DNS Service Discovery

basic data infrastructure

Topsector Logistiek

Colofon

DNS Service Discovery

Auteur
Remco van 't Veer

Januari 2024

basic data infrastructure

Topsector Logistiek

Inhoudsopgave

1 Service Discovery

In een situatie waar verschillende partijen data met elkaar willen delen is het belangrijk dat zij elkaars data gemakkelijk kunnen vinden. Hiervoor moeten afspraken gemaakt worden over wat er hoe gedeeld gaat worden en waar die gegevens vandaan komen.

In deze memo richten we ons op Service Discovery - een mechanisme waarmee systemen elkaar gemakkelijk kunnen vinden – en dan met name discovery met behulp van DNS[1].

1 *Domain Name System, het systeem dat namen aan computer adressen koppelt.*

2 DNS

DNS is een van de oudste standaarden op het Internet welke nog steeds gebruikt wordt. Elke organisatie gebruikt al DNS om gedeeltes van hun infrastructuur publiek te maken. Denk hierbij aan e-mail en websites. Daarnaast is DNS de ruggengraat van veel federatieve diensten zoals VoIP[2], LDAP[3] en XMPP[4] (merk op dat e-mail ook een federatieve dienst is).

Een DNS-zone[5] wordt door een organisatie zelf beheerd, of het beheer wordt uitbesteed. Dit maakt het mogelijk om voor 'hun deel van het Internet' vrij in te vullen welke "namen" daaronder vallen. In deze zones kunnen weer 'subzones' gemaakt worden, welke door eigen afdelingen beheerd kunnen worden, waardoor een hiërarchische structuur ontstaat.

2 Voice over IP, telefonie via het Internet.
3 Lightweight Directory Access Protocol, gebruikers informatie opzoeken.
4 Extensible Messaging and Presence Protocol, veel gebruikt voor chat en IoT toepassingen.
5 Een specifiek deel van de de namen in de DNS.

3 Hoe?

Bij e-mail werkt het - vereenvoudigd - als volgt. Voor elk domein waar men e-mail op ontvangen wil, worden door de organisatie *MX*-records[6] aangemaakt welke verwijzen naar servers waarop e-mail ontvangen kan worden. Bij het versturen van een e-mail wordt aan een DNS server gevraagd welke *MX*-records er bestaan voor het ontvangende domein en contact met die server opgenomen om het bericht te bezorgen. Daarnaast kunnen er ook nog *TXT*-records[7] aangemaakt zijn waarin cryptografische sleutels staan waarmee de origine van de e-mail bewezen kan worden.

De DNS record typen staan vast. Zo zijn *MX*-records bedoelt voor e-mail en niet voor iets anders. Gelukkig is een *TXT*-record vrij te gebruiken en kunnen er meerdere records met dezelfde naam geregistreerd worden waardoor dus lijsten met informatie via DNS opgevraagd kunnen worden. Bij e-mail wordt dit bijvoorbeeld gebruikt als de eerste server waarnaar een *MX*-record verwijst niet bereikbaar is de volgende geprobeerd wordt.

Hieronder beschrijven we de verschillende componenten voor service discovery. Daarna, in sectie 3.5 beschrijven we een concreet voorbeeld van een organisatie met meerdere services.

Voor service discovery zijn de volgende ingrediënten nodig:

3.1 Well-known subdomain

Door een "well-known subdomain" te introduceren kunnen we een punt aangeven met een voorspelbare naam waar opgevraagd kan worden welke diensten er beschikbaar zijn; Service Discovery dus.

Bijvoorbeeld: `_bdi.acme-corp.com.` Dit kan meteen het hoofdniveau zijn van een DNS-zone en toegewezen aan de juiste administrateurs.

Merk op dat dit geen *hostname* is maar een *domainname*. Een hostname, zoals gebruikt bij websites en e-mail, mag geen underscore (_) tekens bevatten. Het gebruik van een underscore geeft aan dat het om een "speciaal" record gaat.

3.2 Discovery

Nu we een duidelijk beginpunt hebben, kan dat ingericht worden zodat er iets te ontdekken valt. Dit doen we met *TXT*-records omdat we daar alle vrijheid hebben en nog meer "speciale" records kunnen maken in ons "well-known subdomain". Hierbij volgen we de vormen:

- `_bdi.<subdomain>` ***`TXT-records`***
  Levert lijst van alle diensten typen (services) voor dit subdomain in de onderstaande vorm.

- `_<service>._<proto>._bdi.<subdomain>` ***`TXT-records`***
  Waar *proto* het Internet protocol is dat de dienst gebruikt (`tcp` of `udp`) en *service* het dienst type is (`ldap, mqtt` etc.). Levert lijst met alle diensten van dat type (instances) in de onderstaande vorm.

- `<instance>._<service>._<proto>._bdi.<subdomain>` ***`TXT-records`***
  Waar *instance* een vrij te kiezen naam is.

6 *MX staat voor "mail exchanger".*
7 *In TXT records kan "vrije" tekst opgeslagen worden.*

3.3 SRV-records

Nu hebben we daadwerkelijke diensten te pakken maar weten nog niet waar we ze precies te vinden is. Underscores mogen immers niet in hostnames voorkomen en het is niet wenselijk een direct *A*-record[8] of *CNAME*-record[9] aan te maken voor deze server. Daarom wijken we uit naar *SRV*-records[10]. Deze records bevatten:

- ***target***
  De hostname of het IP-adres waar deze dienst te bereiken is.

- ***port***
  Het portnummer waar deze dienst te bereiken is.

- ***priority*** en ***weight***
  Waarden die gebruikt worden om een record te kiezen als er meerdere endpoints beschikbaar zijn voor deze dienst.

