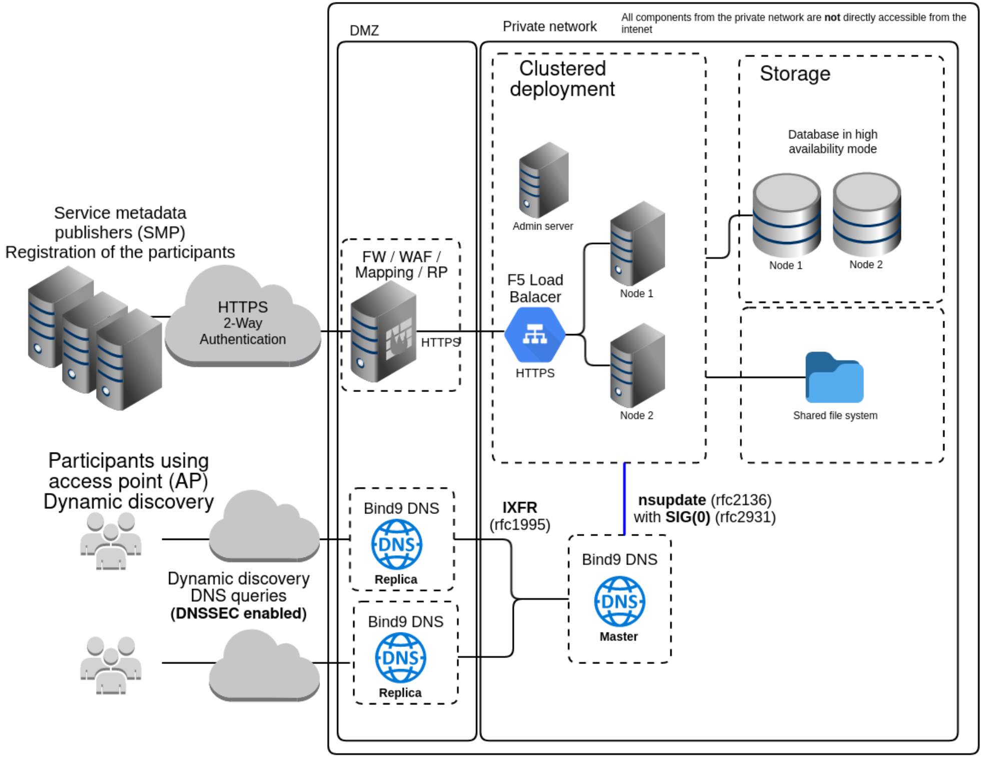
CIWG A+B+C

eDelivery SML service

Jože Rihtaršič
03/04/2024

eDelivery SML infrastructure



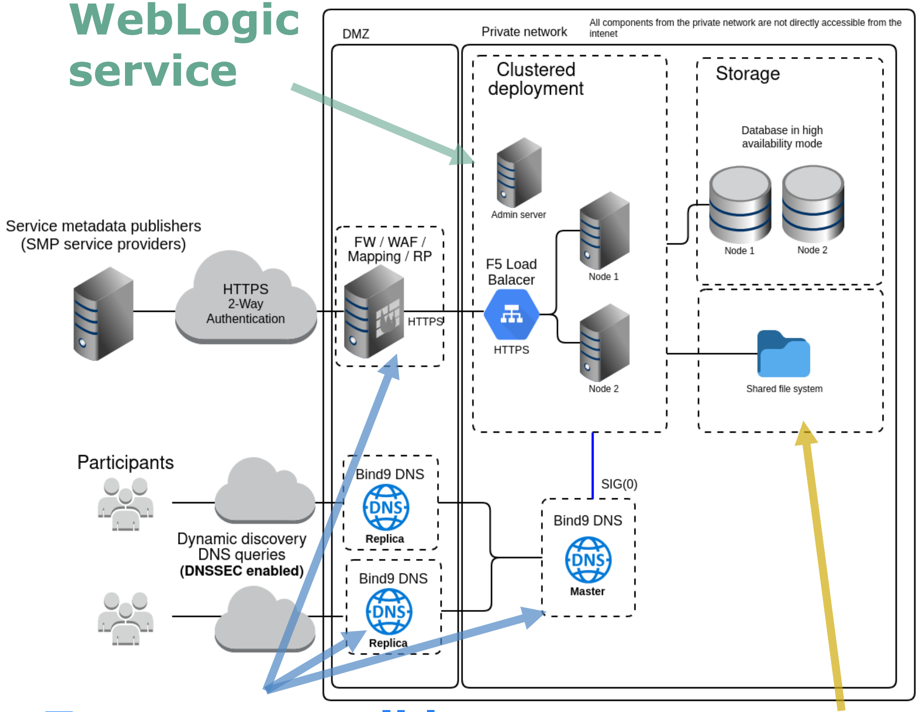
DMZ
Private network
All components from the private network are **not** directly accessible from the intenet
Clustered deployment
Storage
Database in high availability mode
Admin server
Node 1
Node 2
Node 1
Node 2
Service metadata publishers (SMP)
Registration of the participants
HTTPS
2-Way Authentication
FW / WAF / Mapping / RP
HTTPS
F5 Load Balacer
HTTPS
Shared file system
Participants using access point (AP)
Dynamic discovery
Bind9 DNS
DNS
Replica
IXFR (rfc1995)
nsupdate (rfc2136) with SIG(0) (rfc2931)
Bind9 DNS
DNS
Master
Dynamic discovery DNS queries (DNSSEC enabled)
Bind9 DNS
DNS
Replica

