Maarten Smeets

AMIS

JWT Token validatie custom policy

Contents

[Waarom deze policy 2](#_Toc35692180)

[Installeer de custom policy 2](#_Toc35692181)

[Installeer de policy JAR file 2](#_Toc35692182)

[Importeer de policy omschrijving XML 3](#_Toc35692183)

[Gebruiken van de policy 5](#_Toc35692184)

[Verhogen logging custom policy 9](#_Toc35692185)

## Waarom deze policy

Voor het valideren van JWT tokens zijn zogenaamde predefined policies aanwezig in OWSM:

* oracle/http\_jwt\_token\_client\_policy
* oracle/http\_jwt\_token\_over\_ssl\_client\_policy
* oracle/http\_jwt\_token\_service\_policy
* oracle/http\_jwt\_token\_over\_ssl\_service\_policy

Deze policies hebben als uitgangspunt dat het sub veld van de token een op WebLogic te authentiseren gebruiker is. Dit is niet altijd het geval. Daarnaast wil de policy de signature valideren met een key uit een keystore. Soms zijn deze keys beschikbaar via een URL bij een externe leverancier of roteren deze waardoor ze lokaal bijhouden in een keystore af te raden is.

Om toch een aantal aspecten van de JWT token te kunnen valideren zonder de signature te valideren (er vanuit kan worden gegaan dat de signature valide is en de token niet gemanipuleerd is), is deze policy opgesteld.

Controles welke de policy uitvoert:

* De policy kijkt naar aangegeven audience (aud attribuut in de JWT token). Als er een audience in de token wordt aangegeven die ook als configuratie bij de policy is opgegeven (expected\_audience parameter, komma gescheiden lijst), dan geeft de policy hier een akkoord op. Dus stel expected\_audience is aud1,aud2 en in de token is aud: aud1,aud3. Dan zal de policy het goed vinden. Immers, aud1 wordt verwacht en aangegeven.
* Er wordt gekeken naar of de velden sub (subject) en iss (issuer) in de token aanwezig zijn.
* Er wordt gekeken of iss voorkomt in de lijst van trusted\_issuers (policy configuratie, een komma gescheiden lijst van vertrouwde issuers)
* Er wordt gekeken of de token nog geldig is (exp attribuut in de token)
* Er wordt gekeken of de not-before-time (nbt) gevuld is

De policy doet geen identity assertion. Immers dit zou vragen dat de inhoud van het sub veld op WebLogic te authentiseren is. In de praktijk wordt de token als een ‘anonieme’ token beschouwd. Deze geeft toegang maar legt niet de link naar een gebruiker. Om toch bijvoorbeeld de vertaling naar een (systeem) gebruiker te maken kan een client policy gebruikt worden welke verwijst naar een CSF sleutel.

## Installeer de custom policy

### Installeer de policy JAR file

De policy JAR file kan gevonden worden in: oauth2\tokenservice\TokenApplication\ValidateTokenPolicy\Deployables

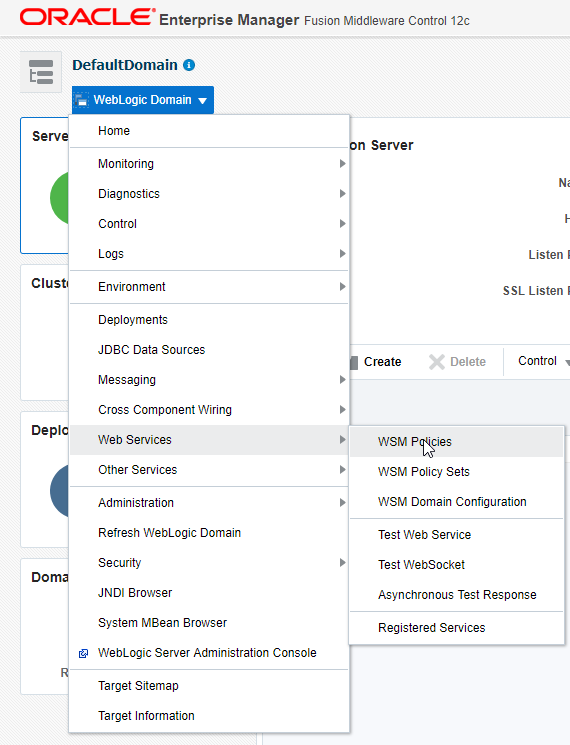
Deze file moet geplaatst worden in WLS\_DOMAIN/lib. In min voorbeeld met de Integrated WebLogic server was dit: C:\Users\maart\AppData\Roaming\JDeveloper\system12.2.1.3.42.170820.0914\DefaultDomain\lib

