A busy year!

ICANN 45 Tech Day/DNS-OARC
Toronto, Canada

Canadian Internet Registration Authority (CIRA)

Jacques Latour

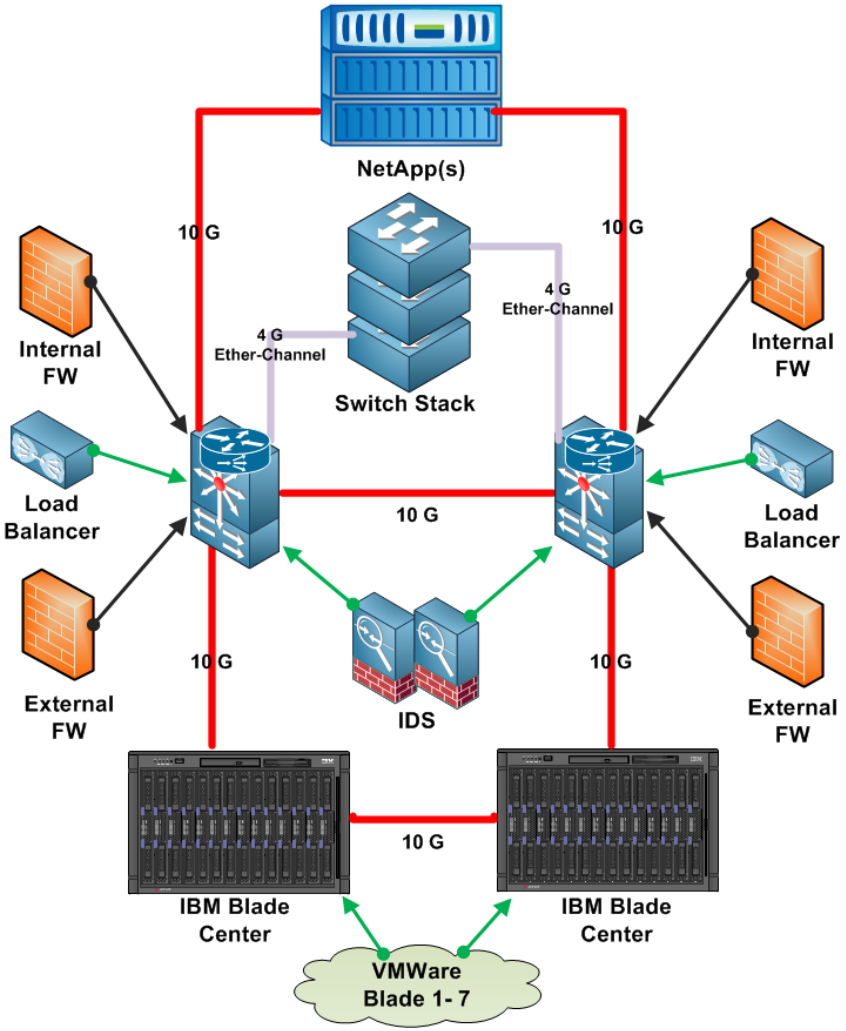
Topics for presentation

Major Technical Projects:

- New network architecture – April 2012
- New registry – June 12, 2012
- DNSSEC – November 2012
- French character IDN – Early 2013

