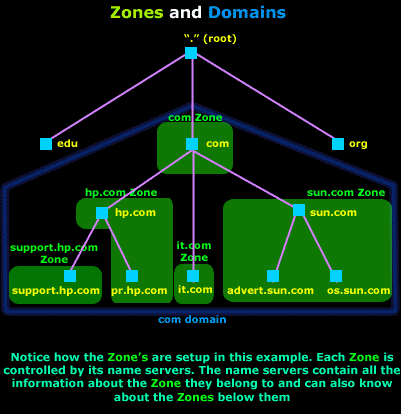
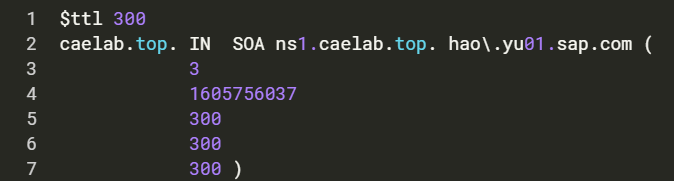
# DNS concept



# 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



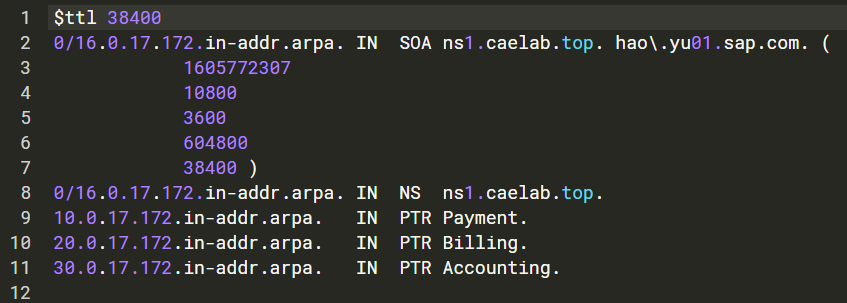
CNAME

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 caelab.top.

WWW. CNAME web.

等同

WWW.caelab.top. CNAME web.caelab.top.

