IBM

IBM i

联网
域名系统

V 7.2

IBM

IBM i

联网
域名系统

V 7.2

注

在使用本资料及其支持的产品之前，请务必阅读第 45 页的『声明』中的信息。

本版本适用于 IBM i 7.2（产品编号 5770-SS1）以及所有后续发行版和修订版，直到新版本中另有声明为止。本版本并不能在所有精简指令集计算机 (RISC) 机型上运行，也不能在 CISC 机型上运行。

本文档可能包含对许可内码的引用。许可内码是机器代码，需要遵守 IBM 机器代码许可协议的条款才许可您使用。

目录

域名系统

域名系统 (DNS) 是一个分布式数据库系统，用于管理主机名及其关联的因特网协议 (IP) 地址。

借助 DNS，人们可以使用简单名称（例如，www.jkltoys.com）而不是使用 IP 地址（例如，IPv4 地址 192.168.12.88 或 IPv6 地址 2001:D88::1）来找到主机。单个服务器可能只负责识别区域的一小部分的主机名和 IP 地址，但是 DNS 服务器可以一起工作，以将所有域名映射到其 IP 地址。一起工作的 DNS 服务器允许计算机通过因特网进行通信。

对于 IBM® i 7.2，DNS 服务基于业界标准 DNS 实现（称为 Berkeley 因特网名称域 (BIND) V9）。对于先前的 IBM i 发行版，DNS 服务基于 BIND V9 或 BIND V8 之前的 BIND。要在 V7R2 中使用新的 BIND V9 DNS 服务器，必须在 IBM i 上安装 IBM i 选项 31 (DNS) 和选项 33（可移植应用程序解决方案环境 (PASE)）以及 5733-SC1 选项 1 (OpenSSH, OpenSSL, zlib)。从 IBM i V6R1 开始，为了安全起见，已将 BIND 4 和 8 替换为 BIND 9。因此，需要将 DNS 服务器迁移至 BIND 9。

IBM i 7.2 的新增内容

请阅读域名系统 (DNS) 主题集合的新信息或有重大改动的信息。

DNS for i5/OS® 在此发行版中支持 DNSSEC。添加了新的命令和配置选项。

新的 DNSSEC 命令

添加了下列用于 DNSSEC 配置和维护的命令:

生成 DNSSEC 密钥 (GENDNSKEY)

"生成 DNS 密钥"(**GENDNSKEY**) 命令将按照 RFC 2535 和 RFC 4034 中的定义来生成 DNSSEC（安全 DNS）的密钥。它还按照 RFC 2845 中的定义来生成与 TSIG（事务签名）配合使用的密钥，或按照 RFC 2930 中的定义来生成与 TKEY（事务密钥）配合使用的密钥。缺省情况下，生成的文件将存储在 /QIBM/UserData/OS400/DNS/_DYN 目录中。

添加 DNSSEC 签名 (ADDDNSSIG)

"添加 DNS 签名"(**ADDDNSSIG**) 命令将签署区域。它生成 NSEC 和 RRSIG 记录，并产生区域的已签署版本。根据每个子区域的密钥集文件存在与否，来确定来自已签署区域的授权的安全性状态（即，子区域是否安全）。

生成 DNSSEC DS RR (GENDNSDSRR)

"生成 DNSSEC DS RR"(**GENDNSDSRR**) 命令将生成授权签署者 (DS) 资源记录 (RR)。

设置 DNSSEC REVOKE 位 (SETDNSRVK)

"设置 DNSSEC REVOKE 位"(**SETDNSRVK**) 命令将读取 DNSSEC 密钥文件，设置密钥上的 REVOKED 位，并创建一对包含现在撤销的密钥的新密钥文件。

新的配置命令

添加了下列命令，以创建 DDNS 的配置和打印区域日志文件的内容。

创建 DDNS 配置 (CRTDDNSCFG)

"创建 DDNS 配置"(**CRTDDNSCFG**) 命令将生成密钥供 NSUPDATE 命令和动态 DNS (DDNS) 服务器使用。它将生成密钥并提供 NSUPDATE 命令以及使用该命令将需要的 named.conf 语法（其中包括示例

update-policy 语句），从而简化了动态区域的配置。注意，DNS 服务器本身可以配置本地 DDNS 密钥以与 NSUPDATE LOCALHOST(*YES) 配合使用。仅当需要更复杂的配置时（例如，如果要从远程系统使用 NSUPDATE），才需要此命令。

转储 DNS 日志文件 (DMPDNSJRNF)

“转储 DNS 日志文件”(**DMPDNSJRNF**) 命令将以人类可读格式转储区域日志文件的内容。

相关概念:

第 12 页的『DNS 安全性扩展 (DNSSEC) 简介』

DNSSEC 是一套将安全性扩展添加到 DNS 的 IETF RFC 规范。

域名系统的 PDF 文件

可查看和打印此信息的 PDF 文件。

要查看或下载本文档的 PDF 版本，请选择《域名系统》（大约 625 KB）。

保存 PDF 文件

要将 PDF 保存在您的工作站上以便查看或打印:

1. 在浏览器中右键单击 PDF 链接。
2. 单击以本地方式保存 PDF 的选项。
3. 浏览到用于保存 PDF 的目录。
4. 单击**保存**。

下载 Adobe Reader

需要在系统上安装 Adobe Reader 以查看或打印这些 PDF。可以从 Adobe Web 站点（www.adobe.com/products/acrobat/readstep.html）  下载免费副本。

相关参考:

第 44 页的『域名系统的相关信息』

IBM Redbooks®出版物、Web 站点和其他信息中心主题集合包含与域名系统 (DNS) 主题集合相关的信息。可查看或打印其中任何 PDF 文件。

域名系统概念

域名系统 (DNS) 是一个分布式数据库系统，用于管理主机名及其关联的因特网协议 (IP) 地址。借助 DNS，您可以使用简单名称（例如，www.jkltoys.com）而不是使用 IP 地址（例如，IPv4 地址 192.168.12.88 或 IPv6 地址 2001:D88::1）来找到主机。

单个服务器可能只负责识别区域的一小部分的主机名和 IP 地址，但是 DNS 服务器可以一起工作，以将所有域名映射到其 IP 地址。一起工作的 DNS 服务器允许计算机通过因特网进行通信。

DNS 数据将分布到域层次结构中。服务器只负责识别数据的一小部分（例如，单个子域）。服务器直接负责的域部分称为区域。具有区域的完整主机信息和数据的 DNS 服务器是该区域的权威服务器。权威服务器可以使用其自己的资源记录来应答有关其区域中的主机的查询。查询过程取决于许多因素。『了解 DNS 查询』说明了客户机可以用来解析查询的途径。

了解区域

域名系统 (DNS) 数据将划分为可管理的数据集（称为*区域*）。并且其中的每个数据集都有特定的区域类型。

区域包含有关 DNS 域的一个或多个部分的名称和 IP 地址信息。包含区域的所有信息的服务器是域（称为*父区域*）的权威服务器。有时，将用于应答对特定子域的 DNS 查询的权限授予其他 DNS 服务器（称为*子区域*）是有意义的。在这种情况下，可以将域的 DNS 服务器配置为将子域查询提交给相应的服务器。

为了备份和冗余，区域数据常常存储在非权威 DNS 服务器的服务器上。这些其他服务器称为辅助服务器，它们从权威服务器中装入区域数据。配置辅助服务器将使您能够均衡对服务器的需求，并且还能够在主服务器发生故障时提供备份。辅助服务器通过执行区域传输从权威服务器中获取区域数据。当辅助服务器初始化时，它从主服务器装入区域数据的完整副本。当区域数据更改时，辅助服务器还会从主服务器或该域的其他辅助服务器重新装入区域数据。

DNS 区域类型

您可以使用 IBM i DNS 来定义区域的若干类型，以帮助您管理 DNS 数据:

主区域 主区域直接从主机上的文件装入区域数据。它可以包含副区域或子区域。它还可以包含资源记录（例如，主机、别名 (CNAME)、IPv4 地址 (A)、IPv6 地址 (AAAA) 或逆向映射指针 (PTR) 记录）。

注: 在其他 BIND 文档中，主区域有时称为*主控区域*。

副区域 副区域定义主区域中的某个区域。副区域使您能够将区域数据组织成可管理的部分。

子区域 子区域定义副区域并委托一个或多个名称服务器来负责管理副区域数据。

别名 (CNAME)
别名为主域名定义了备用名。

主机 主机对象将 A 和 PTR 记录映射到主机。可以使其他资源记录与主机关联。

辅助区域
辅助区域从区域的主服务器或另一辅助服务器装入区域数据。它维护其主区域的完整副本。

注: 在其他 BIND 文档中，辅助区域有时称为*从属区域*。

存根区域
存根区域类似于辅助区域，但是它仅传输该区域的名称服务器 (NS) 记录。

转发区域
转发区域将对特定区域的所有查询定向至其他服务器。

相关概念:

第 4 页的『了解域名系统查询』
域名系统 (DNS) 客户机使用 DNS 服务器来解析查询。查询可能直接来自客户机或客户机上运行的应用程序。

相关任务:

第 27 页的『配置名称服务器上的区域』
配置域名系统 (DNS) 服务器实例后，需要配置名称服务器的区域。

相关参考:

第 13 页的『示例: 内部网的单个域名系统服务器』
此示例描绘了一个简单子网，它具有一个供内部使用的域名系统 (DNS) 服务器。

第 8 页的『域名系统资源记录』
资源记录用来存储有关域名和 IP 地址的数据。您可以使用资源记录查找表来浏览 IBM i 操作系统所支持的

资源记录。

了解域名系统查询

域名系统 (DNS) 客户机使用 DNS 服务器来解析查询。查询可能直接来自客户机或客户机上运行的应用程序。

客户机将包含标准域名 (FQDN)、查询类型（例如，客户机需要的特定资源记录）和该域名的类（通常是因特网 (IN) 类）的查询消息发送至 DNS 服务器。下图以“具有因特网访问权的单个 DNS 服务器”作为示例描绘了样本网络。

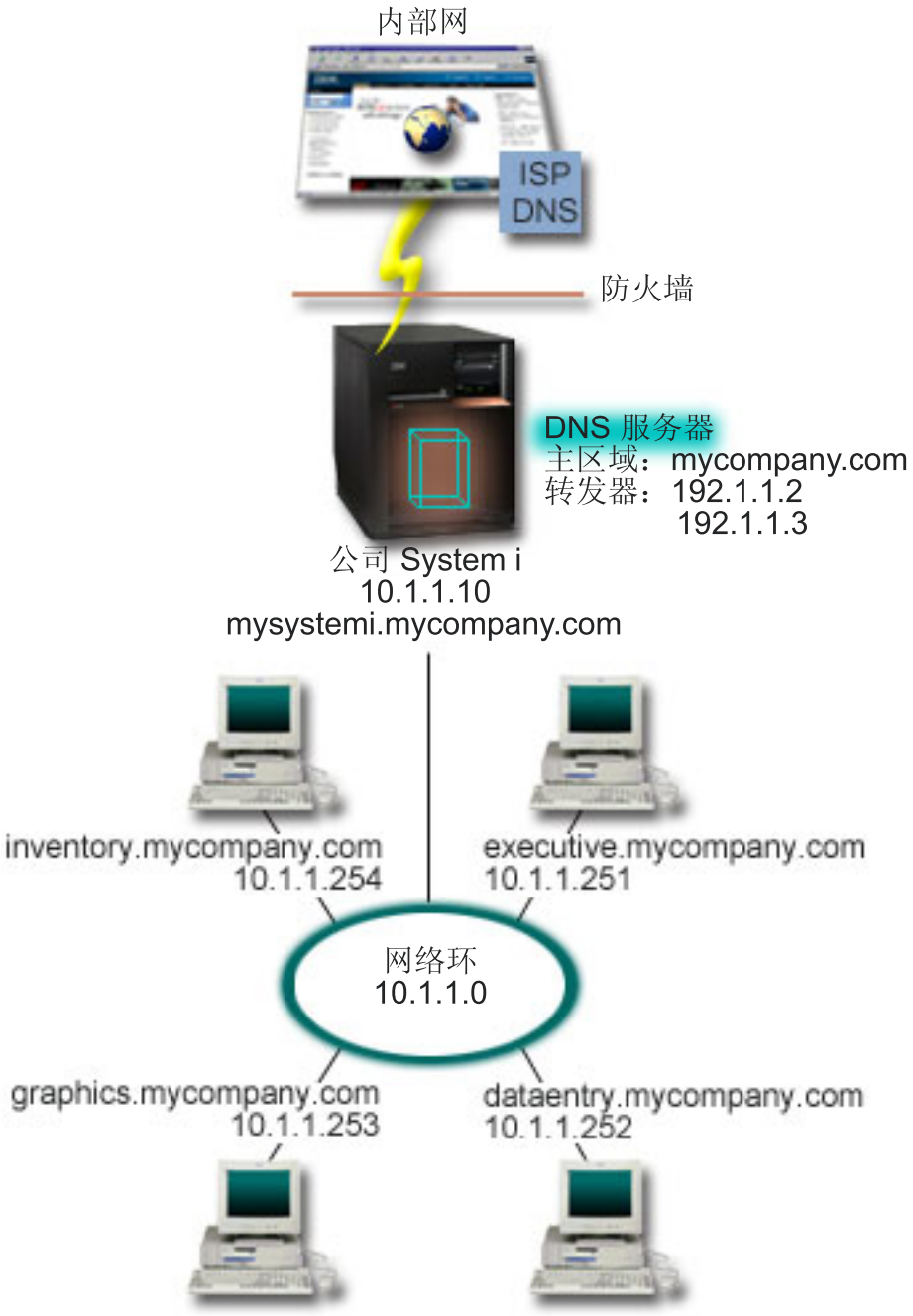

图 1. 具有因特网访问权的单个 DNS 服务器

假定主机 *dataentry* 向 DNS 服务器查询 graphics.mycompany.com。DNS 服务器使用其自己的区域数据并以 IP 地址 10.1.1.253 进行响应。

现在假定 *dataentry* 请求 www.jkl.com 的 IP 地址。此主机不在 DNS 服务器的区域数据中。可以使用两种途径：*递归*或*迭代*。如果某个 DNS 服务器设置为使用*递归*，那么该服务器可以为进行请求的客户机查询或联系其他 DNS 服务器，以完全解析该名称，然后将答案发送回该客户机。此外，进行请求的服务器还会将该答案存储在其高速缓存中，以便下次此服务器接收到该查询时可以使用该答案。如果某个 DNS 服务器设置为使用*迭代*，那么客户机可以尝试自己联系其他 DNS 服务器以解析名称。在此过程中，客户机根据服务器的引荐答案使用单独的查询和其他查询。

相关参考:

第 3 页的『了解区域』
域名系统 (DNS) 数据将划分为可管理的数据集（称为*区域*）。并且其中的每个数据集都有特定的区域类型。

第 15 页的『示例：具有因特网访问权的单个域名系统服务器』
此示例描绘了一个简单子网，它具有一个已直接连接至因特网的域名系统 (DNS) 服务器。

域名系统域设置

域名系统 (DNS) 域设置要求注册域名，以防止其他人使用您的域名。

DNS 允许您在内部网或内部网络上分配名称和地址。它还允许您通过因特网将名称和地址分配到世界上的其余地方。如果要在因特网上设置域，那么需要注册域名。

如果要设置内部网，那么不需要注册供内部使用的域名。是否要注册内部网名称取决于您是否要确保别人在因特网上永远无法使用该名称，而只有您内部才能使用。通过注册您打算在内部使用的名称，将确保您以后要在外部使用域名时永远不会有冲突。

可以通过直接与经授权的域名注册机构联系或通过某些因特网服务提供商 (ISP) 来执行域注册。某些 ISP 提供了为您提交域名注册请求的服务。因特网网络信息中心 (InterNIC) 维护了一个目录，该目录包含由因特网名称与数字地址分配机构 (ICANN) 授权的所有域名注册机构。

相关参考:

第 15 页的『示例：具有因特网访问权的单个域名系统服务器』
此示例描绘了一个简单子网，它具有一个已直接连接至因特网的域名系统 (DNS) 服务器。

相关信息:

因特网网络信息中心 (InterNIC)

动态更新

基于 BIND 9 的 IBM i 域名系统 (DNS) 支持动态更新。外部源（例如，动态主机配置协议 (DHCP)）可以将更新发送至 DNS 服务器。另外，您还可以使用 DNS 客户机工具（例如，动态更新实用程序 (NSUPDATE)）来执行动态更新。

