How to Deploy a Secure DNS Server

Motivation

My primary motivation with this paper is to share how to configure a secure DNS server for an enterprise environment. Below, in the examples you will find the domain name is “fortress.lan” and all of the workstation names are star wars character names. The original setup of this was deployed on a firewall that had several subnets routing and performing DNS queries, e.g. 192.168.139.0/24, 172.31.253.0/24, 10.101.101.0/24 and 10.99.99.0/24. DNS will continue to be attacked by various sources, continue to follow best practices. This is a solid baseline, but should not be considered fool proof; meaning don’t just set it up, but continue to follow security best practices on DNS to ensure you continue to have the right configuration deployed.

History

‘Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates domain names, which can be easily memorized by humans, to the numerical IP addresses needed for the purpose of computer services and devices worldwide. The Domain Name System is an essential component of the functionality of most Internet services.

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over subdomains to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database.

The Domain Name System also specifies the technical functionality of this database service. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in DNS, as part of the Internet Protocol Suite.

The Internet maintains two principal namespaces, the domain name hierarchy and the Internet Protocol (IP) address spaces. The Domain Name System maintains the domain name hierarchy and provides translation services between it and the address spaces. Internet name servers and a communication protocol implement the Domain Name System. A DNS name server is a server that stores the DNS records for a domain name, such as address (A or AAAA) records, name server (NS) records, and mail exchanger (MX) records (see also list of DNS record types); a DNS name server responds with answers to queries against its database.'

Source: http://en.wikipedia.org/wiki/Domain_Name_System

Test environment layout

I used vagrant to create a new CentOS 6.5 server with:

```
Hostname:          darthvader.fortress.lan
IP addr:    eth0: dhcp
            eth1: 192.168.139.10
            eth2: 172.31.253.10
Hard Drive Size:   40GB
Mem:               4GB
CPUs:              2
```

Setup and deployment

After install, elevate to root with "sudo -i" and perform the following install:

```
yum install bind bind-devel bind-libs bind-utils
```

All of the configuration files I used are in the Appendix section at the end of the documents.

Key file layout:

```
/etc/named.conf
/etc/rndc.conf
/etc/sysconfig/named
/var/named/named.ca
/var/named/named.empty
/var/named/named.localhost
/var/named/named.loopback
/var/named/data/
/var/named/dynamic/
/var/named/slave/
/var/named/master/99.99.10.in-addr.arpa
/var/named/master/101.101.10.in-addr.arpa
/var/named/master/139.168.192.in-addr.arpa
/var/named/master/253.31.172.in-addr.arpa
/var/named/master/empty.db
/var/named/master/fortress.lan
/var/named/master/localhost-forward.db
/var/named/master/localhost-reverse.db
```

After installing/modifying said files **AND** changing to match your environment [this is my working reference model that I tailor per customer site], you will need to change ownership and group on several files as follows (again, as root):

```
cd /var/named
find . –type f –print0 | xargs -0 chgrp named
cd /var/named/master
chmod 0640 *
service named restart
```

After this, test from a workstation to verify the DNS service works correctly:

```
dig @192.168.139.10  darthvader.fortress.lan
```

If everything works correcty, change all of your servers /etc/resolv.conf to something similar:

```
search fortress.lan
nameserver 192.168.139.10
domain fortress.lan
```

Conclusion

This is pretty straight forward. I spent weeks getting this working. Future work to make this more secure could be to activate iptables and only allow TCP and UDP port 53 into the DNS server from the subnets authorized, e.g. 192.168.139.0/24. One could activate chroot and move the config files into that directory for security. One could activate SeLinux to protect the kernel. I would also version control the configuration files with git to a local git repository in case the system was ever compromised. There is a lot of possibilities here for future security solutions.

