digitale infrastructuur logistiek

Bevindingen DIL VGU Demo Fase 3

Joost Diepenmaat joost@jomco.nl
Remco van 't Veer remco@jomco.nl

2024-10-02

Dit document beschrijft onze bevindingen bij de implementatie van de VGU demo fase 3. We benoemen hier de pijnpunten, zodat deze als input kunnen dienen voor verbeteringen aan architectuur, componenten en documentatie.

Relevante BDI Building Blocks:

- Autorisatie
- Authenticatie
- Discovery
- Event Pub/Sub

Focus fase 3: gate-out events

In fase 1 blijft de oorspronkelijke vervoerder direct verantwoordelijk voor het plannen van een chauffeur; als deze de rit wil uitbesteden aan een externe partij, kan dat alleen door in het TMS van de vervoerder de externe chauffeur en wagen in te plannen.

In fase 2 willen we demonstreren hoe een opdracht uitbesteed kan worden aan een andere vervoerder die in het BDI netwerk is opgenomen, en na uitbesteding zijn planning en bijbehorende autorisaties kan beheren via het eigen TMS. We willen tegelijkertijd de afhankelijkheid van online services zoveel mogelijk beperken.

In fase 3 willen we demonstreren dat een verlader een update ontvangt als de lading is opgehaald bij het DC door middel van een gate-out event, welke via een event broker (Apache Pulsar) wordt gepropageerd.

Uitgangspunt voor de architectuur in fase 3 is dat we zoveel mogelijk gebruik maken van bestaande iSHARE-protocollen, -componenten en toepassing van het "data bij de bron"-principe.

Bevindingen

Inrichting topics en events

We hebben gekozen voor een topic per transportopdracht omdat dit de meest voor de hand liggende keuze is. Alle events met betrekking tot de opdracht worden gepubliceerd op dat topic.

Eigenaarschap van topics en events

In deze demo is de verlader de initiator van de transportopdracht en daarmee ook de eigenaar van het topic. De producent van een event is eigenaar van het event; in dit geval het DC.

Toegang tot topic

Voor Pulsar is een speciale autorisatie-module gemaakt om naar aanleiding van delegation-evidence in het AR van de topic-eigenaar toegang te verlenen tot het topic.

Zie ook Topsector-Logistiek/Apache-Pulsar-Auth-Plugin en met name org.bdinetwork.pulsarishare.authorization.

Delegation-Evidence bij uitbesteding aan derde

Toegang tot het topic voor een transporteur waaraan uitbesteed is, is net zo omslachtig als in fase 2. Hiervoor zijn extra policies en HTTP headers nodig om Pulsar duidelijk te maken namens wie zij toegang tot het topic wensen te krijgen. Hiervoor wordt door Pulsar de `Delegation-trail` header herkent met daarin een EORI welke aangeeft in wiens plaats de opdracht uitgevoerd wordt. Deze lijst kan dan door Pulsar gebruikt worden om het tussen liggende authorizatie-register te bevragen. Zie ook Referenties.

Dit is in deze demo niet geïmplementeerd omdat het implementeren van een directe transportopdracht al genoeg bevindingen heeft opgeleverd om bij stil te staan. De extra stap tot uitbesteding voegt daar weinig aan toe.

Data bij de bron

Om te zorgen dat notificaties (pulses) zo min mogelijk gevoelige data bevatten, wordt alleen een URL gepubliceerd naar event data. Dat betekent dat de partij die een event publiceert ook een endpoint beschikbaar moet stellen om deze te downloaden. Daarnaast moet een iSHARE token-endpoint aangeboden worden ter authenticatie voor de download, aangezien iSHARE authenticatie een mechanisme is dat al bij alle componenten bekend is.

Een uitdaging is dat er geen manier is om te achterhalen waar het token-endpoint voor een gegeven URL te vinden is. Hiervoor hebben we gekozen voor een

`WWW-Authenticate` header in het `401 Unauthorized` response waarin beschreven staat waar het endpoint is en wat de EORI van de server is (nodig om een `client_assertion` te kunnen opstellen). De consument van het event doet dus eerst een oproep naar de verkregen URL, krijgt dat een `401 Unauthorized` response met daarbij de informatie die nodig is om een token op te halen waarmee nogmaals een oproep gedaan kan worden.

Voorbeeld `WWW-Authenticate` header:

```
WWW-Authenticate Bearer
  scope="iSHARE"
  server_eori=*EORI-PRODUCER*
  server_token_endpoint=*TOKEN-URL-PRODUCER*
```

Alternatieve implementaties voor delen en afschermen van events

Er zijn een alternatieven ter sprake gekomen zijn bij het implementeren van de demo. Deze hebben we nu niet geïmplementeerd, maar kunnen in andere use-cases of verdere uitbreiding van de demo van pas komen.