DHCP 是一种 TCP/IP 标准，使用中央服务器来管理整个网络的 IP 地址和其他配置详细信息。DHCP 服务器通过动态地给客户机指定属性来响应它们的请求。DHCP 允许您在中央位置定义网络主机配置参数并允许自动配置主机。它常常用来将临时 IP 地址分配给其中客户机超过可用 IP 地址数的网络的客户机。

过去，所有 DNS 数据都存储在静态数据库中。必须由管理员创建并维护所有 DNS 资源记录。但是，可以配置基于 BIND 8 或更高版本的 DNS 服务器，域名注册机接受来自其他源的请求以动态更新区域数据。

可以配置 DHCP 服务器，以在它每次将新地址分配给主机时，将更新请求发送至 DNS 服务器。此自动过程将减少快速增长或更改的 TCP/IP 网络以及其中的主机频繁更改位置的网络中的 DNS 服务器管理工作。当使用 DHCP 的客户机接收到 IP 地址时，该数据会立即发送至 DNS 服务器。通过使用此方法，DNS 可以继续成功地解析对主机的查询，即使在主机的 IP 地址更改时也是如此。

您可以配置 DHCP，为客户机更新地址映射（A（对于 IPv4）或 AAA（对于 IPv6））记录和/或逆向查找指针 (PTR) 记录。地址映射记录（A 或 AAA）将机器的主机名映射到其 IP 地址。PTR 记录将机器的 IP 地址映射到其主机名。当客户机的地址更改时，DHCP 可以自动将更新发送至 DNS 服务器，因此网络中的其他主机可以通过 DNS 查询，在新的 IP 地址找到该客户机。对于动态更新的每条记录，将写入一条关联的文本 (TXT) 记录，以标识该记录由 DHCP 写入。

注: 如果设置 DHCP 以仅更新 PTR 记录，那么必须配置 DNS 以允许从客户机更新，以便每个客户机都可以更新其 A 记录（如果客户机使用 IPv4 地址）或其 AAA 记录（如果客户机使用 IPv6 地址）。并非所有 DHCP 客户机都支持发出其自己的 A 或 AAA 记录更新请求。在选择此方法之前，请查阅客户机平台的文档。

通过创建允许发送更新的经授权源的列表来保护动态区域。可以使用单独的 IP 地址、整个子网、已使用共享密钥（称为*事务签名*或 TSIG）签署的包或这些方法的任何组合来定义经授权源。DNS 会在更新资源记录之前验证入局请求包是否来自经授权源。

可以在单个 IBM i 平台上的 DNS 与 DHCP 之间、不同 IBM i 平台之间或 IBM i 平台与其他支持动态更新的系统之间执行动态更新。

注: 在要将动态更新发送至 DNS 的服务器上，需要“动态更新 DNS”(QTOBUPDT) API。它自动随 IBM i 选项 31 (DNS) 一起安装。但是，在 BIND 9 中，**NSUPDATE** 命令是 IBM i 平台上进行更新的首选方法。

相关概念:

动态主机配置协议

相关任务:

第 28 页的『配置域名系统以接收动态更新』
可以配置运行 BIND 9 的域名系统 (DNS) 服务器，域名注册机接受来自其他源的请求以动态更新区域数据。本主题提供有关配置 allow-update 选项以便 DNS 可以接收动态更新的指示信息。

配置 DHCP 以将动态更新发送至 DNS

第 35 页的『重新签署区域』
对于已签署的主区域，如果对该区域的资源记录进行了新的更改，那么该区域需要重新签署。

相关参考:

第 17 页的『示例: 同一 IBM i 上的域名系统和动态主机配置协议』
此示例描绘了同一 IBM i 平台上的域名系统 (DNS) 和动态主机配置协议 (DHCP)。

第 8 页的『域名系统资源记录』
资源记录用来存储有关域名和 IP 地址的数据。您可以使用资源记录查找表来浏览 IBM i 操作系统所支持的资源记录。

QTOBUPT

『BIND 9 功能』
BIND 9 类似于 BIND 8；但是，它提供了用来提高域名系统 (DNS) 服务器的性能的若干功能（例如，视图）。

BIND 9 功能

BIND 9 类似于 BIND 8；但是，它提供了用来提高域名系统 (DNS) 服务器的性能的若干功能（例如，视图）。

单个 IBM i DNS 服务器上的视图

view 语句允许单个 DNS 实例根据查询的来源（例如，因特网或内部网）以不同方式应答查询。

视图功能一种切实有效的应用是分割 DNS 设置，而不必运行多个 DNS 服务器。例如，在单个 DNS 服务器中，您可以定义一个视图来应答来自内部网络的查询，而定义另一个视图来应答来自外部网络的查询。

新的客户机命令

下列客户机命令增强了 DNS 服务器的管理功能:

动态更新实用程序 (NSUPDATE)

动态更新实用程序 (**NSUPDATE**) 命令用来向 DNS 服务器提交“请求评论”(RFC) 2136 中定义的动态 DNS 更新请求。这允许在 DNS 服务器运行时在区域中添加或除去资源记录。因此，您不需要通过手动编辑区域文件来更新记录。单个更新请求可以包含添加或除去多个资源记录的请求，但是，使用 **NSUPDATE** 命令动态添加或除去的资源记录应在同一区域中。

注: 不要使用 **NSUPDATE** 命令或通过 DHCP 服务器手动编辑处于动态控制下的区域。手动编辑可能与动态更新产生冲突，这将导致丢失数据。

启动 DIG 查询 (DIG)

与“名称服务器查找”(**NSLOOKUP**) 命令相比，域信息探索器 (DIG) 是一个功能更强大的查询工具，您可以使用它从 DNS 服务器中检索信息或者测试 DNS 服务器的响应。不推荐使用 **NSLOOKUP** 命令，提供它仅为了与更低版本兼容。在配置系统以使用 DNS 服务器之前，可以使用 DIG 来验证 DNS 服务器是否正确响应。还可以使用 DIG 来检索有关主机、域和其他 DNS 服务器的 DNS 信息。

可以使用“启动 DIG 查询”(**STRDIGQRY**) 命令或其别名 DIG 来启动“域信息探索器”工具。

启动 HOST 查询 (HOST)

“启动 HOST 查询”(**HOST**) 命令用于 DNS 查找。您可以使用它将域名转换为 IP 地址（IPv4 或 IPv6），反之亦然。

远程名称守护程序控制 (RNDC)

“远程名称守护程序控制”(**RNDC**) 命令是一个功能强大的实用程序，它使系统管理员能够控制名称服务器的运行。它读取名为 rndc.conf 的配置文件，以确定如何联系名称服务器以及确定它应使用的算法和密钥。如果找不到 rndc.conf 文件，那么缺省情况下，将使用安装期间创建的 rndc-key._KID 文件，该文件通过回送接口自动授予访问权。

IPv6 支持

BIND 9 支持当前已定义的所有 IPv6 格式的“名称到地址”和“地址到名称”查找。对于正向查找，BIND 9 支持 AAAA 记录和 A6 记录，但是现在不推荐使用 A6 记录。对于 IPv6 逆向查找，BIND 9 支持 ip6.arpa 域以及更早的已不推荐使用的 ip6.int 域中使用的传统“nibble”格式。

日志文件

日志文件用来保存区域的动态更新。首次接收到来自客户机的动态更新时，将自动创建日志文件，并且它不会消失。此文件是二进制文件，不应编辑。

有了日志文件后，服务器在关闭或崩溃后重新启动时，会重放该日志文件，以将最近一次区域转储后发生的所有更新合并到区域中。日志文件还用来存储递增区域传输 (IXFR) 方法的更新。

已重新设计 DNS for IBM i 以使用 BIND 9。要在系统上运行 BIND 9 DNS，系统必须满足某些软件需求。

相关概念:

第 25 页的『域名系统需求』
考虑在 IBM i 平台上运行域名系统 (DNS) 的这些软件需求。

第 5 页的『动态更新』
基于 BIND 9 的 IBM i 域名系统 (DNS) 支持动态更新。外部源（例如，动态主机配置协议 (DHCP)）可以将更新发送至 DNS 服务器。另外，您还可以使用 DNS 客户机工具（例如，动态更新实用程序 (NSUPDATE)）来执行动态更新。

相关参考:

第 19 页的『示例: 通过在同一 IBM i 上设置两个 DNS 服务器来分割防火墙上的 DNS』
此示例描绘了一个域名系统 (DNS) 服务器，该服务器在防火墙上运行，以保护内部数据不会流向因特网，而允许内部用户访问因特网上的数据。此配置通过在同一 IBM i 平台上设置两个 DNS 服务器来实现此保护。

第 24 页的『规划安全措施』
域名系统 (DNS) 提供了安全性选项，以限制外部对服务器的访问。

域名系统资源记录

资源记录用来存储有关域名和 IP 地址的数据。您可以使用资源记录查找表来浏览 IBM i 操作系统所支持的资源记录。

DNS 区域数据库由资源记录集合组成。每个资源记录指定有关特定对象的信息。例如，地址映射 (A) 记录将主机名映射到 IP 地址，而逆向查找指针 (PTR) 记录则将 IP 地址映射到主机名。服务器使用这些记录来应答对其区域中的主机的查询。有关更多信息，请使用下表来查看 DNS 资源记录。

注: 可能已根据 BIND 文档的更改在资源记录查找表中添加或除去了条目。而且，此表并非是 BIND 中列示的所有资源记录的完整列表。

表 1. 资源记录查找表

资源记录	缩写	描述
地址映射记录	A	A 记录指定此主机的 IP 地址。A 记录用来解析对特定域名的 IP 地址的查询。此记录类型在“请求评论”RFC 1035 中定义。
Andrew 文件系统数据库记录	AFSDB	AFSDB 记录指定对象的 AFS 或 DCE 地址。AFSDB 记录的使用与 A 记录相似，它用来将域名映射到其 AFSDB 地址；或从一个单元的域名映射到该单元的经认证的名称服务器。此记录类型在 RFC 1183 中定义。
规范名称记录	CNAME	CNAME 记录指定此对象的实际域名。当 DNS 查询别名并找到指向规范名的 CNAME 记录时，它接着查询那个规范域名。此记录类型在 RFC 1035 中定义。
DNSSEC 后备验证记录	DLV	DLV 记录指定 DNS 授权链外部的 DNSSEC 信任锚。它与 DS 记录使用相同的格式。此记录类型在 RFC 4431 中定义。

表 1. 资源记录查找表 (续)

资源记录	缩写	描述
DNS 密钥记录	DNSKEY	DNSKEY 记录指定 DNSSEC 密钥记录。区域使用专用密钥来签署其权威 RR 集，并将对应的公用密钥存储在 DNSKEY RR 中。此记录类型在 RFC 4034 中定义。
DS 记录	授权签署者	DS 记录指定受委托区域的 DNSSEC 签署密钥。此记录类型在 RFC 4034 中定义。
主机信息记录	HINFO	HINFO 记录指定有关主机的常规信息。标准 CPU 和操作系统名称在“指定编号”RFC 1700 中定义。但是，标准编号的使用并不是必需的。此记录类型在 RFC 1035 中定义。
综合业务数字网记录	ISDN	ISDN 记录指定此对象的地址。此记录将主机名映射到 ISDN 地址。它们仅在 ISDN 网络中使用。此记录类型在 RFC 1183 中定义。
IP V6 地址记录	AAAA	AAAA 记录指定主机的 128 位 IPv6 地址。AAAA 记录类似于 A 记录，用来解析对特定域名的 IPv6 地址的查询。此记录类型在 RFC 1886 中定义。
位置记录	LOC	LOC 记录指定网络组件的物理位置。应用程序可以使用这些记录来评估网络效率或映射物理网络。此记录类型在 RFC 1876 中定义。
邮件交换程序记录	MX	MX 记录为发送至此域的邮件定义邮件交换程序主机。这些记录由简单电子邮件传输协议 (SMTP) 使用，以找到为此域处理或转发邮件的主机以及每个邮件交换程序主机的优先选择值。每个邮件交换程序主机都必须在有效区域中具有对应的主机地址 (A) 记录。此记录类型在 RFC 1035 中定义。
邮件组记录	MG	MG 记录指定邮件组域名。此记录类型在 RFC 1035 中定义。
邮箱记录	MB	MB 记录指定包含此对象的邮箱的主机域名。将发送至域的邮件定向至 MB 记录中指定的主机。此记录类型在 RFC 1035 中定义。
邮箱信息记录	MINFO	MINFO 记录指定应接收此对象的消息或错误的邮箱。MINFO 记录更常用于邮寄列表，而不那么常用于单一邮箱。此记录类型在 RFC 1035 中定义。
邮箱重命名记录	MR	MR 记录指定邮箱的新域名。使用 MR 记录作为已移至另一邮箱的用户的转发项。此记录类型在 RFC 1035 中定义。

表 1. 资源记录查找表 (续)

资源记录	缩写	描述
名称服务器记录	NS	NS 记录指定此主机的权威名称服务器。此记录类型在 RFC 1035 中定义。
下一个安全记录	NSEC	NSEC 记录指定用来证明名称的数据不存在。此记录类型在 RFC 4034 中定义。
NSEC V3 记录	NSEC3	NSEC3 记录指定已证实 DNS 资源记录集不存在的数据。此记录类型在 RFC 5155 中定义。
NSEC3 参数	NSEC3PARAM	NSEC3PARAM 指定与 NSEC3 配合使用的参数。此记录类型在 RFC 5155 中定义。
网络服务访问协议记录	NSAP	NSAP 记录指定 NSAP 资源的地址。NSAP 记录用来将域名映射到 NSAP 地址。此记录类型在 RFC 1706 中定义。
公用密钥记录	KEY	KEY 记录指定与 DNS 名称关联的公用密钥。该密钥可以用于区域、用户或主机。此记录类型在 RFC 2065 中定义。
责任人记录	RP	RP 记录指定负责此区域或主机的人员的因特网邮件地址和描述。此记录类型在 RFC 1183 中定义。
逆向查找指针记录	PTR	PTR 记录指定主机的域名，您希望为该主机定义 PTR 记录。在给定 IP 地址的情况下，PTR 记录允许查找主机名。此记录类型在 RFC 1035 中定义。
DNSSEC 签名	RRSIG	RRSIG 记录指定 DNSSEC 验证流程中使用的数字签名。此记录类型在 RFC 4034 中定义。
路由通过记录	RT	RT 记录指定主机域名，该主机可以充当此主机的 IP 包的转发器。此记录类型在 RFC 1183 中定义。
服务记录	SRV	SRV 记录指定一些主机，这些主机支持该记录中定义的服务。此记录类型在 RFC 2782 中定义。
起始权限记录	SOA	SOA 记录指定此服务器是此区域的权威服务器。权威服务器是一个区域中数据的最佳来源。SOA 记录包含关于该区域的常规信息和辅助服务器的重新装入规则。每个区域只能有一个 SOA 记录。此记录类型在 RFC 1035 中定义。

表 1. 资源记录查找表 (续)

资源记录	缩写	描述
文本记录	TXT	TXT 记录指定要与某个域名关联的多个文本字符串，每个字符串的最大长度为 255 个字符。TXT 记录可以与责任人 (RP) 记录配合使用，以提供有关谁对一个区域负责的信息。此记录类型在 RFC 1035 中定义。 TXT 记录由 IBM i DHCP 用于动态更新。DHCP 服务器会为它更新的每条 PTR 和 A 记录都写入一条关联的 TXT 记录。DHCP 记录具有前缀 AS400DHCP。
熟知服务记录	WKS	WKS 记录指定此对象所支持的熟知服务。最常见的情况是，WKS 记录指示此地址是支持 TCP 还是支持 UDP，或是两种协议都支持。此记录类型在 RFC 1035 中定义。
X.400 地址映射记录	PX	PX 记录是指向 X.400/RFC 822 映射信息的指针。此记录类型在 RFC 1664 中定义。
X25 地址映射记录	X25	X25 记录指定 X25 资源的地址。此记录将主机名映射到 PSDN 地址。它们仅在 X25 网络中使用。此记录类型在 RFC 1183 中定义。

相关概念:

『邮件和邮件交换程序记录』
域名系统 (DNS) 通过使用邮件和邮件交换程序 (MX) 记录来支持高级邮件路由。

相关参考:

第 13 页的『示例: 内部网的单个域名系统服务器』
此示例描绘了一个简单子网，它具有一个供内部使用的域名系统 (DNS) 服务器。

第 3 页的『了解区域』
域名系统 (DNS) 数据将划分为可管理的数据集（称为*区域*）。并且其中的每个数据集都有特定的区域类型。

邮件和邮件交换程序记录

域名系统 (DNS) 通过使用邮件和邮件交换程序 (MX) 记录来支持高级邮件路由。

邮件和 MX 记录由邮件路由程序（例如，简单电子邮件传输协议 (SMTP)）使用。DNS 资源记录中的查找表包含 IBM i DNS 所支持的邮件记录类型。

DNS 包括有关使用邮件交换程序信息发送电子邮件的信息。如果网络在使用 DNS，那么 SMTP 应用程序不会通过打开与 TEST.IBM.COM 的 TCP 连接来传递目标地址为主机 TEST.IBM.COM 的邮件。SMTP 首先查询 DNS 服务器，以查明可以使用哪些主机服务器来传递该消息。

将邮件传递至特定地址

DNS 服务器使用称为*邮件交换程序* (MX) 记录的资源记录。MX 记录将域名或主机名映射到优先选择值和主机名。MX 记录通常用来指定使用一台主机来处理另一台主机的邮件。这些记录还用来指定当无法访问第一台主机时，要将邮件传递至的另一台主机。换句话说，这些记录允许将目标地址为一台主机的邮件传递至其他主机。

同一域名或主机名可能存在多个 MX 资源记录。当同一域或主机存在多条 MX 记录时，每条记录的优先选择（或优先级）值确定尝试这些记录的顺序。最小的优先选择值对应于优先级最高的记录，将首先尝试该记录。当无法访问优先级最高的主机时，发送邮件的应用程序会尝试联系下一台优先级次高的 MX 主机。域管理员或 MX 记录的创建者设置优先选择值。

当名称在 DNS 服务器的权限之内，但尚未对该名称分配 MX 时，DNS 服务器会使用没有任何 MX 资源记录的空列表进行响应。出现这种情况时，发送邮件的应用程序可能会尝试直接建立与目标主机的连接。

注: 建议不要在域的 MX 记录中使用通配符（例如: `*.mycompany.com`）。

示例: 主机的 MX 记录

在以下示例中，系统优先将 fsc5.test.ibm.com 的邮件传递至该主机本身。如果无法访问该主机，那么系统可能将邮件传递至 psfred.test.ibm.com 或 mvs.test.ibm.com（如果也无法访问 psfred.test.ibm.com）。以下是这些 MX 记录将具有的类似内容的示例:

```
fsc5.test.ibm.com   IN MX 0 fsc5.test.ibm.com
                    IN MX 2 psfred.test.ibm.com
                    IN MX 4 mvs.test.ibm.com
```

相关参考:

第 8 页的『域名系统资源记录』
资源记录用来存储有关域名和 IP 地址的数据。您可以使用资源记录查找表来浏览 IBM i 操作系统所支持的资源记录。

DNS 安全性扩展 (DNSSEC) 简介

DNSSEC 是一套将安全性扩展添加到 DNS 的 IETF RFC 规范。

原始 DNS 协议不支持安全性。DNS 数据在主服务器与解析器之间可能被篡改和损坏，因为 DNS 未提供用于验证响应的机制。这使 DNS 容易受到这些类型的攻击。

DNSSEC 在支持 TSIG/SIG0 的服务器之间提供已认证的通信。可以建立信任链来验证数据真实性和完整性。

在 DNS 区域中，将通过区域签署密钥 (ZSK) 签署 DNS 区域数据，并通过密钥签署密钥 (KSK) 签署 ZSK。可以将授权签署者 (DS) 资源记录 (RR)（它源自于 KSK）复制到父区域以形成信任链。所以安全区域的 RR 集将包含: DNSKEY（ZSK 和 KSK）RR、RRSIG（资源记录签名）RR、下一个安全 (NSEC) RR 和（可选）子区域的 DS RR。

当启用安全性的 DNS 解析器获得查询答案时，它将尝试使用区域的 DNSKEY RR 来验证 RRSIG RR。然后它将使用可以从父区域获取的 DS RR 来验证 DNSKEY RR，以同样的方式继续，直到 DNSKEY RR 或 DS RR 与解析器中配置的信任锚匹配为止。

有关 DNSSEC 的更多信息，请参阅 RFC 4033、4034 和 4035。

相关概念:

第 1 页的『IBM i 7.2 的新增内容』
请阅读域名系统 (DNS) 主题集合的新信息或有重大改动的信息。

第 32 页的『管理域名系统』
管理域名系统 (DNS) 服务器的过程包括验证 DNS 功能是否起作用、是否维护 DNSSEC、是否监视性能以及是否维护 DNS 数据和文件。

第 35 页的『管理 DNSSEC』
本主题介绍 IBM i 平台上的 DNSSEC 维护。

示例: 域名系统

您可以使用这些示例来了解如何在网络中使用域名系统 (DNS)。

DNS 是一个分布式数据库系统，用于管理主机名及其关联的 IP 地址。下列示例帮助说明 DNS 如何工作以及您如何才能在网络使用 DNS。这些示例描述了将使用 DNS 的设置和原因。这些示例还链接至相关概念，您可能会发现这些概念对于理解图片很用。

示例: 内部网的单个域名系统服务器

此示例描绘了一个简单子网，它具有一个供内部使用的域名系统 (DNS) 服务器。

下图描绘了在内部网络的 IBM i 平台上运行的 DNS。此单个 DNS 服务器实例已设置为侦听所有接口 IP 地址上的查询。系统是 mycompany.com 区域的主名称服务器。

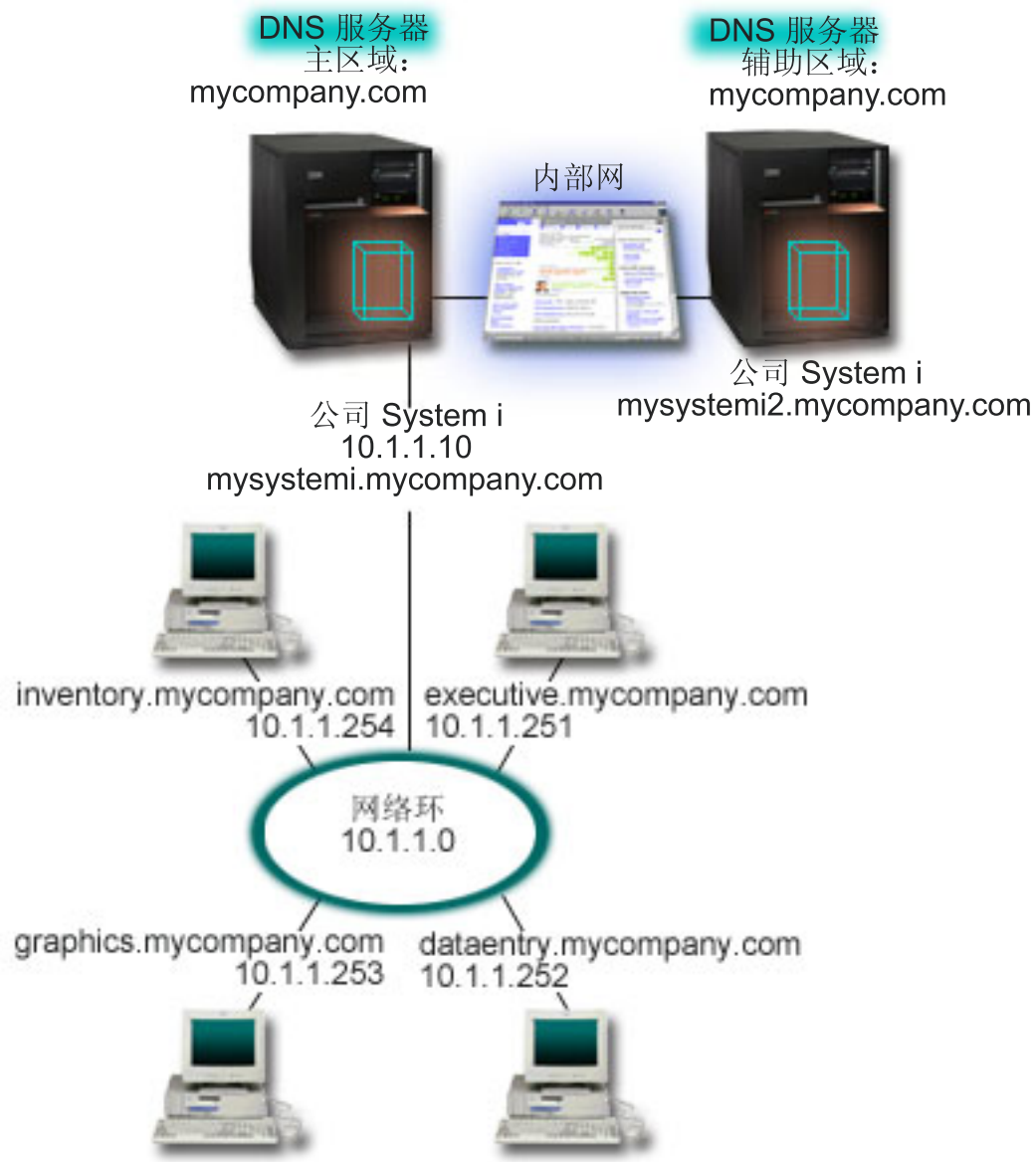

图 2. 内部网的单个 DNS 服务器

区域中的每台主机都有一个 IP 地址和域名。管理员必须通过创建资源记录手动定义 DNS 区域数据中的主机。地址映射记录（A（对于 IPv4）或 AAAA（对于 IPv6））将机器的名称映射到其关联的 IP 地址。这允许网络上的其他主机查询 DNS 服务器，以查找分配给特定主机名的 IP 地址。逆向查找指针 (PTR) 记录将机器的 IP 地址映射到其关联的名称。这允许网络上的其他主机查询 DNS 服务器，以查找与 IP 地址对应的主机名。

除了 A、AAAA 和 PTR 记录之外，DNS 还支持许多其他资源记录，根据内部网上运行的其他基于 TCP/IP 的应用程序，可能需要这些资源记录。例如，如果正在运行内部电子邮件系统，那么可能需要添加邮件交换程序 (MX) 记录，以便 SMTP 可以查询 DNS，以查明哪些系统正在运行邮件服务器。

如果这个小网络是更大内部网的一部分，那么可能必须定义内部根服务器。

辅助服务器

辅助服务器从权威服务器中装入区域数据。辅助服务器通过执行区域传输从权威服务器中获取区域数据。当辅助名称服务器启动时，它从主名称服务器请求指定域的所有数据。辅助名称服务器从主服务器请求已更新的数据有以下两种原因：它接收到来自主名称服务器的通知（如果正在使用 NOTIFY 功能），或者它查询主名称服务器并确定数据已更改。在上图中，mysystemi 服务器是内部网的一部分。另一个系统 mysystemi2 已配置为充当 mycompany.com 区域的辅助 DNS 服务器。辅助服务器可以用来均衡对服务器的需求，并且还可以在主服务器发生故障时提供备份。每个区域至少有一个辅助服务器是一种良好的习惯做法。

相关参考:

第 8 页的『域名系统资源记录』
资源记录用来存储有关域名和 IP 地址的数据。您可以使用资源记录查找表来浏览 IBM i 操作系统所支持的资源记录。

第 3 页的『了解区域』
域名系统 (DNS) 数据将划分为可管理的数据集（称为*区域*）。并且其中的每个数据集都有特定的区域类型。

『示例：具有因特网访问权的单个域名系统服务器』
此示例描绘了一个简单子网，它具有一个已直接连接至因特网的域名系统 (DNS) 服务器。

示例：具有因特网访问权的单个域名系统服务器

此示例描绘了一个简单子网，它具有一个已直接连接至因特网的域名系统 (DNS) 服务器。

下图描绘了与“内部网的单个 DNS 服务器”示例相同的示例网络，但是现在公司已添加与因特网的连接。在此示例中，公司能够访问因特网，但是防火墙已配置为阻止因特网流量进入网络。

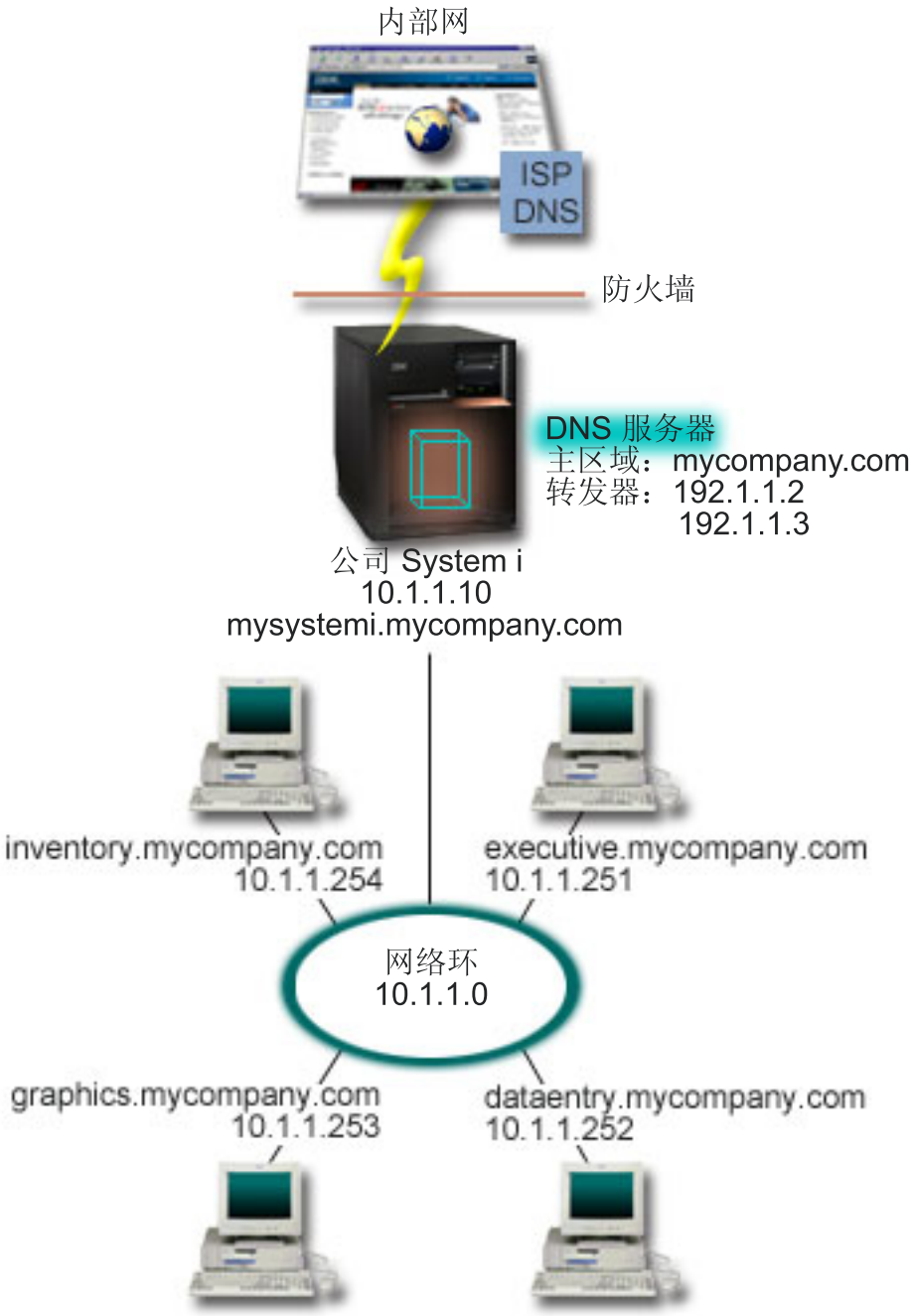

图 3. 具有因特网访问权的单个 DNS 服务器

要解析因特网地址，您至少需要执行下列其中一个任务:

- 定义因特网根服务器

  您可以自动装入缺省因特网根服务器，但是可能需要更新该列表。这些服务器可以帮助解析您自己的区域外部的地址。有关获取当前因特网根服务器的指示信息，请参阅访问外部域名系统数据。
- 启用转发

您可以设置转发，以将对 mycompany.com 的外部区域的查询传递至外部 DNS 服务器（例如，由因特网服务提供商 (ISP) 运行的 DNS 服务器）。如果要启用同时使用转发和根服务器的搜索，那么需要将 forward 选项设置 **first**。服务器首先尝试转发，然后，仅当转发未能解析查询时，才查询根服务器。

