Overgang naar vernieuwde XML Interface via Hub

Onderwerp	:	Overgang naar vernieuwde XML Interface via Hub
Datum	:	2020-10-06
Versie	:	1.0

connecting customers

ANVA

In dit document wordt de overgang naar de vernieuwde XML Interface via Hub beschreven. Veranderingen omvatten onder andere de aanpassingen in de route van het berichtenverkeer en de wijzigingen ten aanzien van authenticatie.

Het doel van het document is tweeledig. Enerzijds willen we met dit document inzicht geven in de achtergrond van deze wijziging. Anderzijds willen we met dit document inzicht geven in de stappen die gezet moeten worden om de overgang te bewerkstelligen.

Inhoudsopgave

Aanleiding voor vernieuwing

De XML Interface is een belangrijk onderdeel van de ANVA Backoffice applicatie. Het wordt in veel uiteenlopende situaties gebruikt door kantoren, partners en andere derde partijen om buiten ANVA om ontwikkelde toepassingen gebruik te laten maken van data en business logica in ANVA Backoffice. In veel gevallen worden deze applicaties uitgevoerd op een andere server dan de ANVA Backoffice-server.

Om het berichtenverkeer mogelijk te maken wordt onder andere gebruikgemaakt van een door ANVA ontwikkelde applicatie genaamd AWACS. Deze applicatie verzorgt de ingang en routering van het XML-bericht. Om een bericht aan AWACS aan te kunnen bieden zal in de praktijk meestal ook een poort in de firewall opengezet moeten worden. Daarnaast bestaat binnen AWACS de optie om een sleutel in te richten die ook in het binnenkomende bericht aangeleverd dient te worden. In de praktijk zien we dat het uitvoeren van deze inrichting veelvuldig vragen oplevert en soms ook niet correct wordt toegepast, met vervolgens risico's op het gebied van informatiebeveiliging tot gevolg. Als leverancier van de XML Interface vinden we dat deze situatie niet langer verantwoord is.

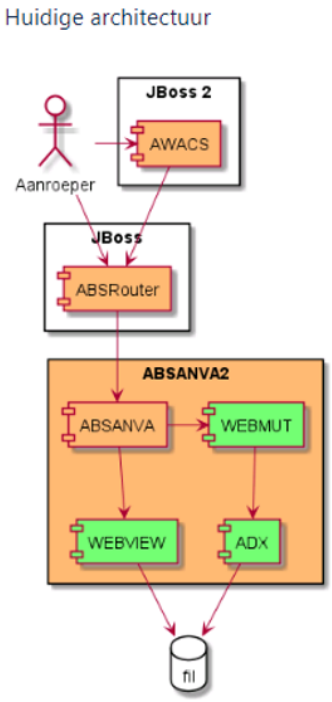
ACHTERGROND **XML** INTERFACE

Hoe werkt het nu?

- Aanroep via AWACS indien verzoek vanaf buiten het domein van de ANVA Backoffice-server plaatsvindt. (vb. cloudapplicatie)
- Aanroep via ABSRouter voor 'interne' verzoeken

Waarom gaat het veranderen?

- AWACS en ABSRouter zijn sterk verouderde programmatuur
- Beveiligingsrisico's aan gebruik AWACS
- De toepassing van de XML Interface moet worden vastgelegd ten behoeve van vernieuwd contractmodel en beter kunnen uitvoeren van lifecycle management



Naast de genoemde beveiligingsrisico's weten we ook niet in voldoende mate op welke manieren er gebruik wordt gemaakt van de XML Interface. Door de jaren heen zijn er veel uiteenlopende functies aan de XML Interface toegevoegd, waarbij sommige functies qua werking ook sterk op elkaar lijken. Bij het uitbreiden of aanpassen van de werking van ANVA Backoffice moet ook met al deze ontwikkelde functies rekening worden gehouden. Om het overzicht te kunnen bewaren en efficient uitbreidingen en onderhoud uit te voeren is het noodzakelijk om beter inzicht te krijgen in het gebruik van de diverse mogelijkheden van de XML Interface. Hiertoe willen we het gebruik van de XML Interface beter in kaart gaan brengen door middel van het tellen van de functies en entiteiten die worden aangeroepen.

