FREE REGISTRY FOR ENUM AND DOMAINS

FRED

cz nic
cz domain registry

Jaromir Talir
http://fred.nic.cz
24.6.2012

Agenda

- Quick intro
- Features (objects, zone file generation, billing,...)
- Technologies (IDN, DNSSEC, ENUM)
- Interfaces (EPP, WHOIS, Webadmin)
- Components (DB, Corba servers, Apache,...)
- Customization
- How to become registry in 15 minutes?
  - Live installation od Fedora 17

Quick intro

About

- Full-blown software for running domain registry
- Multiple domains / any level with objects sharing
- Runs on Linux (plus other Un*xes?)
  - On Windows client only
- 100% free/open source
  - FRED code under GPLv2
  - Including components

APACHE PostgreSQL POWERED ORBit2 omniORB python™

- IPv6 supported

Quick intro

Availability

- http://fred.nic.cz
- Mailing list (archives)
- Available as:
  - Source code
  - DEB (Ubuntu LTS)
  - RPM (Fedora)
- Demo environment:
  - http://www.nic.cz/page/744/registracni-system/

Quick intro

Who is using FRED

- .CZ, 0.2.4.e164.arpa – Czech Republic (2007,2006)
  - .co.cz owner uses FRED for SLD
- .AO – Angola (2008)
- .TZ – Tanzania (2009)
- .CR – Costa Rica (2010)
- .FO – Faroe Islands (2010)
- .EE – Estonia (2010)
- Testing phase - Albania, Rwanda, Congo,...

Features

Overview

- Registry - Registrar - Registrant model
- Objects maintained in registry
- Zone file generation
- Notification of contacts and registrars
- Public requests
- Billing
- Fully audited interfaces
- Technical checks of nameservers

Features

Registry – Registrar - Registrant model

- No direct connection to domain registrants
  - Registry event notification
  - Few public request forms (request for authinfo, blocking request)
- Registrars are responsible for data they enter into registry
  - They have contract with registry
  - Obtain EPP access
- System registrar for own registry manipulation
  - Registration of our domains
  - Deleting expired domains
  - Doing administration changes in registry

Features

Objects in registry

- Primary objects in registry
  - Contacts – contact information
  - Nameserver set – group of nameserver hosts
  - Key set – group of DNSSEC keys
  - Domain – domain name
- Objects are share – any object can be linked to any object
- Full history of changes is archived

Features

Objects in registry - Contact

- Contact information
  - Used for notifications
  - Resolution of legal disputes
- Name and organization – ownership issue (person vs. org.)
- Physical address – letter communication
- Email and notify email – primary event notification
- Phone and fax – last resort call communication
- Identification (passport, birthday, id card, ssn, org. Ident)
- WHOIS disclose flags for all information

Features

Objects in registry – Nameserver set - NSSet

- List of hostnames for NS records in zonefile
  - Hostnames must be from existing TLDs
  - There must be at least 2 different hostnames, max 10
- Each hostname can have list of IP addresses
  - Used for glue records (A) when attached to domain of hostname
  - IP addresses can't be used when tld of hostname is not maintained in this registry
  - Both IPv4 and IPv6 are supported, max 10
- List of administrative contacts
  - Contacted in case of disabling domain or with results of technical checks
- Level of interest for technical checks

Features

Objects in registry – Key set

- List of keys for DS records in zonefile
  - Obtained in the form of DNSKEY record
- DS records are computed during zonefile generation
  - DS = SHA1(domain name + key)
  - Historically remains in database structure, but cannot be shared
- List of administrative contacts
  - Contacted in with results of technical checks

Features

Objects in registry - Domain

- Registrant – required contact
- List of administration contacts
  - Contacted together with Registrant when state of domain changes
- NSSet and KeySet
  - Can be empty – undelegated domains
- Expiration date
- Zone – set of preconfigured rules
  - Global TTL, SOA parameters and zone nameservers
  - Maximum and minimum (a step) registration period
  - ENUM flag and validation period
- Blacklist for unwanted domains

Features

Objects and registrars

- Same rules for domains, contacts, nameserver sets and key sets
- Creating registrar, updating registrar
- Designated registrar – only registrar to make changes
- Transfer supported by shared secret (authinfo)
  - Gain authinfo
  - Give it to new registrar
  - New registrar send EPP transfer command authorized with authinfo
- Holder can ask registry for sending authinfo
- Simplification by cross authorization (holder instead of domain)

Features

Object states

- Objects have associated states
- Automatic states changes according time and situation
  - Linked state for contacs, nssets, keysets
  - Expired, Outzone states for domains
- Manually set states – law enforcement
  - Protect objects against deleting, updating, transferring, renewal
  - Can put expired domain into zonefile or outzone regular domain
- Some state are internal, others are visible in EPP & WHOIS
- Registrants can request protection against transfers and updates