可能需要进行下列配置更改:

- 分配不受限 IP 地址

  在以上示例中，显示了 10.x.x.x 地址。但是，这些地址是受限地址，不能在内部网的外部使用。将它们显示在下面是为了示例目的，但是您自己的 IP 地址由您的 ISP 和其他联网因素确定。

- 注册域名

  如果您能够访问因特网，但是尚未注册，那么需要注册域名。

- 建立防火墙

  建议您不要允许 DNS 直接连接至因特网。您需要配置防火墙或采取其他预防措施来保护 IBM i 平台。

相关概念:

第 5 页的『域名系统域设置』
域名系统 (DNS) 域设置要求注册域名，以防止其他人使用您的域名。

System i 和因特网安全性

第 4 页的『了解域名系统查询』
域名系统 (DNS) 客户机使用 DNS 服务器来解析查询。查询可能直接来自客户机或客户机上运行的应用程序。

相关参考:

第 13 页的『示例: 内部网的单个域名系统服务器』
此示例描绘了一个简单子网，它具有一个供内部使用的域名系统 (DNS) 服务器。

示例: 同一 IBM i 上的域名系统和动态主机配置协议

此示例描绘了同一 IBM i 平台上的域名系统 (DNS) 和动态主机配置协议 (DHCP)。

当 DHCP 将 IP 地址分配给主机时，可以使用该配置来动态更新 DNS 区域数据。

下图描绘了一个小子网网络，它有一个 IBM i 平台，该平台充当四个客户机的 DHCP 和 DNS 服务器。在此工作环境中，假定库存客户机、数据输入客户机和管理客户机使用图形文件服务器中的图形创建文档。这些客户机通过将网络驱动器映射到图形文件服务器的主机名来连接至该服务器。

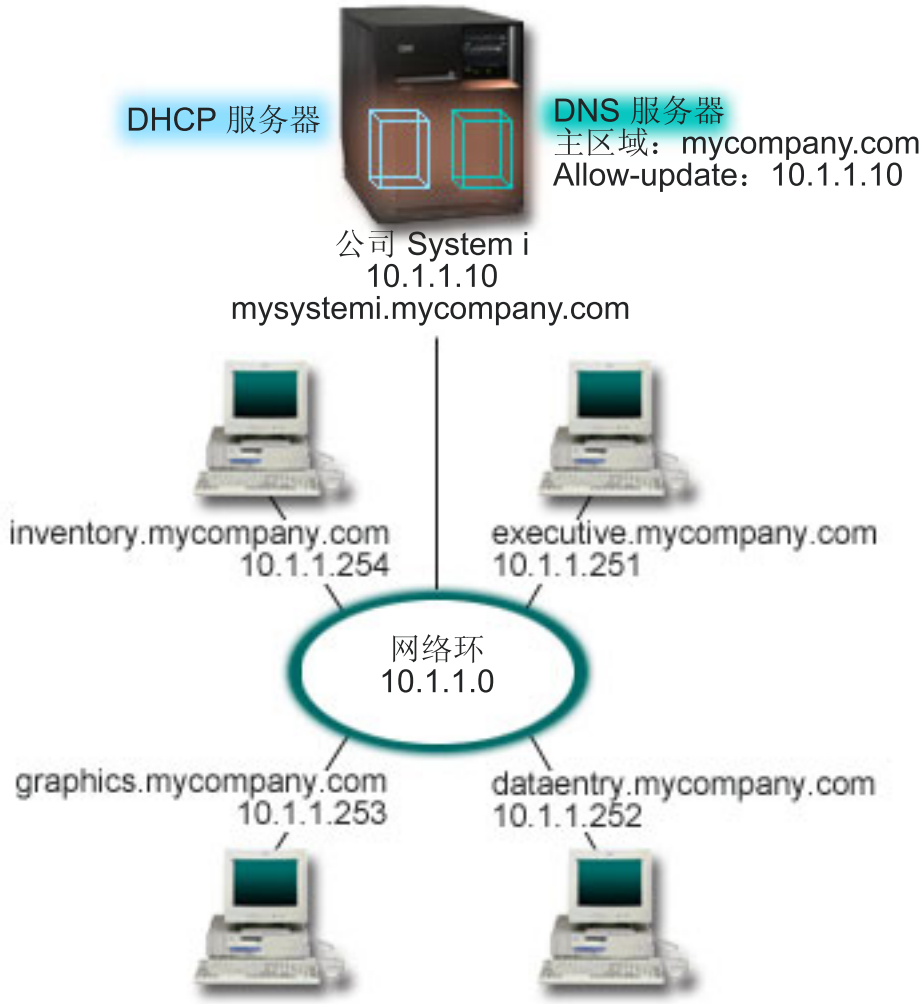

图 4. 同一 IBM i 平台上的 DNS 和 DHCP

DHCP 和 DNS 的先前版本彼此独立。如果 DHCP 将新 IP 地址分配给客户机，那么 DNS 记录必须由管理员手动更新。在此示例中，如果图形文件服务器的 IP 地址因为该地址由 DHCP 分配而更改，那么其从属客户机无法将网络驱动器映射到其主机名，因为 DNS 记录将包含该文件服务器的先前 IP 地址。

借助基于 BIND 9 的 IBM i DNS 服务器，您可以配置 DNS 区域，以接受对 DNS 记录的动态更新以及通过 DHCP 进行的间歇地址更改。例如，当图形文件服务器更新其租赁并且由 DHCP 服务器分配了 IP 地址 10.1.1.250 时，将动态更新关联的 DNS 记录。这允许其他客户机连续不断地查询 DNS 服务器，以按主机名找到图形文件服务器。

要配置 DNS 区域以接受动态更新，请完成下列任务:

- 标识动态区域

  当服务器在运行时，不能手动更新动态区域。这样做可能导致与入局动态更新产生冲突。可以在服务器停止时进行手动更新，但是您将失去服务器关闭期间发送的所有动态更新。因此，您可能要配置单独的动态区域，以最大程度地减小对手动更新的需要。有关配置区域以使用动态更新功能的更多信息，请参阅确定域结构。
- 配置 allow-update 选项

配置了 allow-update 选项的区域将视为动态区域。将逐个区域地设置 allow-update 选项。要接受动态更新，必须对此区域启用 allow-update 选项。对于此示例，mycompany.com 区域具有 allow-update 数据，但是服务器上定义的其他区域可以配置为静态或动态区域。

- 配置 DHCP 以发送动态更新

  您必须对 DHCP 服务器进行授权，以更新它已分发的 IP 地址的 DNS 记录。

- 配置辅助服务器更新首选项

  要使辅助服务器成为当前服务器，可以配置 DNS，以在区域数据更改时使用 NOTIFY 功能将消息发送至 mycompany.com 区域的辅助服务器。还应配置递增区域传输 (IXFR)，这使启用了 IXFR 的辅助服务器能够仅跟踪和装入已更新的区域数据，而不是整个区域。

如果您在不同服务器上运行 DNS 和 DHCP，那么 DHCP 服务器有一些其他配置需求。

相关概念:

第 5 页的『动态更新』
基于 BIND 9 的 IBM i 域名系统 (DNS) 支持动态更新。外部源（例如，动态主机配置协议 (DHCP)）可以将更新发送至 DNS 服务器。另外，您还可以使用 DNS 客户机工具（例如，动态更新实用程序 (NSUPDATE)）来执行动态更新。

相关任务:

配置 DHCP 以将动态更新发送至 DNS

相关参考:

示例: 不同 System i 平台上的 DNS 和 DHCP

示例: 通过在同一 IBM i 上设置两个 DNS 服务器来分割防火墙上的 DNS

此示例描绘了一个域名系统 (DNS) 服务器，该服务器在防火墙上运行，以保护内部数据不会流向因特网，而允许内部用户访问因特网上的数据。此配置通过在同一 IBM i 平台上设置两个 DNS 服务器来实现此保护。

下图描绘了一个简单子网网络，为了安全起见，它使用了防火墙。假定公司有一个保留了 IP 空间的内部网络和一个公众可以访问的网络的外部部分。公司希望其内部客户机能够解析外部主机名以及与外部的人员交换邮件。公司还希望其内部解析器能够访问某些仅供内部使用的区域，在内部网络的外部根本无法访问这些区域。但是，公司不希望任何外部解析器能够访问内部网络。

借助基于 BIND 9 的 IBM i DNS，您可以使用两种方式来实现此目的。第一种方式是公司在同一 IBM i 平台上设置两个 DNS 服务器实例，一个用于内部网，另一个用于其公共域中的一切，此示例中描述了该方式。另一种方式是使用 BIND 9 中提供的视图功能，在有关使用视图来分割防火墙上的 DNS 的示例中描述了该方式。

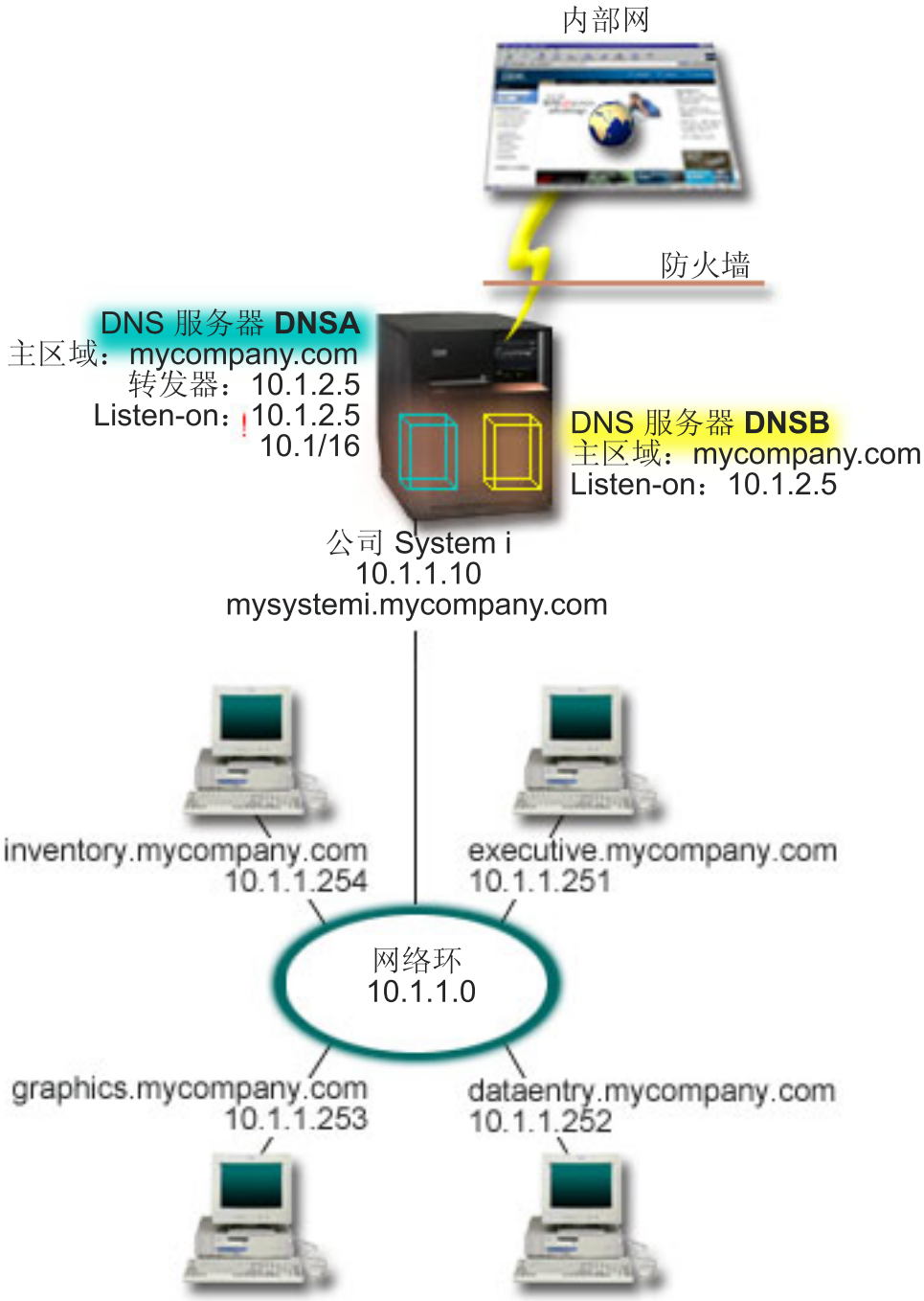

图 5. 通过在同一 System i 上设置两个 DNS 服务器来分割防火墙上的 DNS

使用主区域 mycompany.com 配置了外部服务器 DNSB。此区域数据仅包括打算作为公共域的一部分的资源记录。使用主区域 mycompany.com 配置了内部服务器 DNSA，但是 DNSA 上定义的区域数据包含内部网资源记录。转发器选项已定义为 10.1.2.5。这样会强制 DNSA 将其无法解析的查询转发至 DNSB 服务器。

如果您担心防火墙的完整性或其他安全性威胁，那么可以选择使用 listen-on 选项来帮助保护内部数据。为此，您可以配置内部服务器，以仅允许从内部主机查询内部 mycompany.com 区域。为了完全实现此目的，需要配置内部客户机，以仅查询 DNSA 服务器。您需要考虑使用下列配置设置来分割 DNS:

- Listen-on

在其他 DNS 示例中，只有一个 DNS 服务器在 IBM i 平台上。已将它设置为侦听所有接口 IP 地址。当 IBM i 平台上有多个 DNS 服务器时，您必须定义每个 DNS 服务器所侦听的接口 IP 地址。两个 DNS 服务器不能侦听同一地址。在这种情况下，假定从防火墙进入的所有查询都是在 10.1.2.5 上发送。应将这些查询发送至外部服务器。因此，将 DNSB 配置为侦听 10.1.2.5。将内部服务器 DNSA 配置为接受来自 10.1.x.x 接口 IP 地址（10.1.2.5 除外）上的任何对象的查询。要有效地排除此地址，地址匹配列表必须将排除的地址列示在包括的地址前缀之前。

- 地址匹配列表顺序

  将使用地址匹配列表中与给定地址匹配的第一个元素。例如，要允许 10.1.x.x 网络上除 10.1.2.5 之外的所有地址，ACL 元素的顺序必须是 (!10.1.2.5; 10.1/16)。在这种情况下，地址 10.1.2.5 将与第一个元素进行比较，并且将立即拒绝该地址。

  如果反转了这些元素 (10.1/16; !10.1.2.5)，那么将允许 IP 地址 10.1.2.5 访问，因为服务器会将该 IP 地址与第一个元素进行比较，而该 IP 地址匹配，从而允许该 IP 地址访问，而不会检查其余的规则。

相关参考:

第 6 页的『BIND 9 功能』
BIND 9 类似于 BIND 8；但是，它提供了用来提高域名系统 (DNS) 服务器的性能的若干功能（例如，视图）。

『示例: 使用视图来分割防火墙上的 DNS』
此示例描绘了一个域名系统 (DNS) 服务器，该服务器在防火墙上运行，以保护内部数据不会流向因特网，而允许内部用户使用 BIND 9 提供的*视图*功能来访问因特网上的数据。

示例: 使用视图来分割防火墙上的 DNS

此示例描绘了一个域名系统 (DNS) 服务器，该服务器在防火墙上运行，以保护内部数据不会流向因特网，而允许内部用户使用 BIND 9 提供的*视图*功能来访问因特网上的数据。

下图描绘了一个简单子网网络，为了安全起见，它使用了防火墙。假定公司有一个保留了 IP 空间的内部网络和一个公众可以访问的网络的外部部分。公司希望其内部客户机能够解析外部主机名以及与网络外部的人员交换邮件。公司还希望其内部解析器能够访问某些仅供内部使用的区域，在内部网络的外部无法访问这些区域。但是，公司不希望任何外部解析器能够访问内部网络。

借助基于 BIND 9 的 IBM i DNS，您可以使用两种方式来实现此目的。此示例中描述的方式如下：您可以使用两个不同视图来配置 DNS 服务器以侦听各种查询，一个视图用于内部网，另一个视图用于其公共域中的一切。另一种方式是在同一 IBM i 平台上设置两个 DNS 服务器实例，在有关使用两个 DNS 服务器来分割防火墙上的 DNS 的示例中描述了该方式。