Meesturen data met notificatie

Als bepaalde event data "niet-gevoelig" genoemd kan worden, zodat iedere partij die betrokken is bij een zending deze data ook mag inzien, is het ook mogelijk om deze data direct mee te sturen met de notificatie. De ontvanger kan dan bepalen of er meer informatie nodig is, en deze bij de bron ophalen zoals hiervoor beschreven.

Als de ontvanger dan vaak besluit dat er geen verdere data nodig is, omdat er al genoeg informatie is, of omdat de ontvanger kan zien dat het event niet relevant is, kan het aantal verdere requests naar de bron data terugdringen.

Opslitsen over meerdere topics/brokers

Als er structureel event data afgeschermd moet worden, is een opslitsing over meerdere topics ook een mogelijkheid. Als zendingen uitbesteed worden zou de uitbestedende partij een eigen topic kunnen inrichten, net als de verlader in de huidige opzet. Deze kan dan binnenkomende events filteren en uitwisselen tusssen het topic van zijn opdrachtgever en het eigen topic dat gedeeld wordt met de onderaannemers. Voor uitwisselen en filteren zijn dan wel extra componenten nodig.

Webhooks / long polling

In plaats van een externe broker is het ook mogelijk om notificaties te implementeren via een "long poll", waar consumers direct bij de bron wachten op nieuwe event data. Hierbij is er geen aparte broker meer nodig, deze functionaliteit kan direct geïmplementeerd worden bij de event bron.

Het Digitaal Stelsel Gebouwde Omgeving (DSGO) heeft een andere benadering met webhooks. Hierbij geeft de event bron subscribers direct een bericht (via een point-to-point request). Ook hierbij is geen aparte broker nodig.

Conclusie

Het gebruik van een *event broker* in deze opzet heeft de volgende gevolgen:

- de event broker wordt een extra partij in het afsprakenstelsel

  De event broker moet worden ge-onboard, een iSHARE token-endpoint implementeren en de *associate en autorisatie registers* bevragen om de toegang te verifiëren. Dit levert extra druk op deze componenten en introduceert foutpunten welke stabiele werking kunnen belemmeren.

- er is een ontdekkingsmechanisme (discovery) nodig om event brokers te vinden

  Op dit moment is er geen methode om aan te geven waar de event broker voor een transportopdracht gevonden kan worden. Dit zou onderdeel gemaakt kunnen worden van de transportopdracht data die gestuurd wordt vanuit het ERP naar de betrokken partijen. Het is ook mogelijk hiervoor DNS discovery in te zetten. Dit vergt meer onderzoek.

- eigenaarschap van en toegang tot topics en events in deze opstelling is niet op de proef gesteld

  Het versturen van slechts een gate-out event door het DC geeft geen goed beeld van de rollen die belegd worden in de hele levenscyclus van een transportopdracht. Het onderwerp *wie wat mag zien* is belangrijk in de BDI en komt in deze fase duidelijk naar voren. De hier gekozen aanpak voldoet alleen voor dit ene gate-out event, maar zodra er andere event typen bij gaan komen, gaat afscherming een rol spelen van de event data en *data bij de bron* is hier geen oplossing voor, omdat het feit dat een DC een event verstuurt, al veel te veel prijsgeeft.

- het gebruik van websockets om met Apache Pulsar te verbinden kan een belastende werking hebben op IT-netwerken

  In deze aanpak worden de websockets mogelijkheid van Pulsar gebruikt om notificatie uit te wisselen tussen de systemen omdat websockets een betrouwbare manier zijn om dergelijk verbindingen op te zetten over het internet. Bij het opschalen van deze aanpak zullen consumenten veel websockets open moeten houden om van alle transport opdrachten op de hoogte te blijven. De schaalbaarheid hiervan moet worden uitgezocht.

De toepassing van *data bij de bron* in deze opzet heeft de volgende gevolgen:

- een producent van events moet een publiek bereikbaar end-point aanbieden om events op te halen
- een producent moet een authenticatie mechanisme implementeren om dit end-point te beschermen

- een producent moet ergens kunnen verifiëren of een partij die een event komt ophalen daar ook recht op heeft

  In deze opstelling lijkt het voor de hand te liggen dat zowel de opdrachtgever (verlader) als het transportbedrijf dat bij het DC komt deze gegevens op mag halen. Maar zodra er meer partijen betrokken worden in de opdracht wordt dit veel ingewikkelder. Denk hierbij aan track-and-trace gegevens voor afnemers die de verlader opdracht hebben gegeven, het DC heeft hier geen weet van. Dit kan bijvoorbeeld door middel van Delegation-Evidence zoals bij uitbesteding aan derde aangepakt worden maar is in deze fase niet geïmplementeerd.

Referenties

Zie ook: “Report DNS Pulsar VGU 1.0.pdf” voor een gedetailleerde beschrijving van de Apache Pulsar implementatie.