS 域名查找 IP 地址。在实际应用中，还需要通过 IP 地址查找 DNS 域名，此方式称为反向查找。本实验将介绍反向查找的实现方法。

5.3.1　实验概述

通常使用的 DNS 解析是一种正向查找方式，即通过 DNS 域名查找 IP 地址。而反向查找(Reverse Lookup)可以让 DNS 客户端利用 IP 地址查找主机名称。例如，当用户已经知道一个 IP 地址时，可以通过反向查找发现该地址对应的主机名称。

1. 实验目的

通过前面的实验，已经掌握了 DNS 的工作原理和安装方法。在此基础上，通过本实验，将了解 DNS 正向查找和反向查找的功能，并掌握反向查找的配置方法。

2. 实验原理

实验 1 中,在将 Windows Server 2016 升级为域控制器并安装了 DNS(wldhj.com)后,可以单击“开始”菜单→“Windows 管理工具”→DNS,在弹出的如图 5-30 所示的对话框中,在“正向查找区域”下有一项名为 wldhj.com 的区域,在该区域中显示了 DNS 服务器的名称和对应的 IP 地址等信息。

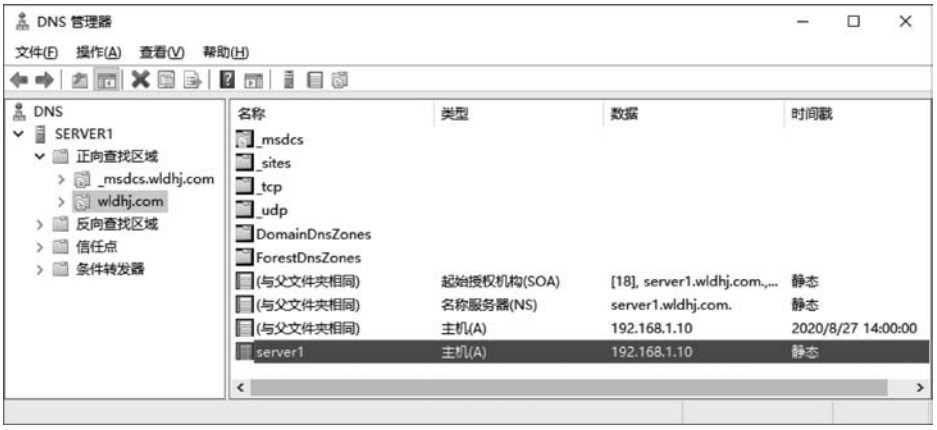

图 5-30 正向查找区域与 DNS 域名之间的对应关系

需要说明的是,一个 DNS“区域”对应一个 DNS 域名,所以可以通过在 DNS 中创建新的“区域”记录添加新的 DNS 域名,如 etongtv.net 等。这也是一台 DNS 服务器可以同时提供多个 DNS 域名解析的一个重要原因。

在安装和配置了 DNS 域名后,在默认情况下系统不会自动设置反向查找功能。为了网络管理的需要,可以通过设置反向查找,实现通过 IP 地址查找 DNS 域名的功能。

3. 实验内容和要求

(1) 深入掌握 DNS 的工作原理。

(2) 掌握正向查找和反向查找的应用功能。

(3) 掌握反向查找的配置方法。

5.3.2 实验规划

1. 实验设备

(1) VMware Workstation 软件虚拟平台。

(2) 虚拟服务器(2 台,名称分别为 Server1 和 Server2,安装 Windows Server 2016 操作系统)。

(3) 测试用 PC(2 台,安装 Windows 10 操作系统)。

(4) 实体计算机(1 台,安装 VMware Workstation 软件)。

2. 实验拓扑

本实验的 DNS 服务器域名为 wldhj.com。如果是一台 DNS 服务器(见本章实验 1),

Server1 的 IP 地址为 192.168.1.10；如果是两台 DNS 服务器(见本章实验 2)，另一台 DNS 服务器 Server2 的 IP 地址为 192.168.1.20，网络拓扑分别与实验 1 和实验 2 中一样。