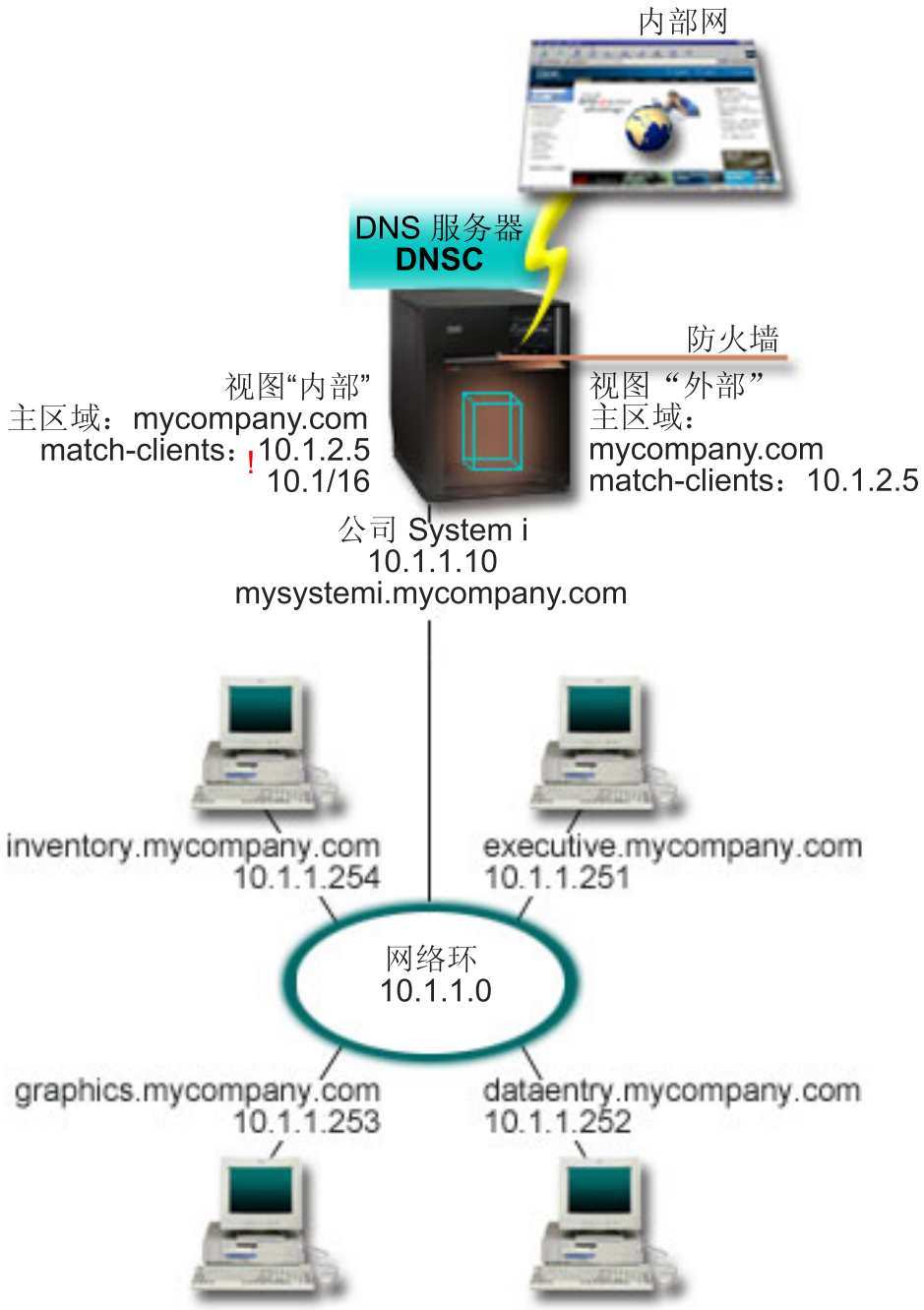

图 6. 使用视图来分割防火墙上的 DNS

DNS 服务器 DNSC 定义两个称为*外部*和*内部*的视图。使用主区域 mycompany.com 配置了*外部*视图，该区域仅包含打算作为公共域的一部分的资源记录，而使用包含内部网资源记录的主区域 mycompany.com 配置了*内部*视图。

如果您担心防火墙的完整性或其他安全性威胁，那么可以选择使用 match-clients 子语句来帮助保护内部数据。为此，您可以配置内部视图，以仅允许从内部主机查询内部 mycompany.com 区域。您需要考虑使用下列配置设置来设置已分割的 DNS:

- Match-clients

view 语句中的 match-clients 采用地址匹配列表作为自变量。仅当查询的 IP 地址与地址匹配列表匹配时，该查询才能查看封闭视图中定义的配置值。如果查询的 IP 地址与多个 view 语句中的多个 match-clients 条目匹配，那么将应用第一个 view 语句。在这种情况下，假定来自防火墙的所有查询都是在 10.1.2.5 中发送。应通过外部视图中的区域数据来处理这些查询。因此，将 10.1.2.5 设置为外部视图的 match-clients。将内部视图配置为接受来自 10.1.x.x 接口 IP 地址（10.1.2.5 除外）上的任何对象的查询。要有效地排除此地址，地址匹配列表必须将排除的地址列示在包括的地址前缀之前。

- 地址匹配列表顺序

  将使用地址匹配列表中与给定地址匹配的第一个元素。例如，要允许 10.1.x.x 网络上除 10.1.2.5 之外的所有地址，ACL 元素的顺序必须是 (!10.1.2.5; 10.1/16)。在这种情况下，地址 10.1.2.5 将与第一个元素进行比较，并且将立即拒绝该地址。

  如果反转了这些元素 (10.1/16; !10.1.2.5)，那么将允许 IP 地址 10.1.2.5 访问，因为服务器会将该 IP 地址与第一个元素进行比较，而该 IP 地址匹配，从而允许该 IP 地址访问，而不会检查其余的规则。

相关参考:

第 19 页的『示例: 通过在同一 IBM i 上设置两个 DNS 服务器来分割防火墙上的 DNS』
此示例描绘了一个域名系统 (DNS) 服务器，该服务器在防火墙上运行，以保护内部数据不会流向因特网，而允许内部用户访问因特网上的数据。此配置通过在同一 IBM i 平台上设置两个 DNS 服务器来实现此保护。

规划域名系统

域名系统 (DNS) 提供了多种解决方案。在配置 DNS 之前，对它在网络中的工作方式进行规划很重要。应评估诸如网络结构、性能和安全性之类的主题。

确定域名系统权限

域名系统 (DNS) 管理员有特殊的权限需求。您还应该考虑权限的安全隐患。

设置 DNS 时，应采取安全预防措施，以保护您的配置。您需要确定哪些用户有权更改配置。

要允许管理员配置和管理 DNS，对于权限级别有一个最低要求。授予所有对象访问权将确保管理员能够执行 DNS 管理任务。建议配置 DNS 的用户应具有安全主管访问权以及所有对象权限 (*ALLOBJ)。使用 System i® 导航器来对用户进行授权。如果您需要更多信息，请参阅 DNS 联机帮助中的“对 DNS 管理员进行授权”主题。

注: 如果管理员的概要文件不具有全部权限，那么必须授予该管理员特定访问权以及对所有 DNS 目录和相关配置文件的权限。

相关参考:

第 38 页的『维护域名系统配置文件』
可以在 IBM i 平台上使用 IBM i DNS 来创建和管理 DNS 服务器实例。DNS 的配置文件由 IBM Navigator for i 管理。不得手动编辑这些文件。请始终使用 IBM Navigator for i 来创建、更改或删除 DNS 配置文件。

确定域结构

如果您是第一次设置域，那么应在创建区域之前对需求和维护进行规划。

确定以下几点很重要: 如何将域或子域划分成区域、如何为网络需求提供最佳服务、如何访问因特网以及如何越过防火墙。这些因素可能比较复杂，必须根据实际情况进行处理。有关更深入的准则，请参阅权威源（例如，O'Reilly 的 DNS and BIND 一书）。

如果您将域名系统 (DNS) 区域配置为动态区域，那么当服务器在运行时，不能对区域数据进行手动更改。这样做可能导致与入局动态更新产生冲突。如果必须进行手动更新，请停止服务器，进行这些更改，然后重新启动服务器。发送至已停止的 DNS 服务器的动态更新将永远不会完成。因此，您可能要分别配置动态区域和静态区域。为此，可以创建完全独立的区域，或者为那些将动态维护的客户机定义新的子域（例如，dynamic.mycompany.com）。

IBM i DNS 提供了用于配置系统的图形界面。在某些情况下，该界面使用的术语或概念在其他源中可能有不同的表示。如果您在规划 DNS 配置时参阅其他信息源，那么记住下列各项可能很有用:

- 在 IBM i 平台上定义的所有区域和对象都在“正向查找区域”和“逆向查找区域”文件夹中进行组织。正向查找区域是用来将域名映射到 IP 地址的区域（例如，A 和 AAA 记录）。逆向查找区域是用来将 IP 地址映射到域名的区域（例如，PTR 记录）。
- IBM i DNS 引用*主区域*和*辅助区域*。
- 该界面使用*副区域*，某些源称其为*子域*。子区域是您已委托一个或多个名称服务器负责的副区域。

规划安全措施

域名系统 (DNS) 提供了安全性选项，以限制外部对服务器的访问。

地址匹配列表

DNS 使用地址匹配列表来允许或拒绝外部实体对某些 DNS 功能的访问。这些列表可以包括特定 IP 地址、子网（使用 IP 前缀）或使用事务签名 (TSIG) 密钥。您可以在地址匹配列表中定义要允许或拒绝其访问的实体的列表。如果您希望能够复用地址匹配列表，那么可以将该列表另存为访问控制表 (ACL)。于是，无论您何时需要提供该列表，都可以调用此 ACL，将装入整个列表。

地址匹配列表项顺序

将使用地址匹配列表中与给定地址匹配的第一项。例如，要允许 10.1.1.x 网络上除 10.1.1.5 之外的所有地址，匹配列表项的顺序必须是 (!10.1.1.5; 10.1.1/24)。在这种情况下，地址 10.1.1.5 将与第一项进行比较，并且将立即拒绝该地址。

如果反转了这些元素 (10.1.1/24; !10.1.1.5)，那么将允许 IP 地址 10.1.1.5 访问，因为服务器会将该 IP 地址与第一项进行比较，而该 IP 地址匹配，从而允许该 IP 地址访问，而不会检查其余的规则。

访问控制选项

DNS 允许您设置限制（例如，谁可以将动态更新发送至服务器、查询数据和请求区域传输）。您可以对下列选项使用 ACL 来限制对服务器的访问:

allow-update
为了使 DNS 服务器接受来自任何外部源的动态更新，您必须启用 allow-update 选项。

allow-query
指定允许哪些主机查询此服务器。如果未指定，那么缺省值是允许来自所有主机的查询。

allow-transfer
指定允许哪些主机接收来自服务器的区域传输。如果未指定，那么缺省值是允许来自所有主机的传输。

allow-recursion
指定允许哪些主机通过此服务器作递归查询。如果未指定，那么缺省值是允许来自所有主机的递归查询。

blackhole

指定一个地址列表，服务器不会接受来自这些地址的查询，也不会使用这些地址来解析查询。来自这些地址的查询将不会得到响应。

保护 DNS 服务器是必不可少的工作。除了本主题中的安全性注意事项之外，各种源（其中包括 IBM i 平台和因特网主题集合）中还涵盖了 DNS 安全性和 IBM i 安全性。*DNS and BIND* 一书也涵盖了与 DNS 相关的安全性。

相关概念:

System i 和因特网安全性

相关参考:

第 6 页的『BIND 9 功能』

BIND 9 类似于 BIND 8；但是，它提供了用来提高域名系统 (DNS) 服务器的性能的若干功能（例如，视图）。

域名系统需求

考虑在 IBM i 平台上运行域名系统 (DNS) 的这些软件需求。

DNS 功能（选项 31）无法自动随操作系统一起安装。您必须特别选择 DNS 进行安装。为 IBM i 添加的 DNS 服务器基于称为 BIND 9 的业界标准 DNS 实现。

安装 DNS 后，您需要将 DNS 服务器从 BIND 4 或 8 迁移至 BIND 9 并进行配置。您还必须安装 IBM Navigator for i PASE（i5/OS 的选项 33）和 OpenSSH, OpenSSL, zlib（5733-SC1，选项 1）。在安装这两个软件程序后，IBM Navigator for i 会自动配置当前 BIND 实现。

如果要将其他平台上的动态主机配置协议 (DHCP) 服务器配置为将更新发送至此 DNS 服务器，那么还必须在该 DHCP 服务器上安装选项 31。DHCP 服务器使用选项 31 提供的编程接口来执行动态更新。

相关概念:

i5/OS PASE

第 26 页的『配置域名系统』

可以使用 IBM Navigator for i 来配置名称服务器和解析域外部的查询。

相关参考:

第 6 页的『BIND 9 功能』

BIND 9 类似于 BIND 8；但是，它提供了用来提高域名系统 (DNS) 服务器的性能的若干功能（例如，视图）。

确定是否安装了域名系统

要确定是否安装了域名系统 (DNS)，请执行下列步骤:

1. 在命令行上输入 `GO LICPGM`，然后按 Enter 键。
2. 输入 `10`（显示已安装的许可程序），然后按 Enter 键。
3. 向下翻页至 **5770SS1 域名系统**（选项 31）。如果已成功安装 DNS，那么“安装状态”为 `*COMPATIBLE`，如下所示:

```
LicPgm     Installed Status     Description
5770SS1    *COMPATIBLE          Domain Name System
```

4. 按 F3 以退出该屏幕。

安装域名系统

要安装域名系统 (DNS)，请执行下列步骤:

1. 在命令行上输入 GO LICPGM，然后按 Enter 键。
2. 输入 11（安装许可程序），然后按 Enter 键。
3. 在域名系统旁边的**选项**字段中输入 1（安装），然后按 Enter 键。
4. 再次按 Enter 键以确认安装。

注: 域名系统 (DNS) 还需要下列产品选项，如果未安装这些选项，那么必须在系统上安装这些选项。

- 可移植应用程序解决方案环境 (PASE)（5770-SS1，选项 33）
- OpenSSH，OpenSSL，zlib（5733-SC1，选项 1）

配置域名系统

可以使用 IBM Navigator for i 来配置名称服务器和解析域外部的查询。

在进行域名系统 (DNS) 配置之前，请参阅『DNS 系统需求』以安装必需的 DNS 组件。

相关概念:

第 25 页的『域名系统需求』
考虑在 IBM i 平台上运行域名系统 (DNS) 的这些软件需求。

在 IBM Navigator for i 中访问域名系统

以下指示信息指导您了解 IBM Navigator for i 中的 DNS 配置界面。

如果您正在使用 IBM i PASE，那么您能够配置基于 BIND 9 的 DNS 服务器。

如果您是第一次配置 DNS，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 单击“操作”下拉列表并选择**新建名称服务器**菜单项。

相关概念:

了解 System i 导航器

配置名称服务器

域名系统 (DNS) 允许您创建多个名称服务器实例。本主题提供有关配置名称服务器的指示信息。

基于 BIND 9 的 IBM i DNS 支持多个名称服务器实例。下列任务指导您完成创建单个名称服务器实例（包括其属性和区域）的过程。

如果您要创建多个实例，请重复这些过程，直到已创建您需要的所有实例为止。可以为每个名称服务器实例指定独立的属性（例如，调试级别和自动启动值）。当您创建新实例时，将创建单独的配置文件。

相关参考:

第 38 页的『维护域名系统配置文件』
可以在 IBM i 平台上使用 IBM i DNS 来创建和管理 DNS 服务器实例。DNS 的配置文件由 IBM Navigator for i 管理。不得手动编辑这些文件。请始终使用 IBM Navigator for i 来创建、更改或删除 DNS 配置文件。

创建名称服务器实例

“新建 DNS 名称服务器配置”向导可以指导您完成定义 DNS 服务器实例的过程。

要启动**新建 DNS 配置**向导，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在左边的导航树中，选择**创建 DNS 服务器**。
3. 遵循向导的指示信息来完成配置过程。

向导需要以下输入:

DNS 服务器名称:

指定 DNS 服务器的名称。它的最大长度为 5 个字符并且必须以字母字符 (A-Z) 开头。如果创建多个服务器，那么每个服务器必须具有唯一名称。此名称在系统的其他区域中称为 DNS 服务器实例名称。

