PART 1 - COPY PASTE EDIT REPEAT

This write up will be a lot less talk and a lot more action. There are a lot of tutorials out there but if you need some better in-depth info, I highly recommend the BIND documentation that ISC has put together. They really have done a fantastic job.

Little note before we get rolling. This setup will allow for being a caching server or all the way to being authoritative (be your own name server). The config files below will have all the meat required to be authoritative, but will be commented out. The initial setup will just be caching. This will give you time to get the system all setup and start using the system, then you can go back through and uncomment the parts you want to use.

I have used this setup for many many years and it has treated me well.

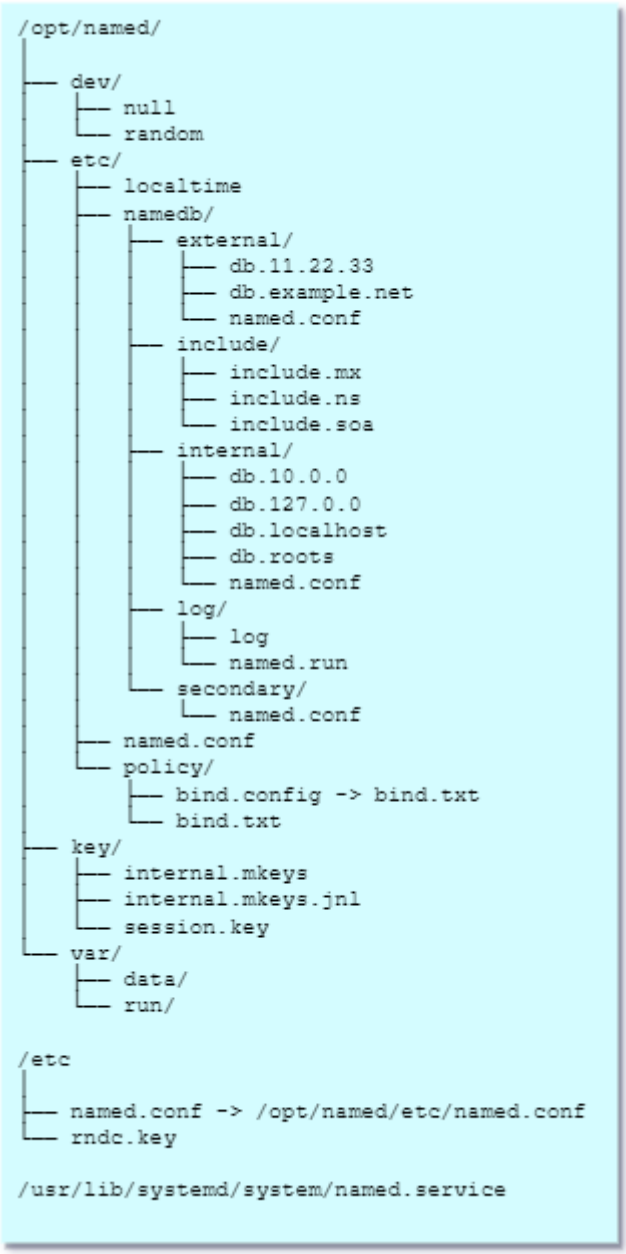
Here comes a warning...

> As you copy and paste these configs into your system, please be sure to check it over real good and change names and IP's to fit your setup. It may require some digging around if you miss something. Just a heads up!

> **UPDATE 2023.07.24:** I published **PART 2**. That page has some additional detail and... complete build scripts! You could build your own script if you just copied all the parts on this page. But I went ahead and did that for you already on the next page. PART 1 is a good working reference, and is also a good break down of the various components. I find it nice to just come grab bits and pieces when needed.

And here we go!

Here is a quick folder and file drill down.
All of this will be created with the script/configs. minus the files that get generated automatically.



SITE AND FILES *(current as of 2023.07.20)*:

ISC BIND9 - https://www.isc.org/bind/

DOCUMENT - https://downloads.isc.org/isc/bind9/9.18.17/doc/arm/Bv9ARM.pdf

GITLAB - https://gitlab.isc.org/isc-projects/bind9/-/tree/v9.18.17/

BIND 9.18.17 - https://downloads.isc.org/isc/bind9/9.18.17/bind-9.18.17.tar.xz

CREATE "NAMED" USER:

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

CREATE JAIL STRUCTURE:

```
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
```

COPY CRYPTO POLICY TO JAIL:

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

DOWNLOAD AND EXTRACT ARCHIVE:

```
cd /opt
wget https://downloads.isc.org/isc/bind9/9.18.17/bind-9.18.17.tar.xz
gtar -xf bind-9.18.17.tar.xz
rm -f bind-9.18.17.tar.xz
```

GRAB DEPENDENCIES *(building with GeoIP2, XML, JSON, LMDB, IDN)*:

```
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 libselinux-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
```

BUILD CONFIG:

```
cd /opt/bind-9.18.17
./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 AND INSTALL:

```
make &&
make install
```

GENERATE RNDC.KEY *(will be placed in /etc)*:

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

This next part is two pieces. Need to copy the key out of the rndc.key and plug it into the named.conf file. You could copy the entire contents of the rndc.key as well and just replace the entire block in the config file.

The build script I attached in another page, will do that part automatically.

CREATE MAIN NAMED.CONF FILE:

```
cat > /opt/named/etc/named.conf << "EOF"
### BIND 9.18.17 - MAIN CONFIG

#acl "lan-net" { 10.0.0.0/24; };

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; };
        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; } keys { rndc-key; };
};

/* replace below block with contents of rndc.key file */
key "rndc-key" {
        algorithm hmac-sha256;
        secret
"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx";
};
```

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

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

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

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

```
};


EOF
```

COPY RNDC.KEY CONTENTS INTO NAMED.CONF *(the block in the named.conf looks exactly the same as the key file)*:

```
cat /etc/rndc.key
```

```
key "rndc-key" {
        algorithm hmac-sha256;
        secret
"xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxx";
};
```

LINK MAIN NAMED.CONF TO /ETC;

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

CHANGE TO INCLUDE FOLDER AND CREATE INCLUDE FILES *(change files to reflect your setup)*:

```
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     servername.internal.tld.  root.internal.tld. (
                                2023072001   ; serial
                                3h           ; refresh
                                1h           ; retry
                                1w           ; expire
                                1h )         ; minimum


EOF
```

```
cat > include.ns << "EOF"
;
; Name Server Record
;

@       IN      NS      servername.internal.tld.

EOF


cat > include.mx << "EOF"
;
; MX Record
;

@       IN      MX 10   mx1.external.tld.
@       IN      MX 20   mx2.external.tld.

EOF
```

CHANGE TO INTERNAL FOLDER AND CREATE LOCAL/INTERNAL ZONES AND CONFIG FILE:

```
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.internal.tld << "EOF"
; -----> internal.tld <-----

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

;
; INTERNAL SYSTEMS
; Host Addresses and Canonical Names
;

;@              IN      A               10.0.0.2
;www            IN      CNAME           @
;ftp            IN      CNAME           @

//router              A       10.0.0.1
//server1             A       10.0.0.2
//server2             A       10.0.0.3
//server3             A       10.0.0.4
//sweetname           CNAME   server1

EOF


cat > db.10.0.0 << "EOF"
; -----> internal.tld - Reverse Zone: 0.0.10.in-addr.arpa. <-----

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

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

; INTERNAL SYSTEMS
; Reverse Pointer Records // note the ending dots

//1       IN      PTR     router.internal.tld.
//2       IN      PTR     server1.internal.tld.
//3       IN      PTR     server2.internal.tld.
//4       IN      PTR     server3.internal.tld.

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 "internal.tld" {
//        type master;
//        file "internal/db.internal.tld";
//        allow-update { key "rndc-key"; };
//        //allow-transfer { secondary ns ip; };
//        notify yes;
// };

// zone "0.0.10.in-addr.arpa." {
```

```
//        type master;
//        file "internal/db.10.0.0";
//        allow-update { key "rndc-key"; };
//        //allow-transfer { secondary ns ip; };
//        notify yes;
// };

EOF
```

CHANGE TO SECONDARY FOLDER AND CREATE SAMPLE CONFIG:

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

cat > named.conf << "EOF"
// SECONDARY ZONE FILE

//zone "internal.tld" {
//        type slave;
//        masters { master ns ip; };
//        file "secondary/db.internal.tld";
//};

EOF
```

CHANGE TO EXTERNAL FOLDER AND CREATE SAMPLE CONFIGS:

```
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 <-----

$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 - Reverse Zone: 33.22.11.in-addr.arpa. <-----

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

44      IN      PTR     example.com.

EOF
```

CREATE SYSTEMD SERVICE:

```
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
```

CREATE SYSCONFIG OPTION FILE *(current option disables ipv6 listening)*:

```
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.
```

```
OPTIONS="-4"

EOF
```

CREATE SCRIPT TO UPDATE ROOTS FILE AND RUN IT:

```
cat > /opt/named/etc/namedb/roots << "EOF"
#!/bin/bash
#
# SCRIPT TO GRAB ROOTS
#

# 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
```

CREATE SCRIPT TO RELOAD BIND AND TAIL THE LOG FILE *(ctrl+c to drop the tail after running the script)*:

```
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
```

CLEAN UP, GRAB ROOTS, AND SET PERMISSIONS:

```
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
```

After all that copy'n and paste'n, you should be ready to go.
Make sure all your data is correct in the files. Once validated, start it up!

RE-READ SYSTEMD, ENABLE, AND START BIND:

```
systemctl daemon-reload
systemctl enable named
systemctl start named
```

CHANGE YOUR RESOLV.CONF:

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

cat > /etc/resolv.conf << "EOF"
nameserver 127.0.0.1

EOF
```

DO A LITTLE TEST:

```
# FORWARD TEST
dig a cloudflare.com

# REVERSE TEST
dig -x 9.9.9.9
```

That's it!

I hope this write up and these configs, love you long time. :)

Revision #18
Created 20 July 2023 12:39:30 by Phatlix
Updated 25 July 2023 07:34:40 by Phatlix