第11章　配置Windows DNS服务器

本章讨论安装和配置Windows 2000 DNS服务器。有一些讨论是关于何时和为什么应该使用或不使用不同的特征的讨论，但重点在于，在假设对 DNS服务器的设计和计划已经完成的前提下逐步了解DNS服务器。

本章内容包括：

- 预备知识。给预备阶段提供一个简短的提示，这将使安装 DNS服务更直接。
- 安装Windows DNS 服务器。介绍在Windows 2000上安装DNS的步骤。
- 配置DNS服务器。介绍服务器的属性
- 域区、子域和手工创建资源记录。简单地介绍如何使用本地服务器。
- 活动目录集成。介绍使用活动目录存储的设置和影响。
- 服务器类型。介绍如何配置与其他服务器的联系。
- 清理域区。简单地讨论清理问题。
- 支持特点。指出一些方法来帮助管理和理解服务器的操作。

本章建立在以前章节中提供的信息的基础上，并提供进一步的讨论。 DNS是目前最流行的名字空间管理服务器。Windows 2000把DNS放到一个更重要的位置， DNS在Windows 2000中比在以前任何的Windows版本中更重要。

最初，使用DNS服务的主要原因之一仅仅是为了让一个用户或一个管理员更容易地独自标识他的系统。开始使用 DNS是因为旧方法（一个单独的 HOST.TXT文件）已经太大了，而且找一个机器名也变得更困难，效率也更低。在 DNS以前， HOST.TXT文件方法有一个非层次的名字空间，因此，一个特定的名字只能有一台主机，因此大家很快采用了新的 DNS命名方法。

假设在几个不同的子网上有300个未命名的机器，你将很快懂得为什么名字服务的意义如此重大。就象在没有任何电话本的情况下记住 300个电话号码。今天，很多服务完全希望而且有的确实需要一个名字，因此，需要在逻辑上有一个名字空间管理工具。

假设在一个分布安全的、客户 /服务器环境中有300个复杂的客户系统，每一个都要定位和访问资源。假设资源时有时无，可用时通告它们的存在，不可用时就取消。下面将开始介绍中心DNS服务是怎样用于新的Windows结构的。

11.1　预备知识

到此为止，你应该对你的网络和对网络的设计目标有一个很清楚的理解了，也应该有了自己的活动目录结构。它在逻辑上由名字空间边界决定，在物理上由服务器的位置和那些服务器上的域区授权映射。配置微软 DNS服务器很简单，安装如此简单以至于你可能会怀疑它的可靠性。但它确实不是骗人的，如果不能正确的设计或安装，就必须重装，如果比较幸运，第二次就可以装好，否则就得修补一下错误了。

你应该不仅较多地了解你的网络和目标，还要知道可连接性以及给你带来的影响等。原

因非常多，但有些是因为使用防火墙、特殊桥和 /或路由网络、远程节点连接、客户负载和访问模式而引起的。现在你还需要了解的其他领域包括是否和在哪儿使用活动目录，是否使用动态DNS，怎样配置它们。

本章面向的读者是那些已经准备好了。已经有了明确计划的人。本章讲述了在未受限制的网络访问的环境中如何建立Windows 2000 DNS，而无论与Internet是全部连接或者只连接部分的内部节点。在计划和设计时应考虑的问题、名字空间的保护等已在第 7章、第9章和第10章中讨论过了。你将要遇到或已遇到的最大困难是，在授权方面如何设计适合于自己的域，以及服务器和域区的放置问题。在此，你必须在头脑中完全清楚每个服务器和客户应放在网络的什么位置，而不仅是大致的想一下。

下面开始介绍安装DNS。

11.2 安装windows DNS服务器

如果windows 2000中的东西都已成了无意识的经验，那就只剩安装不同种类的网络服务了。安装如此简单，以至于你会错误地认为运行这些服务也一样简单。尽管不难，但运行安装程序也需要很好的理解所安装的东西，或者说需要一个配置很好的安装。

前提与安装大部分服务软件类似，需要安装好 Windows 2000服务器并配置好TCP/IP协议。如果此服务器还没有使用指定的 IP地址，应该立即启用。主机名应该是稳定的，主机名已广播给用户后，改变主机名或 IP地址都很麻烦，也很困难，需要以有管理特权的用户登录。除此以外，就不再需要考虑太多其他的了。软件本身很小，并且已选定了合适的服务器。选定的服务器最好有足够的内存，因为为了提高性能， DNS将希望利用你的RAM缓存它的数据库。这当然与域区大小相关，就像在启动分区上需要的存储空间一样；或者说如果使用活动目录存储时， NTDS.DIT存储的地方。

11.2.1 安装步骤

如前所述， DNS服务器的安装过程与其他网络服务的安装过程非常相似，实际的困难在于安装以后的配置。图 11-1显示了网络组件配置对话框，有一个简单的复选框控制 DNS的安

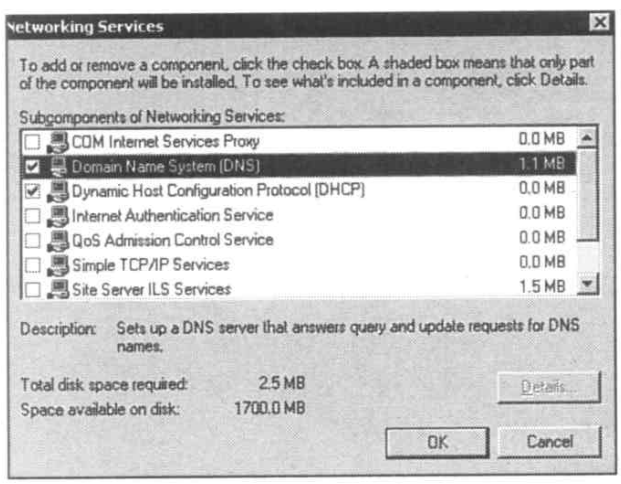

图11-1 在网络组件对话框中选择DNS

装，可以使用服务器配置向导（Configure Your Server Wizard）来配置你的服务器，也可使用以下步骤：

DNS服务器服务的一个必要条件 任何运行DNS服务器服务的机器必须有一个指定的IP地址，应该选择好机器名和地址，以后尽量不要改变。

1) 打开控制面板。

2) 启动“ Add /Remove Programs（添加/删除程序）” 窗口。

3) 单击右边的“ Add/Remove Windows Components（添加/删除Windows组件）” 图标，启动“ Windows Component Wizard（窗口组件向导）”。

4) 选择“ Networking Services（网络服务）”。

5) 单击“ Details（详细）” 按钮，弹出“ Networking Services（网络服务）” 列表。

6) 向下滚动，选中“ Domain Name System（DNS）（域名服务系统）” 旁边的复选框。

7) 至此，使用“ Next（下一步）” 和/或“ Finish（完成）” 按钮，结束窗口组件向导的执行，具体的选择取决于向导中是否还选择了其他选项。

因为Windows 2000中有很多功能，你可以用几种方式来操纵接口。这种情况下，可以用下面一种更快的方法来代替前面的步骤1到步骤3：

1) 使用“ My Network Places（我的网络位置）” 的菜单（单击右键），并选择“ Properties（属性）”，这就打开了一个“ Explorer（浏览器）” 窗口，标在“ Network and Dial-up Comation（网络和拨号连接）” 上。

