So You Inherited a DNS Server...

DNS Best Practices from Day One
How did the DNS find you?

- Because I knew *nix
- No one else would
- It just sort of happened…
- voluntold
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?
Pick a nameserver, login!

- Running a current version of dns software?
- OS?
- How is dns service started on this box? Does this match the version currently running?
- Is there a nanny script in use?
- ntp?
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 configuration

- 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;
  };
}
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.
SOME FUN THINGS YOU OUGHT TO KNOW...
DNS personality disorders

- Clients are often happy even when servers aren’t configured well.

- A bit passive-aggressive… things are acceptable until they’re not.

- OCD, clients and resolvers are content to retry and retry and retry…
There are rules... RFCs

https://www.isc.org/community/community/rfc/dns/

<table>
<thead>
<tr>
<th>RFC</th>
<th>Type</th>
<th>Status</th>
<th>Title</th>
<th>Bgn</th>
<th>Prot</th>
<th>Names</th>
<th>Ops</th>
<th>RR</th>
<th>Proxy</th>
<th>Stub</th>
<th>Auth</th>
<th>Res</th>
<th>Xfr</th>
<th>DDNS</th>
<th>DNSSEC</th>
</tr>
</thead>
<tbody>
<tr>
<td>882</td>
<td>Obsolete</td>
<td></td>
<td>Domain Names – Concepts and Facilities</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>883</td>
<td>Obsolete</td>
<td></td>
<td>Domain Names – Implementation and Specification</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>920</td>
<td></td>
<td></td>
<td>Domain Requirements</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>973</td>
<td>Obsolete</td>
<td></td>
<td>Domain System Changes and Observations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1032</td>
<td></td>
<td></td>
<td>Domain Administrators Guide</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1033</td>
<td></td>
<td></td>
<td>Domain Administrators Operations Guide</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1034</td>
<td>Standard</td>
<td></td>
<td>Domain Names – Concepts and Facilities</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1035</td>
<td>Standard</td>
<td></td>
<td>Domain Names – Implementation and Specification</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1101</td>
<td>Standard</td>
<td></td>
<td>DNS Encoding of Network Names and Other Types</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1123</td>
<td>Standard</td>
<td></td>
<td>Requirements for Internet Hosts – Application and Support</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1178</td>
<td>Informational</td>
<td></td>
<td>Choosing a Name for Your Computer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1183</td>
<td>Experimental</td>
<td></td>
<td>New DNS RR Definitions</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1348</td>
<td>Experimental</td>
<td>Obsolete</td>
<td>DNS NSAP RRs</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1401</td>
<td>Informational</td>
<td></td>
<td>Correspondence between the IAB and DISA on the use of DNS throughout the Internet</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1535</td>
<td>Informational</td>
<td></td>
<td>A Security Problem and Proposed Correction With Widely Deployed DNS Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1536</td>
<td>Informational</td>
<td></td>
<td>Common DNS Implementation Errors and Suggested Fixes</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1537</td>
<td>Informational</td>
<td></td>
<td>Common DNS Data File Configuration Errors</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1591</td>
<td>Informational</td>
<td></td>
<td>Domain Name System Structure and Delegation</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1611</td>
<td>Historic</td>
<td>Historic</td>
<td>DNS Server MIB Extensions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1612</td>
<td>Historic</td>
<td>Historic</td>
<td>DNS Resolver MIB Extensions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

© 2015 ISC
Less caffeine required...
DNS Resolution

Here is the address of www.example.com.

Local caching DNS server

www.example.com?
BACK TO YOUR NEW PREDICAMENT...
Authoritative specific

- Are zone transfers working?
- 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 and beyond

- 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?
Interconnectedness

- Get your boss to send you to DNS-OARC meeting(s)

- Join some lists:
  - dns-operations (DNS OARC)
  - nanog
  - etc
Questions
Thank You!

www.isc.org

info@isc.org