Best Practices for ccTLD Managers

Amman, November 2007

Kim Davies
Manager, Root Zone Services
Internet Assigned Numbers Authority

ICANN

iana

ccTLDs as a public trust

- ccTLDs are designated to operators who will operate them in the best interests of the local communities they serve.
- Operators should strive to tailor operations to best serve the users:
  - Ensure minimum technical standards are met
  - Strive for best practice
  - Operate with policy that suits local requirements

ICANN

#iana

Things we will consider

- Policy and Structure
  - ccTLD Managers (Sponsoring Organisations) responsible for setting the policy for ccTLDs
  - There are many different models
- Operational
  - Technical considerations
  - Best Current Practices

ICANN

iana

Preface

- These are some highlighted points on best practice
  - It is not exhaustive
  - In fact, it is a little random
- There is a wealth of information on ccTLD operations out there

ICANN

#iana

Policy and Structure

ICANN

iana

Management Structure

- Government?
- Not-for-profit?
- Outsourced?
- Most common:
  - Not-for-profit organisation
  - Appropriate membership from the community
  - Chartered for limited scope
  - Some kind of liaison with the government
  - Often light regulatory oversight

ICANN

#iana

Sales model

- Direct Registration
  - No middle man — easier to control most aspects of registration
- Registry-registry model
  - Requires an interface between the registry and registrar
  - Offload end-user interface from registry
- Both

Scope of registration

- Local or global sales?
- Decide what best serves the local community
- For global, consider legal aspects

Human Resources

- Administrative Point of Contact
  - Responsible for domain policy and operation
  - Represents the Local Internet Community and ensures the domain is run for the benefit of the country and its citizens
- Technical Point of Contact
  - Maintains the zone and makes sure systems run
- Programmers and Technical Staff
  - DNS experts, UNIX administrators, etc.
- Finance and Billing
- Lawyers

ICANN

iana

Structuring the TLD

- Flat or hierarchical?
  - Flat — simpler, equal access
  - Hierarchical — more domains, less disputes
    - Difficult to change later
- Two (.co.xy) or Three (.com.xy) letter second level domains?
  - Matter of preference
- Distributing the ccTLD
  - Delegate sub-domains to different registries

ICANN

iana

Dispute Resolution

- Local law prevails
- Alternative Dispute Resolution (ADR) designed to be more lightweight
- UDRP often used as a model
- http://www.icann.org/udrp/udrp.htm

Outsourcing

- There are an increasing number of companies that will provide service to TLD managers
  - Whole registry back-end providers
  - Authoritative name server providers
- ccTLD managers should understand how to run the services themselves before they outsource them
  - Allows you to adequately manage and monitor the performance of your suppliers
- Back-up strategies
  - What if your vendor disappears?
    - It has happened to major ccTLDs before (e.g. in 2002)

ICANN

iana

Operational and Technical

Technical requirements for registry

- Secondary Servers
- Redundant Networks
- Physical and electronic security
- Quality of service (24×7 availability)
- DNS software (BIND, NSD, etc.)
- Registry software
- Diagnostic tools (dig, traceroute, zonecheck, etc.)
- Registry-registrar protocol

ICANN

iana

Server Considerations

- Support technical standards
- Handle loads multiples of the measured peak
- Diverse bandwidth to support above
- Must answer authoritatively
  - Turn off recursion
- Can’t block access to a valid Internet host
- Consider turning off AXFR (zone transfer)

ICANN

#iana

Security Considerations

- Physical security
  - Limited to specific set of individuals
- Power continuity
- Fire detection and retardation
- Backups
- Don’t provide other services on the name servers (mail, ftp, web etc.)
- Keep on a network segment separate from public hosts
- Log attempts at intrusion
- Set your reverse DNS

ICANN

#iana

Communications

- Coordinate downtime between name server operators
- Coordinate backup between servers
  - Keep backups off site
- Exchange logs and statistics between NS operators
- Name server operator personnel should be on call 24×7

ICANN

#iana

Selection and Operation of Secondary NS

- Diversity diversity diversity
  - Don’t place on the same LAN/building/segment
    - Network diversity
    - Geographic diversity
    - Institutional diversity
    - Software and hardware diversity
- Host offline doesn’t mean the DNS doesn’t matter
- How many?
  - $2 \leq x \leq \approx 13$
  - x will vary on local circumstances

ICANN

iana

Resiliancy Considerations

- Functioning name servers are the most important criteria
- But it is not everything there is to a domain registry
  - Billing systems and interfaces
  - WHOIS server, web server
  - registrar APIs
- Consider what your service level targets are, and how your systems will cater to those targets
  - NS always on; others mostly on?