Tot slot is deze telling ook noodzakelijk voor het onlangs vernieuwde contractmodel met als basis het daadwerkelijke gebruik van onze applicaties.

connecting customers
ANVA

Vernieuwde XML Interface via Hub

Zoals uit de achtergrond blijkt hebben we bij ons bij de vernieuwing hoofdzakelijk gericht op het verbeteren van de informatiebeveiliging en tellen van het gebruik. Ten aanzien van de structuur van de XML-berichten is vrijwel niets gewijzigd.

Om de gegevensbeveiliging beter te kunnen waarborgen maken we in de vernieuwde oplossing gebruik van RabbitMQ als message broker. Dit betekent dat niet langer berichten worden ingeschoten op de ANVA Backoffice-server. De ANVA Backoffice-applicatie zet zelf een uitgaande verbinding op met de RabbitMQ-server om daar berichten op te halen die verwerkt moeten worden. Deze opzet elimineert de noodzaak voor het openzetten van poorten voor binnenkomend verkeer in de firewall. Daarnaast wordt bij de verbinding tussen ANVA Backoffice-applicatie en RabbitMQ-server standaard (en zonder uitzondering) gebruikgemaakt van het TLS-protocol, waardoor de privacy en integriteit van het berichtenverkeer altijd gewaarborgd is.

De XML-berichten kunnen alleen via een beveiligd endpoint op ANVA Hub worden aangeboden. Ook hierbij wordt zonder uitzondering gebruikgemaakt van het TLS-protocol voor de encryptie van berichten. Daarnaast dient ook altijd een geldig token in de header van het bericht meegestuurd te worden. ANVA Hub zorgt na de validatie van het bericht inlusief token voor de plaatsing van het bericht op de RabbitMQ-server.

Op ANVA Hub wordt een telling bijgehouden van de aangeroepen functies en entiteiten in de XML-berichten. Er wordt geen telling of andere vorm van opslag bijgehouden over de labels en labelwaardes in de XML-berichten. In het applicatielandschap van ANVA vindt ook geen opslag plaats van de aangeleverde XML-berichten en/of antwoorden.

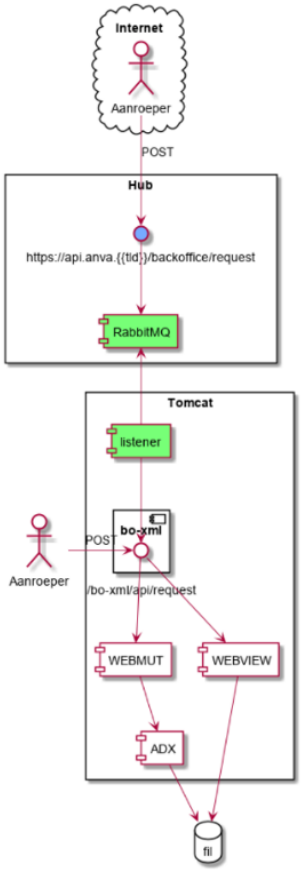
VERNIEUWDE **XML** INTERFACE

Hoe werkt vernieuwde api?

- Aanroep via endpoint op Hub-platform
- Validatie van authenticatie (jwt) op basis van OAuth 2.0 protocol + OpenID Connect layer
- Vluchtig bericht op RabbitMQ-server
- ANVA Backoffice haalt bericht zelf op via uitgaande verbinding (listener) voor verwerking

Voordelen

- Geen poort openzetten/forwarden in firewall voor binnenkomend verkeer
- Expliciete authenticatie is nu vereist, dus service kan niet meer per ongeluk voor iedereen open worden gezet door configuratiefout of ontbrekende configuratie
- Beter inzicht in gebruik van interface tbv contracmodel en lifecycle management door ANVA