Security:
- Regular security updates on all layers: from OS to Application
- mTLS to access API
- Encrypted internal communication
- Auditing (DB level: Who, When What,…)
- Server logs (Event reconstruction)

Redundancy:
- Availability:
  - WebLogic in Cluster (number of nodes can be increased)
  - DNS replicas (Brussels/Luxemburg), Hidden DNS Master
- Data:
  - Oracle DB
  - DNS Zones
  - Daily inconsistency validation

eDelivery SML infrastructure: Organization

Team responsible for WebLogic service

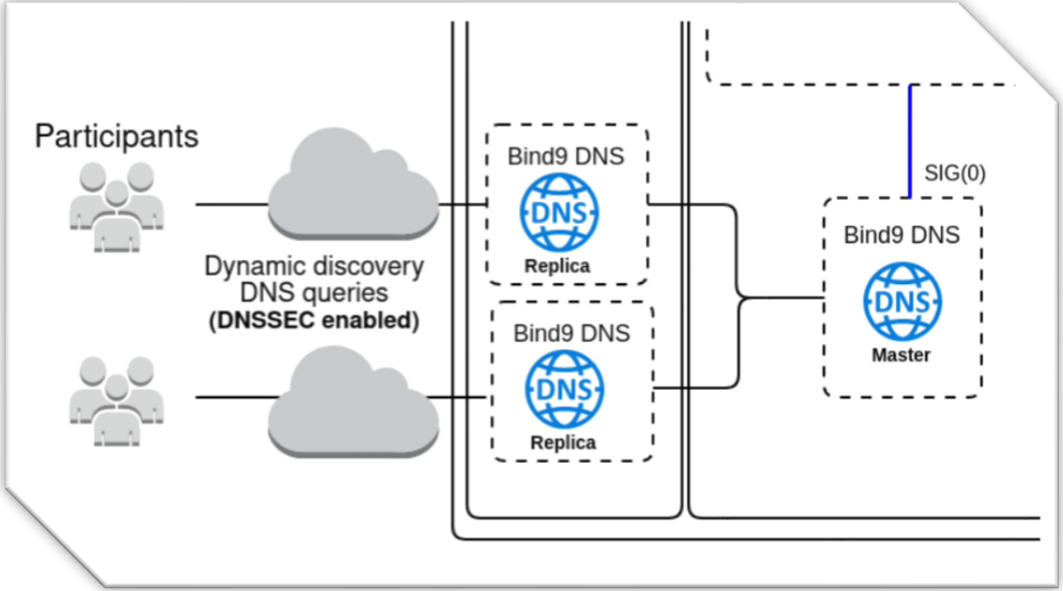


Team responsible for Network

Team responsible for platform services

- eDelivery operational team coordinates various services: WebLogic services, Network services, Platform services …
  - Pros:
    - Teams are experts for the service
  - Cons:
    - Slow responses: communication lag.
    - Limitation on what can be used.
- eDelivery DomiSML limited resources: No full-time developer dedicated to SML service:
  - Maintenance (Library upgrades, security issues, …)
  - Administration tools requested by the SML Operation team.