Appenedix

/etc/named.conf:

```
//
// named.conf
//

acl "friendlies" {
        127.0.0.1/32;
        192.168.139.0/24;
};

acl "dmz" {
        172.31.253.0/24;
};


options {
      listen-on port 53 { 127.0.0.1; };
      listen-on-v6 port 53 { ::1; };
      directory   "/var/named";
      dump-file   "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
      //
      datasize 32768k;
      version "Nunya";
      transfer-format many-answers;
      recursion yes;
      allow-query { "friendlies"; "dmz"; };
      allow-transfer { "none"; };
      allow-update { "none"; };
      stacksize 32768k;
      //
      listen-on       { 127.0.0.1; 192.168.139.10; 172.31.253.10; };
      //
      disable-empty-zone "255.255.255.255.IN-ADDR.ARPA";
      disable-empty-zone
"0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA";
      disable-empty-zone
"1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.IP6.ARPA";
      //
      dnssec-enable yes;
      dnssec-validation yes;
      dnssec-lookaside auto;

      /* Path to ISC DLV key */
      bindkeys-file "/etc/named.iscdlv.key";

      managed-keys-directory "/var/named/dynamic";
};

logging {
        channel my_debug {
                    file "/var/log/named_debug.log" versions 9 size 5m;
```

```
                    severity debug 5;
                    print-time yes;
                    print-severity yes;
                    print-category yes;
        };
        channel security_info {
                    file "/var/log/named_auth.log" versions 9 size 5m;
                    severity notice;
                    print-time yes;
                    print-severity yes;
                    print-category yes;
        };
        channel info {
                    file "/var/log/named_info.log" versions 9 size 5m;
                    severity info;
                    print-time yes;
                    print-severity yes;
                    print-category yes;
        };
        category update { my_debug; };
        category security { security_info; };
        category queries { info; };
};

// RFC 1912
zone "127.in-addr.arpa" { type master; file "master/localhost-reverse.db"; };
zone "255.in-addr.arpa" { type master; file "master/empty.db"; };

// RFC 1912-style zone for IPv6 localhost address
zone "0.ip6.arpa"       { type master; file "master/localhost-reverse.db"; };

// Private Use Networks (RFC 1918)
//zone "10.in-addr.arpa"                { type master; file
"master/empty.db"; };
zone "16.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "17.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "18.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "19.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "20.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "21.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "22.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "23.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "24.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "25.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "26.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "27.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "28.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "29.172.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "30.172.in-addr.arpa"      { type master; file "master/empty.db"; };
//zone "168.192.in-addr.arpa"     { type master; file "master/empty.db"; };

// Link-local/APIPA (RFCs 3330 and 3927)
zone "254.169.in-addr.arpa"     { type master; file "master/empty.db"; };

// TEST-NET for Documentation (RFC 3330)
zone "2.0.192.in-addr.arpa"     { type master; file "master/empty.db"; };
```

```
// Router Benchmark Testing (RFC 3330)
zone "18.198.in-addr.arpa"      { type master; file "master/empty.db"; };
zone "19.198.in-addr.arpa"      { type master; file "master/empty.db"; };

// IANA Reserved - Old Class E Space
zone "240.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "241.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "242.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "243.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "244.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "245.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "246.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "247.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "248.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "249.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "250.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "251.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "252.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "253.in-addr.arpa"         { type master; file "master/empty.db"; };
zone "254.in-addr.arpa"         { type master; file "master/empty.db"; };

// IPv6 Unassigned Addresses (RFC 4291)
zone "1.ip6.arpa"               { type master; file "master/empty.db"; };
zone "3.ip6.arpa"               { type master; file "master/empty.db"; };
zone "4.ip6.arpa"               { type master; file "master/empty.db"; };
zone "5.ip6.arpa"               { type master; file "master/empty.db"; };
zone "6.ip6.arpa"               { type master; file "master/empty.db"; };
zone "7.ip6.arpa"               { type master; file "master/empty.db"; };
zone "8.ip6.arpa"               { type master; file "master/empty.db"; };
zone "9.ip6.arpa"               { type master; file "master/empty.db"; };
zone "a.ip6.arpa"               { type master; file "master/empty.db"; };
zone "b.ip6.arpa"               { type master; file "master/empty.db"; };
zone "c.ip6.arpa"               { type master; file "master/empty.db"; };
zone "d.ip6.arpa"               { type master; file "master/empty.db"; };
zone "e.ip6.arpa"               { type master; file "master/empty.db"; };
zone "0.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "1.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "2.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "3.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "4.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "5.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "6.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "7.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "8.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "9.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "a.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "b.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "0.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "1.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "2.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "3.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "4.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "5.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "6.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "7.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "8.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "9.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
```

```
zone "a.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "b.e.f.ip6.arpa"           { type master; file "master/empty.db"; };

// IPv6 Deprecated Site-Local Addresses (RFC 3879)
zone "c.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "d.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "e.e.f.ip6.arpa"           { type master; file "master/empty.db"; };
zone "f.e.f.ip6.arpa"           { type master; file "master/empty.db"; };

// IP6.INT is Deprecated (RFC 4159)
zone "ip6.int"                  { type master; file "master/empty.db"; };

// IPv6 ULA (RFC 4193)
zone "c.f.ip6.arpa"             { type master; file "master/empty.db"; };
zone "d.f.ip6.arpa"             { type master; file "master/empty.db"; };

// IPv6 Link Local (RFC 4291)//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//

zone "fortress.lan" {
        type master;
        file "master/fortress.lan";
        allow-query { "friendlies"; };
};

zone "99.99.10.in-addr.arpa" {
        type master;
        file "master/99.99.10.in-addr-arpa";
        allow-query { "friendlies"; };
};

zone "101.101.10.in-addr.arpa" {
        type master;
        file "master/101.101.10.in-addr.arpa";
        allow-query { "friendlies"; };
};

zone "139.168.192.in-addr.arpa" {
        type master;
        file "master/139.168.192.in-addr.arpa";
        allow-query { "friendlies"; };
};

zone "253.31.172.in-addr.arpa" {
        type master;
        file "master/253.31.172.in-addr.arpa";
        allow-query { "friendlies"; };
};

zone "." IN {
      type hint;
      file "named.ca";
};

include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
```

