

数据分析与 DNS 服务器维护策略

于群英, 杨文荣

(陕西省生产力促进中心, 陕西 西安 710054)

摘要:针对复杂的网络环境中的 DNS 服务器搭建与发生故障等问题, 较为详尽地阐述了 DNS 实现原理, 并从 DNS 结构、查询原理入手, 对故障现象进行分析, 采用网络诊断命令 nslookup 获得相关数据, 根据返回的数据进行对比分析, 确定故障产生的原因, 探讨解决故障的方法, 系统地提出了由内到外、由 Intranet 到 Internet 逐步展开的策略。实践证明, 该策略能够提高复杂网络环境下的 DNS 的运行效率, 极大地缩短 DNS 故障排除时间, 从而保持网络的畅通。

关键词: DNS; nslookup; 网络维护

中图分类号: TP393

文献标识码: A

文章编号: 1673-629X(2008)06-0210-04

Data Analysis and Strategy of DNS Servers Maintenance

YU Qun-ying, YANG Wen-rong

(Shaanxi Provincial Productivity Promotion Center, Xi'an 710054, China)

Abstractor: Based on the principal of DNS resolving, analyses faults of DNS servers in complicated network environment and research methods to solve it. Emphasize that nslookup command plays an important role in processing the fault. Try to find reasons according to the data that returned by nslookup and to solve it step by step. That is from inside to outside and from Intranet to Internet. It is proved that the method which using in practice is a very effective method. It can raise the DNS operating efficiency and reduce the network breakdown elimination time and keep the network not be broken.

Key words: DNS; nslookup; network maintenance

0 引言

随着互联网的日益普及, 提起 DNS, 许多人对它并不觉得陌生, 因为人们上网时, 都需要设置 DNS 服务器地址, 或直接在 TCP/IP 协议的属性中输入互联网提供商所指定的 IP 地址, 或按互联网提供商的要求设置为自动获取, 否则会出现无法上网的现象。然而, 在构建信息服务体系时 DNS 含义却要复杂得多。

早在 1970 年, 互联网使用名为 hosts.txt 文件, 该文件可以通过 FTP 方式在互联网下载, 随着越来越多的网络加入到互联网, 每一新加入的网络管理员要传送主机名和它相应的 IP 地址, 因此保持 hosts.txt 的更新不仅变得非常困难, 而且 FTP 传输要占用大量网络带宽, 一种新的方法—Domain Name Service 应运而生, 它用于保持互联网中所有的主机相互通信, 即使该主机没有合适的 IP 地址信息也可以通过本地资源来进行通信^[1]。

1 DNS 与 IP 地址

DNS(Domain Name System)帮助用户在互联网上寻找路径^[2]。在互联网上的每一个计算机都拥有一个唯一的地址—IP 地址。由于 IP 地址(为一串数字)不方便记忆, DNS 允许用户使用一串常见的字母(即域名)取代。

ICANN(互联网名称与数字地址分配机构, Internet Corporation for Assigned Names and Numbers)负责协调管理 DNS 各技术要素以确保普遍可解析性, 使所有的互联网用户都能够找到有效的地址。它是通过监督互联网运作当中独特的技术标识符的分配以及顶级域名的授权来做到这一点。

根据 ICANN 的规定, ICANN 将部分 IP 地址分配给地区级的 Internet 注册机构 (Regional Internet Registry), 然后由这些 RIR 负责该地区的登记注册服务。

所谓普遍可解析性, 是指给定一个公共的 ICANN 会址, 能够确保从互联网的任意位置得到所期望的结果被称之为普遍可解析性 (universal resolvability)。这是域名系统中一个极为重要的设计特性, 它使得互联网在今天成为有用的全球资源。如果没有它, 同一个

收稿日期: 2008-01-02

基金项目: 科技部科技计划项目 (2004EE660010)

作者简介: 于群英 (1964-), 女, 江西人, 高级工程师, 研究方向为计算机网络、系统分析、电子政务和工作流分析等。

域名将在不同的情况下指向不同的网络位置,这将引起混乱。

2 DNS 原理剖析

2.1 DNS 层级树状结构

DNS 是许多分层式和分布式的数据组成的系统,这些数据库中有许多不同类型的数据,包括主机名、域名等等。DNS 数据库中的这些名字形成了一种树状层次结构,即名字空间。如图 1 所示。互连网络域名系统是由互连网络上的域名注册机构来管理的,他们负责管理向组织和国家开放的顶级域名,这些域名遵循 ISO-3166 国际标准。

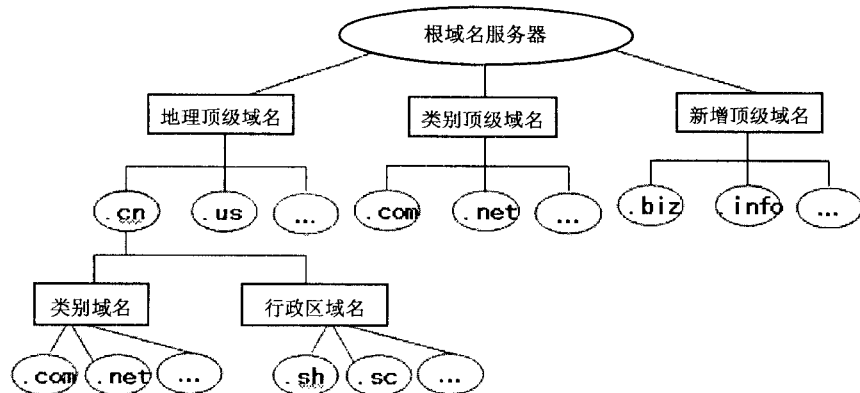


图 1 国际互联网域名体系^[3]

域名分为两大类:一类是在互联网上使用的,是唯一的,并且有相应的公共的 ICANN 会址对应的域名,即互联网域名;一类是仅在企业、学校等单位内部使用的域名,即内网域名。

申请(注册)互联网域名一般步骤:

步骤 1 第一步要做的是确定域名,该域名还没被使用(可以通过域名注册机构),如 dnsexample.gov.cn。

步骤 2 向 ISP 提供商申请网络地址 IP,如 100.1.1.100 和 100.1.1.101。

步骤 3 到域名注册机构申请域名。此时有两种情况:一种是使用注册机构 DNS 的主机(name server),这时仅输入与域名相关的 IP 地址以及其他相关数据;另一种是自主搭建配置 DNS 的主机(以下简称 DNS 服务器),这时要输入主机名及其相对应的 IP 地址(由于使用内网域名时的关键也是自主搭建 DNS 服务器,文中只讨论后在内网中 DNS 服务器的维护,所使用的 IP 及域名均为虚拟),如 dns1.dnsexample.gov.cn,对应的 IP 为 100.1.1.100, dns2.dnsexample.gov.cn 对应的 IP 为 100.1.1.101。

值得注意的是,按国际域名体系, dns.example.gov.cn 应属二级域名,但对于终端用户(申请域名的用

户)来说是一级域名,它下面可以延伸到二级域名(如 blog.dnsexample.gov.cn 等)。

2.2 DNS 的查询原理及过程

DNS 的查询可以在客户机和 DNS 服务器之间进行也可以在两个 DNS 服务器之间进行。一个查询只不过是对特定名字的特定类型的记录的一个请求。例如,一个查询可以请求到指定名字的所有主机资源记录。

有两种查询 DNS 服务器的方法:一种是递归查询,另一种是迭代查询。递归查询迫使 DNS 服务器做出查询成功或失败的响应。域名解析使用最多的就是这种查询方法。在递归查询中,如果需要的话, DNS 服务器必须与其他的 DNS 服务器通讯。但他从其他的 DNS 服务器收到成功响应的信号后,他就将响应返回给客户机。递归查询是查询名字服务器和名字服务器查询中继名字服务器(用来进行解析请求的传递)的一种典型方法。

当 DNS 服务器处理递归查询时,本地区域文件不能进行查询的解析,查询就会转到根 DNS 服务器。每一个标准的 DNS 服务器都有一个 cache 文件,或者叫根服务器列表,包括了 Internet 上的根服务器的对应 IP 地址。这个文件的最新版本的下地址是 <ftp://rs.internic.net/domain/named.cache>。

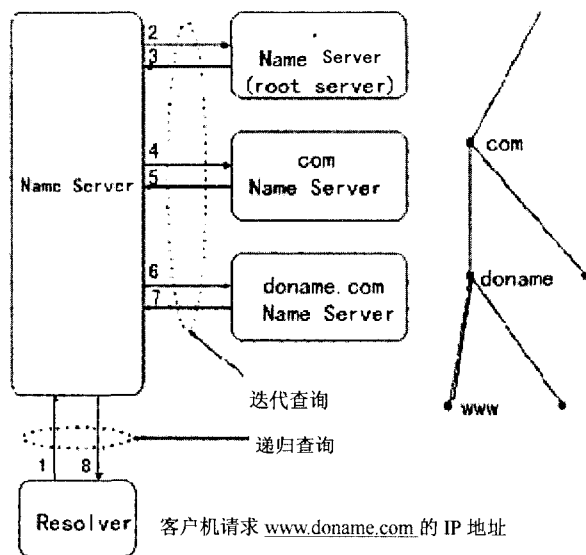
在迭代查询中, DNS 服务器根据本地的区域文件或 cache 文件,提供最好的信息。如果一个名字服务器没有能够回答解析的任何信息,他不会仅仅返回一个简单的否定信息,他会试着在本地域之外查找信息,为了解析一个名字,他可能会查询很多外部的 DNS 服务器。

图 2 显示了两种查询方法的比较。

DNS 数据库中定义的生存时间(TTL)可以保证 DNS 服务器不会存储过时的数据,也可以在客户端定义存储资源记录的最大 TTL,在定义生存时间时需要考虑缓存信息的准确度、DNS 服务器的使用频度和网络阻塞程度等因素^[5]。

如果解析请求是来自缓存,那么生存时间 TTL 也会随着传递过来。这样客户机就能知道相关信息的生存时间 TTL,而且客户机不会根据本身的生存时间 TTL 来改变接受的生存时间 TTL, DNS 数据库的更新因为区域文件中的资源记录是可以变化的,因此它们需要进行更新。DNS 数据库的更新有两种形式:一种

是静态更新,另一种是动态更新。



一个 DNS 数据库包含许多资源记录(RRs)。每一个资源记录标示数据库中的一种特定的资源 DNS 中有许多类型的资源记录项。表 1 是常见的几种记录项的详细信息(注意:这张表不包括全部的记录项):

表 1 资源记录表

描述	类别	TTL	缩写	字段
授权的开始	互联网(IN)	默认 60 分钟	SOA	主名称服务器 DNS 名
				负责人邮箱 DNS 名
				序列号
				刷新间隔
				重试间隔
				超时
				最小默认 TTL
主机项	互联网(IN)	与区域 SOA 相同	A	域
				主机名
				主机 IP 地址
名称服务器	互联网(IN)	与区域 SOA 相同	NS	域
				名称服务器 DNS 名
邮件交换	互联网(IN)	与区域 SOA 相同	MX	域
				主机名(可选)
				邮件交换服务器 DNS 名
				优先号
规范名称	互联网(IN)	与区域 SOA 相同	CNAME	域
				别名
				用于主机 DNS 名称

3 DNS 维护策略

3.1 Nslookup 命令

Nslookup 在进行 DNS 服务器维护时是非常有效的命令,它有许多选项,在 Windows 中可以在进入 Nslookup 后输入?,以获取详细的帮助。

在 Nslookup 中,DNS 服务器表现形式是 name server。如:

```
nameserver = dns1.dnsexample.gov.cn
```

Nslookup 返回的结果是 Non-authoritative answer,表示这个答案是从本地的 DNS 的 cache 中直接读出来的,而不是本地 DNS 向真正负责这个域名的 name server 问来的。

如果要获得某个 domain 的 name server 的别名 aliases,必须用自己的 name server 或 DNS 服务器地址作为解析服务器,即设定 server name。

3.2 DNS 服务器维护

(1)检测 DNS 服务器是否正常。

在 debug 模式中,观察域名服务器在查询时如何一直上溯到根域(如图 3 所示)。

(2)使用 DNS 服务器的地址作为用户 DNS 服务器地址无法上网。

此时需要考虑的是 DNS 服务器记录是否正确。使用 debug 方式对一个已知域名进行解析,在 Got answer 区将会显示如下信息:

```
questions = 1, answers = 1, authority records = 2, additional = 2
```

如果该行只有 Question,没有 Answer,需要检查 DNS 的配置。

(3)二级域名在互联网上不能浏览,而在内网访问正常。

主要原因是域名的 DNS 服务器记录本身有没有解析。

以观察 www.163.com 为例,可以看出获得的 ADDITIONAL RECORDS 信息与它的注册信息是一致的。

```
> set d2
> www.163.com
.....
```

ADDITIONAL RECORDS: (与注册信息一致)

```
- > ns.nease.net
type = A, class = IN, dlen = 4
internet address = 202.106.185.75
ttl = 18000 (5 hours)
- > ns3.nease.net
type = A, class = IN, dlen = 4
internet address = 220.181.28.3
ttl = 18000 (5 hours)
```

.....(略)