2) 在主菜单条中，打开“ Advanced（高级的）” 的下拉菜单并选择“ Optional Networking Components（选择网络组件）”。

安装好DNS以后，工作就可以开始了。如果你安装了一个仅用于缓存的服务器，你的工作就差不多完成了。

刚才发生了什么？当然， DNS服务器已安装好，现在应该运行了。但还有很多其他事情，在“ start（开始）” 菜单中添了一个新选项，并注册在微软管理控制台的快捷方式中，你现在的%Windir%\system32\dns中有一个子目录结构，这是DNS服务器的缺省文件存放位置。并且，现在的注册表中有关于DNS服务器的信息，存储在HKLM\System\Current Control SetServices\DNS中。最后，有一些新的计数器加载到系统监视器中，而且，在屏幕后对你的系统可能还有很多其他的调整。

11.2.2 DNS服务器管理控制台

首先，需要访问的主要工具是DNS服务器管理控制台，可以在Start菜单的“ Administrative Tool-folder（管理工具文件夹）” 中找到它。只要找到 DNS选择项就可以了，也可以从“ Run（运行）” 或使用命令行“ dnsmgmt.msc ” 启动它。尽管不能忽视用于脚本管理的DNSCMD.EXE，但对于大部分DNS管理来说，这是一个基本的工具（参见第12章和第13章）。

在一个管理控制台中可以管理很多 DNS服务器。这些服务器可以是一个在本地，其他都是远程，也可以全部都是远程。如果在你的工作站（或者专业工作站）上安装了 Windows 2000管理工具，则可以管理远程管理这些服务。可以在 Windows 2000服务器版CD的“ \:386 ” 目录，也可以在安装服务器的“ %windir%\system32 ” 上找到ADMINPAK.MSI，然后把它安装到管理机器上。

为便于管理，需要给DNS服务器注册。首先，单击最顶层的 DNS节点，然后可以使用该节点的上下文菜单也可以使用“ Action（动作）”菜单，并选择“ Connect to Computer（连接到计算机）”。你可能发现，管理控制台一开始有一点不稳定。注意，机器的动作对于工具的焦点很敏感。要先点击一个节点，使它在右边扩展，然后就可以得到新焦点的相应菜单。

打开DNS管理控制台，选择“ View ”菜单。在“ View ”菜单中，如果想调整“ Custom（定制）”选项，首先要单击“ Advanced ”在其中启用显示扩展菜单。使用这种“ Advanced View ”模式，还可以在最新的可见节点“ Cached lookups（缓存查找）”中检查缓存记录。

两种更流行的访问 DNS管理界面的方法是使用定制控制台和计算机管理控制台，第一种方法必须自己创建，为了访问第二种方法，可以使用“ My Computer ” 的上下文菜单并选择“ Manage ”，也可以使用“ RUN ”来激活Compmgmt.msc。在控制台打开时，可以在“ Services and Applications（服务和应用）”节点中找到DNS，管理控制台可以方便的收集“ Event(事件) ”访问日志和相关服务，比如把DHCP、WINS、和DNS收集到一个独立的接口中。

在运用自如以前，应该先熟悉管理界面。我们将要看一下 DNS的特点，但首先要注意几个转换和命令。看一下图11-2，此图显示了服务器节点的上下文菜单。

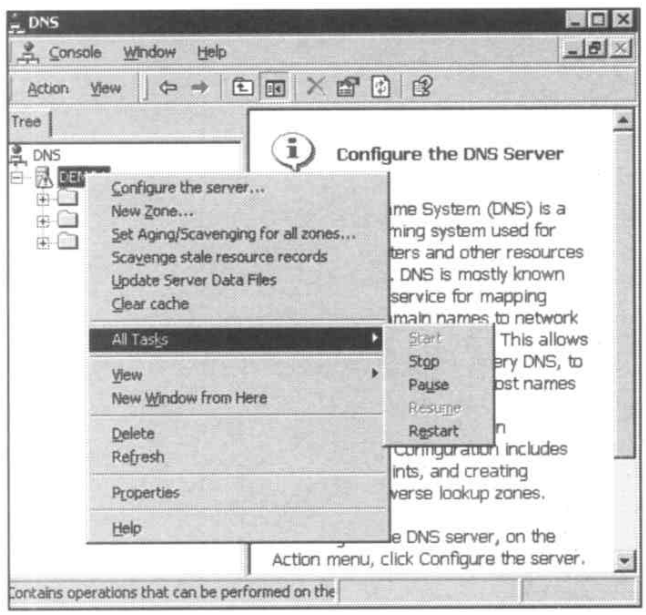

图11-2 一个服务器节点的DNS服务器菜单

“ All Tasks（所有任务）”选项已扩展，显示的服务器功能有“ stop ”、 “ start ”、“ Pause ”、“ Resume ”。在主列表中，“ clear cache ”选项可以清除DNS缓存解析器的缓存。由于Windows 2000 DNS服务器实现了NCACHE规范，所以可能需要更多的刷新缓存，特别是在预配置测试环境中这种需要更多。在此菜单中“ Update Server Data Files ”选项可永久存储配置和域区数据，以确保数据的内存版本与存储版本一致。应该注意到与清理相关的两个选项，“ Set Aging/Scavenging for All Zones ”和 ” Scavenge Stale Resource Records ”表明只要有可能，控制台就支持动态DNS。“ Configure the Server ”选项引出一个向导（以后讨论）。在我们介绍完服务器配置选项后，将首先介绍隐含在“ New Zone ”选项中的关于域区创建的主题。

11.3 DNS服务器配置

在进一步讨论之前应首先熟悉一下 Windows 2000 DNS服务的服务器级控制，图 11-3展示了DNS服务器的属性对话框，选中的是“ Forwarders(转发器) ”选项卡。

可用以下步骤打开DNS服务器属性对话框：

1) 打开DNS服务器管理界面。

2) 单击顶层DNS节点的服务器列表中选中的服务器。

3) 单击“ Action ”菜单或所选服务器的上下文（点亮并单击右键）菜单。

4) 选择“ Properties ”。

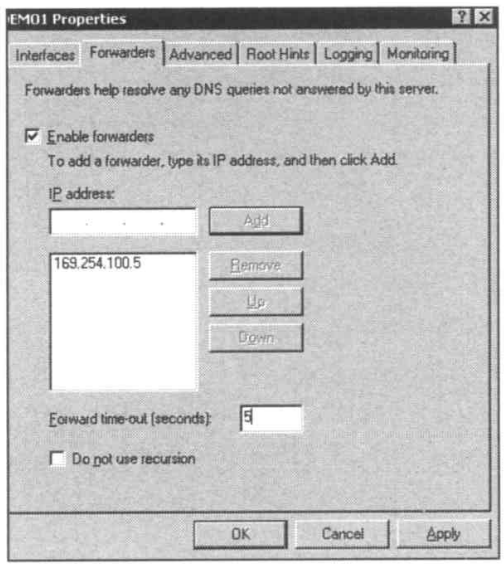

图11-3 Windows 2000 DNS服务器属性对话框中的转发器选项卡

我们需要稍微看一下这个选项和这儿的设置。这是服务器级的设置，意味着它们影响全部的服务器，域区级和资源记录级属性在以后讨论。

11.3.1 DNS服务器属性：接口

如果单击接口选项卡，将会看到可以控制网络接口， DNS服务器通过这些接口接收和响应请求。可以选择全部接口，也可选择手工配置的 IP地址列表。因为这是服务器的配置，也就是说，在缺省情况下DNS服务器允许在所有的接口上访问所有域区。

