EPP and WHOIS

Jaromir Talir • jaromir.talir@nic.cz • 27.05.2014

CZ DOMAIN
REGISTRY

Agenda

- EPP – introduction
- EPP – commands
- WHOIS – introduction
- WHOIS - tricks

EPP introduction

- Extensible Provisioning Protocol
- RFCs – 5730, 5731, 5732, 5733, 5734
- Clients (Registrars) send commands to manipulate objects maintained by Server (Registry)
- Textual structured XML messages – easily readable
- Format of messages defined in XML schema

EPP introduction

- Different transport protocols
  - TCP/SSL
  - SMTP
- Three groups of commands:
  - Session commands
  - Query commands
  - Transform commands

EPP – session commands

- Login - start new session
  - username
  - password
  - prefered language
- Logout – close session
- All other commands must be issued inside the session

EPP – query commands

- Check – Is object available for registration?
- Info – Give me all data about object
- Poll – Do I have any message? I acknowledge reading of message
- Transfer – Is transfer in progress?

EPP – transform commands

- Create - Register new object
- Delete – Delete object
- Renew – Extend validity of object
- Transfer – Ask for transfer of object from current registrar
- Update – Change data of object

EPP – extensions for objects

- Domains
- Contacts
- Hosts
- DS records

EPP – FRED extenstions

- Nameserver set is completely different
- Few changes in contact detail
- Key sets instead of DS for DNSSEC
- Bulk info functions (all registrar domains, all domains by contact, all domains by nsset,...)
- Credit information
- Invocation of technical checks
- Sending authinfo to registrant

EPP – Authentication

- Username, password + client certificate
- Client certificate MD5 hash stored in registrar structure
- Certificate authority must be configured in Apache config file
- Security can be enhanced by firewall rules

EPP – Authorization

- Registrars can modify just object that they owns
- Domains registration permission is set per zone
- Registrars can query data of any object (except authinfo)

EPP – Session management

- Configurable number of parallel registrar session
- Configurable inactivity period after which is session closed

WHOIS - introduction

- Public interface for queries into registry
- RFC 3912
- Simple string query on port 43/TCP
- Simple text response
  - Some common habit responses

WHOIS

- Query can be for any object (domain, contact, ...)
- For ccTLD, address of whois server is hardcoded in whois client
  - whois nic.cz
- For any other object, user has to specify whois server
  - whois -h whois.nic.cz CZ-NIC

WHOIS

- By default, you will get all objects with the same handle
- You can specify type
  - whois -h whois.nic.cz -T contact CZ-NIC
- If you ask for domain, you will get all recursive information (contacts, hosts). You can disable this recursive behavior
  - whois -r nic.cz

WHOIS

- Reverse searching
- All domains owned by registrant
  - whois -h whois.nic.cz -- -r -i registrant JTALIR
- All domains delegated to this nameservers
  - whois -h whois.nic.cz -- -r -i nsset CZ.NIC
- Limits for max 100 records

WHOIS

- Rate limiting to prevent massive data collection
- Based on firewall rules
    - IP address or subnet

WHOIS - web

- Integrated into website
- Hyperlinks to linked objects
- CAPTCHA protection

Thank You

Jaromir Talir • jaromir.talir@nic.cz