ICANN

#iana

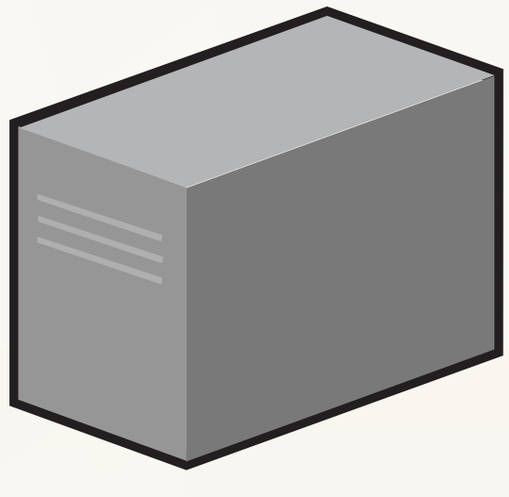
Separation of Services

Separation of Services

- Registries generally start small and organically evolve
- Separation of services means separating the logical functions and elements of the registry
- Two key benefits
  - security — clear delineation of services improves security by creating clear interfaces that can be controlled easily
  - scalability — by having clearly defined services, you can scale individual elements with little problems

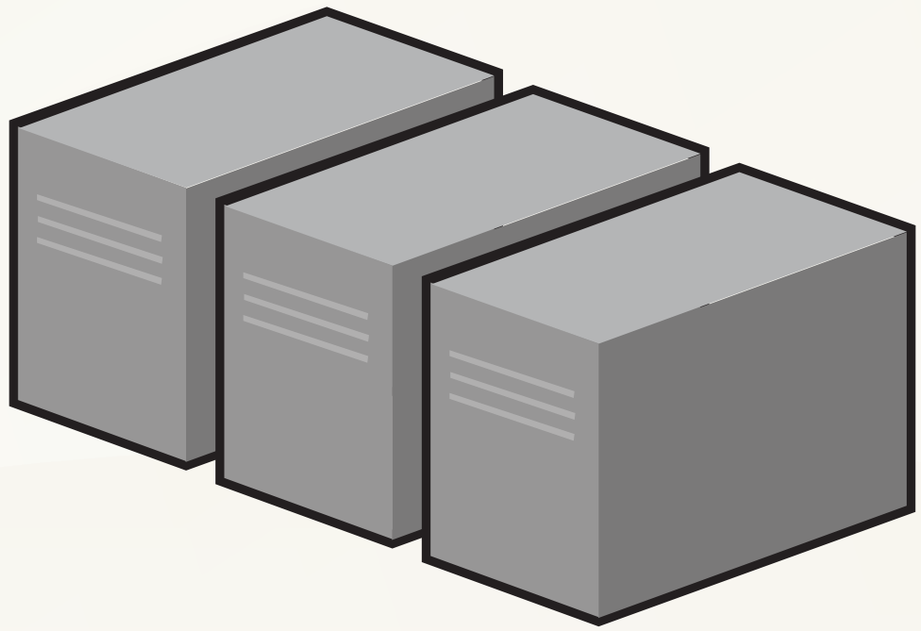
ICANN

iana



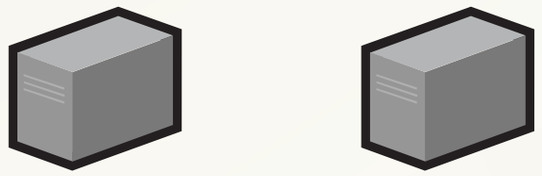
Registry operations - Day 1

- One server
- It does everything

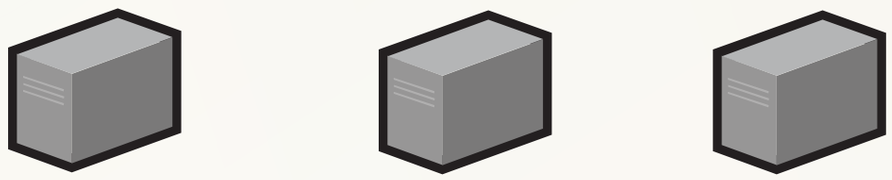


Registry operations - As we grow

- A few servers
- What goes where? How do we scale?