只有停机并重启 DNS服务器以后，此处的改变才生效。可参见服务器上下文菜单中的“ All Tasks ”。

11.3.2 DNS服务器属性：转发器

单击转发器选项卡，就可以使用转发器了（参见图 11-3）。可以回想一下，一个转发器就是一个DNS服务器，前面的 （你在管理的） DNS服务器将把它从用户解析器收到的查询请求发送到这个转发器。这个前面的服务器首先检查它是否能回答这个查询，如果不能则转发。关于使用转发器有一个很容易忽略的方面：转发不能给出完整回答的所有查询。当把转发器

作为从内部到公共DNS名字空间的桥时，转发的机器有权阻止将对内部名字的查询转发到外部DNS服务器来。

用“ Enable Forwarders(启用转发器) ”复选框配置转发器，然后通过反复输入 IP地址并单击“ Add ”就可以构造一个 DNS服务器的列表。注意，可以重新排列已列出的转发器的顺序以得到最好的性能，并把最常用的 DNS服务器放在最上面。

DNS服务器向列表中的机器发送查询请求。选项“ Forward Time-out(seconds)（转发超时(秒)）”表明，DNS服务器等待多长时间以后就使用别的办法来满足用户的查询请求。

启用转发器以后，在最底部有一个“ Do Not Use Recursion（不使用递归）”选项。该选项与转发超时是不能同时选中的。需要解释一下此选项，如果选择了“ Do Not Use Recursion ”，DNS服务器就从属于转发器。不允许 DNS服务器主动来执行一个递归查询，而是受限于转发器的服务。有人可能会想，这个选项的命名有点错误，如果根服务器在根提示下启动迭代查询会怎么样呢？也许这儿应该是“ Do Not Initiate Resolution（不要初始化解析）”，“ Do Not Use Recursion ”使DNS服务器仅从属于指定的转发器。

11.3.3 DNS服务器属性：高级选项

图11-4 显示了DNS服务器的高级属性选项卡，尽管我们不想花费时间来逐一解释所有这些配置选项，还是有很多需要介绍的。

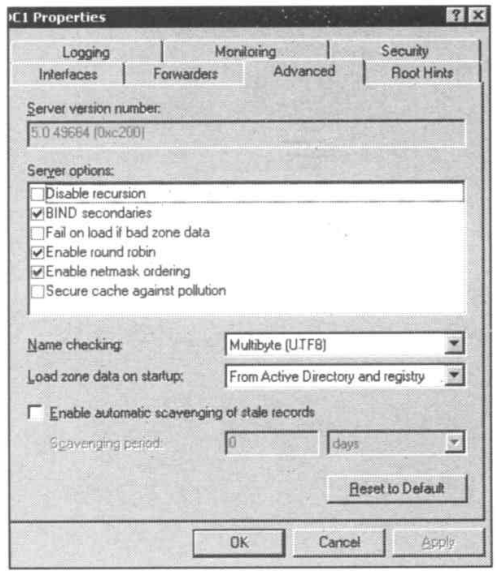

图11-4 Windows 2000 DNS服务器属性对话框中的“ Advanced（高级）”选项卡

如果比较一下图 11-3与图11-4，你会发现多了一个名为“ security（安全性）”的选项卡。图11-3显示了一个成员服务器；而图 11-4显示了一个域控制器上的DNS服务器，该服务器使用活动目录存储域区数据。

1. 名字检查

“ Advanced ”选项卡上的名字检查下拉框控制解析 DNS名字合法性的算法。标准 RFC（ANSI）要求名字必须完全符合 RFC的要求，缺省时为“ Multibyte（多字节）”(UTF-8)，这

是国际组织支持的正在发展中的选项（参见附录 B）。另外两个选项非标准 RFC（ANSI）和全名是更松的名字检查，不同之处在于最后关闭检查和前面的查询中，其名字只要是由 ANSI的字符组成的就可以了。为了实现与世界范围 DNS的互操作，应该使用标准 RFC（ANSI）。

2. 配置和域区文件存储

也许第一件需要说明的事情是服务器怎样在启动时装载域区文件。有三种可选方案：从文件装载、从注册表装载、或者从活动目录和注册表装载。

这儿配置了DNS与活动目录的集成。它的作用很大，但只是一个简单的开关。就像书评家所作的精确评论那样，这是“ 简单的修改带来很多成果。”因为第7章是用来评论这些成果的重大意义的，因此这儿的讨论仅限于 DNS服务器的配置。

当选择从文件装载时，存贮在 %windir%\system 32\dns处的引导文件用来指定要装载的域区。改变存储位置好象是不可能的；启动文件中对目录指令的使用被忽略，而且对域区文件使用全路径也并不令人满意。在这儿，用来重新定位存储的文档的注册表关键字信息也不见了。

当选择从注册表装载时，装载的域区是在注册表键值中指定的。但如果域区名字没有在注册表键值中修改的话，域区数据与选择从文件装载时一样仍在域区文件中。只有使用活动目录存储，才能停止对这些域区文件的使用。

当从文件转换到注册表时，启动文件就会复制到一个需要时创建的子目录（ .\backup）中。再转回文件存储时，将会从注册表信息创建一个新的启动文件。使用文件存储时，注册表中的引导配置信息和引导文件保持同步。

当使用从活动目录和注册表装载时，启动配置信息存储在注册表中，域区数据存储在活动目录中。一旦转换成这种设置，域区数据作为活动目录对象传送到存储器中，并可使用 LDAP工具进行读访问，这些域区数据包括用户的和活动目录控制台的“ dsa.msc ”。由于发生了这种转换，启动文件又一次移到 .\backup中，并且留下一个BOOT.TXT文件告诉你发生了这种变化。

表11-1总结了不同设置下使用的存储位置。

表11-1 DNS配置和域区数据存储

选 项	配 置	域区数据
From File	文本文件和注册表	文本文件
From Registry	注册表	文本文件
Active Directory	注册表	活动目录

一旦说到文件，最好不要忽略使用“ Update Server Data File（更新服务器数据文件）”选项。在编辑引导或域区文件以前，该选项使得 DNS服务器把缓存的任何变化都装入硬盘配置中，图11-2显示了此选项。

3. 不允许递归

不要把“ Disable Recursion ”选项与“ Forwarders ”选项卡中相似的设置混淆，该选项控制将要接受的查询类型。

启用不允许递归以后，此 DNS服务器就象一个根服务器，仅接收迭代查询，缺省情况下 Windows 2000 DNS服务器配置成接受递归查询。

4. 绑定辅服务器

该选项不影响两个Windows 2000 DNS服务器之间域区传送的执行，如果有一个到 BIND服务器或查不出的服务器的域区传送，将强迫使用一个低效但很完全的域区传送。该选项在NT 4 DNS服务器中。如果有一个到早于 4.9.4的BIND版本的的传送，就要确保实现绑定辅服务器，这样服务器就不用在传送消息中发送很多的资源记录了。

5. 如果域区数据错误就会加载失败

这是一个不言自明的选项，如果域区文件包含错误数据，在启用了此选项时就会导致加载失败。未启用时，就是缺省状态， DNS服务器仅仅输出错误信息，忽视一些数据继续加载域区。开始编辑以前，万一在手工编辑工作中犯了同样的错误，记住对此选项的设置，将会证明这种设置非常有用。

提到文件，应注意：如图 11-5所示，编辑域区和数据文件并不总是有好的结果，记着首先更新文件并注意是否实现了动态更新。

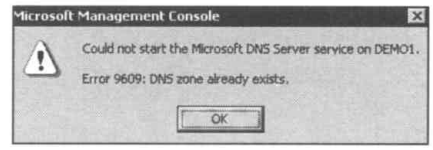

图11-5 一段友好的消息告诉你你的启动文件或域区文件没有编辑好

6. 启用循环

该选项允许DNS服务器在一个主机名中多个 A记录的IP地址间循环。在负载平衡的情况下，并没使用什么技术，但这里的负载分配是各种各样的，在响应最后一次查询时 DNS服务器列出所跟踪的IP地址，并在连续回答的过程中使IP列表旋转。

7. 启用网络掩码排序

这是Windows 2000 DNS服务器的一个特点，它允许服务器在返回查询结果时设置 IP地址的优先级。当一台主机有多个A记录时，如果DNS服务器确定其中的记录可以与查询客户的本地子网相匹配，在回答时就首选那些记录。该选项缺省值为是。

8. 保护缓存不受污染

这个特点控制Windows 2000 DNS服务器怎样把相关回答加入它的缓存中。如果启用了此选项，而相关主机与查询主机又有相同的父域，那么相关回答只需加到缓存中就可以了。例如，在hq.example.net中查询主机时，如果DNS服务器返回给example.net中的名字服务器一个相关主机，它就会被缓存；如果返回的是 bad.hack.com中的相关主机，就不缓存，而且在的解析中也不会缓存。缺省情况下不启用此功能。在启用此功能以前，应该考虑受益与验证所需的额外查询开销之比。

11.3.4 DNS服务器属性：根提示

此选项卡显示当前缓存或根提示文件。这已在图 4-11中表示过了，缺省情况下使用Internet根服务器。在此可以很快地检查到 DNS服务器的配置，记住该文件的操作是对于配置内部名字空间服务器很关键，因此在故障检修时可用于证实是否在使用正确的根提示。

11.3.5 DNS服务器属性：日志

该选项卡允许你选择将要把什么日志到调试日志文件中。对于一个繁忙的 DNS服务器，需要仔细检查掩码。可以在 %windir%\systems\dns\dns.log中找到日志文件，该文件是一个ASCII文本文件。

表11-2提供了有关该选项的更多信息。可能会有帮助，因为选择此选项时屏幕上没有任何信息。

表11-2 DNS服务器记录选项

选 项	解 释
Query	入站查询日志
Notify	入站通告消息日志
Updata	入站动态更新日志
Questions	入站查询的应答日志
Answers	查询的反馈消息的应答部分日志
Send	服务器发送的查询的序数
Receive	服务器入站的查询的序数
UDP	UDP入站请求的序数
TCP	TCP入站请求的序数
Full packets	整包发送的序数
Write through	写入域区的包的序数

此日志的能力，特别是与其他可用工具，如监视器（即系统监视器）、事件日志结合使用时，会形成一个强大的信息资源。希望你不常使用此日志功能，当你确实需要使用此日志时，记住它会降低服务器的性能，而且很快就会产生大量的文件数据。

11.3.6 DNS服务器特性：监视

该选项卡可使你向远程DNS服务发送一个递归的测试查询，或在本地系统执行一个简单测试。只需检查所希望的测试并单击“ Test Now（现在测试）”按钮即可。“ Remote（远程）”选项更有趣，既使使用循环调度也是静态的，它只能用于两台正在交流并使用同一种语言的服务器。也可以在指定的时间间隔执行循环测试。

11.3.7 DNS服务器属性：安全性

该选项卡只能在至少对一个域区启用了活动目录集成才能使用。“ Security ”选项卡的简单形式如图11-6所示，就是我们所熟悉的Windows 2000中用于编辑访问控制列表（ACLs）的

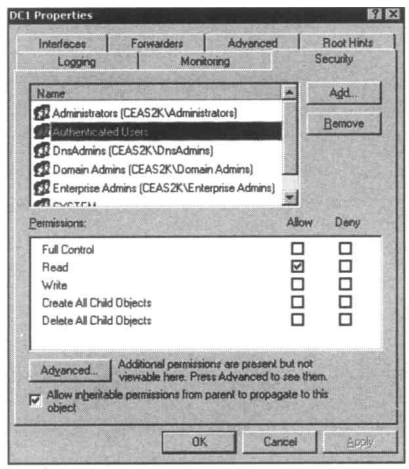

图11-6 集中在DNS服务器上的安全编辑器

安全对话框，它依赖于活动目录中DNS对象的安全配置。

高亮显示的Authenticated Users记录表明此用户组可以读这个用户记录表。第 7章讨论了使用活动目录集成时的安全性。

11.4 域区、子域和手工创建资源记录

为使用本地服务器，有两种选择。如果安装仅用于缓存的服务器，希望使用的是 Internet上的根提示，那么已经完成了。只要把客户机指向此服务器就可以了。也许想指定一些转发器，但工作方式不变。如需要有一个仅用于缓存的服务器用于内部名字空间，调整根文件并指定转发器（如果有的话）。

11.4.1 创建域区

很可能需要支持内部或公共 DNS名字空间的有代表性的部分。假设 test.example .net域需要一个主服务器。下面是需要做的，假设刚开始配置此服务器，因此需要首先创建一个域：

1) 打开DNS服务器管理界面。

2) 单击选中的服务器节点。

3) 使用选中服务器的“ Action ”菜单或上下文菜单，并选择“ New Zone ”来启动“ New Zone Wizard ”。

4) 单击Next，然后选择创建一个标准的服务器域区。这一步可以在活动目录集成以后，但在此可检查域区文件。单击 ” Next ”。

5) 选择创建一个向前查询域区，单击“ Next ”。

6) 输入此DNS域的名字。单击Next。

7) 对于域文件，可以自选名字而不使用缺省情况下建议使用的名字（此例中，使用test.example.net.dns）。注意，也可以输入正在使用的域区文件的名字。此处使用缺省的，单击“ Next ”, 然后单击“ Finish ”。

这样不会花费很长时间。如果扩展“ Forward Lookup Zone ”节点，就会看到新域区。创建辅服务器域区也一样简单，但有一些特别的信息需要收集，比如到哪儿获得域区信息。