connecting customers
ANVA

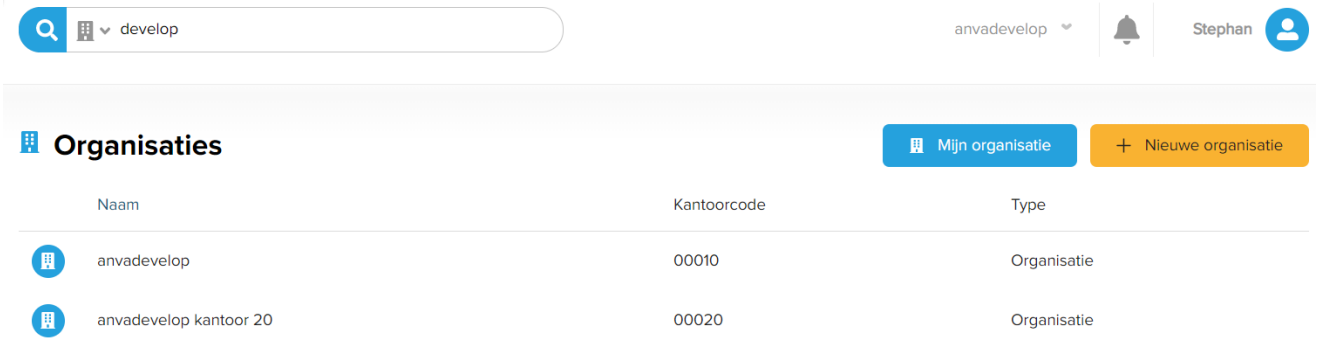
Organisatie en gebruikersaccount aanmaken op ANVA Hub

Deze actie moet door een medewerker van ANVA worden uitgevoerd.

Pad: https://hub.anva.io (productiedomein)

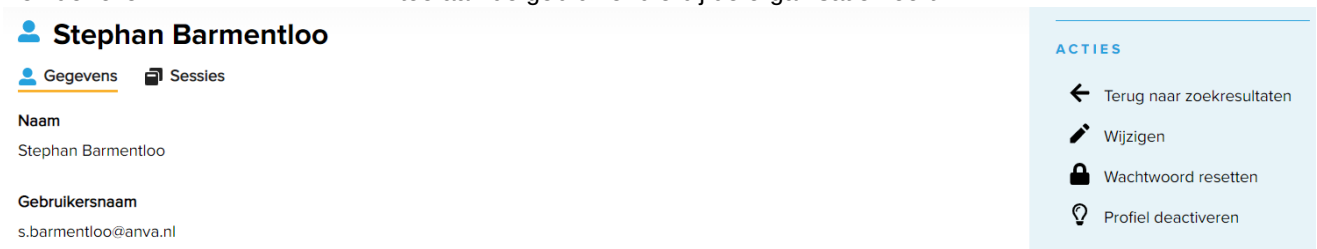
Pad: https://hub.anva.cloud (acceptatiedomein)