EDelivery SML infrastructure – Bind9



Bind9 limitations:

- Standard setup (eDelivery service Zone-In-Memory)
- The Domain Name System Security Extensions (DNSSEC) is a feature of the Domain Name System (DNS) that enables authenticity verification of the responses **(10x increase of memory consumption)**
- For **2Mio DNS record** (1Mio Participants), the BIND9 server consumes approx. **1,6GB** of physical memory (RAM) and 5GB disk space.
- DNSSEC re-signing of **5Mio** DNS records: **1d 12h**.
- Reboot DNS server: (**2Mio** DNS records) takes **20+ minutes**.

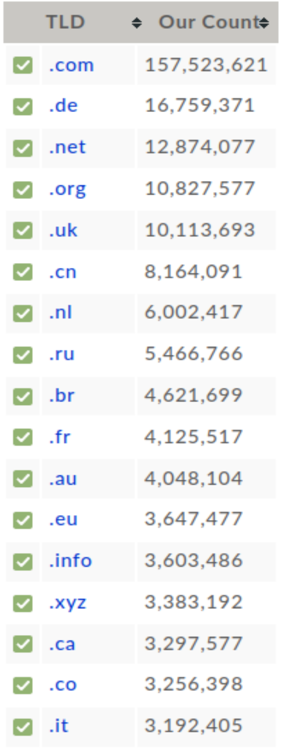
EDelivery SML infrastructure with the: Bind9

Features	In memory	DLZ (Dynamically Loadable Zones)
Startup time	Slow	Fast
Response time	Fast	Slow **DLZ is not recommended for use on high-query-volume servers**
DNSSEC extension	Build in feature	Not an (out-of-the-box) option
Memory	High consumption	Low consumption
Replicas (Master/Slave)	***AXFR*** *(All/Full zone transfer) and* ***IXFR*** *(Incremental zone transfer)*	*Only* ***AXFR*** *No automatic replica update*

Alternatives: CoreDNS, PowerDNS, Amazon Route 53, Custom Java implementation, …

Challenges: .edelivery.tech.ec.europa.eu.

- **Top DNS domain transition**: **.edelivery.tech.ec.europa.eu.**
  - Facilitate **the establishment** of various exchange networks:
    - Minimizing the costs for Proof of Concept (PoC), demos; for networks to discover optimal configuration (reuse of eDelivery example implementation)
    - Lowering the "cost activation barrier" for network establishment
    - Ensuring interoperability (Maintaining common profiles/enable various vendors)
    - Sharing good practices
    - Not intended for big productions (Resources and Responsibilities)
  - Multiple domains/Networks such as: Invoice exchange(PEPPOL), Registered delivery(ERDS), eHealth record exchange, … (Reusability, reduce investment costs, …)
- **Big DNS zone**: DNS software solutions are optimized according to user requirements. Most free/opensource authoritative DNS servers handle between a few dozen to several Million DNS records.
- **Legal restrictions of the top DNS domain owners**: DNS domains are bought/loaned from the domain registrar. Single top domain:
  - Pros
    - Network owner has better control over the registered users
    - Increased security and network control
  - Cons
    - The domains (including the top-level domains (TLDs)) are under the legal jurisdiction of the country in which the domain registrar and subdomain owner has its seat.



