

DNS服务器配置管理

学习目标

- 了解 DNS 简介以及域名空间结构。
- 掌握 DNS 的工作原理。
- 掌握 DNS 服务器的类型。
- 掌握 DNS 服务器的安装。
- 掌握部署主 DNS 服务器、部署辅助 DNS 服务器、部署存根 DNS 服务器、部署委派 DNS 服务器等相关操作方法。

5.1 DNS 基础知识

域名系统(Domain Name System, DNS)是进行域名和与之相对应的 IP 地址转换的服务器。 DNS 中保存了一张域名和与之相对应的 IP 地址的表,以解析消息的域名。域名是 Internet 中某 一台计算机或计算机组的名称,用于在数据传输时标识计算机的电子方位(有时也指地理位置)。 域名是由一串用点分隔的名称组成的,通常包含组织名,且始终包括两到三个字母的后缀,以指明 组织的类型或该域名所在的国家或地区。

5.1.1 DNS 简介



V5-1

DNS的核心思想是分级,是一种分布式的、分层次型的、客户端/服务器模式的数据库管理系统。它主要用于将主机名和电子邮件地址映射成 IP 地址。一般来说,每个组织都有自己的 DNS 服务器,并维护域名映射数据库记录或资源记录。每个登记的域都将自己的数据库列表提供给整个网络复制。

IP 地址是主机的身份标识,对于人类来说,记住大量的诸如 202.199.184.189 的 IP 地址太难

了;相对而言,主机名一般具有一定的含义,比较容易记忆。因此,如果计算机能够提供某种工具, 使人们可以方便地根据主机名获得 IP 地址,那么这个工具将备受青睐。在网络发展的早期,一种 简单的实现方法就是把域名和 IP 地址的对应关系保存在一个文件中,计算机利用这个文件进行域 名解析。例如,在 Linux 操作系统中,这个文件就是/etc/hosts,其内容如下。

[root@localhost ~] # cat /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
: : 1 localhost localhost.localdomain localhost6 localhost6.localdomain6
[root@localhost ~] #

这种方式实现起来很简单,但是它有一个非常大的缺点,即内容更新不灵活。每台主机都要 配置这样的文件,并及时更新内容,否则就得不到最新域名信息。因此,它只适用于一些规模小的 网络。随着网络规模的不断扩大,用单一文件实现域名解析的方法显然不再适用,取而代之的是 基于分布式数据库的 DNS。DNS将域名解析的功能分散到不同层级的 DNS 服务器中,这些 DNS 服务器协同工作,提供可靠、灵活的域名解析服务。

这里以日常生活中的常见例子进行介绍:公路上的汽车都有唯一的车牌号,如果有人说自己 的车牌号是 80H80,那么我们无法知道这个号码属于哪个城市,因为不同的城市都可以分配这个 号码。现在假设这个号码来自辽宁省沈阳市,而沈阳市在辽宁省的城市代码是 A,现在把城市代 码和车牌号码组合在一起,即 A80H80,是不是就可以确定这个车牌号码的属地了呢?答案还是否 定的,因为其他的省份也有代码是 A 的城市,需要把辽宁省的简称"辽"加入进去,即"辽 A80H80",这 样才能确定车牌的属地。

在这个例子中,辽宁省代表一个地址区域,定义了一个命名空间,这个命名空间的名称是 "辽"。辽宁省的各个城市也有自己的命名空间,如"辽 A"表示沈阳市,"辽 B"表示大连市,在各个 城市的命名空间中才能给汽车分配车牌号码。在 DNS 中,域名空间就是"辽"或"辽 A"这样的命 名空间,而主机名就是实际的车牌号码。

与车牌号的命名空间一样,DNS的域名空间也是分级的。在 DNS 域名空间中,最上面一层被称为"根域",用"."表示。从根域开始向下依次划分为顶级域、二级域等各级子域,最下面一级是主机。子域和主机的名称分别称为域名和主机名,域名又有相对域名和绝对域名之分,就像 Linux 文件系统中的相对路径和绝对路径一样,如果从下向上将主机名及各级子域的所有绝对域名组合在一起,用"."分隔,就构成了主机的完全限定域名(Fully Qualified Domain Name,FQDN)。例如,辽宁省交通高等专科学校的 Web 服务器的主机名为 www,域名为 lncc. edu. cn,那么其 FQDN 就是 www. lncc. edu. cn,通过 FQDN 可以唯一地确定互联网中的一台主机。

5.1.2 域名空间结构

DNS 服务器提供了域名解析服务,那么是不是所有的域名都可以交给一台 DNS 服务器来解 析呢?这显然是不现实的,因为互联网中有不计其数的域名,且域名的数量还在不断增长。一种 可行的方法是把域名空间划分成若干区域进行独立管理。区域是连续的域名空间,每个区域都由 特定的 DNS 服务器来管理。一台 DNS 服务器可以管理多个区域,每个区域都在单独的区域文件 中保存域名解析数据。

V5-2

1. 根域和顶级域

在 DNS 域名空间结构中, 根域位于最顶层, 提供根域名服务, 管理根域的 DNS 服务器称为根



域服务器。在 Internet 中,根域是默认的,一般不需要表示出来。顶级域位于根域的下一层,常见 的顶级域有商业机构.com、教育/学术研究单位.edu、财团法人等非营利机构.org、官方政府单位 .gov、网络服务机构.net、专业人士网络.pro,以及代表国家和地区的中国.cn、美国.us、日本.jp 等。顶级域服务器负责管理顶级域名的解析,在顶级域服务器下面还有二级域服务器等。假如现 在把解析 www.lncc.edu.cn的任务交给根域服务器,根域服务器并不会直接返回这个主机名的 IP 地址,因为根域服务器只知道各个顶级域服务器的地址,并把解析.cn顶级域名的权限"授权" 给其中一台顶级域服务器(假设是服务器 A)。如果根域服务器收到的请求中包括.cn顶级服务器 的地址,则这个过程会一直继续下去,直到最后有一台负责处理.lncc.edu.cn的服务器直接返回 www.lncc.edu.cn的 IP 地址。在这个过程中,DNS 把域名的解析权限层层向下授权给下一级 DNS 服务器,这种基于授权的域名解析就是 DNS 的分级管理机制,又称区域委派。

全球共有 13 台根域名服务器,这 13 台根域名服务器中的名称分别为 A~M,10 台放置在美国,另外 3 台分别放置在英国、瑞典和日本。其中,1 台为主根服务器,放置在美国;其余 12 台均为 辅根服务器,9 台放置在美国,2 台放置在英国和瑞典,1 台放置在日本。所有根域名服务器均由美国政府授权的互联网域名与号码分配机构统一管理,负责全球互联网域名根服务器、域名体系和 IP 地址等的管理。这 13 台根域名服务器可以指挥类似 Firefox 或 Internet Explorer 等的 Web 浏 览器和电子邮件程序控制互联网通信。

2. 子域

在 DNS 域名空间中,除了根域和顶级级域之外,其他域都称为子域。子域是有上级域的域, 一个域可以有多个子域。子域是相对而言的,如 www.lncc.edu.cn 中,lncc.edu.cn 是 cn 的子域, lncc 是 edu.cn 的子域。

和根域相比,顶级域实际是处于第二层的域,但它们还是被称为顶级域。根域从技术的含义 上是一个域,但常常不被当作一个域。根域只有几个根级成员,它们的存在只是为了支持域名树 的存在。

第二层域(顶级域)是属于单位团体或地区的,用域名的最后一部分即域后缀分类。例如,域 名 edu. cn 代表中国的教育系统。多数域后缀可以反映使用这个域名所代表的组织的性质,但并不 总是很容易通过域名后缀来确定使用该域名所代表的组织或单位的性质。

3. 主机

在域名层次结构中,主机可以存在于根以下的各层上。由于域名树是层次型的,而不是平面型的。因此只要求主机名在每一连续的域名空间中是唯一的,而在相同层中可以有相同的名字。如 www.lncc.edu.cn、www.ryjiaoyu.com都是有效的主机名。也就是说,即使这些主机有相同的名字 www,但都可以被正确地解析到唯一的主机,即只要主机是在不同的子域,就可以重名。

5.1.3 DNS 的工作原理



V5-3

DNS 域名的解析方法主要有两种:一种是通过 hosts 文件进行解析;另一种是通过 DNS 服务器进行解析。

1. hosts 文件

hosts 文件解析是 Internet 最初使用的一种查询方式。采用 hosts 文件进行解析时,必须由手



工输入、删除、修改所有 DNS 名称与 IP 地址的对应数据,即把全世界所有的 DNS 名称写在一个文件中,并将该文件存储到解析服务中。客户端如果需要解析名称,就到解析服务器上查询 hosts 文件。全世界所有的解析服务器上的 hosts 文件都需要保持一致。当网络规模较小时,hosts 文件解析还是可以采用的。然而,当网络规模越来越大时,为保持网络里所有的服务器中的 hosts 文件的一致性,就需要进行大量的管理和维护工作。在大型网络中,这将是一项沉重的负担,此种方法显然是不适用的。

在 Windows Server 2019 操作系统中, hosts 文件位于%systemroot%system32\drivers\etc 目录中。本例中的 hosts 文件位于 C:\Windows\system32\drivers\etc 目录下。该文件是一个纯文本文件, 如图 5.1 所示。

🔳 hosts - iā	專本			- 0	×	
文件(F) 编辑	(E) 格式(O) 查看(V) 帮助(H)				
# Copyrigh #	nt (c) 199	3-2009 Microsoft C	orp.			^
# This is a #	sample H	OSTS file used by	Microsoft TCP/IP fo	r Windows.		
# This file # entry sho # be place # The IP a # space. #	contains ould be k d in the t ddress ar	the mappings of IF sept on an individu first column follow ad the host name s	addresses to host i al line. The IP addresed by the correspon hould be separated	names. Each ss should ding host name by at least one	e.	
# Addition # lines or f #	ally, com ollowing	ments (such as the the machine name	se) may be inserted e denoted by a '#' sy	on individual /mbol.		
# For exam	nple:					
#	10107					
# 102.5	4.94.97	rhino.acme.com	# source serve	r	>	~
			Windows (CRL 第1	行, 第13100%		