Listen-on IP 地址:

两个 DNS 服务器不能侦听同一 IP 地址。缺省设置是侦听所有 IP 地址。如果要创建其他服务器实例，那么不能将它们配置为侦听所有 IP 地址。否则，它们无法同时运行。必须为每个服务器指定这些 IP 地址。

根服务器:

您可以装入缺省因特网根服务器列表，也可以指定您自己的根服务器（例如，内部网的内部根服务器）。

注: 仅当您具有因特网访问权并期望您的 DNS 能够完全解析因特网名称时，才应考虑装入缺省因特网根服务器。

服务器启动:

您可以指定服务器是否应在 TCP/IP 启动时自动启动。当您运行多个服务器时，可以相互独立地启动和结束各个实例。

编辑域名系统服务器属性

创建名称服务器后，可以编辑属性（例如，allow-update 和调试级别）。这些选项仅应用于您更改的服务器实例。

要编辑域名系统 (DNS) 服务器实例的属性，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击***您的 DNS 服务器***并选择**配置**。
3. 在“DNS 配置”页面中，选择 **DNS 服务器**并选择**文件 > 属性**。
4. 编辑您要编辑的相应属性。

配置名称服务器上的区域

配置域名系统 (DNS) 服务器实例后，需要配置名称服务器的区域。

要配置服务器上的区域，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击***您的 DNS 服务器***并选择**配置**。
3. 在“DNS 配置”页面中，通过单击**正向查找区域**或**逆向查找区域**文件夹，选择要创建的区域类型。
4. 选择**文件 > 新建 > 主区域/辅助区域/存根区域/转发区域**。
5. 遵循向导的指示信息来完成创建过程。

相关概念:

第 31 页的『访问外部域名系统数据』
当您创建域名系统 (DNS) 区域数据时，服务器能够解析对该区域的查询。

相关任务:

『配置域名系统以接收动态更新』
可以配置运行 BIND 9 的域名系统 (DNS) 服务器，域名注册机接受来自其他源的请求以动态更新区域数据。本主题提供有关配置 allow-update 选项以便 DNS 可以接收动态更新的指示信息。

第 31 页的『导入域名系统文件』
域名系统 (DNS) 可以导入现有区域数据文件。执行以下省时过程，以根据现有配置文件创建新区域。

相关参考:

第 3 页的『了解区域』
域名系统 (DNS) 数据将划分为可管理的数据集（称为*区域*）。并且其中的每个数据集都有特定的区域类型。

配置名称服务器上的视图

BIND 9 提供的其中一个功能是 *view* 语句，该语句允许单个域名系统 (DNS) 实例根据查询的来源（例如，因特网或内部网）以不同方式应答查询。视图的一个特定应用是分割 DNS 设置，而不必运行多个 DNS 服务器。

要配置服务器上的视图，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击***您的 DNS 服务器***并选择**配置**。
3. 在“DNS 配置”页面中，单击**视图**并选择**文件 > 新建 > 查看**。
4. 遵循向导的指示信息来完成创建过程。

配置域名系统以接收动态更新

可以配置运行 BIND 9 的域名系统 (DNS) 服务器，域名注册机接受来自其他源的请求以动态更新区域数据。本主题提供有关配置 allow-update 选项以便 DNS 可以接收动态更新的指示信息。

创建动态区域时，应考虑网络结构。如果域的某些部分仍然需要手动更新，那么您可能要考虑设置单独的静态和动态区域。如果需要对动态区域进行手动更新，那么必须停止动态区域服务器，并在完成更新后将其重新启动。停止服务器会强制它使用自首次从区域数据库中装入其区域数据以来已进行的所有动态更新来更新区域数据库。如果您不停止服务器，那么您将失去对区域数据库的所有手动更新，因为正在运行的服务器将覆盖这些更新。但是，停止服务器以进行手动更新意味着您可能会失去服务器关闭期间发送的动态更新。

在 allow-update 语句中定义了对象时，DNS 指示区域是动态区域。要配置 allow-update 选项，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击***您的 DNS 服务器***并选择**配置**。
3. 在“DNS 配置”页面中，展开**正向查找区域**或**逆向查找区域**。
4. 单击要编辑的主区域并选择**文件 > 属性**。
5. 在“主区域属性”页面中，单击**选项**选项卡。
6. 在“选项”页面上，展开**访问控制 > allow-update**。
7. DNS 会使用地址匹配列表来验证经授权的更新。要将对象添加到地址匹配列表，请选择地址匹配列表项类型并单击**添加**。可以添加 IP 地址、IP 前缀、访问控制表或密钥。
8. 当完成地址匹配列表的更新时，单击**确定**以关闭“选项”页面。

相关任务:

第 27 页的『配置名称服务器上的区域』
配置域名系统 (DNS) 服务器实例后，需要配置名称服务器的区域。

配置 DHCP 以将动态更新发送至 DNS

第 34 页的『对动态区域进行手动更新』
如果 DNS 服务器实例正在运行，那么在 IBM Navigator for i 中对动态区域进行手动更新（例如，添加资源记录）时应加以特别考虑，因为手动更改与动态更新之间可能产生冲突。

配置 DNSSEC

域名系统 (DNS) 允许您为域服务器配置 DNSSEC。本主题提供有关配置 DNSSEC 的指示信息。

基于 BIND 9 的 IBM i DNS 支持 DNSSEC。下列任务指导您完成为域服务器配置 DNSSEC 的过程。

配置可信密钥/受管密钥

以下指示信息可以指导您完成配置可信密钥/受管密钥的过程。

要配置可信密钥/受管密钥，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 右键单击您的 DNS 服务器并选择**配置**
3. 在树中单击 DNS 服务器节点并选择**文件 > 属性**。
4. 单击**可信密钥/受管密钥**选项卡，添加/编辑/删除/查看这些密钥。
5. 单击“确定”

配置 DNSSEC 选项

以下指示信息可以指导您完成配置 DNSSEC 选项的过程。

要启用 DNSSEC 选项，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 右键单击您的 DNS 服务器并选择**配置**
3. 在树中单击 DNS 服务器节点并选择**文件 > 属性**。
4. 单击“选项”选项卡，展开**选项 > 布尔选项**。
5. 单击**启用 DNSSEC** 选项，然后选中“启用”复选框以启用该选项。
6. 单击**验证 DNSSEC** 选项，然后选中“启用”复选框以启用该选项。
7. 单击“确定”

签署主区域

以下指示信息可以指导您完成在 DNS 服务器上签署区域的过程。

要签署区域，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 右键单击您的 DNS 服务器并选择**配置**
3. 展开“DNS 服务器 > 正向查找区域/逆向查找区域”，选择要签署的主区域。
4. 选择**文件 > DNSSEC > 签署**。
5. 遵循向导的指示信息来完成签署过程。

注: 应使用 ZSK 和 KSK 密钥来签署区域。使用“NEW”选项创建用于签署的 ZSK 和 KSK 密钥。

重新签署主区域

以下指示信息可以指导您完成在 DNS 服务器上重新签署区域的过程。

要重新签署区域，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 右键单击您的 DNS 服务器并选择**配置**
3. 展开“DNS 服务器 > 正向查找区域/逆向查找区域”，选择要重新签署的主区域。
4. 选择**文件 > DNSSEC > 重新签署**。
5. 遵循向导的指示信息来完成重新签署过程。

注: 可以使用新的 ZSK 或 KSK 密钥重新签署区域。使用“NEW”选项创建用于重新签署的密钥。

相关任务:

第 35 页的『重新签署区域』

对于已签署的主区域，如果对该区域的资源记录进行了新的更改，那么该区域需要重新签署。

取消签署主区域

以下指示信息可以指导您完成在 DNS 服务器上取消签署区域的过程。

要取消签署区域，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 右键单击您的 DNS 服务器并选择**配置**
3. 展开“DNS 服务器 > 正向查找区域/逆向查找区域”，选择要取消签署的主区域。
4. 选择**文件 > DNSSEC > 取消签署**。
5. 遵循向导的指示信息来完成取消签署过程。

为动态区域配置 DNSSEC

本主题提供有关为动态区域配置 DNSSEC 的指示信息。

对于安全（已签署）区域，您还可以配置 allow-update 或 update-policy 选项，以使该区域成为动态区域。注意，allow-update 和 update-policy 选项具有类似功能，所以配置其中一个选项就足够了。还可以配置 auto-dnssec 选项，以使该区域执行自动区域签署。

配置 allow-update 选项:

可以配置运行 BIND 9 的域名系统 (DNS) 服务器，域名注册机接受来自其他源的请求以动态更新区域数据。本主题提供有关配置 allow-update 选项以便 DNS 可以接收动态更新的指示信息。

请参阅第 28 页的『配置域名系统以接收动态更新』这一节。

配置 update-policy 选项:

以下指示信息可以指导您完成配置 update-policy 选项的过程。

要配置 update-policy 选项，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 右键单击您的 DNS 服务器并选择**配置**。
3. 展开“DNS 服务器 > 正向查找区域/逆向查找区域”，选择要配置的主区域。

4. 选择**文件 > 属性**。
5. 单击“选项”选项卡，展开**选项 > 布尔选项**。
6. 单击 update-policy 选项，指定使用本地更新策略规则，或者单击“添加”以添加规则。
7. 单击“确定”。

配置 auto-dnssec 选项:

以下指示信息可以指导您完成配置 auto-dnssec 选项的过程。

要配置 auto-dnssec 选项，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 右键单击您的 DNS 服务器并选择**配置**
3. 展开“DNS 服务器 > 正向查找区域/逆向查找区域”，选择要配置的主区域。
4. 选择**文件 > 属性**。
5. 单击“选项”选项卡，展开**选项 > 其他**。
6. 单击 auto-dnssec 选项，选择“允许/维护/关闭”
7. 单击“确定”。

导入域名系统文件

域名系统 (DNS) 可以导入现有区域数据文件。执行以下省时过程，以根据现有配置文件创建新区域。

可以通过导入区域数据文件来创建主区域，该文件应是基于 BIND 语法的有效区域配置文件。该文件应位于集成文件系统目录中。导入该文件后，DNS 会验证它是否为有效区域数据文件并将其添加到指定的服务器实例的 named.conf 文件。

要导入区域文件，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击您的 DNS 服务器并选择**配置**。
3. 在“DNS 配置”页面中，选择**文件 > 导入区域**。
4. 遵循向导的指示信息来导入主区域。

相关任务:

第 27 页的『配置名称服务器上的区域』
配置域名系统 (DNS) 服务器实例后，需要配置名称服务器的区域。

记录验证

“导入域数据”功能将读取正在导入的文件的每条记录并进行验证。

在“导入域数据”功能完成后，可以在已导入的区域的“其他记录”属性页面上分别检查任何出错的记录。

注意:

1. 导入较大的主域可能需要若干分钟。
2. “导入域数据”功能不支持 $include 伪指令。“导入域数据”的有效性检验过程将包含 $include 伪指令的行识别为出错的行。

访问外部域名系统数据

当您创建域名系统 (DNS) 区域数据时，服务器能够解析对该区域的查询。

根服务器对于直接连接至因特网或大型内部网的 DNS 服务器的功能很关键。DNS 服务器必须使用根服务器，才能应答有关未包含在其自己的域文件中的主机的查询。

为了到处搜索以获取更多信息，DNS 服务器必须知道要查看的位置。在因特网上，DNS 服务器查看的第一个位置是根服务器。根服务器将 DNS 服务器定向至层次结构中的其他服务器，直到找到答案或者确定没有答案为止。

IBM Navigator for i 的缺省根服务器列表

仅当您具有因特网连接并且要在因特网上解析您的 DNS 服务器上未解析的名称时，才应使用因特网根服务器。在 IBM Navigator for i 中提供了缺省因特网根服务器列表。该列表是发布 IBM Navigator for i 时的当前列表。您可以通过将它与 InterNIC 站点上的列表进行比较，验证缺省列表是否为最新列表。更新您的配置的根服务器列表，以使它保持为当前列表。

获取因特网根服务器地址

顶级根服务器的地址有时会更改，保持这些地址为当前地址是 DNS 管理员的责任。InterNIC 维护了因特网根服务器地址的当前列表。要获取因特网根服务器的当前列表，请执行下列步骤:

1. 使用文件传输协议 (FTP) 以匿名方式登录 InterNIC 服务器: `FTP.INTERNIC.NET` 或 `RS.INTERNIC.NET`
2. 下载以下文件: `/domain/named.root`
3. 将该文件存储在以下目录路径中: `/QOpenSys/QIBM/ProdData/OS400/DNS/ROOT.FILE`

防火墙后面的 DNS 服务器可能没有定义根服务器。在这种情况下，DNS 服务器只能根据其自己的主域数据库文件或其高速缓存中存在的条目来解析查询。它可能会将非现场查询转发至防火墙 DNS。在这种情况下，防火墙 DNS 服务器充当转发器。

内部网根服务器

如果 DNS 服务器是大型内部网的一部分，那么您可以具有内部根服务器。如果 DNS 服务器将不访问因特网，那么不需要装入缺省因特网服务器。但是，应添加内部根服务器，以便 DNS 服务器可以解析其域外部的内部地址。

相关任务:

第 27 页的『配置名称服务器上的区域』
配置域名系统 (DNS) 服务器实例后，需要配置名称服务器的区域。

管理域名系统

管理域名系统 (DNS) 服务器的过程包括验证 DNS 功能是否起作用、是否维护 DNSSEC、是否监视性能以及是否维护 DNS 数据和文件。

相关概念:

第 12 页的『DNS 安全性扩展 (DNSSEC) 简介』
DNSSEC 是一套将安全性扩展添加到 DNS 的 IETF RFC 规范。

验证域名系统功能是否起作用

域信息探索器 (DIG) 工具可以帮助您从域名系统 (DNS) 服务器收集信息以及测试该服务器的响应。可以使用 DIG 来验证 DNS 服务器是否正常工作。

请求与回送 IP 地址 (127.0.0.1) 关联的主机名。应使用主机名 (localhost) 来响应。还可以查询您正在尝试验证的服务器实例中定义的特定名称。这将确认您正在测试的特定服务器实例是否在正常运行。

要使用 DIG 验证 DNS 功能，请执行下列步骤:

1. 在命令行上输入 DIG HOSTNAME('127.0.0.1') REVERSE(*YES)。

   应显示以下信息（其中包括回送主机名）:

```
;; global options: printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id:865
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL:1

;; QUESTION SECTION:
;1.0.0.127.in-addr.arpa.          IN   PTR

;; ANSWER SECTION:
1.0.0.127.in-addr.arpa.  86400   IN    PTR  localhost.

;; AUTHORITY SECTION:
0.0.127.in-addr.arpa.   86400   IN    NS   ISA2LP05.RCHLAND.IBM.COM.

;; ADDITIONAL SECTION:
ISA2LP05.RCHLAND.IBM.COM. 38694   IN    A   9.5.176.194

;; Query time: 552 msec
;; SERVER: 9.5.176.194#53(9.5.176.194)
;; WHEN: Thu May 31 21:38:12 2007
;; MSG SIZE rcvd: 117
```

   如果 DNS 服务器返回回送主机名 **localhost**，那么它响应正确。

2. 按 Enter 键以退出该会话。

注: 如果使用 DIG 时需要帮助，请输入 ?DIG 并按 Enter 键。

管理安全密钥

安全密钥允许您限制对域名系统 (DNS) 数据的访问。

有两种类型的与 DNS 相关的密钥，它们是 DNS 密钥和动态更新密钥。它们在保护 DNS 配置方面各有不同的作用。下列描述说明了它们各自与 DNS 服务器的关系。

管理域名系统密钥

域名系统 (DNS) 密钥是为 BIND 定义的密钥，由 DNS 服务器在验证人局更新时使用。

您可以配置密钥并对其指定名称。然后，当您要保护 DNS 对象（例如，动态区域）时，可以在地址匹配列表中指定该密钥。

要管理 DNS 密钥，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击要管理的 DNS 服务器实例并选择**配置**。
3. 在“DNS 配置”页面中，选择**文件 > 管理密钥**。

在“管理密钥”页面中，您可以执行相应的管理任务。

管理动态更新密钥

动态更新密钥由动态主机配置协议 (DHCP) 服务器用于保护动态更新。

当域名系统 (DNS) 与 DHCP 位于同一 IBM i 平台上时，这些密钥必须存在。如果 DHCP 位于其他 IBM i 平台上，那么您必须将相同的动态更新密钥文件分发至每个远程 IBM i 平台，远程平台需要这些文件才能将动态更新发送至权威服务器。可以通过 FTP 和电子邮件等来分发这些文件。

