

## 第8章 与BIND服务器合作

本章内容包括：

- 域名服务器间的通信。尽管域名服务器与早期的基于 BIND的域名服务器的通信是兼容的，但还是会出现问题。该节对这些域名服务器之间的通信提供了一些预防措施。
- 从BIND移植到Windows 2000 DNS。该节给出了用微软 DNS集成或代替基于BIND的域名服务器的一些必需的操作。
- 在Windows上运行BIND。尽管还没有支持Windows 2000域环境的选项可供选择，还是给出了目前在Windows上有局限的BIND的警告。
- 其他启动文件和域区文件的不同。从 BIND到微软 DNS的移植以及BIND和微软 DNS的集成。需要注意这里提供到的一些域区和配置文件细节。

### 8.1 域名服务器间的通信

所有的域名服务器都应该可以互相通信。如果它们没有（或不能）的话，Internet主机名将永远不会被解析。微软 DNS在如何与其他域名服务器通信方面与 RFC标准一致。域名服务器必须理解的通信内容有查询、查询响应和域区传送。查询和响应作为名字解析的基本要素其意义是不言自明的。客户端向服务器发出的查询可能会导致服务器发出附加的查询直到找到答案并返回给客户端。域区传送是允许主服务器向从属服务器传播信息的机制，由此提高了“分布式”系统的能力。消息格式和查询报文有相同的结构和位排列顺序。Windows 2000 DNS服务器对迭代查询和递归查询都做出正确的接收和响应。尽管 Windows 2000 DNS服务器是与标准兼容的，但还是要注意一些具有由可选项带来的特征的问题。

活动目录的使用对 DNS服务的选择造成了一定的限制。需要对 SRV记录类型的支持。如果支持动态更新，就建议使用递增传送和通告选项。最早成功地支持这种结合的 BIND版本是 BIND 8.1.2。

在进入具体讨论之前，先要提到的一点是使用微软专有的 WINS和WINS-R记录时，忘记把它们从传送到非微软的DNS服务器的域区信息中排除会带来问题。

#### 8.1.1 与BIND 4.9.4及更早的版本间的通信

一般地讲，使用 BIND 4.X除了在一些非常特殊的情况下，不能很好地满足所有的需求。如果使用域环境，活动目录需要 DNS支持SRV记录。在需要交互式操作的一些情况下需要考虑这些问题。

对于Windows 2000 DNS服务器以及基于BIND 4.9.4甚至更早版本的域名服务器，需要注意的一点是域区传送期间发送的消息。尽管已写入 RFC中，BIND的早期版本和它的派生物在包括多个资源记录的消息上还是会出问题。如果发生这种情况，管理员应注意设置 Windows 2000 DNS服务器在域区传递期间向 BIND服务器发送只包括一个资源记录的消息。这样做减少了与域区传送自身相关的许多问题，同时也保护网络中其他域名服务器的“健康”和“完好”。

在NT 4.0中这能够通过启动文件中不注释 Bind Secondaries行来实现，或者在所有的版本中编辑注册表里 Bind Secondaries的键值，或者在 Windows 2000中的服务器属性中的“Advanced（高级）”选项卡中设置BIND辅服务器选项。在 Windows 2000中这个选项对两个 Windows 2000 DNS服务器间的传送不产生影响，这个设置是服务器范围内的，影响对辅服务器的所有域区传送。

在NT 4.0中，如果管理员想通过编辑注册表里的启动文件来实现改变，这时域名服务系统从注册表启动并正在运行，管理员应该依照以下几个步骤：

- 1) 改变注册表键值为“从文件启动”而不是“从注册表启动”。
- 2) 创建一个与目前配置匹配的启动文件。
- 3) 重启域名服务器以使它从文件启动。
- 4) 打开DNS管理器并在“DNS菜单下执行”Update Server Data Files（更新服务器数据文件）。

注册表里影响这个操作的键值包括一个二进制操作符， Bind Secondaries 的键值设置为0或1即可。二进制值1代表是，表示将使用BIND辅服务器，0代表非状态。