$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

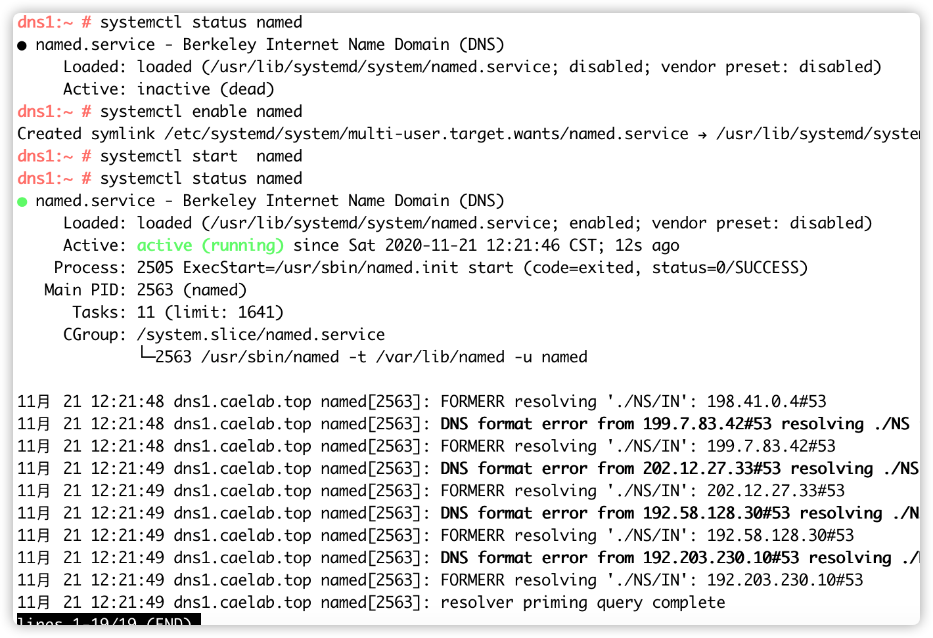
# DNS bind Installation on Linux

#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

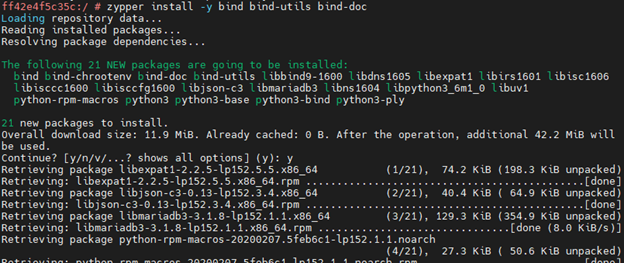
docker exec -it leap /bin/bash

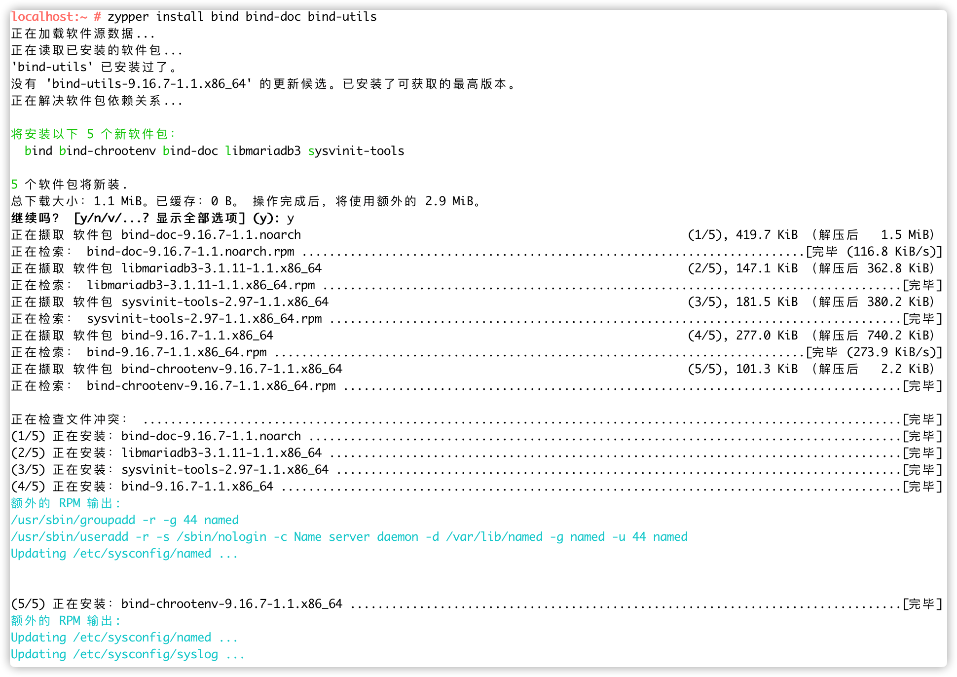
## Install bind in Leap

zypper --gpg-auto-import-keys ref

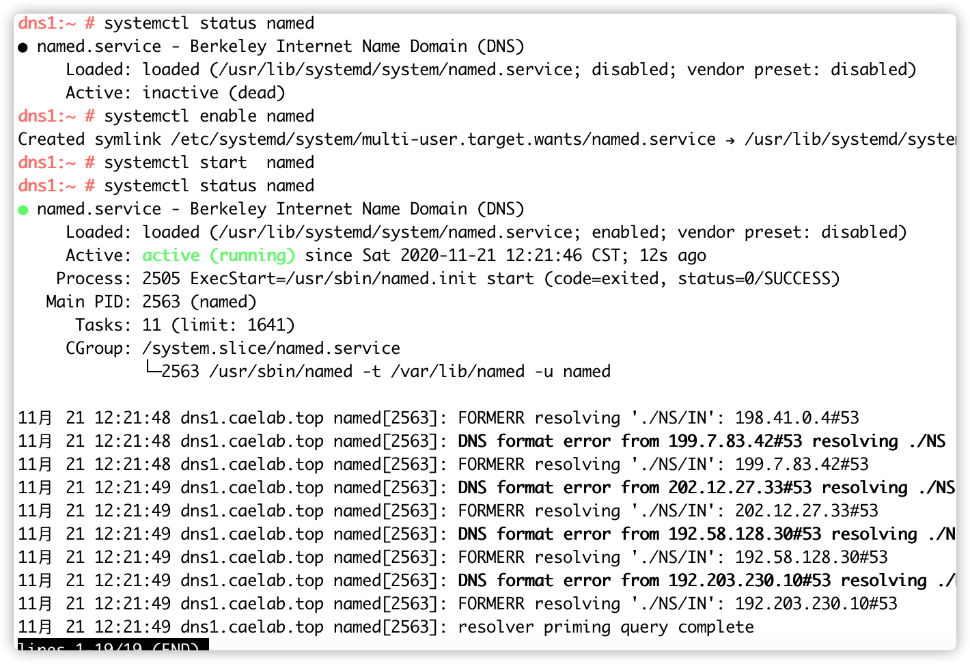
zypper up

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

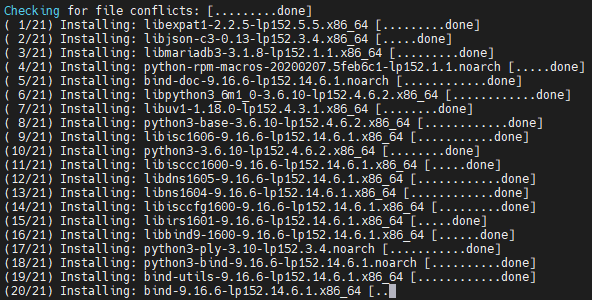
RUN zypper up

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 -d --name=leapdns restart=always \

-p 53:53/tcp -p 53:53/udp -p 953:953/tcp -p 953:953/udp \

-v /opt/lib:/var/lib/bind \

leapdns:latest

# DNS architecture

## Single server config

### Single Cache server

acl sapcorpnets { 192.168.1.0/24; 192.168.2.0/24; };

options {

directory "/etc/namedb";

allow-query { sapcorpnets; };

};

// Provide a reverse mapping for the loopback

// address 127.0.0.1

zone "0.0.127.in-addr.arpa" {

type primary;

file "localhost.rev";

notify no;

};

### Single SOA server

options {

directory "/etc/namedb";

allow-query-cache { none; };

allow-query { any; };

recursion no;

};

zone "0.0.127.in-addr.arpa" {

type primary;

file "localhost.rev";

notify no;

};

zone "caelab.top" {

type primary;

file "caelab.top.zone";

allow-transfer {

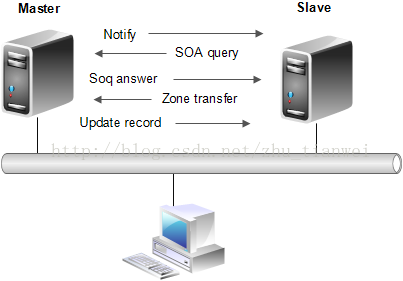
192.168.1.2;

192.168.3.4;

};

};

## 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 )

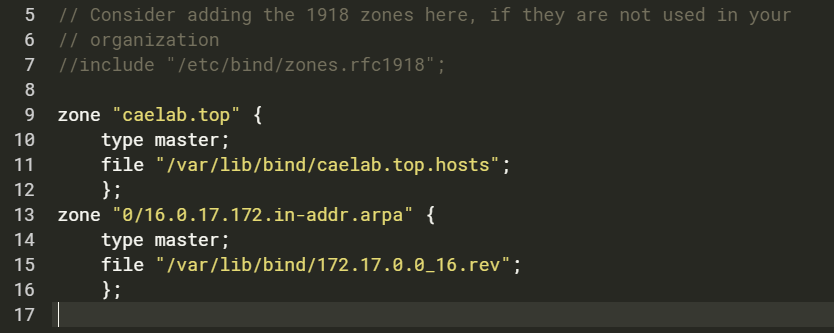
caelab.top. 5M IN NS ns1.caelab.top.