1) 像以前一样启动“ New Zone Wizard ”。

2) 单击“ Next ”，然后选择创建一个标准的辅服务器域区。单击“ Next ”。

3) 选择创建一个标准辅服务器域区。单击“ Next ”。

4) 输入DNS域的名字。因为此处是一个辅服务器域区，因此要与主服务器上的相同。单击Next。

5) 输入DNS服务器的IP地址，这些地址将用于指定主服务器向哪些辅服务器域区传送；如果是在DNS服务器管理控制台中配置的 DNS服务器，浏览并从中作出选择，把所有的主服务器都输入以后，进一步证实它们的排列顺序也是正确的。

6) 单击“ Next ”，然后单击“ Finish ”。此处不允许选择文件名，如果不想使用缺省名必须以后再修改。

除了由网络的反向 IP地址指定的域区，其他反向查询域区的创建也一样简单。创建步骤如下：

1) 像以前一样启动“ New Zone Wizard ”。

2) 单击“ Next ”，然后选择创建一个标准的主服务器域区。单击“ Next ”。

3) 选择创建一个反向查询域区，单击“ Next ”。

4) 与在命名网络时一样输入IP地址。例如：10.10将使用部分A类IP地址，因为它用于网络10.10.0.0/16。注意，它会生成一个域名。单击“ Next ”。

5) 在此也可以选择使用另一个文件名，只是单击“ Next ”，然后单击“ Finish ”。

现在已有了一个反向查询域区来处理从 10.10.0.0到10.10.255.255的IP地址，在节点“ Reverse Lookup Zones ”中将有显示

如果单击任何一个新域区，从而更详细的显示它的资源记录，会发现每个域区都有两个记录：开始授权（SOA）和名字服务（NS）记录,都可用来确定你的服务器。SOA标明所使用的帐号。

如果到目录%windir%\system32\dns看一下，就会发现新的域区文件，如果到 HKLM\System\CurrentControlset\Services\DNS\Zones中看一个关键字，就会看到这些域区的记录，包括域区名。最后如果在%windir%\system32\dns中打开根文件，会发现除了没有目录指令以外，它只是一个很小的NAMED.BOOT文件。

辅服务器域区稍有不同，因为向导要求你提供主 DNS服务器的IP地址。这些机器用来提供域区传送数据。在创建一个辅服务器并用它来作传送以前，首先授权或稍微提供保证主管辅域区的服务器会被它的主服务器允许执行传送。如果不想这个新辅服务器被查询，就不正式授权此服务器。就象在域区属性中将要看到的一样， Windows 2000完全实现了“ Notify ”选项和递增传送（IXFR）。你很可能想在主机上为你的辅服务器配置“ Notify ”选项，如果域区允许动态更新，这种方式的优点还是很重要的。

11.4.2 域区传送和其他属性

打开向前查询域区的属性，你会看到如图 11-7所示的属性单，显示的名字为“ SOA ”和“ Name Servers ”的选项卡，这在第4章中已讨论过了。

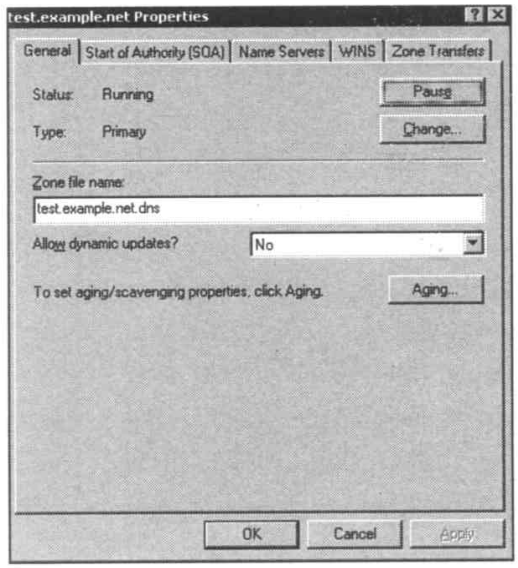

图11-7 一般的前向查询域区属性对话框

WINS（反向域区中的WINS－R）选项卡也在第4章中讨论过了，DNS服务的内涵在第16章 中详细讨论，这三项都与单一的资源记录类型联系密切。

1. 一般设置

缺省情况下，标准域区由动态 DNS的更新机制创建。启用这个特征只需把对“ Allow Dynamic Update? ”的回答由No改为Yes，并应用这个改变。当创建一个集成的活动目录域区时，缺省时是“ Only Secure Updates ”，没有集成显然是办不到的。第 7章在使用集成的活动目录存储中，在一定程度上讨论了这个问题。

在这一部分，可以看到域区的当前状态，可以暂停和重启域区，它比服务器节点提供的服务器级暂停和重用控制更好。除了类型，还显示了该域区是一个标准的主服务器域区还是辅服务器或集成的活动目录域区；“ Change ”按钮打开一个对话框，在此可以改变类型。注意“ Aging ”按钮。图7-1显示了此按钮的配置，它可以清理域区中陈旧的记录。

一旦使用了DDNS和安全性，很可能有无用的资源记录留在域区文件中。这些记录是有害的，可能会导致应该被允许的注册不能完成，而且使域区增大从而降低了查询速度。第 7章详细论述了清理过程。

2. 域区传送

通过域区传送项卡可以配置域区传送的类型和安全特征。图 11-8显示了此选项卡与“ Notify ”按钮（被上面的窗口覆盖），从而显示了启用更新通知的特征的设置。 NT 4.0也有“ Notify ”按钮，但因它的域区传送不是递增式的，所以使用不太方便。

在主要选项卡上，不复选“ Allow Zone Transfers ”可使域区传送功能失效。一旦启用域区传送，就可以通过IP地址提供一个服务器列表，可以向这些服务器发送传送请求。或者允许传送到任何服务器，或者只允许转送（此处显示的）到域区中 NS记录指定的机器。图 11-8显示了被“ Notify ”对话框覆盖的“ Notify ”按钮。“ Notify ”设置可以用来取消通知，也可以启用通知向目标DNS Notify发送消息，或者送到NS指定的机器或者送到一个专门输入的机器列表中。

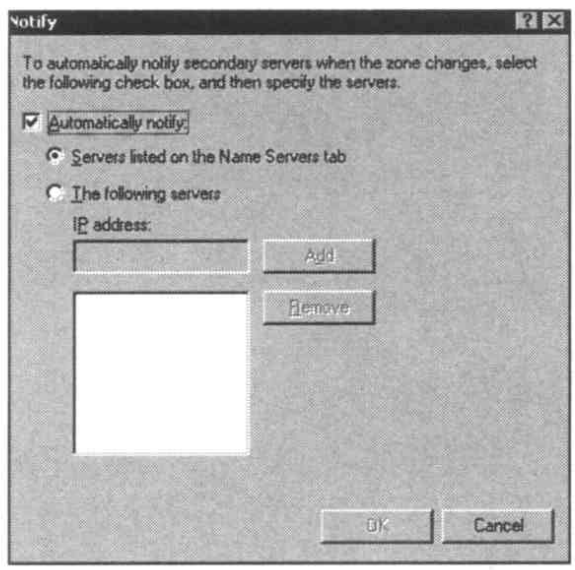

图11-8 域区传送选项卡和“ Notify ”对话框

Windows 2000 DNS服务器总能执行递增式的域区传送，不管它是否依赖于收到了一个AXFR或IXFR请求。一旦IXFR有一个递增式的传送请求，除非版本差别很大，否则 DNS服务器都会照做。当DNS服务器的“ Change ”由于发生了很大的变化而不能支持 IXFR请求时，就会协商使用全域区传送并使用 AXFR指令。

