**DNS服务基础**

**所有完整的域名都要以点结尾，最高域是根域**

DNS工作原理

DNS解析的作用（域名解析 将域名解析为ip地址）

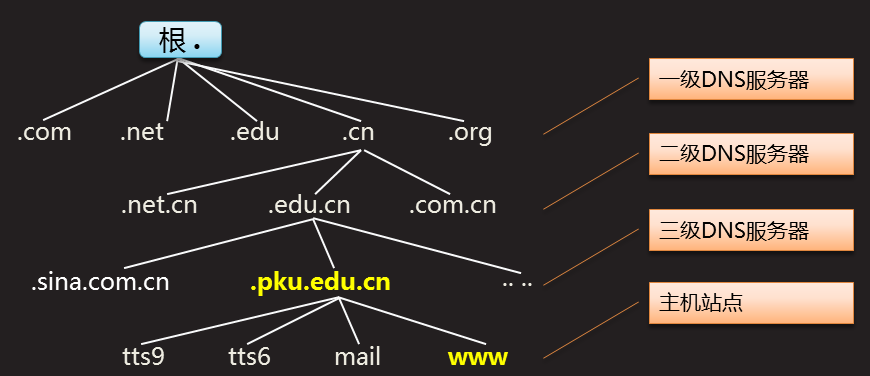
DNS服务器的功能

正向解析：根据注册的域名查找对应的IP地址

反向解析：根据IP地址查找对应的域名，不常用

DNS分布式结构

大型、分布式的互联网DNS解析库



FQDN，完全合格主机名

=站点名.域名后缀

=站点名.....二级域.一级域

常见的一级域名

国家/地区域：.cn、.us、.kr、.hk、.tw

组织域：.com、.net、.edu、.org、.gov、.mil

DNS域名管理

IANA，互联网数字分配机构

internet assigned numbers authority

整个域名系统最高的权威机构

主管DNS根、.int、.arpa等国际话域名资源

CNNIC，中国互联网络信息中心

china internet network information center

主管国家顶级域名.cn

域名代理/注册/购买服务商

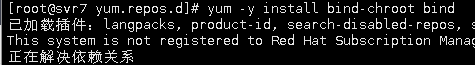
新网：[www.xinnet.com](http://www.xinnet.com)

万网：[www.net.cn](http://www.net.cn)

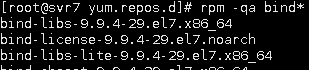
中国互联：http://hulian.top

基础DNS搭建（BIND服务解析）

BIND域名服务yum -y install bind-chroot bind



bind-chroot包提供安全方面的机制，提供虚拟根的支持，检测DNS是否异常，如果异常，会圈/var/named/chroot中运行（牢笼政策）



BIND服务器端程序

主要执行程序：/usr/sbin/named

系统服务：named

默认端口：tcp/udp 53

运行时的虚拟根环境：/var/named/chroot

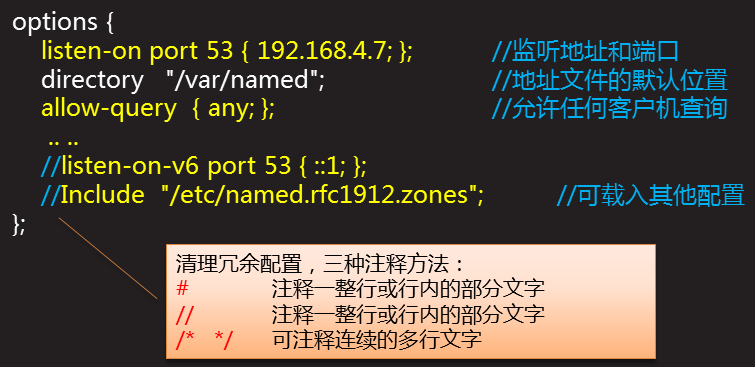
主配置文件：/etc/named.conf

地址库文件：/var/naemd

named.conf配置文件（设置本机负责解析的域名）

全局部分

设置监听地址/端口、地址库存放位置等



listen-on port里的地址指的是提供服务的IP地址，any或者删除，默认为所有用户提供服务

区域配置部分

定义DNS区域、类型、地址文件路径等

关键词IN表示internet，可省略



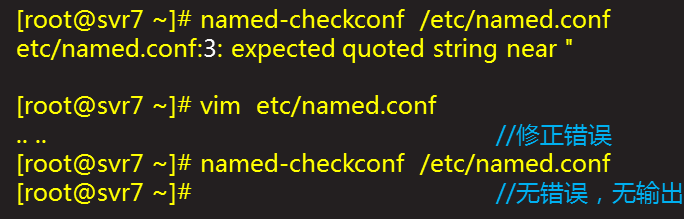
zone括号里的是设置负责解析的域名

type类型有master（主），slave（从），hint（只有根域才用）

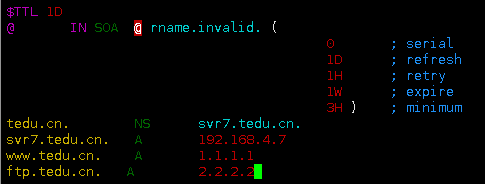
file起名随意，最后在/var/named写入该文件

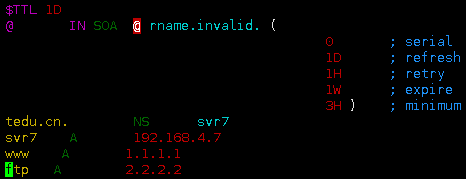
检查配置语法

格式：named-checkconf [配置文件]