需要说明的是，在同时具有两台 DNS 服务器的网络中，由于 DNS 是建立在 Windows Server 2016 活动目录数据库中，所以当其中任意一台 DNS 服务器进行了相关设置后，其结果都会被系统自动同步到另一台 DNS 服务器上。所以，具体的配置操作过程与 DNS 服务器的数目没有直接的关系。

5.3.3　实验步骤

(1) 在任意一台 DNS 服务器上，单击“开始”菜单→“Windows 管理工具”→DNS，打开“DNS 管理器”对话框。选择“反向查找区域”，显示如图 5-31 所示的信息，说明在安装 DNS 服务器后，默认情况下不会设置反向查找功能。

图 5-31　设置反向查找功能

(2) 右击“反向查找区域”，在弹出的快捷菜单中选择“新建区域”，弹出“欢迎使用新建区域向导”对话框。单击“下一步”按钮，弹出如图 5-32 所示的对话框。各选项的说明如下。

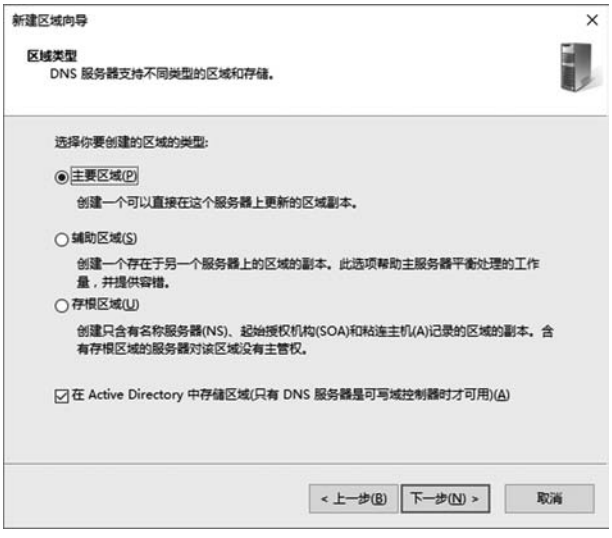

图 5-32　选择反向区域的类型

- 主要区域：用于创建一个直接在本地计算机上运行和更新的区域文件。
- 辅助区域：将反向查找区域文件存储在另一台计算机上，主要用于 DNS 反向查找的容错和多台服务器的负载均衡。
- 存根区域：在功能上与“主要区域”类似，但只包含少数的记录，如 NS(Name Server)、SOA(Start of Authority)等。

在具体实现中，如没有特殊要求，则一般选择“主要区域”。另外，由于区域记录会被存储在区域文件中，但是 DNS 服务器本身是域控制器(多数情况是这样)，即在这台 DNS 服务器上安装了活动目录。这时，为了将 DNS 记录与活动目录进行有机整合，可以勾选“在 Active Directory 中存储区域”，这样区域记录就会被存储到活动目录数据库中。

(3) 单击“下一步”按钮，弹出如图 5-33 所示的对话框。由于本实验在上一步中选择了“在 Active Directory 中存储区域”，即将 DNS 记录与活动目录进行整合，所以需要选择“至此域中的所有域控制器(为了与 Windows 2000 兼容)：wldhj.com”。

图 5-33 选择复制区域数据的方式

(4) 单击“下一步”按钮，选择“IPv4 反向查找区域”，再单击“下一步”按钮，在如图 5-34 所示对话框的“网络 ID”文本框中输入反向查找区域 IP 地址的网络 ID。

其中，由于该 DNS 服务器的 IP 地址为 192.168.1.10，子网掩码为 255.255.255.0，所以网络 ID 应为 192.168.1。这时，系统会自动在“反向查找区域名称”下面显示反向查找区域名称 1.168.192.in-addr.arpa。当然，也可以在选择“反向查找区域名称”选项后，直接在“反向查找区域名称”文本框中输入 1.168.192.in-addr.arpa。不过，从设置的方便性和可靠性考虑，建议使用前一种方法。

