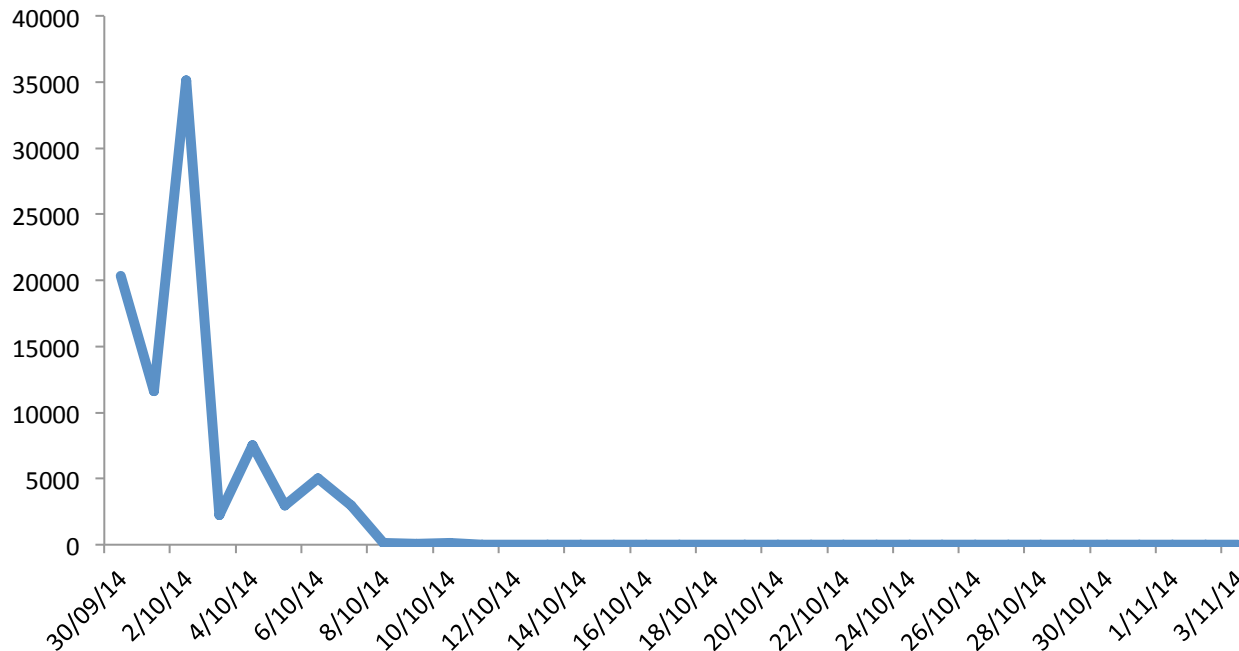


Registry Update



Second Level Registrations

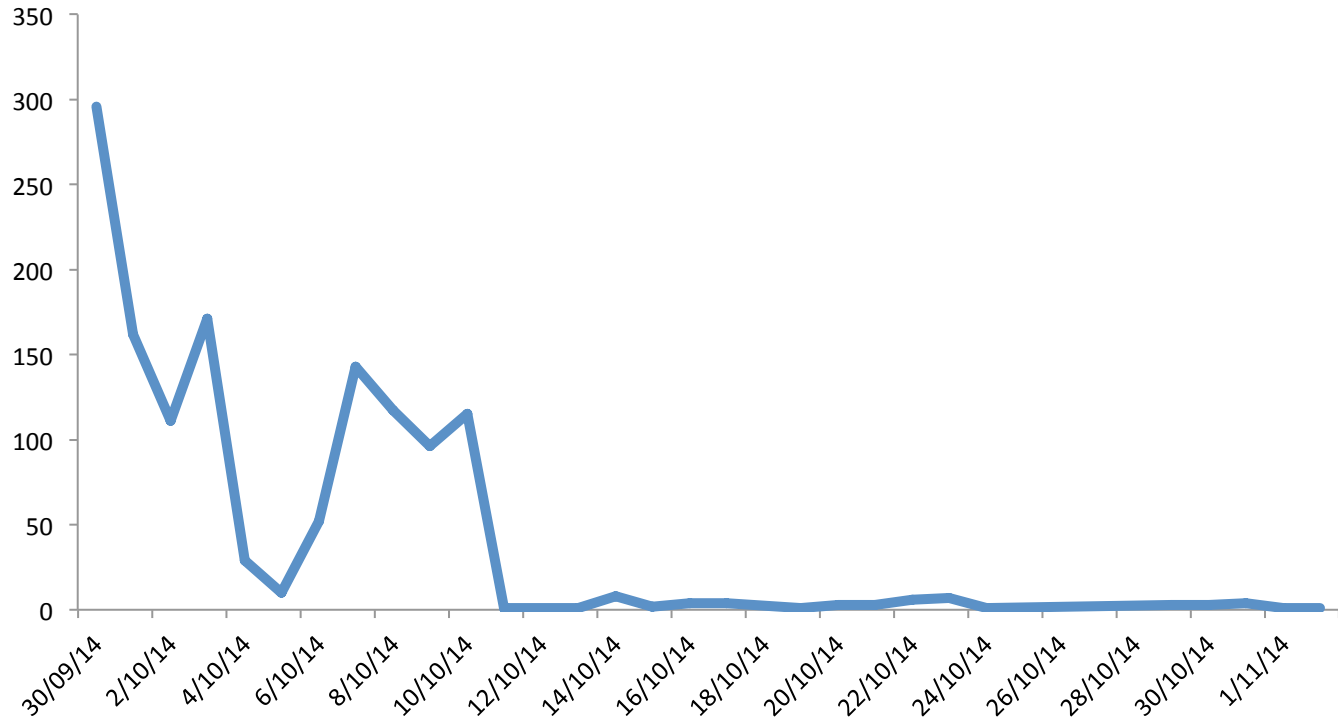
2LR Create Error Count



DomainCreate second level registration error counts by day for PRE domains. High numbers for the first week.



