

PART 2 - SCRIPTS AND DETAILS

Heyoooo!

So here are a couple scripts. Yep. A "couple".

I wanted a way to standup a primary DNS server or a quick way to rebuild that server. But I also wanted a way to standup or rebuild a secondary server without a need to edit my single script each time. Plus, I find that when I have to edit scripting like that, I am seriously prone to error and will screw something up. So two build scripts.

At the top of each will be some variables that need defined, that pertain to your setup. I am leaving information filled in for both scripts, in hopes that it gives some insight into what belongs there. I have tested these scripts (with the variables that are in them) and they worked flawless for me.

Couple notes.

- These scripts are set for a internal network using a 10.0.0.0/24 subnet. Please peruse through the scripts ~~and change any 10.0.0.x or 0.0.10 values. Reverse records use IP addresses in reverse (imagine that), so pay attention for that. I didn't get fancy with these scripts, and didn't try to do that work automatically.~~ Nevermind... I got quazi fancy. You should only need to plug your info into the top variables.
- I use a internal domain of "internal". I don't use a tld inside my network, so note that as well. If you have a .local or something make sure you add it in the domain variable.

Like in my initial BIND setup write up, the primary script if left the way it is will build a caching resolver server. If you un-comment the zone information in the internal/named.conf then the script will build a internal DNS server for your network. If you want to run a secondary server, you will need to uncomment the "allow-transfer" in the named.conf file. **Fill in all the variables whether your going to use a secondary or not. I wrote the scripts to be complete for both systems. Once you build your primary DNS server, you can go into the configs and clear out the slave / secondary data and 2nd NS server entry.**

Here is some of my mentality explained in regards to the structure. I compartmentalize my networks into three folders,

- internal - my internal network or networks go in this folder

- secondary - my slave servers (redundant servers) use this folder when syncing with my master server
- external - if I want to host DNS for a actual external facing domain (like a .com .net .org .etc...) and be authoritative for that/those domains, I will configure them in the external folder. Configuration is no different then how my "internal" networks get configured. But the outside world will need to request records for these domains. So they are "external" to my network.

Because there is a potential for a "external" configuration, I have also separated my configurations using "views". You will notice in the root named.conf file that I have "internal" and "external" views configured. Views allow us better control of who has access to what domain information. My setup consists of internal networks and secondary (slave) servers being a part of the "internal view" and any outside facing domain names or authoritative configurations being part of the "external view". Each "view" can have a completely different set of configurations and allows or denies (such as ACL definitions). The "external view" holds the "external" folder, and its configs. The external view could also have its own "secondary" (slave) folder and configurations as well (the folder would need a different name obviously, like maybe "secondary-ext"). But, running secondary for external domains is going to be out of scope for these scripts. The idea is the same as the internal setup though. I just didn't include the buildout for it.

If your looking to do some authoritative / external domain record hosting, you should read up and treat your configurations and those servers just like you would a internet facing firewall. It will require a bit more thought and care.

OK. :)

Here are the scripts. The "master / primary" script has everything in it, but the internal domain "allow-transfer" is commented out along with the secondary and external configs. It is populated with the provided variables, so if you want to use them, just uncomment the relevant sections. The "slave / secondary" script is exactly like the primary script, except the variables have been adjusted for the second server, and nothing is commented out. No need to disable parts of this one if your going to build a slave system. I did pull out the examples for external. If you're going to use that, just grab that section from the primary script.

I hope these save you a boat load of time and/or help you understand the BIND setup just a bit better.

