



Fancy lifestyle photo of
Jimmy Bergman
Loopia AB

Tools and Requirements for a Registrar

Who am I?

- Responsible for development at Loopia AB
- Loopia is the largest .SE registrar and DNS operator (in number of zones)
- Our name servers are authoritative for around 370 000 zones out of which 638 (Thu Oct 16 13:56:20) are DNSSEC enabled



Goal

- To get all .se domains handled by our name servers signed
- This will mean that a significant percentage of all .se domains get signed without involving getting lots of different organizations on board
- Which in turn increase usefulness of DNSSEC; thus giving other operators more incentive to get on board (at least that's what we're hoping for)



Requirements

1. The solution used needs to be able to handle addition/removal of at least 2000 zones per day.
2. We need to be able to handle at least in the order of 100 changed records per second
3. The changes should propagate to all authoritative name servers within a short timeframe (currently we do it within 1 minute)
4. The solution needs to be able to handle 400 000 zones without requiring insane amounts of memory
5. We need to be able to handle large query-loads, but not fantasy-numbers (something like 1000 – 10 000 qps)



Current solution (except for DNSSEC)

- Zones stored in a relational database
- We replicate data to a local BDB databases every minute
- Bind-DLZ is used to serve DNS data from the BDB database (queried live)
- This setup handles our requirements with a large margin
- Only hot zones are stored in memory (internal BDB cache). We get a large hit rate with only 256 KB cache.



Why not use stock Bind?

- Tried the following simple example on Bind 9.5.0-P2 today:
 - 400 000 zones, one file for every zone
 - Every zone had 15 records and was 861 bytes
 - Ran on dual core 2.4 GHz Intel Xeon with 1 GB ram process limit
- Got out of memory errors for 400 000 zones. Tried with 200 000 and got out of memory errors again. With 117 000 zones Bind used around 1 GB and worked.
- Startup (with 117 000 zones) took 6 min 24 seconds
- 'rndc reconfig' took 20 seconds
- During this time no queries where answered



Problems

- The DLZ zone storage backend doesn't support DNSSEC
- Example: The logic to send NSEC records together with NXDOMAIN is implemented in the default zone file backend.
- Good tools for handling signing policy, key-management, communication with parent (.se) and rollover is needed
- We have tools for automating this which we use with stock Bind for our current DNSSEC enabled domains
- These tools are not suitable for larger scale deployment



Solutions

- Our current plan is to develop or somehow arrange support for using DNSSEC in Bind-DLZ
- Timeframe is not currently set
- For signing / key management we place our hope in the OpenDNSSEC project
 - We will try to be of help in any way we can
 - I think that scope for developing tools should shift from *what does TLDs need* to *what is needed for getting broad DNSSEC deployment*
- Focusing on trying to persuade large DNS operators to sign all or a large number of their handled zones could mean that a large part of all zones got signed faster
- Since the same operators often have simple websites for administering zones it could also mean lowering the bar for registrants which want DNSSEC enabled zones



Questions?

