

CDS Scanning and other consistency checks

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

ICANN-77 - June 2023 - Washington



My Desires and Background

Internet for everybody – that is secure

Registry operator EDU.ZA zone (Non EPP, Web base, 182 Domains, 128 (108) with a Website (SSL)

Registrar (not ICANN accredited) for 1443 Domains, 221 Agents (40% of DNS is Local)

ICANN DNS Study of Africa, 2022
<https://dnsstudy.africa>

Infrastructure

All systems are homegrown (existed before cPanel)

LAMP – Linux (Gentoo) / Apache / MySQL / PHP

Great belief in Automation

DNS / DNSSEC / TLSA / SSL – etc

Customer details are all in the Database

Adding DNSSEC

```
dnssec-policy "my-ecdsa256-policy" {  
    dnskey-ttl 3600;  
    keys {  
        ksk lifetime 370d algorithm ecdsa256;  
        zsk lifetime 34d algorithm ecdsa256;  
    };  
    purge-keys 10d;  
};  
  
zone "whois.edu.za" {  
    type master;  
    file "/etc/bind/pri/whois.edu.za/db.whois.edu.za";  
    key-directory "/etc/bind/pri/whois.edu.za/keys";  
    dnssec-policy "my-ecdsa256-policy";  
    serial-update-method date;  
};
```

CDS Scanning – as a Registr...

A PHP script that walks through the Database, Domain by Domain, checks the Nameservers, connects to the Nameservers (check consistency), checks for CDS records (changes?), checks for a Website (SSL/etc)

PHP Script is at:

<https://dnsstudy.africa/CDS-poll.txt>

CDS scanning

How this works

- A php script runs at 3:01am, digs every “remote” domain for CDS
 - existing signed via DNSSEC aware resolver
 - all non-signed via TCP to the first listed Nameserver
- CDS 0 0 0 00 (null record) – 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

LogFile

CDS-poll-dns2.php: 2023-06-09 01:05:01 CDS Poll of 'edu.za' - 182 domains

dom1.edu.za: 2×CDS, 2×NS, @46 sec

ewc.edu.za: 0×CDS, 2×NS, 75 sec SOA lookup: failed on fread() for data length

malutifet.edu.za: 0×CDS, 2×NS, 394 sec

nic.edu.za: 1×CDS, 2×NS, @414 sec

nkangalafet.edu.za: 0×CDS, 2×NS, 715 sec: SOA lookup: Connection timed out

utvetc.edu.za: 0×CDS, 0×NS, 791 sec: SOA lookup: Connection timed out

whois.edu.za: 2×CDS, 4×NS, @795 sec

xn--caf-dma.edu.za: 2×CDS, 2×NS, @797 sec

Thank you

Questions?

Mark Elkins

mje@posix.co.za