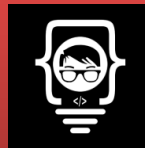




Ubuntu Server 从入门到精通

第八章：DNS服务





# DNS服务

你是老谁家小谁

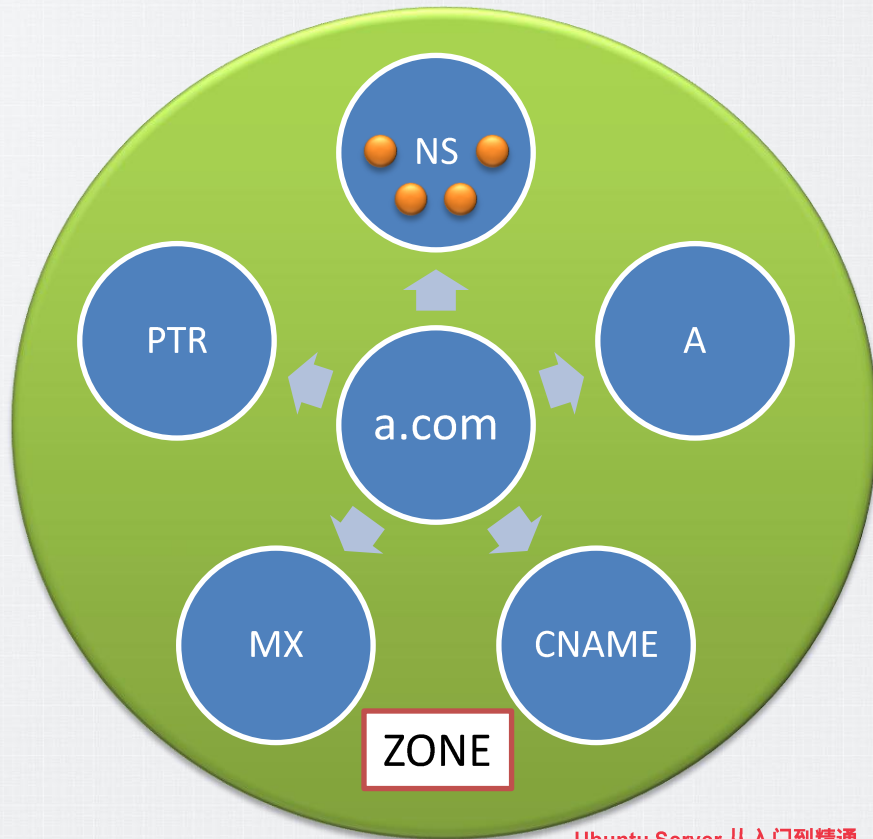
- DNS ( Domain Name Service )
  - 将容易记忆的主机名映射到IP地址
- 计算机命名规范
  - Netbios 名称
  - Hostname
  - DNS分布式名称系统
- DNS服务结构
  - 域名 ( sina.com.cn )
  - FQDN ( www.sina.com.cn )
    - fully qualified domain names