Features

Time considerations, expiration/renewal

- Expired domains are held for 30 days in zone
- Then domain is disable and for 30 days it stays in registry
  - Domain can be still renewed
- Then domain is deleted and made available to others
- Contacts, nssets and keysets are deleted after 6 month of not using it
  - Handles are protected for 2 month before new registration
- Registrants are notified about these changes by email
- All these numbers here are configurable

Features

Zonefile generation

- Rules when domain is generated into zone:
  - Must have nameserver set
  - Current date is before expiration date + 30 days
  - There are no requests to hold domain out of zone
- Process is invoked by cron job
- Just delegation (and secure delegation) in zones
  - NS + A, DS records
- Checks for number of changes to protect against bugs
- Hidden master is restarted with generated zone file
- Secondary servers download new version

Features

Notification of contacs

- Notification of EPP actions
  - Optional on presence of notify email in contact
- Notification about state changes of object
  - Email sent to registrant and administration contacts on expiration, removal from zone and deleting
  - Before deleting we sent them letter with warning
- Template system for email content
- Emails are archived
- Undelivered emails handling

Features

Notification of registrars

- EPP poll messaging system
  - Messages generated asynchronously
  - Registrars call periodically poll request and poll acknowledge
- Registrars are notified:
  - Configurable time before expiration or ENUM domain validation
  - Object owned by registrar is transferred or deleted
  - Credit drops under configurable limit
  - Result of technical checks invoked using EPP
  - Daily count of EPP requests (in case of request billing)

Features

Public requests

- Public can request some actions from registry
  - Ask for authinfo if registrar doesn't cooperate
  - Ask to block/unblock object against update and/or transfer
- Request forms are part of public web interface
- Some requests must be authorized
  - Using digitally signed email or officially signed letter
  - Must be checked and confirmed by administrator using webadmin

Features

Billing

- Prepaid and postpaid credit model
- Periodical scan for payments on our accounts
- Identification of registrar from payment data
- Advance invoice is generated with credit
- Each create and renew domain operation lower credit
  - According to price list, prices are per zone
  - If there is no enough credit, operation fail (in prepaid mode)
- EPP requests can be counted and paid
- Once a month we issue accounting invoice
  - List of operations in last month

Features

Technical checks

- Checks of nameservers in registry
  - Nameservers are reachable
  - They run DNS
  - They contain domains delegated to them
  - Heterogeneous systems on nameservers
- They are only informative!
  - Do not affect registration process
- Periodical or manually requested
  - Results of periodical tests sent to email of nameserver admins
  - Results of requested tests sent to registrar over EPP messaging

Technologies

IDN

- Internationalized Domain Names
- Almost full support
- Whois service is ready
- EPP interface blocks IDN registrations
  - No request for IDN in .CZ
  - But easy to enable it
- Character set checking is missing

Technologies
DNSSEC

- Secure extension to DNS based on cryptography
- .CZ is secured since October 2008
- Fully available in FRED...
  - Registration of subdomain keys (Key set object)
  - Zone file generation (DS records)
- ... but with support of other tools (Bind tools for DNSSEC)
  - TLD key generation (dnssec-keygen)
  - TLD zone signing (dnssec-signzone)

