

Domain Name System (DNS)

Setting up an Authoritative Name Server

Ayitey Bulley
abulley@ghana.com

AINOG-2003

Objectives

- Write a valid zone file
- Explain how the SOA record is used
- The `named.conf` file
 - Configure a master nameserver for a domain
 - Configure a slave nameserver for a domain
- Choose a suitable secondary nameserver (RFC-2182)
- Reload a running nameserver and check the log files

AINOG-2003

The Zone Data Files

- Most entries are called DNS resource records (RR)
- Resource records must start in the first column of a line.
- The order in which RRs appear though not a requirement are as follows:

AINOG-2003

The Zone Data Files

- SOA records
 - Indicates authority for the zone
- NS records
 - Lists a name server for the zone
- Other records
 - A
 - Name-to-address mapping
 - PTR
 - Address-to-name mapping
 - CNAME
 - Canonical name (for aliases)

AINOG-2003

The Zone Data Files

- Comments make zone data files easier to read and understand
- Comments start with a semi-colon (;) and finish at the end of the line
- The nameserver ignores comments and blank lines.

AINOG-2003

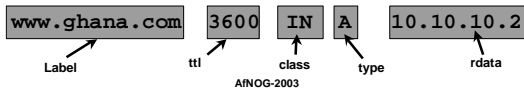
Setting the default TTL (RFC-2308)

- `$TTL` is used to set the default TTL for a zone
- It sets the TTL for all records in the file that follow it
- Nameservers supply this TTL in query responses, allowing other servers to cache the data for the TTL interval
- `$TTL` values are usually between 1-hour (1h) and 1-week (1w)
- `$TTL` is used for BIND version 8.2 and later.

AINOG-2003

Structure of Resource Records

- Resource records consist of it's name, it's TTL, it's class, it's type and it's RDATA
- TTL is a timing parameter
- IN class is widest used
- There are multiple types of RR records
- Everything behind the type identifier is called rdata



RRs in a Zone File

```

ripe.net. 2h IN SOA ns.ripe.net. olaf.ripe.net. (
    2003061000 ; Serial
    12h ; Refresh 12 hours
    4h ; Retry 4 hours
    4d ; Expire 4 days
    2h ; Negative cache 2 hours
)
ripe.net. 2h IN NS ns.ripe.net.
ripe.net. 2h IN NS ns.eu.net.

pinkie.ripe.net. 1h IN A 193.0.1.162
host25.ripe.net. 1h IN A 193.0.3.25
    
```

Label ttl class type rdata

AINOG-2003

Resource Record: SOA

```

net. 3600 IN SOA A.GTLD-SERVERS.net. nstld.verisign-grs.com. (
    2002021301 ; serial
    30M ; refresh
    15M ; retry
    1W ; expiry
    1D ) ; neg. ans. ttl
    
```

Master server Contact address

Serial number

Timing parameter

AINOG-2003

The named.conf file

- The named.conf file is the configuration file read when the named daemon starts up
- Is used to control the behavior of the named daemon

AINOG-2003

Named.conf:- Master Config. For Domain

```

options {
    directory "/etc/namedb";
};

/*
Comment
*/

// Another Comment Style
//

zone "domain.com" {
    type master;
    file "m/domain.com.bak";
};
    
```

Domain Name

Server Type

Zone Data File

AINOG-2003

Named.conf:- Slave Config. For Domain

```

options {
    directory "/etc/namedb";
};

/*
Comment
*/

// Another Comment Style
//

zone "domain.com" {
    type slave;
    file "s/domain.com.bak";
    masters { 192.168.1.1; };
};
    
```

Domain Name

Server Type

Zone Data File

IP Address of Master

AINOG-2003

Choice of Sec. Name Server (RFC-2182)

- See DNS Session 2

AINOG-2003

Reloading a running server

- To reload a running server the `ndc` utility is used (BIND 8)
- E.G.
 - # `ndc reload`
 - # `ndc reload <domain>`

AINOG-2003

Reload a running server & check the logs

- To reload a running server the `ndc` utility is used in BIND 8
- E.G.
 - # `ndc reload`
 - # `ndc reload afnogws.gh`
- After reloading the server you should check for errors in the log files
 - # `grep named /var/log/messages`

AINOG-2003

Some Common Errors

- Forgot to increment Serial Number
- Forgot to Reload Primary Name Server
- Slave Name Server Can't Load Zone Data
- Syntax Error in Configuration File or Zone Data File
- Missing Dot at the End of a Domain in Zone Data File

AINOG-2003

Some Common Errors

- Missing Root Hints Data
- Loss of Network Connectivity
- Missing Sub-domain Delegation
- Incorrect Sub-domain Delegation

- See DNS and BIND 4th edition, Chapter 14 on Troubleshooting DNS and BIND

AINOG-2003