1. Controleer of de organisatie al aanwezig is op ANVA Hub.

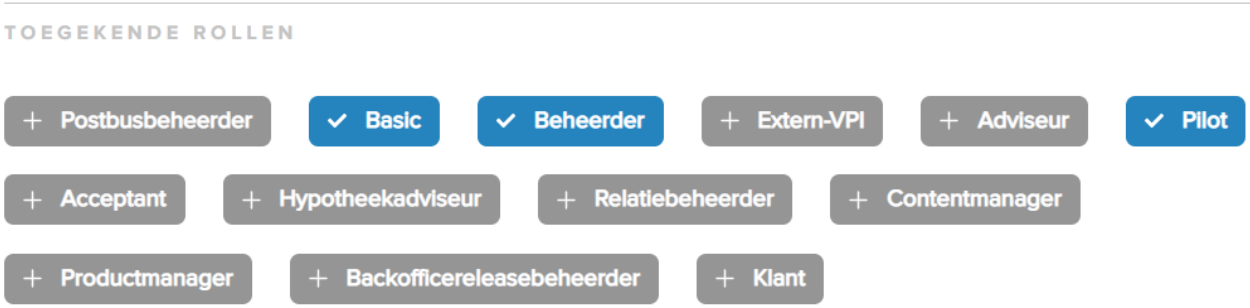


2. Indien de organisatie niet aanwezig is, maak deze aan inclusief een gebruiker voor de beheerder van de organisatie.

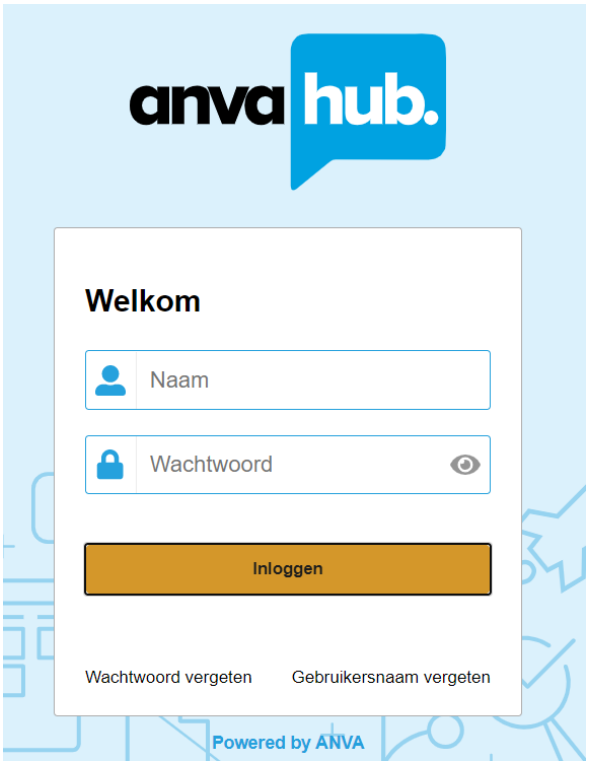
3. Ken de rollen ‘Beheerder’ en ‘Pilot’ toe aan de gebruiker die bij de organisatie hoort.

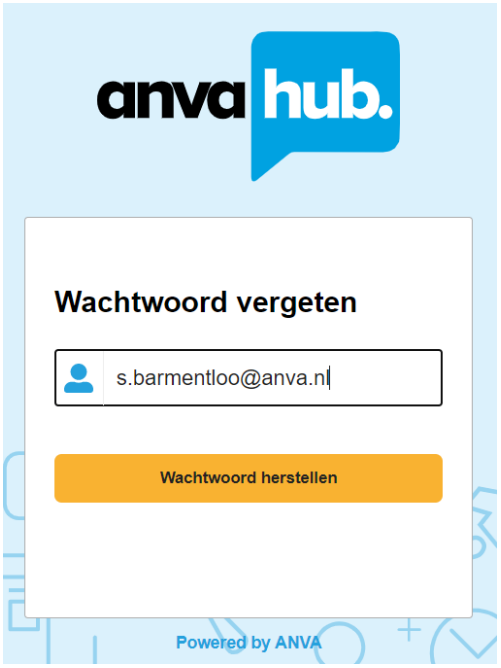


connecting customers
ANVA



4. Instrueer de beheerder van de organisatie om via het ‘wachtwoord vergeten’-proces een nieuw wachtwoord aan te maken voor het account en daarmee te activeren.





connecting customers
ANVA

Wachtwoord herstel ANVA Hub

N noreply@anva.io(noreply@anva.io via amazonses.com)
Aan Stephan Barmentloo

De werkelijke afzender van dit bericht verschilt van de normale afzender. Klik hier voor meer informatie.

Geachte heer/mevrouw,

U heeft een herstel wachtwoord aangevraagd

Ga naar https://api.anva.cloud/identity/forgot-password/reset?username=s.barmentloo@anva.nl&token=fhyppMgzUIYkiAwhihmVylNiDSvPni

Met vriendelijke groet,

ANVA Hub

connecting customers
ANVA

OpenID client aanmaken en configureren op ANVA Hub

Ten behoeve van authenticatie moet er een OpenID client worden aangemaakt. Deze actie kan door een medewerker van Customer Support worden uitgevoerd zodra zij de aanvraag en toestemming hebben gekregen van de beheerder van de organisatie.

Zodra de ANVA medewerker toestemming heeft, zal hij/zij een gebruiker en OpenID aanmaken op ANVA Hub. De beheerder van de organisatie ontvangt vier gegevens die de externe partij nodig heeft:

- Tenantcode/organisatiecode
- OpenID Client ID
- OpenID Client Secret*
- Domein/omgeving

  * Het secret is niet zichtbaar voor een ANVA medewerker, deze moet de beheerder zelf vernieuwen vanwege veiligheidsredenen. Het secret kan daarna ook op ieder moment worden vernieuwd.