图 5.1 Windows Server 2019 中的 hosts 文件

2. DNS 服务器

DNS 服务器是目前 Internet 最常用也最便捷的域名解析方法。全世界有众多 DNS 服务器各 司其职,协同工作,构成了一个分布式的 DNS 域名解析网络。例如,Incc. edu. cn 的 DNS 服务器只 负责本域内数据的更新,而其他 DNS 服务器并不知道也无须知道 Incc. edu. cn 域中有哪些主机, 但它们知道 Incc. edu. cn 的 DNS 服务器的位置;当需要解析 Incc. edu. cn 时,它们就会向 Incc. edu. cn 的 DNS 服务器请求帮助。采用这种分布式解析结构时,一台 DNS 服务器出现故障问题并 不会影响整个体系,而数据的更新操作也只在其中的一台或几台 DNS 服务器上进行,使整体的解 析效率大幅提高。

下面介绍 DNS 的查询过程。

(1)当用户在浏览器地址栏中输入 www.163.com 域名访问该网站时,操作系统会先检查自 己本地 hosts 文件中是否有这个网址映射关系。如果有,则先调用这个 IP 地址映射,完成域名 解析。

(2) 如果 hosts 文件中没有这个域名的映射,则查找本地 DNS 解析器缓存,查看其中是否有 其网址映射关系。如果有,则直接返回,完成域名解析。



(3)如果 hosts 文件与本地 DNS 解析器缓存中都没有相应的网址映射关系,则查找 TCP/IP 参数中设置的首选 DNS 服务器。在此称其为本地 DNS 服务器。本地 DNS 服务器收到查询时,如 果要查询的域名包含在本地配置区域资源中,则返回解析结果给客户端,完成域名解析。此解析 具有权威性。

(4)如果要查询的域名未由本地 DNS 服务器区域解析,但该服务器已缓存了此网址映射关系,则调用这个 IP 地址映射,完成域名解析。此解析不具有权威性。

(5)如果本地 DNS 服务器本地区域文件与缓存解析都失效,则根据本地 DNS 服务器的设置 (是否设置转发器)进行查询。如果未使用转发模式,则本地 DNS 服务器会把请求发至 13 台根 DNS 服务器。根 DNS 服务器收到请求后会判断这个域名(.com)是谁来授权管理的,并会返回一 个负责该顶级域名服务器的 IP 地址。本地 DNS 服务器收到 IP 信息后,将会联系负责.com 域的 服务器。负责.com 域的服务器收到请求后,如果自己无法解析,则会发送一个管理.com 域的下 一级 DNS 服务器的 IP 地址(163.com)给本地 DNS 服务器。当本地 DNS 服务器收到这个地址 后,就会查找 163.com 域服务器,重复上面的动作,进行查询,直至找到 www.163.com 主机。

(6)如果使用的是转发模式,则此 DNS 服务器会把请求转发至上一级 DNS 服务器,由上一级 DNS 服务器进行解析。如果上一级 DNS 服务器无法解析,则查找根 DNS 服务器或把请求转至上一级,以此循环。不管是本地 DNS 服务器使用的是转发还是根服务器,最后都要将结果返回给本地 DNS 服务器,由此 DNS 服务器再返回给客户端。

5.1.4 DNS 服务器的类型

按照配置和功能的不同, DNS 服务器可分为不同的类型。常见的 DNS 服务器类型有以下 4 种。

1. 主 DNS 服务器

V5-4

主 DNS 服务器对所管理区域的域名解析提供最权威和最精确的响应,是所管理区域域名信息的初始来源。搭建主 DNS 服务器需要准备全套的配置文件,包括主配置文件、正向解析区域文件、反向解析区域文件、高速缓存初始化文件和回送文件等。正向解析是指从域名到 IP 地址的解析,反向解析正好相反。

2. 辅助 DNS 服务器

辅助 DNS 服务器也称从 DNS 服务器,它从主 DNS 服务器中获得完整的域名信息备份,可以 对外提供权威和精确的域名解析服务,可以减轻主 DNS 服务器的查询负载。辅助 DNS 服务器的 域名信息和主 DNS 服务器完全相同,它是主 DNS 服务器的备份,提供的是冗余的域名解析服务。

3. 高速缓存 DNS 服务器

高速缓存 DNS 服务器将从其他 DNS 服务器处获得的域名信息保存在自己的高速缓存中,并利用这些信息为用户提供域名解析服务。高速缓存 DNS 服务器的信息具有时效性,过期之后便不再可用。高速缓存 DNS 服务器不是权威服务器。

4. 转发 DNS 服务器

转发 DNS 服务器在对外提供域名解析服务时,优先从本地缓存中进行查找。如果本地缓存 没有匹配的数据,则会向其他 DNS 服务器转发域名解析请求,并将从其他 DNS 服务器中获得的



结果保存在自己的缓存中。转发 DNS 服务器的特点是可以向其他 DNS 服务器转发自己无法完成的解析请求任务。

5.2 技能实践

配置 DNS 服务器的首要任务是建立 DNS 区域和域的树状结构。DNS 服务器以区域为单位 来管理服务。区域是一个数据库,用来链接 DNS 名称和相关数据,如 IP 地址和网络服务,在 Internet 环境中一般用二级域名来命名,如 abc. com。DNS 区域分为两类:一类是正向搜索区域, 即域名到 IP 地址的数据库,用于提供域名转换为 IP 地址的服务;另一类是反向搜索区域,即 IP 地址到域名的数据库,用于提供 IP 地址转换为域名的服务。

5.2.1 安装 DNS 服务器

在安装 Active Directory 域服务角色时,可以选择一起安装 DNS 服务器角色。如果没有安装,则可以在计算机上通过"服务器管理器"安装 DNS 服务器角色。

1. 安装 DNS 服务器角色

安装 DNS 服务器角色,具体步骤如下。

(1)选择"服务器管理器"→"管理"→"添加角色和功能"选项,持续单击"下一步"按钮,直到出现"选择服务器角色"窗口时,勾选"DNS服务器"复选框, 弹出"添加角色和功能向导"对话框,如图 5.2 所示。

(2) 在"添加角色和功能向导"对话框中,单击 "添加功能"按钮,返回"选择服务器角色"窗口,持续 单击"下一步"按钮,最后单击"安装"按钮,开始安装 DNS 服务器。安装完毕后,单击"关闭"按钮,完成 DNS 服务器角色的安装。

2. DNS 服务的启动和停止

要启动或停止 DNS 服务,可以使用"DNS 管理器"控制台、"服务"控制台、net 命令 3 种方式,具体步骤如下。

V5-5

图 5.2 "添加角色和功能向导"对话框

(1) 使用"DNS管理器"控制台。

选择"服务器管理器"→"工具"→DNS选项,弹出"DNS管理器"窗口,在左侧控制台树中右击 服务器 SERVER-01选项,在弹出的快捷菜单中选择"所有任务"→"启动"、"停止"、"暂停"、"恢复" 或"重新启动"选项,即可启动或停止 DNS 服务,如图 5.3 所示。

(2) 使用"服务"控制台。

选择"服务器管理器"→"工具"→"服务"选项,弹出"服务"窗口,找到 DNS Server 服务,如 图 5.4 所示;双击 DNS Server 服务,弹出"DNS Server 的属性(本地计算机)"对话框,在服务状态 区域,单击"启动"或"停止"按钮,即可启动或停止 DNS 服务,如图 5.5 所示。



>⇒ 2 🖬 🗙			
 DNS ISERVER-01 正向查找 反向查找 简 信任点 留 条件转发 	名称 配置 DNS 服务器(C) 创建款认应用程序目录分区(T) 新建区域(Z) 为所有区域设置を化/清理(S) 清除过时资源记录(N) 更新服务器数据文件(U) 清除委件(E) 启动 nslockup (A)		
	所有任务(K)	>	配置 DNS 服务器(C)
	查看(V)	>	清除过时资源记录(N)
	删除(D) 刷新(F) 导出副事(I)		更新服务器数据文件(U) 清除缓存(E) 启动 nslookup (A)
	写出/J&(C) 属性(R)		启动(S)
	帮助(H)		19正(O) 暫停(U)
			恢复(M)

图 5.3 "DNS 管理器"窗口

3. 服务(本地)	◎ 服务(本地)						
	DNS Server	名称	描述	状态	启动类型	登录为	
		DevQuery Background D	使应		手动(触发	本地系统	
	<u>停止</u> 此服务	DFS Namespace	可以	正在	自动	本地系统	
	<u> 暂停</u> 此服务 第二つた此服务	DFS Replication	使你	正在	自动	本地系统	
	里启动匹服务	DHCP Client	为此	正在	自动	本地服务	- 1
		Diagnostic Policy Service	诊断	正在	自动(延迟	本地服务	- 1
	描述:	Diagnostic Service Host	诊断		手动	本地服务	
	使 DNS 客户端可以通过应答 DNS 查	Diagnostic System Host	诊断		手动	本地系统	
	個和动态 DNS 更新请求来解析 DNS 夕約 前里停止法服务 修于法进行	Distributed Link Tracking	维护		手动	本地系统	
	DNS 更新。如果禁用该服务,则所有	Distributed Transaction C	协调	正在	自动延迟	网络服务	
	明确依赖它的服务都将启动失败。	DNS Client	DNS	正在	自动(触发	网络服务	
		DNS Server	使 D	正在	自动	本地系统	
		Downloaded Maps Man	供应		禁用	网络服务	
		DS Role Server	此服		手动	本地系统	
		Encrypting File System (E	提供		手动(触发	本地系统	
		Enterprise App Manage	启用		手动	本地系统	
		Extensible Authentication	可扩		手动	本地系统	
		Serie Replication	将文		禁用	本地系统	
		Runction Discovery Provi	FDP		手动	本地服务	
		Sunction Discovery Reso	发布		手动(触发	本地服务	
		10 Ganlacation Consist			ALC: FR	士袖石坛	

图 5.4 "服务"窗口

(3) 使用 net 命令。

以域管理员用户账户登录服务器 server-01,在命令提示符下输入命令 net stop dns 停止 DNS 服务;输入命令 net start dns 启动 DNS 服务,如图 5.6 所示。



