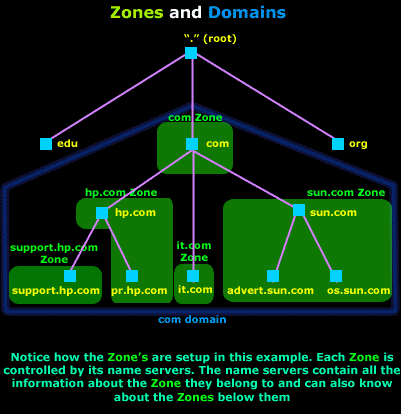
456

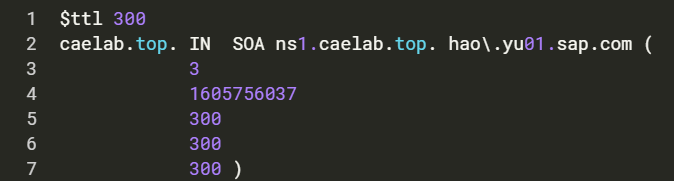
# DNS concept



# Explanation of terms

## General record

SOA record

An SOA record is a Start of Authority. Every domain must have a Start of Authority record at the cutover point where the domain is delegated from its parent domain. For example, if the domain mycompany.com is delegated to name servers, we must include an SOA record for the name mycompany.com in our authoritative DNS records. 

NS record

Lists a nameserver for this zone



A

Name-to-address mapping



MX

Email address to receive email



HINFO

Hardware information



TXT

Txt message information



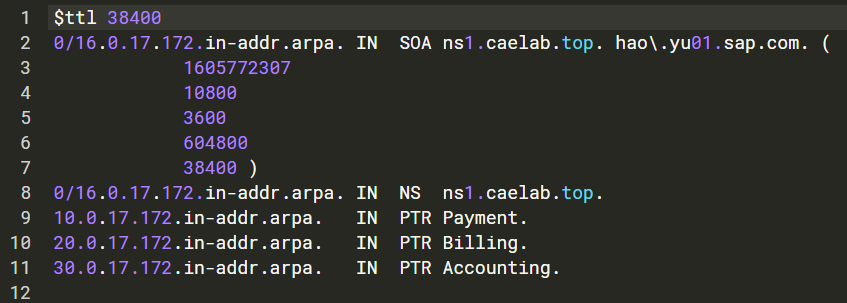
CNAME

Canonical name (for aliases)



PTR Records

Here are the PTR records we added for network 172.17.0.0/24



## Config file explain

@

符号“ /”或“ @”代表当前原点。在区域文件的开头

$ORIGIN

首次读取区域时， $ORIGIN < zone\_name> .，后跟尾随点

$ORIGIN example.com.

WWW CNAME MAIN-SERVER

等同

WWW.EXAMPLE.COM. CNAME MAIN-SERVER.EXAMPLE.COM.

$INCLUDE

Including config file such as follows

include "/etc/bind/named.conf.options";

include "/etc/bind/named.conf.local";

include "/etc/bind/named.conf.default-zones";

