**JAVELIN CROSS ACCOUNT ACCESS**

**There can be scenarios where LLM model will be in a account different from where Javelin has been installed. In these cases**

**we have to use cross account roles.**

**Steps:-**

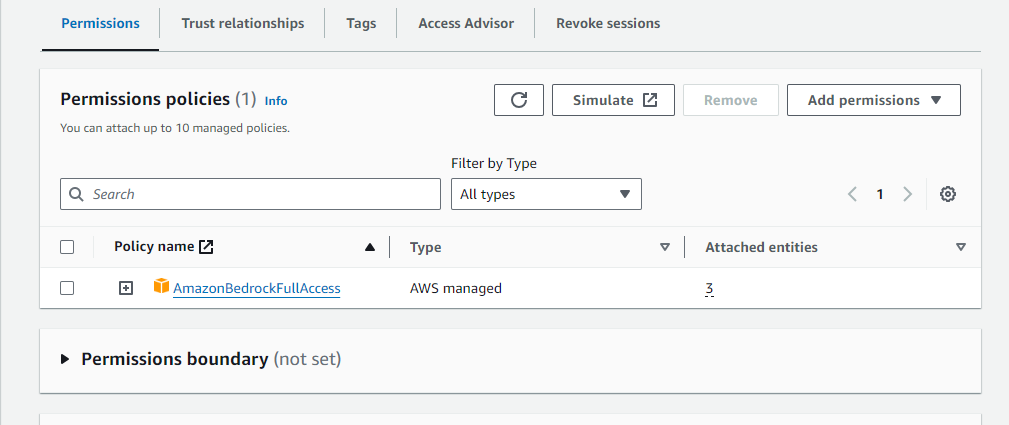
**This will be done in 2 steps.**

**1. Role creation with AmazonBedrockFullAccess** **in division account from where the LLM models to be used(Division control)**

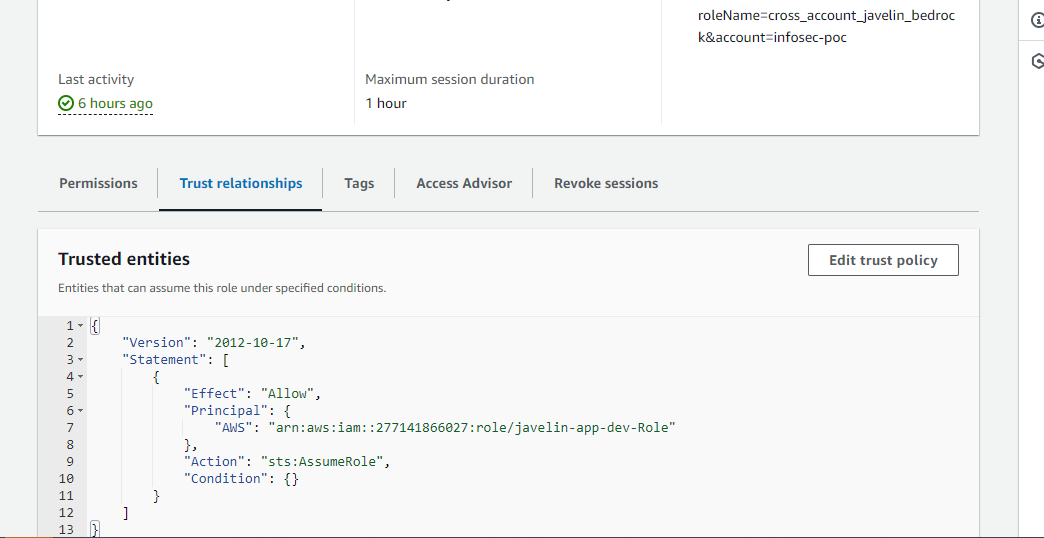
**2. Assume Role creation in Javelin account (Infosec Control)**

**1.Role creation with AmazonBedrockFullAccess** **in division account.**

* Create a Role in the account from where the LLM models have to be utilized (e.g. cross\_account\_javelin\_bedrock )
* Attach a policy(e.g. AmazonBedrockFullAccess ) or an inline policy with specific models to be fetched in the above created role.



* Provide above created role ARN to infosec team for assuming this role with Javelin role. Infosec Team with the help of CloudOps Team will add the required policy in Javelin account to assume this role
* Once the above role has been assumed by Javelin role, infosec team will provide the Javelin role ARN to respective division who will add this role in the trust relationship



**2. Assume Role creation in Javelin account which will be under infosec control**

* **In account where Javelin is installed,** create an inline assume role policy(e.g**. javelin-cross-account-access-policy**) and attach in the role(e.g. **javelin-app-dev-role**) which includes the trust policy allowing it to be assumed by entities authenticated by the OIDC provider. This policy will allow the Javelin App service account to assume the role created in step 1 which in turn allow Javelin to access the LLM models in another account.

This role will be provided to Division to get added in the trust relationship of Division account