图 5.6 net 命令启动、停止 DNS 服务

服务名称: DNS 显示名称: DNS Server 描述: 使 DNS 客户論可以通过应答 DNS 查询和动态 DNS ^ 更新请求未解析 DNS 名称,如果停止该服务,将无法 * 词功行文件的路径: C:\Vindows\system32\dns.exe 自动类型(E): 自动 * 服务状态: 正在运行 直动(5) 停止(7) 暂停(P) 恢复(R) 当从此处启动服务时,你可指定所适用的启动参数。 当动参数(M): C:\Vinet start dns DNS Server 服务正在启动, DNS Server 服务正在启动, DNS Server 服务正在启动, DNS Server 服务已经启动成功。		
振る名称: DNS Server 読述: 使 DNS 客户論可以通过应答 DNS 查询和动态 DNS へ 更新请求未解析 DNS 名称,如果停止该服务,将无法 出版行文件的路径: :(Windows\system32\dns.exe 活动決型(E): 自动 ~ 招快型(E): 自动 ~ 招供数本: 正在运行 <u> 「取(S) 停止(T) 暂停(P) 恢复(R)</u> 私从此处启动服务时,你可指定所适用的启动参数。 記述: 「如本: 「」」」 私以此处启动服务时,你可指定所适用的启动参数。 記述: 「」」 こ: \`net start dns DNS Server 服务正在信心. DNS Server 服务正在信心. DNS Server 服务正在信心. DNS Server 服务正在信心. DNS Server 服务正在信心.	资名称: DNS	
 描述: 使 DNS 客户調可以通过应答 DNS 查询和动态 DNS へ 更新请求未解析 DNS 名称、如果停止读服务、将无法、 进行 DNC 面新 的甲基面法服务 副新有相通体转应 × 可执行文件的路径: C:\Windows\system32\dns.exe 自动类型(E): 自动 × 服务状态: 正在运行 国动(S) 停止(T) 暂停(P) 恢复(R) 当从此处启动服务时,你可指定所适用的启动参数。 自动参数(M): 回 管理员: C:\Windows\system32\cmd.exe - C:\\net stop dns DNS Server 服务正在停止、 DNS Server 服务已经归动 点功。 Server 服务已经归动 点功。	显示名称: DNS Server	
可执行文件的路径: C:\Windows\system32\dns.exe 启动类型(E): 自动 ~ 服务状态: 正在运行	世述: 使 DNS 客户論可以通过应答 DNS 查询和动态 DNS 更新请求来解析 DNS 名称、如果停止该服务,将无法 讲行 DNS 番新 如果禁用论服务。则断有用确仿赖令	•
C:\Windows\system32\dns.exe 启动类型(E): 自动 服务状态: 正在运行 启动(S) 停止(T) 暂停(P) 恢复(R) 当从此处启动服务时,你可指定所适用的启动参数。 DNS Server 服务已成功停止。 启动参数(M): C:\>net start dns DNS Server 服务已在启动。 DNS Server 服务已在启动。 DNS Server 服务已经启动成功。	可执行文件的路径:	
启动类型(f): 自动	C:\Windows\system32\dns.exe	
服务状态: 正在运行 <u>启动(S)</u> 停止(T) 暂停(P) 恢复(R) 当从此处启动服务时,你可指定所适用的启动参数。 启动参数(M): C:\>net stop dus DNS Server 服务正在停止。 DNS Server 服务已成功停止。 C:\>net start dns DNS Server 服务正在启动。 DNS Server 服务已经启动成功。	自动类型(E): 自动	~
当从此处启动服务时,你可指定所适用的启动参数。 当从此处启动服务时,你可指定所适用的启动参数。 启动参数(M): 定:\>net stop dns DNS Server 服务已成功停止。 C:\>net stop dns DNS Server 服务已成功停止。 C:\>net stop dns DNS Server 服务已成功。 DNS Server 服务已经启动成功。	最务状态: 正在运行 启动(S) 停止(T) 暂停(P) 恢复(R)	國 管理员: C:\Windows\system32\cmd.exe -
启动参数(M): DNS Server 服务正在启动。 DNS Server 服务已经启动成功。	当从此处启动服务时,你可指定所适用的启动参数。	C:\\net stop dns DNS Server 服务正在停止。 DNS Server 服务已成功停止。
	启动参数(M):	C:\>net_start_dns DNS Server 服务正在启动 DNS Server 服务已经启动成功。

图 5.5 "DNS Server 的属性(本地计算机)"对话框

5.2.2 部署主 DNS 服务器

在实际应用中,DNS 服务器一般会与活动目录区域集成,所以当安装完成 DNS 服务器,新建 区域后,直接提升该服务器为域控制器,将新建区域更新为活动目录集成区域。

1. 项目规划

部署主 DNS 服务器网络拓扑结构图,如图 5.7 所示。

主要区域 abc.com	角色:第一台域控制器&DNS1服务器 主机名: server-01 IP地址: 192.168.100.100/24 网关: 192.168.100.2 DNS: 192.168.100.100	8
	A	角色: DNS客户端 主机名: Win10-user01 IP地址: 192.168.100.10/24 网关: 192.168.100.2 首选DNS: 192.168.100.100

图 5.7 部署主 DNS 服务器网络拓扑结构图



V5-6



一个区域的主要区域建立在该区域的主 DNS 服务器上。主要区域的数据库文件是可读写的,所有针对该区域的添加、修改和删除等写入操作都必须在主要区域中进行。

配置 DNS 区域时,常用的术语如下。

- 全限定域名 (Fully Qualified Domain Name, FQDN)带有主机名和域名的名称,可以从逻辑上准确地表示出主机在什么地方,也可以说全限定域名是主机名的一种完全表示形式。
 从全限定域名中包含的信息可以看出主机在域名树中的位置。
- 初始授权记录(Start Of Authority, SOA)用于表示一个区域的开始,记录的所有信息是用 于控制这个区域的。每个区域数据库文件都必须包含一个 SOA 记录,并且必须是其中的 第一个资源记录,用以标记 DNS 服务器所管理的起始位置。
- 名称服务器(Name Server, NS)记录,用于标识一个区域的 DNS 服务器。
- 主机记录(Address, A)也称为 Host 记录,实现正向解析,建立 DNS 名称到 IP 地址的映射,用于正向解析。
- 规范名称(Canonical Name)记录,也称为别名(Alias)记录,定义主机记录的别名,用于将 DNS域名映射到另一个主要的或规范的名称,该名称可能为 Internet 中规范的名称, 如 www。
- 指针(domain name PoinTeR, PTR)记录, 实现反向解析, 建立 IP 地址到 DNS 名称的映射。
- 邮件交换器(Mail exchanger, MX)记录,用于指定交换或者转发邮件信息的服务器,该服务器知道如何将邮件传送到最终目的地。

在部署 DNS 服务器之前,须完成如下配置。

(1) 在服务器 server-01 上部署域环境,域名为 abc. com。

(2) 设置 DNS 服务器的 TCP/IP 属性,设置 IP 地址、子网掩码、默认网关和 DNS 服务器地址 等相关信息。

(3) 设置 Windows 10 客户端主机的 TCP/IP 属性,设置 IP 地址、子网掩码、默认网关和 DNS 服务器地址等相关信息。

2. 创建正向主要区域

在 DNS 服务器上创建正向主要区域 abc. com,具体步骤如下。

(1) 在 DNS 服务器上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口, 展开 DNS 服务器目录树,右击"正向查找区域"选项,在弹出的快捷菜单中选择"新建区域"选项, 如图 5.8 所示;弹出"新建区域向导"对话框,如图 5.9 所示。

(2) 在"新建区域向导"对话框中,单击"下一步"按钮,弹出"区域类型"对话框,如图 5.10 所示;选中"主要区域"单选按钮,默认勾选"在 Active Directory 中存储区域(只有 DNS 服务器是可写域控制器时才可用)"复选框,单击"下一步"按钮,弹出"Active Directory 区域传送作用域"对话框,如图 5.11 所示。

(3) 在"Active Directory 区域传送作用域"对话框中,选中"至此域中域控制器上运行的所有 DNS 服务器(D): abc. com"单选按钮,单击"下一步"按钮,弹出"区域名称"对话框,输入区域名称, 如 xyz. com(注意,如果是活动目录集成的区域,则不需要指定区域文件,否则需要指定区域文件 xyz. com. dns),如图 5.12 所示;单击"下一步"按钮,弹出"动态更新"对话框,如图 5.13 所示。



 ▲ DNS 管理器 文件(F) 操作(A) 查看(N ◆ ◆ △ 〒 Q 	Ŋ 帮助(H) ┃ 🖬 🗊 │ 🔒 🗐 🗊			- 0	×
 ▲ DNS ✓ 副 SERVER-01 > □ 正向查找区域 	名称 副 abc.com	<u> </u>	状态 正在运行	DNSSEC 状态 未签名	5
 > 反向查找区域 > 信任点 > <	新建区域(Z) 查看(V) >				
	刷新(F) 导出列表(L)				
	報助(H)				
	<	26- 1		_	3

图 5.8 "DNS 管理器"窗口

欢迎使用新建区域向导
此向导帮助你为 DNS 服务器创建一个新区域。
区域将 DNS 名称转换成相关数据,例如 IP 地址或网络服务。
单击"下一步"继续。

图 5.9 "新建区域向导"对话框

新建区域向导		×
区域类型 DNS 服务器支持不同类型的区域和存储。		
选择你要创建的区域的类型:		
• 主要区域(P)		
创建一个可以直接在这个服务器上更新的区	域副本。	
○辅助区域(S)		
创建一个存在于另一个服务器上的区域的副 量,并提供容错。	本。此选项帮助主服务器平衡处理的工作	
○存根区域(U)		
创建只含有名称服务器(NS)、起始授权机构 有存根区域的服务器对该区域没有主管权。	i(SOA)和粘连主机(A)记录的区域的副本。	含
☑在 Active Directory 中存储区域(只有 DNS	服务器是可写域控制器时才可用)(A)	
	<上一步(B) 下一步(N) >	取消

图 5.10 "区域类型"对话框



建区域向导 Active Directory 区域传送作用域	×
ALCONTRACT MART MARKED DIAS AND	
选择如何复制区域数据:	
○至此林中域控制器上运行的所有 DNS 服务器(A): abc.com	
● 至此域中域控制器上运行的所有 DNS 服务器(D): abc.com	
○至此域中的所有域控制器(为了与 Windows 2000 兼容)(O): abc.com	
○到在此目录分区的作用域内指定的所有域控制器(C):	
	×
< 上一步(B) 下一步(N) >	取消

图 5.11 "Active Directory 区域传送作用域"对话框

新区域的名称是什么? 区域名称描定 DNS 命名空间的部分,该部分由此服务器管理。这可能是你组织单位的域名(例 如, microsoft.com)或此域名的一部分(例如, newzone.microsoft.com)。区域名称不是 DN: 服务器名称。 区域名称(Z): xyz.com	反域名称	5
区域名称描定 DNS 命名空间的部分,该部分由此服务器管理。这可能是你组织单位的域名(例 如, microsoft.com)或此域名的一部分(例如, newzone.microsoft.com)。区域名称不是 DN: 服务器名称。 区域名称(Z): xyz.com	新区域的名称是什么?	
区域名称(Z): xyz.com	区域名称指定 DNS 命名空间的部 如,microsoft.com)或此域名的一 服务器名称。	分,该部分由此服务器管理。这可能是你组织单位的域名(例 -部分(例如,newzone.microsoft.com)。区域名称不是 DNS
xyz.com	区域名称(Z):	
	xyz.com	

