Security, Stability and Resiliency

.CR

NIC Costa Rica

Mauricio Oviedo

moviedo@nic.cr

JUNIO 22, 2015
Where to get...

- Highly secure system
- Fault tolerant
- Fully distributed
- Economically feasible
Existing Infrastructure: How can we use it better?
Existing infrastructure: Areas of improvement

- Better leverage of existing devices
- Move to a virtualized environment
- Adjust the existing services to benefit from the new platform
- Scalable enough to adapt to new projects: e.g. full site replication
Virtualization Platform: **GANETI**

- Cluster virtualization management system
- Based on Xen or KVM
- Designed by Google for Google (Open Source since 2007)
- Ability to provide an HA environment via DRBD disk replication
- Can start with a single node and scale up easily
- Live instance operations
GANETI Platform: Basic Deployment

Cluster Node

VLAN Trunk or Open vswitch

Ganeti Cluster
GANETI Platform: Complex Deployment

Source: https://www.synnefo.org/about/

Mauricio Oviedo
moviedo@nic.cr
JUNIO 22, 2015
GANETI Platform: Our Deployment

Mauricio Oviedo
moviedo@nic.cr
JUNIO 22, 2015
Transition of Existing Services
Existing Services: FRED Registry System

- Previously deployed as a centralized set of components
- Distribution of the different components
  - Different security policies can be applied
  - Increase availability in case of failure
  - Different HA approaches for some components
  - Load Sharing
- Migration with no disruption or downtime
Existing Services: FRED Registry System

Mauricio Oviedo
moviedo@nic.cr
JUNIO 22, 2015
Existing Services: DNSSEC

• Transition to a different DNSSEC signing process

• Requirements:
  • Secure
  • Efficient
  • HA system to benefit from new technology
  • Possibility to be used by our customers
  • Well documented
  • Possibility to create backups
  • Auditable
**DNSSEC:** Smart Cards + SW Signing

- Migration Process started with ICANN & NSRC DNSSEC Workshop in CR, April 2014
- Fully deployed in October 2014
- Smart Cards being used for KSKs & ZSKs generation
  - Key bundles generated include several ZSK rotations
- 2048b Keys
- Modified Richard Lamb’s CD for Keys’ generation + modified version of script & dnssec-signzone for SW signing
DNSSEC: Smart Cards + SW Signing

- 2 Full Key Ceremonies, one for .CR and another one for the subzones
- Time taken for full signing: 20 seconds
- KSK and its backups never leave the SCs, kept offline in safe
Existing Services: DNSSEC
Distributed .CR DNS System
.CR DNS Distribution: Name Servers

- You never have enough Anycast 😊

- Added PCH Anycast Cloud to get presence in every continent and major IXPs around the world

- ISC & RIPE Anycast clouds + Servers in CR, NIC.CL and NIC.MX

- ~ 70 Name Servers

- Working with LACTLD to participate in it’s Anycast project as “user & node”

- Direct connection to Costa Rica’s National IXP, CRIX

Mauricio Oviedo moviedo@nic.cr JUNIO 22, 2015
.CR DNS Distribution: Name Servers
.CR DNS Distribution: Name Servers
Conclusions: Putting it all together...
Prepare it to grow

Improvement cycle never stops

Ask for ideas!!

Improvemnt != $$$$$$$