/etc/rndc.conf:

```
# Start of rndc.conf
key "rndc-key" {
      algorithm hmac-md5;
      secret "xf7AyUflJBVBDlOAHV279Q==";
};

options {
      default-key "rndc-key";
      default-server 127.0.0.1;
      default-port 953;
};
# End of rndc.conf
```

/etc/sysconfig/named:

```
# BIND named process options
# ~~~~~~~~~~~~~~~~~~~~~~~~~
# Currently, you can use the following options:
#
# ROOTDIR="/var/named/chroot"  --  will run named in a chroot environment.
#                              you must set up the chroot environment
#                              (install the bind-chroot package) before
#                              doing this.
#     NOTE:
#     Those directories are automatically mounted to chroot if they are
#     empty in the ROOTDIR directory. It will simplify maintenance of your
#         chroot environment.
#          - /var/named
#          - /etc/pki/dnssec-keys
#          - /etc/named
#          - /usr/lib64/bind or /usr/lib/bind (architecture dependent)
#
#       Those files are mounted as well if target file doesn't exist in
#       chroot.
#          - /etc/named.conf
#          - /etc/rndc.conf
#          - /etc/rndc.key
#          - /etc/named.rfc1912.zones
#          - /etc/named.dnssec.keys
#        - /etc/named.iscdlv.key
#
#     Don't forget to add "$AddUnixListenSocket /var/named/chroot/dev/log"
#     line to your /etc/rsyslog.conf file. Otherwise your logging becomes
#     broken when rsyslogd daemon is restarted (due update, for example).
#
# OPTIONS="whatever" --  These additional options will be passed to named
#                    at startup. Don't add -t here, use ROOTDIR instead.
OPTIONS="-4"
#
# KEYTAB_FILE="/dir/file" --  Specify named service keytab file (for GSS-TSIG)
#
# DISABLE_ZONE_CHECKING -- By default, initscript calls named-checkzone
#                          utility for every zone to ensure all zones are
```

```
#                       valid before named starts. If you set this option
#                       to 'yes' then initscript doesn't perform those
#                       checks.
```