图 5.12 "区域名称"对话框

(4) 在"动态更新"对话框中,单击"下一步"按钮,弹出"正在完成新建区域向导"对话框,如 图 5.14 所示;单击"完成"按钮,返回"DNS管理器"窗口,如图 5.15 所示。

3. 创建反向主要区域

反向查看区域用于通过 IP 地址查询 DNS 名称。创建反向主要区域的具体步骤如下。 (1) 在 DNS 服务器上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口,



新建区域向导	×
动态更新 你可以指定这个 DNS 区域接受安全、不安全或非动态的更新。	
动态更新能使 DNS 客户端计算机在每次发生更改时,用 DNS 服务器注册并动态 灵。	更新资源记
请选择你想允许的动态更新类型:	
〇 只允许安全的动态更新(适合 Active Directory 使用)(S)	
Active Directory 集成的区域才有此选项。	
④允许非安全和安全动态更新(A)	
任何客户接受资源记录的动态更新。	
▲ 因为可以接受来自非信任源的更新,此选项是一个较大的安全弱点。	
〇不允许动态更新(D)	
此区域不接受资源记录的动态更新。你必须手动更新这些记录。	
< 上一步(B) 下一步(N) >	取消

图 5.13 "动态更新"对话框

正在完成新建区域向导
你已成功完成了新建区域向导。你指定了如下设置:
名称: xyz.com ^ 类型: Active Directory 集成的主要区域 查找类型: 前进
注意:你应该现在将记录添加到区域,或者确保记录得到动态更新。然后,你可以用 nslookup 验证名称解析。
要关闭此向导并创建新区域,请单击"完成"。

图 5.14 "正在完成新建区域向导"对话框

展开 DNS 服务器目录树,右击"反向查找区域"选项,在弹出的快捷菜单中选择"新建区域"选项, 如图 5.16 所示;弹出"新建区域向导"对话框,如图 5.17 所示。

(2) 在"新建区域向导"对话框中,连续单击"下一步"按钮,直到弹出"反向查找区域名称"对话框,选中"IPv4反向查找区域"单选按钮,单击"下一步"按钮,弹出"反向查找区域名称-网络 ID"对



文件(F) 操作(A) 查看(V) ◆ ◆ ▲ 記 記 ※ 圖 @	帮助(H)				
L DNS ✓ I SERVER-01	名称 ③ abc.com	类型 标准主要区域	状态 正在运行	DNSSEC : 未签名	状态
> 》 正向查找区域 > 》 反向查找区域 > 》 信任点	yz.com	Active Directory	正在运行	未签名	
> 🔛 条件转发器	<				

图 5.15 完成创建正向主要区域

 ▲ DNS ▲ Ender ▲ Ender	 â DNS 管理器 文件(F) 操作(A) 查看(V) 帮助(H) 21 □□ 1 □ □ 同	– 🗆 X
> □ 各件转发器 查看(V) > □ 条件转发器 □ 易新(F) □ 示(F) □ ∩ (F) □	 ■ DNS ■ SERVER-01 > ■ 正向查找区域 > ■ 反向查找区域 > ■ 反向查找区域 		新区域 ** IS)允许将 DNS 命名空间分成区域。每个区域存储有
	> 🔛 品色紙 > 🔛 条件转发器	查看(V) >> 刷新(F) 帮助(H)	_ 3成,请在"操作"菜单,单击"新建区域"。

图 5.16 新建"反向查找区域"窗口



图 5.17 "新建区域向导"对话框



话框,选中"输入网络 ID"单选按钮,当网络 ID 输入为 192.168.100 时,反向查找区域的名称自动 变为 100.168.192.in-addr.arpa,如图 5.18 所示;单击"下一步"按钮,弹出"动态更新"对话框,选 中"允许非安全和安全动态更新"单选按钮,单击"下一步"按钮;弹出"正在完成新建区域向导"对 话框,单击"完成"按钮,完成区域的创建,返回"DNS 管理器"窗口,如图 5.19 所示。

新建区域向导		×
反向查找区域名称 反向查找区域将 IP 地址转换为 DNS 名称。		
要标识反向查找区域,请键入网络 ID 或区域 ⑥ 网络 ID(E):	名称。	
192 .168 .100 .		
, 网络 ID 是属于该区域 IP 地址的部分。用	目正常(不是反向的)顺序输入网络 ID。	
如果在网络 ID 中使用了一个零,它会出 10.in-addr.arpa 区域,网络 ID 10.0 会	现在区域名称中。例如,网络 ID 10 会创建 创建 0.10.in-addr.arpa 区域。	
○反向查找区域名称(V):		
100.168.192.in-addr.arpa		
	< 上一步(B) 下一步(N) > 取	[消
		END

图 5.18 "反向查找区域名称"对话框

 ▲ DINS 管理部 文件(F) 操作(A) 查看(V) 非 ◆ ◆ △ 記 ※ 圖 ④ 	#助(H) 副 🛛 🗊 🛔 🗐 🗊		
 ▲ DNS → I Enpat/SERVER-01 > I Enpat/SEV > Epat/SEV > I Enpat/SEV > I Enpat/SEV 	名称 M 100.168.192.in-addr.arpa	<u>类型</u> Active Directory	状态 正在运行
- ma and - country	<		

图 5.19 完成创建反向主要区域

4. 创建资源记录

DNS 服务器需要根据区域中的资源记录提供该区域的名称解析。因此,在区域创建完成之后,需要在区域中创建所需要的资源记录。

(1) 新建主机。

在 DNS 服务器上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口,展开 DNS 服务器目录树,右击"正向查找区域"→abc. com 选项,在弹出的快捷菜单中选择"新建主机 (A 或 AAA)"选项,如图 5.20 所示;弹出"新建主机"对话框,单击"添加主机"按钮,完成新建主机



添加,如图 5.21 所示。

			- 0	×
 ▲ DNS ▲ SERVER-01 ▲ 正向查找区域 → 圖 abc.com → 圖 友向查找区域 → 圖 反向查找区域 → 圖 信任点 新建主机(A 或 AA > 圖 条件转发器 新建卸件交换器(N) 新建碱(O) 新建香飯(G) 				
 > □ 女Zcom > □ 反向查找区 2 信任点 新建主机(A 或 AA > □ 条件转发器 新建则名(CNAME 新建如件交换器(M 新建城(O) 新建添添(G) 	s (1 .0.)	类型	数据	
其他新记录(C)… DNSSEC(D) 所有任务(K) 查看(V) 删除(D) 刷新(F) 导出列表(L)… 雇性(R)	AA)(S))(A))X)(M) >	起始授权机构(SOA) 名称服务器(NS) 主机(A) 主机(A)	[67], server-01.abc.com server-01.abc.com. 192.168.100.100 192.168.100.100	

图 5.20 创建资源记录

新建主机		×
名称(如果为空则使用其父域名称))(N):	
DNS1		
完全限定的域名(FQDN):		
DNS1.abc.com.		
IP 地址(P):		
192.168.100.100		

图 5.21 "新建主机"对话框

(2) 新建别名。

DNS 同时还是 Web 服务器,为其设置别名 www,具体步骤如下。



在 DNS 服务器上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口,展开 DNS 服务器目录树,右击"正向查找区域"→abc.com 选项,在弹出的快捷菜单中选择"新建别名 (CNAME)"选项,弹出"新建资源记录"对话框,输入别名及目标主机的完全合格的域名,如图 5.22 所示;单击"确定"按钮,返回"DNS 管理器"窗口,如图 5.23 所示。

新建资源记录		×
别名(CNAME)		
别名(如果为空则使用父域)(S):		
www		
完全限定的域名(FQDN)(U):		
www.abc.com.		
目标主机的完全合格的域名(FQDN)(F):		
DNS1.abc.com		浏览(B)
	确定	取消

图 5.22 "新建资源记录"对话框

► ➡ 22 m X 🗈 🔒	2 51 1 9 9		
 ▲ DNS ✓ I E向查找区域 > I 正向查找区域 > I zpo查找区域 > I zpo查找区域 > I 反向查找区域 > I 反向查找区域 > I 条件转发器 	名称 msdcs sites tcp udp DomainDnsZones ForestDnsZones Incc	类型	数据
	 □ (与父文件夹相同) □ (与父文件夹相同) □ (与父文件夹相同) □ (与父文件夹相同) □ server-01 □ DNS1 □ WWW 	起始授权机构(SOA) 名称服务器(NS) 主机(A) 主机(A) 主机(A) 到名(CNAME)	[67], server-01.abc.com server-01.abc.com. 192.168.100.100 192.168.100.100 192.168.100.100 DNS1.abc.com

图 5.23 完成新建别名窗口

(3) 新建邮件交换器。

在 DNS 服务器上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口,展开 DNS 服务器目录树,右击"正向查找区域"→abc.com 选项,在弹出的快捷菜单中选择"新建邮件交 换器(MX)"选项,弹出"邮件交换器(MX)"选项卡,输入主机或子域以及邮件服务器的完全限定的 域名(FQDN),设置邮件服务器优先级,如图 5.24 所示;单击"确定"按钮,返回"DNS 管理器"窗 口,如图 5.25 所示。

主机或子域(H):		
mail		
E默认方式,当创建邮/ 或名称,但是在多数部 完全限定的域名(FQDN)	4交换记录时,DNS 使用父域名 晷,不填写以上字段。)(U):	。你可以指定主机。
mail.abc.com.		
邮件服务器的完全限定的	的域名(FQDN)(F):	
邮件服务器的完全限定的 DNS1.abc.com 邮件服务器优先级(S):	的域名(FQDN)(F):	浏览(8)
邮件服务器的完全规定的 DNS1.abc.com 邮件服务器优先级(S): 10	的或名(FQDN)(F):	浏览(B)
邮件服务器的完全规定的 DNS1.abc.com 邮件服务器优先级(S): 10	的现在。(FQDN)(F):	浏览(8)