MASTER / PRIMARY

```
#!/bin/bash
#
# BUILD INTERNAL PRIMARY / MASTER DNS SERVER
#
```

```
#####  
#####  
# SETUP VARIABLES  
  
# current bind download  
BG="https://downloads.isc.org/isc/bind9/9.18.17/bind-9.18.17.tar.xz"  
  
# you can plug in more or remove NS records from the include/include.ns file  
# server ip  
SRV="10.0.0.2"  
# secondary server ip  
SLV="10.0.0.3"  
# network subnet  
SUB="10.0.0.0/24"  
  
# server name  
SRN="ns1"  
# secondary server name  
SLN="ns2"  
# internal domain  
DMN="internal"  
  
# use whoever your email hoster is or if you run mail servers... then you know what goes here  
# you can plug in more or remove MX records from the include/include.mx file  
# mail server (mx 1)  
MXO="alt1.gmail-smtp-in.l.google.com"  
# mail server (mx 2)  
MXT="alt2.gmail-smtp-in.l.google.com"  
  
#####  
#####  
  
DS=$(date "+%Y%m%d"); # DATE STAMP  
PIN=`echo $SRV | cut -d . -f 4`  
SIN=`echo $SLV | cut -d . -f 4`  
NIN=`echo $SUB | cut -d "." -f1-3`  
set `echo "$SUB" | sed 's/\./ /g`  
REV=$3.$2.$1
```

```
adduser named -r -u 25 -U -M -s /sbin/nologin -d /opt/named -c "BIND9"
```

```
mkdir /opt/named &&
```

```
cd /opt/named &&
```

```
mkdir -p dev etc/namedb var/{run,data} &&
```

```
mkdir -p /opt/named/etc/namedb/{include,internal,external,secondary,log} &&
```

```
mkdir -p /opt/named/etc/policy &&
```

```
mknod /opt/named/dev/null c 1 3 &&
```

```
mknod /opt/named/dev/random c 1 8 &&
```

```
chmod 666 /opt/named/dev/{null,random} &&
```

```
cp /etc/localtime /opt/named/etc &&
```

```
chown -R named.named /opt/named
```

```
cp /usr/share/crypto-policies/DEFAULT/bind.txt /opt/named/etc/policy
```

```
cd /opt/named/etc/policy
```

```
ln -s bind.txt bind.config
```

```
dnf -y install gcc libgcc glibc-devel jemalloc jemalloc-devel \
```

```
json-c-devel keyutils-libs-devel krb5-devel libcap-devel \
```

```
libcom_err-devel libedit-devel libidn2-devel libmaxminddb \
```

```
libnghttp2-devel libselenium-devel libsepol-devel libuv-devel \
```

```
libverto-devel libxcrypt-devel libxml2-devel lmdb-devel \
```

```
ncurses-devel openssl-devel pcre2-devel pcre-devel \
```

```
readline-devel xz-devel zlib-devel libmaxminddb-devel
```

```
cd /opt
```

```
wget ${BG}
```

```
gtar -xf bind-*
```

```
BDIR=$(find . -maxdepth 1 -type d -name 'bind*' -exec basename {} ./ ';')
```

```
cd /opt/$BDIR
```

```
./configure \
```

```
    --with-libidn2 \
```

```
    --with-libxml2 \
```

```
    --with-json-c \
```

```
    --with-lmdb \
```

```
    --enable-geoip \
```

```
    --with-maxminddb \
```

```
--with-openssl \  
--disable-static \  
--prefix=/usr \  
--sysconfdir=/etc \  
--localstatedir=/var \  
--enable-full-report
```

```
make &&
```

```
make install
```

```
rndc-confgen -a -b 512
```

```
RKF=$(cat /etc/rndc.key)
```

```
cat > /opt/named/etc/named.conf << EOF
```

```
# BIND CUSTOM CONFIG
```

```
acl "lan-net" { ${SUB}; };
```

```
options {
```

```
    directory          "/etc/namedb";  
    dump-file           "/var/data/named.db";    /* rndc dumpdb */  
    statistics-file     "/var/data/named.stats"; /* rndc stats */  
    memstatistics-file   "/var/data/mem.stats";   /* writes on exit */  
    secroots-file       "/var/data/named.secroots"; /* rndc secroots */  
    recursing-file      "/var/data/named.recursing"; /* rndc recursing */  
    pid-file            "/var/run/named.pid";  
    version             "[secured]";
```

```
