BIND Part 1

pschiu

Outline

- Installation
- Basic Configuration

Installing ISC BIND

- Step
  - # pkg install bind911
  - or
  - # cd /usr/ports/dns/bind911
  - # make install clean
  - or
  - # yum install bind.x86_64
  - # yum install bind-chroot.x86_64
  - or
  - # pacman -S bind
  - or
  - # tar -xzvf bind-9.11.0-P3.tar.gz ……..

pkg install on FreeBSD

```
[root@jal rc.d]#pkg install bind911
Updating FreeBSD repository catalogue...
FreeBSD repository is up-to-date.
All repositories are up-to-date.
Checking integrity... done (0 conflicting)
The following 1 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
        bind911: 9.11.0P3
Number of packages to be installed: 1

The process will require 59 MiB more space.

Proceed with this action? [y/N]: y
[1/1] Installing bind911-9.11.0P3...
[1/1] Extracting bind911-9.11.0P3: 100%
Message from bind911-9.11.0P3:
**********************************************************************
*                                                                    *
*           _   _____ _____ _____ _   _ _____ ___ ___ _   _ _        *
*          / \|_   _|_   _| ____| \ | |_   _|_ _/ _ \| \ | | |       *
*         / _ \ | |   | | |  _| |  \| | | |  | | | | |  \| |        *
*        / ___ \| |   | | | |___| |\  | | |  | | |_| | |\  |        *
*       /_/   \_\_|   |_| |_____|_| \_| |_| |___\___/|_| \_|        *
*                                                                    *
*   BIND requires configuration of rndc, including a "secret" key.  *
*    The easiest, and most secure way to configure rndc is to run    *
*   'rndc-confgen -a' to generate the proper conf file, with a new   *
*            random key, and appropriate file permissions.           *
*                                                                    *
*     The /usr/local/etc/rc.d/named script will do that for you.     *
*                                                                    *
**********************************************************************
```

named in FreeBSD

- startup
  - Edit /etc/rc.conf
    - named_enable="YES"
  - Manual utility command
    - % rndc {stop | reload | flush …}
      - In old version of BIND, use ndc command
- Configuration files
  - /usr/local/etc/namedb/named.conf
    - main Configuration file
  - /usr/local/etc/namedb/named.root
    - DNS root server cache hint file
  - Zone data files
- See your BIND version
  - % dig @140.113.1.1 version.bind txt chaos

```
version.bind.       0       CH      TXT     "9.8.1-P1"
version.bind.       0       CH      TXT     "9.10.4-P2"
version.bind.       0       CH      TXT     "There is no version."
version.bind.       0       CH      TXT     "JAL-DNS-Ver-1.8"
```

BIND Configuration – named.conf (1)

- /usr/local/etc/namedb/named.conf
  - Roles of this name server
    - Master, slave, or stub
  - Global options
  - Zone specific options

- named.conf is composed of following statements:
  - include, options, server, key, acl, zone, view, controls, logging, trusted-keys

BIND Configuration – named.conf (2)

- Address Match List
  - A generalization of an IP address that can include:
    - An IP address
      - Ex. 140.113.17.1
    - An IP network with CIDR netmask
      - Ex. 140.113/16
      - Ex. 140.113.0.0/16
    - The ! character to do negate
    - The name of a previously defined ACL
    - A cryptographic authentication key
  - First match
  - Example:
    - { !1.2.3.4; 1.2.3/24; };
    - { 168.95/16; 140.113.209/24; 140.113.235/24; 127.0.0.1; };
    - { 2001:288:4001::/48; };

BIND Configuration – named.conf include

- The "include" statement
  - Used to separate large configuration file
  - Another usage is used to separate cryptographic keys into a restricted permission file
  - Ex:
    - include "/usr/local/etc/namedb/rndc.key";

```
-rw-r--r--  1 root  wheel 28980 Feb 18  22:40 named.conf
-rw-r-----  1 root  bind    141 Jan  6   2016 rndc.key
```

  - If the path is relative
    - Relative to the directory option
      - Default path: /usr/local/etc/namedb/working/
    - Ex: chroot
      - /var/named/

BIND Configuration – named.conf acl

- The "acl" statement
  - Define a class of access control
  - Define before they are used
  - Syntax

```
acl acl_name {
   address_match_list;
};
```

  - Predefined acl classes
    - any, localnets, localhost, none
  - Example

```
acl CSnets {
     140.113.235/24; 140.113.17/24; 140.113.209/24;
};
acl NCTUnets {
     140.113/16; 140.126.237/24; 2001:288:4001::/48;
};
allow-transfer {localhost; CSnets; NCTUnets};
```

BIND Configuration – named.conf key

- The "key" statement
  - Define a encryption key used for authentication with a particular server
  - Syntax

```
key "key-id" {
    algorithm string;
    secret "string";
}
```