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

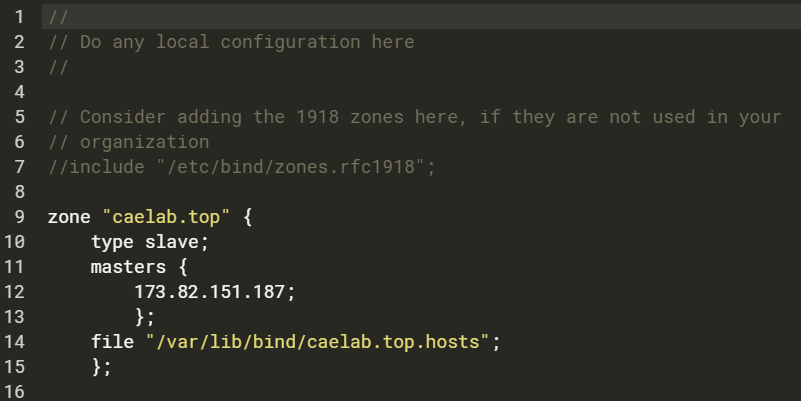
ns1.caelab.top. IN A 173.82.151.187

ns2.caelab.top. IN A 80.251.214.31

zone file



Slave server , set type as slave and sync from master



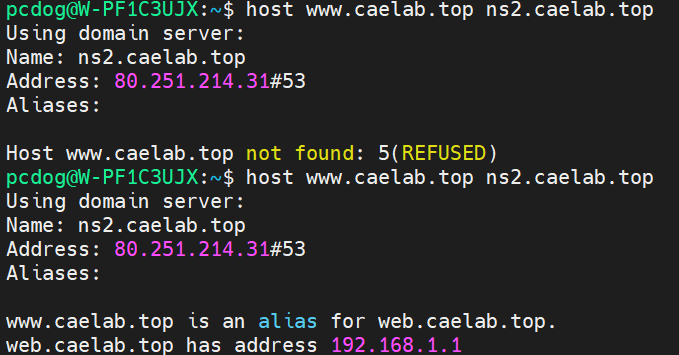
Add 2 record in NS1 Server

web.caelab.top. IN A 192.168.1.1

www.caelab.top. IN CNAME web

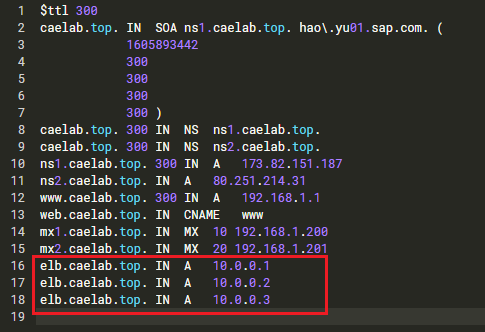
Check the record in NS2 server

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

## Network 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"; };

};

## Chrooted

specifying the -t to running BIND in sandbox, run the daemon as an unprivileged user

/usr/local/sbin/named -u LaoWang -t /var/named

## Dynamic update

Allow-update { localhost;};

## Bogus server

//old server return no correct record

server 192.168.1.38 {

bogus yes;

keys { rndc-key; };

};

## blackhole

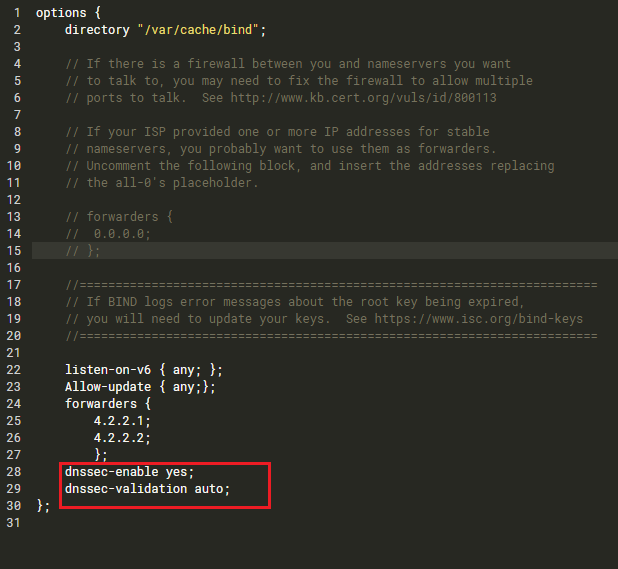
// no respond for this server

blackhole

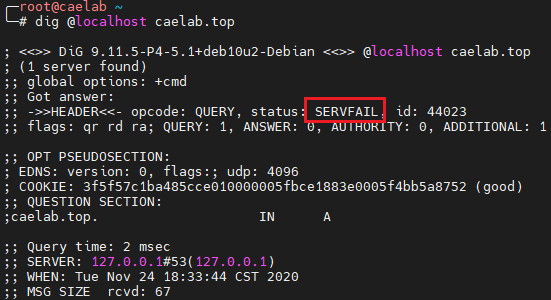
{192.100/16; };

## DNSSEC

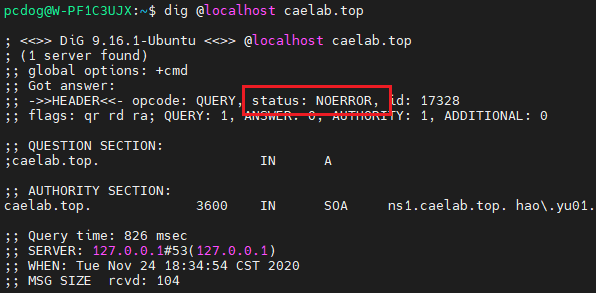
Enable in option



Dig result shows in servfail status



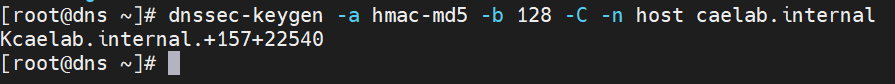
A validated response should have the AD (Authenticated Data) bit flag set and the header will have the status: NOERROR.



## dns sec-keygen utility

create a key in /var/named/keys

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

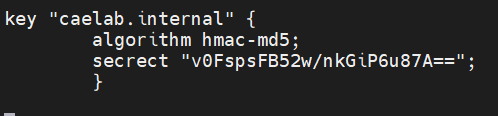




cat Kcaelab.internal.+157+22540.private



Config secret key in option



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;

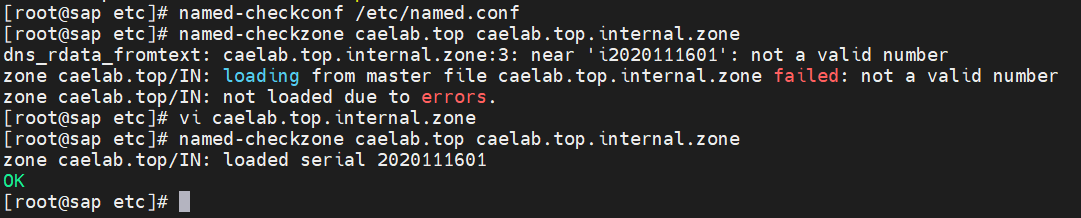
};

