BIND Best Practices from Day 1

05 October 2016

Logistics

- Webinar is scheduled for 1 hour
- This session will be recorded and posted at http://www.isc.org/webinars
- Participants are muted to improve audio quality for everyone.
- We want questions! Please enter into the WebEx Q&A tab
  - The presenter may defer some questions until the end of the presentation

Presenters

Eddy Winstead

ISC

Senior Sales Engineer

The Question

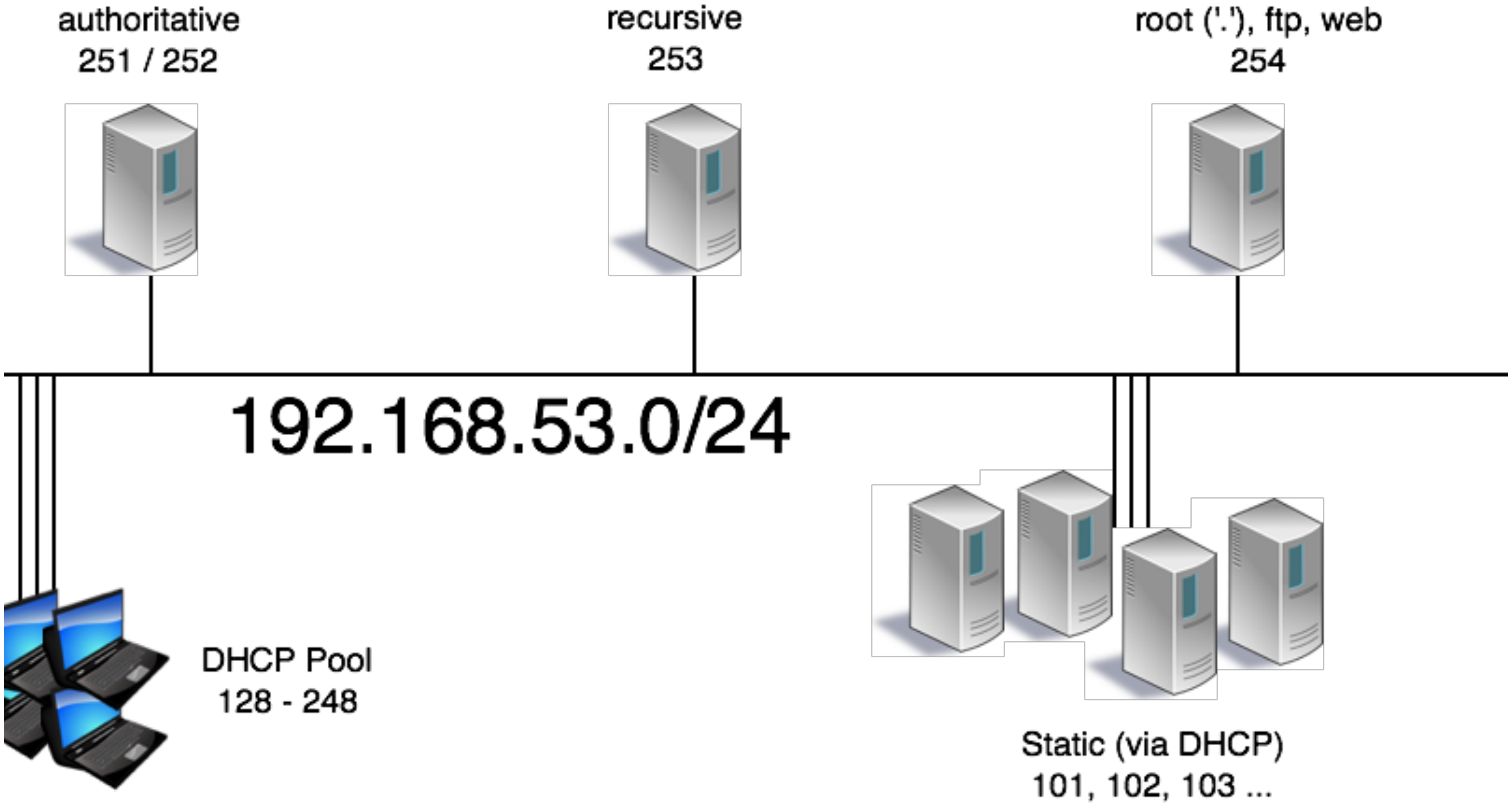
- What would you do if dropped into an existing organization to run their DNS?

First action, Recon!

- Actually, first action is freak out!
- 2nd action is caffeine, then deep breath and recon:

Any network or infrastructure diagrams available?

diagrams


authoritative
251 / 252
recursive
253
root ('.'), ftp, web
254
192.168.53.0/24
DHCP Pool
128 - 248
Static (via DHCP)
101, 102, 103 ...

Pick a nameserver, login!

- Running a current version of BIND?

  named –V
- OS?
- How is named started on this box? Does this match the version currently running?
- Is there a nanny script in use?

named -V

```
% named -V
BIND 9.8.4-P2 built with '--prefix=/usr' '--infodir=/usr/share/info' '--mandir=/usr/share/man' '--enable-threads' '--enable-getifaddrs' '--disable-linux-caps' '--with-openssl=/usr' '--with-randomdev=/dev/random' '--without-idn' '--without-libxml2'
using OpenSSL version: OpenSSL 0.9.8zd-freebsd 8 Jan 2015
```

On to named.conf

- Do the global options make sense?
- Basic security check:
  - TSIG secured zone transfers?
  - allow-transfer?
  - allow-query (is this an open resolver?)

Global options

```
options {
        directory "/etc/namedb/";
        dnssec-enable yes;
        dnssec-validation yes;
        allow-recursion { none; };
        allow-query { any; };
        allow-transfer { none; };
        notify no;
        key-directory "/etc/namedb/keys";
        max-journal-size 32k;
        zone-statistics yes;
        listen-on { 192.168.53.251; };
        listen-on-v6 { 2001:db8:100::251; };
        notify-source 192.168.53.251;
        notify-source-v6 2001:db8:100::251;
};
```

zone stanzas

```
zone "example.com" IN {
  file "example.com-zone";
  type slave;
  masters { 192.168.53.4; 192.168.53.8; };
  notify no;
};
```

logging

- Is the logging stanza sane and actually occurring?
- Check the config as well as the actual logs.
- Have a look at the system logs

logging stanza

```
logging {
        channel query_log {
                file "logs/query.log" versions 5 size 1M;
                severity info;
                print-time yes;
        };
        category queries { query_log; };
};
```

named-checkconf is your friend

```
$ named-checkconf –z

zone ./IN: loaded serial 121 (DNSSEC signed)
zone test.dnslab.org/IN: loaded serial 50
(DNSSEC signed)
```

rndc

- Is rndc configured?
- If not, ‘rndc-confgen –a’

- rndc status

- rndc notify zone
- rndc retransfer zone

Recon Repeat

- Repeat the prior Recon for all known nameservers!
- If diagrams were available, check to see if configs match stated functionality.

Authoritative specific

- Use external tools to check service:
  - DNSViz
  - dnscheck.iis.se
  - ednscomp.isc.org (firewall check)

Recursive specific

- Perform queries against these servers via dig

```
dig @192.168.53.53 www.example.com.
```

- Are they answering appropriately?

- Are they refusing appropriately?

Actions for Day 2

- Meet with the following teams:
  - Provisioning: how fast for new servers?
  - Operations: how’s life?
  - Security: about those firewalls…
  - Monitoring: alerting on?, peak traffic?
  - Architecture: future plans?
  - Management: support?

Questions

?

Thank You!

www.isc.org

info@isc.org