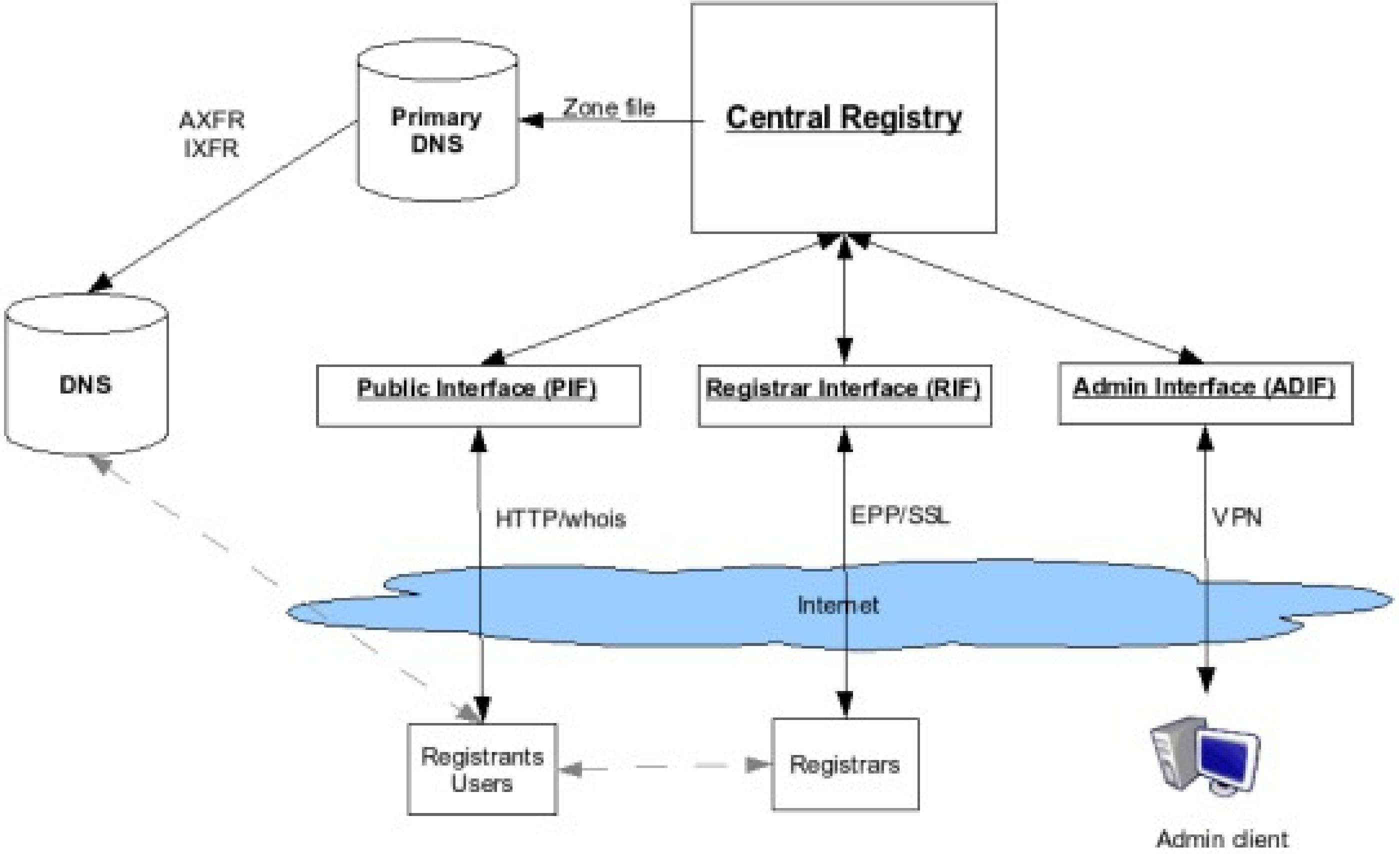
Technologies

ENUM

- Support Voice over IP technology
- Phone numbers registered as domains in DNS
  - +420 222 745 111 -> 1.1.1.5.4.7.2.2.2.0.2.4.e164.arpa
- DNS as dictionary (yellow pages) for phone numbers
- Fully supported in FRED
  - Unlimited level of domain registrations
  - Checking of overlapping registrations
  - ENUM domain has validation date (updated by registrar)

Interfaces

Schema



Interfaces

Registrar interface

- EPP protocol with slightly modified standard
  - Nameserver set is completely different
  - Few changes in contact detail
  - Key sets instead of DS for DNSSEC
- Nonstandard extensions
  - Bulk info functions (all registrar domains, all domains by contact, all domains by nsset,...)
  - Credit information
  - Invocation of technical checks
  - Sending authinfo to registrant
- Referential implementation of client in python