  - Example:

```
key "serv1-serv2" {
    algorithm hmac-md5;
    secret "ibkAlUA0XXAXDxWRTGeY+d4CGbOgOIr7n63eizJFHQo=";
}
```

  - This key is used to
    - Sign DNS request before sending to target
    - Validate DNS response after receiving from target

BIND Configuration – named.conf option (1)

- The “option” statement
  - Specify global options
  - Some options may be overridden later for specific zone or server
  - Syntax:

```
options {
        option;
        option;
};
```

- There are about 50 options in BIND9
  - version “There is no version.”; [real version num]

```
version.bind.       0       CH      TXT     "9.8.1-P1"
version.bind.       0       CH      TXT     "9.10.4-P2"
version.bind.       0       CH      TXT     "There is no version."
version.bind.       0       CH      TXT     "JAL-DNS-Ver-1.8"
```

  - directory “/etc/namedb/db”;
    - Base directory for relative path and path to put zone data files

BIND Configuration – named.conf option (2)

- notify yes | no [yes]
  - Whether notify slave sever when relative zone data is changed
- also-notify 140.113.235.101; [empty]
  - Also notify this non-NS server
- recursion yes | no [yes]
  - Recursive name server
- allow-recursion {address_match_list }; [all]
  - Finer granularity recursion setting
- check-names {master|slave|response action};
  - check hostname syntax validity
    - Letter, number and dash only
    - 64 characters for each component, and 256 totally
  - Action:
    - ignore: do no checking
    - warn: log bad names but continue
    - fail: log bad names and reject
  - default action
    - master fail
    - slave warn
    - response ignore

BIND Configuration – named.conf option (3)

- listen-on port ip_port address_match_list; [53, all]
  - NIC and ports that named listens for query
  - Ex: listen-on port 5353 { 192.168.1/24; };
- query-source address ip_addr port ip_port; [random]
  - NIC and port to send DNS query
- forwarders { in_addr; ... }; [empty]
  - Often used in cache name server
  - Forward DNS query if there is no answer in cache
- forward only | first; [first]
  - If forwarder does not response, queries for forward only server will fail
- allow-query address_match_list; [all]
  - Specify who can send DNS query to you
- allow-transfer address_match_list; [all]
  - Specify who can request zone transfer to you
- blackhole address_match_list; [empty]
  - Reject queries and would never ask them for answers

BIND Configuration – named.conf option (4)

- transfer-format one-answer | many-answers; [many-answers]
  - Ways to transfer data records from master to slave
  - How many data records in single packet
- transfers-in num; [10]
- transfers-out num; [10]
  - Limit of the number of inbound and outbound zone transfers concurrently
- transfers-per-ns num; [2]
  - Limit of the inbound zone transfers concurrently from the same remote server
- transfer-source IP-address;
  - IP of NIC used for inbound transfers

BIND Configuration – named.conf server

- The "server" statement
  - Tell named about the characteristics of its remote peers
  - Syntax

```
server ip_addr {
  bogus no | yes;
  provide-ixfr yes | no;  (for master)
  request-ixfr yes | no;  (for slave)
  transfers num;
  transfer-format many-answers | one-answer;
  keys { key-id; key-id};
};
```

  - ixfr
    - Incremental zone transfer
  - transfers
    - Limit of number of concurrent inbound zone transfers from that server
    - Server-specific transfers-in
  - keys
    - Any request sent to the remote server is signed with this key

BIND Configuration – named.conf zone (1)

- The "zone" statement
  - Heart of the named.conf that tells named about the zones that it is authoritative
  - zone statement format varies depending on roles of named
    - Master or slave
  - Basically

```
Syntax:
zone "domain_name" {
        type master | slave | stub;
        file "path";
        masters { ip_addr; ip_addr; };
        allow-query { address_match_list; };        [all]
        allow-transfer { address_match_list; };     [all]
        allow-update { address_match_list; };
         [empty]
};
```

BIND Configuration – named.conf zone (2)

- Master server zone configuration

```
zone "cs.nctu.edu.tw" IN {
    type master;
    file "named.hosts";
    allow-query { any; };
    allow-transfer { localhost; CS-DNS-Servers; };
    allow-update { none; };
};
```

- Slave server zone configuration

```
zone "cs.nctu.edu.tw" IN {
    type slave;
    file "cs.hosts";
    masters { 140.113.235.107; };
    allow-query { any; };
    allow-transfer { localhost; CS-DNS-Servers; };
};
```

BIND Configuration – named.conf zone (3)