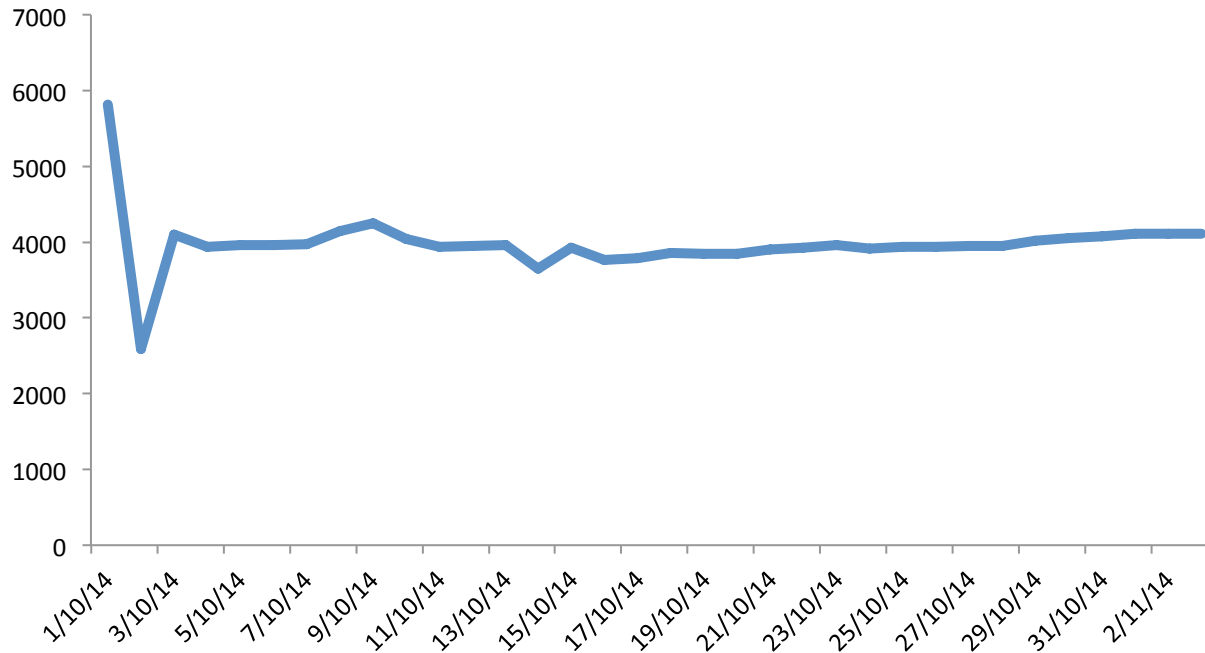
2LR Create Error Count minus 3 registrars



High number of errors from the previous slide due to 3 registrars. DomainCreate second level registration error counts very low after the first couple of weeks since Go-Live.