$TTL

Time to live

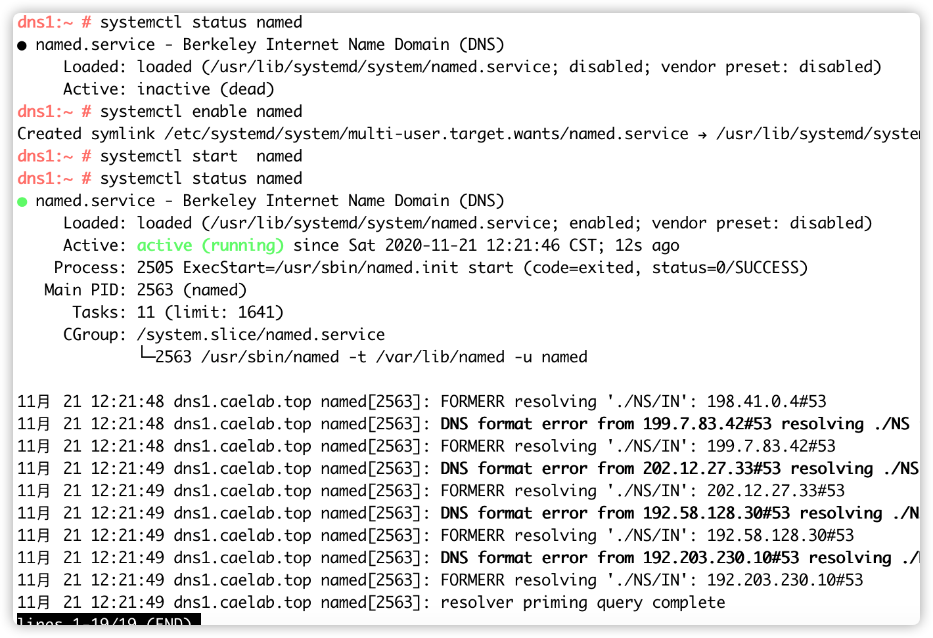
# DNS bind Installation on Linux

#sudo zypper up

#sudo zypper install -y bind bind-utils bind-doc



Make sure services and 53 port is up and running



# Running openSUSE leap+bind in docker

## pull images

Docker pull opensuse/leap

docker run -it --name=leap -p 53:53/tcp -p 53:53/udp -p 953:953/tcp -p 953:953/udp -d opensuse/leap /usr/sbin/named