对区域传送过程的这些优化对实现了动态更新的域区来说是很重要的。当配置“ Notify ”选项时，不要忘了许可服务器（即列入表中），这样它就可以接收域区传送，并且不管哪个服务器作为主服务器都可以配置通知。

11.4.3 授权和子域

使用DNS管理控制台授权与创建域区的过程大致相同。既然有一台 DNS服务器主要用于text.example.net，就应该看一看它能做些什么。图 11-9显示了主服务器域区的上下文菜单。辅服务器域区的上下文菜单与此差别很大，因为辅服务器没有资源授权，因此在辅服务器上不能创建记录，但可以向它发传送请求（发 IXFR请求）。

图11-9中，域example.net已扩展，显示了固定记录的存在。因为你没有创建 example.net域区,所以在你的服务器上将会有所不同。此处已创建了 exmaple.net和许多独立的DNS域名。

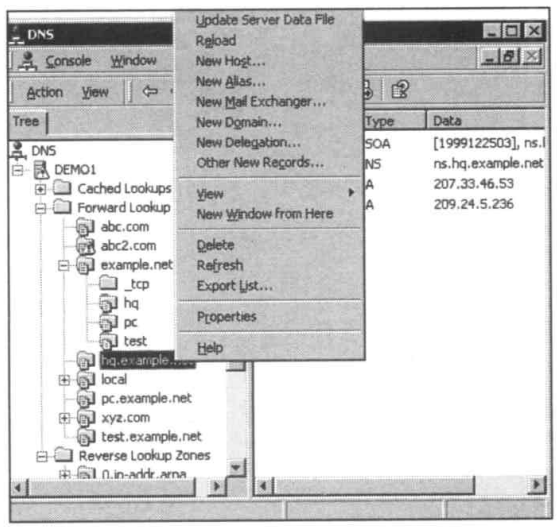

图11-9 主服务器域区的菜单选项

如果查看上下文菜单，你会发现有很多可创建新记录的选项，其中有两个选项，标记为“ New Domain ”和“ New Delegation ”。下面部分讨论它们可以做些什么，有哪些不同。

1. 新的DNS域

使用“ New Domain ”选项将立即需要一个新域名，仅此而已。在第 4章的讨论中，有时也称它为创建一个子域，该选项不经授权就可以创建一个部分名字空间。

1) 打开DNS服务器管理控制台，扩展需要定义新域区的服务器。

2) 把光标定位在需要定义的主域区上（例如，用 example.net定义west.example.net），并在此域区的上下文菜单（单击右键）中选择“ New Domain ”。

3) 在“ New Domain ”的对话框中，输入新域区的名字。在上一步的例子中，这儿的名字

应是west。

4) 单击“ OK ”，在这个域区的下面就会有一个以节点形式出现的新文件夹。

一旦选择了“ New Domain ”，就必须输入一个合法的有效的符号而不应有任何句点，例如，上面的输入是west，而不是west.，也不是west.example.net。选择OK按钮就可以启用了。单击OK以后，在这个域区节点中就创建了一个以此输入为名的新文件夹。图标是一个简单的文件夹，它是空的。如果现在你想在这个新建的子域 west.example.net中为某个机器创建一个A记录，给它一个记录名Bld12-r1023，该记录就会在example.net 下的west文件夹中显示。如果你在磁盘上更新服务器文件，然后检查 example.net的域区文件，就会看到刚注册的名字为Bld12-r1023.west的A记录。

2. 新的DNS授权

“ New Delegation ”选项用来创建一个授权的子域，包括一个用来回答查询请求的 NS记录。该选择会弹出 ” New Delegation Wizard ”。就像在New Domain中一样，第一个对话框要求输入一个标号，没有任何句点“ . ”，该标号将成为你将授权节点中的新子域的名字 .。

1) 打开DNS服务器管理控制台，扩展将要定义的新授权的服务器。

2) 将光标定位在将要授权域区的主域区 ,例如，用example.net定义east.example.net,并在这个域区的上下文菜单（单击右键）中选择“ New Delegation ”。

3) 在“ New Delegation Wizard ”中，首先单击“ Next ”进入。在“ Delegated Domain Name ”对话框中，输入“ Delegated Domain ”正文中新域区的名字。在上一步的例子中，此处为east,没有其他后缀。注意，被授权域区完整的合法域名（FQDN）显示在变灰的正文框中。单击“ Next ”。

4) 现在你需要指定一个名字服务器来处理该域。单击“ Add ”，打开“ New Resource Record ”对话框来创建NS记录。

5) 浏览此机器的A记录或CNAME记录，或通过IP每次输入一个记录。对每一台输入的机器，在授权的域区中会产生一个新的 NS记录。

6) 单击“ Next ”，然后单击“ Finish ”来关闭向导。新域区的节点将出现在选择“ New Delegation ”的节点的下面。

提供一个子域名以后，你可以输入任意一个将要授权（不是资源授权）服务器的地址。可以通过FQDN或IP地址加入服务器，但是，如果待连接的 DNS服务器的A记录或CNAME记录已经存在于已连接到管理控制台的 DNS服务器的DNS数据库中，最简单的办法就是浏览。每个服务器把收到的 NS记录加入新域区中。关闭向导以后，将会有一个新的带有特殊图标的子文件夹，打开它可以显示 NS记录。更新服务器文件并检查域区文件也显示 NS记录。DNS服务器管理控制台不允许在新节点中添加记录。被授权者已在父域区中创建了一个固定记录，此处假设在被授权的服务器中将存在一个域区。

3. 资源记录

在第4章中比较详细的讨论了主要的资源记录类型，而在附录 F中可以找到其余资源记录类型的信息。因为第 4章中包括对操作屏幕的截取，输入的信息也是可预测的，所以在本章中不包括在主域区中如何手工创建资源记录。很多创建记录的选项都弹出给一个简单的带有必要的细节的对话框，其中还作了一些合理的假设，并用创建 RR来结束，你可以继续在对话框中创建另一个记录。

当光标落在一个主域区上或主域区内时，在上下文菜单中经常有很多常用的资源记录选项。选择“ Other New Records ”，你就几乎可以选择任何 RFC指定的 资源记录类型（在Windows 2000的最初版本中好象去掉了 DNAME，但在我们出版时又加上了）及一些 RFCs未指定的类型（至少现在还未指定，如对 ATM的支持）。记住，你总可以停止一个使用域区文件存储的域区，也可以直接编辑它。确保首先去除任何更新过的缓存文件，并在你重新开始以前提高版本以便于传送这些更改。对于有经验的管理员来说是相当标准的经历。