listen-on port 53      { 127.0.0.1; ${SRV}; };
```

```
listen-on-v6           { none; };
```

```
#forwarders            { 9.9.9.9; 1.1.1.1; };
```

```
allow-query            { 127.0.0.1; lan-net; };
```

```
#querylog              no;
```

```
managed-keys-directory "/key";
```

```
session-keyfile        "/key/session.key";
```

```
dnssec-validation    auto;

#disable-empty-zone  ".";

#include              "/etc/policy/bind.config";

};

/* https://kb.isc.org/docs/aa-00769 */
#statistics-channels {
#   inet 127.0.0.1 port 8080 allow { 127.0.0.1; };
#};

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

${RKF}

logging {

    channel default_debug {
        file "log/named.run";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity dynamic;
    };

    channel my_log {
        file "log/log";
        print-time yes;
        print-category yes;
        print-severity yes;
        severity info;
    };

    channel my_lame {
        file "log/lame";
```

```
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_xfer {
    file "log/xfer";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_query {
    file "log/query";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_dnssec {
    file "log/dnssec";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_ddns {
    file "log/ddns";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_client {
```

```
    file "log/client";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_auth {
    file "log/auth";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
category default      { my_log; default_debug; };
category general      { my_log; default_debug; };
category config       { my_log; default_debug; };
category network      { my_log; default_debug; };
category zoneload     { my_log; default_debug; };
category dispatch     { my_log; default_debug; };

category queries      { my_query; default_debug; };
category query-errors { my_query; default_debug; };

category lame-servers { my_lame; default_debug; };
category edns-disabled { my_lame; default_debug; };

category notify       { my_xfer; default_debug; };
category xfer-in      { my_xfer; default_debug; };
category xfer-out     { my_xfer; default_debug; };

category security     { my_client; default_debug; };
category client       { my_client; default_debug; };

category dnssec       { my_dnssec; default_debug; };

category update       { my_ddns; default_debug; };
category update-security { my_ddns; default_debug; };
```



```
category resolver      { my_auth; default_debug; };
category cname         { my_auth; default_debug; };
category delegation-only { my_auth; default_debug; };
```

```
};
```

```
view "internal" {
    match-clients { localhost; ${SRV}; lan-net; };
    allow-recursion { localhost; ${SRV}; lan-net; };
    allow-transfer { none; };

    include "internal/named.conf";
    include "secondary/named.conf";
};
```

```
view "external" {
    match-clients { any; };
    allow-recursion { none; };

    include "external/named.conf";

};
```

```
EOF
```

```
ln -s /opt/named/etc/named.conf /etc/named.conf
```

```
cd /opt/named/etc/namedb/include
```

```
cat > include.soa << EOF
```

```
;
```

```
; SOA Record
```

```
;
```

```
\$TTL 3h
```

```
; *** THERE ARE DOTS ON THE ENDS OF THESE AND NO @ ON THE EMAIL ADDRESS ***
```

```
@ IN SOA ${SRN}.${DMN}. root.${DMN}. (
```

```
    ${DS}01 ; serial
```

```
    3h      ; refresh
```

```
1h      ; retry
1w      ; expire
1h )    ; minimum
```

EOF

```
cat > include.ns << EOF
```

```
;  
; Name Server Record  
;
```

```
@      IN      NS      ${SRN}.${DMN}.  
@      IN      NS      ${SLN}.${DMN}.
```

EOF

```
cat > include.mx << EOF
```

```
;  
; MX Record  
;
```

```
@      IN      MX 10   ${MXO}.  
@      IN      MX 20   ${MXT}.
```

EOF

```
cd /opt/named/etc/namedb/internal
```

```
cat > db.localhost << "EOF"
```

```
;  
; LOCALHOST FORWARD ZONE  
;
```

```
$include "include/include.soa"  
$include "include/include.ns"
```

```
localhost.      IN      A      127.0.0.1
```

EOF

```
cat > db.127.0.0 << "EOF"
```

```
;
```

```
; LOCALHOST REVERSE ZONE
```

```
;
```

```
$include "include/include.soa"
```

```
$include "include/include.ns"
```

```
1      IN      PTR      localhost.
```

```
EOF
```

```
cat > db.${DMN} << EOF
```

```
; -----> ${DMN} - Internal Forward Zone<-----
```

```
\$include "include/include.soa"
```

```
\$include "include/include.ns"
```

```
\$include "include/include.mx"
```

```
;
```

```
; INTERNAL SYSTEMS
```

```
; Host Addresses and Canonical Names
```

```
;
```

```
;@      IN      A      ${SRV}
```

```
;www     IN      CNAME    @
```

```
;ftp     IN      CNAME    @
```

```
${SRN}      A      ${SRV}
```

```
${SLN}      A      ${SLV}
```

```
EOF
```

```
cat > db.${NIN} << EOF
```

```
; -----> ${DMN} - Internal Reverse Zone <-----
```

```
\$include "include/include.soa"
```

```
\$include "include/include.ns"
```

```
; INTERNAL SYSTEMS
```

```
; Reverse Pointer Records // note the ending dots
```

```
${PIN}      IN      PTR      ${SRN}.${DMN}.
```

```
${SIN}      IN      PTR      ${SLN}.${DMN}.
```

```
EOF
```

```
cat > named.conf << EOF
```

```
zone "." {
```

```
    type hint;
```

```
    file "internal/db.roots";
```

```
};
```

```
zone "localhost" {
```

```
    type master;
```

```
    file "internal/db.localhost";
```

```
    notify no;
```

```
};
```

```
zone "0.0.127.in-addr.arpa" {
```

```
    type master;
```

```
    file "internal/db.127.0.0";
```

```
    notify no;
```

```
};
```

```
// zone "${DMN}" {
```

```
//     type master;
```

```
//     file "internal/db.${DMN}";
```

```
//     allow-update { key "rndc-key"; };
```

```
//     //allow-transfer { ${SLV}; };
```

```
//     notify yes;
```

```
// };
```

```
// zone "${REV}.in-addr.arpa." {
```

```
//     type master;
```

```
// file "internal/db.${NIN}";
// allow-update { key "rndc-key"; };
// //allow-transfer { ${SLV}; };
// notify yes;
// };
```

EOF

cd /opt/named/etc/namedb/secondary

cat > named.conf << EOF

// SECONDARY ZONE FILE

```
//zone "${DMN}" {
//     type slave;
//     masters { ${SRV}; };
//     file "secondary/db.${DMN}";
//};
```

```
//zone "${REV}.in-addr.arpa." {
//     type slave;
//     masters { ${SRV}; };
//     file "secondary/db.${NIN}";
//};
```

EOF

cd /opt/named/etc/namedb/external

cat > named.conf << "EOF"

// EXTERNAL FORWARD ZONES

```
//zone "example.com" {
//     type master;
//     file "external/db.example.com";
//     notify no;
//};
```

// EXTERNAL REVERSE ZONES

```
//zone "33.22.11.in-addr.arpa." {
```

```
// type master;
// file "external/db.11.22.33";
// notify no;
//};
```

EOF

```
cat > db.example.com << "EOF"
; -----> example.com - External Forward Zone <-----
```

```
$include "include/include.soa"
$include "include/include.ns"
$include "include/include.mx"
```

```
;
; Host Addresses and Canonical Names
;
```

```
@      IN      A      11.22.33.44
www     IN      CNAME   @
ftp     IN      CNAME   @
```

EOF

```
cat > db.11.22.33 << "EOF"
; -----> example.com - External Reverse Zone <-----
```

```
$include "include/include.soa"
$include "include/include.ns"
```

```
44      IN      PTR     example.com.
```

EOF

```
cat > /usr/lib/systemd/system/named.service << "EOF"
[Unit]
Description=Berkeley Internet Name Domain (DNS)
Wants=nss-lookup.target
Before=nss-lookup.target
```

After=network.target

[Service]

Type=forking

Environment=NAMEDCONF=/etc/named.conf

EnvironmentFile=/etc/sysconfig/named

ExecStart=/usr/sbin/named -u named -t /opt/named -c \${NAMEDCONF} \$OPTIONS

ExecReload=/usr/sbin/rndc null > /dev/null 2>&1; then /usr/sbin/rndc reload

ExecStop=/usr/sbin/rndc stop > /dev/null 2>&1

PrivateTmp=true

[Install]

WantedBy=multi-user.target

EOF

cat > /etc/sysconfig/named << "EOF"

BIND named process options

~~~~~

#

OPTIONS="whatever" -- These additional options will be passed to named

at startup. Don't add -t here, enable proper

-chroot.service unit file.

#

NAMEDCONF=/etc/named/alternate.conf

-- Don't use -c to change configuration file.

Extend systemd named.service instead or use this

variable.

#

DISABLE_ZONE_CHECKING -- By default, service file calls named-checkzone

utility for every zone to ensure all zones are

valid before named starts. If you set this option

to 'yes' then service file doesn't perform those

checks.

ONLY USE IPV4

OPTIONS="-4"

EOF

