Security and Scalability Considerations

Rodney Joffe
SVP and Senior Technologist, NeuStar

NeuStar™

Introduction

A Registry is much more than a database and software; it includes:

- Network infrastructure – firewalls, load balancers, routers, packet shapers
- Protocol and application servers
- DNS and WHOIS servers
- Billing systems
- Monitoring systems
- Security and intrusion detection systems

Must be designed and managed with security, stability, and robustness in mind

Must be supported by comprehensive security and contingency plans

Data and Infrastructure Security

What does a Registry need to protect?

- SRS Database
- WHOIS Database
- DNS Infrastructure
- Billing and Financial Systems
- Web Servers
- Customer Relationship Management Systems

Security Management

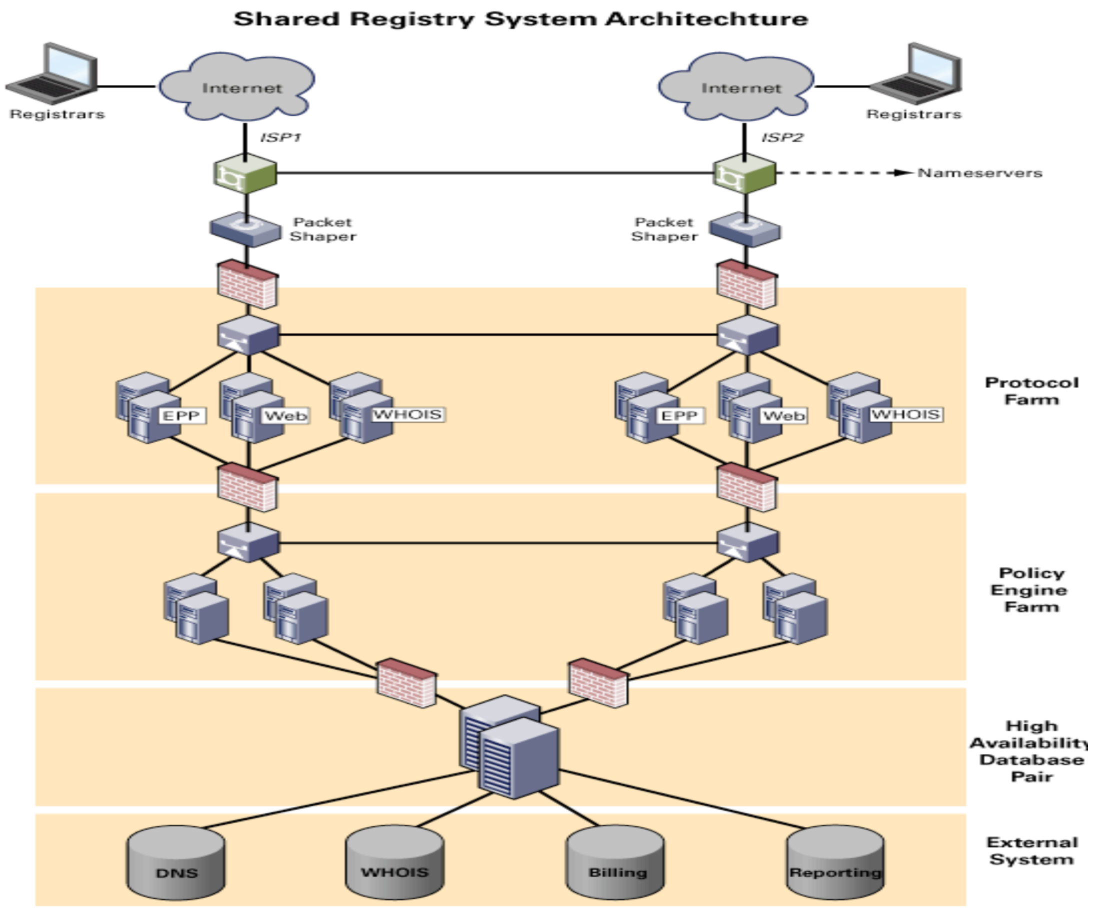
Areas of Consideration:

- Security Policy
- Security Organization
- Personnel Security Policies
- Physical and Environmental Security
- Operations and Communications
- Entitlements Management (Info access)
- System development and Maintenance (Production Support)
- Security Incident Management
- Continuity of Business (COB)
- Auditing

Security Mitigation Strategies

- Multiple Firewall Layers
- Intrusion Detections Systems
- No direct access to the database
- Multiple control mechanisms to manage registrar connectivity – IP addresses; passwords, and certificates
- Registrar connections should be managed by dedicated packet shaping hardware
- File level access controls
- Regular internal and third-party audits

Registry Architecture



NeuStar™

Scalability – Areas of Consideration

- Network Infrastructure
- Internet Bandwidth
- Database
- Protocol and Application Servers
- DNS Network
- WHOIS Databases
- Registrar Connectivity
- Billing and Financial Systems
- OT&E Environment