2LRs without nameservers



Large number of 2LRs have no name servers. This number has remained surprisingly consistent around 4,000. The number of .co.nz domains that have no nameservers is less than a 1,000. Possibly due to the transfer/registration process ignoring nameservers and registrars not updating the domain after registration?



EPP - Extensible Provisioning Protocol

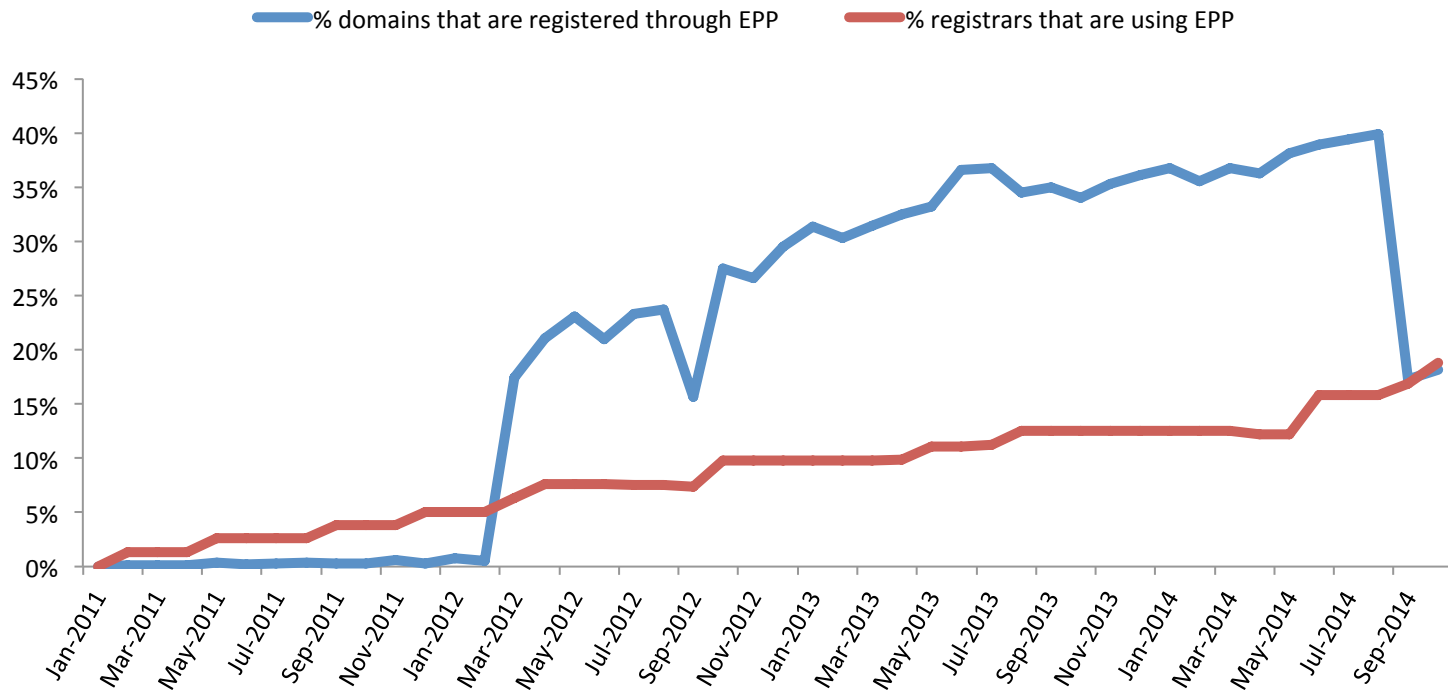
- Flexible XML based protocol
- Adopted by a large number of domain name registries
- NZRS EPP server is no longer a proxy – using our internal language
- Some minor SRS transactions are not supported eg AccountDetailsQry



What you need to do to connect via EPP

- Communication via encrypted SSL connection over TCP/IP
- Registrars need to provide a CSR
- NZRS will return the certificate signed by the NZRS CA
- IP address(es) used for communication with the EPP server need to be whitelisted by us
- Registrars also require a password and login id





- EPP deployed in January 2011. Steady increase of registrars using EPP since then.
- Several registrars moved from SRS to EPP in March 2012.
- Sharp drop in % of domains registered through EPP in September 2014 – probably due to some EPP registrars not offering 2LR registrations?



Web Services

Domain Name Availability

Releasing Domains List



Domain Name Availability

This API is designed to provide registrars with a simplified process for availability checks via a web interface.

Returns the domain availability and status code from the registry for domains specified in domain parameters.

ACLs: Whitelist for Registrar IP address

Method: GET

Resource URL: <http://srs-json.srs.net.nz/1.0/availability>

Parameters:

- **string** - A single string to be looked up across all 2LDs.
- **domains[]** - One or more domains to be checked for availability.



Domain Name Availability

Response details

Response key	Valid response data
status	Alphanumeric human readable string explaining the status code
code	Numeric status code
domain	The domain name as stored in the register
original	If the domain has an IDN, this field will contain the domain name in the script intended by the registrant, encoded in UTF-8.



Example Request

GET	http://srs-json.srs.net.nz/1.0/availability
GET Parameters	domains[]=example-domain.co.nz&domains[]=example-domain.net.nz&domains[]=example-domain.kiwi.nz

Example Response

```
[{"domain": "example-domain.co.nz",  
  "status": "Available",  
  "code": "220"},  
{"domain": "example-domain.net.nz",  
  "status": "Available",  
  "code": "220"},  
{"domain": "example-domain.kiwi.nz",  
  "status": "Available",  
  "code": "220"}]
```



Example Request

GET	http://srs-json.srs.net.nz/1.0/availability
GET Parameters	string=example-domain

Example Response

```
[ {"domain": "example-domain.nz",  
  "status": "Active",  
  "code": "200"  
},  
{"domain": "example-domain.ac.nz",  
  "status": "Available",  
  "code": "220"  
},
```

..... All other 2LDs

```
{"domain": "example-domain.parliament.nz",  
  "status": "Available",  
  "code": "220"}]
```



Releasing Domains List

This API is designed to provide registrars with a simplified process for acquiring domain drop list information via a web interface. Returns a list of domain names that are about to be released from the registry within the next two days.

ACLs: Whitelist for Registrar IP address

Method: GET

Resource URL: <http://srs-json.srs.net.nz/1.0/droplist>

Parameters: None



Releasing Domains List

Response details

Response key	Valid response data
registered	The date the domain was registered.
domain	The domain name as stored in the register
cancel_date	The date the domain was cancelled
drop_date	The date that the domain is expected to be released by the registry via the release domains scheduled job.
release_date	The date the domain is available to be released (cancel + 90)
registrar_id	The registrar id that currently manages the domain.



Example Request

GET	http://srs-json.srs.net.nz/1.0/droplist
-----	---

Example Response

```
[{
  "registered": "2008-07-06T19:14:17+13",
  "domain": "testdomain.co.nz",
  "cancel_date": "2014-08-06T03:20:33+13",
  "drop_date": "2014-11-05T00:30:00+13",
  "release_date": "2014-11-04T03:20:33+13",
  "registrar_id": 9921
},
{
  "registered": "2013-08-06T08:46:10+13",
  "domain": "testdomaindata.co.nz",
  "cancel_date": "2014-08-06T07:59:20+13",
  "drop_date": "2014-11-05T00:30:00+13",
  "release_date": "2014-11-04T07:59:20+13",
  "registrar_id": 9830
}]
```



UDAI

(Unique Domain Authentication
Identification IDs)



CHANGES to UDAI processing

- New UDAs are NOT created when:
 - a domain is transferred
 - a change in Registrant contact details is made
- UDAs expire after 30 days
- UDAs expire on:
 - a domain transfer (and a new one will not be automatically created post transfer).
 - 30 days after generation.

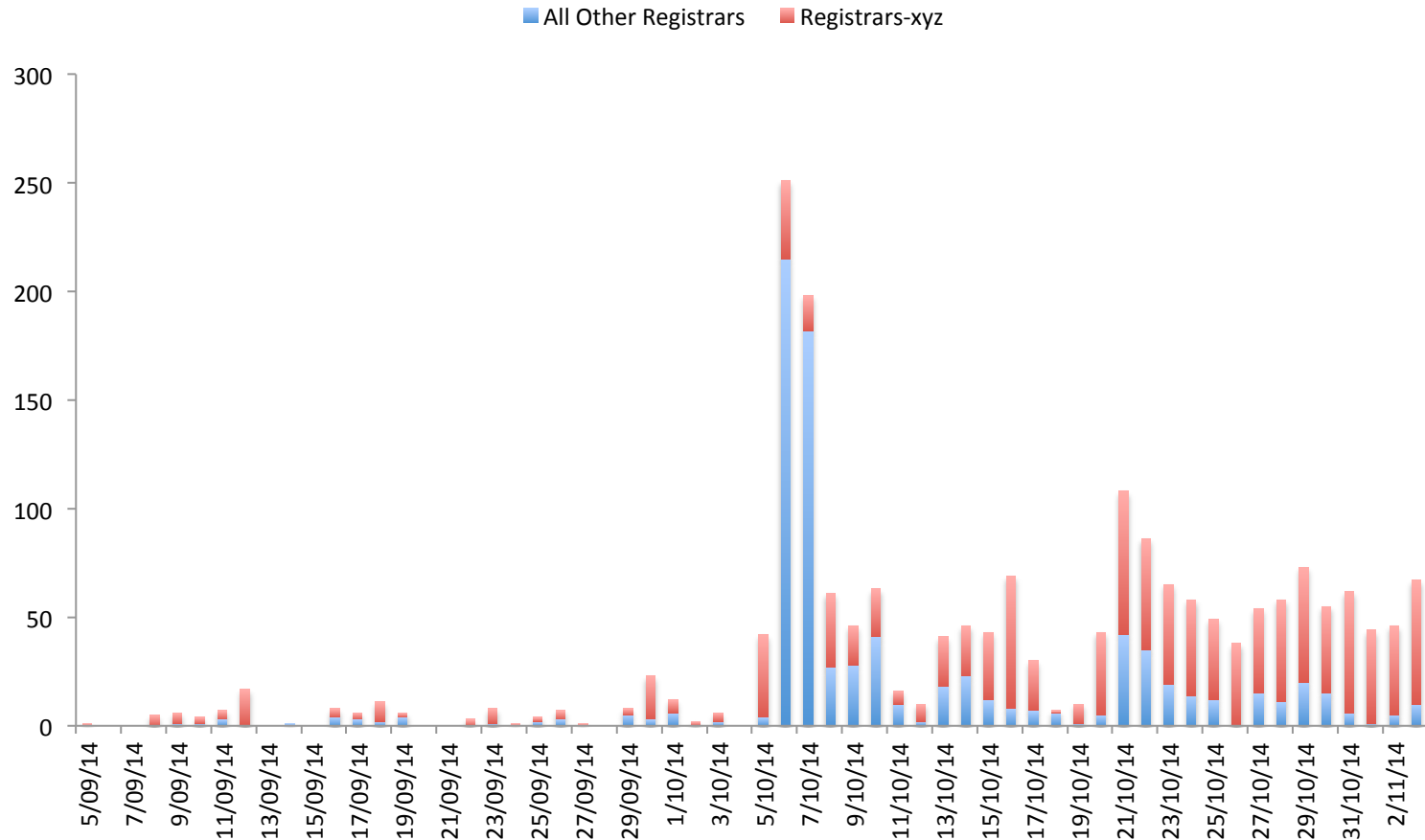


Reasons for the change

- Analysis of SRS transactions showed that for the majority of transactions, new UDAs were generated before a domain was transferred.
- Security - No control over the storage of UDAs by Registrars, Resellers or Registrants. Unsecured storage could lead to compromise of domain names.
- Multiple ways for generating UDAs



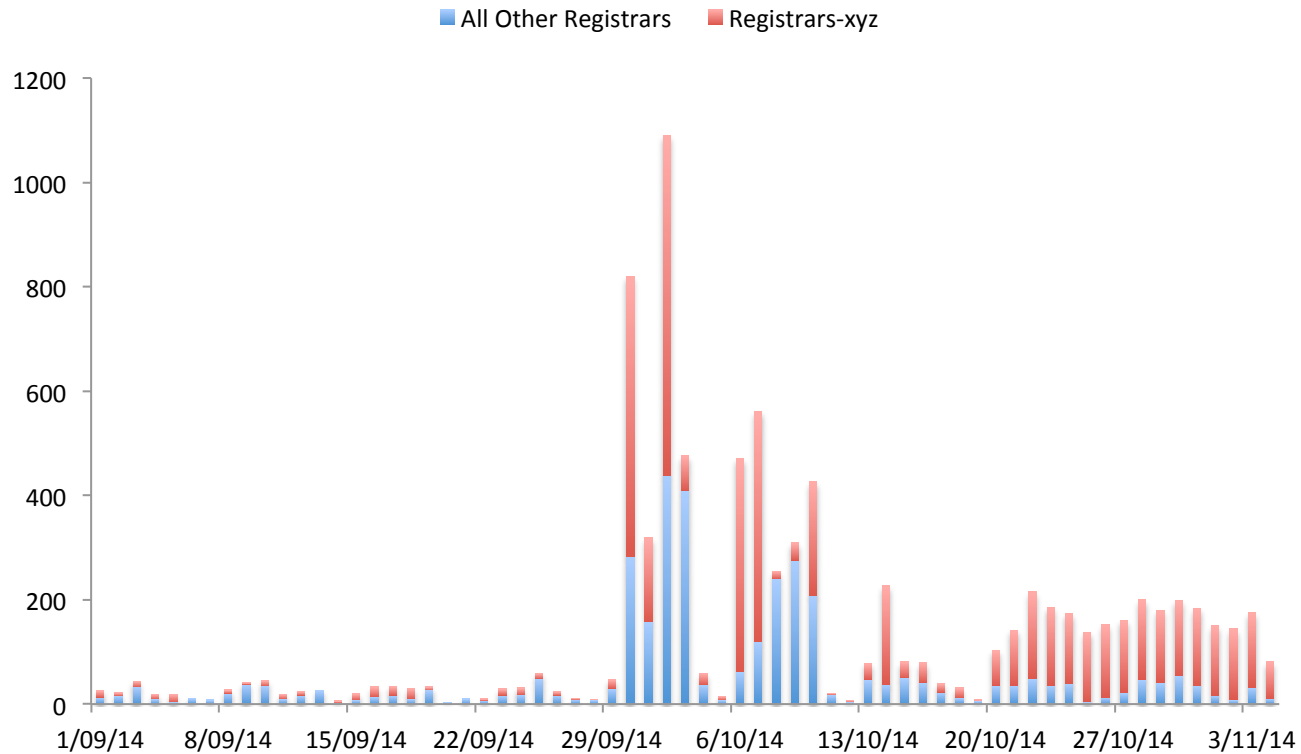
UDAI Expired Error Messages



Three registrars account for the majority of UDAI expired errors



UDAI invalid error messages



Three registrars account for the majority of UDAI invalid errors



SRS Future Protocol Changes?

- Warning Messages
- Domain Renew Transaction
- Domain Transfer Transaction



SRS Warning Messages

The SRS protocol does not include a placeholder for returning a warning to the registrar.

The benefits of a warning are:

- Notify registrars that some data has been ignored
- Notify registrars that certain actions are deprecated (with link to new method)
- Useful for registrars when debugging why a particular request has failed



Domain Renew Transaction

The current renewal process is part of a domain update with a specific 'renew' instruction flag.

Proposed Change

- Create a separate Domain Renew transaction that only accepts the Term and BilledUntilDate (Expiry Date)
- The renew function under DomainUpdate will be deprecated after a period of time



Domain Transfer Transaction

The current process is a domain update from a new registrar with a valid UDAI is automatically inferred as a transfer.

Proposed Change

- Create a separate transaction that only allows a domain to be transferred, requires the UDAI and does nothing else.
- The transfer function under DomainUpdate will be deprecated after a period of time



Other Potential SRS Changes

Infrastructure Improvements:

- New WHOIS server
- Load balancing / Multiple Front Ends
- Automatic failover between sites
- PostgreSQL database upgrade
- Hardware upgrade

RIK VM image



SRS Security

Heartbleed (CVE-2014-0160)

- No impact on SRS as the SSL library version on front-end servers was never vulnerable to heartbleed.
- No registrars requested new GPG keys or EPP SSL certificates as a direct result of heartbleed. (hopefully as a result of effective front-end vs. back-end segmentation..)

Poodle (CVE-2014-3566)

- SSLv3 is disabled in the SRS Test Environment.
- Approximately 5 active registrars are still defaulting to SSLv3 connections in production, and we'll follow up with registrars as we see these connections.