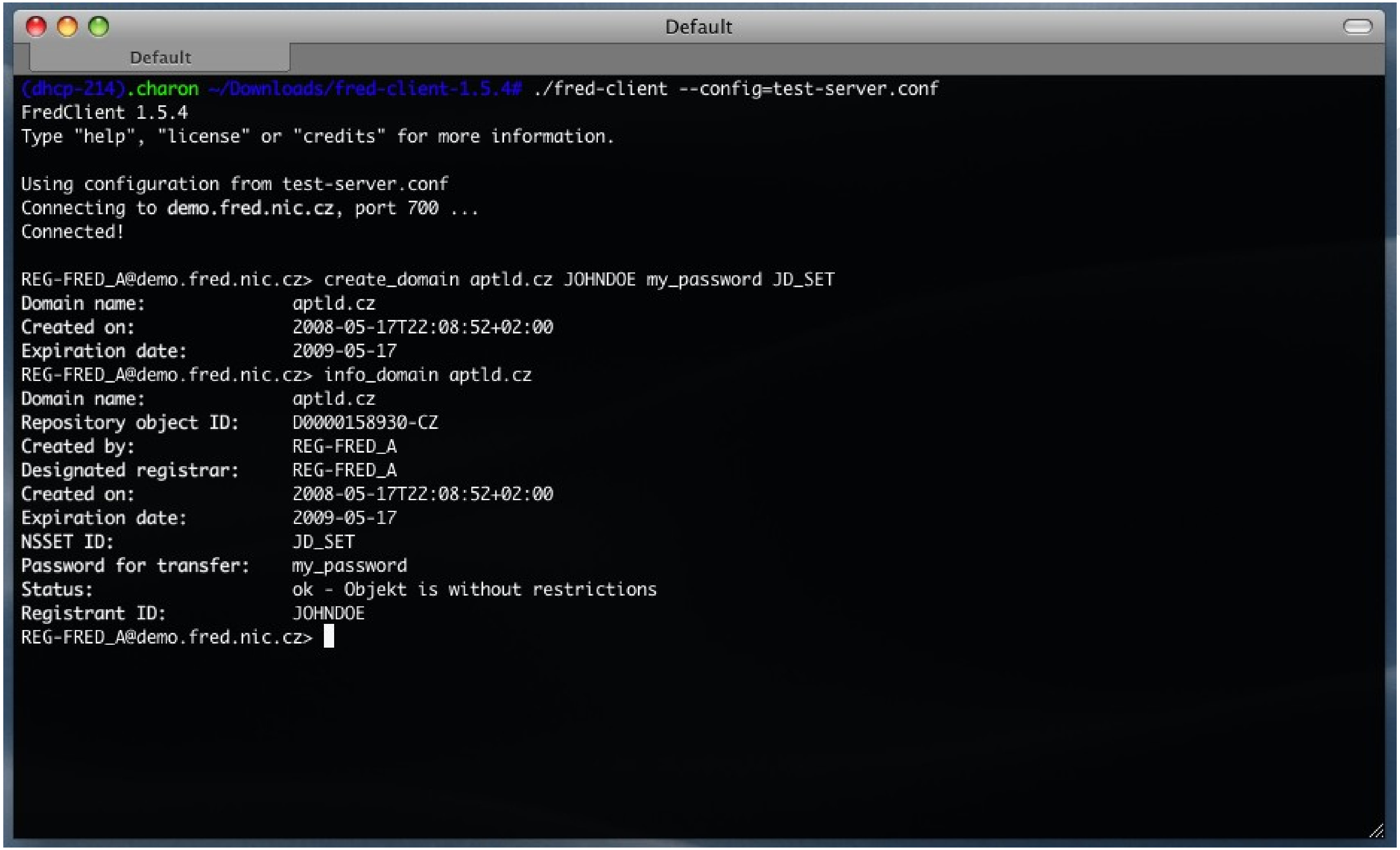
Interfaces

Registrar interface

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

Interfaces

Registrar interface



```
(dhcp-214).charon ~/Downloads/fred-client-1.5.4# ./fred-client --config=test-server.conf
FredClient 1.5.4
Type "help", "license" or "credits" for more information.

Using configuration from test-server.conf
Connecting to demo.fred.nic.cz, port 700 ...
Connected!

REG-FRED_A@demo.fred.nic.cz> create_domain aptld.cz JOHNDOE my_password JD_SET
Domain name:              aptld.cz
Created on:               2008-05-17T22:08:52+02:00
Expiration date:          2009-05-17
REG-FRED_A@demo.fred.nic.cz> info_domain aptld.cz
Domain name:              aptld.cz
Repository object ID:     D0000158930-CZ
Created by:               REG-FRED_A
Designated registrar:     REG-FRED_A
Created on:               2008-05-17T22:08:52+02:00
Expiration date:          2009-05-17
NSSET ID:                 JD_SET
Password for transfer:    my_password
Status:                   ok - Objekt is without restrictions
Registrant ID:            JOHNDOE
REG-FRED_A@demo.fred.nic.cz>
```