};

# Tools

## named-checkconf

named-checkconf /etc/named.conf

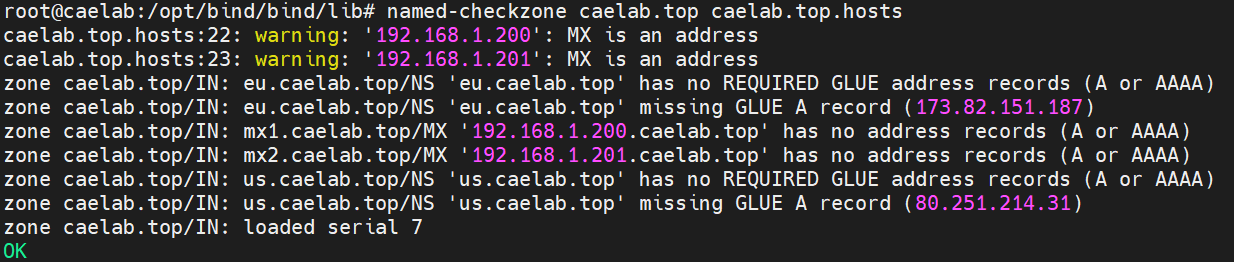


Once syntax is checked then rerun the command should be valid config file



## named-checkzone

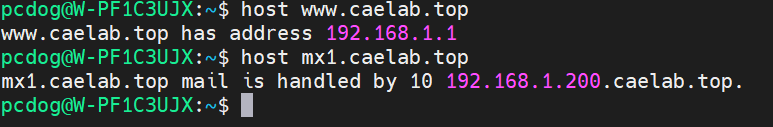
named-checkzone www.caelab.top caelab.top.internal.zone

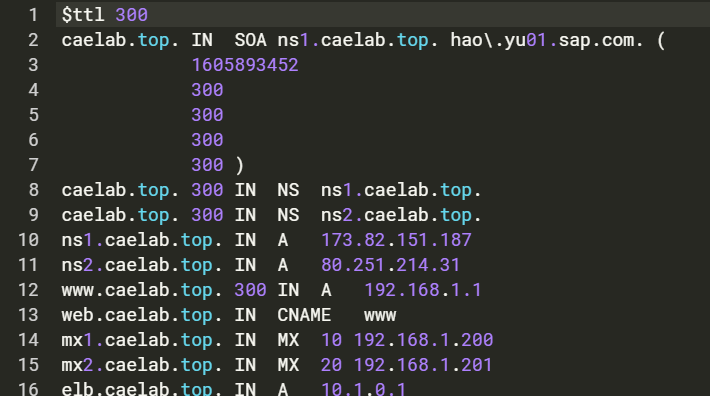


## Nslookup

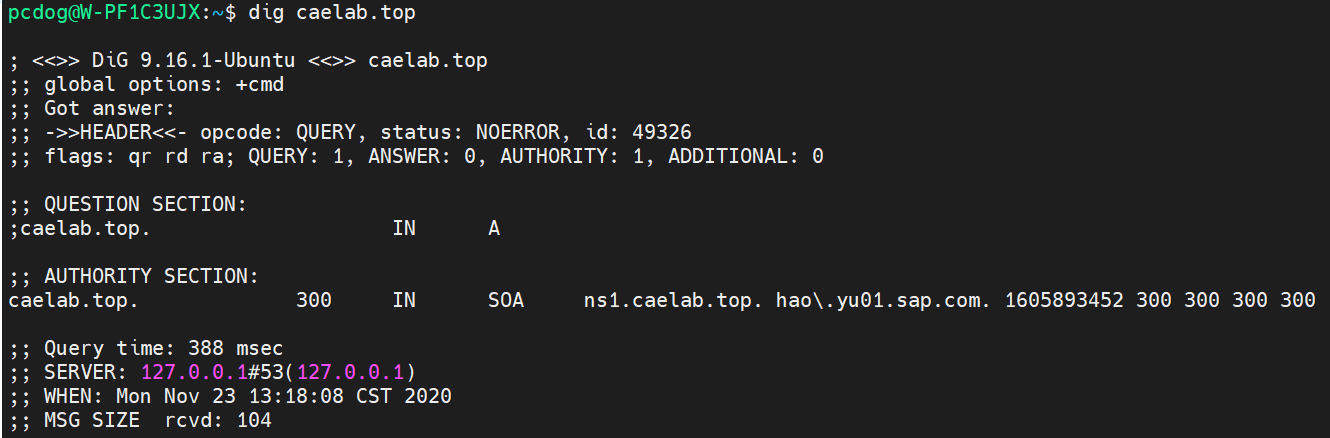


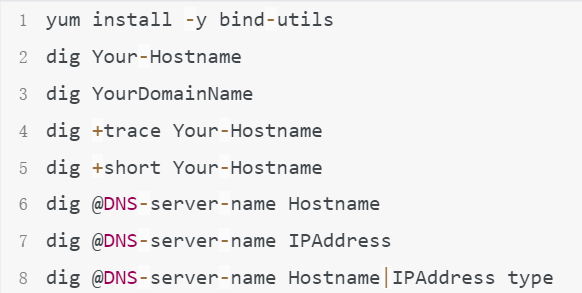
## Host





## Dig





## NDC (bind8) / RNDC (bind9)

### Enable RNDC key

key rndc-key {

algorithm hmac-md5;

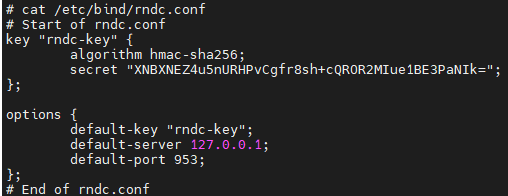
secret "XNBXNEZ4u5nURHPvCgfr8sh+cQROR2MIue1BE3PaNIk=";

};

controls {

inet 127.0.0.1 port 953 allow { 127.0.0.1; } keys { rndc-key; };

};



systemctl restart bind

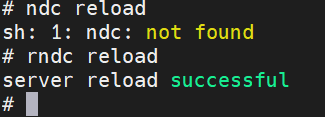
### RNDC command

apply zone or setting

NDC command failed :