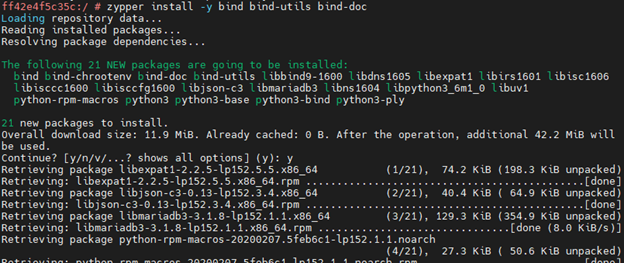
docker exec -it leap /bin/bash

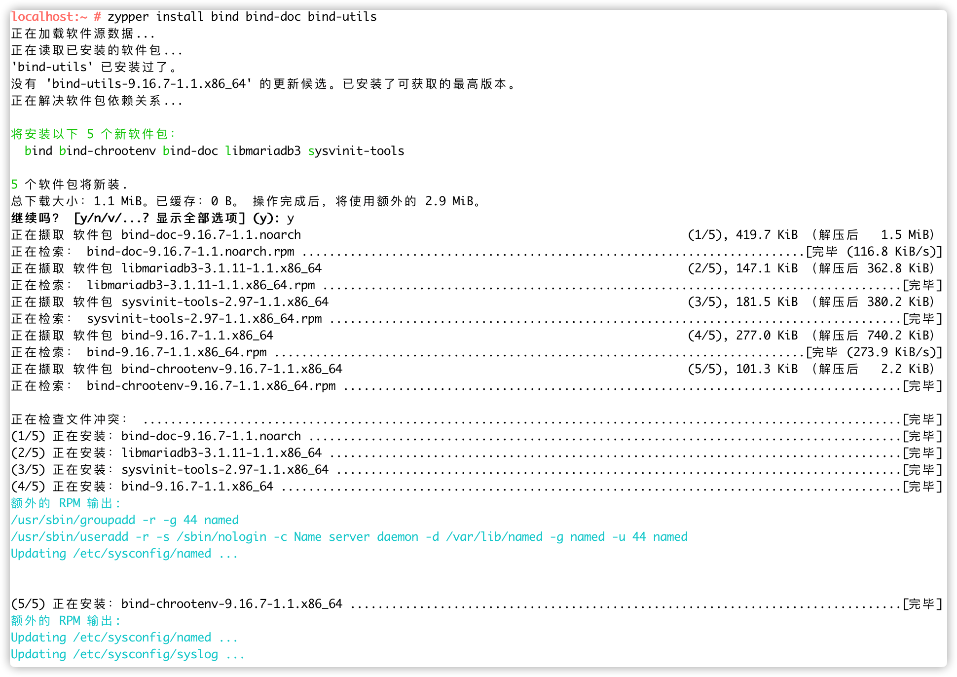
## Install bind in Leap

zypper --gpg-auto-import-keys ref

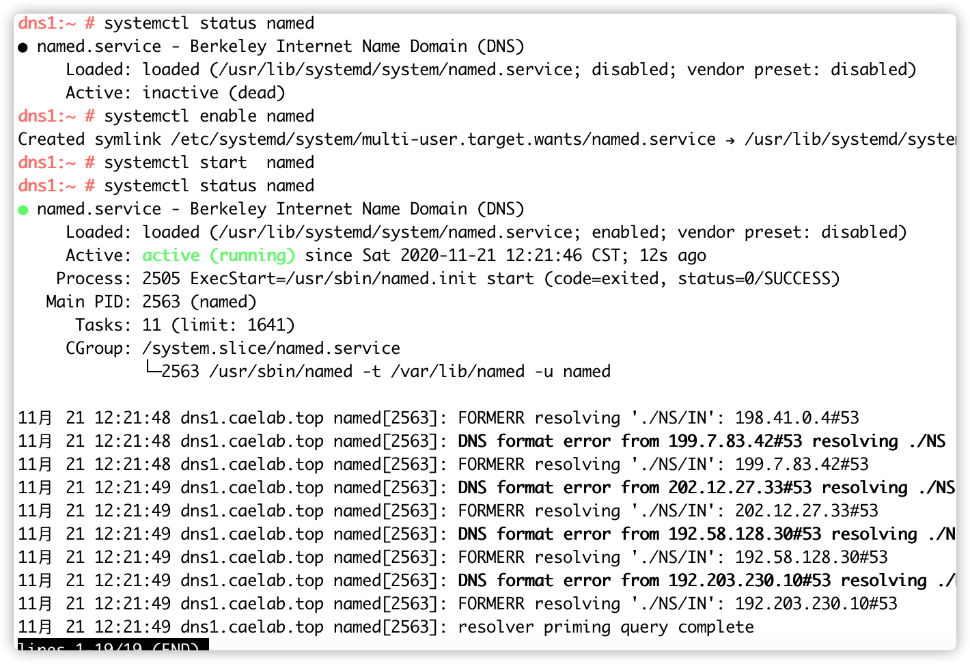
zypper up

zypper install -y bind bind-utils bind-doc





Check serveries



# Build customize leap bind9 built-in

## customize openSUSE leap

FROM opensuse/leap

MAINTAINER hao.yu01@sap.com

RUN zypper --gpg-auto-import-keys ref

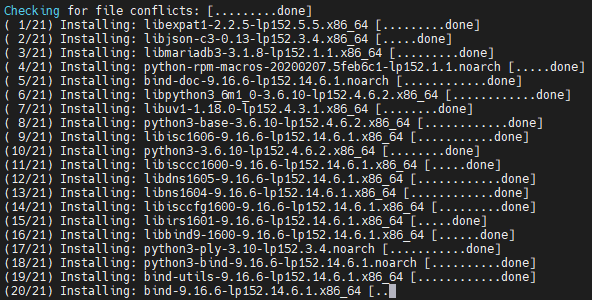
RUN zypper up

RUN zypper install -y bind bind-utils bind-doc

RUN zypper install -y vim which iputils telnet net-tools-deprecated

EXPOSE 53

CMD ["/usr/sbin/named"]



## Build the image

docker build -t leapdns:latest .

## Run image

docker run -it --name=leapdns -p 53:53/tcp -p 53:53/udp -p 953:953/tcp -p 953:953/udp -d leapdns:v1 -v

docker run -d --name bind9 -p 53:53/tcp -p 53:53/udp -v /opt/bind:/etc/bind -v /opt/lib:/var/lib/bind bind9:latest

# DNS architecture

## Single server config

## Master and slave replication

Create master zone in master server in

named.conf

$ttl 300

caelab.top. IN SOA ns1.caelab.top. hao\.yu01.sap.com. (

8

300

300

300

300 )

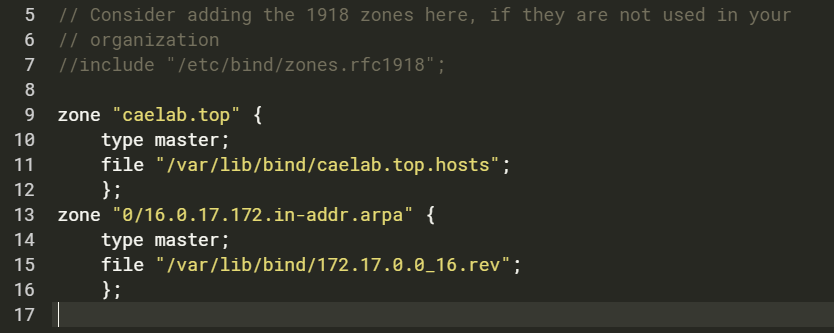
caelab.top. 5M IN NS ns1.caelab.top.

caelab.top. 300 IN NS ns2.caelab.top.