要管理动态更新密钥，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 选择**管理 DNS 动态更新密钥**。

然后，您可以在“管理动态更新密钥”页面中执行相应的管理任务。

对动态区域进行手动更新

如果 DNS 服务器实例正在运行，那么在 IBM Navigator for i 中对动态区域进行手动更新（例如，添加资源记录）时应加以特别考虑，因为手动更改与动态更新之间可能产生冲突。

如果需要添加、编辑或删除动态区域的资源记录，建议在字符界面中使用 RUNDNSUPD 或 NSUPDATE 命令向 DNS 服务器提交动态更新请求。例如，下列命令为 myhost.mycompany.com 添加一条具有 IP 地址 192.168.1.100 的 A 记录。

```
RUNDNSUPD BCHFILE(*NONE)
> update add myhost.mycompany.com 86400 A 192.168.1.100
> send
> quit
```

注: 以“>”开头的行是运行 RUNDNSUPD 后发出的交互式命令。

如果必须在 IBM Navigator for i 中进行手动更改，那么在进行更改之前，可以在字符界面中使用 RNDC 命令以使区域文件同步。注意，您可能会失去手动更改期间发送的动态更新。

要进行手动更改，请执行下列步骤（假定 DNS 服务器正在运行）:

1. 关闭 IBM Navigator for i 中所有已打开的 DNS 配置页面。
2. 在字符界面中，在命令行上输入命令 RNDC RNDCCMD(freeze zonename)，其中 zonename 是动态区域的名称。此命令将导致该区域冻结并且使动态更新（存储在日志文件中）在区域文件中同步。对于冻结的区域，将不接受任何动态更新。注意，在运行此命令后，将除去该区域的日志文件。
3. 在 IBM Navigator for i 中停止服务器实例；或者在字符界面中，在命令行上输入命令 RNDC RNDCCMD (stop)。
4. 在 IBM Navigator for i 中对区域进行手动更改，例如，添加资源记录。
5. 在 IBM Navigator for i 中重新启动服务器实例；或者在命令行上输入 STRTCPSVR SERVER(*DNS) DNSSVR (instancename) 以重新启动服务器，其中 instancename 是服务器实例的名称。
6. 在字符界面中，在命令行上输入命令 RNDC RNDCCMD(thaw zonename)，其中 zonename 是动态区域的名称。此命令将导致重新装入该区域并再次接受对该区域的动态更新。

相关任务:

第 28 页的『配置域名系统以接收动态更新』
可以配置运行 BIND 9 的域名系统 (DNS) 服务器，域名注册机接受来自其他源的请求以动态更新区域数据。本主题提供有关配置 allow-update 选项以便 DNS 可以接收动态更新的指示信息。

管理 DNSSEC

本主题介绍 IBM i 平台上的 DNSSEC 维护。

相关概念:

第 12 页的『DNS 安全性扩展 (DNSSEC) 简介』

DNSSEC 是一套将安全性扩展添加到 DNS 的 IETF RFC 规范。

验证 DNSSEC 功能是否起作用

可以使用 DIG（域信息探索器）工具来验证 DNSSEC 功能是否正常起作用。

假定 DNS 服务器上有一个名为 example.com 的已签署区域，并且在该区域中有 host1.example.com 的一条 A 记录 192.168.1.101。

要使用 DIG 验证 DNSSEC 功能，请执行下列步骤:

1. 在命令行上输入 DIG HOSTNAME(host1.example.com) DMNNAMSVR('127.0.0.1') DNSSEC(*YES)。

   如果状态码是 NOERROR 并且在 ANSWER 部分中有 A 和 RRSIG 记录（如下所示），那么 DNS 服务器响应正确:

   ```
   ;; global options:   +cmd
   ;; Got answer:
   ;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64408
   ;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 2, ADDI-TIONAL: 1

   ;; OPT PSEUDOSECTION:
   ; EDNS: version: 0, flags: do; udp: 4096
   ;; QUESTION SECTION:
   ;host1.example.com.             IN      A

   ;; ANSWER SECTION:
   host1.example.com.      172800  IN      A       192.168.1.101
   host1.example.com.      172800  IN      RRSIG   A 5 3 172800 20131116055306 20131017055306 11643
   example.com. i4xLG5ZIc+ifzvdUe91jjPlys2tjM3f1KFSa6H/iDnQfcUNWAS6aEDPY Tpr5ir6xs72mqJYepK5uaWarxDZAZ
   a86yf7QjRI+9ab7t36O+Og9DRGT qS3G/8JfyZIFeck1QSYT6Hm3JCdaWMWPEfT+l/sYfS3H1YDdN9RxrXMN 5I0=

   ;; AUTHORITY SECTION:
   example.com.            172800  IN      NS      ...
   example.com.            172800  IN      RRSIG   NS ...
     ...
   ```

2. 按 Enter 键以退出该会话。

重新签署区域

对于已签署的主区域，如果对该区域的资源记录进行了新的更改，那么该区域需要重新签署。

请考虑下列情况:

- 已将新的资源记录（A 和 MX 资源记录等）添加到已签署的区域，或者现有记录已更改
- ZSK/KSK 密钥已更改或者将到期
- 接收到对动态区域的动态更新请求

对于静态区域，如果 ZKS/KSK 密钥或其他资源记录已更改，那么您需要对该区域执行手动区域重新签署。对于动态区域，在接收到动态更新后，区域重新签署将由服务器实例自动执行，所以不需要手动重新签署。

相关概念:

第 5 页的『动态更新』
基于 BIND 9 的 IBM i 域名系统 (DNS) 支持动态更新。外部源（例如，动态主机配置协议 (DHCP)）可以将更新发送至 DNS 服务器。另外，您还可以使用 DNS 客户机工具（例如，动态更新实用程序 (NSUPDATE)）来执行动态更新。

相关任务:

第 30 页的『重新签署主区域』
以下指示信息可以指导您完成在 DNS 服务器上重新签署区域的过程。

密钥滚动注意事项

为了安全起见，应定期滚动 KSK/ZSK 密钥。

建议每 12 个月替换 KSK 密钥一次，并且每个月或每个季度替换 ZSK 密钥一次。

管理动态区域的 DNSSEC

本主题介绍动态区域的 DNSSEC 维护。

DNSSEC 和动态更新

如果某个动态区域部署了 DNSSEC，那么 DNS 服务器将定期重新签署该区域，以确保还将签署由于动态更新而取消签署的记录。

注: DNS 服务器需要知道 ZSK/KSK 专用密钥的位置才能签署区域，所以您需要为使用 DNSSEC 的动态区域配置 `key-directory` 选项。

使用 NSUPDATE 命令维护 DNSSEC

可以使用 `NSUPDATE` 命令对动态区域执行与 DNSSEC 相关的操作。例如，可以使用该命令将 ZSK/KSK 密钥添加到动态区域，以签署该区域或执行密钥滚动。

下面显示了通过将 ZSK/KSK 密钥添加到动态区域来签署该区域的步骤:

1. 准备要执行的批处理文件 (batch.file)。批处理文件的内容可能类似于以下内容。注意，该文件的末尾有一个空白行。

   ```
   ttl 3600
   update add domainname DNSKEY 256 3 7 AwEAA...
   update add domainname DNSKEY 257 3 7 AwEAA...
   send
   ```

2. 在字符界面中，在命令行上输入命令 `NSUPDATE BCHFILE(batch.file)`，然后按 Enter 键。

动态区域的自动区域签署/自动密钥滚动

通过将 `auto-dnssec` 选项配置为“维护”，可以使动态区域自动签署，并且 ZSK/KSK 密钥自动滚动。您只需要提供用于区域维护的对应 ZSK/KSK 密钥。执行以下步骤以准备这些密钥:

1. 准备用来签署该区域的正确 ZSK/KSK 密钥。可以在字符界面中使用命令 `GENDNSKEY` 生成这些密钥。
2. 授予用户 QTCP 对 ZSK/KSK 密钥和区域文件的访问权。

在字符界面中，对于每个公用密钥，输入命令 CHGAUT OBJ('/QIBM/UserData/OS400/DNS/_DYN/K<*key-id-n*>.+aaa+nnnnn.key') USER(QTCP) DTAAUT(*RWX) OBJAUT(*ALL)；对于每个专用密钥，输入命令 CHGAUT OBJ('/QIBM/UserData/OS400/DNS/_DYN/K<*key-id-n*>.+aaa+nnnnn.private') USER(QTCP) DTAAUT(*RWX) OBJAUT(*ALL)；对于正在使用的区域文件，输入命令 CHGAUT OBJ('/QIBM/UserData/OS400/DNS/<*instance*>/zonefile') USER(QTCP) DTAAUT(*RWX) OBJAUT(*ALL)

注：您可以参阅第 30 页的『为动态区域配置 DNSSEC』这一节，以了解 auto-dnssec 选项的配置步骤。

访问域名系统服务器统计信息

数据库转储和统计信息工具可以帮助您复查和管理服务器性能。

域名系统 (DNS) 提供了若干诊断工具。它们可以用来监视服务器的性能。

相关参考:

第 38 页的『维护域名系统配置文件』

可以在 IBM i 平台上使用 IBM i DNS 来创建和管理 DNS 服务器实例。DNS 的配置文件由 IBM Navigator for i 管理。不得手动编辑这些文件。请始终使用 IBM Navigator for i 来创建、更改或删除 DNS 配置文件。

访问服务器统计信息

服务器统计信息总结了服务器自其最近一次重新启动或重新装入其数据库以来，接收到的查询和响应的数目。

域名系统 (DNS) 允许您查看服务器实例的统计信息。信息连续附加到此文件，直到删除该文件为止。在评估服务器接收到的流量的多少以及追查问题时，此信息可能很有用。可以在 DNS 联机帮助主题“了解 DNS 服务器统计信息”中获得有关服务器统计信息的更多信息。

要访问服务器统计信息，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击***您的 DNS 服务器***并选择**配置**。
3. 在“DNS 配置”页面中，选择**查看 > 服务器统计信息**。

您还可以使用“远程名称守护程序控制”(**RNDC**) 命令来显示 named.stats 文件中的服务器统计信息。对应的命令如下:

```
RNDC RNDCCMD('stats')
```

访问活动服务器数据库

活动服务器数据库包含区域信息和主机信息，其中包括某些区域属性（例如，起始权限 (SOA) 信息）和通过主机属性（例如，邮件交换程序 (MX) 信息，此信息在跟踪问题时很有用）。

域名系统 (DNS) 允许您查看服务器实例的权威数据、高速缓存数据和提示数据的转储。该转储包括来自服务器的所有主区域和辅助区域（正向和逆向映射区域）的信息以及服务器已通过查询获取的信息。

您可以使用 IBM Navigator for i 来查看活动服务器数据库转储。如果您需要保存这些文件的副本，那么数据库转储文件名是 IBM i 目录路径 /QIBM/UserData/OS400/DNS/<server instance>/ 中的 named_dump.db，其中 <*server instance*> 是 DNS 服务器实例的名称。可以在 DNS 联机帮助主题“了解 DNS 服务器数据库转储”中获得有关活动服务器数据库的更多信息。

要访问活动服务器数据库转储，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。

2. 在右窗格中，右键单击***您的 DNS 服务器***并选择**配置**。
3. 在“DNS 配置”页面中，选择**查看 > 活动服务器数据库**。

您还可以使用“远程名称守护程序控制”(**RNDC**) 命令来显示 named_dump.db 文件中的活动服务器数据库信息。对应的命令如下:

```
RNDC RNDCCMD('dumpdb -all')
```

维护域名系统配置文件

可以在 IBM i 平台上使用 IBM i DNS 来创建和管理 DNS 服务器实例。DNS 的配置文件由 IBM Navigator for i 管理。不得手动编辑这些文件。请始终使用 IBM Navigator for i 来创建、更改或删除 DNS 配置文件。

DNS 配置文件存储在下面列示的集成文件系统路径中。

注: 以下文件结构适用于在 BIND 9 上运行的 DNS。

在下表中，按所显示路径的层次结构列示文件。应备份带有保存图标  的文件以保护数据。应定期删除带有删除图标  的文件。

名称	图标	描述
/QIBM/UserData/OS400/DNS/		DNS 的起始目录。
/QIBM/UserData/OS400/DNS/ ***<instance-n>/***		DNS 实例的起始目录。
ATTRIBUTES		DNS 使用此文件来确定您正在使用的 BIND 版本。
BOOT.AS400BIND4		已转换为此实例的 BIND 8 named.conf 文件的 BIND 4.9.3 服务器配置和策略文件。如果您将 BIND 4.9.3 服务器迁移至 BIND 9，那么将创建此文件。它充当迁移备份，当 BIND 9 服务器正常工作时，可以删除此文件。
named.ca		此服务器实例的根服务器的列表。
named.conf		此文件包含配置数据。它告知服务器将管理的特定区域、区域文件所在的位置、可以动态更新的区域、转发服务器所在的位置以及其他选项设置。
named_dump.db		为活动服务器数据库创建的服务器数据转储。
named.memstats		服务器内存统计信息（如果在 named.conf 中配置了此统计信息）。
named.pid		用于保存正在运行的服务器的进程标识。每次启动 DNS 服务器时将创建此文件。它用于“数据库”、“统计信息”和“更新服务器”功能。不要删除或编辑此文件。
named.random		服务器生成的熵文件。

名称	图标	描述
named.recursing		递归的服务器查询（如果 IBM Navigator for i 请求了这种查询）。
named.run		缺省调试日志（如果请求了此日志）。它可以滚动为 named.run.0 和 named.run.1 等等。
named.stats		服务器统计信息。
<*primary-zone-n*>.db		它是此服务器上特定域的主区域文件。该文件包含此区域的所有资源记录。每个区域都有一个单独的 .db 文件。
<*primary-zone-n*>.jnl		用于保存区域的动态更新的日志文件。首次接收到动态更新时，将创建此文件。服务器在关闭或崩溃后重新启动时，会重放该日志文件，以将最近一次区域转储后发生的所有更新合并到区域中。此文件还用于递增区域传输 (IXFR)。这些日志文件不会消失。此文件是二进制文件，不应编辑。
<*primary-zone-n*>.db+<YYYYMMDDHHMMSS>.signed		它是特定域的主区域文件的已签署版本。它还包含用于 DNSSEC 的资源记录（RRSIG 资源记录等）。
db.<*secondary-zone-n*>		此服务器上特定域的辅助区域文件。它包含此区域的所有资源记录。如果无法访问主服务器，那么将使用此文件在启动时初始装入辅助服务器。每个区域都有一个单独的 .db 文件。
/QIBM/UserData/OS400/DNS/_DYN/		用于保存动态更新所需的文件的目录。
<*key_id-n*>._KEY		指向使用 <*key_id-n*> 密钥的 DNSSEC 密钥的符号链接。它始终指向创建的最后一个 K<*key_id-n*>.+*aaa*+*nnnnn*.key 密钥。
<*key_id-x*>._DUK. <*zone-a*>		动态更新密钥，使用 <*key_id-x*> 密钥启动对 <*zone-a*> 的动态更新请求时需要此密钥。
<*key_id-x*>._KID		包含 key 语句的文件，用于名为 <*key_id-x*> 的 key_id
<*key_id-y*>._DUK. <*zone-a*>		动态更新密钥，使用 <*key_id-y*> 密钥启动对 <*zone-a*> 的动态更新请求时需要此密钥。
<*key_id-y*>._DUK. <*zone-b*>		动态更新密钥，使用 <*key_id-y*> 密钥启动对 <*zone-b*> 的动态更新请求时需要此密钥。
<*key_id-y*>._KID		包含 key 语句的文件，用于名为 <*key_id-y*> 的 key_id

k<*key_id-n*>.+aaa+nnnnn.key k<*key_id-n*>.+aaa+nnnnn.private		使用以下 <*key_id-n*> 的 DNSSEC 公用密钥 / 专用密钥对： K{name}.+{algorithm}.+{identifier}.key K{name}.+{algorithm}.+{identifier}.private 如果此 <*key_id-n*> 的密钥对已存在，那么将创建具有其他标识部分的新密钥对。
dsset-*primary-zone-n*.		此文件用来为父区域管理员提供对应的 DS 记录。
keyset-*primary-zone-n*.		此文件用来为父区域管理员提供 DNSKEY。
rndc-confgen.random.*nnnnnn* dnssec-keygen.random.*nnnnn* dnssec-signzone.random.*nnnnn*		需要熵文件的各种命令的熵文件。*nnnnn* 部分是创建该文件的作业的作业号。仅当命令由于某种原因而取消并且未清除时，才会留下这些部分。
<*instance-n*>/session.key		在服务器启动时生成，并用于来自本地主机的动态更新。不要删除或编辑此文件。

