**Conceitos Básicos de DNS**

"*Domain Name Service*" is a standard TCP/IP protocol designed to provide name-to-IP address resolution. (others, such as NIS and LPAD, can also provide name resolution, but they also provide other operations).

Client DNS is configured by /etc/resolv.conf and /etc/nssswitch:

#cat /etc/resolv.conf

#cat /etc/nsswitch

Main DNS software are:

BIND (Berkeley Internet Name Domain) is the most widely used.

dnsmask is designed for small networks and can be used as DNS Forwarder and DHCP. It's lightweight and easy to configure.

djbdns intends to inpose security standars than the others.

PowerDNS was designed to provide load balancing, where different IP addresses were provided by the DNS server to spread the load of URL requests between multiple web servers.

1.2 The primary DNS configuration file

Cache DNS server: The default instalation of bind9 is for a caching name server. Just install and start bind.

acl "test\_env" { localhost, 192.168.11.0/24; !192.168.11.15; };

allow-query { "test\_env" };

1.3 Standard DNS-based commands.

The rndc command can be used to perform specific actions on the named server. Ex:

# rndc reload reloads all configuration files. It’s equivalente to “kill -1 `pidof named`”

# rndc reload <zone> reloads only the specified zone configuration.

rndc comes ready to use on centos7/RHEL7, but, eventual you may need to reconfigure it, means, recreate the /etc/rndc.conf and /etc/rndc.key files:

# rndc-confgen > /etc/rndc.conf

# chmod 640 /etc/rndc.conf

# kill -1 `pidof named`

Copy to /etc/named.conf the lines after “Use with the following ...” removing the “#” or just update the information, specially the secret.

Other rndc commands are, among many others ...:

# rndc dumpdb Dumps the server’s cache and/or all zone lile information for the named server.

# rndc flush Removes from memory the named cache.

# rndc reconfig Roloads only new configuration entries and new zones without reloading existing zone files.

# rndc status|stop

host command is used for simple hostname to IP address resolution:

# host www.google.com

# host www.google.com 8.8.8.8 (the default is to use the DNS from /etc/resolv.conf)

dig command can provide more detailed information about the name resolution query:

# dig @8.8.8.8 www.google.com

2. CREATE AND MAINTAIN DNS ZONES

2.1

3. SECURING A DNS SERVER

Internet

Rede Local

DNS local

Cliente

root DNS server

Query:

www.foo.com

Response:

200.155.1.5

Caching, forwarder, authoritative

root servers are aware of the DNS servers for the top level domains (.com, .edu, .net, etc.) if they don’t know the answare

Top level DNS ex: .com

DNS server