11.5 活动目录集成

域区存储中使用活动目录有很多影响，这在第 7章中已经比较详细的讨论过了。因为把一个域区转换成这种存储模式如比简单，只要在域区属性的“ General ”选项卡中使用“ Change ”按纽（参考图11-7）就可以了，所以很容易忽略很多影响和可能使用到的的新选项。

集成以后域区文件存储在活动目录中，就像图 11-10中看到的一样。该图显示了“ Active Directory Users ”和计算机管理控制台上微软 DNS容器的扩展。（需要实现高级模式。）

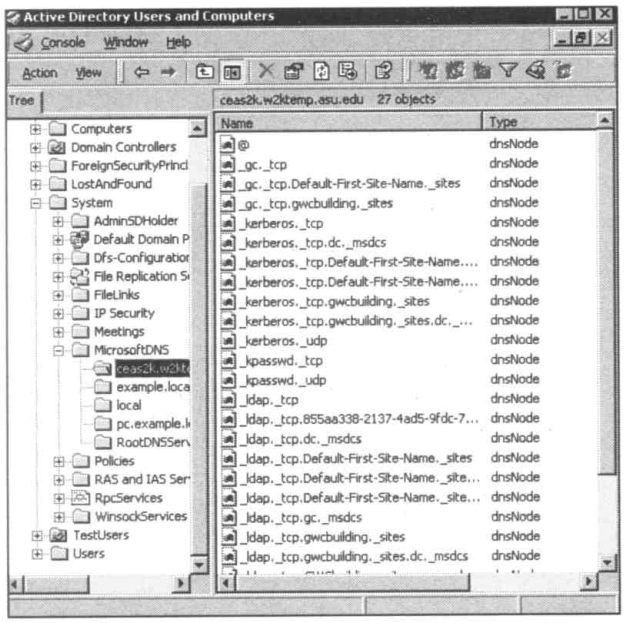

图11-10 活动目录中对域区数据的累积

此控制台的显示是非层次的而不是按域区组织的。此显示是只读的，只有安全性描述可更改。可见部分表明了通过 LDAP查询可得到此域区文件。如果你不在意，此 LDAP可提供一个环绕路线，包括所有你想保护和传送的域区数据。

参考第7章讨论一下把你的域区集成到这种存储模式的其他方面。此处没有考虑到的主要方面是复制机器和网络以及域控制器上 DNS服务器的负载。它们在第9章中讨论过。到此，我们在结束此部分以前提醒你，简单的转换并不简单。

11.6 服务器类型

因为这部分内容已分散到前面的部分中，此处只非常简单地列一下配置一个服务器的各

种操作类型所需的设置。

11.6.1 使用转发器

象前面讨论的一样，前向服务器是在服务器属性中的服务器级别设置中配置的。Windows 2000 DNS服务器向这些机器发送递归查询。Windows 2000 DNS服务器总是把迭代查询发送到其他DNS服务器，而不是前向服务器。

在下面的许多配置中都可使用前向服务器。一旦指定，在它转发收到的查询以后前向DNS服务器可能解析也可能不自己解析。如果不允许这样做，Windows 2000 DNS服务器在等待前向服务器回答过期以后开始自己解析查询。

11.6.2 只用于缓存

只用于缓存的DNS服务器没有主服务器和辅服务器域区，只依赖于其他 DNS服务器的服务，并缓存结果为以后的查寻提供非授权的回答。Windows 2000 DNS服务器在最初安装的配置中没有任何域区，只有一个根提示文件适于 Internet使用。因此，最初配置的安装是一个只用于缓存的服务器。

你可能想做两件事来完成作为一个只用于缓存的服务器的配置。首先，如果在内部 DNS设计中使用DNS服务器，你当然希望调整根提示文件。第二，设置服务器使用从所有相似的事件中选定的转发器和在名字空间内部设计中可解析的转发器是一个很好的主意。

11.6.3 从服务器

从服务器在这里不是指域区传送的辅服务器，而是指配置的 DNS服务器仅用作转发器。它不同于只用于缓存的服务器，因为它们不能解析收到的任何查询而只是转发查询。为把DNS服务器设置成从服务器，首先把它设置成转发器。然后在服务器属性的转发器选项卡中设置选项“ Do Not Use Recursion ”。有一个效率可能很低但可以实现相同结果的相似的实现方法，那就是调整它的根提示文件，从而只有它自己知道，就像 UNIX服务器那样。

11.6.4 授权从服务器

因为想有一个好的名称，所以称这种配置为授权从服务器。这种配置与刚才介绍的从服务器很相似。不同之处仅在于这种 DNS服务器也被授权了主服务器和 /或辅服务器域区。这种配置中，使用转发器并缓存他们的结果。然而，如果以服务器的权力来要求查询一个主机，可从域区文件返回对此查询的授权回答。相反，如果转发器可以解析此查询，就只返回答案。值得重申的是：使用“ Do Not Use Recusion ”选项时，DNS服务器仍提供授权回答。

11.7 迭代

缺省情况下Windows 2000 DNS服务器既接受迭代查询又接受递归查询。但可以改成只接受迭代查询。通过检查服务器的属性“ Advanced ”选项中的“ Disable recursion ”就可以做到。迭代服务器有较少的工作量，因此有较高的能力。迭代服务器与公共 DNS服务器一样值得注意，因为这种配置可增加服务器抵抗基于服务器进程过载的攻击。

11.8 域区清理

使用动态更新会带来问题，除安全性问题以外，最大的问题可能是域区内容管理。在此提醒的重要性在于，如果在使用此功能之前没有充分考虑它的结果，那么， Windows 2000 DNS服务器的清理能力可能会使你很头痛。在深入考虑本章提到的 Aging和Scavening选项以前，先参考一下第7章的讨论。

11.9 支持特征

Windows 2000的DNS服务器有能力基于自己运行，它可以在一段时间以非常健壮的方式运转。然而，它的服务也有疏漏，还需要讨论一下你的主要选择。

11.9.1 记录

监视着服务器是一个不间断的任务。第一次设置 DNS服务时，盯着服务器非常重要，并且可以知道在你的服务器上装载了多少东西，以及发现一些或大或小的问题。

你已看过了服务器属性中的记录选项卡，有一点不幸是此工具不能基于每个域区启用，但仍能提供有价值的信息。再一次探讨在负载很重的服务器上此工具的使用。它不仅是循环操作，而且还能迅速生成大量文件。

我们还没有提到加载“ Windows Event ”，在Windows 2000中它有一个新的DNS加载方式。图11-11显示了打开的“ Computer Management ”控制台。 DNS事件加载是一个很好的观察台，因为任何严重的问题都会在此显示，但不要依赖它作为平衡容量和性能的信息源。

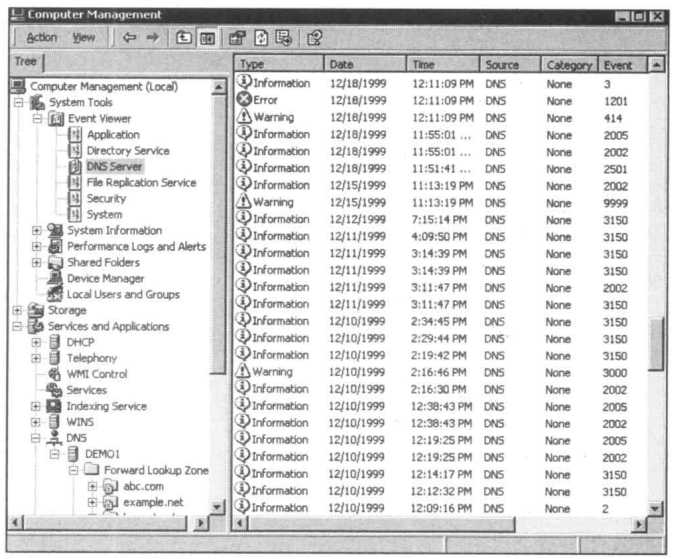

图11-11 DNS服务器事件日志

“ Computer Manegement ”控制台可以在“ My Computer ”的上下菜单中的“ Manage ”选项中找到，或者运行Compmgmt.msc。注意，在图11-11中，节点“ System Tools ”和“ Event Log ”已被扩展，在详细面板上“ DNS Event Log ”已显示了加载的日志。在底部，已扩展了“ Services and Applications（服务和应用）”，显示了对DNS管理界面的全部访问，该界面在“ Computer Management ”控制台中作为内嵌负载。

11.9.2 统计和监视

如果对Windows NT和Windows 2000不熟悉，你可能还没有发现系统监视的价值，在“Administrative Tools”文件夹中选择“Performance”可弹出此工具，或者也可运行Perfmon.msc。在NT 4.0中，称此工具为性能监视器，而且还在用这个名字。监视器以三种模式工作：Live Viewing，Logging 和Alerting。如果单击图标（+）给该表加上计数器，就会出现一个对话框，在此首先要选择感兴趣的对象，这种情况下当然是 DNS，然后是将要使用的对象中的计数器。

可以为后面的视图记录全部的日志文件对象。非常好的一点是，你也可以在计数器上列出条件，这将会激发事件日志信息。然后，如果有一个工具，比如 SMS（System Management Server），那么，这些事件日志消息可以激发计划好的行为、电子邮件消息等。

为使你了解DNS对象所能提供的扩展信息，表 11-3列出了这些计数器。仔细看一下对象列表，你会发现内存的使用很容易监视，你可以知道到你的服务器有多么大的能力，对于一个DNS服务器来说，内存是最关键的资源。Notify、IXFR、AXFR和传送计数器使你了解一个域区传送的负载以及是否IXFR传送将会导致AXFR传送，假设只有IXFR应该发生。动态更新和安全更新计数器提供有关服务器的动态域区管理活动的信息。其他的一些组合可用于查看服务器的查询负载，等等。

表11-3 系统监视器中的DNS对象计数器

AXFR Request Received
AXFR Request Sent
AXFR Response Received
AXFR Success Received
AXFR Success Sent
Cache Memory
Database Node Memory
Dynamic Update NoOperation
Dynamic Update NoOperation/sec
Dynamic Update Queued
Dynamic Update Received
Dynamic Update Received/sec
Dynamic Update Rejected
Dynamic Update TimeOuts
Dynamic Update Written to Database
Dynamic Update Written to Database/sec
IXFR Request Received
IXFR Request Sent
IXFR Response Received
IXFR Success Received
IXFR Success Sent
IXFR TCP Success Received
IXFR UDP Success Received
Nbtstat Memory

（续）

Notify Received
Notify Sent
Record Flow Memory
Recursive Queries
Recursive Queries/sec
Recursive Query Failures
Recursive Query Failures/sec
Recursive Send TimeOuts
Recursive TimeOuts/sec
Secure Update Failure
Secure Update Received
Secure Update Received/sec
TCP Message Memory
TCP Query Received
TCP Query Received/sec
TCP Response Sent
TCP Response Sent/sec
Total Query Received
Total Query Received/sec
Total Response Sent
Total Response Sent/sec
UDP Message Memory
UDP Query Received
UDP Query Received/sec
UDP Response Sent
UDP Response Sent/sec
WINS Lookup Received
WINS Lookup Received/sec
WINS Response Sent
WINS Response Sent/sec
WINS Reverse Lookup Received
WINS Reverse Lookup Received/sec
WINS Reverse Response Sent
WINS Reverse Response Sent/sec
Zone Transfer Failure
Zone Transfer Request Received
Zone Transfer SOA Request Sent
Zone Transfer Success

11.10 DNS服务器注册表记录

Windows 2000中的DNS服务器有大量的注册表关键字，其中大部分键值可以通过 DNS 服

务器管理控制台配置，注册表中的根位置是HKLM\System\Current Control\Set\Services\DNS；下面是子关键字\Parameters，在这儿可以配置全局设置，如表11-5所示；域区设置，如表11-4所示，按FQDN将域区分开存储。

表11-4 域区相关的DNS注册表键值

值	类 型	描 述
Aging	Reg_Dword	0无效，1有效
AllowUpdate	Reg_Dword	0无效，1有效，2安全更新
DatabaseFile	Reg_Sz	%windir%\system32\dns 中的区域文件名
DSintegrated	Reg_Dword	0无效，1有效
MasterServers	Reg_Sz	以空格隔开的IP列表
NoRefreshInterval	Reg_Dword	小时（十六进制）
NotifyLevel	Reg_Dword	0通告无效，1通告NS服务器，2使用通告服务器
NotifyServers	Reg_Sz	以空格隔开的IP列表
RefreshInterval	Reg_Dword	小时（十六进制）
SecureSecondaries	Reg_Dword	0无效，1NS服务器，2使用从属服务器
SecondaryServers	Reg_Sz	以空格隔开的IP列表
Type	Reg_Dword	0缓存区域，1主要的，2从属的

表11-5 DNS服务器全局注册表键值

值	类 型	描 述
BindSecondaries	Reg_Dword	0无效，1有效
BootMethod	Reg_Dword	1文件，2注册表，3AD和注册表
CleanupInterval	Reg_Dword	清除缓存的时间间隔（缺省为900s）
DisableAutoReverseZones	Reg_Dword	0F=有效，1T=无效（0.,127., 255.inaddr.arp）
Forwarders	Reg_Sz	以空格隔开的IP列表
ForwardingTimeout	Reg_Dword	秒（十六进制）
IsSlave	Reg_Dword	0无效，1有效
ListenAddresses	Reg_Sz	以空格隔开的IP列表
NoRecursion	Reg_Dword	0=接受递归，1=接受迭代
RecursionRetry	Reg_Dword	秒（十六进制）（每次）
RecursionTimeout	Reg_Dword	秒（十六进制）（总计）
PreviousLocalHostname	Reg_Sz	字符串主机名
ScavengingInterval	Reg_Dword	小时（十六进制）
SecureResponses	Reg_Dword	0无效，1有效

11.11 小结

到目前为止已查看了Windows 2000 DNS服务器的选项，并讨论了对于安装配置来说最重要的几个方面。通过本章，应该能毫无问题地安装 DNS服务器，并开始加入域区数据。对需要深入讨论的问题，提供了相关章节作为参考资料。