# DNS记录类型

你是老谁家小谁

- NS 域名服务器记录
- A 主机记录
- CNAME 别名记录
- MX 邮件交换记录
- PTR 指针记录（反向查询）
- SOA 起始授权记录

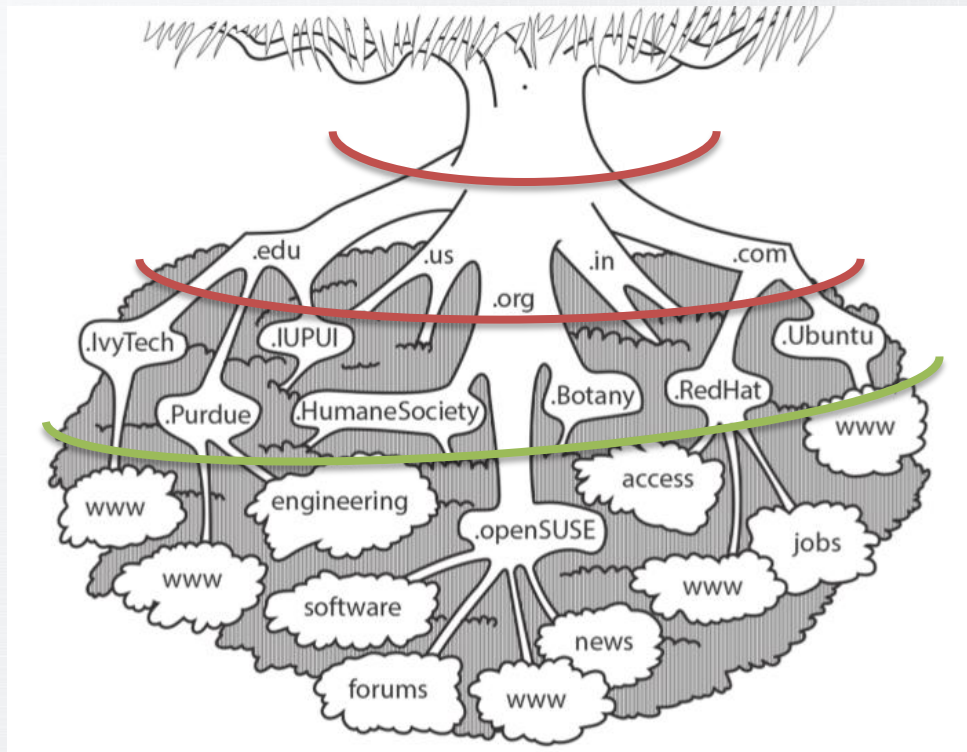


....

# DNS服务

你是老谁家小谁

- DNS命令空间
- 逐级委派
- ICANN负责管理
- www.ubuntu.com.



# DNS查询结构

你是老谁家小谁

- 三种DNS服务器

- Master

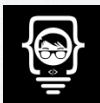
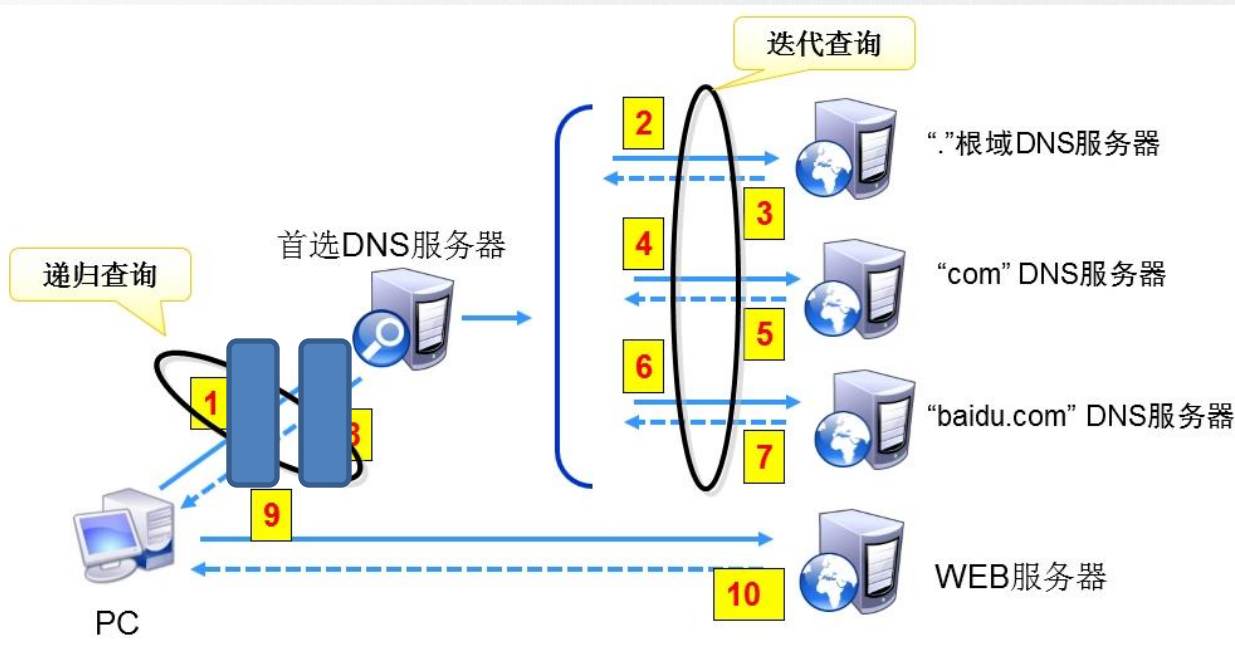
- Slave

- Cache

- TTL

- Forward

- 同时是三种角色







# 安装DNS服务

你是老谁家小谁

- BIND (Berkley Internet Naming Daemon)
- `sudo apt install bind9 dnsutils`
  - DNS服务器只保存和解析本域各种域名记录
  - DNS服务器都包含13个根域域名服务器地址
    - 事实分布于世界的数百台服务器
  - DNS服务器的DNS服务器配置
    - 自己做迭代
    - 指定递归域名服务器
- DNS默认服务端口
  - TCP 53 / UDP 53





# BIND的替代方案

你是老谁家小谁

- Djbdns
  - Dbndns、ndjbdns
- dnsmasq
  - DNS + DHCP 打包的轻量解决方案
- PowerDNS
  - 模块化开源DNS服务器软件

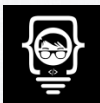




# 配置Cache DNS服务器

你是老谁家小谁

- 主配置文件 /etc/bind/named.conf
  - include "/etc/bind/named.conf.options";
  - include "/etc/bind/named.conf.local";
  - include "/etc/bind/named.conf.default-zones";







