DENIC eG
DNS@DENIC

Sabine Dolderer (DENIC eG)
December 7th, 2006
Goals of DENIC's Name Server Setup

- Diversity of locations
- Diversity in technology (hardware/software)
- High stability, security and availability
- Reliability, security and authenticity of the information
- Support of scalability and extensibility through the setup
- Support of IPV6
Name Server Locations (NSLs)

11 name server Setups all over the world

5 Unicast Setups in Frankfurt (DE), Stuttgart (DE), Santa Clara (US), Amsterdam (NL), London (UK)

- 1 Anycast Setupt with Locations in Berlin (DE), Frankfurt (DE), Vienna (AT), Stockholm (SE), Tokyo (JP), Elmsford (US)

- 3 new locations until the end of 2006:
  - Seoul (KR) -> active
  - Miami (US) -> active
  - São Paolo (BR) -> nearly active
DENIC's Name Server Setup

- Redundant management server in the registry server locations (RSL)
- Administrative access to the NSL only over secured network layer
- Each NSL consists of one management server and at least three DNS server
- Identical hard- and software configuration within a NSL
- Diversity of hard- and software platform between different NSLs
- Diversity of the hosting and Internet provider
- 8 reloads a day
DENIC's Name Server Setup

- Zone file distribution incremental, secured, centrally controlled
- Alternative DNS-Software available on all servers
- Recent version of the zone files at least of a day are available to do rollback
- Load on each server has to be maximum 5% of the possible load to provide enough reserves
The NSLs operate at least three identical name servers per location.

**Extensive Redundancy / High Availability**
- Intra-location equivalence: equal HW and SW setup of the name servers within a location (several types of HW, SW & operating systems)
- Inter-location diversity: different HW, SW and operating systems are active across locations

**Excess Capacity**
- Switches at <1% of forwarding capacity and system load
- Processing reserve on all components

**Advanced Security**
- Out-of-band management only; Intensive logging
- Separate management interfaces on every component (heavily filtered)
- No management network access on any other interfaces
- Shut down of unused switch ports in "dead" VLAN
Nameserver Setup
Name Server Setup - Management

NSL - Out-of-Band (OoB) - Management

NSL 1

NSL OoB-Management Layer

Loghost
Power-Switch
Console Server
Switch

VPN-Gateway

Internet

Primary RSL

RSL OoB-Management Network

VPN-Gateway

Central NSL Management Server

NSL 2

NSL OoB-Management Layer

Loghost
Power-Switch
Console Server
Switch

VPN-Gateway

Secondary RSL

RSL OoB-Management Network

VPN-Gateway

Central NSL Management Server
Status (Zonefile) 06.12.2006

- Domains: 10.326.432 (incl. 330.773 IDN-Domains)
- Average 3.000 new domains each day
- Zone entries: 21.840.312
- Zonefile size: ~ 800 MB
- Used memory: ~ 2,5 GB (bind)
DNS Monitoring

- 24/7 automatic monitoring of key indicators
- Longtime capacity observation
- Consistent checks of the zones before delivery
- Authentication of the zones after delivery
- Integrated alarm system
- External, neutral monitoring by RIPE NCC (dnsmon.ripe.net)
Status of external Services
Monitoring: Load dns-us2

Nameserverauslastung dns-de3

Qmax (v240_bind8): 1000000

- srv1 MAX: 7.76 AVG: 2.38 MIN: 0.00
- srv2 MAX: 8.28 AVG: 3.46 MIN: 0.00
- srv3 MAX: 8.35 AVG: 3.88 MIN: 0.00

06.12.2006 13:25:14
Monitoring: Longtime Capacity (3 Year Stat)
## Monitoring Zonefile Distribution...

<table>
<thead>
<tr>
<th>IP-Adresse</th>
<th>SN Server erwartet</th>
<th>AA-Flag</th>
<th>Letzte Aktion</th>
<th>Status</th>
<th>Statusänderung um</th>
<th>Aktualisiert um</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.1.1</td>
<td>2008022042</td>
<td>true</td>
<td>Aktivierung Zone auf DNS-Server</td>
<td>SUCCESS</td>
<td>20.02.05 10:45:35</td>
<td>20.02.06 10:46:43</td>
</tr>
<tr>
<td>2.2.2.2</td>
<td>2008022042</td>
<td>false</td>
<td>Warte auf gestarteten DNS-Server</td>
<td>START</td>
<td>20.02.05 10:45:49</td>
<td>20.02.06 10:46:43</td>
</tr>
<tr>
<td>3.3.3.3</td>
<td>2008022042</td>
<td>true</td>
<td>Aktivierung Zone auf DNS-Server</td>
<td>SUCCESS</td>
<td>20.02.05 10:37:26</td>
<td>20.02.06 10:46:43</td>
</tr>
<tr>
<td>4.4.4.4</td>
<td>2008022042</td>
<td>true</td>
<td>Aktivierung Zone auf DNS-Server</td>
<td>SUCCESS</td>
<td>20.02.05 10:45:35</td>
<td>20.02.06 10:46:43</td>
</tr>
<tr>
<td>5.5.5.5</td>
<td>2008022042</td>
<td>false</td>
<td>Warte auf gestarteten DNS-Server</td>
<td>START</td>
<td>20.02.05 10:45:49</td>
<td>20.02.06 10:46:43</td>
</tr>
<tr>
<td>6.6.6.6</td>
<td>2008022042</td>
<td>true</td>
<td>Aktivierung Zone auf DNS-Server</td>
<td>SUCCESS</td>
<td>20.02.05 10:37:26</td>
<td>20.02.06 10:46:43</td>
</tr>
</tbody>
</table>

**strohbach@denic.de**
DNS: External Monitoring (dnsmon.ripe.net)
Thank you for your attention!

Any questions?