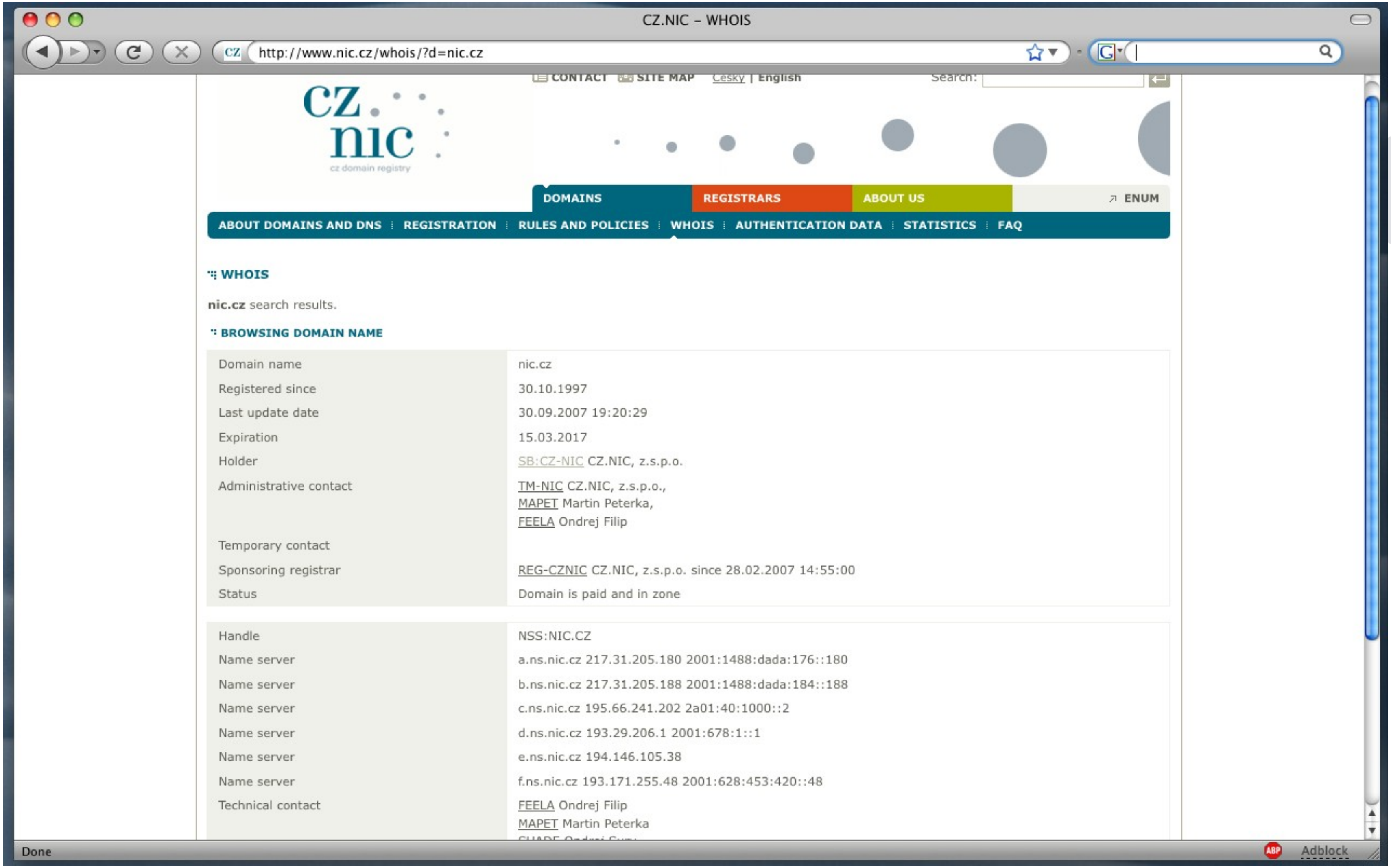
Interfaces

Public interface

- Two forms – web based, classical unix whois
- Common features
  - Lookup into all objects (domain, contact, nameserver set, registrars)
  - Privacy concerns (disclose flags about details of contact)
- Classical unix whois
  - Reverse search (domains by holder...)
- Web whois
  - Hypertext links between associated objects
  - CAPTCHA
  - Online list of registrars
  - Forms to apply for some service from registry

Interfaces

Public interface



WHOIS

nic.cz search results.