(5) 单击“下一步”按钮，弹出如图 5-35 所示的对话框。由于本实验将 DNS 记录集成到活动目录中，所以系统会自动选择“只允许安全的动态更新”。

(6) 单击“下一步”按钮，会显示前面的设置信息。如果设置无误，单击“确定”按钮，完成反向查找区域的设置。

图 5-34　设置反向查找区域的网络 ID

图 5-35　选择动态更新方式

5.3.4　结果验证

单击“开始”菜单→“Windows 管理工具”→DNS，在弹出的如图 5-36 所示的对话框中，在“反向查找区域”下有一项名为 1.168.192.in-addr.arpa 的区域，在该区域中显示了 DNS 服务器的名称和对应的 IP 地址等信息。

进一步，如果本实验采用本章实验 2 的配置，此时，在 Server2 上进入 DNS 管理器，如图 5-37 所示，在刷新后，“反向查找区域”下有一项名为 1.168.192.in-addr.arpa 的区域，可以看出，Server2 已经把反向查找区域同步过来了。

图 5-36 显示已设置的反向查找区域信息

图 5-37 在 Server2 中同步了反向查找区域信息

在设置了正向查找区域和反向查找区域后,在 DNS 客户端进入命令提示符窗口,输入 nslookup 命令,将显示 DNS 服务器默认的完整主机名称和对应的 IP 地址。本实验中的 DNS 服务器域名为 Server1. wldhj. com,对应的 IP 地址为 192. 168. 1. 10。这时输入 wldhj. com 将显示通过正向查找所得到的 DNS 域名、IP 地址等信息;如果输入 DNS 服务器的 IP 地址,则会显示该 IP 地址对应的 DNS 域名等信息。测试过程和结果如图 5-38 所示。

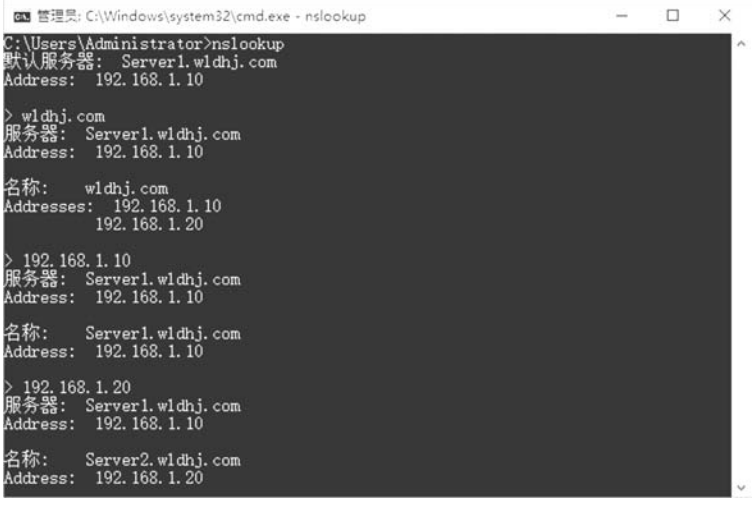

图 5-38 利用 nslookup 命令测试 DNS 服务器

需要注意的是，如果想要执行 nslookup 命令后默认服务器不是 Unknown，这需要回到 DNS 服务器的正向查找区域中，找到此服务器对应的主机记录，在其属性中勾选“更新相关的指针(PTR)记录”才能实现。

5.4　实验 4　使 DNS 提供 WWW、Mail、FTP 等解析服务


视频讲解

不管是 Intranet(企业内部网络)还是 Internet，在访问相关的资源时一般使用 HTTP 或 FTP 方式。例如，通过 http://www.wldhj.com 访问 WWW 服务，通过 ftp://ftp.wldhj.com 访问 FTP 网站，通过 http://mail.wldhj.com 访问邮件服务器等。本实验将在已创建的 DNS 域名服务器上，介绍针对各种具体应用的域名的 DNS 解析实现方法。