```
cat > /opt/named/etc/namedb/roots << "EOF"
```

```
#!/bin/bash
```

```
# TRY DIG IF WGET FAILS
```

```
# dig @a.root-servers.net . ns > /opt/named/etc/namedb/internal/db.roots
```

```
wget --user=ftp --password=ftp ftp://ftp.internic.net/domain/named.cache -O  
/opt/named/etc/namedb/internal/db.roots
```

```
chown named.named /opt/named/etc/namedb/internal/db.roots
```

```
exit
```

EOF

```
cat > /opt/named/etc/namedb/reload << "EOF"
```

```
#!/bin/bash
```

```
#
```

```
# SCRIPT TO CLEAR LOGS AND RESTART BIND
```

```
# CAN BE USED AFTER MAKING CHANGES. IF
```

```
# YOU DONT WANT TO CLEAR LOGS AFTER CHANGES
```

```
# THE JUST RUN 'rndc reload' FROM THE CLI.
```

```
#
```

```
### WIPE LOGS THEN TOUCH NEW LOG AND DEBUG LOG
```

```
rm -f /opt/named/etc/namedb/log/*
```

```
touch /opt/named/etc/namedb/log/log
```

```
touch /opt/named/etc/namedb/log/named.run
```

```
chown -R named.named /opt/named
```

```
### STOP SERVICE
```

```
systemctl stop named
```

```
sleep 2
```

```
### START SERVICE AND TAIL DEBUG LOG (ctrl+c to quit tail)
```

```
systemctl start named && tail -f /opt/named/etc/namedb/log/named.run
```



```
exit
```

```
EOF
```

```
cd /opt
```

```
rm -fR bind-*
```

```
chmod +x /opt/named/etc/namedb/roots
```

```
chmod +x /opt/named/etc/namedb/reload
```

```
/opt/named/etc/namedb/roots
```

```
chown root:named /etc/rndc.key /etc/named.conf
```

```
chmod 640 /etc/rndc.key /etc/named.conf
```

```
chown -R named:named /opt/named
```

```
systemctl daemon-reload
```

```
systemctl enable named
```

```
cp -a /etc/resolv.conf /etc/resolv.conf.bak
```

```
cat > /etc/resolv.conf << "EOF"
```

```
nameserver 127.0.0.1
```

```
nameserver 1.1.1.1
```

```
#search internal
```

```
EOF
```

```
printf "\n\n START SERVICE AFTER VALIDATING INSTALL OR MAKING MODIFICATIONS \n\n"
```

```
exit
```

SLAVE / SECONDARY

```
#!/bin/bash
```

```
#
```

```
# BUILD INTERNAL SECONDARY / SLAVE DNS SERVER
```

```
#
```

```
#####
```

```
#####
```

```
# SETUP VARIABLES
```

```
# current bind download
```

```
BG="https://downloads.isc.org/isc/bind9/9.18.17/bind-9.18.17.tar.xz"
```

```
# you can plug in more or remove NS records from the include/include.ns file
```

```
# server ip
```

```
SRV="10.0.0.2"
```

```
# secondary server ip
```

```
SLV="10.0.0.3"
```

```
# network subnet
```

```
SUB="10.0.0.0/24"
```

```
# server name
```

```
SRN="ns1"
```

```
# secondary server name
```

```
SLN="ns2"
```

```
# internal domain
```

```
DMN="internal"
```

```
# use whoever your email hoster is or if you run mail servers... then you know what goes here
```

```
# you can plug in more or remove MX records from the include/include.mx file
```