图 5.24 "邮件交换器(MX)"选项卡

 ▲ DNS → III E向查找区域 > III E向查找区域 > III E向查找区域 > III E向查找区域 > III 反向查找区域 > III 信任点 > III 条件转发器 	名称 msdcs sites tcp udp DomainDnsZones ForestDnsZones Incc	美型	数据
	 □ (与父文件夹相同) □ (与父文件夹相同) □ (与父文件夹相同) □ (与父文件夹相同) 	起始授权机构(SOA) 名称服务器(NS) 主机(A)	[67], server-01.abc.com server-01.abc.com. 192.168.100.100
	server-01	主机(A)	192.168.100.100
	DNS1	主机(A)	192.168.100.100
	www	别名(CNAME)	DNS1.abc.com
	mail	邮件交换器(MX)	[10] DNS1.abc.com

图 5.25 完成新建邮件交换器窗口



(4) 新建指针。

在 DNS 服务器上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口,展开 DNS 服务器目录树,右击"反向查找区域"→100.168.192.in-addr.arpa 选项,在弹出的快捷菜单中 选择"新建指针(PTR)"选项,弹出"指针(PTR)"选项卡,输入主机 IP 地址以及主机名;如图 5.26 所示;单击"确定"按钮,返回"DNS 管理器"窗口,如图 5.27 所示。

旨针(PTR)		
主机 IP 地址(P):		
192.168.100.100		
完全限定的域名(FQDN)(F):		
100.100.168.192.in-addr.arp	a	
主机名(H):		
DNS1.abc.com	浏览(8).	
□ 允许任何经过身份验证的用, 置只适用于新名称的 DNS 说	户用相同的名称来更新所有 DNS 记录。这个 记录(O),	Ng
□ 允许任何经过身份验证的用序 置只适用于新名称的 DNS 词	^白 用相同的名称来更新所有 DNS 记录。这个 记录(O)。	₩ Ng

图 5.26 "指针(PTR)"选项卡

 ▲ DNS 管理器 文件(F) 操作(A) 查看(V) 帮助(H) ◆ ● ② 〒 ※ □ → 図 □ 			- 0	×
 ■ DNS ■ SERVER-01 > □ 正向查找区域 > □ abc.com > □ xyz.com > □ 反向查找区域 □ 100.168.192.in-addr.arpa > □ 使年点 	名称 (与父文件夹相同) (与父文件夹相同) (与父文件夹相同) (与父文件夹相同) (5) (5) (5) (5) (5) (5) (5) (5) (5) (5	类型 起始授权机构(SOA) 名称服务器(NS) 指针(PTR)	数据 [1], server-01.abc.com., h server-01.abc.com. DNS1.abc.com	时间 静动
> 🔛 条件转发器	<			3

图 5.27 完成新建指针窗口

5. 客户端测试主 DNS 服务器

配置 DNS 客户端主机的相关信息, 配置信息如下。



(1) 配置 DNS 客户。

以管理员身份登录 DNS 客户端 Win10-user01 主机,打开"Internet 协议版本 4(TCP/IPv4)属性"对话框,相关地址配置信息,如图 5.28 所示。

nternet 协议版本 4 (TCP/IPv4) [重性
常规	
如果网络支持此功能,则可以获 络系统管理员处获得适当的 IP	取自动指派的 IP 设置。否则,你需要从网 设置。
○自动获得 IP 地址(O)	
●使用下面的 IP 地址(S):	
IP 地址(I):	192 . 168 . 100 . 10
子网掩码(U):	255 . 255 . 255 . 0
默认网关(D):	192.168.100.2
○ 自动获得 DNS 服务器地址	E(B)
●使用下面的 DNS 服务器均	b址(E):
首选 DNS 服务器(P):	192 . 168 . 100 . 100
备用 DNS 服务器(A):	192 . 168 . 100 . 101
□ 退出时验证设置(L)	高级(V)
	油 完 - 10%
	WEAC POLING

图 5.28 "Internet 协议版本 4(TCP/IPv4)属性"对话框

(2) 使用 nslookup 命令测试 DNS 服务器是否正常工作。

在客户端 Win10-user01 主机上,按 Win+R 组合键,弹出"运行"窗口,输入 cmd 命令,打开 "管理员: C:\Windows\system32\cmd. exe"或"管理员: 命令提示符"窗口。

nslookup 命令是用来进行手动 DNS 查询的最常用的工具。这个工具有两种工作模式: 非交 互模式和交互模式。

① 非交互模式。

非交互模式要在命令行中输入完整的命令:nslookup www.abc.com,如图 5.29 所示。

使用命令 nslookup 测试 DNS1 服务器,如图 5.30 所示;测试 mail 邮件服务器,如图 5.31 所示。

② 交互模式。

输入 nslookup 命令,不需要参数,就可以进入交互模式。任何一种模式都可以将参数传递给 nslookup,但在域名服务器出现故障时,大多使用交互模式。在交互模式下,可以在提示符>下输入 help 或?获得帮助信息,如图 5.32 所示;查找 DNS 区域信息,如图 5.33 所示。查找邮件服务器 记录信息,如图 5.34 所示;查找指针记录信息,如图 5.35 所示。查找别名记录信息,如图 5.36 所示;查找主机记录信息,如图 5.37 所示。使用 exit 命令,退出 nslookup 环境。





图 5.29 非交互模测试 DNS 服务器窗口

\>nslookup DNS1.abc.com	C:\>
务器: DNS1.abc.com	C:\>nslookup mail.abc.com
dress: 192.168.100.100	服务器: DNSL.abc.com
称: DNS1. abc. com	Address: 192.108.100.100
dress: 192. 168. 100. 100	名称: mail.abc.com
\lor	C:\>_

图 5.30 测试 DNS1 服务器

C:服Ad Ad

图 5.31 测试 mail 邮件服务器

::\/hstooxdp 默认服务器: server-01.abc.com \ddress: 192.168.100.100
前令: (标识付认大与表示,U 表示可选) KAME — 打印有关使用默认服务器的主机/域 NAME 的信息 KAMEI NAME2 — 同上,但将 NAME2 用作服务器
help or ?
all — 11月15版次、当則服务器和主机 [no]debug — 打印调试信息 [no]d2 — 打印详细的调试信息
[no]defname — 将域名附加到每个管询 [no]recurse — 询问查询的递归应答
[no]search - 使用環境系列表 [no]vc - 始終使用虚拟电路 domaji=NAMF - 海客社補安公署力 NAMF
srchlist=W1[/N2//N6] - 将说设置为 N1,并将搜索列表设置为 N1、N2 等 root=NAME - 将根服务器设置为 NAME
retry=X
vs、PTR、SOA 和 SRV) querytype=X - 与类型相同
class=X - 设置查词类(如 IN (Internet)和 ANY) [no]msxfr - 使用 NS 快速区域传送 ivfrve=W - 田王 IVEP 使浮揚式約当前版本
server NAME - 将默认服务器设置为 NAME,使用当前默认服务器 lserver NAME - 将默认服务器设置力 NAME,使用初始服务器
toot
_d _ 列田所有记录 _t TYPE _ 列出给定 RFC 记录类型(例如 A、CNAME、MX、NS 和 PTR 等)
印に求 ziew FILE
vnnv. abc. com
kdress: 192.168.100.100
名称: DNS1.abc.com Address: 192.168.100.100
)

图 5.32 nslookup 命令交互模式







图 5.35 查找指针记录信息

器: server-01.abc.com ess: 192.168.100.100 primary name server = server-01.abc.com responsible mail addr = hostmaster serial = 74 refresh = 900 (15 mins) retry = 600 (10 mins) 86400 (1 day) TL = 3600 (1 hour) TTT

图 5.34 查找邮件服务器记录信息

> set type=cna > www.abc.com 服务器: serve Address: 192.	ame er-01. abc. com 168. 100. 100	n		
www.abc.com >	canonical	name	Π	DNS1. abc. com

tvpe

图 5.36 查找别名记录信息

说明: set type 表示设置查找的类型。 set type=NS表示查找区域; set type=MX表示查找邮件服务器记录; set type=PTR 表示查找指针记录; exit set type=cname 表示查找别名记录; set type=A表示查找主机记录。

图 5.37 查找主机记录信息

168.100.100 server-01.

ress:

192.168.100.100

server-01. abc. com 192. 168. 100. 100

(3) 使用 ping 命令测试 DNS 服务器,如图 5.38 所示。



图 5.38 ping 命令测试 DNS 服务器

6. 管理 DNS 客户端缓存

可以使用 ipconfig 命令查看本地网卡相关信息,如 IP 地址、网关地址、物理 MAC 地址、DNS 地址等信息;也可以使用 ipconfig 命令来管理 DNS 客户端的缓存。

(1) 查看本地网卡相关信息,执行命令如下。

ipconfig /all

执行命令的结果如图 5.39 所示。 (2) 查看 DNS 客户端缓存,执行命令如下。

ipconfig /displaydns



::\>ipconfig /all
Vindows IP 配置
主机名 win10-user01 王 DNS 后缀 abc.com 节点类型
人太网道配益 EthernetU:
连接特定的 DNS 后缀 : 描述 : 加速 : 加速 : DHCP 已信用 : 1 : 00-0C-29-62-86-32 DHCP 已信用 : 1 :

图 5.39 查看本地网卡相关信息

执行命令的结果如图 5.40 所示。

C:\>ipconfig /displaydns	
Windows IP 配置	
_ldaptcp. default-first-site-namesites. dcmsdcs. abc. com	
记录名称::_ldaptcp.Default-First-Site-Namesites.dcmsdcs.abc. 记录类型:33 生存时间::317 数据长度:16 部分:答案 SRV 记录::答案 SRV 记录:319 100 389	Com
记录名称:server-01.abc.com 记录类型1 生存时间317 数据长度4 部分	
client.wns.windows.com	
记录名称	

图 5.40 查看 DNS 客户端缓存

(3) 清空 DNS 客户端缓存,执行命令如下。

ipconfig /flushdns

5.2.3 部署辅助 DNS 服务器

一个区域的辅助区域建立在该区域的辅助 DNS 服务器上。辅助区域的数据库文件是主要区域数据库文件的副本,需要定期地通过区域传输主要区域的备份以获得更新。辅助区域的主要作



用是均衡 DNS 解析的负载以提高解析效率,同时提供容错能力。必要时可以将辅助区域转换为 主要区域。辅助区域内的记录是只读的,不可以修改。

1. 项目规划

部署辅助 DNS 服务器网络拓扑结构图,如图 5.41 所示。



图 5.41 部署辅助 DNS 服务器网络拓扑结构图

(1) 在 DNS1 服务器上,首选 DNS: 192.168.100.100,备用 DNS: 192.168.100.101,建立 A 资源主机记录(FQDN 为 DNS2.abc.com,IP 地址为 192.168.100.101)。