Als externe partij ontvang je al deze gegevens van de beheerder van de organisatie. ANVA mag deze gegevens vanwege veiligheidsredenen niet direct aan de externe partij verstrekken. Zodra de OpenID is aangemaakt is hij te beheren door een beheerder van de organisatie.

Authenticatie token opvragen via OpenID Connect client credential flow

De OpenID Connect client credential flow kan worden gebruikt voor authenticatie wanneer het berichtenverkeer plaatsvindt tussen een externe applicatie en ANVA Hub, waarbij het niet van belang is dat de authenticatie op gebruikersniveau plaatsvindt.

Onderstaand voorbeeldbericht voor het verkrijgen van een authenticatietoken kan worden gebruikt op het acceptatiedomein van ANVA Hub (.cloud)

```
1. POST /identity/token HTTP/1.1
2. Host: api.anva.cloud
3. authorization: Basic
   YTRhYjkwYzEtMzczNi00NTExLWE1NjQtYjRkODgxZDBmYjA5OlNjdmF2bHNlQXJJb0dMUnFxS
   EZsWEdienVmT2xvRg
4. Content-Type: application/x-www-form-urlencoded
5. scopes=Basic orgCode:anvadevelop&grant_type=client_credentials
```

Regel 1 beschrijft het endpoint waar een POST-request naar verstuurd kan worden

Regel 2 beschrijft het (acceptatie)domein van ANVA Hub waar de request naar verstuurd kan worden

Regel 3 beschrijft de header van de request, waarin een key ‘authorization’ is opgenomen. De value van de key bevat de waarde ‘Basic’ met een spatie gevolgd door een base64-encoded string van het clientId en clientSecret. In bovenstaand voorbeeld de combinatie ‘a4ab90c1-3736-4511-a564-b4d881d0fb09:ScvavlseArIoGLRqqHFlXGbzufOloF’.

Regel 4 beschrijft eveneens de header van de request, waarin een key ‘Content-Type’ is opgenomen. De value van de key bevat de waarde ‘application/x-www-form-urlencoded’ om het formaat van de response aan te geven.

Regel 5 beschrijft de body van de request, waarin 2 keys zijn opgenomen. De eerste key ‘scopes’ met als value ‘Basic orgCode:anvadevelop’ geeft aan welke subset aan rechten het token moet bevatten en voor welke organisatie het token gebruikt mag worden. Zowel de opgegeven rechten als organisatie moeten uiteraard aan de gebruikte OpenID client zijn toegekend; het is dus niet mogelijk om meer rechten aan te vragen of bij een andere organisatie ‘in te loggen’ dan op basis van de configuratie van de OpenID client is toegestaan. De tweede key in de body betreft ‘grant_type’ met als value ‘client_credentials. Deze key en value geeft aan op basis van welke OpenID Connect methode een token verkregen moet worden. De client_credential methode is geschikt voor tokens die worden gebruikt bij systeem naar systeem berichtenverkeer.

De response kent de onderstaande indeling, waarbij de key ‘access_token’ het daadwerkelijke token (jwt) bevat, waarmee authenticatie uitgevoerd kan worden op de endpoints van ANVA Hub, waaronder ook het endpoint voor het XML Interface-berichtenverkeer.


```
{
    "access_token":
"eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJvcmdhbml6YXRpb25jb2RlIjoiYW52YWRldmVsb3
AiLCJjbGllbnRpZCI6ImE0YWI5MGMxLTM3MzYtNDUxMS1hNTY0LWI0ZDg4MWQwZmIwOSIsImlzcyI6Ik
FOVkEiLCJhY2NvdW50dHlwZSI6IlN5c3RlbSIsImFudmF1c2VybmFtZSI6IlNURVBIQU5CIiwiZ3JvdX
BzIjpbIjEwMCJdLCJvbkJlaGFsZk9mVXNlcm5hbWUiOiJzdGVwaGFuYiIsIm0ySWQiOiI5NzEzOTQ2My
0xNjI4LTRlZjItODQ4OS0xZmRlOGI2YzQ1MDkiLCJvbkJlaGFsZk9mQW52YVVzZXJuYW1lIjoiU1RFUE
hBTkIiLCJvcmdhbml6YXRpb25uYW1lIjoiYW52YWRldmVsb3AiLCJvcmdhbml6YXRpb24iOiI3ZTZiYj
E2MC05MWQ5LTQwOTMtYmM1MC05Njk5ZDQ0NmU3NzQiLCJleHAiOjE2MDE5Njc3MDQsImlhdCI6MTYwMT
kzMTcwNCwianRpIjoiMTFlZTU5ODctMDU2YS00ZjJmLTg0N2EtMzhiYTQyMGVlMzJlIn0.qJTnF6ZB7z
qje9I_S2JoqaHShza5OndKCE_Blhm-KKQ",
    "token_type": "Bearer",
    "expires_in": "3600"
}
```