```
# mail server (mx 1)
```

```
MXO="alt1.gmail-smtp-in.l.google.com"
```

```
# mail server (mx 2)
```

```
MXT="alt2.gmail-smtp-in.l.google.com"
```

```
#####  
#####
```

```
DS=$(date "+%Y%m%d"); # DATE STAMP
```

```
PIN=`echo $SRV | cut -d . -f 4`
```

```
SIN=`echo $SLV | cut -d . -f 4`
```

```
NIN=`echo $SUB | cut -d "." -f1-3`
```

```
set `echo "$SUB" | sed 's/\./ /g`
```

```
REV=$3.$2.$1
```

```
adduser named -r -u 25 -U -M -s /sbin/nologin -d /opt/named -c "BIND9"
```

```
mkdir /opt/named &&
cd /opt/named &&
mkdir -p dev etc/namedb var/{run,data} &&
mkdir -p /opt/named/etc/namedb/{include,internal,external,secondary,log} &&
mkdir -p /opt/named/etc/policy &&
mknod /opt/named/dev/null c 1 3 &&
mknod /opt/named/dev/random c 1 8 &&
chmod 666 /opt/named/dev/{null,random} &&
cp /etc/localtime /opt/named/etc &&
chown -R named.named /opt/named
```

```
cp /usr/share/crypto-policies/DEFAULT/bind.txt /opt/named/etc/policy
cd /opt/named/etc/policy
ln -s bind.txt bind.config
```

```
dnf -y install gcc libgcc glibc-devel jemalloc jemalloc-devel \
json-c-devel keyutils-libs-devel krb5-devel libcap-devel \
libcom_err-devel libedit-devel libidn2-devel libmaxminddb \
libnghttp2-devel libsasl-devel libsepol-devel libuv-devel \
libverto-devel libxcrypt-devel libxml2-devel lmdb-devel \
ncurses-devel openssl-devel pcre2-devel pcre-devel \
readline-devel xz-devel zlib-devel libmaxminddb-devel
```

```
cd /opt
wget ${BG}
gtar -xf bind-*
BDIR=$(find . -maxdepth 1 -type d -name 'bind*' -exec basename {} ./ ';' )
```

```
cd /opt/$BDIR
./configure \
    --with-libidn2 \
    --with-libxml2 \
    --with-json-c \
    --with-lmdb \
    --enable-geoip \
    --with-maxminddb \
    --with-openssl \
    --disable-static \
```

```
--prefix=/usr \  
--sysconfdir=/etc \  
--localstatedir=/var \  
--enable-full-report
```

```
make &&  
make install
```

```
rndc-confgen -a -b 512  
RKF=$(cat /etc/rndc.key)
```

```
cat > /opt/named/etc/named.conf << EOF  
# BIND CUSTOM CONFIG
```

```
acl "lan-net" { ${SUB}; };
```

```
options {
```

```
    directory          "/etc/namedb";  
    dump-file          "/var/data/named.db";    /* rndc dumpdb */  
    statistics-file    "/var/data/named.stats"; /* rndc stats */  
    memstatistics-file  "/var/data/mem.stats";   /* writes on exit */  
    secroots-file      "/var/data/named.secroots"; /* rndc secroots */  
    recursing-file     "/var/data/named.recurring"; /* rndc recurring */  
    pid-file           "/var/run/named.pid";  
    version            "[secured]";
```

```
listen-on port 53      { 127.0.0.1; ${SLV}; };  
listen-on-v6           { none; };
```

```
#forwarders            { 9.9.9.9; 1.1.1.1; };
```

```
allow-query            { 127.0.0.1; lan-net; };  
#querylog              no;
```

```
managed-keys-directory "/key";  
session-keyfile        "/key/session.key";  
dnssec-validation      auto;
```

```
#disable-empty-zone      ".";
```

```
#include                  "/etc/policy/bind.config";
```

```
};
```

```
/* https://kb.isc.org/docs/aa-00769 */
```

```
#statistics-channels {
```

```
#    inet 127.0.0.1 port 8080 allow { 127.0.0.1; };
```

```
#};
```

```
controls {
```

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

```
};
```

```
${RKF}
```

```
logging {
```

```
    channel default_debug {
```

```
        file "log/named.run";
```

```
        print-time yes;
```

```
        print-category yes;
```

```
        print-severity yes;
```

```
        severity dynamic;
```

```
    };
```

```
    channel my_log {
```

```
        file "log/log";
```

```
        print-time yes;
```

```
        print-category yes;
```

```
        print-severity yes;
```

```
        severity info;
```

```
    };
```

```
    channel my_lame {
```

```
        file "log/lame";
```

```
        print-time yes;
```

```
        print-category yes;
```

```
    print-severity yes;
    severity info;
};
```

```
channel my_xfer {
    file "log/xfer";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_query {
    file "log/query";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_dnssec {
    file "log/dnssec";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_ddns {
    file "log/ddns";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_client {
    file "log/client";
    print-time yes;
```