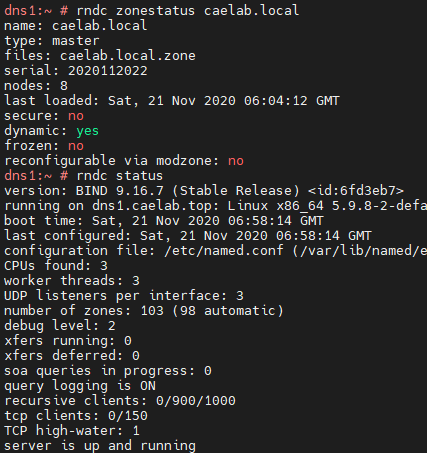
rndc: 'reload' failed: bad zone

#rndc reload

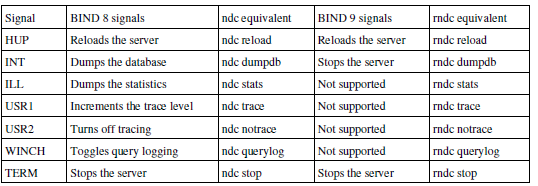


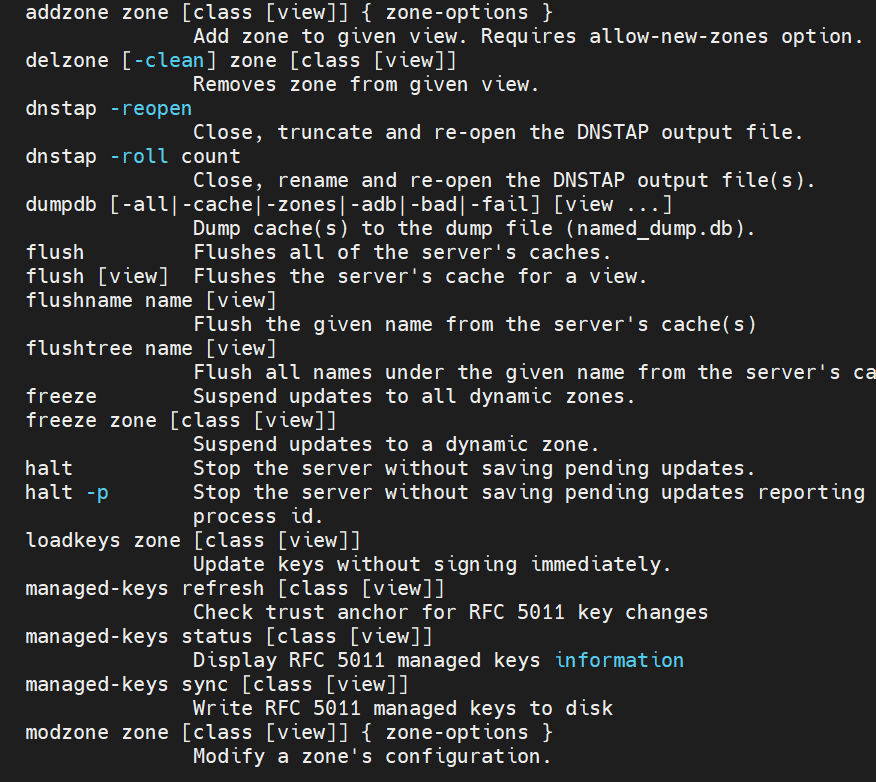
#rndc status

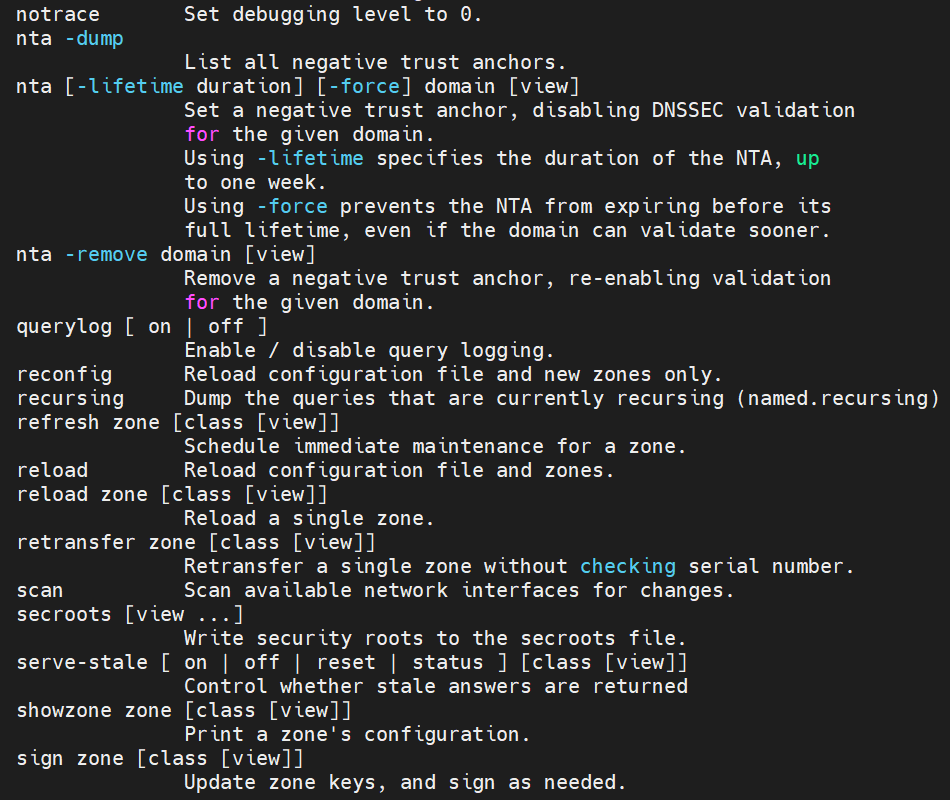
#rndc zonestatus caelab.local

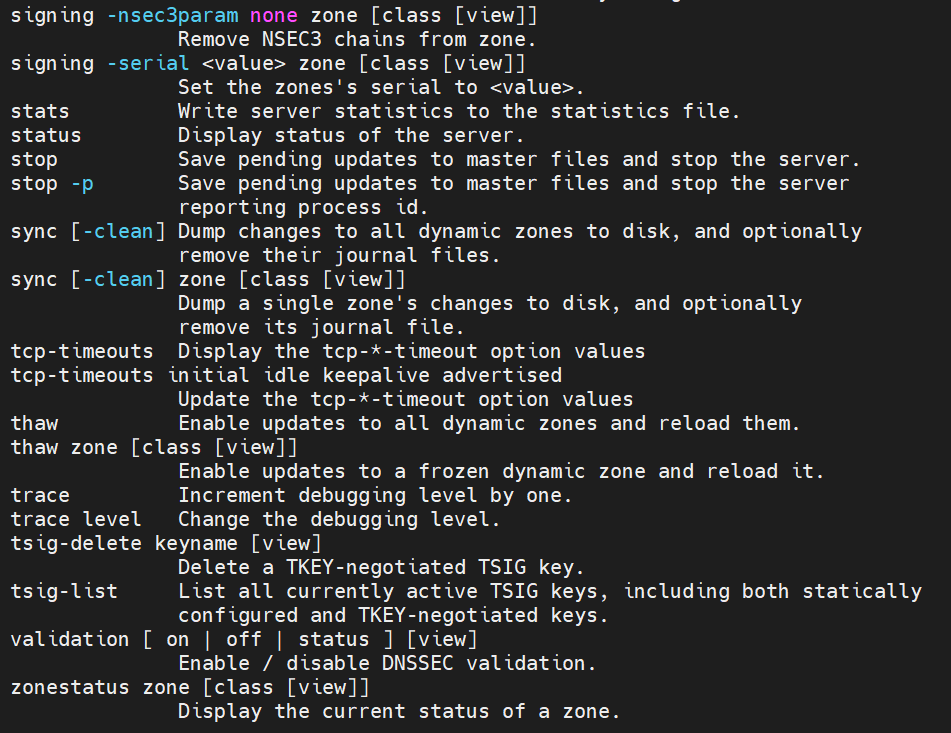


rndc different band8 vs band 9



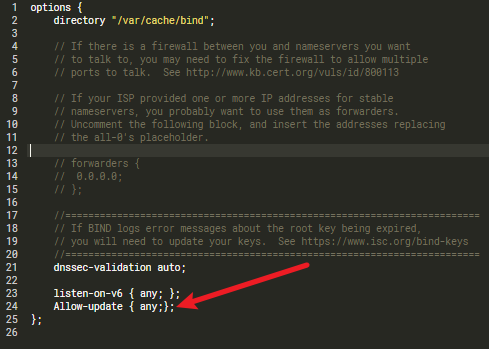






## nsupdate

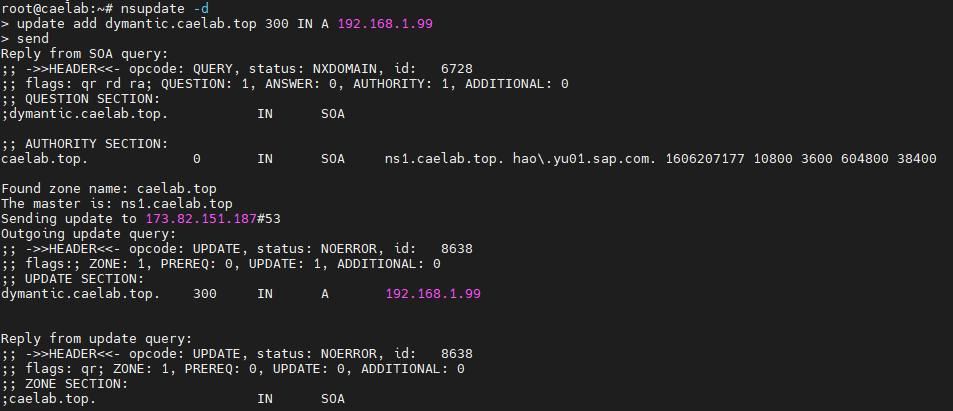
enable allow-update from anywhere

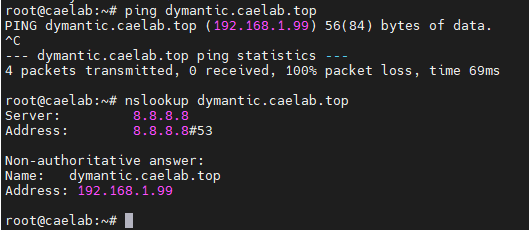


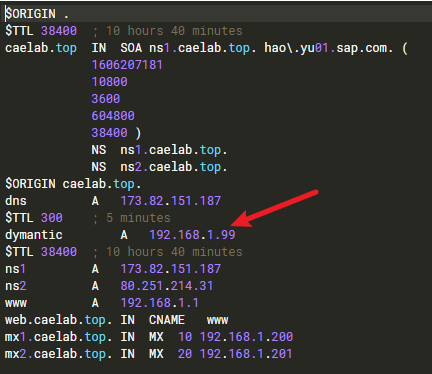
# nsupdate

> update add host.caelab.top 300 IN A 192.168.1.99

> send







Update dynamic record data flow

#write journal file

rndc stop

#disable dynamic update

rndc freeze zone

#reload changes and re-enable dynamic update

rndc thaw zone

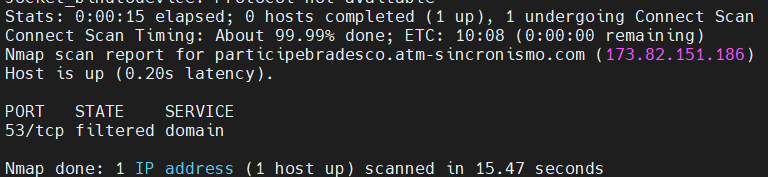
## Nmap

#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/lib/named

/var/lib/named/data

/var/lib/named/dynamic

/var/lib/named/named.ca #根解析库

/var/lib/named/named.empty

/var/lib/named/named.localhost #本地主机解析库

/var/lib/named/named.loopback

/var/lib/named/slaves #从文件夹

/var/run/named

/var/lib/named/dyn #managed key directory

/var/log/named\_dump.db #dump file

/var/log/named.stats #statistis file

/var/log/named\_querylog #client query log

## Log path

Dump file /var/log/named\_dump.db

Status file /var/log/named.stats

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

# Option parameter list

allow-new-zones <boolean>;

allow-notify { <address\_match\_element>; ... };

allow-query { <address\_match\_element>; ... };

allow-query-cache { <address\_match\_element>; ... };

allow-query-cache-on { <address\_match\_element>; ... };

allow-query-on { <address\_match\_element>; ... };

allow-recursion { <address\_match\_element>; ... };

allow-recursion-on { <address\_match\_element>; ... };

allow-transfer { <address\_match\_element>; ... };

allow-update { <address\_match\_element>; ... };

allow-update-forwarding { <address\_match\_element>; ... };

also-notify [ port <integer> ] [ dscp <integer> ] { ( <primaries> |

<ipv4\_address> [ port <integer> ] | <ipv6\_address> [ port

<integer> ] ) [ key <string> ]; ... };

alt-transfer-source ( <ipv4\_address> | \* ) [ port ( <integer> | \* )

