DNS Troubleshooting

SOA Fields

What is SOA? (Start of Authority)

```
    @       IN      SOA     ns1.thegummibear.com. root.ns1.thegummibear.com. (
```

- `@` represents `owner-name` or explicit domain name in FQDN format
  - i.e. You could replace `@` with `thegummibear.com.`
- `IN` stands for class of record `Internet` (some historic options)
- First FQDN is primary master (end with a dot)
- Second is email address of person responsible for zone (can't use @sign)

SOA Fields

```
    2017012001      ; Serial
    3600   ; Refresh
    300   ; Retry
```

- Serial = Has to be incremented
- Refresh = Time when slave will try to refresh zone from the master (recommend 1200-43200 seconds)
- Retry = Time between retries if slave fails to contact master (180-900)

SOA Fields

```
    241920  ; Expire
    60)   ; Negative Cache TTL
```

- Expire = When zone data is no longer authoritative (used by slave only)
  - Everytime refresh expires the slave will attempt to read the SOA record from the zone master (if sn is higher). If contact is made the expiry and refresh values are reset and the cycle starts again. If the slave fails to contact the master it will retry every retry period but continue to respond authoritatively for the zone until the expiry value is reached at which point it will stop answering authoritatively for the domain. (2-4 weeks)
- Negative cache ttl = If i request a domain that doesn't exist, client should cache for this long.

DNS Debugging

Steps (order matters)

- Configure master
- Configure slave
- Delegation (recursive lookups)
  - not just yet
  - Can we dig an A record for a host inside our domain?
  - How about outside our domain?

---

dig

Examples:

- `dig @nameserver.ip hostname RECORDTYPE`
- `dig @ns1.thegummibear.com www.thegummibear.com A`
- `dig @ns1.thegummibear.com www.nfl.com A` (will fail until we enable recursion)
- `dig @ns1.thegummibear.com thegummibear.com NS`
- `dig @ns2.thegummibear.com thegummibear.com SOA`

Master Troubleshooting

- Only 2 files we edited:
  - `/etc/bind/named.conf.local`
  - `/etc/bind/db.yourzonefile`
  - Did you increment Serial after making change?
- ALWAYS READ SYSLOG MESSAGES FOR ERRORS
- Test from same machine, different machine, test A records, NS, SOA,

---

Slave Troubleshooting

- Only edit `/etc/bind/named.conf.local`
- Check syslog
- dig, same checks as on master

Delegation (Recursive Lookups)

We haven't enabled this fully yet, but

- Glue records
- Make sure recursion is only allowed to members of your domain (restrict by ip address)

Misc

After making changes on registrar to point to your nameservers, may have to wait for cache to expire before changes will appear.

Do digs from top down to troubleshoot.