5.4.1　实验概述

在本章前面的实验中已经介绍了域名 wldhj.com 的创建方法，为了实现通过 DNS 的解析访问不同的资源，还需要在 DNS 上配置相应的资源记录。

1. 实验目的

在安装 DNS 时，直接创建的是没有具体资源记录的域名，如 wldhj.com。但是，在具体访问某类资源(如 WWW、FTP、Mail 等)时，还需要在已有的域名上添加相应的资源记录，形成完整的统一资源定位符(Uniform Resource Locator，URL)(如 http://www.wlhj.com、ftp://ftp.wldhj.com 等)，用户通过 URL 访问具体的网站。通过本实验的练习就能够掌握资源记录的规则和创建方法。

2. 实验原理

每个区域文件(区域文件指存放区域数据的文件，该文件是一个数据库文件)都由一些资源记录(Resource Record，RR)组成，每个资源记录包含一些网络上的资源信息，如 IP 地址等。掌握这些资源记录，是有效地配置和管理 DNS 服务器的基础。

1) 管理者起始记录

管理者起始(SOA)记录用于记录该区域内主要名称服务器(即保存该区域数据正本的 DNS 服务器)与此区域管理者的电子邮件账号。当新建一个区域后，SOA 就会被自动创建，所以 SOA 是区域内的第 1 个记录文件。SOA 记录的格式如下。

```
@ IN SOA < source host > < contact e - mail > < ser.no.>
< refresh time >
< retry time > < expiration time > < TTL >
```

SOA 定义了 DNS 区域的一般参数，包括谁是管理该区域的认证服务器。表 5-1 所示为存放在 SOA 记录中的属性。

表 5-1 SOA 记录结构

字　段	含　义
source host	对该文件进行维护的主机名
contact e-mail	此区域管理者的电子邮件地址
ser. no. (serial number)	数据库文件的版本号,每次改变时都要增加
refresh time	标准辅助服务器等待检查主机的数据库文件是否改变的时间间隔(以 s 为单位),如果改变将发出区域传输请求
retry time	标准辅助服务器在发生一次传输失败后,等待重发的时间间隔(以 s 为单位)
expiration time	标准辅助服务器保持尝试下载一个区域信息的持续时间。这个时间超过预计的值后,旧的区域信息将被抹去
TTL(Time to Live)	允许 DNS 服务器缓存来自该数据库文件的资源记录的时间间隔(以 s 为单位),当单个的资源记录没有优先值时,这个值将与所有来自该区域文件的查询响应一起发送

2) 名字服务器记录

名字服务器(Name Server,NS)记录用于记录管辖此区域的名称服务器,包括主要名称服务器和辅助名称服务器,这样就允许其他名字服务器到该域查找名字。一个区域文件可能有多个名字服务器记录,这些记录的格式如下。

```
<domain> @ IN NS <nameserver host>
```

其中,domain 是该域的域名; nameserver host 是名字服务器在该域的完全限定域名(FQDN)。

3) 主机记录

主机(A Host)记录也叫作 A 记录,它是用来静态地建立主机名与 IP 地址之间的对应关系,以便提供正向查询的服务。主机记录的格式比较简单,下面是一个例子。

```
ftp IN A 172.16.1.10
vod IN A 172.16.1.10
```

主机记录将主机名(如 ftp、vod)与一个特定的 IP 地址联系起来。

4) 指针记录

在 DNS 数据库中,主机记录可能是使用率最高且最容易被用户接受的记录,因为在 Internet 中,用户可以依据这些记录将 www. wldhj. com 和 ftp. wldhj. com 这样的 FQDN 转换成对应的 IP 地址,以便让浏览器和其他程序能够找到。其中,在主机记录中还有一个与它很相似的记录:指针(PRT)记录。主机记录将一个主机名映射到一个 IP 地址上;而指针记录则正好相反,它是将一个 IP 地址映射到一个主机上。指针记录为反向查询提供了条件,用户有时要求 DNS 服务器找出与一个特定地址相对应的 FQDN,这是一个很有用的功能,它可以防止某些非法用户用伪装的或不合法的域名使用 E-mail 或 FTP 服务。

