ICANN Technical Engagement

ICANN 75 Tech Day

Yazid Akanho; Champika Wijayatunga; Nicolas Antoniello

OCTO-TE
ICANN Office of the CTO

Sept. 19, 2022

Who we are ?

- Team mainly in charge of DNS Secured Operations Outreach/Training/Capacity Building programs.

- Regionalized team to better align diverse regional needs and ICANN Strategic Goals.

Adiel Akplogan,
Vice President for
Technical Engagement

Carlos Alvarez,
Trust and Public Safety
Engagement Director

David Huberman

Champika Wijayatunga

Nicolás Antoniello

Yazid Akanho

What we do ?

◉ Technical content (English, French, Spanish) on DNS, DNSSEC, DNS security for the community in a more digestive approach.

◉ Capacity building (webinars + hands-on), Technical support and collaboration :

with + 20 registries from various regions (.BJ, .CI, .CM, .FJ, .SN, .TG, .RW, .PK, .SA, .PG, …): improve operational processes, fix technical and configs issues or DNSSEC signing preparation: readiness assessment, build test infrastructure, testing, etc.

to increase DNSSEC validation and improve DNS ops. at ISP/MNOs : a dozen of operators assisted (MTN, Orange, GEMNET Pakistan, …).

to NOGs, regional Orgs., on-demand: Soudan, South Africa, Senegal, CABASE, APTLD, LACTLD, ANUIES, USTTI, Nordics, INNOG, AFRALO, LACRALO, …

LEAs in all regions: INTERPOL, Criminal justice authorities, CERTs, LE, GAC representatives.

ICANN Learn: two technical courses soon, plan to integrate the virtual lab platform.

◉ Different regional approaches based on specificities and needs.

TE Course catalogue

Technical Engagement Training Course Catalogue

If you are interested in having the Technical Engagement team present any of the courses listed in the catalogue, or would like more information, please do not hesitate to contact us.

ICANN's Technical Mission

DNS 101

DNSSEC 101

Advanced DNS

Advanced DNSSEC

Registry Operations for ccTLDs

OSINT: Fighting DNS Abuse (DNS Abuse for LEAs)

DNS Abuse: Threats and Mitigation

Introduction to RDAP for Domain Names Registrations

DNS Ecosystem Security

DNS for Internet Service Providers

Network Operation Security

UA: Email Address Internationalization (EAI)

UA: Universal Acceptance for Java Developers

Request training and hands-on : email us at OCTO@icann.org

The online lab platform

◉ A set of individual virtual machines (LXC containers) running on AWS LightSail or EC2 host.

◉ Suitable for Covid-19 lockdown and post-pandemic: Deploy online and connect from almost anywhere, all you need is a browser and an internet connection.

◉ Efficiency: time saving on deployment compared to physical infrastructure.

◉ 'Hardwareless':

hardware management is always risky (loss, physical damage during transportation, power issues, etc.).

Helpful in jurisdictions with hardware restrictions or infosec cyber risk.

◉ Scalable:

run parallel trainings with different audiences in different configuration.

integration to ICANN learn (under analysis).

OCTO029: a guidebook for DNSSEC deployment

- ◉ Aims to assist ccTLD registry operators in understanding DNSSEC deployment at a TLD.

- ◉ Target audience:

    TLD registry managers, staff, registrars, registrants

    Operator who administers zones

    Anyone willing to have an overview of how to deploy DNSSEC on a ccTLD.

    Either you are already DNSSEC signed or not, you can glean insights on

- ◉ DNSSEC deployment checklist: a list of adjustable action items that aims to simplify your journey into DNSSEC deployment.

- ◉ Adopted by two ccTLDs in Africa : moving on their own speed; one has improved their operations and internal processes; the second is in test.

- ◉ Download the guidebook : https://www.icann.org/en/system/files/files/octo-029-12nov21-en.pdf

Few observations

◉ Greater awareness and concern regarding improving on cybersecurity posture and resiliency within institutions and organizations in all regions.

◉ Translated to many requests for training and capacity building in DNS and security best practices including hands-on.

◉ Some ccTLDs hesitant to sign their zones - their concerns is that DNSSEC may 'break' their DNS.

◉ Lending technical assistance and support requires a lot of patience.

◉ There is still much to do.