相关概念:

第 23 页的『确定域名系统权限』
域名系统 (DNS) 管理员有特殊的权限需求。您还应该考虑权限的安全隐患。

第 37 页的『访问域名系统服务器统计信息』
数据库转储和统计信息工具可以帮助您复查和管理服务器性能。

相关任务:

第 26 页的『配置名称服务器』
域名系统 (DNS) 允许您创建多个名称服务器实例。本主题提供有关配置名称服务器的指示信息。

高级域名系统功能

本主题说明有经验的管理员如何使用域名系统 (DNS) 高级功能更轻松地管理 DNS 服务器。

IBM Navigator for i 中的 DNS 提供了一个具有高级功能的界面，以配置和管理 DNS 服务器。以快捷方式为熟悉 IBM i 图形界面的管理员提供了下列任务。这些任务提供了同时为多个实例更改服务器状态和属性的快速方法。

相关任务:

第 43 页的『更改域名系统调试设置』
域名系统 (DNS) 调试功能可以提供有助于您确定和解决 DNS 服务器问题的信息。

启动或停止域名系统服务器

如果 IBM Navigator for i 界面中的域名系统 (DNS) 不允许您同时启动或停止多个服务器实例，那么可以使用字符界面来同时为多个实例更改这些设置。

要使用字符界面来同时启动所有 DNS 服务器实例，请在命令行上输入 `STRTCPSVR SERVER(*DNS) DNSSVR (*ALL)`。要同时停止所有 DNS 服务器，请在命令行上输入 `ENDTCPSVR SERVER(*DNS) DNSSVR(*ALL)`。

更改调试值

对于具有大区域并且不希望在服务器首次启动并装入所有区域数据时收集大量调试数据的管理员，更改调试级别很有用。

IBM Navigator for i 界面中的域名系统 (DNS) 不允许您在服务器运行时更改调试级别。但是，当服务器在运行时，您可以使用字符界面来更改调试级别。要使用字符界面更改调试级别，请执行下列步骤，将命令中的 *nnnnn* 替换为服务器实例的名称:

1. 在命令行上输入 `ADDLIBLE QDNS`，然后按 Enter 键。
2. 更改调试级别:
   - 要打开调试或者将调试级别增大 1 级，请输入 `RNDC RNDCCMD('trace')`，然后按 Enter 键。
   - 要关闭调试，请输入 `RNDC RNDCCMD('notrace')`，然后按 Enter 键。

域名系统故障诊断

域名系统 (DNS) 日志记录和调试设置可以帮助您解决 DNS 服务器的问题。

DNS 的运行方式与其他 TCP/IP 功能和应用程序非常相似。与 SMTP 或 FTP 应用程序一样，DNS 作业在 QSYSWRK 子系统下运行，并在用户概要文件 QTCP 下生成作业日志，这些作业日志包含与 DNS 作业关联的信息。如果 DNS 作业结束，那么您可以使用作业日志来确定原因。如果 DNS 服务器未返回期望的响应，那么作业日志可能包含有助于问题分析的信息。

DNS 配置由若干文件组成，每个文件中具有不同类型的记录。DNS 服务器的问题通常是由于 DNS 配置文件中具有不正确的条目。出现问题时，请验证 DNS 配置文件是否包含您期望的条目。

标识作业

如果您检查作业日志以验证 DNS 服务器功能（例如，使用 WRKACTJOB），请考虑下列命名准则:

- 如果您正在运行基于 BIND 9 的服务器，那么您运行的每个服务器实例都有一个单独的作业。作业名以五个固定的字符 (QTOBD) 开头，后面跟有实例名称。例如，如果您有两个实例 INST1 和 INST2，那么其作业名将为 QTOBDINST1 和 QTOBDINST2。

记录域名系统服务器消息

域名系统 (DNS) 提供了许多日志记录选项，当您尝试查找问题来源时，可以调整这些选项。日志记录通过提供各种严重性级别、消息类别和输出文件来提供灵活性，以便您可以对日志记录进行微调，以帮助您查找问题。

BIND 9 提供了若干日志记录选项。您可以指定将记录的消息类型、发送每种消息类型的位置以及要记录的每种消息类型的严重性。一般情况下，缺省日志记录设置就合适了，但是，如果您要更改这些设置，那么建议您参阅其他源的 BIND 9 文档，以获取有关日志记录的信息。

日志记录通道

DNS 服务器可以将消息记录到不同输出通道。通道指定发送日志记录数据的位置。您可以选择下列通道类型:

- **文件通道**

  记录到文件通道的消息将发送至文件。缺省文件通道为 i5os_debug 和 i5os_QPRINT。缺省情况下，调试消息将记录到 i5os_debug 通道，该通道是 named.run 文件，但是您还可以指定将其他消息类别发送至此文件。记录到 i5os_QPRINT 的消息类别将发送至用户概要文件 QTCP 的 QPRINT 假脱机文件。除了提供的缺省通道之外，您还可以创建您自己的通道。

- **系统日志通道**

记录到此通道的消息将发送至服务器的作业日志。缺省系统日志通道为 i5os_joblog。路由至此通道的日志记录消息将发送至 DNS 服务器实例的作业日志。

- **空通道**

  将废弃记录到空通道的所有消息。缺省空通道为 i5os_null。如果您不希望某些类别的消息出现在任何日志文件中，那么可以将这些类别路由至空通道。

消息类别

消息按类别进行分组。您可以指定应记录到每个通道的消息类别。类别如下:

客户机 处理客户机请求。

配置 配置文件解析和处理。

数据库 与数据库相关的消息，这些数据库由 DNS 服务器在内部使用以存储区域数据和高速缓存数据。

缺省值 日志记录选项的定义，用于那些尚未定义特定配置的类别。

delegation-only
仅授权。它记录由于以下原因已强制发送至 NXDOMAIN 的查询: 提示或存根区域声明中有 delegation-only 区域或 delegation-only。

分派 将入局包分派至要在其中处理这些包的服务器模块。

dnssec
DNS 安全性扩展 (DNSSEC) 和事务签名 (TSIG) 协议处理。

常规 catch-all 类别，用于那些未分类到任何其他类别的事物。

lame-servers
远程服务器中具有错误配置的低效率服务器，由 BIND 9 在解析期间尝试查询这些服务器时发现。

网络 网络操作。

通知 NOTIFY 协议。

解析器 由高速缓存名称服务器为客户机执行的 DNS 解析（例如，递归查找）。

安全性 批准和拒绝请求。

xfer-in
服务器正在接收的区域传输。

xfer-out
服务器正在发送的区域传输。

不匹配的
无法确定其类或者没有匹配视图的已指定消息。还会将一行摘要记录到客户机类别。最好将此类别发送至文件或标准错误。缺省情况下，此类别将发送至空通道。

更新 动态更新。

update-security
批准和拒绝更新请求。查询指定应记录查询的位置。启动时，除非指定了 querylog 选项，否则指定类别查询将启用查询日志记录。

查询日志条目将报告客户机的 IP 地址和端口号、查询名称、类和类型。它还会报告是否设置了“期望递归”标志（如果已设置则报告 +，如果未设置则报告 -）、EDNS 是否在使用中 (E) 或者是否签署了查询 (S)。

日志文件可以变大，并且可以定期删除。停止和启动 DNS 服务器时，将清除 DNS 日志文件中的所有内容。

消息严重性

通道允许您按消息严重性进行过滤。对于每个通道，您可以指定将记录的消息的严重性级别。有以下严重性级别可用:

- 紧急
- 错误
- 警告
- 注意
- 信息
- 调试（指定调试级别 0 至 11）
- 动态（继承服务器启动调试级别）

将会记录具有您选择的严重性以及在列表中高于它的任何级别的所有消息。例如，如果您选择“警告”，那么通道会记录“警告”、“错误”和“紧急”消息。如果您选择“调试”级别，那么可以指定 0 至 11 之间的值，此值表示您要记录的调试消息的级别。

更改日志记录设置

要访问日志记录选项，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击***您的 DNS 服务器***并选择**配置**。
3. 在“DNS 配置”页面中，右键单击 **DNS 服务器**并选择**属性**。
4. 在“服务器属性”页面上，选择**通道**选项卡，以创建新的文件通道或通道属性（例如，记录到每个通道的消息的严重性）。
5. 在“服务器属性”页面上，选择**日志记录**选项卡，以指定记录到每个通道的消息类别。

有关严重性级别的故障诊断提示

i5os_joblog 通道的缺省严重性级别设置为“错误”。此设置用来减少参考消息和警告消息的数量，否则这些消息会降低性能。如果您遇到问题，但作业日志未指示问题来源，那么可能需要更改严重性级别。执行以上过程，以访问“通道”页面并将 i5os_joblog 通道的严重性级别更改为“警告”、“注意”或“信息”，以便您可以查看更多日志记录数据。解决问题后，请将严重性级别重置为“错误”，以减少作业日志中消息的数目。

更改域名系统调试设置

域名系统 (DNS) 调试功能可以提供有助于您确定和解决 DNS 服务器问题的信息。

DNS 提供了 12 个级别的调试控制。日志记录通常提供较容易的查找问题的方法，但是在某些情况下，可能必须调试。在正常情况下，已关闭调试（值 = 0）。建议首先使用日志记录来尝试解决问题。

有效调试级别为 0 至 11。您的 IBM 服务代表可帮助您确定适当的调试值以诊断 DNS 问题。1 或更大的值会将调试信息写入以下 IBM i 目录路径中的 named.run 文件: `/QIBM/UserData/OS400/DNS/<server instance>`，其中 <*server instance*> 是 DNS 服务器实例的名称。只要调试级别设置为 1 或更高级别，并且 DNS 服务器继续运行，named.run 文件就会继续增大。您还可以使用“服务器属性 - 通道”页面来指定 named.run 文件的最大大小和版本数的首选项。

要更改 DNS 服务器实例的调试值，请执行下列步骤:

1. 在 IBM Navigator for i 中，展开**网络 > 服务器 > DNS 服务器**。
2. 在右窗格中，右键单击***您的 DNS 服务器***并选择**配置**。
3. 在“DNS 配置”页面中，右键单击 DNS 服务器并选择**属性**。
4. 在“服务器属性 - 常规”页面上，指定服务器启动调试级别。
5. 如果服务器正在运行，请停止并重新启动服务器。

注: 当服务器在运行时，对调试级别的更改不会生效。此处设置的调试级别将在服务器下次完全重新启动后得到使用。如果需要在服务器运行时更改调试级别，请参阅『高级 DNS 功能』。

相关概念:

第 40 页的『高级域名系统功能』
本主题说明有经验的管理员如何使用域名系统 (DNS) 高级功能更轻松地管理 DNS 服务器。

域名系统的相关信息

IBM 红皮书出版物、Web 站点和其他信息中心主题集合包含与域名系统 (DNS) 主题集合相关的信息。可查看或打印其中任何 PDF 文件。

IBM 红皮书

AS/400® TCP/IP Autoconfiguration: DNS and DHCP Support (5181 KB)

此 Redbooks 出版物描述了 IBM i 中包括的域名系统 (DNS) 服务器和动态主机配置协议 (DHCP) 服务器支持。它可以通过示例来帮助您对 DNS 和 DHCP 支持进行安装、定制、配置和故障诊断。

Web 站点

- *DNS and BIND*（第五版）。Paul Albitz 和 Cricket Liu。由 O'Reilly and Associates,Inc. 于 2006 年在加州的塞巴斯托波出版。ISBN 书号: 0-59610-057-4。
- Internet System Consortium (ISC) Web 站点中的 The BIND Administrator Reference Manual（PDF 版本）。
- Internet Software Consortium Web 站点 包含 BIND 的新闻、链接和其他资源。它还提供了与 DNS 相关的 RFC 的列表
- InterNIC 站点维护了一个目录，该目录包含由因特网名称与数字地址分配机构 (ICANN) 授权的所有域名注册机构。

相关参考:

第 2 页的『域名系统的 PDF 文件』
可查看和打印此信息的 PDF 文件。

声明

本信息是为在美国国内供应的产品和服务而编写的。

IBM 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您所在区域当前可获得的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务的操作，由用户自行负责。

IBM 可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并不意味着授予用户使用这些专利的任何许可。您可以用书面形式将许可查询寄往:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

有关双字节 (DBCS) 信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

以下段落对于英国和与当地法律有不同规定的其他国家或地区均不适用: INTERNATIONAL BUSINESS MACHINES CORPORATION“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某特定用途的保证。某些国家或地区在某些交易中不允许免除明示或暗含的保证。 因此本条款可能不适用于您。

本信息可能包含技术方面不够准确的地方或印刷错误。本信息将定期更改；这些更改将编入本信息的新版本中。IBM 可以随时对本出版物中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对任何非 IBM Web 站点的引用都只是为了方便起见才提供的， 不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: (i) 使其能够在独立创建的程序和其它程序（包括本程序）之间进行信息交换，以及 (ii) 使其能够对已经交换的信息进行相互使用，请与下列地址联系:

IBM Corporation
Software Interoperability Coordinator, Department YBWA

3605 Highway 52 N
Rochester, MN 55901
U.S.A.

只要遵守适当的条款和条件，包括某些情形下的一定数量的付费， 都可获得这方面的信息。

本文档中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际程序许可协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的。实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的 资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问 题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

本信息仅用于规划的用途。在所描述的产品可用之前，此处的信息可能更改。

本信息包含日常业务经营中使用的数据和报告的示例。为了尽可能完整地说明这些示例，这些示例中包括个人、公司、品牌和产品的名称。所有这些人名或名称均系虚构，如有实际的企业名称和地址与此雷同，纯属巧合。

版权许可证:

本信息包含源语言形式的样本应用程序，用以阐明在不同操作平台上的编程技术。如果是为按照在编写样本程序的操作平台上的应用程序编程接口 (API) 进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例尚未在所有条件下经过全面测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。这些实例程序“按现状”提供，不附有任何种类的保证。对于因使用样本程序所引起的任何损害，IBM 概不负责。

这些样本程序的每份拷贝或其任何部分或任何衍生产品，都必须包括如下版权声明:

©（贵公司的名称）（年份）。此部分代码是根据 IBM Corp. 的样本程序衍生出来的。

© Copyright IBM Corp.（输入年份）。

编程接口信息

本《域名系统》出版物介绍了一些预期的编程接口，这些接口允许客户编写程序来获取 IBM i 的服务。

商标

IBM、IBM 徽标和 ibm.com 是 International Business Machines Corp., 在全球许多管辖区域的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。当前的 IBM 商标列表，可从 Web 站点 www.ibm.com/legal/copytrade.shtml 上『版权和商标信息』部分获取。

Adobe、Adobe 徽标、PostScript 以及 PostScript 徽标是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

其他产品和服务名称可能是 IBM 或其他公司的商标。

条款和条件

如果符合以下条款和条件，那么授予您使用这些出版物的许可权。

个人使用: 只要保留所有的专有权声明，您就可以为个人、非商业使用复制这些出版物。未经 IBM 明示同意，您不可以分发、显示或制作这些出版物或其中任何部分的衍生产品。

商业使用: 只要保留所有的专有权声明，您就可以仅在企业内复制、分发和显示这些出版物。未经 IBM 明示同意，您不可以制作这些出版物的衍生产品，或者在您的企业外部复制、分发或显示这些出版物或其中的任何部分。

在本许可权中除明示地授权以外，没有把其他许可权、许可证或权利（无论是明示的，还是默示的）授予其中包含的出版物或任何信息、数据、软件或其他知识产权。

一旦使用这些出版物损害了 IBM 的利益，或者 IBM 确定以上指令未被正确遵守，那么 IBM 保留自行决定撤销此处授予的许可权的权利。

您不可以下载、出口或再出口此信息，除非完全符合所有适用的法律和法规，包括所有美国出口法律和法规。

IBM 对这些出版物的内容不作任何保证。这些出版物以“按现状”的基础提供，不附有任何形式的（无论是明示的，还是默示的）保证，包括（但不限于）对非侵权性、适销性和适用于某特定用途的默示保证。

程序号: 5770-SS1

Printed in China