/var/named/named.ca:

```
; <<>> DiG 9.9.4-P2-RedHat-9.9.4-12.P2 <<>> +norec NS . @a.root-servers.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26229
;; flags: qr aa; QUERY: 1, ANSWER: 13, AUTHORITY: 0, ADDITIONAL: 24

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1472
;; QUESTION SECTION:
;.                      IN    NS

;; ANSWER SECTION:
.                   518400      IN    NS    a.root-servers.net.
.                   518400      IN    NS    b.root-servers.net.
.                   518400      IN    NS    c.root-servers.net.
.                   518400      IN    NS    d.root-servers.net.
.                   518400      IN    NS    e.root-servers.net.
.                   518400      IN    NS    f.root-servers.net.
.                   518400      IN    NS    g.root-servers.net.
.                   518400      IN    NS    h.root-servers.net.
.                   518400      IN    NS    i.root-servers.net.
.                   518400      IN    NS    j.root-servers.net.
.                   518400      IN    NS    k.root-servers.net.
.                   518400      IN    NS    l.root-servers.net.
.                   518400      IN    NS    m.root-servers.net.

;; ADDITIONAL SECTION:
a.root-servers.net.     518400      IN    A     198.41.0.4
b.root-servers.net.     518400      IN    A     192.228.79.201
c.root-servers.net.     518400      IN    A     192.33.4.12
d.root-servers.net.     518400      IN    A     199.7.91.13
e.root-servers.net.     518400      IN    A     192.203.230.10
f.root-servers.net.     518400      IN    A     192.5.5.241
g.root-servers.net.     518400      IN    A     192.112.36.4
h.root-servers.net.     518400      IN    A     128.63.2.53
i.root-servers.net.     518400      IN    A     192.36.148.17
j.root-servers.net.     518400      IN    A     192.58.128.30
k.root-servers.net.     518400      IN    A     193.0.14.129
l.root-servers.net.     518400      IN    A     199.7.83.42
m.root-servers.net.     518400      IN    A     202.12.27.33
a.root-servers.net.     518400      IN    AAAA  2001:503:ba3e::2:30
c.root-servers.net.     518400      IN    AAAA  2001:500:2::c
d.root-servers.net.     518400      IN    AAAA  2001:500:2d::d
f.root-servers.net.     518400      IN    AAAA  2001:500:2f::f
h.root-servers.net.     518400      IN    AAAA  2001:500:1::803f:235
i.root-servers.net.     518400      IN    AAAA  2001:7fe::53
j.root-servers.net.     518400      IN    AAAA  2001:503:c27::2:30
k.root-servers.net.     518400      IN    AAAA  2001:7fd::1
l.root-servers.net.     518400      IN    AAAA  2001:500:3::42
m.root-servers.net.     518400      IN    AAAA  2001:dc3::35
```

```
;; Query time: 58 msec
;; SERVER: 198.41.0.4#53(198.41.0.4)
;; WHEN: Wed Apr 23 14:52:37 CEST 2014
;; MSG SIZE  rcvd: 727
```

/var/named/named.empty:

```
$TTL 3H
@       IN SOA      @ rname.invalid. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
```

/var/named/named.localhost:

```
$TTL 1D
@       IN SOA      @ rname.invalid. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
```

/var/named/named.loopback:

```
$TTL 1D
@       IN SOA      @ rname.invalid. (
                                0       ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )    ; minimum
        NS      @
        A       127.0.0.1
        AAAA    ::1
        PTR     localhost.
```

/var/named/master/99.99.10.in-addr.arpa:

```
$TTL  86400

@       IN SOA  fortress.lan.   darthvader.fortress.lan.        (
              2003102600  ; Serial
              10800       ; Refresh (3 hours)
              3600        ; Retry (1 hour)
              604800            ; Expire (1 week)
              86400  )    ; Minimum (1 day)

              IN NS darthvader.fortress.lan.
66            IN PTR  padme.fortress.lan.
100           IN PTR  truelove.fortress.lan.
```

/var/named/master/101.101.10.in-addr.arpa:

```
$TTL  86400

@     IN SOA  fortress.lan.   darthvader.fortress.lan.        (
            2003102600  ; Serial
            10800       ; Refresh (3 hours)
            3600        ; Retry (1 hour)
            604800            ; Expire (1 week)
            86400  )    ; Minimum (1 day)

            IN NS darthvader.fortress.lan.
1           IN PTR  shumai.fortress.lan.
2           IN PTR  pooja.fortress.lan.
```