Lab Overview

◉ A set of individual virtual machines (LXC containers) running on AWS LightSail or EC2 host.

◉ Tuned and tested to run over 350 containers at the same time including "real" authoritative DNS lab server and networking virtual routers.

◉ Full IPv4 and IPv6 support.

◉ Developed template servers includes:

> Recursive DNS servers (BIND and UNBOUND)
>
> Authoritative DNS servers (NSD and BIND + OpenDNSSEC)
>
> Routers (FRR)
>
> Other: Client (Ubuntu); RPKI validator (FORT); routers for ANYCAST for DNS labs

◉ Ability to dynamically deploy infrastructure according to specific needs of each lab and number of participants.

◉ Extensible architecture in order to add future features.

Lab Overview

grpX network topology
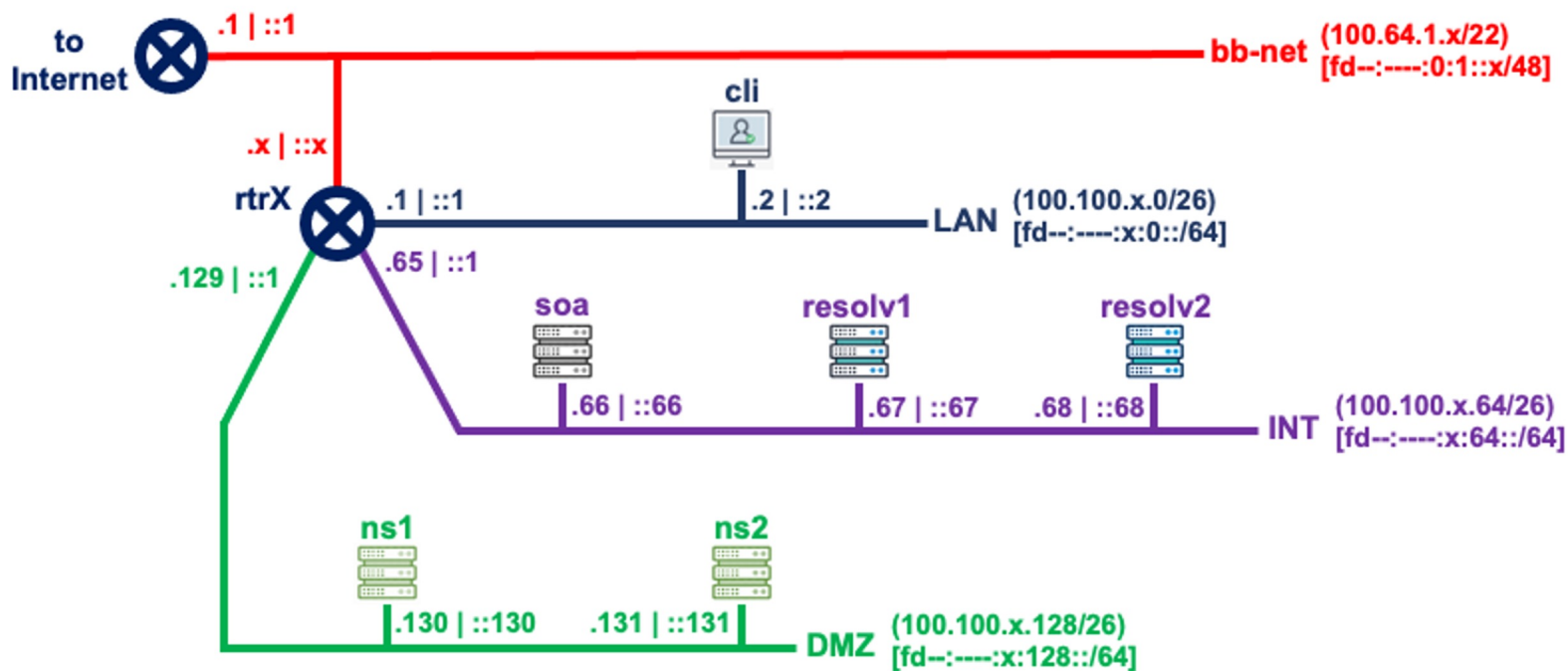
Lab address space: (100.64.0.0/10) [fd--:----::/32]

Click on selected device to access its terminal

Engage with ICANN – Thank You and Questions

One World, One Internet

ICANN

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann