TNE30019/TNE80014 – Unix for Telecommunications

Dynamically Updating DNS Entries

Dr. Jason But

Swinburne University

Outline

Dynamic DNS (DDNS)

- Updating DNS Database means changing zone file contents
- Changes to configuration require restart of `named`

Potential Problems

- Periods of unavailability
- Configuration errors must be fixed before coming back online
- If multiple servers, need to be careful with serial numbers

Dynamic DNS (DDNS)

- Update Database **without** restarting `named`
- Zone file updates are managed by DNS server

DHCP as Dynamic DNS Client

Not the only use for DDNS

- Just an example application
- Don't need DHCP to configure DDNS

Why DHCP + DDNS

- DHCP allocates IP addresses to hosts
- As IP address is allocated to new host
- We would like to update DNS server such that name of new host resolves to that IP address

Need to configure `dhcpd` and `named` to work together

- `dhcpd` must be able to (securely) connect to `named`
- `named` must be able to accept database changes from (remote) `dhcpd` server

Securing Updates

There are two alternatives for secure communications:

Encrypted Communications

Contents of messages between DDNS Client and server are encrypted

Authenticated Communications

Messages between DDNS Client and server are cleartext but messages are digitally signed

So which type would we like for DDNS?

Generating DDNS Update Key

`ddns-confgen -k ''KEY-NAME''`

- Prints to screen SHA256 symmetric key along with instructions
- Can use `-q` option to only get key and shell redirect save to file
- Key is used to secure communications between `named` and DDNS client
- Ensures updates can only be made by holders of key

More information on key generation

```
man ddns-confgen
```


Configuring BIND – `named.conf`

Specifying the key

```
key  "KEY-NAME" {
   algorithm  hmac-sha256;
   secret     "AbCdEfGhIj*WhAtEvEr=";
};
```

- `KEY-NAME` must match name specified during generation

Configuring zone to be dynamic

```
zone  "domain.hello." {
   type          master;
   notify        no;
   file          "database.filename";
   allow-update  {key KEY-NAME; }; };
```

- Reverse zones can also be specified as dynamic
- Should do both if DHCP will be client

BIND – Journal Files

- Once configured (and restarted) dynamic updates will be immediately processed
- After update is complete, queries for entries will be answered

Journal Files

- BIND now manages zone files, so zone files need to be updateable by `bind` user
- Binary journal file logs differences between saved zone file and current database

Writing to disk

- Database is in RAM for quick responses to queries
- Journal files are updated immediately after update to DB
- Zone file updated periodically or when `named` restarts

Configuring DHCP – dhcpd.conf

Specifying the key

```
key  "KEY-NAME" {
   algorithm  hmac-sha256;
   secret     "AbCdEfGhIj*WhAtEvEr==";
};
```

- NOTE: Same format as for named.conf

Tell dhcpd to update zone

```
ddns-updates on;
zone  "domain.hello." {
   primary    dns_server_ip_address;
   key        KEY-NAME;
};
```

- zone name must match an authoritative zone in DNS server
- After assigning address in matching zone, dhcpd will update forward and reverse zones in DNS server

DHCP+DNS Update Procedure

1. Workstation/PC is turned on
2. PC sends hostname and requests IP from DHCP server
3. DHCP server sends back IP lease
4. DHCP server contacts DNS server with hostname and allocated IP address
5. DNS server updates mapping between hostname and IP

- Requests to DNS server for that particular hostname will result in correct IP address being resolved
- Reverse resolution requests for IP address will resolve to hostname that currently holds that IP