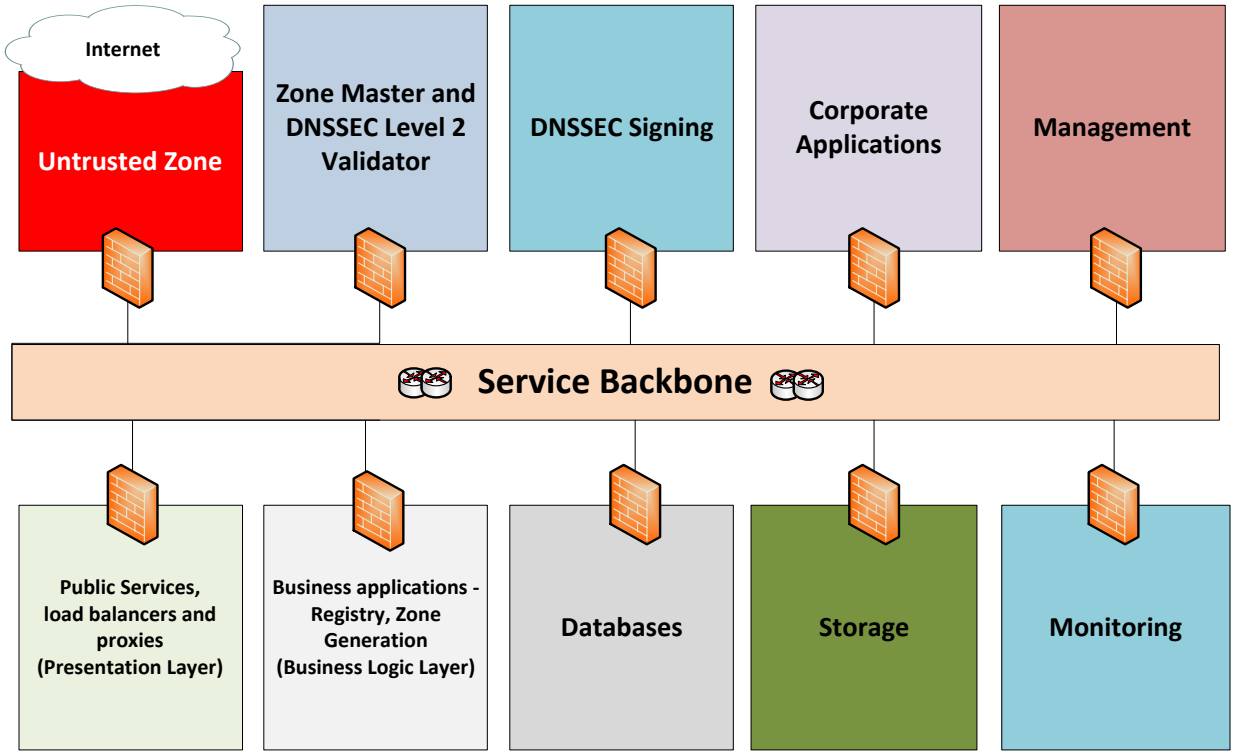
New RGY Network Architecture

- Platform for virtualization
- High availability
- Internal & external firewalls
- 10 Gig Core Infrastructure
  - Palo Alto firewall
  - F5 Load balancers
  - NetApp storage
  - Cisco Nexus
  - IBM BladeCenters