Tevens moeten de JAR files uit oauth2\tokenservice\TokenApplication\ValidateTokenPolicy\lib naar dezelfde folder gekopieerd worden behalve de volgende JAR bestanden: oracle.logging-utils.jar, wsm-policy-core.jar, wsm-agent-core.jar. Deze bestanden zijn nodig als er ontwikkeld wordt, maar niet meer als de policy op de applicatieserver staat. Daar zijn deze JAR bestanden al aanwezig.

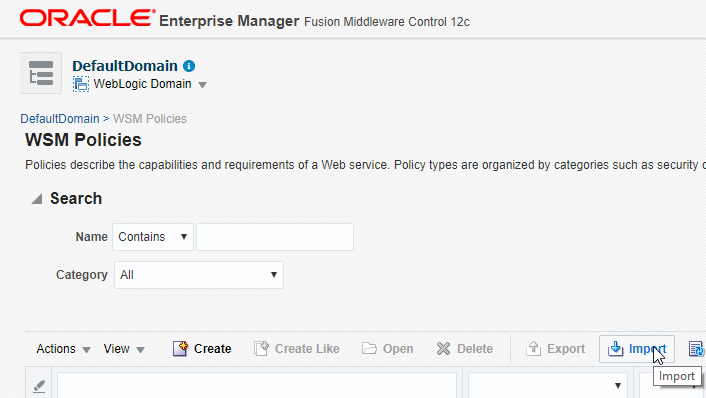
Nadat dit gedaan is moet de applicatieserver opnieuw opgestart worden om de policy beschikbaar te maken.

### Importeer de policy omschrijving XML

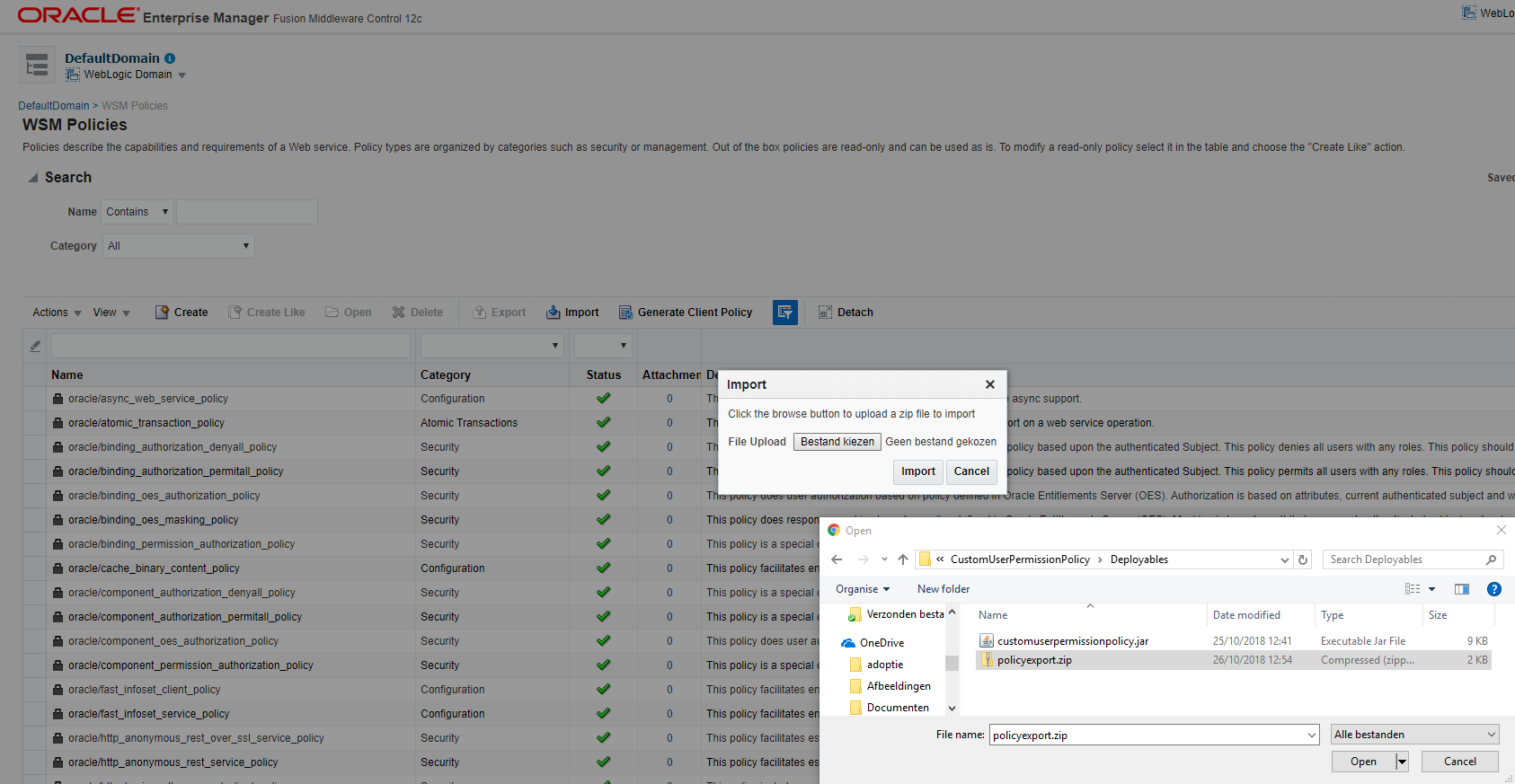
Login EM Fusion Middleware Control en ga naar de OWSM policies pagina;

