ccTLD Best Practices & Considerations

John Crain
Internet Corporation for Assigned Names and Numbers
ccTLD 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
Things we’ll consider

- Policy and Structure
  - ccTLD Managers (Sponsoring Organisations) responsible for setting ccTLD policy
  - There are many different models

- Operational
  - Technical Considerations
  - Best Current Practices (BCP)
Preface

- These are some highlighted points from a few key documents on best practice
  - It is not exhaustive
- There is a wealth of information on ccTLD Operations out there
  - Check meeting proceedings; regional organisation websites
Policy and Structure
Some options

- Government?
- Not for profit?
- Outsource?

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

- Direct registration
  - No middle man – easier to control most aspects of registration

- Registry–registrar model
  - Requires an interface between registry and registrar
  - Offloads end-user interface from registry

- Both
Scope of Registration

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

- Administrative Point of Contact
  - Responsible for making clear rules for domain policy and operation.
  - Should represent the local Internet community and ensure ccTLD run for benefit of 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
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) TLDs?
  - Matter of preference, really
- Distributed distribution?
  - Delegating sub domains to other parties
  - gov.xy, ed.xy
Other considerations

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

- There are an increasing number of companies that will provide TLD services to 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 manage and monitor performance of suppliers
- Back-up strategy! What if your supplier fails?
Operational and Technical
Technical Requirements for Registry

- Secondary Servers
- Networks (redundant)
- Physical and Electronic Security
- Quality of Service (24/7 availability!)
- DNS software (BIND, NSD, etc.)
- Registry software
- Diagnostic tools (ping, traceroute, zonecheck, dig)
- Registry Registrar Protocol
Server Considerations

- Support technical standards
- Handle load multiple times the measured peak
- Diverse bandwidth to support above
- Must answer authoritatively
  - Turn off recursion
- Should “NOT” block access from a valid Internet host
Security Considerations

- Physical security
  - Limited to a specific set of individuals
- Power continuity for 48 hours
- Fire detection and retardation
- Backups
- Don’t provide other services on the servers (mail, ftp, web etc.)
- Keep on a separate network segment from public hosts
- Log attempts at intrusion
- Set your reverse DNS
Communications

- Coordinate downtime between nameserver operators
- Coordinate backups between servers; keep backups off site
- Exchange logs and statistics between nameserver operators
- Nameserver operator personnel should be on call 24x7
Selection and Operation of Secondary DNS Servers

- Diversity, diversity and diversity
  - Don’t place all on the same LAN/building/segment
    - Network diversity
    - Geographical diversity
    - Institutional diversity
    - Software and hardware diversity
- Host offline doesn’t mean DNS doesn’t matter!
- How many?
  - $1 < x < 13$ (x will vary dependent on circumstances)
Resiliency Requirements

- Functioning name servers are the most critical/visible service
  - All other services also need to be considered
    - Billing
    - Whois server, webservers
    - Registrar APIs
- Consider your service level targets and how you will meet them
- DNS servers always on, other systems mostly on?
Separation of services
Registries generally start small and evolve

Separation of services means separating the logical functions and elements of the registry

Two key benefits:

- **SECURITY**: Clear separation of services is a manner in which to create logical security zones
- **SCALABILITY**: You can scale only the services that need to grow as they need to grow
- Separate by exposure!
  - Back-office, Public facing

- 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.
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?
More information
Forums

- Regional organisations
  - APTLD (www.aptld.org) – Your local group
  - CENTR (www.centr.org)
  - LACTLD (www.lactld.org)
  - AfTLD (www.aftld.org)

- Country Code Network Operators Group
  - www.ccnog.org
Sources for information

- RFC 1591 – ccTLD governance
- RFC 2870 – Root Server BCP
- Accountability Frameworks
  - [http://ccnso.icann.org/announcements/announcement-06jan06.html](http://ccnso.icann.org/announcements/announcement-06jan06.html)
- ccTLD Best Current Practice Draft
  - Currently a draft under development, comments welcome to the authors.
Thankyou for your attention!

John Crain
john.crain@icann.org