(2) 在 DNS2 服务器上,首选 DNS: 192.168.100.101,备用 DNS: 192.168.100.100。

(3) 在 DNS2 服务器上建立一个辅助区域 abc. com,此区域内的记录是从其主服务器 DNS1 通过区域传递复制过来的。

2. 新建辅助区域(DNS2)

DNS2 上新建辅助区域,并设置让此区域从 DNS1 上复制区域记录,主要操作如下。

(1) 在 DNS2 上,选择"服务器管理器"→"添加角色和功能"选项,弹出"添加角色和功能向导" 窗口,勾选"DNS 服务器"复选框,按向导在 DNS2 服务器上完成 DNS 服务器的安装。

(2)在DNS2上,选择"服务器管理器"→"工具"→DNS选项,弹出"DNS管理器"窗口,右击 "正向查找区域"选项,在弹出的快捷菜单中选择"新建区域"选项,单击"下一步"按钮,弹出"区域 类型"对话框,如图 5.42 所示;在"区域类型"对话框中,选中"辅助区域"单选按钮,单击"下一步" 按钮,弹出"正向或反向查找区域"对话框,如图 5.43 所示。

(3) 在"正向或反向查找区域"对话框中,单击"下一步"按钮,弹出"区域名称"对话框,输入区域名称 abc. com,如图 5.44 所示;单击"下一步"按钮,弹出"主 DNS 服务器"对话框,在主服务器区域中,输入 IP 地址: 192.168.100.100(即主 DNS1 服务器的地址),如图 5.45 所示。

(4) 在"主 DNS 服务器"对话框中,单击"下一步"按钮,弹出"正在完成新建区域向导"对话框,如图 5.46 所示;单击"完成"按钮,返回"DNS 管理器"窗口,如图 5.47 所示。

(5) 重复步骤(2)~步骤(4),新建"反向查找区域"的辅助区域,操作步骤类似,这里不再赘述。 完成新建辅助区域的结果,如图 5.48 所示。

3. 确认 DNS1 是否允许区域传送

180

如果 DNS1 不允许将区域记录传送给 DNS2,那么 DNS2 向 DNS1 提出区域传送请求时会被

新建区域向导	×
区域类型 DNS 服务器支持不同类型的区域和存储。	
选择你要创建的区域的类型:	
○主要区域(P)	
创建一个可以直接在这个服务器上更新的区域副本。	
●辅助区域(S)	
创建一个存在于另一个服务器上的区域的副本。此选项帮助主服务器平衡处理 量,并提供容错。	的工作
○存根区域(U)	
创建只含有名称服务器(NS)。起始授权机构(SOA)和粘连主机(A)记录的区域的 有存根区域的服务器对该区域没有主管权。	副本。含
□ 在 Active Directory 中存储区域(只有 DNS 服务器是可写域控制器时才可用)(/	A)
< 上一步(B) 下一步(N) >	取消

图 5.42 "区域类型"对话框

確区域向导	
正向或反向查找区域	38
你可以使用区域进行正向或反向查找。	
选择你想创建的查找区域类型:	
●正向查找区域(F)	
正向查找区域将 DNS 名称转换为 IP 地址,并提供可用网络服务的信	息.
○ 后向書抄区端(R)	
又问重找达成将 IP 地址转换为 UN3 名称。	
< T-20	10.月

图 5.43 "正向或反向查找区域"对话框

拒绝。下面设置让 DNS1 允许区域传送给 DNS2,相关配置如下。

(1) 在 DNS1(server-01)上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器" 窗口,右击"正向查找区域"→abc.com 选项,在弹出的快捷菜单中选择"新建主机(A 或 AAA)"选 项,弹出"新建主机"对话框,如图 5.49 所示;输入名称和 IP 地址,单击"添加主机"按钮,返回 "DNS 管理器"窗口,可以看到 DNS2 添加主机完成,如图 5.50 所示。



新建区域向导
区域名称 新区域的名称是什么?
区域名称指定 DNS 命名空间的部分,该部分由此服务器管理。这可能是你组织单位的域名(例如, microsoft.com)或此域名的一部分(例如, newzone.microsoft.com)。区域名称不是 DNS服务器名称。
区域名称(Z):
abc.com
< 上一步(B) 下一步(N) > 取消

图 5.44 "区域名称"对话框

	NHJ OTTO MAJJARE JAJA		
主服务器: IP 地址	服务器 FQDN	已验证	删除(D)
<单击此处添加 IP 地址	或 DNS 名称>	1840	1 4000
W 192,108,100,100	server-ur.abc.com	WEAL	上核(U)
			下移(0)

图 5.45 "主 DNS 服务器"对话框



-	正在完成新建区域向导	
	你已成功完成了新建区域向导。你指定了	如下设置:
	名称: abc.com	^
	类型: 辅助区域	
	查找类型:前进	
	文件名: abc.com.dns	~
	注意:你应该现在将记录添加到区域,或 新。然后,你可以用 nslookup 验证名称	者确保记录得到动态更 %解析。
	要关闭此向导并创建新区域,请单击"完"	īč".

图 5.46 "正在完成新建区域向导"对话框

 ▲ DNS ▲ DNS2 ▲ 正向查找区域 > ● 反向查找区域 > ● 信任点 > ● 条件转发器 	.com \$	类型 辅助区域	状态 正在运行	DNSSEC 状态	密钥主机	

图 5.47 完成 abc. com 辅助 DNS 服务器配置

 ▲ DNS 管理器 文件(F) 操作(A) 查看(V) 報告 ◆ ● 22 million □ □ □ □ □ □ 	b(H)			- 0	×
 ◎ DNS > ◎ DNS2 > ◎ 正向查找区域 > ◎ 反向查找区域 > ◎ 信任点 > ◎ 余件转发器 	名称 副 100.168.192.in-addr.arpa	类型 辅助区域	状态 正在运行	DNSSEC ≵	怸
	<				3

图 5.48 完成"反向查找区域"的辅助区域



Windows Server 2019网络管理项目教程(微课视频版)

新建主机	×
名称(如果为空则使用其父域名称	5)(N):
DNS2	
完全限定的域名(FQDN):	
DNS2.abc.com.	
IP 地址(P):	
192.168.100.101	
□ 创建相关的指针(PTR)记录(C)	
□ 允许所有经过身份验证的用户 录(Q)	用相同的所有者名称来更新 DNS 记
	添加主机(出) 取消

图 5.49 "新建主机"对话框

• • 2 🖬 🗙 🖬 🕒				
DNS SERVER-01 → 正向查找区域 > ③msdcs.abc.com > ③abc.com > ③abc.com > ③xz.com > ◎反向查找区域	名称 msdcs sites tcp udp DomainDnsZones ForestDnsZones	英型		时间歇
> 🔝 信任点 > 🔛 条件转发器	 □(与父文件夹相同) □(与父文件夹相同) □(与父文件夹相同) □(与父文件夹相同) □(DNS1 □ mail □ server-01 □ www □DNS2 	起始授权机构(SOA) 名称服务器(NS) 主机(A) 主机(A) 邮件交換器(MX) 主机(A) 則名(CNAME) 主机(A)	[28], server-01.abc.com server-01.abc.com. 192.168.100.100 [10] DNS1.abc.com. 192.168.100.100 DNS1.abc.com. 192.168.100.101	静态 静态 2022/2/21 11:00:00 静态 静态 静态

图 5.50 DNS2 添加主机完成窗口

(2)在DNS1(server-01)上,选择"服务器管理器"→"工具"→DNS选项,弹出"DNS管理器" 窗口选择"正向查找区域"→abc.com选项,在弹出的快捷菜单中选择"属性"选项,弹出"abc.com 属性"对话框,如图 5.51 所示;在"abc.com 属性"对话框中,选择"区域传送"选项卡,勾选"允许区 域传送"复选框,选中"只允许到下列服务器"单选按钮,单击"编辑"按钮,弹出"允许区域传送"对 话框,在"辅助服务器 IP 地址"区域,输入 IP 地址: 192.168.100.101,如图 5.52 所示。

(3) 在"允许区域传送"对话框中,单击"确定"按钮,返回"abc. com 属性"对话框,如图 5.53 所示; 在"abc. com 属性"对话框中,单击"确定"按钮,返回"DNS 管理器"窗口。

(4) 在 DNS2 上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口,单击 "正向查找区域"→abc. com 选项,可以看到在 DNS2 服务器上,已经把 DNS1 区域信息传送过来 了。此时,DNS1 与 DNS2 服务器区域信息是一致的,如图 5.54 所示。



图 5.52 "允许区域传送"对话框

区域的	步送将区域的副本发送到请求副本	的服务器。				Ι.	1.1+ T 1+ 1+ 1+			
日光	午区域传送(<u>Q</u>):						元计达和特达			
C)到所有服务器(I)						DNS 区域(Z):			
0	口有在"久众服冬器"洗顶卡中列	出於服务器	(5)				abc.com			
) 只允许到下列服务器(出)	4430673 H	œ				辅助服务器的 IP 地址	(5):		
	ID Http:	B2.55.5					IP 地址	服务器 FQDN	已验证	新新考(D)
			a record		- 1		192.168.100.101			
										上移山
										下修(0)
				编辑	(E)					
3	指定辅助服务器接收区域更新通知	0, 清单击	通知"。	() (1)	N					
				ARAN (<u> </u>					

图 5.51 "abc. com 属性"对话框

50.001	n 雇性				?	×
常规	起始授权机构(SOA)	名称服务器	WINS	区域传送	安全	
区域	传送将区域的副本发送到	则请求副本的服	段 器。			
₩	许区域传送(0):					
()到所有服务器(1)					
()只有在"名称服务器"边	顿卡中列出的	的服务器(<u>S)</u>		
() 只允许到下列服务器(H)				
	IP 地址		服务器	FQDN		
	192.168.100.101		-			
		111 - Wi	UNS2			
			DNS2		编辑低)
			UNS2		编辑(E)
tan t	更指定辅助服务器接收区	(城更新通知,	JNS2 请单击")	直知"。	编辑(E)

图 5.53 "abc. com 属性"对话框



文件(E) 操作(A) 查看(A)) #助山)			
 DNS DNS2 正向查找区域 页向查找区域 信任点 新件转发器 	各称 msdcs sites tcp udp DomainDnsZones ForestDnsZones	英型	数据	时间戳
	□ (与父文件夹相同) □ (与父文件夹相同)	起始授权机构(SOA) 名称服务器(NS)	[31], server-01.abc.c server-01.abc.com.	静态 静态
	(与父文件夹相同)	主机(A)	192.168.100.100	静态
	DNS1	主机(A)	192.168.100.100	静态
	DNS2	主机(A)	192.168.100.101	静态
	mail	邮件交换器(MX)	[10] DNS1.abc.com.	静态
	server-01	主机(A)	192.168.100.100	静态
	D www	别名(CNAME)	DNS1.abc.com	静木