5) 别名记录

别名(Canonical Name 或 CNAME)记录用来记录某台主机的别名。别名记录在平时有广泛的应用,它可以给一台主机设置多个别名,每个别名代表一个应用。例如,有一台名

为 wq. wldhj. com 的主机，它同时可以有两个别名，一个为 mail. wldhj. com，用于邮件服务；另一个为 ftp. wldhj. com，用于 FTP 服务。也就是说，这 3 个不同名称的主机返回的 IP 地址完全相同。下面是实现 FTP 别名的命令。

```
ftp IN CNAME wq
wq IN A 172.16.1.18
```

6）邮件交换记录

邮件交换（Mail Exchanger，MX）记录可以告诉用户，哪些服务器可以为该域接收邮件。接收邮件的服务器一般是专用的邮件服务器，也可以是一台用来转送邮件的主机。每个 MX 记录有两个参数：preference 和 mailserver，格式如下。

```
<domain> IN MX <preference> <mailserver host>
```

为什么要使用 MX 记录呢？例如，已创建的域名为 wldhj. com 的局域网，在这个局域网内部，所有的用户使用 someone@abc. net 的方式（如 wq@abc. net、lfj@abc. net 等）收发邮件，不过，这样只能实现用户在局域网内部进行邮件的交换。如果局域网接入 Internet 后，局域网中的用户还要与 Internet 上的其他用户交换邮件，也就是说还需要一个指向 ISP 的邮件服务器（假如域名为 wldhj. com）。这样，当用户在局域网内部发送邮件时（邮件的后缀为@abc. net），一般可由局域网内部的邮件服务器完成交换；当用户需要向局域网之外的 Internet 上的其他用户发送邮件时，则通过指向 ISP 的邮件服务器进行交换。下面是实现这一功能的两条 MX 记录。

```
abc.net.  IN MX 10 mail.abc.net
abc.net.  IN MX 100 mail.wldhj.com
```

其中，两种记录中的 preference 字段的值各不相同，一个是 10，另一个是 100。当一个域中有两个以上的 MX 记录时，DNS 服务器首先使用 preference 值较小的一个邮件服务器，如果其中一个邮件服务器无法通信时，再依次试用 preference 值较大的其他邮件服务器，直到找到需要的邮件服务器为止。

7）服务记录

服务（SRV）记录用来记录提供特殊服务的服务器的相关数据。例如，它可以记录域控制器的完整的计算机名与 IP 地址，使客户端登录时可以通过此记录寻找域控制器，以便审核登录者的身份。以下是一个 SRV 记录的例子，通过这个例子可以帮助了解 SRV 记录的功能。

```
ldap.tcp.wldhj.com SRV 10 100 389
wq.wldhj.com
ladp.tcp.wldhj.com SRV 20 50 389
lfj.wldhj.com
```

其中，第 1 行语句中 ldap. tcp. wldhj. com 是一个复合字段，它包括一个服务名 ldap（ldap 代表 LDAP 服务；如果是 Kerberos 服务，则该服务名应为 kerb）、一个传输协议 tcp

(有时使用 udp)和一个提供该服务的域名 wldhj.com。所以,ldap.tcp.wldhj.com 表示这是一个关于 wldhj.com 域的一个 LDAP 服务器的记录;SRV 表示记录的类型,即服务记录;SRV 后面的 10 是优先级,类似于 MX 记录中的 preference 字段,DNS 服务器首先使用优先级低的记录;优先级后面的数据 100 表示权重,与优先级不同的是,权重的值越大,被选中的概率越高。权重主要用于对优先级相同的记录,该首先使用哪一个。最后的数字 389 表示服务使用的端口号,其中 LDAP 服务使用的端口号是 389,而 Kerberos 服务使用的端口号则是 88。第 3 行的语句功能与第 1 行相似。