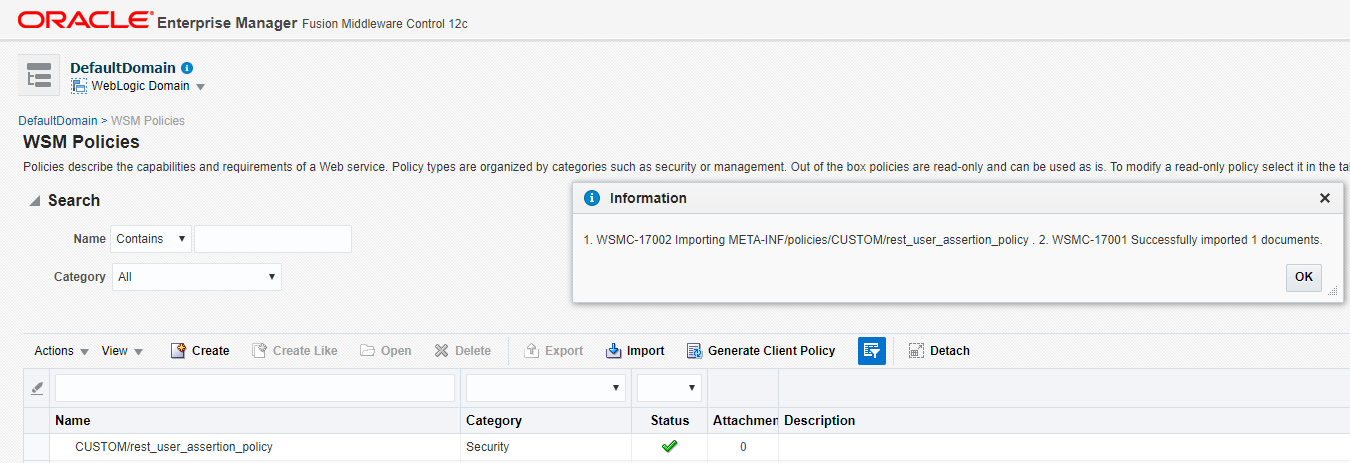


Importeer de custom policy



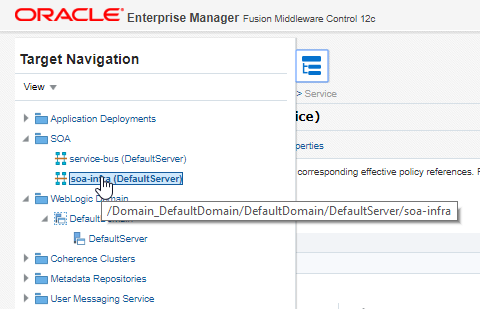
Selecteer policyexport.zip in de Deployables folder