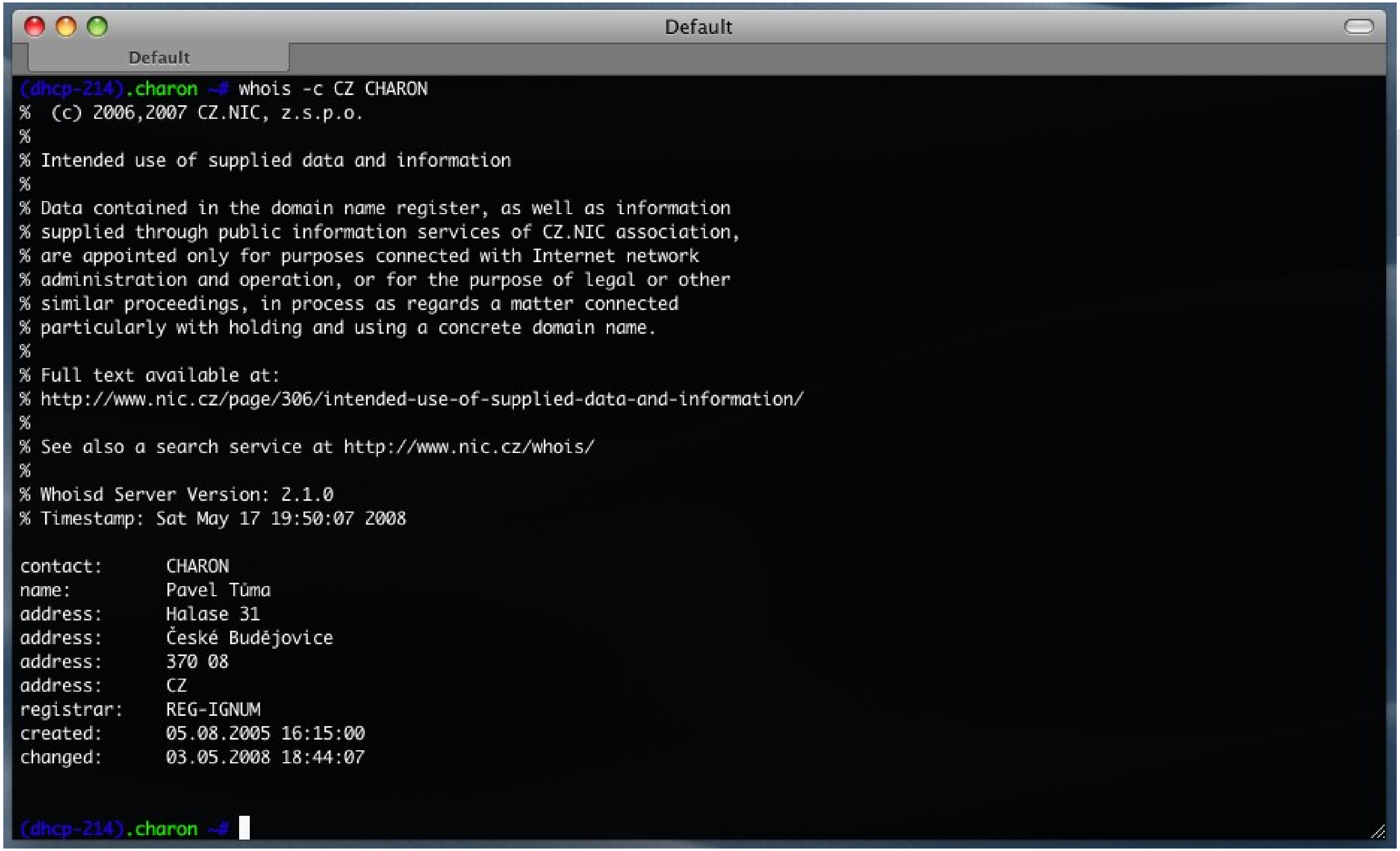
BROWSING DOMAIN NAME

Domain name	nic.cz
Registered since	30.10.1997
Last update date	30.09.2007 19:20:29
Expiration	15.03.2017
Holder	SB:CZ-NIC CZ.NIC, z.s.p.o.
Administrative contact	TM-NIC CZ.NIC, z.s.p.o., MAPET Martin Peterka, FEELA Ondrej Filip
Temporary contact	
Sponsoring registrar	REG-CZNIC CZ.NIC, z.s.p.o. since 28.02.2007 14:55:00
Status	Domain is paid and in zone

Handle	NSS:NIC.CZ
Name server	a.ns.nic.cz 217.31.205.180 2001:1488:dada:176::180
Name server	b.ns.nic.cz 217.31.205.188 2001:1488:dada:184::188
Name server	c.ns.nic.cz 195.66.241.202 2a01:40:1000::2
Name server	d.ns.nic.cz 193.29.206.1 2001:678:1::1
Name server	e.ns.nic.cz 194.146.105.38
Name server	f.ns.nic.cz 193.171.255.48 2001:628:453:420::48
Technical contact	FEELA Ondrej Filip MAPET Martin Peterka SUADE Ondrej Sury

Interfaces

Public interface



```
(dhcp-214).charon ~# whois -c CZ CHARON
%  (c) 2006,2007 CZ.NIC, z.s.p.o.
%
% Intended use of supplied data and information
%
% Data contained in the domain name register, as well as information
% supplied through public information services of CZ.NIC association,
% are appointed only for purposes connected with Internet network
% administration and operation, or for the purpose of legal or other
% similar proceedings, in process as regards a matter connected
% particularly with holding and using a concrete domain name.
%
% Full text available at:
% http://www.nic.cz/page/306/intended-use-of-supplied-data-and-information/
%
% See also a search service at http://www.nic.cz/whois/
%
% Whoisd Server Version: 2.1.0
% Timestamp: Sat May 17 19:50:07 2008

contact:       CHARON
name:          Pavel Tůma
address:       Halase 31
address:       České Budějovice
address:       370 08
address:       CZ
registrar:     REG-IGNUM
created:       05.08.2005 16:15:00
changed:       03.05.2008 18:44:07


(dhcp-214).charon ~#
```

Interfaces

Administration interface

- Command line tools support regular processes
- Web based, mainly for making queries into database:
  - Current and historical data of domains, contacts, nssets and keysets
  - All requests into registry
  - Communication history (emails, sms, letters)
  - Invoices and payments
- Export to CSV
- Few update features:
  - Registrar creation and update
  - Processing of public requests created through public interface
  - Processing of payments