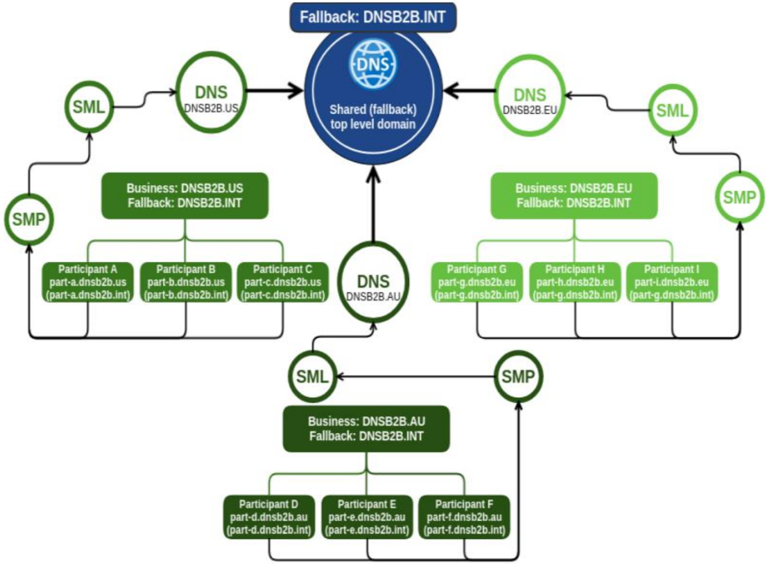
	TLD ⬍	Our Count⬍
☑	.com	157,523,621
☑	.de	16,759,371
☑	.net	12,874,077
☑	.org	10,827,577
☑	.uk	10,113,693
☑	.cn	8,164,091
☑	.nl	6,002,417
☑	.ru	5,466,766
☑	.br	4,621,699
☑	.fr	4,125,517
☑	.au	4,048,104
☑	.eu	3,647,477
☑	.info	3,603,486
☑	.xyz	3,383,192
☑	.ca	3,297,577
☑	.co	3,256,398
☑	.it	3,192,405

(Domain tools, Retrieved On: 03/04/2024)

Option 1: Federated DNS services using fallback

Most enterprises do not perform business globally, the regional SML service providers register participants in the regional DNS top domain e.g.:

- USA: dnsb2b.us, Singapore: dnsb2b.sg, Europe: dnsb2b.eu, Australia: dnsb2b.au, …
- and one international fallback domain, e.g. dnsb2b.int.



Advantages:

- Smaller regional DNS zones (lower DNS maintenance costs)
- Regional legal jurisdiction for the top domain.
- Robust international network. Issues in one region does not produce issues globally.
- Network owner (can) define the official list of top domain
- Global discovery can be provided as additional service by the regional SML service provider (Additional fees).
- The upgrade of the discovery clients/libraries to be able to use an additional top domain is not complex.

Disadvantages:

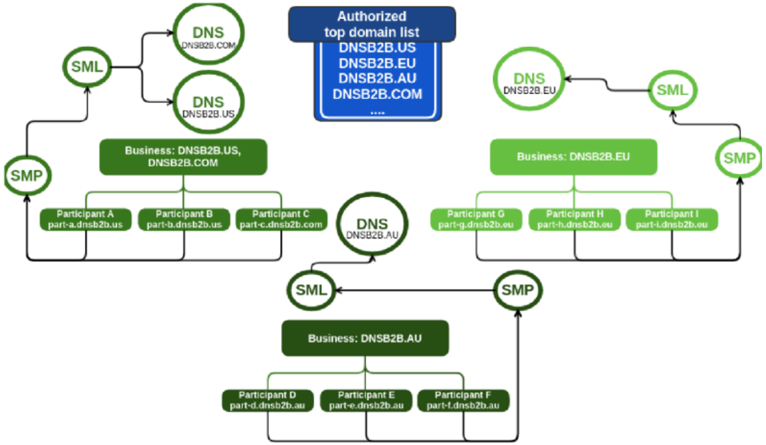
- The discovery clients must be able to configure two top DNS domains: regional top domain and international top domain.
- It is not clear who manages/owns the international DNS zone.

Security consideration:

- Same identifier can be registered on two domains with different targeted SMP data.

Option 2: Federated DNS services using list of top domains

Message exchange network defines a list of the authorized DNS domains that offer SML DNS services for the business domain. If dynamic discovery does not resolve one DNS domain, it can try the next one in the list, etc. The list order can be different for various regions to increase lookup efficiency.



Advantages:

- Smaller regional DNS zones (lower DNS maintenance costs).
- SML service providers operates only the regional DNS service.
- AP sets discovery list order which suits best for the region (Enhancement: logic based on participant identifier).
- Network owner (can) manage the official list of top domain
- Robust international network. Issues in one region does not produce issues globally
- No need for "international" SML service provider

Disadvantages:

- The discovery clients must be able to configure multiple top DNS domains
- Slow discovery when multiple top domains are queried.

Security consideration:

- Same identifier can be registered on two domains with different targeted SMP data.

Thank you