地址库文件（记录主机名与IP地址的对应记录）@等同于负责的域名





全局TTL配置项及SOA记录

$TTL（生存时间，默认缓存一天）

SOA（授权信息开始，后面跟邮箱，邮箱没有@，用点分隔）

分号“；”开始的部分表示注释

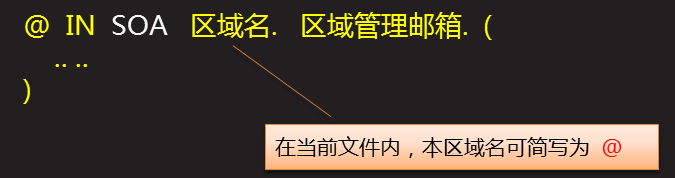
0：代表版本号，主从同步用

1D：缓存没有的消息

1H：每个一小时从访问主

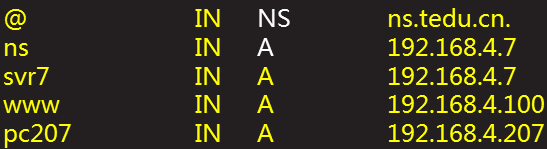
1W：从联系主，一周没有联系，就认为挂掉了

3H：当从联系主没有回应，会三个小时以后再访问



NS（标注域名的名字服务器），域名服务器记录，NS前边写这个地址库负责的域名是什么，末尾要有点，后面要写域名的名字服务器是什么，默认有点

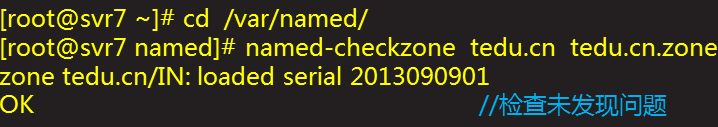
A，地址记录，仅用于正向解析，正向解析的记录



指明dns服务器名称和地址，必须有

检查配置语法

格式：named-checkzone 区域名 配置文件



**特殊解析**

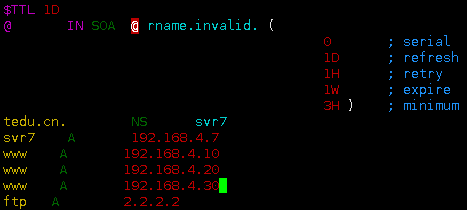
地址记录的应用

DNS轮询（基于DNS站点进行轮询）（地址库写三条一样的即可）

基于DNS的站点负载均衡

一个域名对应多个不同IP地址

每个IP提供镜像服务内容



泛域名解析

匹配本区域内为定义的任何主机

直接以\*条目匹配

一般只用在正向区域文件中



有规律的泛域名解析

$GENERATE造数工具（造1-50个数字）



解析记录的别名

tts和ftp是同一服务器

**DNS子域名授权**

配置子域名

子域名的作用

适用于同一个DNS组织

父/子域的解析工作由不同的DNS服务器负责

父DNS服务器应该尤为子域迭代的能力

按理环境及要点

子DNS：pc207.bj.tedu.cn 192.168.4.207

负责bj.tedu.cn域的解析

父DNS：svr7.tedu.cn 192.168.4.7

负责tedu.cn域的解析

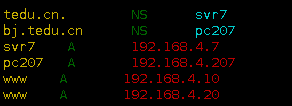
当客户机向父DNS查询www.bj.tedu.cn时，授权给子DNS处理，获得反馈结果后发给客户机

基本配置步骤：

1. 配置父DNS（www.tedu.cn->192.168.4.100）
2. 配置子DNS（www.bj.tedu.cn->1.2.3.4）
3. 在父DNS中，添加子域授权配置

子域域名. IN NS 子DNS的FQDN.