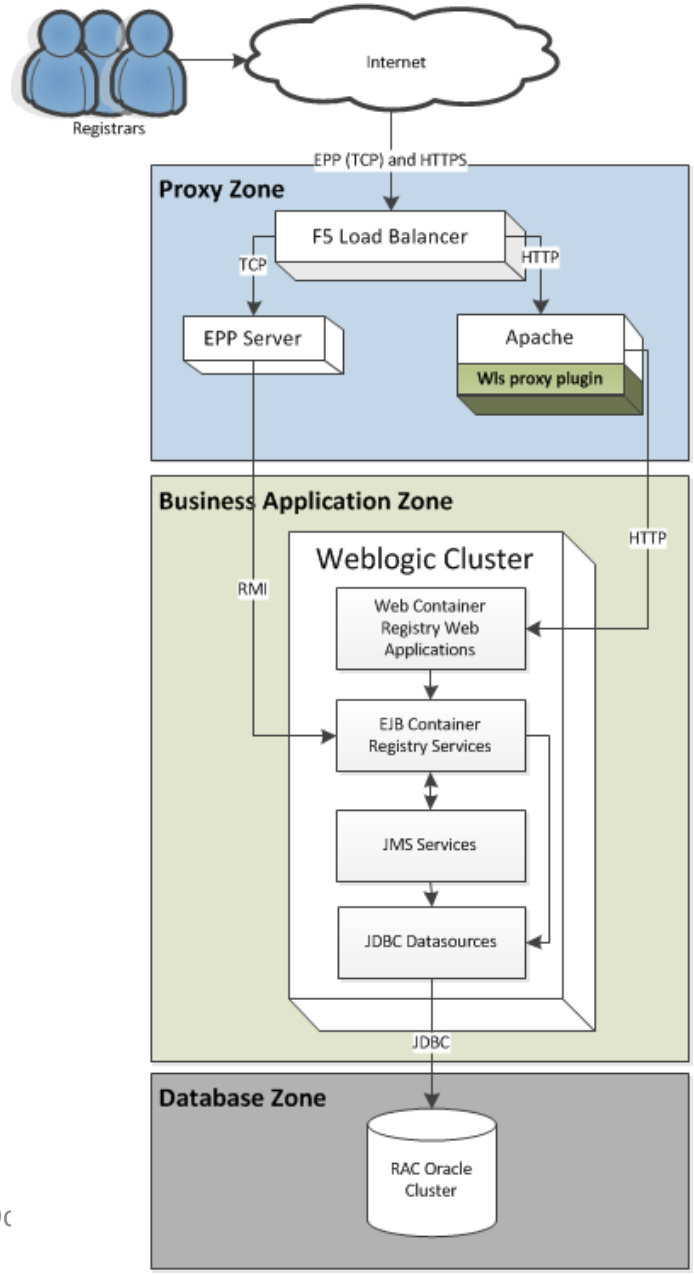
New Network Security Architecture

- Developed a virtual zone architecture
- With granular security policies by zones



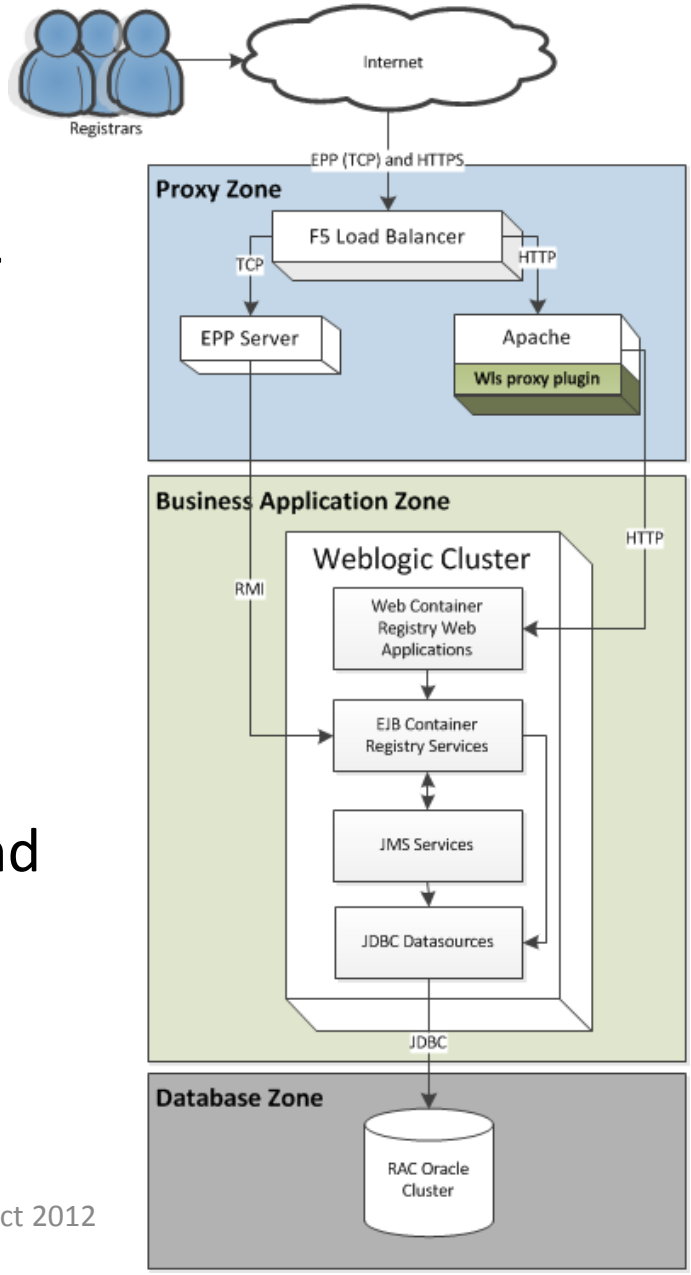
New Registry Platform

- 18 months project
- Ported & rewrote registry code to middleware platform on June 12, 2012
- Better software architecture, new development work is more efficient
- 3 Tier security architecture, build on top of new network & security infrastructure
- Significantly reduced downtime for software release
- Improved processing with reduced hardware requirements
- Increased complexity – more training



Some Highlights

- F5 load balancer terminates all SSL
- Applications hosted on Weblogic cluster running 4 managed servers (nodes) across 2 physical servers
- Service layer implemented using Stateless EJB
- Distributed JMS used for asynchronous processing
- Database access abstracted using JPA and Hibernate (less dependant on Oracle)
- Oracle 10g RAC 3 nodes cluster



CIRA IDN Policy and Business Requirements

- CIRA intends to offer French character IDNs within the .CA Registry.
- Accepted French characters:
  - é, è, ë, ê, à, â, î, ï, ù, ü, û, ö, ô, ç, œ, æ, and ÿ
- **Administrative bundling**
- EPP now in OT&E
- Target date:
  - Production early 2013

CIRA IDN Administrative Bundle

- All registered domain variants with the **same canonical representation** make up a bundle.
  - oeuvre.ca
  - œuvre.ca
  - oeuvré.ca
- Domains in a bundle are sponsored by the **same registrar**.
- All domains in a bundle have the **same registrant contact id**.
- Registered variants are registered and managed independently, and are only administratively linked by the criteria above.
- new concept, a standard, an RFC?

CIRA IDN Technical Challenges

- **Domain Transfers** and **Registrant Updates**
  - Most significant design issue - same for both operations
  - Requirement that all variants be registered to same registrant contact id and registrar BUT domains are managed independently.

DNSSEC

- We expect to have our zone signed

November 12, 2012

- Official start date: not sure ☺
- Key signing ceremony: September 4, 2012
  - Went well, according to script !!!
  - CIRA DPS online, no real comments
  - KSK, RSA, size: 2048 bits, length: 365 days
  - ZSK: RSA, site: 1024 bits, length: 30 days

http://www.cira.ca/assets/Documents/DNSSEC/CIRA-DPS-EN-0-Public-Final-v1-4.pdf

Why it took so long?

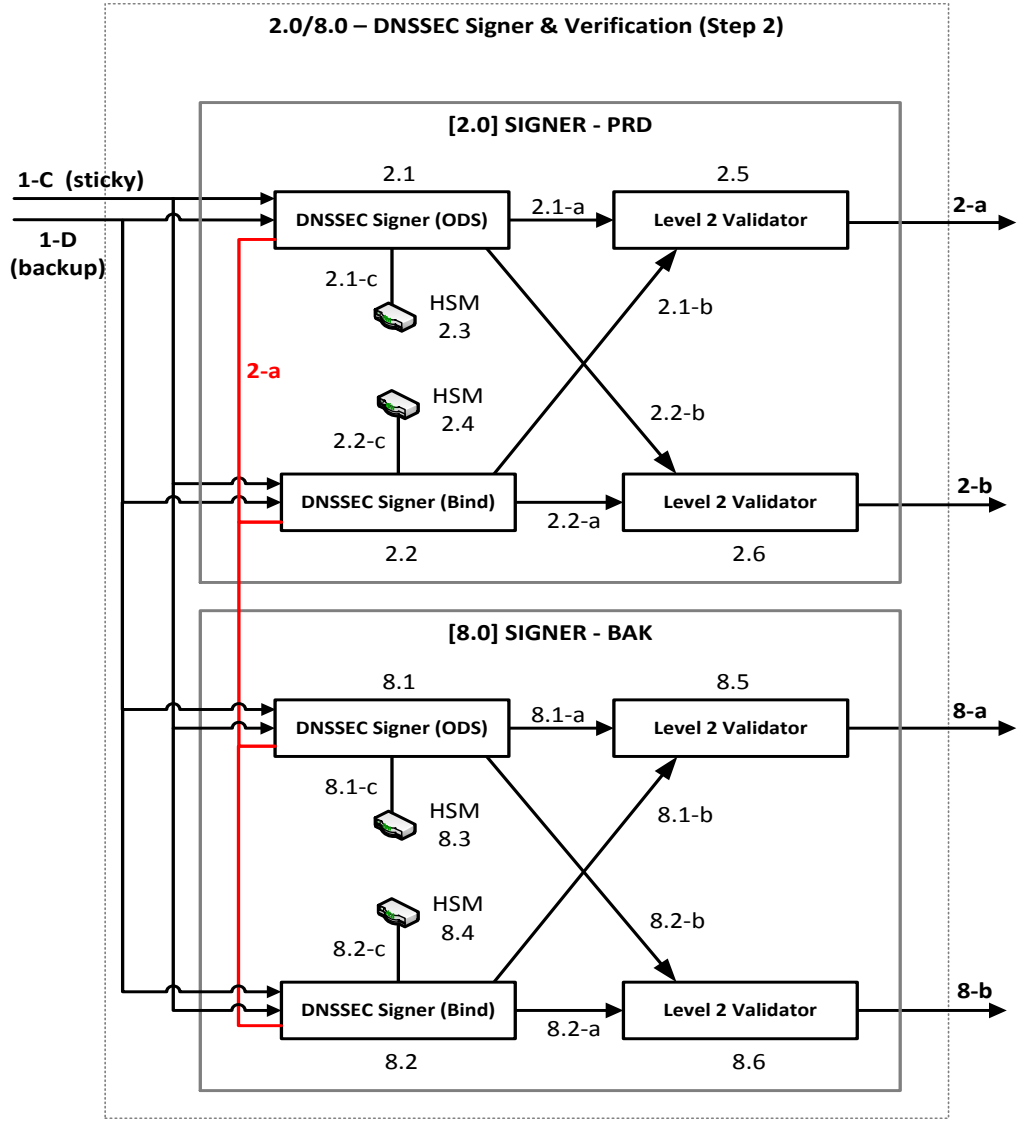
- We used a different approach to sign .ca
  - Risk adverse, high availability & resilient solution
- Dual Independent signing engines
  - We create two independent signed zones using Bind and OpenDNSSEC
- Comprehensive DNSSEC validation process
  - We perform multiple levels of zone file validation
  - If there's an issue with either signer or HSM, we stop
  - Hardest task, important because it is the only way to detect a signer engine implementation problem