NT 4.0存在一个缺点，即缺少一个工具来产生与注册表设置匹配的 DNS启动文件，这在 Windows 2000版本中已被克服。由于在传递中可能会丢失配置设置的事实，在启动文件和注册表间的摇摆不定会给它自身带来问题，所以，管理员在进行这些或其他一些改变时应非常注意每个细节。Windows 2000已经解决了这些问题，因为当服务器从文件启动时注册表和启动文件被保持一致。

### 8.1.2 与BIND 8通信

对于BIND 8，不需要再担心消息中资源记录的数量，但是 BIND8又有一些新的有趣的特征。如果BIND 8被用来作主服务器，微软 DNS管理及必须注意向主服务器发出正确的查询。也就是说，BIND 8能过滤来自于特定地址和端口的请求。一个运行BIND 8的系统有两个地址，并向外部网络和内部网络都提供域区信息。BIND 8服务器能够被配置为基于接收到查询的接口，甚至是用作通信的端口数而对查询给出不同的响应。BIND 8允许管理员定义谁来执行域区传送，谁向系统发出查询，甚至客户端向服务器发出查询时允许的端口数。如果用微软 DNS作为辅服务器，要确保访问控制被正确地设置以允许辅服务器的域区传送，并保证辅服务器指向正确的接口。

如前所述，BIND 8.1.2支持要使用活动目录的最低要求。所以，在 BIND 8.1.2或更高版本中使用BIND作为一个辅服务器不仅是可能的，而且是不会出问题的。但是，BIND 8.1.2或更高版本在很多环境中都会受到侵犯，有时甚至 Windows 2000 DNS服务器的源权威的委托授权也可能是不可能的。在这种情况下，需要解决很多问题。

当BIND作为主服务器时，必须提到的事实是无法保证 Windows 2000客户机实现所理解和使用的动态更新过程的安全，至少在 Windows 2000最初的版本是这样的。这意味着不能使用本来可供使用的安全机制。结果是可能选择不使用动态更新。这又意味着必须手工地维护 A记录、指针记录和其他一些记录类型的记录，还包括 SRV记录和它们结构。第7章提供了对这些问题的深入的讨论。如果只有最初的 NETLOGON.DNS记录被添加，Windows 2000活动目录不会优化它的访问路径。如果 netlogon可以对一些站点比如 \_Site,更新SRV记录，则活动目录

会优化它的访问路径。

## 8.2 从BIND到Windows 2000 DNS的移植

一个运行BIND的管理员想要实现Windows 2000的DNS方法必须首先回答两个问题：

- Windows 2000 DNS将会与BIND联合使用吗？如果是，那它是主服务器还是辅服务器？还有使用什么版本的BIND？
- Windows 2000 DNS将完全代替BIND服务器吗？或者说它的功能只用于域里被授权的一部分（子域）吗？

如果Windows 2000 DNS服务器将和BIND联合使用，则必须知道使用的是哪个版本的BIND。如果BIND 8和Windows 2000 DNS一起使用，而Windows 2000 DNS作为辅服务器，并且不使用活动目录，则建立Windows 2000 DNS的问题就会很小。管理员只需要对辅域建立Windows 2000 DNS。除非Windows 2000 DNS计算机也是一个辅主服务器，即还有其他辅服务器从它那里得到域区，那么就没有其他事情要做了。对于主服务器，问题就只是与服务器的建立相关。Windows 2000 DNS服务器不载入BIND 8的配置文件，这就意味着Windows 2000 DNS的配置必须手动进行或使用一个拆开的配置文件。关于手动配置的更多信息，见第11章。

希望随着DNSSEC和DNSIND工作组的巩固，它们为使支持动态更新的标准修订本得到一致认可而做出的努力能得到认可，即产生出得到广泛工业实现的产品。到那时，DNS服务器通过所有权的使用来保护更新操作的方法将只剩下有限的交互式操作能力。Windows 2000 DNS的实现不支持RFC 2137并且限制了个人的选择。但是有很多其他的DNS实现支持这个RFC。

如果不需要支持活动目录，就应该了解和考虑前面部分提到的问题。最简单的共存方法是Windows 2000在它的DNS服务中使用时将源权威委托授权给它。

如果微软DNS服务器将作为主服务器，也需要域区文件的来源。域区文件如果来自一台存在的服务器，则能被复制。因为它们都是格式化的文本文件，不需要给出特殊警告。唯一潜在的问题是可能有新添加的还不被微软DNS支持的资源记录类型。微软说这样的记录将被跳过，并且Windows 2000几乎支持所有的资源记录类型。

在实际移植中，要考虑Windows 2000 DNS接替一个作为主服务器的BIND主机这种情况。因为争论的缘故，Windows 2000 DNS被设置为活动目录的参与者，在活动目录中DNS记录将被集成。开始时，需要为Windows 2000服务器安装操作系统和DNS服务器（见第11章）。在这些完成后，下一步是移植域区数据到新的服务器。推荐最简单的方法是按下列步骤执行：

- 1) 通过在DNS管理界面中创建辅域区，将Windows 2000 DNS服务器设为辅服务器。
- 2) 验证新的“从属”服务器对从BIND执行域区传送有访问权。
- 3) 启动新服务器，或手动地强迫传送，或使用辅域区 context菜单里的“Transfer from Master（从主服务器传递）”选项。在几秒钟内（通常情况下），域区文件会传送到新的服务器。
- 4) 验证新服务器配置为从文件启动（在服务器属性的“Advanced（高级）”选项卡中）。
- 5) 让新域名服务器脱机，依照步骤6~8，重新设置主服务器。
- 6) 删除对刚被传送的辅域区的域区配置（启动文件）；注意这并不是说删除域区文件本身。

- 7) 使用主服务器指令并把刚传送的域区文件作为域的来源来创建新的配置。
- 8) 改变新服务器的IP地址以匹配已存在的先前的主服务器。
- 9) 关掉已存在的主服务器，使新的 Windows 2000 DNS 服务器联机。
- 10) 需要时改变成活动目录集成的存储模式。

### 8.3 在Windows 上运行BIND

在NT上建立一个域名服务器的另外一个可能性是使用移植到 NT上的BIND。这种方法的一个缺点就是对NT的BIND端口是基于BIND 4.9.7的。现在它是一个不被推荐的版本，并且没有付诸任何努力来支持这个版本。使用户对这个端口失望的另一个因素是它是为 NT 4.0准备的。这个版本在Windows 2000版本下是有疑问的。如果打算运行BIND，就应该不使用这个方法，而应选择一个基于UNIX的解决办法。

### 8.4 其他启动文件和域区文件的不同

应该记住的一个主要事情是配置微软 DNS服务器时的WINS集成。因为RFC文件关于DNS的部分不要求支持WINS的使用，并且WINS已经变得不流行，将主要用作支持传统的操作系统和应用程序，但这在几年内任然是一个问题。如果使用WINS支持NetBIOS客户端（见第16章）并且使用WINS伪资源记录，记住在向所有的非微软 DNS服务器进行域区传送时去掉这些记录。

Windows 2000 DNS服务器在它的启动文件中只有缓存、主服务器和辅服务器指令。其他信息可能会导致问题或被忽略。

最后值得一提的不同点是BIND XFRNETS指令。本质上，微软 DNS不支持这个指令，并且它会在事件日志里产生一个错误信息，但是不会阻碍域名服务器的操作，仅仅标记一下这条不合法的指令，然后继续。

### 8.5 小结

本章收集了对提供给BIND和微软 DNS交互式操作的选项的评价。它表明了选择范围依赖于个人的目标，特别依赖于活动目录所需要或者在使用活动目录时所推荐的被支持的 DNS特征。当不需要活动目录支持时，除了一些特定的 BIND配置扩展外，BIND 8.1.2和Windows 2000 DNS完全可以互相交换和交互操作。