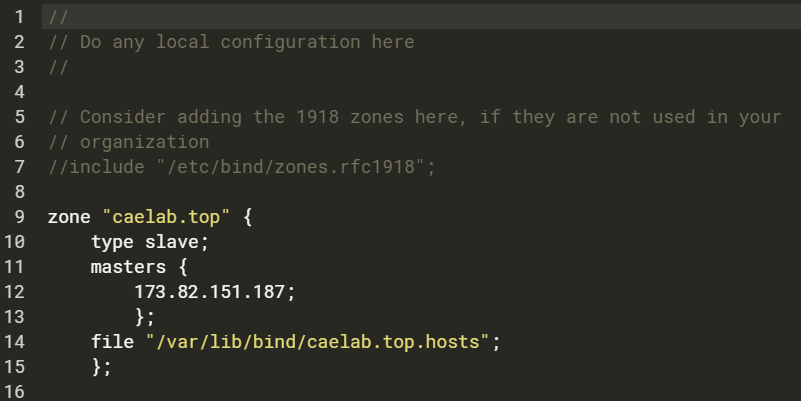
ns1.caelab.top. IN A 173.82.151.187

ns2.caelab.top. IN A 80.251.214.31

zone file



Slave server , set type as slave and sync from master



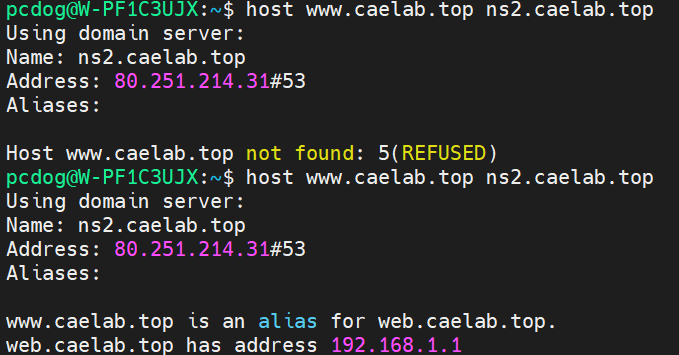
Add 2 record in NS1 Server

web.caelab.top. IN A 192.168.1.1

www.caelab.top. IN CNAME web

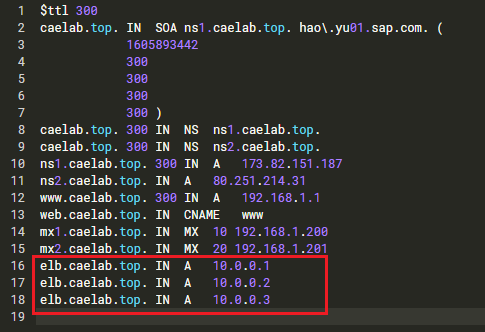
Check the record in NS2 server

First time did not find the record but after wait for 300 second then record is sync to NS2 from NS1



## Round-robin DNS

Same A record have multiple IP address can become a traffic load balance



# Security

## ACL

Bind v4

acl cae\_shanghai {

10.0.0.0/8};

Bind v8/v9

allow-query

{ 192.249.249/24; 192.253.253/24; 192.253.254/24; };

Define

acl "SAP-NET" { 10.59/16; };

zone "sap.corp" {

type slave;

file "cae.sap.corp";

masters { 10.59.152.2; };

allow-query { "SAP-NET"; };

};

Dynamic update permission

Allow-update { any;};

#old server return no correct record

Bogus server

server 10.0.0.2 {

bogus yes;};

blackhole

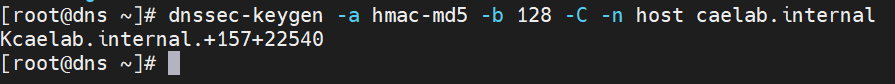
{192.168/16; };

## DNSSEC

dns sec-keygen utility

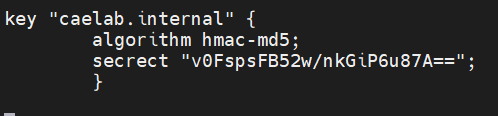
/var/named/keys

dnssec-keygen -a hmac-md5 -b 128 -C -n host caelab.internal



cat Kcaelab.internal.+157+22540.private

create a key



TSIG

not requirement private and public key

use single shared sceret

need to be securely distributed

need secure traffic between NS

allow vs view

dns query filter

listen-on binding on port

allow-query-on 这使得可以在面向内部接口上进行查询，而不必知道内部网络的地址

options {

allow-query-on { 203.0.113.17; };

allow-recursion-on { 10.0.0.17; };

allow-query-cache-on { 10.0.0.17; };

};

equal

acl corpnets {

10.0.0.0/16;

172.16.0.0/12;