```
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
channel my_auth {
    file "log/auth";
    print-time yes;
    print-category yes;
    print-severity yes;
    severity info;
};
```

```
category default      { my_log; default_debug; };
category general      { my_log; default_debug; };
category config       { my_log; default_debug; };
category network      { my_log; default_debug; };
category zoneload     { my_log; default_debug; };
category dispatch     { my_log; default_debug; };
```

```
category queries      { my_query; default_debug; };
category query-errors { my_query; default_debug; };
```

```
category lame-servers { my_lame; default_debug; };
category edns-disabled { my_lame; default_debug; };
```

```
category notify       { my_xfer; default_debug; };
category xfer-in      { my_xfer; default_debug; };
category xfer-out     { my_xfer; default_debug; };
```

```
category security     { my_client; default_debug; };
category client       { my_client; default_debug; };
```

```
category dnssec       { my_dnssec; default_debug; };
```

```
category update       { my_ddns; default_debug; };
category update-security { my_ddns; default_debug; };
```

```
category resolver     { my_auth; default_debug; };
category cname        { my_auth; default_debug; };
```

```
category delegation-only { my_auth; default_debug; };
```

```
};
```

```
view "internal" {
```

```
    match-clients { localhost; ${SLV}; lan-net; };
```

```
    allow-recursion { localhost; ${SLV}; lan-net; };
```

```
    allow-transfer { none; };
```

```
    include "internal/named.conf";
```

```
    include "secondary/named.conf";
```

```
};
```

```
view "external" {
```

```
    match-clients { any; };
```

```
    allow-recursion { none; };
```

```
    include "external/named.conf";
```

```
};
```

```
EOF
```

```
ln -s /opt/named/etc/named.conf /etc/named.conf
```

```
cd /opt/named/etc/namedb/include
```

```
cat > include.soa << EOF
```

```
;
```

```
; SOA Record
```

```
;
```

```
\$TTL 3h
```

```
; *** THERE ARE DOTS ON THE ENDS OF THESE AND NO @ ON THE EMAIL ADDRESS ***
```

```
@      IN      SOA      ${SLN}.${DMN}. root.${DMN}. (
```

```
        ${DS}01  ; serial
```

```
        3h      ; refresh
```

```
        1h      ; retry
```

```
        1w      ; expire
```

```
        1h )    ; minimum
```


EOF

```
cat > include.ns << EOF
```

```
;
```

```
; Name Server Record
```

```
;
```

```
@    IN    NS    ${SLN}.${DMN}.
```

```
@    IN    NS    ${SRN}.${DMN}.
```

EOF

```
cat > include.mx << EOF
```

```
;
```

```
; MX Record
```

```
;
```

```
@    IN    MX 10  ${MXO}.
```

```
@    IN    MX 20  ${MXT}.
```

EOF

```
cd /opt/named/etc/namedb/internal
```

```
cat > db.localhost << "EOF"
```

```
;
```

```
; LOCALHOST FORWARD ZONE
```

```
;
```

```
$include "include/include.soa"
```

```
$include "include/include.ns"
```

```
localhost.    IN    A    127.0.0.1
```

EOF

```
cat > db.127.0.0 << "EOF"
```

```
;
```

```
; LOCALHOST REVERSE ZONE  
;
```

```
$include "include/include.soa"  
$include "include/include.ns"
```

```
1      IN      PTR      localhost.
```

```
EOF
```

```
cat > named.conf << EOF
```

```
zone "." {  
    type hint;  
    file "internal/db.root";  
};
```

```
zone "localhost" {  
    type master;  
    file "internal/db.localhost";  
    notify no;  
};
```

```
zone "0.0.127.in-addr.arpa" {  
    type master;  
    file "internal/db.127.0.0";  
    notify no;  
};
```