- Forward zone and reverse zone

```
zone "cs.nctu.edu.tw" IN {
    type master;
    file "named.hosts";
    allow-query { any; };
    allow-transfer { localhost; CS-DNS-Servers; };
    allow-update { none; };
};


zone "235.113.140.in-addr.arpa" IN {
    type master;
    file "named.235.rev";
    allow-query { any; };
    allow-transfer { localhost; CS-DNS-Servers; };
    allow-update { none; };
};
```

BIND Configuration – named.conf zone (4)

- Example
  - In named.hosts, there are plenty of A or CNAME records

```
$ORIGIN cs.nctu.edu.tw.
…
bsd1            IN      A       140.113.235.131
csbsd1          IN      CNAME   bsd1
bsd2            IN      A       140.113.235.132
bsd3            IN      A       140.113.235.133
bsd4            IN      A       140.113.235.134
bsd5            IN      A       140.113.235.135
…
```

  - In named.235.rev, there are plenty of PTR records

```
$ORIGIN 235.113.140.in-addr.arpa.
…
131             IN      PTR     bsd1.cs.nctu.edu.tw.
132             IN      PTR     bsd2.cs.nctu.edu.tw.
133             IN      PTR     bsd3.cs.nctu.edu.tw.
134             IN      PTR     bsd4.cs.nctu.edu.tw.
135             IN      PTR     bsd5.cs.nctu.edu.tw.
…
```

BIND Configuration – named.conf zone (5)

- Setting up root hint
  - A cache of where are the DNS root servers

```
zone "." IN {
    type hint;
    file "named.root";
};
```

- Setting up forwarding zone
  - Forward DNS query to specific name server, bypassing the standard query path

```
zone "nctu.edu.tw" IN {
    type forward;
    forward first;
    forwarders { 140.113.250.135; 140.113.1.1; };
};

zone "113.140.in-addr.arpa" IN {
    type forward;
    forward first;
    forwarders { 140.113.250.135; 140.113.1.1; };
};
```

BIND Debugging and Logging

Logging (1)

- Terms
  - Channel
    - A place where messages can go
    - Ex: syslog, file or /dev/null
  - Category
    - A class of messages that named can generate
    - Ex: answering queries or dynamic updates
  - Module
    - The name of the source module that generates the message
  - Facility
    - syslog facility name
  - Severity
    - Priority in syslog
- Logging configuration
  - Define what are the channels
  - Specify where each message category should go
- When a message is generated
  - It is assigned a “category”, a “module”, a “severity”
  - It is distributed to all channels associated with its category

Logging (2)

- The “logging” statement
  - Either “file” or “syslog” in channel sub-statement
    - size:
      - ex: 2048, 100k, 20m, 15g, unlimited, default
    - facility:
      - ex: local0 ~ local7
    - severity:
      - critical, error, warning, notice, info, debug, dynamic

```
logging {
    channel_def;
    channel_def;
    …
    category category_name {
        channel_name;
        channel_name;
        …
    };
};
```

```
channel channel_name {
    file path [versions num|unlimited] [size siznum];
    syslog facility;

    severity severity;
    print-category yes|no;
    print-severity yes|no;
    print-time yes|no;
};
```

Logging (3)

- Predefined channels

default_syslog	Sends severity info and higher to syslog with facility daemon
default_debug	Logs to file "named.run", severity set to dynamic
default_stderr	Sends messages to stderr or named, severity info
null	Discards all messages

- Available categories

default	Categories with no explicit channel assignment
general	Unclassified messages
config	Configuration file parsing and processing
queries/client	A short log message for every query the server receives
dnssec	DNSSEC messages
update	Messages about dynamic updates
xfer-in/xfer-out	zone transfers that the server is receiving/sending
db/database	Messages about database operations
notify	Messages about the "zone changed" notification protocol
security	Approved/unapproved requests
resolver	Recursive lookups for clients

Logging (4)

- Example of logging statement

```
logging {
    channel security-log {
        file "/var/log/named/security.log" versions 5 size 10m;
        severity info;
        print-severity yes;
        print-time yes;
    };
    channel query-log {
        file "/var/log/named/query.log" versions 20 size 50m;
        severity info;
        print-severity yes;
        print-time yes;
    };
    category default        { default_syslog; default_debug; };
    category general        { default_syslog; };
    category security       { security-log; };
    category client         { query-log; };
    category queries        { query-log; };
    category dnssec         { security-log; };
};
```

https://jal.tw/dns:bind_log

Debug

- Named debug level
  - From 0 (debugging off) ~ 11 (most verbose output)
  - % named -d2 (start named at level 2)
  - % rndc trace (increase debugging level by 1)
  - % rndc trace 3 (change debugging level to 3)
  - % rndc notrace (turn off debugging)
- Debug with “logging” statement
  - Define a channel that include a severity with “debug” keyword
    - Ex: severity debug 3
    - All debugging messages up to level 3 will be sent to that particular channel