};

options {

allow-query { any; };

allow-recursion { corpnets; };

allow-query-cache { corpnets; };

};

10.6. bind9引入了视图，这是另一种在防火墙环境中非常有用的机制。视图允许您向一个主机社区提供一个名称服务器配置，向另一个社区提供不同的配置社区。如果您在接收查询的主机上运行名称服务器，这一点特别方便您的内部主机和Internet上的主机（我们将在下一章讨论这一点）。

如果不配置任何视图，bind9会自动创建一个单独的隐式视图，并显示给所有人

查询它的主机。要显式地创建视图，可以使用view语句，它采用视图的名称

view "internal" {

};

您可以使用match clients view子语句选择哪些主机“查看”特定视图，该子语句采用地址匹配列表作为参数。如果不指定具有匹配客户端的主机社区，则适用于所有主机。

acl "internal" {

192.249.249/24; 192.253.253/24; 192.253.254/24; localhost;

};

view "internal" {

match-clients { "internal"; };

recursion yes;

zone "movie.edu" {

type master;

file "db.movie.edu";};

zone "249.249.192.in-addr.arpa" {

type master;

file "db.192.249.249";};

zone "." {

type hint;

file "db.cache";};};

view "external" {

match-clients { any; };

recursion no;

zone "movie.edu" {

type master;

file "db.movie.edu";};

zone "249.249.192.in-addr.arpa" {

type master;

file "db.192.249.249";};

zone "." {

type hint;

file "db.cache";};};

blacklist

options {

/\* Don't waste your time trying to respond to queries from RFC 1918

private addresses \*/

blackhole {

10/8;

172.16/12;

192.168/16;

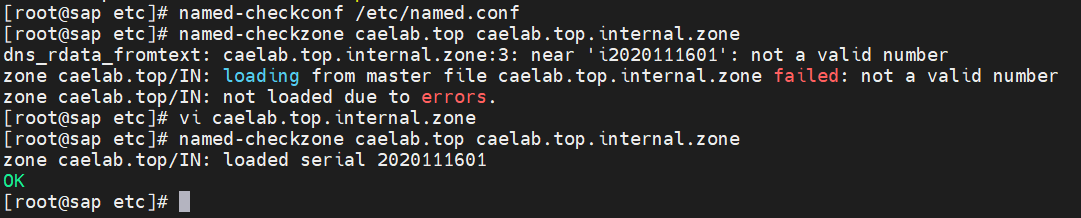
};

};

# Tools

## named-checkconf

named-checkconf /etc/named.conf

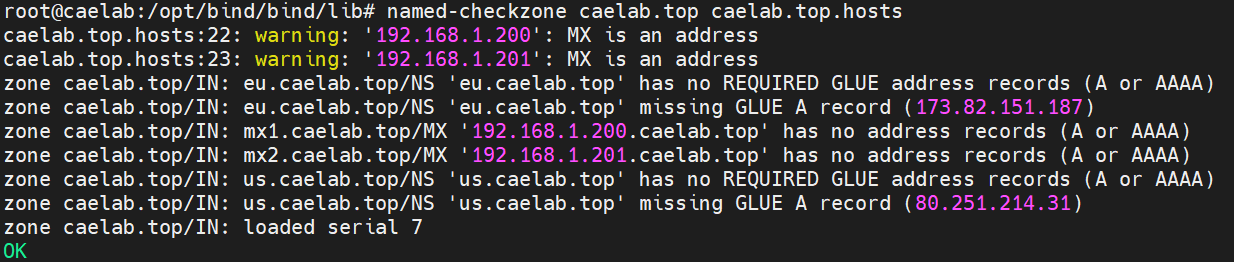


Once syntax is checked then rerun the command should be valid config file



## named-checkzone

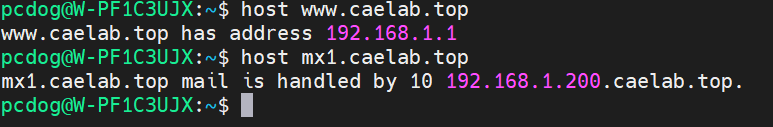
named-checkzone www.caelab.top caelab.top.internal.zone