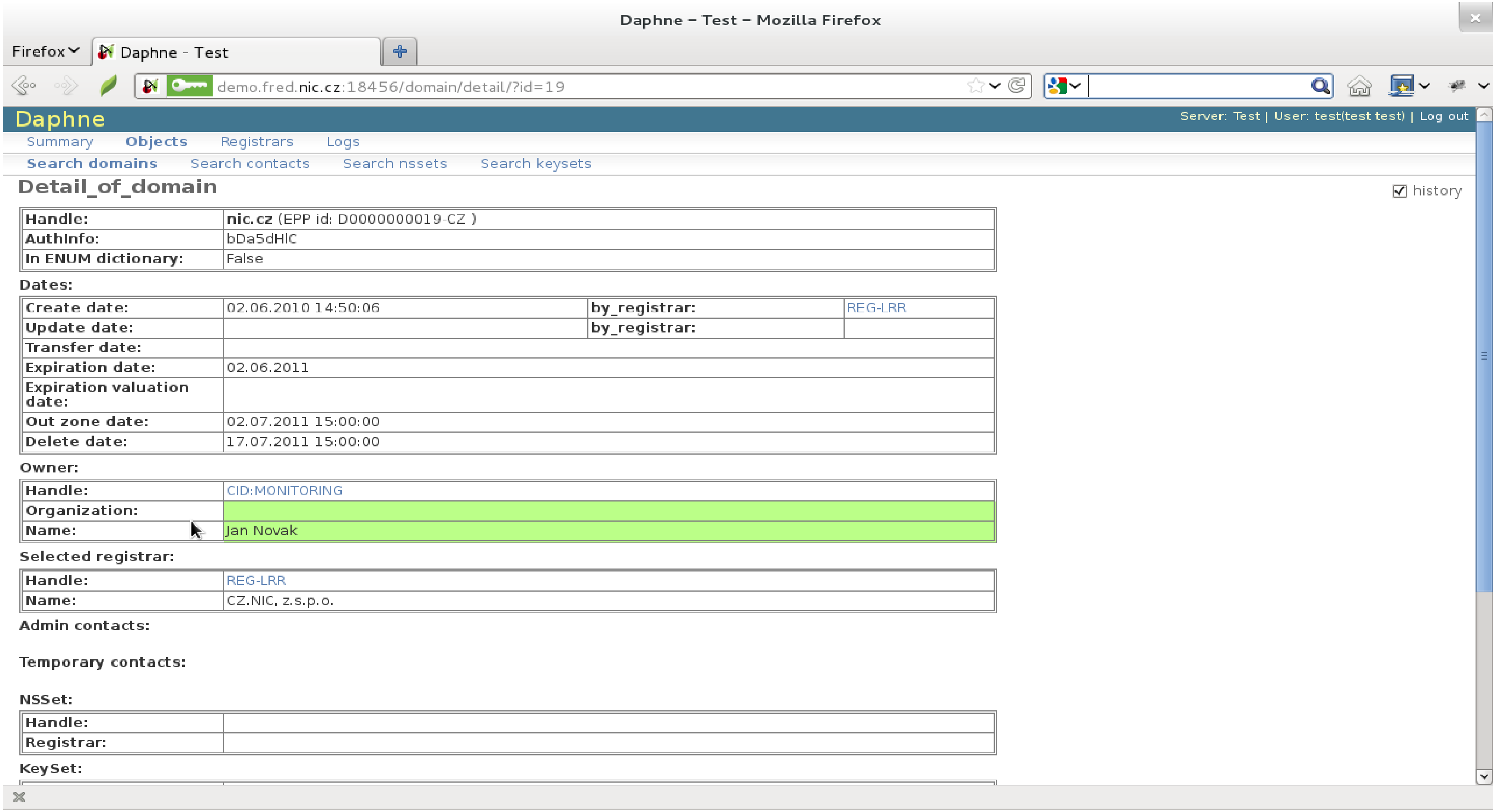
Interfaces

Administration interface

- Authentication
  - Either disabled or LDAP passwords
- Authorization
  - Simple text file mapping usernames to permissions
  - Individual permissions for object types and update functions

Interfaces

Administration interface



Daphne – Test – Mozilla Firefox
Firefox
Daphne - Test
demo.fred.nic.cz:18456/domain/detail/?id=19
Daphne
Server: Test | User: test(test test) | Log out
Summary
Objects
Registrars
Logs
Search domains
Search contacts
Search nssets
Search keysets

Detail_of_domain

☑ history

Handle:	**nic.cz** (EPP id: D0000000019-CZ)
AuthInfo:	bDa5dHlC
In ENUM dictionary:	False

Dates:

Create date:	02.06.2010 14:50:06	**by_registrar:**	REG-LRR
Update date:		**by_registrar:**	
Transfer date:			
Expiration date:	02.06.2011		
Expiration valuation date:			
Out zone date:	02.07.2011 15:00:00		
Delete date:	17.07.2011 15:00:00		

Owner:

Handle:	CID:MONITORING
Organization:	
Name:	Jan Novak

Selected registrar:

Handle:	REG-LRR
Name:	CZ.NIC, z.s.p.o.

Admin contacts:

Temporary contacts:

NSSet:

Handle:	
Registrar:	

KeySet:

Components

Database

- PostgreSQL >= 8.1
- Schema contained in fred-db package
- Two schemas:
  - Fred tables
  - Audit tables (Request logger) – monthly partitioned
- Replication to second locality using Slony
- Daily backups using pg_dump utility
- Size (after 6 years)
  - Base - 15 GB (5 mil. objects with 10 mil. history records)
  - Mail archive – 30 GB (11 mil. archived emails)
  - Request logging – 130 GB/month (25 mil. records/month)

Components

Application corba servers

- CORBA – middleware technology for remote procedure calls
    - OmniORB – C++ and Python implementation
    - OrbIT – C implementation (in apache modules)
- OmniNames – Nameservice for CORBA servers
    - Servers register their functionality
    - Clients seek for references to these services
- C++ servers
    - fred-rifd for registrar functionality
    - fred-pifd for public interface functionality
    - fred-adifd for administration functionality

Components

Application corba servers

- C++ servers
  - fred-logd for request logging functionality
  - fred-msgd for messaging functionality (sms, letters)
  - fred-mifd for new mojeid project funcionality – not needed
- Python server – fred-pyfred
  - Zonefile generation backend
  - Email generation / sending backend
  - Technical checks backend
  - File archiver

Components

Scripts

- genzone_client
  - Python script to be installed on master DNS server
  - It is CORBA client that gets all domains to be in zone and generates zonefile
  - Can invoke post-generation scripts
- fred-admin
  - C++ binary for internal administration
  - Mainly used for regular jobs:
    - domain expiration, notification, billing
  - Useful for nitialization (configuring zone, registrars,...)