/var/named/master/139.168.192.in-addr.arpa:

```
$TTL  86400

@     IN SOA  fortress.lan.   darthvader.fortress.lan.        (
            2003102600  ; Serial
            10800       ; Refresh (3 hours)
            3600        ; Retry (1 hour)
            604800      ; Expire (1 week)
            86400  )    ; Minimum (1 day)

      IN NS darthvader.fortress.lan.

1     IN PTR      darthvader.fortress.lan.
2     IN PTR      palpatine.fortress.lan.
3     IN PTR      landocalrissian.fortress.lan.
4     IN PTR      countdooku.fortress.lan.
5     IN PTR      bobafett.fortress.lan.
6     IN PTR      macewindu.fortress.lan.
7     IN PTR      quigonjinn.fortress.lan.
8     IN PTR      marajadeskywalker.fortress.lan.
9     IN PTR      hansolo.fortress.lan.
10    IN PTR      admackbar.fortress.lan.
11    IN PTR      nyratagira.fortress.lan.
12    IN PTR      nomanor.fortress.lan.
13    IN PTR      wedge.fortress.lan.
14    IN PTR      passel.fortress.lan.
15    IN PTR      sagoro.fortress.lan.
16    IN PTR      ponda.fortress.lan.
17    IN PTR      hermione.fortress.lan.
18    IN PTR      edcel.fortress.lan.
19    IN PTR      aldar.fortress.lan.
20    IN PTR      garm.fortress.lan.
21    IN PTR      sio.fortress.lan.
22    IN PTR      anakin.fortress.lan.
23    IN PTR      depa.fortress.lan.
24    IN PTR      jarjar.fortress.lan.
```

```
25    IN PTR      doda.fortress.lan.
26    IN PTR      bossk.fortress.lan.
27    IN PTR      brakiss.fortress.lan.
28    IN PTR      joruus.fortress.lan.
29    IN PTR      chewbacca.fortress.lan.
30    IN PTR      ronet.fortress.lan.
31    IN PTR      corde.fortress.lan.
32    IN PTR      salacious.fortress.lan.
33    IN PTR      barquin.fortress.lan.
34    IN PTR      admdaala.fortress.lan.
35    IN PTR      mjrderlin.fortress.lan.
36    IN PTR      lexi.fortress.lan.
37    IN PTR      daultay.fortress.lan.
38    IN PTR      dorme.fortress.lan.
39    IN PTR      tundra.fortress.lan.
40    IN PTR      kyp.fortress.lan.
41    IN PTR      onaconda.fortress.lan.
42    IN PTR      toryn.fortress.lan.
43    IN PTR      jangofett.fortress.lan.
44    IN PTR      fiolla.fortress.lan.
45    IN PTR      gallandro.fortress.lan.
46    IN PTR      gasgano.fortress.lan.
47    IN PTR      ghent.fortress.lan.
48    IN PTR      greedo.fortress.lan.
49    IN PTR      nutegunray.fortress.lan.
50    IN PTR      cptgrammel.fortress.lan.
51    IN PTR      runehaako.fortress.lan.
52    IN PTR      corranhorn.fortress.lan.
53    IN PTR      ysanneisard.fortress.lan.
54    IN PTR      jaxxon.fortress.lan.
55    IN PTR      moffjerjerrod.fortress.lan.
56    IN PTR      jessa.fortress.lan.
57    IN PTR      jettster.fortress.lan.
58    IN PTR      jira.fortress.lan.
59    IN PTR      kabe.fortress.lan.
60    IN PTR      talon.fortress.lan.
61    IN PTR      kylekatarn.fortress.lan.
62    IN PTR      nevakee.fortress.lan.
63    IN PTR      taskee.fortress.lan.
64    IN PTR      obiwankenobi.fortress.lan.
65    IN PTR      ketwoi.fortress.lan.
66    IN PTR      padme.fortress.lan.
67    IN PTR      lumiya.fortress.lan.
68    IN PTR      madine.fortress.lan.
70    IN PTR      elanmak.fortress.lan.
72    IN PTR      lynme.fortress.lan.
73    IN PTR      monmothma.fortress.lan.
75    IN PTR      ruwee.fortress.lan.
76    IN PTR      ryoo.fortress.lan.
77    IN PTR      sola.fortress.lan.
78    IN PTR      momaw.fortress.lan.
79    IN PTR      jocasta.fortress.lan.
80    IN PTR      po.fortress.lan.
81    IN PTR      nien.fortress.lan.
82    IN PTR      hermi.fortress.lan.
83    IN PTR      barris.fortress.lan.
84    IN PTR      poggle.fortress.lan.
```

```
85      IN PTR      yarael.fortress.lan.
86      IN PTR      qeldroma.fortress.lan.
87      IN PTR      quadinaros.fortress.lan.
88      IN PTR      rancisis.fortress.lan.
89      IN PTR      maxrebo.fortress.lan.
90      IN PTR      reti.fortress.lan.
91      IN PTR      sabe.fortress.lan.
92      IN PTR      zevsenesca.fortress.lan.
93      IN PTR      darthsidious.fortress.lan.
94      IN PTR      lukeskywalker.fortress.lan.
95      IN PTR      elansleazebaggano.fortress.lan.
96      IN PTR      anakinsolo.fortress.lan.
97      IN PTR      hansolo.fortress.lan.
98      IN PTR      jacensolo.fortress.lan.
99      IN PTR      jainasolo.fortress.lan.
100     IN PTR      truelove.fortress.lan.

150     IN PTR      ca-01.fortress.lan.
```