] [ dscp <integer> ];

alt-transfer-source-v6 ( <ipv6\_address> | \* ) [ port ( <integer> |

\* ) ] [ dscp <integer> ];

answer-cookie <boolean>;

attach-cache <string>;

auth-nxdomain <boolean>; // default changed

auto-dnssec ( allow | maintain | off );

automatic-interface-scan <boolean>;

avoid-v4-udp-ports { <portrange>; ... };

avoid-v6-udp-ports { <portrange>; ... };

bindkeys-file <quoted\_string>;

blackhole { <address\_match\_element>; ... };

cache-file <quoted\_string>;

catalog-zones { zone <string> [ default-masters [ port <integer> ]

[ dscp <integer> ] { ( <primaries> | <ipv4\_address> [ port

<integer> ] | <ipv6\_address> [ port <integer> ] ) [ key

<string> ]; ... } ] [ zone-directory <quoted\_string> ] [

in-memory <boolean> ] [ min-update-interval <duration> ]; ... };

check-dup-records ( fail | warn | ignore );

check-integrity <boolean>;

check-mx ( fail | warn | ignore );

check-mx-cname ( fail | warn | ignore );

check-names ( primary | master |

secondary | slave | response ) (

fail | warn | ignore );

check-sibling <boolean>;

check-spf ( warn | ignore );

check-srv-cname ( fail | warn | ignore );

check-wildcard <boolean>;

clients-per-query <integer>;

cookie-algorithm ( aes | siphash24 );

cookie-secret <string>;

coresize ( default | unlimited | <sizeval> );

datasize ( default | unlimited | <sizeval> );

deny-answer-addresses { <address\_match\_element>; ... } [

except-from { <string>; ... } ];

deny-answer-aliases { <string>; ... } [ except-from { <string>; ...

} ];

dialup ( notify | notify-passive | passive | refresh | <boolean> );

directory <quoted\_string>;

disable-algorithms <string> { <string>;

... };

disable-ds-digests <string> { <string>;

... };

disable-empty-zone <string>;

dns64 <netprefix> {

break-dnssec <boolean>;

clients { <address\_match\_element>; ... };

exclude { <address\_match\_element>; ... };

mapped { <address\_match\_element>; ... };

recursive-only <boolean>;

suffix <ipv6\_address>;

};

dns64-contact <string>;

dns64-server <string>;

dnskey-sig-validity <integer>;

dnsrps-enable <boolean>;

dnsrps-options { <unspecified-text> };

dnssec-accept-expired <boolean>;

dnssec-dnskey-kskonly <boolean>;

dnssec-loadkeys-interval <integer>;

dnssec-must-be-secure <string> <boolean>;

dnssec-policy <string>;

dnssec-secure-to-insecure <boolean>;

dnssec-update-mode ( maintain | no-resign );

dnssec-validation ( yes | no | auto );

dnstap { ( all | auth | client | forwarder | resolver | update ) [

( query | response ) ]; ... };

dnstap-identity ( <quoted\_string> | none | hostname );

dnstap-output ( file | unix ) <quoted\_string> [ size ( unlimited |

<size> ) ] [ versions ( unlimited | <integer> ) ] [ suffix (

increment | timestamp ) ];

dnstap-version ( <quoted\_string> | none );

dscp <integer>;

dual-stack-servers [ port <integer> ] { ( <quoted\_string> [ port

<integer> ] [ dscp <integer> ] | <ipv4\_address> [ port

<integer> ] [ dscp <integer> ] | <ipv6\_address> [ port

<integer> ] [ dscp <integer> ] ); ... };

dump-file <quoted\_string>;

edns-udp-size <integer>;

empty-contact <string>;

empty-server <string>;

empty-zones-enable <boolean>;

fetch-quota-params <integer> <fixedpoint> <fixedpoint> <fixedpoint>;

fetches-per-server <integer> [ ( drop | fail ) ];

fetches-per-zone <integer> [ ( drop | fail ) ];

files ( default | unlimited | <sizeval> );

flush-zones-on-shutdown <boolean>;

forward ( first | only );

forwarders [ port <integer> ] [ dscp <integer> ] { ( <ipv4\_address>

| <ipv6\_address> ) [ port <integer> ] [ dscp <integer> ]; ... };

fstrm-set-buffer-hint <integer>;

fstrm-set-flush-timeout <integer>;

fstrm-set-input-queue-size <integer>;

fstrm-set-output-notify-threshold <integer>;

fstrm-set-output-queue-model ( mpsc | spsc );

fstrm-set-output-queue-size <integer>;

fstrm-set-reopen-interval <duration>;

geoip-directory ( <quoted\_string> | none );

glue-cache <boolean>; // deprecated

heartbeat-interval <integer>;

hostname ( <quoted\_string> | none );

inline-signing <boolean>;

interface-interval <duration>;

ixfr-from-differences ( primary | master | secondary | slave |

<boolean> );

keep-response-order { <address\_match\_element>; ... };

key-directory <quoted\_string>;

lame-ttl <duration>;

listen-on [ port <integer> ] [ dscp

<integer> ] [ tls <string> ] {

<address\_match\_element>; ... };

listen-on-v6 [ port <integer> ] [ dscp

<integer> ] [ tls <string> ] {

<address\_match\_element>; ... };

lmdb-mapsize <sizeval>;

lock-file ( <quoted\_string> | none );

managed-keys-directory <quoted\_string>;

masterfile-format ( map | raw | text );

masterfile-style ( full | relative );

match-mapped-addresses <boolean>;

max-cache-size ( default | unlimited | <sizeval> | <percentage> );

max-cache-ttl <duration>;

max-clients-per-query <integer>;

max-ixfr-ratio ( unlimited | <percentage> );

max-journal-size ( default | unlimited | <sizeval> );

max-ncache-ttl <duration>;

max-records <integer>;

max-recursion-depth <integer>;

max-recursion-queries <integer>;

max-refresh-time <integer>;

max-retry-time <integer>;

max-rsa-exponent-size <integer>;

max-stale-ttl <duration>;