XML Interface-bericht versturen via endpoint op ANVA Hub

Het XML Interface-bericht kan als POST-request via het /backoffice/request endpoint worden verstuurd. Het XML-bericht is vrijwel ongewijzigd ten opzichte van de oude situatie met AWACS en ABSRouter. Met name de header van het bericht is veranderd, aangezien er geen AWACS key en datasource meer meegestuurd hoeft te worden, maar in de plaats daarvan moet in de header van het bericht het jwt worden opgenomen.

Onderstaande request is een voorbeeld van een XML-bericht dat via het endpoint op ANVA Hub verstuurd kan worden.

```
1. POST /backoffice/request HTTP/1.1
2. Host: api.anva.cloud
3. Content-Type: application/xml
4. Authorization: Bearer
   eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJvcmdhbml6YXRpb25jb2RlIjoiYW52Y
   WRldmVsb3AiLCJjbGllbnRpZCI6ImE0YWI5MGMxLTM3MzYtNDUxMS1hNTY0LWI0ZDg4MWQ
   wZmIwOSIsImlzcyI6IkFOVkEiLCJhY2NvdW50dHlwZSI6IlN5c3RlbSIsImFudmF1c2Vyb
   mFtZSI6IlNURVBIQU5CIiwiZ3JvdXBzIjpbIjEwMCJdLCJvbkJlaGFsZk9mVXNlcm5hbWU
   iOiJzdGVwaGFuYiIsIm0ySWQiOiI5NzEzOTQ2My0xNjI4LTRlZjItODQ4OS0xZmRlOGI2Y
   zQ1MDkiLCJvbkJlaGFsZk9mQW52YVVzZXJuYW1lIjoiU1RFUEhBTkIiLCJvcmdhbml6YXR
   pb25uYW1lIjoiYW52YWRldmVsb3AiLCJvcmdhbml6YXRpb24iOiI3ZTZiYjE2MC05MWQ5L
   TQwOTMtYmM1MC05Njk5ZDQ0NmU3NzQiLCJleHAiOjE2MDE5Njc3MDQsImlhdCI6MTYwMTk
   zMTcwNCwianRpIjoiMTFlZTU5ODctMDU2YS00ZjJmLTg0N2EtMzhiYTQyMGVlMzJlIn0.q
   JTnF6ZB7zqje9I_S2JoqaHShza5OndKCE_Blhm-KKQ
5. <REQUEST>
      <FUNCTION NAME="webview.select">
            <PARAM NAME="select">
                  <RELATIES>
                        <RELATIE>
                              <PK/>
                              <L NR="*"/>
                              <MEMO/>
                        </RELATIE>
                        <WHERE>
                              <PK EQ="NAWBES_00000001"/>
                        </WHERE>
                  </RELATIES>
            </PARAM>
      </FUNCTION>
   </REQUEST>
```

Regel 1 beschrijft het endpoint waar de POST-request met het XML-bericht naar verstuurd kan worden.

Regel 2 beschrijft het (acceptatie)domein van ANVA Hub waar de request naar verstuurd kan worden.

Regel 3 beschrijft een key in de header van het bericht die het content-type definieert van de response.

Regel 4 beschrijft een key in de header van het bericht waarmee de authenticatie wordt geregeld. De key ‘Authorization’ bevat als value het token-type ‘Bearer’ met daarna een spatie en vervolgens het eerder verkregen access_token.

Regel 5 beschrijft de body van de request, waarin het grotendeels onveranderde XML-bericht opgenomen kan worden.

De response op ingestuurde XML-berichten is onveranderd.