/var/named/master/253.31.172.in-addr.arpa:

```
$TTL  86400

@       IN SOA  fortress.lan.   darthvader.fortress.lan.        (
              2003102600  ; Serial
              10800       ; Refresh (3 hours)
              3600        ; Retry (1 hour)
              604800            ; Expire (1 week)
              86400  )    ; Minimum (1 day)

              IN NS darthvader.fortress.lan.
1             IN PTR  seitaria.fortress.lan.
2             IN PTR  darthmaul.fortress.lan.
```

/var/named/master/empty.db:

```
; $FreeBSD: src/etc/namedb/master/empty.db,v 1.1.10.1 2009/04/15 03:14:26
kensmith Exp $

$TTL 3h
@ SOA @ nobody.localhost. 42 1d 12h 1w 3h
      ; Serial, Refresh, Retry, Expire, Neg. cache TTL

@       NS    @

; Silence a BIND warning
@       A     127.0.0.1
```

/var/named/master/fortress.lan:

```
$TTL  86400

@       IN SOA  fortress.lan.   darthvader.fortress.lan. (
              2003102600  ; Serial
              10800       ; Refresh (3 hours)
              3600        ; Retry (1 hour)
              604800            ; Expire (1 week)
              86400  )    ; Minimum (1 day)
```

```
            IN    NS    darthvader.fortress.lan.

localhost   IN    A     127.0.0.1

; DMZ & Firewall
shumai              IN    A     10.101.101.1
pooja       IN    A     10.101.101.2

; DMZ
seitaria    IN    A     172.31.253.1
darthmaul   IN    A     172.31.253.2
padme       IN    A     10.99.99.66
truelove    IN    A     10.99.99.100

; Internal Fortress
darthvader  IN    A     192.168.5.1
palpatine   IN    A     192.168.5.2
landocalrissian   IN    A     192.168.5.3
countdooku  IN    A     192.168.5.4
bobafett    IN    A     192.168.5.5
macewindu   IN    A     192.168.5.6
quigonjinn  IN    A     192.168.5.7
marajade8   IN    A     192.168.5.8
hansolo             IN    A     192.168.5.9
admackbar   IN    A     192.168.5.10
nyratagira  IN    A     192.168.5.11
nomanor             IN    A     192.168.5.12
wedge       IN    A     192.168.5.13
passel              IN    A     192.168.5.14
sagoro              IN    A     192.168.5.15
ponda       IN    A     192.168.5.16
hermione    IN    A     192.168.5.17
edcel       IN    A     192.168.5.18
aldar       IN    A     192.168.5.19
garm        IN    A     192.168.5.20
sio         IN    A     192.168.5.21
anakin              IN    A     192.168.5.22
depa        IN    A     192.168.5.23
jarjar              IN    A     192.168.5.24
doda        IN    A     192.168.5.25
bossk       IN    A     192.168.5.26
brakiss             IN    A     192.168.5.27
joruus              IN    A     192.168.5.28
chewbacca   IN    A     192.168.5.29
ronet       IN    A     192.168.5.30
corde       IN    A     192.168.5.31
salacious   IN    A     192.168.5.32
barquin             IN    A     192.168.5.33
admdaala    IN    A     192.168.5.34
mjrderlin   IN    A     192.168.5.35
lexi        IN    A     192.168.5.36
daultay             IN    A     192.168.5.37
dorme       IN    A     192.168.5.38
tundra              IN    A     192.168.5.39