子域的FDNQ. IN A 子DNS的IP地址



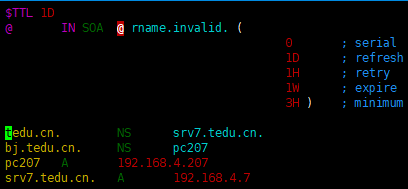
1. 测试子域FQDN查询

为父DNS启用子域授权

修改父域的地址库文件

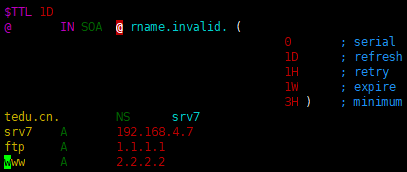
添加子域NS记录

确保有可用的DNS服务器的A记录



测试子域FQDN查询

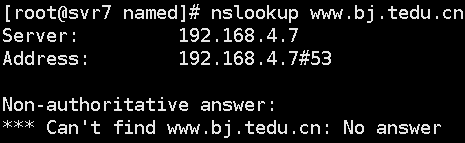
向父DNS可查询子域中的站点



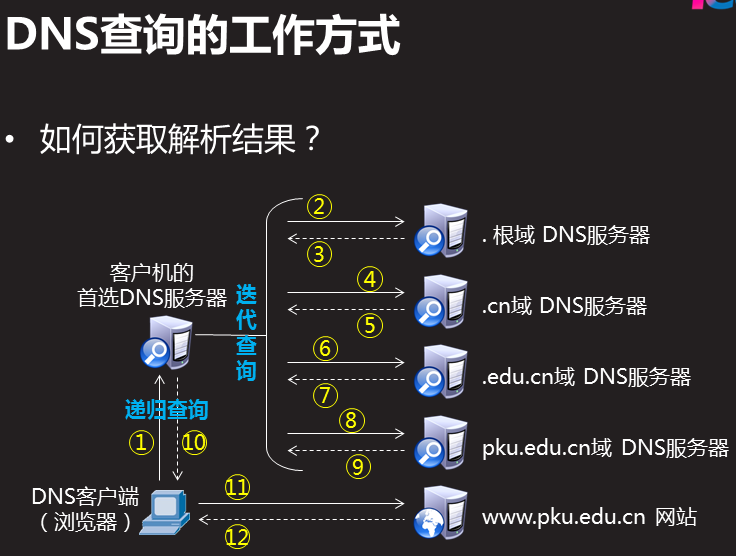
递归/迭代授权

递归解析：指DNS服务器与其他DNS服务器交互，最后将解析结果带回来的过程

关闭递归解析，yes是解析，没有是解析



迭代解析：指DNS服务器与其他DNS服务器交互，最终将会告知下一个DNS服务地址

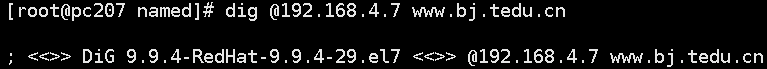


验证迭代查询

dig命令，更专用的DNS测试工具

有软件包bind-utils提供

格式：dig @DNS服务器 目标地址



**缓存dns**

**作用：缓存解析结果，提高解析速度**

缓存DNS概述

互联网DNS角色

权威/官方DNS

至少管理一个DNS区域，需要IANA等官方机构的授权

典型应用：根域DNS、一级域DNS...

缓存DNS

不需要管理任何DNS区域，但是能够替客户机查询。而且通过缓存、复用查询结果来加快速度

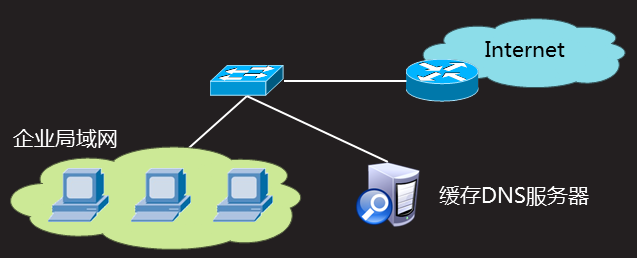
典型应用：ISP服务商、企业局域网

缓存DNS的适用场景

主要适用环境

互联网出口带宽较低的企业局域网络

ISP服务商的公共DNS



解析记录来源

方式1：全局转发

将请求转发给指定的公共DNS（其他缓存DNS），请求递归查询

方式2：根域迭代

依次向跟、一级、二级.....域的DNS服务器迭代

全局转发式缓存（用内存缓存）

配置要点

基本配置步骤

1. 建立named.conf主配置文件

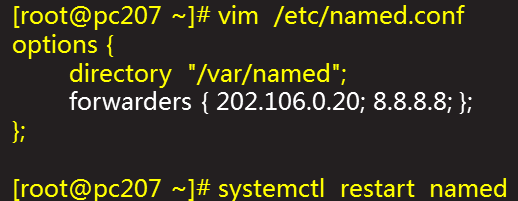
设置forwarders {公共DNS;}; 转发器

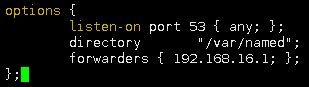
1. 启动named服务
2. 验证缓存DNS服务器

添加转发器，并启用named服务

以转发至202.106.0.20、8.8.8.8为例

前提条件：缓存DNS与上述DNS之间网络通常





测试查询效果

前提条件及效果

只要202.106.0.20、8.8.8.8能提供的解析记录

向本例中的缓存DNS一样可以查到