max-transfer-idle-in <integer>;

max-transfer-idle-out <integer>;

max-transfer-time-in <integer>;

max-transfer-time-out <integer>;

max-udp-size <integer>;

max-zone-ttl ( unlimited | <duration> );

memstatistics <boolean>;

memstatistics-file <quoted\_string>;

message-compression <boolean>;

min-cache-ttl <duration>;

min-ncache-ttl <duration>;

min-refresh-time <integer>;

min-retry-time <integer>;

minimal-any <boolean>;

minimal-responses ( no-auth | no-auth-recursive | <boolean> );

multi-master <boolean>;

new-zones-directory <quoted\_string>;

no-case-compress { <address\_match\_element>; ... };

nocookie-udp-size <integer>;

notify ( explicit | master-only | primary-only | <boolean> );

notify-delay <integer>;

notify-rate <integer>;

notify-source ( <ipv4\_address> | \* ) [ port ( <integer> | \* ) ] [

dscp <integer> ];

notify-source-v6 ( <ipv6\_address> | \* ) [ port ( <integer> | \* ) ]

[ dscp <integer> ];

notify-to-soa <boolean>;

nta-lifetime <duration>;

nta-recheck <duration>;

nxdomain-redirect <string>;

pid-file ( <quoted\_string> | none );

port <integer>;

preferred-glue <string>;

prefetch <integer> [ <integer> ];

provide-ixfr <boolean>;

qname-minimization ( strict | relaxed | disabled | off );

query-source ( ( [ address ] ( <ipv4\_address> | \* ) [ port (

<integer> | \* ) ] ) | ( [ [ address ] ( <ipv4\_address> | \* ) ]

port ( <integer> | \* ) ) ) [ dscp <integer> ];

query-source-v6 ( ( [ address ] ( <ipv6\_address> | \* ) [ port (

<integer> | \* ) ] ) | ( [ [ address ] ( <ipv6\_address> | \* ) ]

port ( <integer> | \* ) ) ) [ dscp <integer> ];

querylog <boolean>;

random-device ( <quoted\_string> | none );

rate-limit {

all-per-second <integer>;

errors-per-second <integer>;

exempt-clients { <address\_match\_element>; ... };

ipv4-prefix-length <integer>;

ipv6-prefix-length <integer>;

log-only <boolean>;

max-table-size <integer>;

min-table-size <integer>;

nodata-per-second <integer>;

nxdomains-per-second <integer>;

qps-scale <integer>;

referrals-per-second <integer>;

responses-per-second <integer>;

slip <integer>;

window <integer>;

};

recursing-file <quoted\_string>;

recursion <boolean>;

recursive-clients <integer>;

request-expire <boolean>;

request-ixfr <boolean>;

request-nsid <boolean>;

require-server-cookie <boolean>;

reserved-sockets <integer>;

resolver-nonbackoff-tries <integer>;

resolver-query-timeout <integer>;

resolver-retry-interval <integer>;

response-padding { <address\_match\_element>; ... } block-size

<integer>;

response-policy { zone <string> [ add-soa <boolean> ] [ log

<boolean> ] [ max-policy-ttl <duration> ] [ min-update-interval

<duration> ] [ policy ( cname | disabled | drop | given | no-op

| nodata | nxdomain | passthru | tcp-only <quoted\_string> ) ] [

recursive-only <boolean> ] [ nsip-enable <boolean> ] [

nsdname-enable <boolean> ]; ... } [ add-soa <boolean> ] [

break-dnssec <boolean> ] [ max-policy-ttl <duration> ] [

min-update-interval <duration> ] [ min-ns-dots <integer> ] [

nsip-wait-recurse <boolean> ] [ nsdname-wait-recurse <boolean>

] [ qname-wait-recurse <boolean> ] [ recursive-only <boolean> ]

[ nsip-enable <boolean> ] [ nsdname-enable <boolean> ] [

dnsrps-enable <boolean> ] [ dnsrps-options { <unspecified-text>

} ];

root-delegation-only [ exclude { <string>; ... } ];

root-key-sentinel <boolean>;

rrset-order { [ class <string> ] [ type <string> ] [ name

<quoted\_string> ] <string> <string>; ... };

secroots-file <quoted\_string>;

send-cookie <boolean>;

serial-query-rate <integer>;

serial-update-method ( date | increment | unixtime );

server-id ( <quoted\_string> | none | hostname );

servfail-ttl <duration>;

session-keyalg <string>;

session-keyfile ( <quoted\_string> | none );

session-keyname <string>;

sig-signing-nodes <integer>;

sig-signing-signatures <integer>;

sig-signing-type <integer>;

sig-validity-interval <integer> [ <integer> ];

sortlist { <address\_match\_element>; ... };

stacksize ( default | unlimited | <sizeval> );

stale-answer-enable <boolean>;

stale-answer-ttl <duration>;

stale-cache-enable <boolean>;

stale-refresh-time <duration>;

startup-notify-rate <integer>;

statistics-file <quoted\_string>;

synth-from-dnssec <boolean>;

tcp-advertised-timeout <integer>;

tcp-clients <integer>;

tcp-idle-timeout <integer>;

tcp-initial-timeout <integer>;

tcp-keepalive-timeout <integer>;

tcp-listen-queue <integer>;

tkey-dhkey <quoted\_string> <integer>;

tkey-domain <quoted\_string>;

tkey-gssapi-credential <quoted\_string>;

tkey-gssapi-keytab <quoted\_string>;

tls-port <integer>;

transfer-format ( many-answers | one-answer );

transfer-message-size <integer>;

transfer-source ( <ipv4\_address> | \* ) [ port ( <integer> | \* ) ] [

dscp <integer> ];

transfer-source-v6 ( <ipv6\_address> | \* ) [ port ( <integer> | \* )

] [ dscp <integer> ];

transfers-in <integer>;

transfers-out <integer>;

transfers-per-ns <integer>;

trust-anchor-telemetry <boolean>; // experimental

try-tcp-refresh <boolean>;

update-check-ksk <boolean>;

use-alt-transfer-source <boolean>;

use-v4-udp-ports { <portrange>; ... };

use-v6-udp-ports { <portrange>; ... };

v6-bias <integer>;

validate-except { <string>; ... };

version ( <quoted\_string> | none );

zero-no-soa-ttl <boolean>;

zero-no-soa-ttl-cache <boolean>;

zone-statistics ( full | terse | none | <boolean> );

};