DNSSEC.UA With Knot

Hostmaster.UA
2024-01-24
CSNOG 2024 Zlin

2011-2014

2011-11-08 UA.UA KSK

2011-12-01 UA.UA signed

2011-12-02 UA RSA KSK (UADOM 2011)

2012-02-07 Lighthouse DNS Resolver

2012-03-27 UA zone signed, algoritm 10

2012-04-13 UA DS in root

2014-04-01 UA migrated to EPP

2019, The Government Mandate

КАБІНЕТ МІНІСТРІВ УКРАЇНИ

ПОСТАНОВА

від 12 червня 2019 р. № 493 Київ

Про внесення змін до деяких постанов Кабінету Міністрів України щодо функціонування офіційних веб-сайтів органів виконавчої влади

1. Офіційний веб-сайт (веб-портал) органу виконавчої влади та офіційні веб-ресурси, що пов’язані з діяльністю органу виконавчої влади (далі - офіційний веб-сайт), повинні бути розміщеними в домені GOV.UA та у разі потреби у домені .УКР. Домен, на якому розміщений офіційний веб-сайт, повинен бути підписаний із застосуванням технології захисту доменних імен DNSSEC. https://zakon.rada.gov.ua/laws/show/493-2019-%D0%BF

2019, DNSSEC Actions

2019-03-19 gov.ua DS added

2019-08-01 com.ua DS added

2019-09-05 kyiv.ua DS added

2019-10-04 Production DNSSEC in ten EPP domains

2019, Algorithm Rollover

2019-10-29	Generated ECDSA KSK
2019-10-30	Generated ECDSA ZSK
2019-10-31	Parallel signing in UA
2019-11-07	IANA: Root zone updated
2019-11-15	IANA: old DS removed
2019-11-19	Removed old RSA keys
2019-11-26	Enabled full NSEC3 in UA
2019-12-02	First ECDSA ZSK rollover

2023, Time of a Change

What was non-ideal with our setup?

Some scripts to rotate ZSKs

ZSK rotation with overlap (1-4 days)

RRSIG generated every hour

NSEC3 salt was static

Schedule achieved by crontab

Why Knot?

What are the benefits of Knot signer?

Can rotate ZSK by schedule

ZSK do not overlap

RRSIG generated only when needed

NSEC3 salt rotated (magic -1 *)

Small IXFR updates possible

6connect folks used it already

2023, Timeline

2023-09-28 started migration

2023-11-15 finished second level of UA

2023-12-xx journal incident happened

Knot developers were super helpful

We have learned that some combinations of options are incompatible with our specific setup

What can possibly go wrong?

excessive IXFR updates and triggered BIND bug, with these settings:

```
zonefile-load: difference
journal-content: changes
```

this is better - journal keeps track of all zone data:

```
zonefile-load: difference
journal-content: all
```

and this is even better (no duplicate updates on Knot restart):

```
zonefile-load: difference-no-serial
journal-content: all
```

I still plan to open a bug with ISC on this…

Plan for UA zone signer

create new virtual Knot server (w/ntpd)

make this Knot server to be inline signer
copy KSK/ZSK keys over

watch the magic done by Knot
(ZSK rotation, RRSIG and NSEC3 update, small IXFR to test BIND server)

watch journal and log files

Switchover, using intermediate transfer servers to minimize config changes

Knot: he good, the odd, and the weird

Configuration: spaces matter, no tabs!

magic ACLs (notify and transfer)

Another bug was found and a patch was delivered in a day: "-1" value was broken

we run custom build of 3.3.3 release

cool to be able to bump serial by knotc zone-begin/zone-set/zone-commit

logs are very readable comparing to BIND

Knot: he good, the odd, and the weird (2)

IXFR change sets are small (thanks to smart RRSIG rotation)

key repository: keymgr ua list human

After BIND key import, wrong key is rotated

Sometimes serial is advanced additionally due to zone re-signing

SOA email field is converted to lowercase *why*

How to tell Knot is running the zone?
; dig +dnssec DNSKEY UA | grep -c RRSIG

Takeaways

Set small goals

Have a backup plan

Know how to reach developers

Don’t be afraid to fail — but fix fast!

Ask industry experts then become one

and...

DON’T PANIC!

Contacts

dnssec@hostmaster.ua

https://hostmaster.ua/dnssec

Twitter: @cctldua

Facebook: Hostmaster.UA