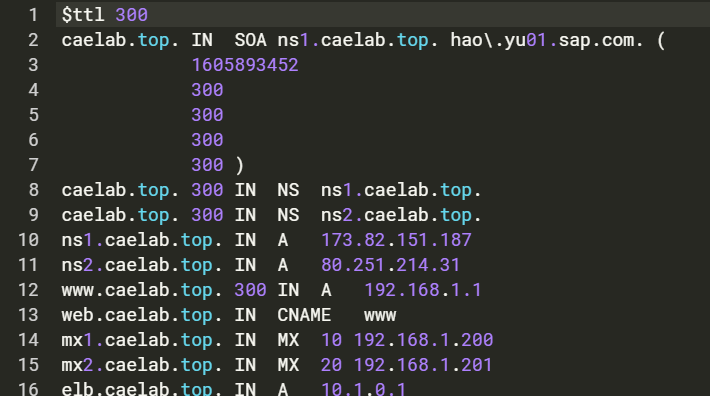


## Nslookup

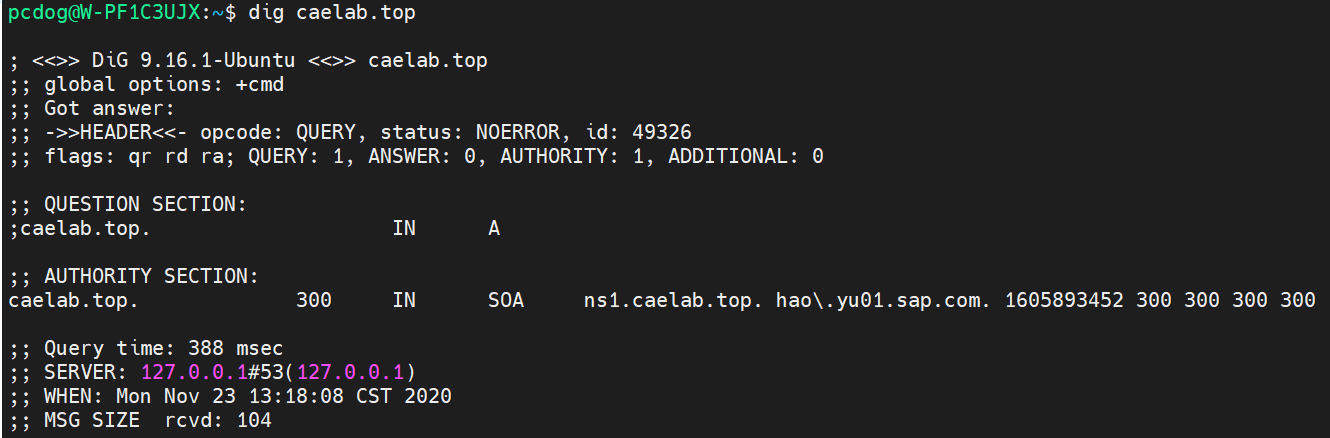


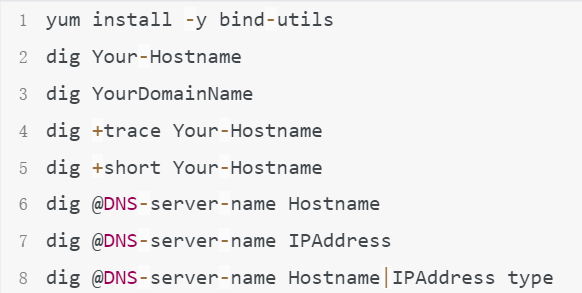
## Host





## Dig





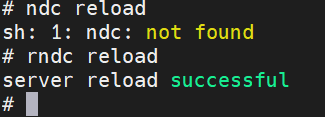
## NDC (bind8) / RNDC (bind9)

apply zone or setting

NDC command failed :