# 配置Cache DNS服务器

你是老谁家小谁

- 全局转发DNS服务器
- `sudo vi /etc/bind/named.conf.options`
  - `acl "local" {` # options 块之前
  - `10.1.8.0/24;` # 本地网段
  - `};`
  - `options {`
  - `recursion yes;`
  - `allow-recursion { local; };`
  - `listen-on { 10.0.2.53; };`
  - `forwarders {`
  - `9.9.9.9;`
  - `8.8.8.8;`
  - `};`
  - `};`



# 配置Cache DNS服务器

你是老谁家小谁

- 区域转发
- `sudo vi /etc/bind/named.conf.options`
  - `zone "sina.com.cn" {`
  - `type forward;`
  - `forwarders {`
  - `192.168.60.101;`
  - `192.168.60.102;`
  - `};`
  - `}`
- `sudo systemctl restart bind9.service`

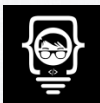




# 配置Master DNS服务器

你是老谁家小谁

- 指定区域文件（正向区域）
  - `sudo vi /etc/bind/named.conf.local`
  - `zone "lab.com" {`
  - `type master;`
  - `file "/etc/bind/db.lab.com";`
  - `};`



# 配置Master DNS服务器

你是老谁家小谁

- 编辑区域文件

- `sudo cp db.local db.lab.com`
- 管理邮箱 [root@lab.com](mailto:root@lab.com)
- \$TTL 允许缓存时长 (1D)
- 手动增加 Serial
- Slave 更新周期
  - Refresh、Retry、Expire
  - 8H、1D、2W
- Class
  - IN、CH、HS
- () 多行内容 (SOA)

```
;; BIND data file for lab.com
$TTL      604800
@         IN      SOA      ns.lab.com. root.lab.com. (
                                2           ; Serial
                                604800      ; Refresh
                                86400       ; Retry
                                2419200     ; Expire
                                604800 )    ; Negative Cache TTL
;
@         IN      NS       ns
@         IN      A        10.1.8.2
ns        IN      A        10.1.8.145
@         IN      MX       10    mx1
@         IN      MX       20    mx2
mx1       IN      A        10.1.8.145
mx2       IN      A        10.1.8.2
www       IN      CNAME     web
web       IN      CNAME     w3
w3        IN      A        10.1.8.2
```



# 配置Master DNS服务器

你是老谁家小谁

- 服务器配置检查

- `sudo named-checkconf` # 检查语法错误
- `sudo named-checkzone lab.com /etc/bind/db.lab.com` # 正向区域检查
- `sudo named-checkzone lab.com /etc/bind/db.10` # 反向区域检查

- 客户端解析验证

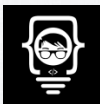
- `dig lab.com ns @10.1.8.10`
- `dig www.lab.com @10.1.8.10`
- `dig lab.com a @10.1.8.10`
- `dig lab.com mx @10.1.8.10`



# 配置Master DNS服务器

你是老谁家小谁

- nslookup
  - server 10.1.8.100      # DNS服务器
  - set q=ns      # 查询记录类型a、mx、soa.....
  - lab.com      # 查询目标（域名、FQDN）
- Windows 本地缓存DNS解析结果
  - ipconfig /displaydns
  - ipconfig /flushdns
- Ubuntu Linux 默认不在本地缓存DNS解析结果



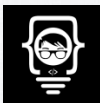




# 配置Master DNS服务器

你是老谁家小谁

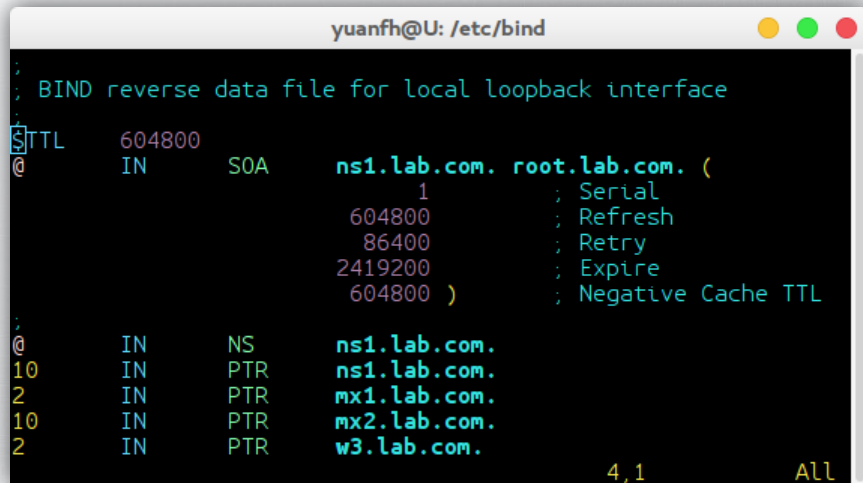
- 反向区域
  - IP解析到域名（反垃圾邮件）
  - `sudo vi /etc/bind/named.conf.local`
  - `zone "8.1.10.in-addr.arpa" {`
  - `type master;`
  - `file "/etc/bind/db.10.1.8";`
  - `};`



