Gathering the Children DS'

An Experiment

by Mark Elkins <mje@posix.co.za>

ICANN-69 - Oct 2020

Context

Management of the EDU.ZA zone...

- For post-school non-University Domain names

- Closed space, used by only the above

- DNSSEC Signed and IDN enabled (ISO 8859-1)

- 150+ Domains (since 2010) – 8 are Signed

- Totally Web based management & WHOIS

DNSSEC Management

(before) Registrars/Registrants can...

- Send an Update via the Web interface (needs manual validation)

- Provide a unique TXT string in their zone (automagical update)

DNSSEC Management

Registrars/Registrants can now...

- Simply sign their domain and include the correct CDS records in the zone

- Newly signed Domains, Trust Chain completed after 3 days

- Existing signed Domains acted upon daily

DNSSEC Management

A php script runs at 3am, digs every domain for CDS,
existing signed via DNSSEC aware resolver,
all non-signed via TCP to the first listed Nameserver.

- CDS 0 0 0 0 – will remove all DS records

- Mirrors the CDS to DS records

- New CDS records are recorded and if no changes after three days, are deemed to be valid

Other consequences

The "dig" uncovers any Nameserver anomalies

gcol.edu.za: Error: dig +nofail +tcp @nippy.foo.co.za +short gcol.edu.za cds

dig: couldn't get address for 'nippy.foo.co.za': not found

Current log

CDS-poll.php: 2020-09-30 01:05:01 CDS Poll of 'edu.za' - 153 domains

centralislamicschool.edu.za: 1×CDS, 12 sec

dnssec.edu.za: 1×CDS, 15 sec

gcetc.edu.za: 2×CDS, 24 sec

nic.edu.za: 1×CDS, 51 sec

nic.edu.za: ID:584: SQL update "cds1stat=3,"

parkme.edu.za: 2×CDS, 62 sec

sae.edu.za: 2×CDS, 73 sec

twpacademy.edu.za: Error - Dig gave ";; communications error to 129.232.248.30#53: connection reset"

whois.edu.za: 2×CDS, 93 sec

xn--caf-dma.edu.za: 1×CDS, 93 sec

--- Zone scan took 93 seconds - 0 DS changes ---

Thank you

Questions?

Mark Elkins

mje@posix.co.za