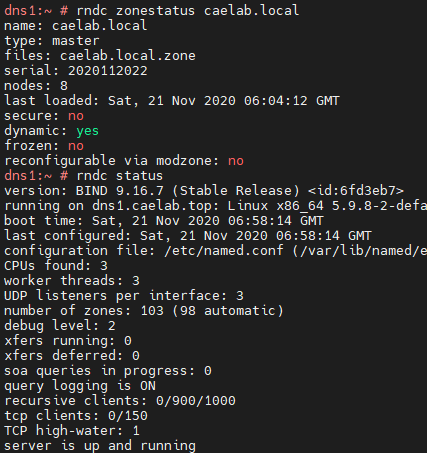
rndc: 'reload' failed: bad zone

#rndc reload

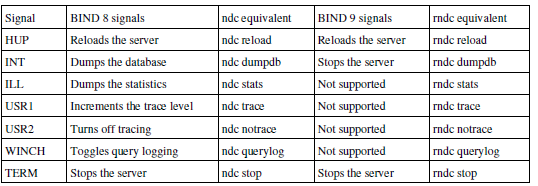


#rndc status

#rndc zonestatus caelab.local

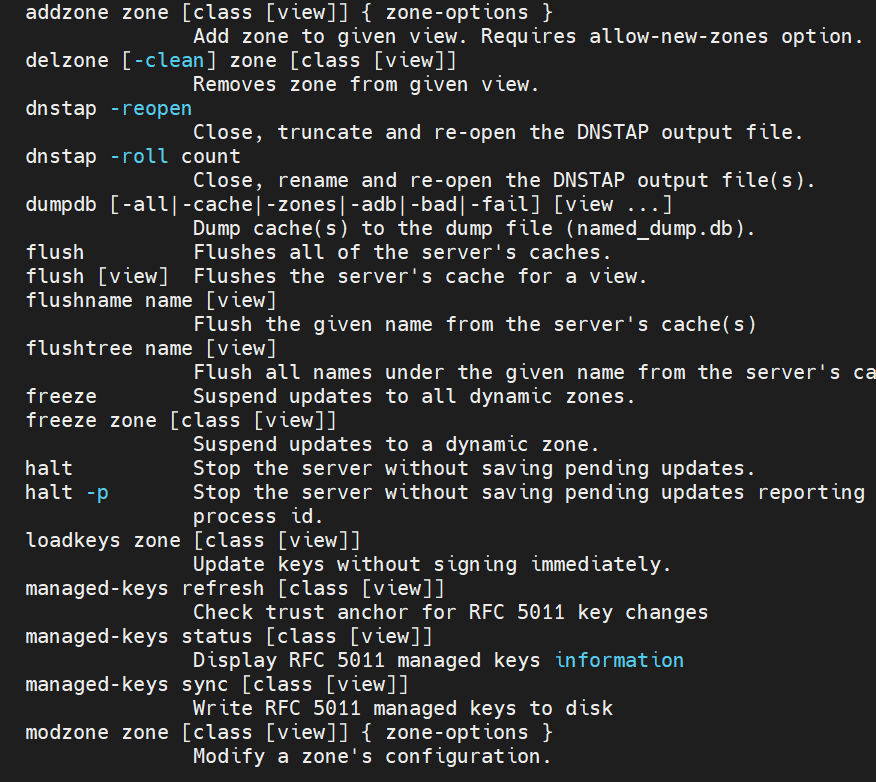


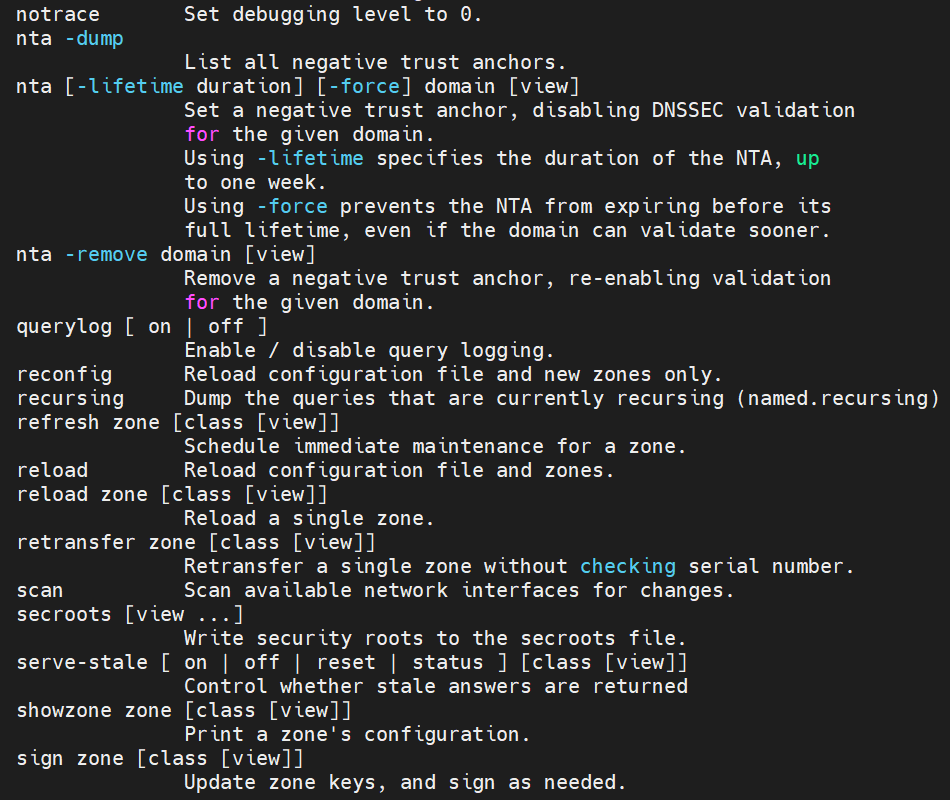
rndc different band8 vs band 9

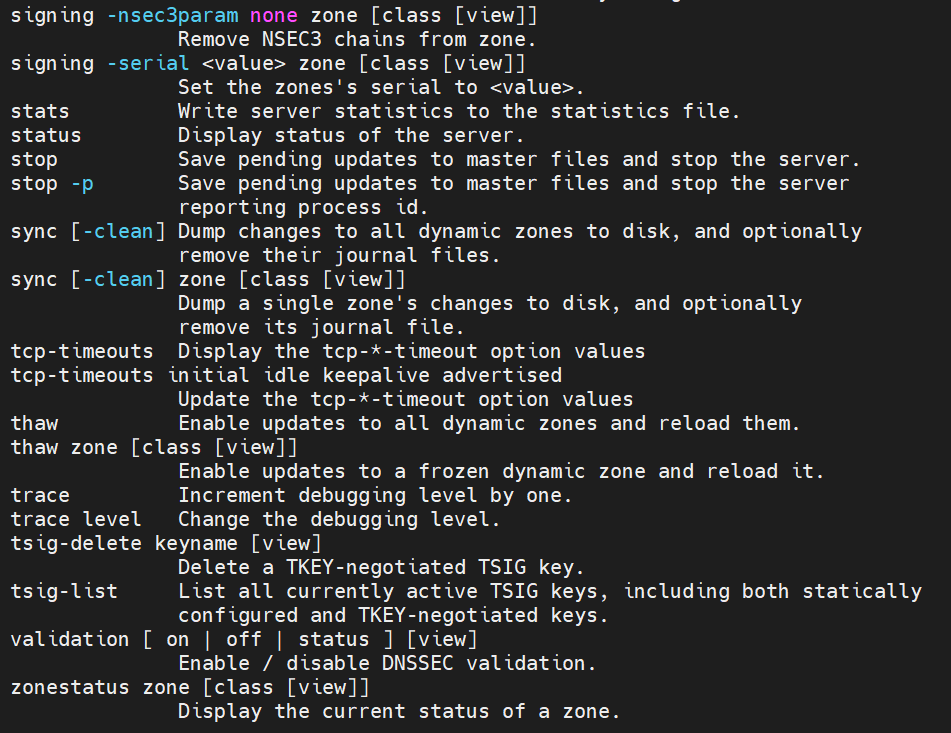


ndc -c 127.0.0.1/953

ttl demo / ttl cache







## nsupdate

# nsupdate

> update add host.caelab.local 300 IN A 192.168.57.3

> send

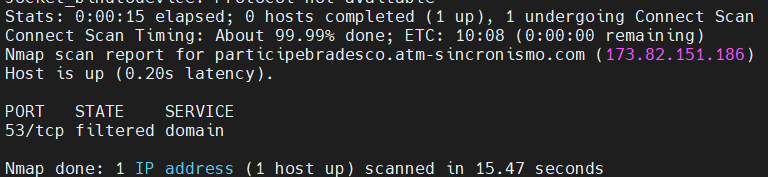
## Nmap

#tcp port check

nmap -p 53 173.82.151.186

#udp port check

nmap -sU -p 53 173.82.151.186



# Path

## Config path

/etc/named.conf #bind主配置文件

/etc/named.iscdlv.key

/etc/named.rfc1912.zones #定义zone的文件

/etc/named.root.key

/etc/portreserve/named

/etc/rc.d/init.d/named #bind脚本文件

/etc/rndc.conf #rndc配置文件

/usr/sbin/rndc #远程dns管理工具

/usr/sbin/rndc-confgen #生成rndc密钥

/var/log/named.log

/var/named

/var/named/data

/var/named/dynamic

/var/named/named.ca #根解析库

/var/named/named.empty

/var/named/named.localhost #本地主机解析库

/var/named/named.loopback

/var/named/slaves #从文件夹

/var/run/named

## Log path

grep daemon /etc/syslog.conf

grep named /var/adm/messages

/var/log/named.log

rcp /etc/named.conf host:/etc

rcp db.cache db.127.0.0 host:db-file-directory