Date: 20-09-2024

Author: Fedor Kaufman, Huibert Alblas

DNS as a service discovery mechanism for BDI

Executive summary

Federated data sharing initiatives currently arise mostly among groups of organization who know and trust each other. These parties know where to find each other's endpoints, as they are exchanged in (a manual manner) during the setup phase. Sharing data in a federated manner with unknown parties introduces the challenge of discovering each other's endpoints.
It was noticed that the internet solved this problem already a long time ago by using the Domain Name System (DNS).

Topsector Logistiek published a whitepaper with a design for DNS as federated service discovery mechanism.[1] This report describes the steps taken to realize this design in a proof of concept (PoC), and concludes that it works as intended.

[1] Studie DNS als service detectie mechanisme voor BDI: https://topsectorlogistiek.nl/studie-dns-als-service-detectie-mechanisme-voor-bdi/

Table of Contents

Introduction

Unlike a centralized database, DNS operates across a vast network of interconnected servers worldwide, each playing a role in translating user-friendly domain names into machine-friendly data records (often, but not limited to, URL's). These point users to alternative domains, email servers, and eventually to a machine readable IP address. This distributed architecture not only enhances the speed of queries and reduces the burden on individual servers but also fortifies the system against potential disruptions or attacks. The network of DNS servers is traditionally provided by Internet providers, but nowadays also by large companies such as Microsoft, Google and Cloudflare. These organizations do not charge for the use of their DNS service.

Topsector Logistiek has published a whitepaper outlining a design for leveraging DNS as a federated service discovery mechanism.[2] This report covers the process and learnings of realizing this in a Proof of Concept (PoC).

Setup

The realization of DNS as a service registry for service discovery has been split into two parts. At first the DNS registry of the domain name 'bdi-demo.nl' is populated with the records inspired from the samples in the DNS study[3]. Thereafter the DNS is queried from a Python script.

Populating the DNS registry

The usecase includes 2 services that are presented via DNS, an iShare service and a Pulsar service. Figure 1 shows the content of the DNS in a graph structure.

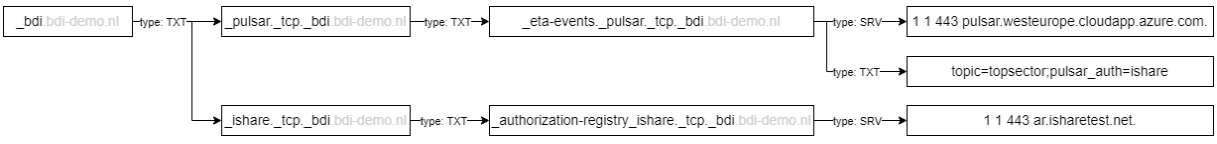

Figure 1 - DNS content visualized in a graph structure

DNS records contain 4 parts:

Name: The name of the subdomain

Time to live: The duration the record remains in the DNS caches.

Type: DNS record type

Value: The text value, target IP, or target url

[2] Studie DNS als service detectie mechanisme voor BDI: https://topsectorlogistiek.nl/studie-dns-als-service-detectie-mechanisme-voor-bdi/

[3] Studie DNS als service detectie mechanisme voor BDI

Table 1 shows the tabular representation of Figure 1. These values can be entered in almost any DNS service. (Note: TTL = 1 min for all records)

Name	Type	Value
_bdi	TXT	_pulsar._tcp._bdi.bdi-demo.nl
	TXT	_ishare._tcp._bdi.bdi-demo.nl
_pulsar._tcp._bdi	TXT	_eta-events._pulsar._tcp._bdi.bdi-demo.nl
_eta-events._pulsar._tcp._bdi	TXT	topic=topsector;pulsar_auth=ishare
_eta-events._pulsar._tcp._bdi	SRV	1 1 443 pulsar.westeurope.cloudapp.azure.com.
_ishare._tcp._bdi	TXT	_authorization-registry._ishare._tcp._bdi.bdi-demo.nl
_authorization-registry._ishare._tcp._bdi	SRV	1 1 443 ar.isharetest.net.

Table 1 - DNS records

requesting DNS records

In order to retrieve the data from the DNS, one starts by querying a DNS service from the well known subdomain for a particular domain. For example _bdi.bdi-demo.nl. This query will find two TXT records. The values from these TXT records will be used to query the DNS service again, until all information has been retrieved. In the end it is known that 2 services are presented, an iShare authorization registry located at ar.isharetest.nl, and a pulsar eta-events service located at pulsar.westeurope.cloudapp.azure.com.

```
Service: pulsar, Protocol: tcp
    Instance: eta-events
        Url:        _eta-events._pulsar._tcp._bdi.bdi-demo.nl
        Extra info:   topic=topsector;pulsar_auth=ishare
        SRV record:   prio: 1 | host: pulsar.westeurope.cloudapp.azure.com | port: 443 | weight: 1
Service: ishare, Protocol: tcp
    Instance: authorization-registry
        Url:        _authorization-registry._ishare._tcp._bdi.bdi-demo.nl
        SRV record:   prio: 1 | host: ar.isharetest.net | port: 443 | weight: 1
```

Request via API

In order to simplify the Querying of the DNS, an API service has been created. When supplying a domain to this discovery service, it returns the supported services with their hostname, port and additional settings to access this service in a JSON format.

https://servicediscovery.bdi-demo.nl/discover/_bdi.{domain}

For example:

https://servicediscovery.bdi-demo.nl/discover/_bdi.bdi-demo.nl

The result of the request of the DNS records is a JSON structure, showing the services and their protocol, and the specific instances and how to connect to them.

Security

When using DNS, it is crucial that there is no doubt whether the data we receive comes from the real DNS. For this we successfully use DNSSEC, a widely supported standard for securely requesting DNS records.

Semantics

The DNS Discovery standard provides flexibility in naming the services, instances and extra information. It is important for users to know what to expect when querying the DNS records, therefore it a standard list for naming services, instances and extra information should be defined. The MIME type system could be taken as an example, as it defines names, but does not restrict users to these names only.

Conclusion

The concept of 'DNS as a service registry' works in practice to find which services are exposed. It fits within the BDI concept and works together with the other BDI components.

The user of the services only needs a domain name in order to get all information about the provided services from the DNS. This makes a dynamic system, where services of different service providers act as if it’s one system. And where the hosting of these services can be moved without the need of informing all users.

References

BDI
https://bdinetwork.org

BDI service discovery
https://topsectorlogistiek.nl/studie-dns-als-service-detectie-mechanisme-voor-bdi/