Components

Scripts

- transproc
  - Python script for bank transaction processing
  - From different sources creates general payment XML
  - General XML is uploaded using fred-admin
- doc2pdf
  - Python script for PDF file generation
  - Wrapper around reportlab PDF library
  - Contains templates for invoices, letters, public request forms

Components

Cron

- Many regular procedures are scheduled using Cron
- Zonefile generation
  - Using genzone_client
- Domain expiration and unused objects handling
  - Processing notification, disabling and deleting of domains
  - Deleting of unused unlinked contacts, nssets, keysets
  - Using fred-admin –object_regular_procedure (at least daily)
- Bank transaction polling
  - Usign transproc

Components

Apache modules

- Reuse apache connection handling, ssl layer etc..
- Module mod-eppd
  - Listen on port 700 for incoming EPP requests over SSL
  - Parse XML in EPP requests and transform them to backend function calls
  - Logging of requests
- Module mod-whoisd
  - Listen on port 43 for incoming WHOIS requests
  - Transform them to backend function calls
  - Logging of requests
- Module mod-corba
  - Common CORBA client functionality for both modules

Components

Web components

- Web whois
  - Set of python scripts + apache + mod_python
  - Simpletal template engine for presentation
  - Python CORBA client for communication with backend
  - Logging each request
- WebAdmin (aka Daphne)
  - Standalone fred-webadmin-server application
  - Could be also embedded into apache + mod_python
  - Written using python cherrypy framework

Components

EPP client

- Python script for EPP communication
  - Given to registrars
  - Used for internal administration
- Set of libraries to be embedded into registrar systems
- Command line application
  - Includes help
  - History of actions
  - Interactive parameter filling (using: !command_name)

Customization

Overview

- Manual at this time
- Zone configuration
  - Name, SOA headers, periods
  - Admin command line tools to generate templates
- Email templates
  - ClearSilver templating system
- PDF documents
  - ReportLab templating system
- Object state change parameters
- Configuration options of application

How to become registry

Installation

- Install OS Fedora 17 (http://www.fedoraproject.org)
- Configure installation mechanism to know about our repository with FRED packages:
  - yum install http://archive.nic.cz/yum/fred/17/x86_64/fred-repo-1.0-1.noarch.rpm
- Install all fred components
  - yum install fred-*
- Install bind nameserver
  - yum install bind
- If you have just installed PostgreSQL, it must be initialized:
  - /usr/bin/postgresql-setup initdb

How to become registry

Startup

- Start all servers:
  - service omniNames start
  - service postgresql start
  - service fred-server start
  - service httpd start
  - service fred-webadmin-server start
  - service named start

How to become registry

Configuration

- Configure your zone for zone file generation:

  -
    ```
    /usr/sbin/fred-admin --zone_add --zone_fqdn=test
        --ex_period_min=12 --ex_period_max=120 --ttl=18000
        --hostmaster=hostmaster@nic.co  --refresh=10600
        --update_retr=3600 --expiry=1209600 --minimum=7200
        --ns_fqdn=ns.nic.test
    ```

  -
    ```
    /usr/sbin/fred-admin --zone_ns_add --zone_fqdn=sv
        --ns_fqdn=ns.nic.test --addr=111.111.111.111
    ```

How to become registry

Configuration

- Create new Bind configuration files for new zones:

  ```
  /usr/bin/genzone_client -g /etc/named.fred.conf -z /var/named
  ```

- Update Bind configuration to include new config file:

  ```
  echo 'include "/etc/named.fred.conf";' >> /etc/named.conf
  ```

- Update Bind configuration to accept queries:

  ```
  sed -i 's/\tlisten-on/\t#listen-on/g' /etc/named.conf
  sed -i 's/\tallow-query/\t#allow-query/g' /etc/named.conf
  sed -i 's/recursion yes;/recursion no;/g' /etc/named.conf
  ```

- Configure regular zone file generation:

  ```
  echo "*   *   *   *   *  root ( /usr/bin/genzone_client -z /var/named -o; /etc/init.d/named restart )" > /etc/cron.d/fred-genzone
  ```

How to become registry

Remaining

- Configure price of domain for each zone
- Customize components
  - Change style and translation of emails
  - Change style of PDF generated files
- Migration of data
  - Use FRED registry client

How to become registry

Relyable service

- Multiple authoritative nameservers
  - Configure distribution of zone files
- Dual localities
  - Configure replication of database
- Monitoring
  - Setup monitoring procedures

Thank you

Questions?

Jaromir Talir

jaromir.talir@nic.cz

http://fred.nic.cz