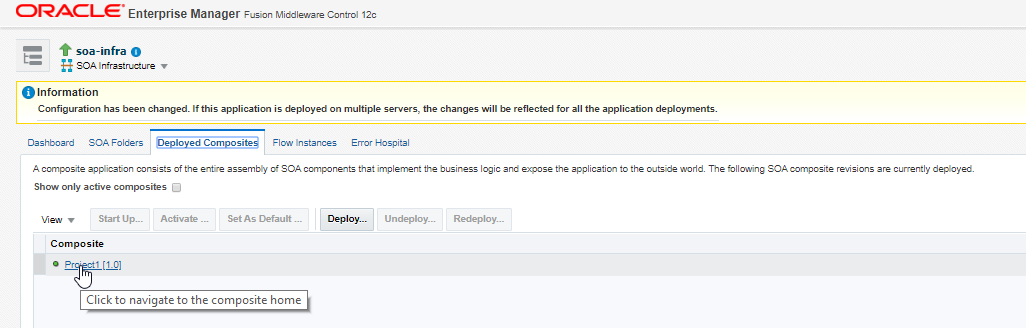


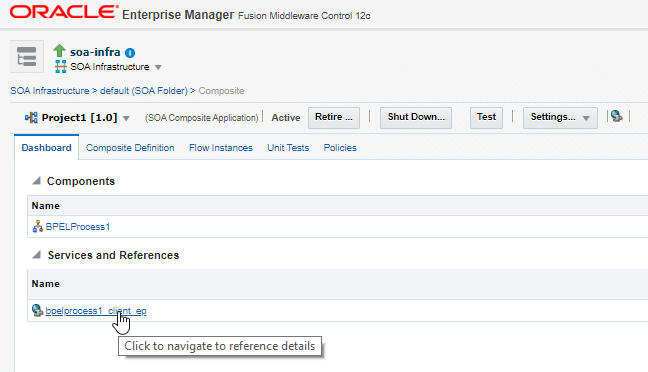


## Gebruiken van de policy

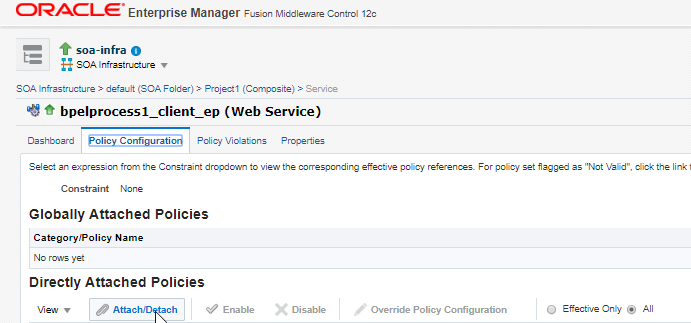
De policy kan handmatig in de EM toegevoegd worden aan een service binding:

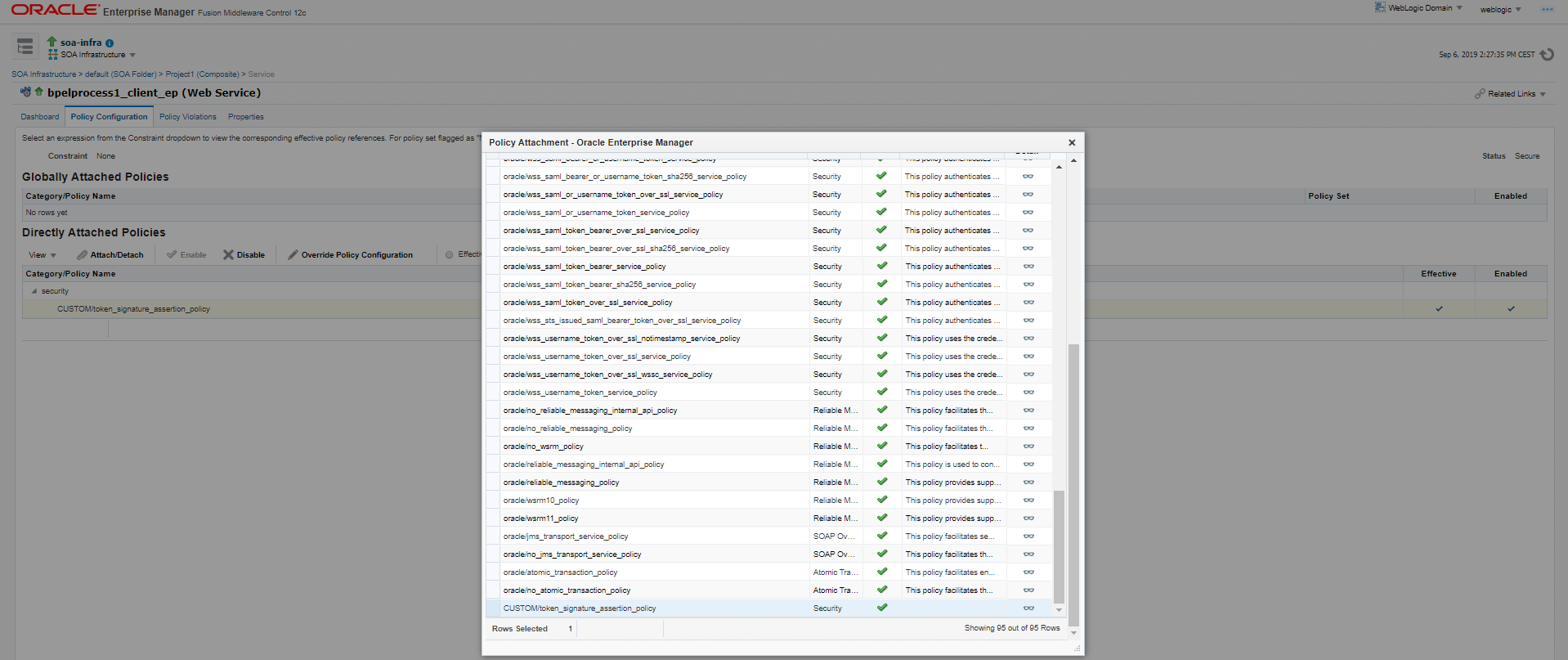




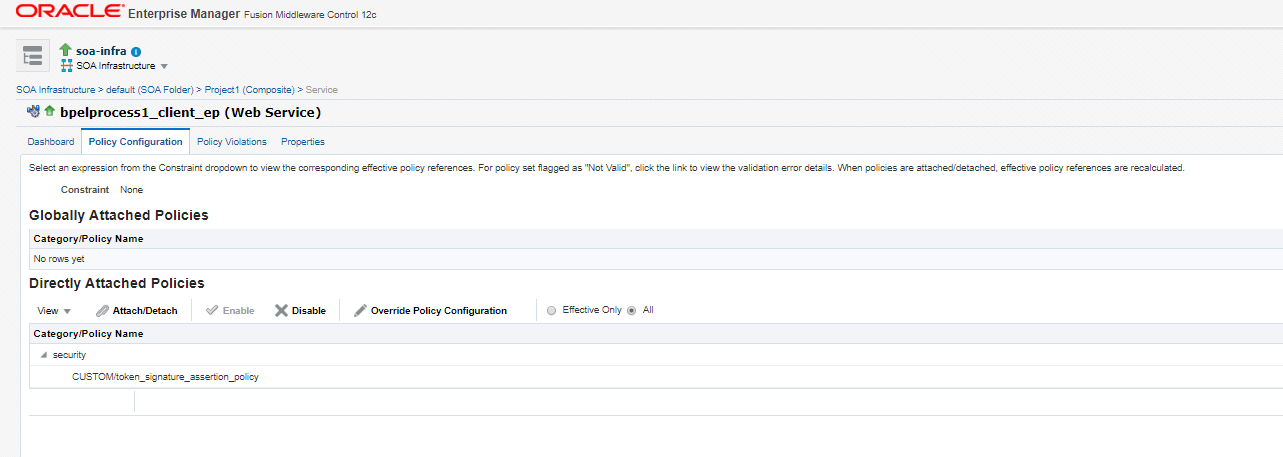






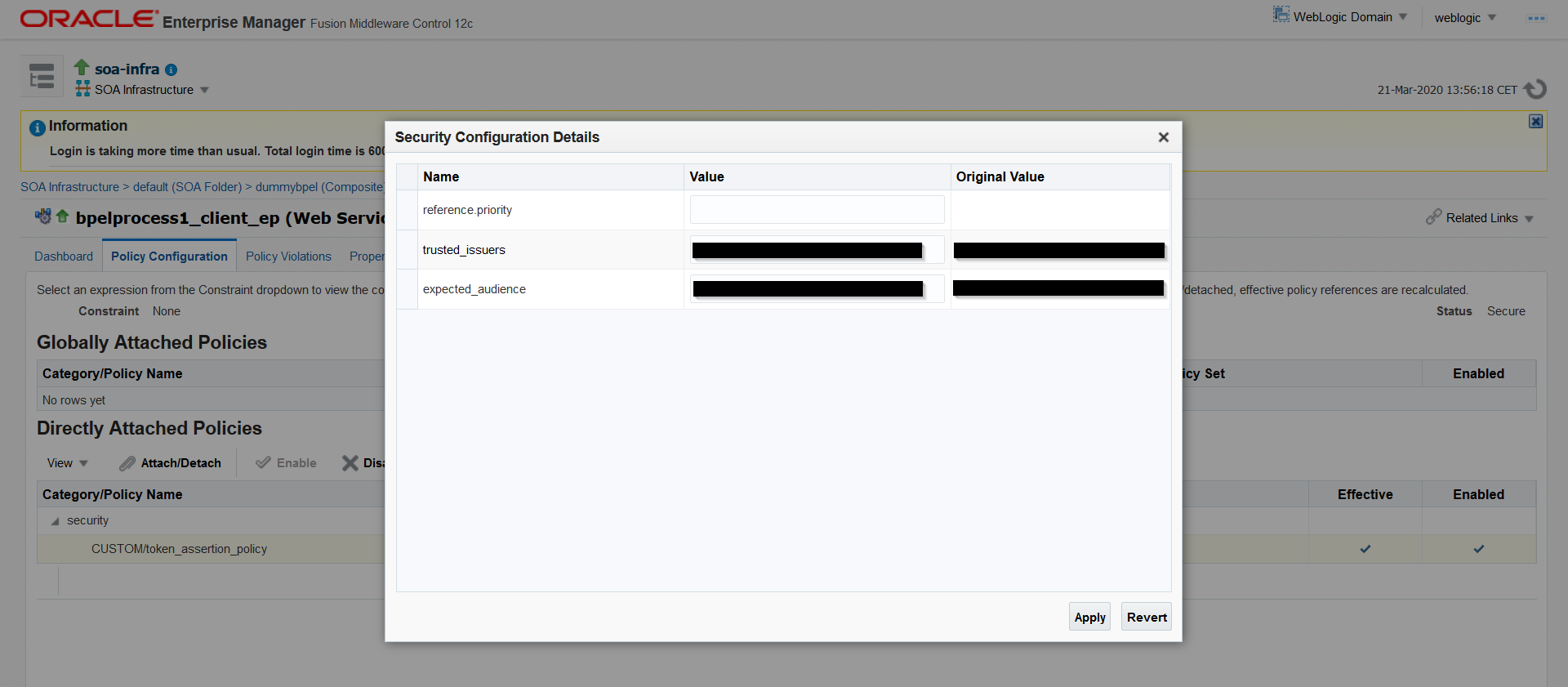


Voeg vervolgens de CUSTOM/token\_assertion\_policy policy toe