第 2 行的 wq.wldhj.com 和第 4 行的 lfj.wldhj.com 分别表示提供该服务的 DNS 服务器名。

以上介绍了 DNS 数据库中经常用到的几个资源记录类型的作用和功能,除此之外,还有用来记录主机的相关数据(如 CPU 的类型、操作系统的类型等)的 HINFO 记录等。在后面的相关操作中,将具体介绍这些记录是如何使用的。

3. 实验内容和要求

(1) 熟悉 DNS 的工作原理和过程。

(2) 熟悉资源记录的功能和应用特点。

(3) 掌握资源记录的创建和应用方法。

5.4.2 实验规划

1. 实验设备

(1) VMware Workstation 软件虚拟平台。

(2) 虚拟服务器(2 台,名称分别为 Server1 和 Server2,安装 Windows Server 2016 操作系统)。

(3) 测试用 PC(2 台,安装 Windows 10 操作系统)。

(4) 实体计算机(1 台,安装 VMware Workstation 软件)。

2. 实验拓扑

网络拓扑可参见本章实验 2 的图 5-22。wldhj.com 是在前面实验中已创建的域名,本实验将在该域名上提供 Web 浏览、FTP 下载、电子邮件、视频点播等服务,具体规划如表 5-2 所示,域名结构如图 5-39 所示。

表 5-2 在 wldhj.com 上创建主机名

主机名称	功能	服务器 IP 地址
www.wldhj.com	Web 浏览	192.168.1.10
ftp.wldhj.com	FTP 下载	192.168.1.10
vod.wldhj.com	视频点播	192.168.1.10
mail.wldhj.com	电子邮件	192.168.1.20
english.wldhj.com	英语学习站点解析	192.168.1.20
card.wldhj.com	校园一卡通站点解析	192.168.1.20
…	…	…

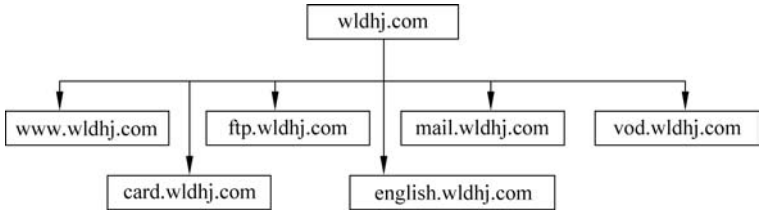

图 5-39　规划的域名结构

5.4.3　实验步骤

本实验根据图 5-39 的规划，分别以 www. wldhj. com 和 mail. wldhj. com 为例，介绍其实现方法。

1. www. wldhj. com 的实现步骤

打开 DNS 管理器，在“正向查找区域”中右击要添加主机记录的域名（本实验为 wldhj. com），在弹出的快捷菜单中选择“新建主机（A 或 AAAA）”，在“新建主机”对话框的“名称”文本框中输入新建主机的名称（本实验为 www），然后在“IP 地址”文本框中输入该 DNS 服务器的 IP 地址（本实验为 192. 168. 1. 10）。由于 A 记录是将 DNS 名称映射到 IP 地址，而 PTR 资源记录是将 IP 地址映射到 DNS 名称，所以如果要将 IP 地址映射到 DNS 名称时，可以勾选“创建相关的指针（PTR）记录”。然后单击“添加主机”按钮，如图 5-40 所示。