# 配置Master DNS服务器

你是老谁家小谁

- 编辑反向区域文件
- `sudo cp /etc/bind/db.127 /etc/bind/db.10.1.8`
- `sudo vi /etc/bind/db.10.1.8`



```
yuanfh@U: /etc/bind
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      ns1.lab.com. root.lab.com. (
; Serial
        604800      ; Refresh
        86400       ; Retry
        2419200     ; Expire
        604800 )    ; Negative Cache TTL
;
@         IN      NS       ns1.lab.com.
10        IN      PTR      ns1.lab.com.
2         IN      PTR      mx1.lab.com.
10        IN      PTR      mx2.lab.com.
2         IN      PTR      w3.lab.com.

                                4,1      All
```



# 配置Slave DNS服务器

你是老谁家小谁

- 为实现冗余容错，通常会为每个域安装多个Slave DNS服务器
- 修改记录只在Master上操作，通过版本号通知Slave服务器同步
- 安全考虑
  - 服务器全局禁止区域传输（同步本域所有DNS记录）
  - 至允许指定IP、指定区域的Slave服务器进行区域传输
  - 区域数据同步使用TCP 53端口
  - `dig @ns1.lab.com lab.com axfr`
  - `sudo vi named.conf.options`
  - `allow-transfer { none; };`

```
recursion yes;  
allow-recursion { local; };  
listen-on { 10.1.8.10; };  
allow-transfer { none; };  
forwarders {  
    202.106.0.20;  
    9.9.9.9;  
};
```



# 配置Slave DNS服务器

你是老谁家小谁

- 修改master服务器配置
- `sudo vi /etc/bind/named.conf.local`
  - `allow-transfer { 10.0.2.54; };`

```
zone "lab.com" {
    type master;
    file "/etc/bind/db.lab.com";
    allow-transfer { 10.1.8.20; };
};

zone "8.1.10.in-addr.arpa" {
    type master;
    file "/etc/bind/db.10.1.8";
    allow-transfer { 10.1.8.20; };
};
```



....

# 配置Slave DNS服务器

你是老谁家小谁

- 修改master服务器配置
- `sudo vi /etc/bind/db.lab.com`
  - ns2 IN A 10.1.8.20

```
$TTL      604800
@         IN      SOA      ns1.lab.com. root.lab.com. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       ns1.
@         IN      NS       ns2.
ns1       IN      A        10.1.8.10
ns2       IN      A        10.1.8.20
```

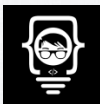




# 配置Slave DNS服务器

你是老谁家小谁

- 安装第二台DNS服务器并配置
- `sudo vi /etc/bind/named.conf.options`
  - `acl "local" {`
  - `10.1.8.0/24;`
  - `};`
  - `options {`
  - `recursion yes;`
  - `allow-recursion { local; };`
  - `listen-on { 10.1.8.20; };`
  - `allow-transfer { none; };`
  - `.....`







# 配置Slave DNS服务器

你是老谁家小谁

- 配置第二台DNS服务器
- `sudo vi /etc/bind/named.conf.local`
  - `/var/cache/bind/`
  - `grep bind /var/log/syslog`

```
zone "lab.com" {  
    type slave;  
    file "db.lab.com";  
    masters { 10.1.8.10; };  
};  
  
zone "8.1.10.in-addr.arpa" {  
    type slave;  
    file "db.10.1.8";  
    masters { 10.1.8.10; };  
};
```

# 创建 slave 区域

# 同步文件存放目录 (option)

# 查看日志



# 配置Slave DNS服务器

你是老谁家小谁

- 记录更新通知
  - Slave 服务器到达更新周期时拉
  - 客户端数据加密保存（不能直接修改）
  - Master 服务器通知版本号
  - `sudo vi /etc/bind/named.conf.local`
  - `Also-notify { 10.1.8.20; };`

```
zone "lab.com" {  
    type master;  
    file "/etc/bind/db.lab.com";  
    allow-transfer { 10.1.8.20; };  
    also-notify { 10.1.8.20; };  
};  
  
zone "8.1.10.in-addr.arpa" {  
    type master;  
    file "/etc/bind/db.10.1.8";  
    allow-transfer { 10.1.8.20; };  
    also-notify { 10.1.8.20; };  
};
```



...

# Questions?