另一个原因是软件或硬件防火墙。在服务器上检查是否允许 domain(53 端口)的 tcp 及 udp 连接,或暂时停止一些服务(如 ipchains/iptables),看外部是否能够连接。此外还要检查防火墙是否打开 53 端口。

```

> set debug
> www.sohu.com
Server: dns1.dnsexample.gov.cn
Address: 100.1.1.100
Got answer:
HEADER:
opcode = QUERY, id = 2, rcode = NXDOMAIN
header flags: response, auth, answer, want recursion, recursion avail.
questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:
www.sohu.com.dnsexample.gov.cn, type = A, class = IN
AUTHORITY RECORDS:
-> dnsexample.gov.cn
ttl = 3600 (1 hour)

(.....)
Got answer:
HEADER:
opcode = QUERY, id = 3, rcode = NXDOMAIN
header flags: response, auth, answer
questions = 1, answers = 0, authority records = 1, additional = 0

QUESTIONS:
www.sohu.com.gov.cn, type = A, class = IN
AUTHORITY RECORDS:
-> gov.cn

(.....)
Got answer:
HEADER:
opcode = QUERY, id = 4, rcode = NOERROR
header flags: response, want recursion, recursion avail.
questions = 1, answers = 10, authority records = 0, additional = 0

QUESTIONS:
www.sohu.com, type = A, class = IN
ANSWERS:
-> www.sohu.com
canonical name = d7.a.sohu.com
ttl = 600 (10 mins)

```

图3 域名跟踪

(4) 域名解析有时正常有时不正常。

通常是域名的多个DNS服务器上的解析不一致,同步有问题。

依次查询该域名的每个DNS服务器,检查结果是否一致。在所有的服务器中,如果有的服务器没有返回结果,不会影响到域名的正常解析,因为此时解析客户端会尝试其他的服务器,只有当所有的服务器都没有结果才会报错。但是如果dns1服务器上上和dns2服务器上的解析不一致,则会出现域名解析时有时不对的故障。检测方式:分别输入下面两行命令,对输出的

结果进行比较。

```
# lookup www.163.com dns1.dnsexample.gov.cn
```

```
# lookup www.163.com dns1.dnsexample.gov.cn
```

4 结束语

在DNS服务器配置搭建和故障排除的过程中,可从DNS结构、查询原理入手,使用Nslookup命令来获取相关信息,首先判断DNS服务器的设置是否正确,然后检查它在内网的工作状态是否正常,最后再检查它在互联网上工作状态,这就形成了由近到远、由内到外进行维护方式,从而使DNS服务器保持正常运转。

参考文献:

[1] Sun Microsystems, Inc. Solaris 2. x Network Administration SA - 380, Sun Service, Part Number 802-6159-01, Revision C[R].

U. S. A: Sun Microsystems, Inc., 1996.

[2] ICANN. The global Internet community working together to promote the stability and integrity of the Internet[EB/OL]. 2006-03-26. <http://www.icann.org/tr/english.html>.

[3] 陈海涛, 岳虹, 田艳芳. Windows 2000 DNS 技术指南[M]. 北京: 机械工业出版社, 2000.

[4] 金灵. 域名系统(DNS)大观之基本知识[J/OL]. CNNIC 通讯第9期, 2001, <http://www.cnnic.cn/resource/daily/2001-1/3-2.shtml>.

[5] Mockapetris P. DOMAIN NAMES - CONCEPTS and FACILITIES[S]. RFC1034. [s.l.]: [s.n.], 1987.

(上接第209页)

电网中的应用[M]. 北京: 科学出版社, 2003.

[3] van der Aalst W, van Hee K. Workflow Management: Models, Methods and Systems[M]. 王建民, 闻立杰译. 北京: 清华大学出版社, 2004.

[4] 范玉顺. 工作流管理技术基础[M]. 北京: 清华大学出版社, 2001.

[5] 韦华颖, 詹剑锋, 王沁. 分布式构件技术综述[J]. 计算机应用研究, 2004(10): 12-15.

[6] 姚全珠, 戴建峰. 基于构件和XML的信息系统集成平台的研究[J]. 计算机工程与应用, 2004(19): 113-115.

[7] WFMC. The workflow reference model[S/OL]. 2005.

<http://www.wfmc.org/standards/model.htm>.

[8] Open GIS Consortium. Geography Markup Language (GML) Implementation Specification[S]. Reference number OGC 03-105r1, Version: 3.1.0, 2004.

[9] Workflow Management Coalition. Workflow Process Definition Interface - XML Process Definition Language[S]. Document Number WFMC - TC - 1025, Document Status - Version 1.0, 2002.

[10] Salimifard K K, Wright M. Petrinet - based modeling of workflow systems: An overview[J]. European Journal of Operational Research, 2001, 134: 664-676.