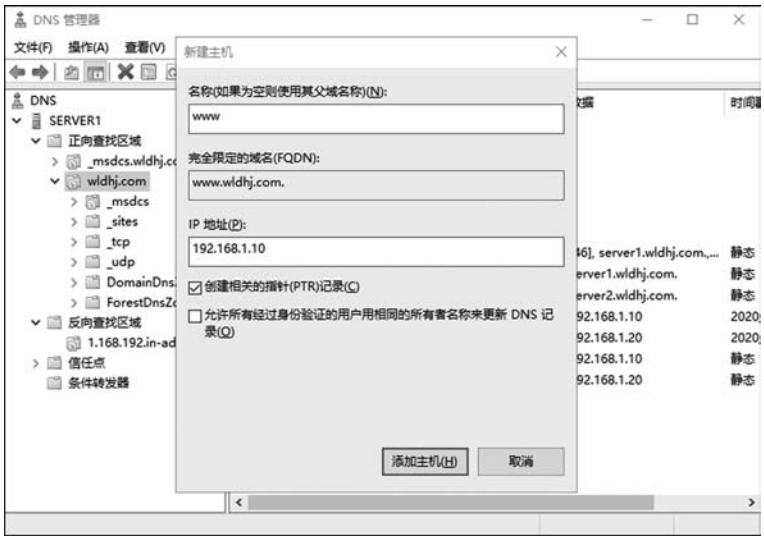

图 5-40　添加 www 主机记录

根据应用需求，通过相同的方法，用户可以在域名中添加 ftp、vod 等各种主机记录，如图 5-41 所示。

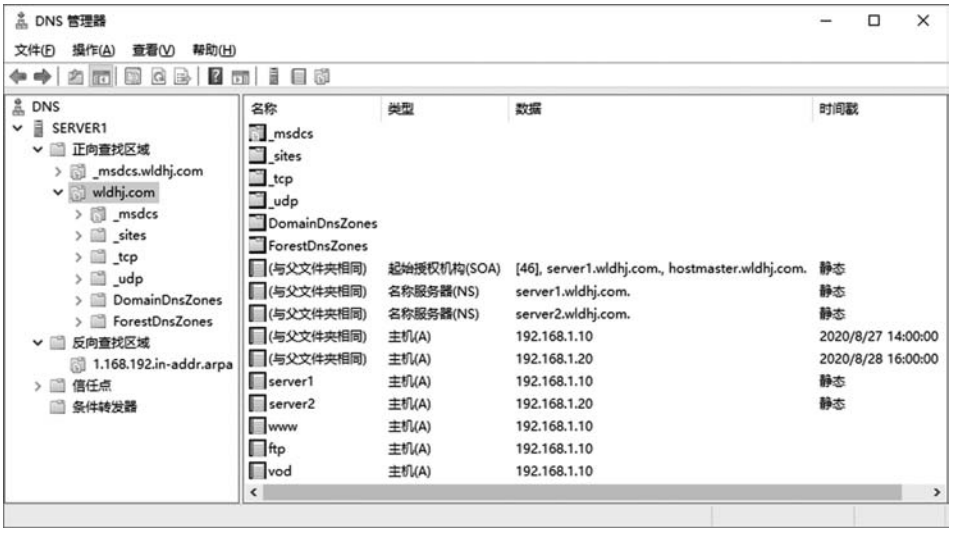

图 5-41 显示在 wldhj.com 中添加的主机记录

2. mail.wldhj.com 的实现步骤

对于邮件系统的域名解析必须同时具有两个记录：一个是主机记录(即 A 记录,本实验为 mail),该主机记录的 IP 地址即邮件服务器的 IP 地址,这样邮件服务器的 FQDN 将为 mail.wldhj.com；另外,还要创建一个 MX 记录,对邮件进行传递或转发,当用户要发送邮件时,首先将邮件传递到本地邮件交换服务器(SMTP Server),本地邮件交换服务器在接收到邮件后再将其转发到目的地的邮件交换服务器。

A 记录 mail 的创建方法与 www 相同,下面介绍 MX 记录的创建方法。在 DNS 管理器中右击要添加 MX 记录的域名(本实验为 wldhj.com),在弹出的快捷菜单中选择“新建邮件交换器(MX)”,如图 5-42 所示,设置 MX 记录的相关参数,具体说明如下。

图 5-42 设置 MX 记录

(1) 主机或子域。输入邮件交换服务器(SMTP 服务器)所负责的域名,现在习惯于使用 mail 作为邮件的主机记录,即通过类似于 http://mail.wldhj.com 登录基于 Web 方式的邮件服务器,所以可以在"主机或子域"文本框中输入主机名 mail。