```
EOF
```

```
cd /opt/named/etc/namedb/secondary
```

```
cat > named.conf << EOF
```

```
;  
; SECONDARY ZONE FILE  
;
```

```
zone "${DMN}" {  
    type slave;  
    masters { ${SRV}; };
```

```
file "secondary/db.${DMN}";  
};
```

```
zone "${REV}.in-addr.arpa." {  
    type slave;  
    masters { ${SRV}; };  
    file "secondary/db.${NIN}";  
};
```

EOF

```
cd /opt/named/etc/namedb/external  
touch named.conf
```

```
cat > /usr/lib/systemd/system/named.service << "EOF"
```

[Unit]

Description=Berkeley Internet Name Domain (DNS)

Wants=nss-lookup.target

Before=nss-lookup.target

After=network.target

[Service]

Type=forking

Environment=NAMEDCONF=/etc/named.conf

EnvironmentFile=-/etc/sysconfig/named

ExecStart=/usr/sbin/named -u named -t /opt/named -c \${NAMEDCONF} \$OPTIONS

ExecReload=/usr/sbin/rndc null > /dev/null 2>&1; then /usr/sbin/rndc reload

ExecStop=/usr/sbin/rndc stop > /dev/null 2>&1

PrivateTmp=true

[Install]

WantedBy=multi-user.target

EOF

```
cat > /etc/sysconfig/named << "EOF"
```

```
# BIND named process options
```

```
# ~~~~~~  
#  
# OPTIONS="whatever" -- These additional options will be passed to named  
# at startup. Don't add -t here, enable proper  
# -chroot.service unit file.  
#  
# NAMEDCONF=/etc/named/alternate.conf  
# -- Don't use -c to change configuration file.  
# Extend systemd named.service instead or use this  
# variable.  
#  
# DISABLE_ZONE_CHECKING -- By default, service file calls named-checkzone  
# utility for every zone to ensure all zones are  
# valid before named starts. If you set this option  
# to 'yes' then service file doesn't perform those  
# checks.  
  
# ONLY USE IPV4  
OPTIONS="-4"
```

EOF

```
cat > /opt/named/etc/namedb/roots << "EOF"
```

```
#!/bin/bash
```

```
# TRY DIG IF WGET FAILS
```

```
# dig @a.root-servers.net . ns > /opt/named/etc/namedb/internal/db.roots
```

```
wget --user=ftp --password=ftp ftp://ftp.internic.net/domain/named.cache -O  
/opt/named/etc/namedb/internal/db.roots
```

```
chown named.named /opt/named/etc/namedb/internal/db.roots
```

```
exit
```

EOF

```
cat > /opt/named/etc/namedb/reload << "EOF"
```

```
#!/bin/bash
```

```
#
# SCRIPT TO CLEAR LOGS AND RESTART BIND
# CAN BE USED AFTER MAKING CHANGES. IF
# YOU DONT WANT TO CLEAR LOGS AFTER CHANGES
# THE JUST RUN 'rndc reload' FROM THE CLI.
#

### WIPE LOGS THEN TOUCH NEW LOG AND DEBUG LOG
rm -f /opt/named/etc/namedb/log/*
touch /opt/named/etc/namedb/log/log
touch /opt/named/etc/namedb/log/named.run
chown -R named.named /opt/named

### STOP SERVICE
systemctl stop named
sleep 2

### START SERVICE AND TAIL DEBUG LOG (ctrl+c to quit tail)
systemctl start named && tail -f /opt/named/etc/namedb/log/named.run

exit

EOF

cd /opt
rm -fR bind-*

chmod +x /opt/named/etc/namedb/roots
chmod +x /opt/named/etc/namedb/reload
/opt/named/etc/namedb/roots

chown root:named /etc/rndc.key /etc/named.conf
chmod 640 /etc/rndc.key /etc/named.conf
chown -R named.named /opt/named

systemctl daemon-reload
systemctl enable named

cp -a /etc/resolv.conf /etc/resolv.conf.bak
```

```
cat > /etc/resolv.conf << "EOF"
nameserver 127.0.0.1
nameserver 1.1.1.1
#search internal
EOF

printf "\n\n START SERVICE AFTER VALIDATING INSTALL OR MAKING MODIFICATIONS \n\n"
exit
```

That's it!

Happy DNS'n! :)

Revision #10

Created 24 July 2023 16:42:12 by Phatlix

Updated 25 July 2023 08:09:56 by Phatlix