Risk Adverse

- CIRA's solution took in account known DNSSEC related service impacting outages;
  - DNSSEC software issues
  - Key management issues
  - Implementation issues (infrastructure)
  - Operational issues

DNSSEC Signer & Validation

- Online signer sets located in different facilities/cities
  - DR site always up to date
- Worked closely with OpenDNSSEC team to make v1.4.0 functional for our production, although they recommend it's not for production use yet ☺
- Total of 4 AEP Keyper HSM on-line with key synchronizations



Our Validation Process

- **Level 1 Validation: (pre-signing)**
  - Check md5 sum – Verifies that .md5 checksum matches .zone contents
  - Check percent change – has the file size changed by more than $x percent (currently 1%)
  - Check file diff – has the contents of the file changed by more than $x lines (currently 15K lines)
  - named-checkzone – Verify 'named-checkzone' succeeds on the unsigned zone

- **Level 2 Validation: (post-signing, validation code independent from signers)**
  - Check md5 sum – Verifies that .md5 checksum matches .zone contents
  - ldns – Verify that the zone can be read into ldns-readzone with no errors (ldns-verify-zone in future)
  - Required files met – Requires the two independently signed zones to compare. If one is missing, signing set is marked bad.
  - Check dnskey – Verify that the KSK has not changed
  - validns – Validate all RRSIGs and the NSEC3 chain and on the two zones
  - Check rrsigs – validate signer engines - Zero out signature and timestamp data, signed zones should be identical
  - named-checkzone – Verify 'named-checkzone' succeeds on the signed zone

- **A corrupted or suspected zone will not be published**

Challenges

- Bind and OpenDNSSEC
  - Both produce different, although valid signed zone files
  - Both handle signing differently, still finding new occurrence when behaviour changes (i.e. bind retained RRSIGS of retired ZSK)
- What is the right process for signing a zone?
- Other issues we identified: (for you to read later on)
  - ODS locks up when <serial> is set to "keep" option if a zone is not delivered (tries to re-sign the zone it's already signed).
  - ODS + AEP Keyper 1% of the time in our experience went into a loop of 10 iterations for 60 seconds each failing to talk to the HSM somehow.
  - All 4 signers are independent and do not communicate with each other. While all begin with the initial config with identical key rollover times, the servers themselves can take different amounts of time to complete the rollover, thus setting future rollovers a few seconds apart. Over time, this becomes problematic, compensated by adding cronjob to HUP ods-enforcerd
  - Validdns - Zone-cut bug was detecting "No NSEC3 records for "ab.ca", "on.ca", etc...which there was no zone cut for.
  - Occasional odd errors generated by the AEP-supplied PKCS11 library indicating unreachability when connectivity is fine

Questions?

LUNCH TIME!!!