图 5.54 DNS2 完成区域信息传送窗口

5.2.4 部署存根 DNS 服务器

一个区域的存根区域类似于辅助区域,也是主要区域的只读副本,但存根区域只从主要区域 中复制名称服务器(Name Server, NS)记录、初始授权(Start Of Authority, SOA)记录、主机 (Address, A)记录的副本,而不是所有的区域数据库信息。

存根区域的 NS、SOA 与 A 资源记录是从其主服务器(此区域的授权服务器)复制过来的,当 主服务器内的这些记录发生变化时,它们通过区域转送的方式复制过来。存根区域的区域转送只 会传送 NS、SOA 与 A 资源记录。其中 A 资源记录用来记载授权服务器的 IP 地址,此 A 资源记 录需要跟随 NS 记录一并被复制到存根区域,否则拥有存根区域的服务器无法解析到授权服务器 的 IP 地址。当有 DNS 客户端查询(查询模式为递归查询)存根区域内的资源记录时,DNS 服务器 会利用区域内的 NS 记录得知此区域的授权服务器,然后向授权服务器查询(查询模式为迭代查 询)。如果无法从存根区域内找到此区域的授权服务器,那么 DNS 服务器会采用标准方式向根 (Root)查询。

1. 项目规划

部署存根 DNS 服务器网络拓扑结构图,如图 5.55 所示。

(1) 在 DNS1 服务器上,首选 DNS: 192.168.100.100,备用 DNS: 192.168.100.101,建立 A 资源主机记录(FQDN 为 DNS2.abc.com,IP 地址为 192.168.100.101)。

(2) 在 DNS2 服务器上,首选 DNS: 192.168.100.101,备用 DNS: 192.168.100.100。

(3)在 DNS2 服务器上建立一个正反向存根区域 abc. com,并将此区域的查询请求转发给此 区域的授权服务器 DNS1 来处理。存根区域内的记录是从其主服务器 DNS1 通过区域传递复制 过来的。

2. 新建存根区域(DNS2)

DNS2 上新建存根区域,并设置让此区域从 DNS1(此区域的授权服务器)上复制区域记录。





图 5.55 部署存根 DNS 服务器网络拓扑结构图

(1) 在 DNS2 上,选择"服务器管理器"→"添加角色和功能"选项,弹出"添加角色和功能向导" 窗口,勾选"DNS 服务器"复选框,按向导提示在 DNS2 服务器上完成 DNS 服务器的安装。

(2) 在 DNS2 上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口,右击 "正向查找区域"选项,在弹出的快捷菜单中选择"新建区域"选项,单击"下一步"按钮,弹出"区域 类型"对话框,如图 5.56 所示;在"区域类型"对话框中,选中"存根区域"单选按钮,单击"下一步" 按钮,弹出"区域名称"对话框,如图 5.57 所示。

新建区域向导	×
区域类型 DNS 服务器支持不同类型的区域和存储。	
选择你要创建的区域的类型:	
○主要区域(P)	
创建一个可以直接在这个服务器上更新的区域副本。	
○辅助区域(<u>S</u>)	
创建一个存在于另一个服务器上的区域的副本。此选项帮助主服务器平衡处理的工作 员,社理研究性	
● 存根区域(U)	
创建只含有名称服务器(NS)、起始授权机构(SOA)和粘连主机(A)记录的区域的副本。 有存根区域的服务器对该区域没有主管权。	ŝ
一在 Active Directory 中存储区域(只有 DNS 服务器是可写域控制器时才可用)(A)	
< 上一步(<u>B</u>) 下一步(<u>N</u>) > 国	Cilli

图 5.56 "区域类型"对话框

(3) 在"区域名称"对话框中,输入区域名称 abc. com,单击"下一步"按钮,弹出"区域文件"对 话框,如图 5.58 所示;选中"创建新文件、文件名为"单选按钮,单击"下一步"按钮,弹出"主 DNS



建区域向导	×
区域名称 新区域的名称是什么?	
区域名称描定 DNS 命名空间的音如,microsoft.com)或此域名的服务器名称。	时分,该部分由此服务器管理。这可能是你组织单位的域名(例 一部分(例如,newzone.microsoft.com)。区域名称不是 DNS
区域名称(乙):	
abc.com	

图 5.57 "区域名称"对话框

服务器"对话框,输入主服务器地址,如图 5.59 所示。

新建区域向导	×
区域文件 你可以创建一个新区域文件和使用从另一个 DNS 服务器复制的文件。	
你想创建一个新的区域文件,还是使用一个从另一个 DNS 服务器复制的现存文	件?
创建新文件,文件名为(C):	
abc.com.dns	
○使用此现存文件(型):	
要使用此现存文件,请确认它已经被复制到该服务器上的 %SystemRoot%\system32\dns 文件夹,然后单击"下一步"。	
< 上一步(B) 下一步(N) >	取消

图 5.58 "区域文件"对话框

(4) 在"主 DNS 服务器"对话框中,单击"下一步"按钮,弹出"正在完成新建区域向导"对话框,如图 5.60 所示;单击"下一步"按钮,返回"DNS 管理器"窗口,完成存根区域创建,如图 5.61 所示。



着定你要从中加载区域。 問い及転法 A 法通行寻	的 DNS 服务器。通过音	间 SOA 资源记录。	区域根处的 NS 资源词
килх 和建 А 页原记录 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 - 1825 -	ロンピス化士りはなみず新川山気が	TRLAN.	
IP 地址	服务器 FQDN	已验证	删除(<u>D</u>)
<单击此处添加 IP 地址	止或 DNS 名称>		
192.168.100.100	server-01.abc.com	确定	上移(U)
			下移(Q)

图 5.59 "主 DNS 服务器"对话框

新建区域向导		3
	正在完成新建区域向导	
	你已成功完成了新建区域向导。你指定了如下	7设置:
	名称: abc.com	^
	类型:存根区域	
	查找类型: 前进	
	文件名: abc.com.dns	~
	注意:你应该现在将记录添加到区域,或者确新。然后,你可以用 nslookup 验证名称解析	保记录得到动态更 f.
	要关闭此向导并创建新区域,请单击"完成"。	
	< 上一步(B) 完成	取消

图 5.60 "正在完成新建区域向导"对话框



▲ DNS 管理器 文件(E) 操作(A) 查看(V) 帮助(H) ◆ ◆ 2 (E) × (E) → (E) (E) (E)	108		-		×
 ▲ DNS ◆ 圓 DNS2 > □ 正向重抗区域 	名称 (与父文件夹相同) (与父文件夹相同)	类型 起始授权机构(SOA) 名称服务器(NS)	数据 [31], server-01.abc.com server-01.abc.com.	时间戦 静志 静志	
 ○ abc.com > ○ 反向置抗区域 > ○ 100.168.192.in-addr.arpa ○ 信任点 > ○ 条件转发器 	server-01	主切(A)	192.168.100.100	静态	

图 5.61 完成存根区域创建窗口

3. 确认 DNS1 是否允许区域传送

如果 DNS1 不允许将区域记录传送给 DNS2,那么 DNS2 向 DNS1 提出区域传送请求时会被 拒绝。下面设置让 DNS1 允许区域传送给 DNS2,相关配置如下。

(1)在DNS1(server-01)上,"DNS管理器"窗口中选择"正向查找区域"→abc.com选项,在弹出的快捷菜单中选择"属性"选项,弹出"abc.com属性"对话框,在"abc.com属性"对话框中,选择 "区域传送"选项卡,勾选"允许区域传送"复选框,选中"只允许到下列服务器"单选按钮,单击"编辑"按钮,弹出"允许区域传送"对话框,在"辅助服务器 IP 地址"区域,输入 IP 地址: 192.168.100.101 (即 DNS2 服务器的 IP 地址)。

(2) 类似地,右击"反向查找区域"选项,添加反向查找区域 100.168.192.addr.arpa,在弹出的 快捷菜单中选择"属性"选项,重复以上操作,这里不再赘述。设置让 DNS1 可以将反向查找区域 的记录通过区域传送复制给 DNS2。

如果确定所有配置都正确,但一直看不到这些记录;请单击区域 abc. com 后按 F5 键执行刷 新操作;如查仍然看不到,可以将"DNS 管理器"控制台关闭再重新打开。

存根区域的 DNS 服务器默认每隔 15 分钟自动请求其主服务器执行区域传送的操作;也可以选中存根区域后右击,在弹出的快捷菜单中选择"从主服务器传输"或"从主服务器传送区域的新副本"选项,选择手动要求执行区域传送的操作,不过它只会传送 NS、SOA 与记载着授权服务器 IP 地址的 A 资源记录。

5.2.5 部署委派 DNS 服务器

DNS名称解析是通过分布式结构来管理和实现的,它允许将 DNS 名称空间根据层次结构分 割成一个或多个区域,并将这些区域委派给不同的 DNS 服务器进行管理。例如,某区域的 DNS 服务器(以下称"委派服务器")可以将其子域委派给另一台 DNS 服务器(以下称"受委派服务器") 全权管理,由受委派服务器维护该子域的数据库,并负责响应针对该子域的名称解析请求。而委 派服务器则无须进行任何针对该子域的管理工作,也无须保存该子域的数据库,只需要保留到达 受委派服务器的指向,即当 DNS 客户端请求解析该子域的名称时,委派服务器将无法直接响应该 请求,但其明确知道应该由哪个 DNS 服务器(即受委派服务器)来响应该请求。

采用区域委派可有效地均衡负载。将子域的管理和解析任务分配到各个受委派服务器,可以 大幅降低父级域或顶级域服务器的负载任务,提高解析效率。同时,这种分布式结构使得真正提



供解析的受委派服务器更接近于客户端,从而减少了带宽资源的浪费。部署区域委派需要在委派 服务器和受委派服务器中都进行必要的配置。

1. 项目规划

部署委派 DNS 服务器网络拓扑结构图,如图 5.62 所示。



图 5.62 部署委派 DNS 服务器网络拓扑结构图

(1) 在 DNS1 服务器上,首选 DNS: 192.168.100.100,备用 DNS: 192.168.100.101,建立 A 资源主机记录(FQDN 为 DNS2.abc.com,IP 地址为 192.168.100.101)。

