ccTLD Constituency  11.11.2001

Shared Secondary Services
Current Situation

- Secondary service is very often a voluntary agreement
- People who knows each other
- Standard configuration works
- Increase of load causes problems
Current Problems

• No defined service level agreements
• No coordinated monitoring of the systems according to
  • load
  • logging
  • security incidents
• No influence which software or hardware is used on the remote systems
• No information about personal or organizational changes
Current Problems

- Relying on standard zone transfer
  - usually no compressed transfers
  - no secure or redundant transfer
  - no emergency shutdown
- Problems occurred if zonefile size is bigger than the “standard”
- No optimal placing according to the global Internet infrastructure
- Problems only seen by an “outside view”
The Ideal World

TLD nameservers

- are ran by the responsible registry
- are running on different hardware
- are running under different software (at least releases)
- will be checked by different consistency algorithms
- are located on ideal places according to the needs of the TLD and the global Internet infrastructure
The Ideal World

The advantages are

• Security and reliability are controlled and documented by regular checks
• Through the heterogeneous implementation security incidents will not destroy the whole system
• Load problems will be seen and fixed in advance
• The reactions can be very fast by security or other incidents
• The staff maintaining the system is on a similar level and can be trained according to the current situation
Problems with the Ideal Approach

• Running servers on various places in the world is
  • expensive
  • a technical problem
  • a logistical problem
• Difficult as an initial approach

Exchange of information is necessary
The First Ideas

9/1999  Technical CENTR Meeting
11/1999 Meeting in Frankfurt
Workplan discussed
in 2000  First test installations in Frankfurt
(managed by ATNIC), Vienna and
Amsterdam (manage by DENIC)
in 2001  Workplan to organize servers in US
and Asia
SSS – Shared Secondary Service

• Server administered and financed by one TLD admin
• The service one system can be shared by a limited amount of registries
• Access can be granted for administrative purposes so each registry is able to monitor their services
Technical Principles

- several nameserver processes running in an own chroot environment
  - running on an own virtual IP interface
  - separate configuration files and zone files accessible for the TLD admin
  - own logfiles available
  - different software choice is possible
Advantages

• running 2-3 secondaries as SSS-admin and participate in other 6-9
  • up to 13 servers per TLD
  • financial and personal advantages
• possibility for same policy and software for each nameserver of the TLD
Advantages

- possibility for compressed or incremental zonefile exchange
- asap reactions possible
- separate statistic- and logdata available
Disadvantage

• not the “highest” security level - needs trust in the operators of the different zone (therefore a limit of 3-5 per box seems sensible)
• but a huge improvement of the current situation
• more security and reliability than the voluntary solution.
First Results

- On a test system bind 8.2 works fine
- Some minor modifications in the named control scripts need to be done to raise the security
- Automatical monitoring service must be developed
Questions