kyp         IN    A     192.168.5.40
onaconda    IN    A     192.168.5.41
toryn       IN    A     192.168.5.42
```

```
jangofett   IN    A     192.168.5.43
fiolla            IN    A     192.168.5.44
gallandro   IN    A     192.168.5.45
gasgano           IN    A     192.168.5.46
ghent       IN    A     192.168.5.47
greedo            IN    A     192.168.5.48
nutegunray  IN    A     192.168.5.49
cptgrammel  IN    A     192.168.5.50
runehaako   IN    A     192.168.5.51
corranhorn  IN    A     192.168.5.52
ysanneisard IN    A     192.168.5.53
jaxxon            IN    A     192.168.5.54
moffjerjerrod     IN    A     192.168.5.55
jessa       IN    A     192.168.5.56
jettster    IN    A     192.168.5.57
jira        IN    A     192.168.5.58
kabe        IN    A     192.168.5.59
talon       IN    A     192.168.5.60
kylekatarn  IN    A     192.168.5.61
nevakee           IN    A     192.168.5.62
taskee            IN    A     192.168.5.63
obiwankenobi      IN    A     192.168.5.64
ketwoi            IN    A     192.168.5.65
padme       IN    A     192.168.5.66
lumiya            IN    A     192.168.5.67
madine            IN    A     192.168.5.68
elanmak           IN    A     192.168.5.70
lynme       IN    A     192.168.5.72
monmothma   IN    A     192.168.5.73
ruwee       IN    A     192.168.5.75
ryoo        IN    A     192.168.5.76
sola        IN    A     192.168.5.77
momaw       IN    A     192.168.5.78
jocasta           IN    A     192.168.5.79
po          IN    A     192.168.5.80
nien        IN    A     192.168.5.81
hermi       IN    A     192.168.5.82
barris            IN    A     192.168.5.83
poggle            IN    A     192.168.5.84
yarael            IN    A     192.168.5.85
qeldroma    IN    A     192.168.5.86
quadinaros  IN    A     192.168.5.87
rancisis    IN    A     192.168.5.88
maxrebo           IN    A     192.168.5.89
reti        IN    A     192.168.5.90
sabe        IN    A     192.168.5.91
zevsenesca  IN    A     192.168.5.92
darthsidious      IN    A     192.168.5.93
lukeskywalker     IN    A     192.168.5.94
elansleaze  IN    A     192.168.5.95
anakinsolo  IN    A     192.168.5.96
hansolo           IN    A     192.168.5.97
jacensolo   IN    A     192.168.5.98
jainasolo   IN    A     192.168.5.99
truelove    IN    A     192.168.5.100

ca-01       IN    A     192.168.5.150
```

/var/named/master/localhost-forward.db:

```
; $FreeBSD: src/etc/namedb/master/localhost-forward.db,v 1.1.10.1 2009/04/15
03:14:26 kensmith Exp $

$TTL 3h
localhost. SOA localhost. nobody.localhost. 42 1d 12h 1w 3h
      ; Serial, Refresh, Retry, Expire, Neg. cache TTL

      NS    localhost.

      A     127.0.0.1
      AAAA  ::1
```

/var/named/master/localhost-reverse.db:

```
; $FreeBSD: src/etc/namedb/master/localhost-reverse.db,v 1.1.10.1 2009/04/15
03:14:26 kensmith Exp $

$TTL 3h
@ SOA localhost. nobody.localhost. 42 1d 12h 1w 3h
      ; Serial, Refresh, Retry, Expire, Neg. cache TTL

      NS    localhost.

1.0.0 PTR   localhost.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 PTR localhost.
```