IT 3100 - Domain Name System Revisited

Curtis Larsen

DSU-CIT

Fall 2013
Domain Name System - Revisited
   Load Balancing
   DNS Wildcard
   Named Configuration Checks
   Advanced Named Commands
   Named Access Control Lists
   Other DNS Thoughts
Load Balancing

- High traffic sites may produce too much traffic for one server to handle.
- This situation can apply to many services, but HTTP is an obvious one.
- In this case, it is easy to bring up extra servers with the same content.
- Clients need not be made aware, if the same FQDN points to multiple IP addresses.
- This can be accomplished with multiple A records for one name.
- DNS servers rotate the IPs when they return them.
- This rotation causes roughly even distribution of load.
Load Balancing Example

• Zone file entries:

  abe     IN     A     144.38.214.10
  abe     IN     A     144.38.214.11
  abe     IN     A     144.38.214.12

• Query 1:

  $ dig @144.38.214.2 abe.dsutux.us A | egrep ^abe
  abe.dsutux.us. 3600 IN A 144.38.214.10
  abe.dsutux.us. 3600 IN A 144.38.214.11
  abe.dsutux.us. 3600 IN A 144.38.214.12

• Query 2:

  $ dig @144.38.214.2 abe.dsutux.us A | egrep ^abe
  abe.dsutux.us. 3600 IN A 144.38.214.12
  abe.dsutux.us. 3600 IN A 144.38.214.10
  abe.dsutux.us. 3600 IN A 144.38.214.11
DNS Wildcard

- Some sites want all host names to be specified, or give negative hit.
- Some sites want to wildcard so unspecified names are all handled by a single record.
- For example, this is appropriate for sites with a large number of virtual hosts on the same web server.
DNS Wildcard Example

- Zone file entries:
  * IN A 144.38.214.13
  IN MX 10 mail

- Queries:
  $ dig @144.38.214.2 bob.dsutux.us A | grep ^bob
  bob.dsutux.us. 3600 IN A 144.38.214.13
  $ dig @144.38.214.2 barney.dsutux.us A | grep ^barney
  barney.dsutux.us. 3600 IN A 144.38.214.13
  $ dig @144.38.214.2 fred.dsutux.us MX | grep ^fred
  fred.dsutux.us. 3600 IN MX 10 mail.dsutux.us.
Named Configuration Checks

• /var/log/syslog shows errors when named is restarted.
• named.conf* and all zone files (db.*) can have syntax errors.
• Want to check for syntax errors before restarting named?
• named-checkconf or named-checkconf -z
• named-checkzone
Named Configuration Checks Examples

- Configuration file error:
  
  ```
  $ named-checkconf
  /etc/bind/named.conf.options:32: unknown option 'foo'
  /etc/bind/named.conf.options:33: unexpected token near '}'
  ```

- No configuration file error:
  
  ```
  $ named-checkconf
  $
  ```

- Test loading of zone files (no errors):
  
  ```
  $ named-checkconf -z
  zone dsutux.us/IN: loaded serial 2013102901
  zone games.horgoth.com/IN: loaded serial 2013100801
  zone 0-31.214.38.144.in-addr.arpa/IN: loaded serial 20131001
  zone localhost/IN: loaded serial 2
  zone 127.in-addr.arpa/IN: loaded serial 1
  zone 0.in-addr.arpa/IN: loaded serial 1
  zone 255.in-addr.arpa/IN: loaded serial 1
  ```
Named Configuration Checks Examples

- Zone file no error:
  
  ```
  $ named-checkzone dsutux.us /etc/bind/db.dsutux.us
  zone dsutux.us/IN: getaddrinfo(ns1.ubuntu.dsutux.us) failed: Temporary failure in name resolution
  zone dsutux.us/IN: getaddrinfo(ns2.ubuntu.dsutux.us) failed: Temporary failure in name resolution
  zone dsutux.us/IN: loaded serial 2013102901
  OK
  ```

- Zone file error:
  
  ```
  $ named-checkzone dsutux.us /etc/bind/db.dsutux.us
  /etc/bind/db.dsutux.us:103: unknown RR type 'bad'
  zone dsutux.us/IN: loading from master file /etc/bind/db.dsutux.us failed: unknown class/type
  zone dsutux.us/IN: not loaded due to errors.
  ```
Named Configuration Checks Examples

- Test loading of all zone files with error:

  $ named-checkconf -z
  /etc/bind/db.dsutux.us:103: unknown RR type 'bad'
  zone dsutux.us/IN: loading from master file /etc/bind/db.dsutux.us failed: unknown class/type
  zone dsutux.us/IN: not loaded due to errors.
  _default/dsutux.us/IN: unknown class/type
  zone games.horgoth.com/IN: loaded serial 2013100801
  zone 0-31.214.38.144.in-addr.arpa/IN: loaded serial 2013100201
  zone localhost/IN: loaded serial 2
  zone 127.in-addr.arpa/IN: loaded serial 1
  zone 0.in-addr.arpa/IN: loaded serial 1
  zone 255.in-addr.arpa/IN: loaded serial 1
sudo rndc commands:

- reload # reload all configuration files
- reload zone # reload one zone
- stats # write stats to /var/cache/bind/named.stats
- dumpdb # write cache to /var/cache/bind/named_dump.db
- flush # empty cache
- -h # see full list of commands
Named ACL

- In the named.conf* files, you can define and use access control lists.
- Allows for write once, use many configuration.
- Fix/update in one place.
- Already have any, none, localhost, and localnets.
Named ACL Example

- Configure caching lookup clients in named.conf.options:

```plaintext
cacl my_LAN {
    144.38.214.0/27;
};
...
allow-query { my_LAN; localhost; };
allow-recursion { my_LAN; localhost; };
...
```

- Configure slave IPs in named.conf.local:

```plaintext
cacl my_SLAVES {
    144.38.214.3;
};
...
allow-transfer { my_SLAVES; localhost; };
...
```
Other DNS Thoughts

• Bind9 can simultaneously serve as a caching lookup and authoritative server. Would there be times when it would be advantageous to separate the functionality into separate servers?

• Behind a single public IP, NAT configuration, multiple machines are running. How could you make the public internet see the single IP for translation, but the internal machines see the local network address for machines?

• Views.