3rd-party



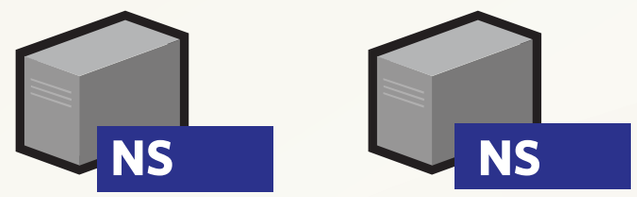
Public-facing

Back-office

Separate by exposure

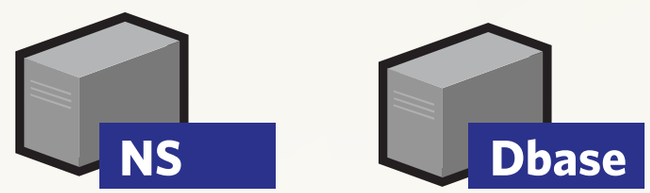
ICANN

iana



3rd-party

Public-facing

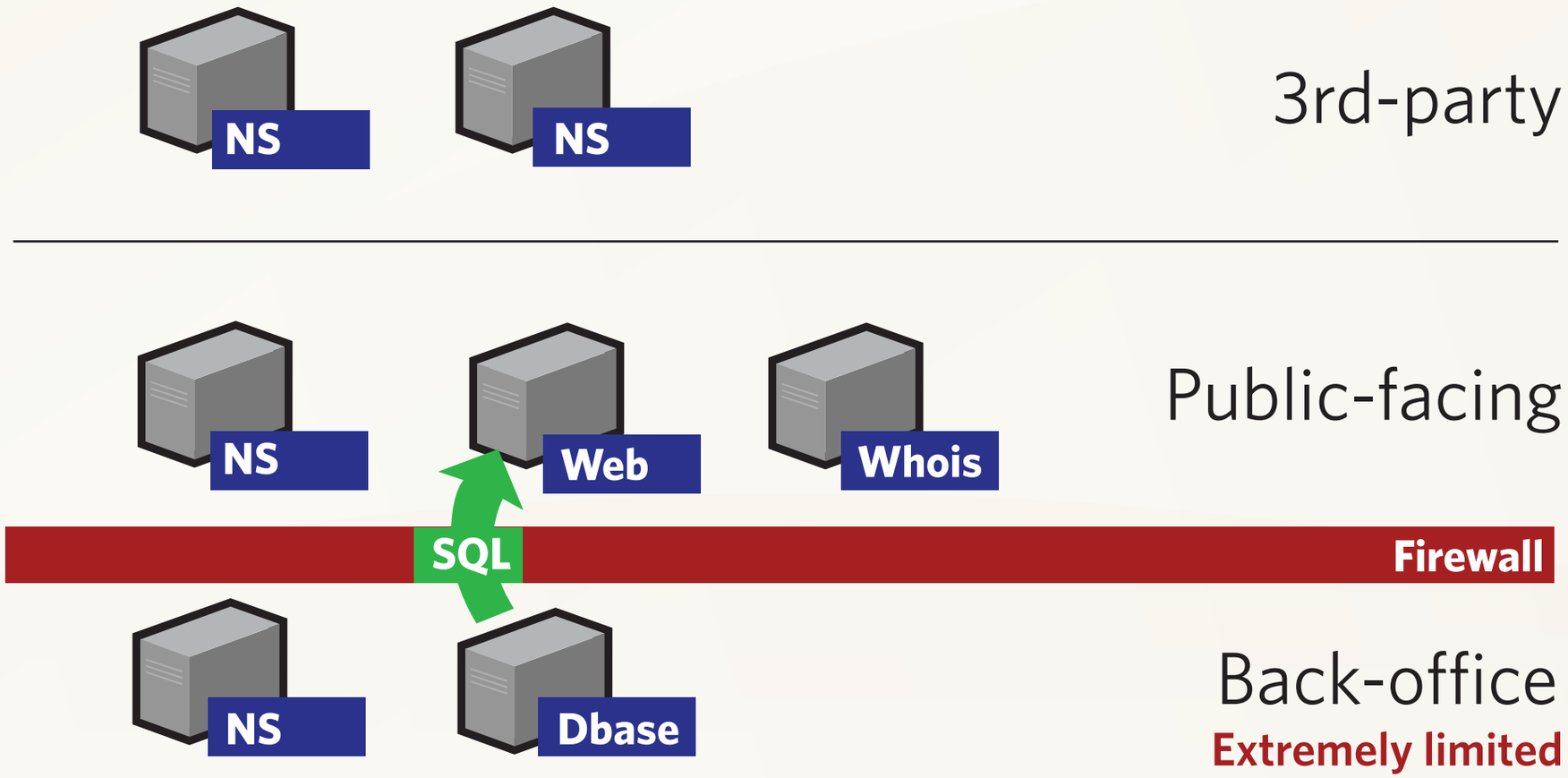


Back-office

Separate by Service

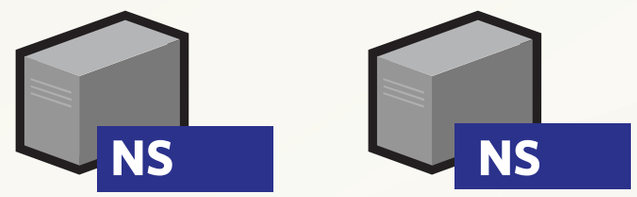
ICANN

iana



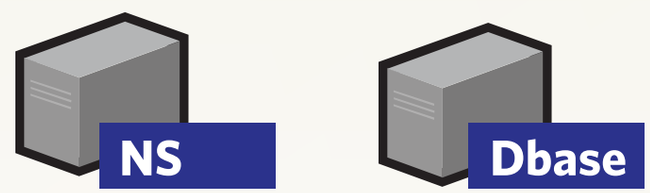
Security

- Isolated functions can be firewalled
- Explicit interfaces in and out of services



3rd-party

Public-facing

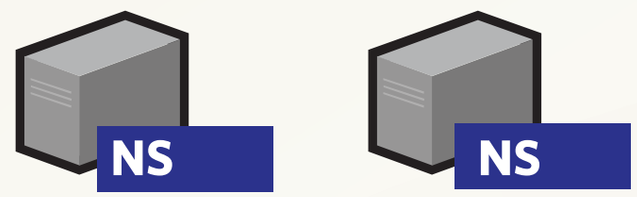


Back-office

Separate by Service

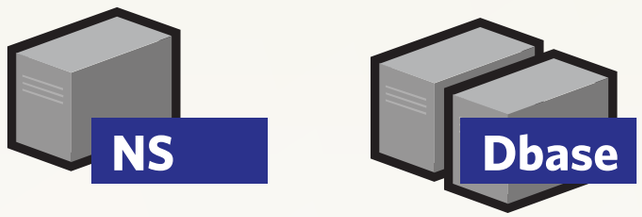
ICANN

iana



3rd-party

Public-facing



Back-office

Scaling services

- Easily grow based upon demand

ICANN

iana

Separation Summary

- Place each function/service in its own logical box
- Work out what interfaces the functions must have between each other
- Open firewall to connections along these explicit paths
- Provide clear APIs between the functions
- The clear APIs should allow scaling of particular functions by adding extra servers, etc.

ICANN

iana

Security Specifics

- Consider whether services are public-facing
- If they are not, place them in an area inaccessible from the public Internet
  - Constrain access as much as possible with a bastion host
- Consider finer-grained security
  - Is billing data more sensitive than WHOIS data?
    - Perhaps separate these services internally?

ICANN

iana

References

Documents

- RFC 2870 — Root Server Name Operational Requirements
  - Documents designed for root servers
  - Still useful for TLD operators - requirements are not that different
- RFC 2182 — Selection and Operation of Secondary DNS Servers
- ccTLD Best Practice Draft
  - See NSRC web site

ICANN

iana

Forums

- Regional organisations
  - APTLD (www.aptld.org)
  - CENTR (www.centr.org)
  - LACTLD (www.lactld.org)
  - AfTLD (www.aftld.org)
- ccNSO Information Sharing Working Groups
- www.ccnog.org

Thank you for your attention!

Kim Davies
kim.davies@icann.org