Tools

Tools – nslookup

- Interactive and Non-interactive
  - Non-Interactive
    - % nslookup cs.nctu.edu.tw.
    - % nslookup –type=mx cs.nctu.edu.tw.
    - % nslookup –type=ns cs.nctu.edu.tw. 140.113.1.1
  - Interactive
    - % nslookup
    - > set all
    - > set type=any
    - > set server host
    - > set lserver host
    - > set debug
    - > set d2

```
csduty:~ -lwhsu- nslookup
> set all
Default server: 140.113.235.107
Address: 140.113.235.107#53
Default server: 140.113.235.103
Address: 140.113.235.103#53
Default server: 140.113.1.1
Address: 140.113.1.1#53

Set options:
  novc                  nodebug          nod2
  search                recurse
  timeout = 0           retry = 3        port = 53
  querytype = A         class = IN
  srchlist = cs.nctu.edu.tw/csie.nctu.edu.tw
>
```

pkg install bind-tools

28

Tools – dig

- Usage
  - % dig cs.nctu.edu.tw
  - % dig cs.nctu.edu.tw mx
  - % dig @ns.nctu.edu.tw cs.nctu.edu.tw mx
  - % dig -x 140.113.209.3
    - Reverse query
  - % dig +trace jal.tw
  - % dig +dnssec jal.tw
- Find out the root servers
  - % dig @a.root-servers.net . ns

29

```
# pkg install bind-tools
```

29

How to debug a name server

- Trace from root
  - % dig ns tw.

```
tw.                     86399   IN      NS      g.dns.tw.
tw.                     86399   IN      NS      d.dns.tw.
tw.                     86399   IN      NS      i.dns.tw.
tw.                     86399   IN      NS      ns.twnic.net.
tw.                     86399   IN      NS      b.dns.tw.
tw.                     86399   IN      NS      sec4.apnic.net.
tw.                     86399   IN      NS      h.dns.tw.
tw.                     86399   IN      NS      a.dns.tw.
tw.                     86399   IN      NS      c.dns.tw.
tw.                     86399   IN      NS      f.dns.tw.
tw.                     86399   IN      NS      e.dns.tw.
```

  - % dig ns idv.tw

```
idv.tw.                 79726   IN      NS      a.twnic.net.tw.
idv.tw.                 79726   IN      NS      h.twnic.net.tw.
idv.tw.                 79726   IN      NS      f.twnic.net.tw.
idv.tw.                 79726   IN      NS      i.dns.tw.
idv.tw.                 79726   IN      NS      g.twnic.net.tw.
idv.tw.                 79726   IN      NS      e.twnic.net.tw.
idv.tw.                 79726   IN      NS      b.twnic.net.tw.
idv.tw.                 79726   IN      NS      d.twnic.net.tw.
idv.tw.                 79726   IN      NS      c.twnic.net.tw.
idv.tw.                 79726   IN      NS      sec4.apnic.net.
```

How to debug a name server – cont.

- % dig ns nasa.idv.tw. @a.dns.tw.

```
nasa.idv.tw.            86400   IN      NS      ns1.nasa.idv.tw.
nasa.idv.tw.            86400   IN      NS      ns2.nasa.idv.tw.
nasa.idv.tw.            86400   IN      NS      ns3.he.net.
```

- % dig ns nasa.idv.tw. @ns1.nasa.idv.tw.
- % dig ns nasa.idv.tw. @ns2.nasa.idv.tw.
- % dig ns nasa.idv.tw. @ns3.he.net.

- % dig any nasa.idv.tw. @ns1.nasa.idv.tw.
- % dig soa nasa.idv.tw. @ns1.nasa.idv.tw.
- % dig soa nasa.idv.tw. @ns2.nasa.idv.tw.
- % dig soa nasa.idv.tw. @ns3.he.net.

```
nasa.idv.tw.            86399   IN      SOA     nasa.idv.tw.
pschiu.cs.nctu.edu.tw. 2017030100 7200 600 1209600 2400
```

How to debug a name server – cont.

- % dig soa nasa.idv.tw. @8.8.8.8

```
nasa.idv.tw.            86399   IN      SOA     nasa.idv.tw.
pschiu.cs.nctu.edu.tw. 2017030100 7200 600 1209600 2400
```

- % dig soa nasa.idv.tw. @168.95.1.1

```
nasa.idv.tw.            86399   IN      SOA     nasa.idv.tw.
pschiu.cs.nctu.edu.tw. 2017030100 7200 600 1209600 2400
```

Tools – host

- host command
  - % host cs.nctu.edu.tw.
  - % host –t mx cs.nctu.edu.tw.
  - % host 140.113.1.1
  - % host –v 140.113.1.1

33