Als er meerdere *SRV*-records bestaan voor een dienst moeten de endpoints waar naartoe verwezen worden precies dezelfde dienst leveren. De *priority* en *weight* gegevens worden gebruikt om uit de lijst records de beste kandidaat te kiezen (zie RFC 2782 voor meer informatie).

Nu weten we waar we informatie vandaan moeten halen, met welk protocol, op welke server en via welk portnummer.

3.4 TXT-records

Voor sommige diensten zijn de gegevens uit het *SRV*-record niet genoeg. Daarvoor is het mogelijk om nog extra *TXT*-records aan te maken met dezelfde naam als het *SRV*-record. Wat hierin staat is afhankelijk van de specifieke dienst en het gebruikte protocol maar hier kan gedacht worden aan zaken zoals de benodigde rechten om gebruik te kunnen maken de dienst.

Informatie wordt in deze records aangeven als attributen met een naam en een waarde welke gekoppeld worden met een `=` teken en attributen worden gescheiden door een `;` teken. Hoewel alle tekens mogelijk zijn in *TXT*-records, worden er door DNS service providers vaak restricties gelegd op het gebruik. Helaas zijn deze regels niet bij alle providers hetzelfde maar alle providers zullen wel alle cijfers, letters, **+**, **/**, **=**, **;** tekens en spaties ondersteunen[11].

Een voorbeeld: `quality=high; resolution=seconds`

8 Adres record, een hostname naar een IP-adres.
9 Common name record, een hostname alias die weer naar een andere hostname verwijst.
10 Service records beschrijven waar een server is.
11 Met letters en cijfers worden de ASCII standaard letters en cijfers bedoelt.

3.5 Een voorbeeld

We nemen als voorbeeld ACME Corporation. Zij hebben als "well-known subdomain":

- `_bdi.acme-corp.com`

De bijbehorende *TXT*-records vertellen dat zij SPARQL en MQTT endpoints hebben.

- `_bdi.acme-corp.com. 3600 IN TXT`[12]
  `"_sparql._tcp._bdi.acme-corp.com"`

- `_bdi.acme-corp.com. 3600 IN TXT`
  `"_mqtt._tcp._bdi.acme-corp.com"`

We zoomen in op MQTT en vinden daar:

- `_mqtt._tcp._bdi.acme-corp.com. 3600 IN TXT`
  `"warehouse-status-events._mqtt._tcp._bdi.acme-corp.com"`

- `_mqtt._tcp._bdi.acme-corp.com. 3600 IN TXT`
  `"logistic-events._mqtt._tcp._bdi.acme-corp.com"`

We vinden server met het *SRV*-record:

- `logistic-events._mqtt._tcp._bdi.acme-corp.com. 3600 IN SRV`
  `"1 1 443 mqqt.logistics.acme-corp.com"`[13]

- `logistic-events._mqtt._tcp._bdi.acme-corp.com. 3600 IN SRV`
  `"2 1 443 mqqt-backup.logistics.acme-corp.com"`

En extra informatie:

- `logistic-events._mqtt._tcp._bdi.acme-corp.com. 3600 IN TXT`
  `"queue=main; auth=ishare"`

We weten nu dat we voor *MQTT* berichten contact moeten maken met *mqqt.logistics.acme-corp.com* (en als deze niet beschikbaar is *mqqt-backup.logistics.acme-corp.com*) op poortnummer 443, dat alles wat interessant is te vinden is op queue *main* en dat autorisatie via *iSHARE* geregeld is.

3.6 Oorsprong

Het bovenstaande is losjes gebaseerd op de DNS-SD[14]. Deze standaard is echter niet bruikbaar omdat deze gebruik maakt van *PTR*-records welke erg onpraktisch in gebruik zijn omdat deze vooral gebruikt worden om ongewenste e-mail tegen te gaan en daarom door weinig DNS service providers aangeboden worden. Daarnaast wordt er meer controle over de record verondersteld dan providers toelaten; mogelijke tekens in naam en waarde bijvoorbeeld.

12 Met 3600 wordt aangeven dat het record een uur (3600 seconden) onthouden mag worden.
13 De getallen 1, 1 en 433 zijn respectievelijk de priority, weight en port van deze service.
14 Zie ook RFC 6763.

4 Beveiliging

Het DNS platform is beveiligd door middel van DNSSEC[15]. Het gebruik van DNSSEC is vereist voor een veilige implementatie van het hier beschreven mechanisme. DNSSEC is een wijd ondersteunde standaard en alle DNS service providers ondersteunen deze.

15 *Domain Name System Security Extensions, hiermee wordt voorkomen dat een ander zich voor kan doen als de getroffen organisatie en daarmee valse informatie verstrekt op logingegevens steelt.*

5 Tot slot

Het hier beschreven mechanisme is een aanzet voor een service discovery systeem en is daarmee niet compleet. Met name sectie 3.4 over het gebruik van *TXT*-records kan per *service type* verder uitgewerkt worden en is er waarschijnlijk behoefte aan afspraken voor de te kiezen *instance* namen in sectie 3.2.

DNS is een belangrijk onderdeel voor het goed functioneren van het Inter- net en daarmee gehard in de strijd, meerdere federatieve diensten maken al tientallen jaren succesvol gebruik van DNS als register en implementeren hiermee vormen van service discovery. Het beheer is gemakkelijk hiërarchisch te distribueren door middel van zones. Door deze eigenschappen is DNS een uitermate geschikte kandidaat voor de implementatie van service discovery.

Topsector Logistiek
Ezelsveldlaan 59
2611 RV Delft
+31 15 251 65 65
www.topsectorlogistiek.nl

Topsector Logistiek