NeuStar™

Scalability Strategies

- High availability, redundant network
  - Hot stand-by data centers
  - No single points of failure
- Architectural design that is scalable
  - Load balanced server farms
  - Separate protocol and application server layers
- Enterprise grade software (Oracle, etc)
- Broad Global DNS Network
- Multiple ISP Connections
- Pre-established contingency plans

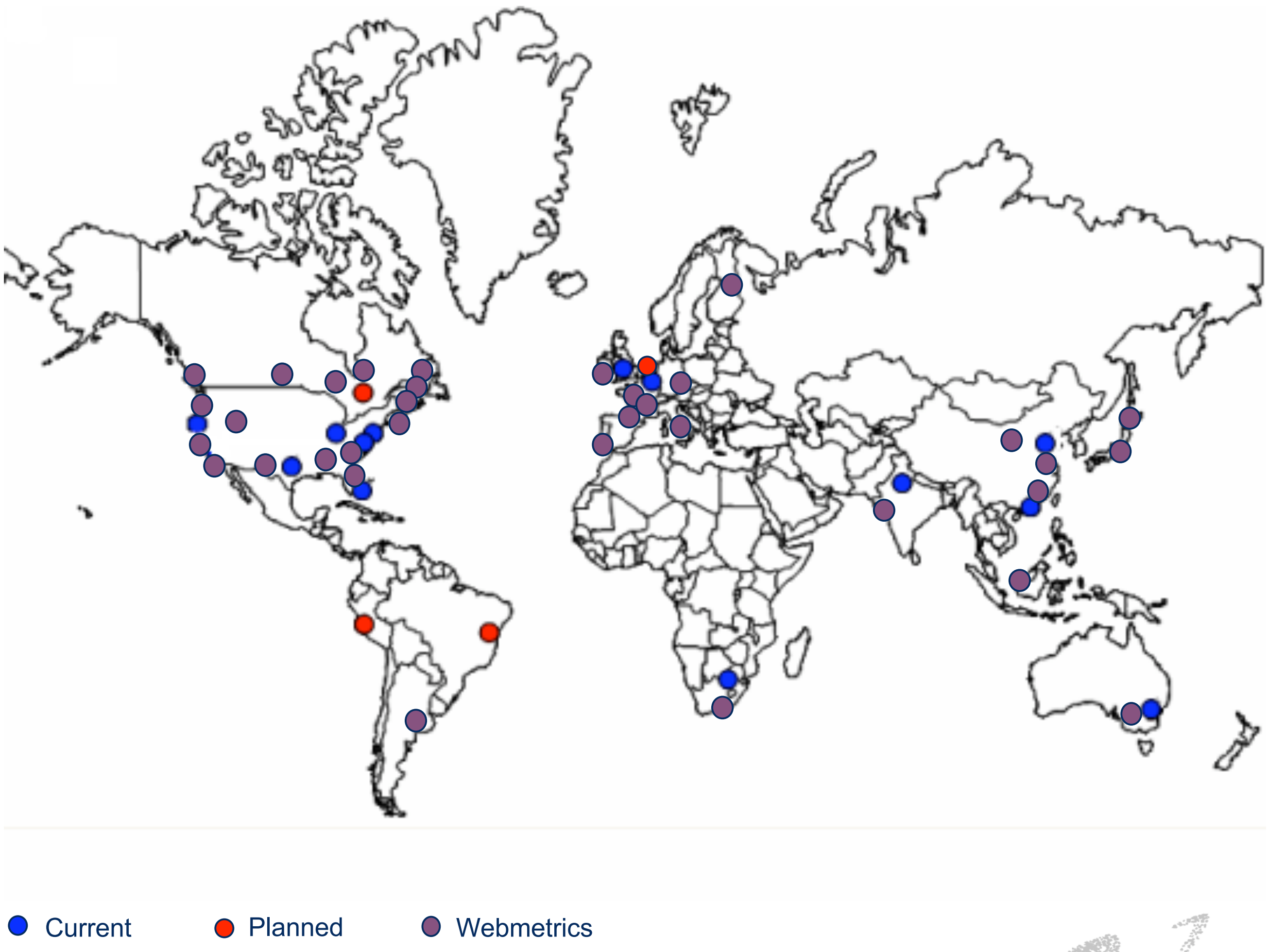
System Monitoring

- System and resource monitoring is necessary for proper planning
- Critical resource monitoring includes:
  - Storage capacity
  - CPU usage
  - Memory usage
  - Data throughput
  - Internet capacity
  - Power supply
  - Availabiliyt
- 24 X 7 Network Operations Center and Network Monitoring System
  - Monitor for Security Breaches
  - Detect infrastructure and hardware issues
  - Timely response and coordination

DNS and Monitoring Infrastructure

UltraDNS Data Centers

- **Americas**
  - California
  - Florida
  - Illinois
  - New York
  - Texas
  - Virginia
  - Brazil
  - Peru
  - Canada
- **Europe**
  - Luxembourg
  - London
  - Amsterdam
- **Africa**
  - Johannesburg
- **Asia-Pacific**
  - Beijing
  - Hong Kong
  - Noida (India)
  - Sydney



NEUSTAR™

NeuStar™

Trusted to bring networks together