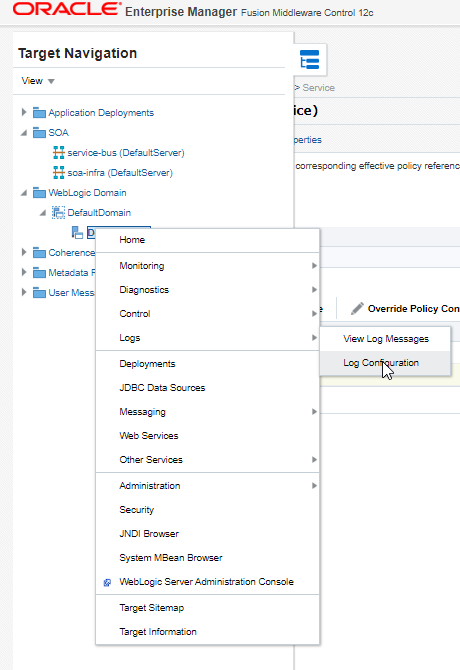
Vervolgens configureer deze

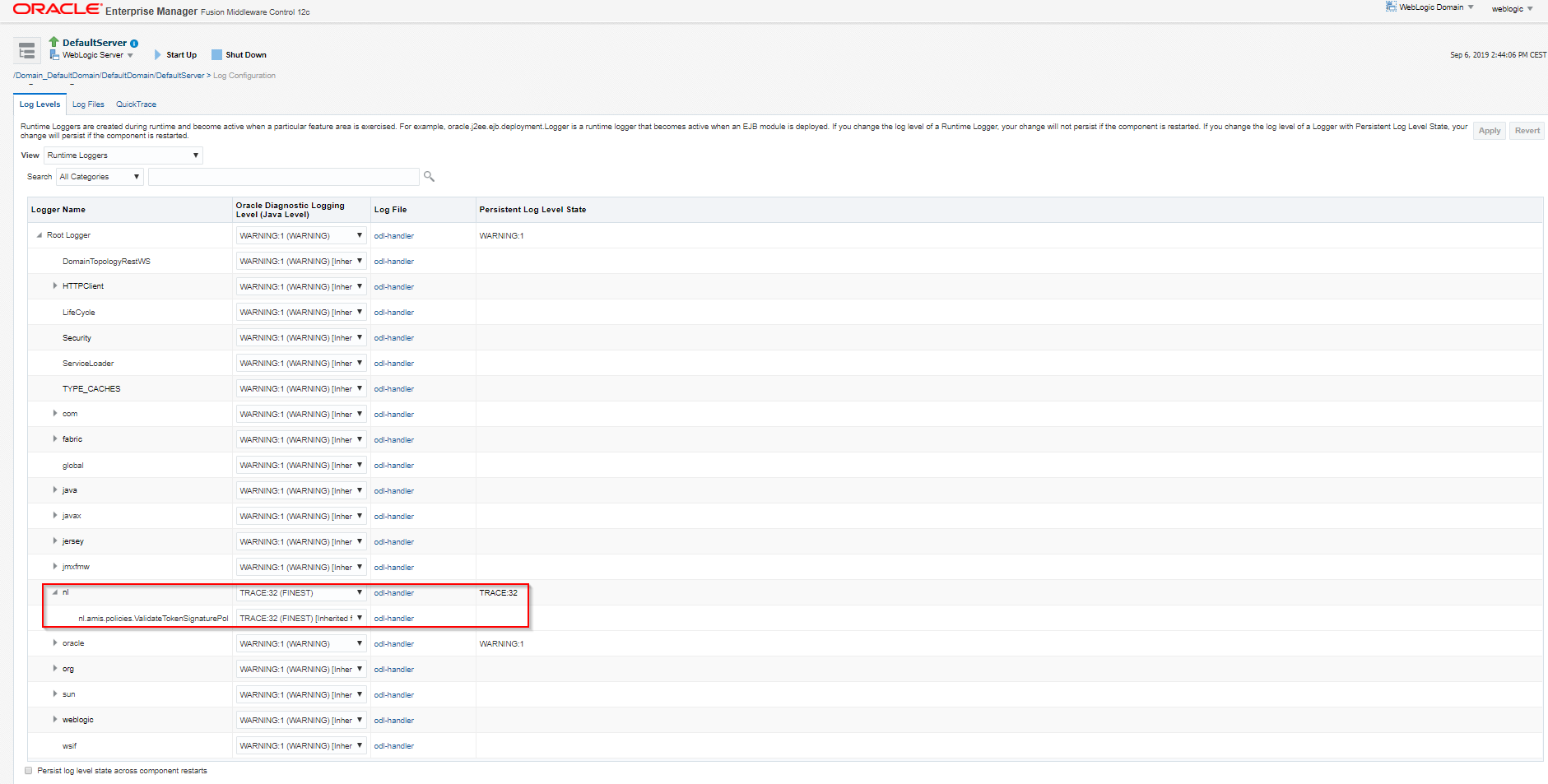




### Verhogen logging custom policy

De custom policy maakt gebruik van het zgn ADFLogger framework. Hierdoor is logging eenvoudig in de EM te zien en te configureren.





Tevens is het loglevel te persisteren.