(2) 在 DNS2 服务器上,首选 DNS: 192.168.100.101,备用 DNS: 192.168.100.100,建立 A 资源主机记录(FQDN 为 DNS2.abc.com,IP 地址为 192.168.100.101)。

(3) 将 DNS2 服务器升级为域控制器,安装 Active Directory 域服务,父域为 abc. com,子域控 制域为 lncc. abc. com。

2. 配置受委派服务器(DNS2)

在受委派 DNS 服务器 DNS2 上创建主区域 lncc. abc. com,并且在该域中创建资源记录,然后 在委派 DNS 服务器 DNS1 上创建委派域 lncc,具体配置步骤如下。

(1) 在 DNS2 上,选择"服务器管理器"→"添加角色和功能"选项,弹出"添加角色和功能向导" 对话框,勾选"DNS 服务器"复选框,按向导在 DNS2 服务器上完成 DNS 服务器的安装。

(2)在 DNS2 上,选择"服务器管理器"→"工具"→DNS 选项,弹出"DNS 管理器"窗口,右击 "正向查找区域"选项,在弹出的快捷菜单中选择"新建区域"选项,弹出"新建区域向导"对话框,单 击"下一步"按钮,弹出"区域类型"对话框,如图 5.63 所示;在"区域类型"对话框中,选中"主要区 域"单选按钮,单击"下一步"按钮,弹出"区域名称"对话框,如图 5.64 所示。

(3) 在"新建区域向导"对话框中,连续单击"下一步"按钮,最后单击"完成"按钮,创建区域完成后,新建资源记录,如建立主机 client. lncc. abc. com,对应的 IP 地址: 192.168.100.10; DNS2. lncc. abc. com 对应的 IP 地址: 192.168.100.101。

(4) 创建反向主要区域 100.168.192. in-addr. arpa, 如图 5.65 所示。

(5)将 DNS2 升级为子域控制器。需要说明的是,将 DNS2 升级为子域控制器在部署委派域 时并不是必需的步骤。在 DNS2 上安装 Active Directory 域服务,在安装过程中,选择"将新域添加



新建区域向导	×
区域类型 DNS 服务器支持不同类型的区域和存储。	
选择你要创建的区域的类型:	
●主要区域(P)	
创建一个可以直接在这个服务器上更新的区域副本。	
○ 辅助区域(5)	
创建一个存在于另一个服务器上的区域的副本。此选项帮助主服务器平衡处理的工作 量、并提供容错。	
○存根区域①	
创建只含有名称服务器(NS)、起始授权机构(SOA)和粘连主机(A)记录的区域的副本。含有存根区域的服务器对该区域没有主管权。	
一在 Active Directory 中存储区域(只有 DNS 服务器是可写域控制器时才可用)(A)	
< 上一步(B) 下一步(D) > 取	Ä

图 5.63 "区域类型"对话框

SALE C	《城向导	×
E	8名称 新区域的名称是什么?	
	区域名称描定 DNS 命名空间的部分,该部分由此服务器管理。这可能 如,microsoft.com)或此域名的一部分(例如,newzone.microsoft.co 服务器名称。	還你追訳单位的域名(例 om),区域名称不是 DNS
	区域名称(Z): Incc.abc.com	

图 5.64 "区域名称"对话框

▲ DNS 管理器 文件(P)操作(A)查看(V)帮助(H) ◆ ◆ ▲ 100 米 100 @ ■ 120 0			- 0	×
 ▲ DNS > ■ DNS2 > ■ 正向査找区域 ※ 回 反向査找区域 ※ 回 反向查找区域 ③ 100.168.192.in-addr.arpa > ■ 信任点 > ■ 条件转发器 	名称 (与父文件共相同) (与父文件共相同) DNS2 client	荷型 起始授权机构(SO 名称級务欄(NS) 主机(A) 主机(A)	数据 [1], dns2, hostmast dns2. 192.168.100.101 192.168.100.10	er.

图 5.65 DNS2 管理器设置完成后的界面



到现有林"单选按钮,选择域类型为"子域",父域为 abc. com,子域为 lncc,完成安装后,计算机自动 重启。至此,DNS2 成功升级为子域 lncc. abc. com 的域控制器。

(6)在 DNS1上,选择"服务器管理器"→"工具"→DNS选项,弹出"DNS管理器"窗口,右击
"正向查找区域"选项,在弹出的快捷菜单中选择"新建委派"选项,弹出"新建委派向导"对话框,如图 5.66 所示;单击"下一步"按钮,弹出"受委派域名"对话框,如图 5.67 所示。

新建委派向导		>
	欢迎使用新建委派向导	
	此向导会帮助你在此 DNS 服务器或另一个 DNS 服务器上, 为一个子城委派授权机构到一个不同的区域。区域委派有助于 简化管理。	
	单击"下一步"继续。	
	< 上一步(B) 下一步(N) > 取満	

图 5.66 "新建委派向导"对话框

受派域名 你提供的 DNS 域的授权机构将被委派到不同的区域。	
指定要委派的 DNS 域的名称。	
委派的域(D):	
Incc	
Incc.abc.com	

图 5.67 "受委派域名"对话框



(7) 在"受委派域名"对话框中,输入委派的域,单击"下一步"按钮,弹出"名称服务器"对话框,如图 5.68 所示;单击"添加"按钮,弹出"新建名称服务器记录"对话框,如图 5.69 所示。

指定你想要主持此委派的区域的 DNS 服务	器的名称和 IP 地址。	
名称服务器(S): 服务器先全限定的域名(FQDN)	IP 地址	
添加(A) 编辑(E) 翻	₿®	

图 5.68 "名称服务器"对话框

各器索全限完的域名(FODN)(S)·		
NS2.Incc.abc.com		解析®
NS 记录的 IP 地址(A):		
P 地址	已验证	删除(<u>D</u>)
单击此处添加 IP 地址>		
9 192.168.100.101	确定	上移(山)
		下移(Q)

图 5.69 "新建名称服务器记录"对话框

(8) 在"新建名称服务器记录"对话框中,输入服务器完全限定的域名,在"此NS记录的IP地址"区域,输入IP地址: 192.168.100.101(即DNS2服务器的地址),单击"确定"按钮,返回"名称





(9) 在"正在完成新建委派向导"对话框中,单击"完成"按钮,返回"DNS管理器"窗口,可以查

	< 上一步(<u>8</u>) 完成	取消
图 5.71	"正在完成新建委派向导"对话框	

102	为留元主限在印刷	A(FQUIN)		IP ABAE	
D	NS2.Incc.abc.co	n.		[192.168.100.10	1]
	添加(<u>A</u>)	编辑(E)	删除(B) <上一步(B)	下-步四 >	取消
		图 5.70 "	'名称服务器"对	话框	
新建委	派向导				×

正在完成新建委派向导

已指定下列设置: 名称:

你已成功完成了新建委派向导。

Incc.abc.com

要关闭此向导并创建委派,请单击"完成"。

尔可以选择一个或多个主持受委派区域的名称服务	
指定你想要主持此委派的区域的 DNS 服务器的名	5称和 IP 地址。
名称服务器(S):	
服务器完全限定的域名(FQDN)	IP 地址
DNS2.Incc.abc.com.	[192.168.100.101]

服务器"对话框,如图 5.70 所示; 单击"下一步"按钮,弹出"正在完成新建委派向导"对话框,如 图 5.71 所示。

看刚刚创建的受委派 DNS 服务器选项,如图 5.72 所示。

盖 DNS 管理器 文件(E) 操作(A) 查看(V) 解出	0HD			-	×
← → 2 🗊 🗙 🖬 🖻 🖻	2				
 ▲ DNS ✓ Im Enjegi/Zxit > Im Im Enjegi/Zxit > Im schc.com > Im schc.schc.com > Im schc.schc.schc.schc.schc.schc.schc.schc	名称 (与父文件夹相同)	类型 名称服务器(NS)	数据 DNS2Jncc.abc.com.	R3(B)	

图 5.72 受委派 DNS 服务器的界面

(10)使用具有管理员权限的用户账户客户端 Win10-user01,首选 DNS 服务器的 IP 地址设置为 192.168.100.100,使用 nslookup 命令进行测试 DSN2.lncc.abc.com、client.lncc.abc.com。如 果成功,说明 IP 地址为 192.168.100.100(DNS1 服务器)的服务器到 IP 地址为 192.168.100.101 (DNS2 服务器)的服务器委派成功,如图 5.73 所示。

C:\>nsloo	okup DNS2. 1ncc. abc. com
服务器:	UnKnown
Address:	192. 168. 100. 101
名称:	DNS2. 1ncc. abc. com
Address:	192. 168. 100. 101
C:\>nslo	okup client. Incc. abc. com
服务器:	UnKnown
Address:	192, 168, 100, 101
名称:	client.lncc.abc.com
Address:	192.168.100.10
C:\>	

图 5.73 测试委派 DNS 服务器成功



1. 选择题

(1) 域名系统 DNS 排	是供了一个()命名方案。	
A. 分级	B. 分组	C. 分层	D. 多层



(2)顶级域中表示商业机构]组织的是()。		
A. edu	B. com	C. net	D. org
(3)顶级域中表示教育、学	术研究单位组织的是((),	
A. edu	B. com	C. net	D. org
(4) 顶级域中表示网络服务	机构组织的是()	0	
A. edu	B. com	C. net	D. org
(5)在 DNS 域名空间中, 最	上面一层被称为"根 [」]	或",用()表示。	
A. *	B. !	C. &.	D
(6) 在 Windows Server 20	19 的 DNS 服务器上7	不可以新建的区域类型	[有()。
A. 主要区域]	B. 辅助区域	C. 存根区域	D. 转换区域
(7) 下面表示全限定域名的]是()。		
A. SOA	B. NS	C. FQDN	D. PTR
(8) 下面表示邮件交换器的]是()。		
A. CNAME	B. MX	C. NS	D. FQDN
(9) 下面表示名称服务器的]是()。		
A. SOA	B. NS	C. FQDN	D. PTR
(10) 下面表示别名的是()。		
A. CNAME	B. MX	C. NS	D. FQDN
(11) 下面表示指针记录的;	是()。		
A. SOA	B. NS	C. FQDN	D. PTR
(12) 下面表示主机记录的;	是()。		
A. CNAME	B. MX	С. А	D. NS
2. 简答题			

- (1) 简述根域和顶级域。
- (2) 简述 DNS 的工作原理。
- (3) 简述 DNS 服务器的类型。