(2) 邮件服务器的 FQDN。指上述域邮件传递工作的邮件服务器的 FQDN。例如,在本实验中,可将邮件服务器放置在 wldhj.com 域中的 Server2 服务器上,其 FQDN 名称为 server2.wldhj.com。

(3) 邮件服务器优先级。用于同一域中存在多台邮件服务器的情况,用于创建多个 MX 资源记录,并给不同的邮件服务器设置不同的优先级,其中 0 最高。这样,当其他的邮件交换服务器要传递邮件到该域中的邮件交换服务器时,它会先将邮件传递到优先级较高的邮件交换服务器,如果传递失败,则选择优先级较低的邮件交换服务器。如果两台邮件交换服务器具有相同的优先级,便会随机选择一台。

通过以上设置,负责域 mail.wldhj.com 邮件传递的邮件交换服务器是主机名称为 server2.wldhj.com 的主机,其优先级为 10,该本地邮件交换服务器的 IP 地址为 192.168.1.20。设置为 MX 记录和邮件交换服务器主机记录后的显示如图 5-43 所示。需要注意的是,在图 5-41 中应同时显示 MX 记录和邮件交换服务器的主机记录。

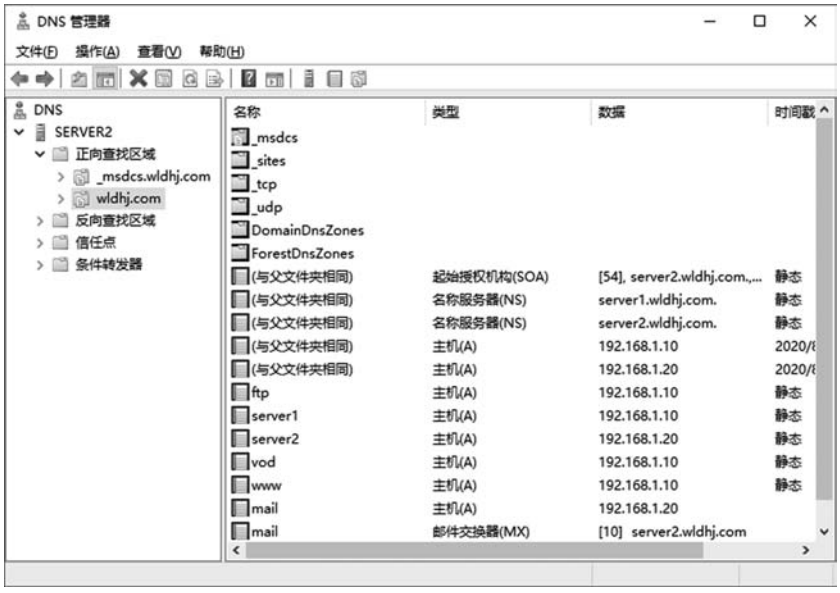

图 5-43　设置了 MX 记录和邮件交换服务器主机记录后的显示

5.4.4　结果验证

将测试用的 PC 的首选 DNS 服务器和备用 DNS 服务器的 IP 地址分别设置为 192.168.1.10 和 192.168.1.20,然后在命令提示符窗口执行 ping www.wldhj.com 命令,将返回 192.168.1.10 这个 IP 地址,并且网络是畅通的,这说明 DNS 服务器的解析是正常的。另外,还可以执行 nslookup 命令进行测试,也可以在测试用的 PC 上打开 IE 浏览器,在地址栏中输入 http://www.wldhj.com,当在 192.168.1.10 的服务器上安装了 Internet 信

息服务时,将显示相应的页面内容。这些内容将在本书第 6 章中专门进行介绍。对于邮件服务器的完整测试,由于需要安装和配置邮件服务器,所以在这里不再进行专门介绍。

本章小结

本章介绍了 DNS 的配置和应用过程,从基于活动目录的第 1 台 DNS 服务器的配置开始,对其他备份 DNS 服务器配置、DNS 服务器的反向查找区域的配置,以及典型主机资源记录的配置等进行了实验。