Configuring OIDC providers in cloud for interaction in GitHub actions

AWS:

* Navigate to AWS **IAM** Console.
* Click on **Identity providers** from the left menu options.
* Click on **Add Provider** and the**n OpenId Connect.**
* Provider url as [**https://token.actions.githubusercontent.com**](https://token.actions.githubusercontent.com) **and** Click on Get thumbprint.
* For the "**Audience**": Use **sts.amazonaws.com**
* Click **Add Provider**
* Navigate to newly created provider details.
* Under Audiences, add repo org url eg. <https://github.kyndryl.net/MCMP-IST>
* Copy the role arn, will need this while creating custom policy for role.
* Click on the Assign role button from the top right corner and then select Create New Role.
* Select type of identity as **Web Identity** and in the audience’s dropdown select **sts.amazonaws.com**
* Click on Next permissions.
* Check the checkbox for [AdministratorAccess](https://us-east-1.console.aws.amazon.com/iam/home#/policies/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess) policy.
* Click on the **Create Policy** button and then click on JSON tab.
* Clean everything in editor and paste the below json

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": [

"sts:AssumeRole",

"sts:TagSession"

],

"Resource": [

"arn:aws:iam::753022563888:role/gh-actions-role"

]

}

]

}

* Update the string under Resource object by the role arn you copied earlier.
* Click Next tags and Next Review.
* Give proper name to policy and click on Create Policy
* Return to **Create Role page** and **search** for **newly created policy** and check it and click Next tags 🡪Next Review
* Give proper Role Name and click on Create Role.
* A screenshot of a computer

  Description automatically generated with medium confidence
* Navigate to details of newly created role.

A screenshot of a computer

Description automatically generated with medium confidence

* Click on Trust Relationships and then Edit policy. Update the content with below json.

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"Federated": "arn:aws:iam:: 7342952540452:oidc-provider/token.actions.githubusercontent.com"

},

"Action": "sts:AssumeRoleWithWebIdentity",

"Condition": {

"StringLike": {

"token.actions.githubusercontent.com:sub": "repo:github.kyndryl.net/MCMP-IST/mcmp-resources-cleanup-scripts:\*"

},

"ForAllValues:StringEquals": {

"token.actions.githubusercontent.com:iss": "https://token.actions.githubusercontent.com",

"token.actions.githubusercontent.com:aud": "sts.amazonaws.com"

}

}

},

{

"Sid": "",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam:: 7342952540452:user/nikitha.g.m@kyndryl.com"

},

"Action": "sts:AssumeRole"

},

{

"Sid": "",

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::7342952540452:user/nikitha.g.m@kyndryl.com"

},

"Action": "sts:TagSession"

}

]

}

* Update username and Account Id in the json wherever required.
* Update the value of "token.actions.githubusercontent.com:sub" by github repo url.
* In github actions, add the step below after checkout step.
* - uses: 'actions/checkout@v3'   
  - name: configure aws credentials  
   uses: aws-actions/configure-aws-credentials@v1  
   with:  
   aws-access-key-id: ${{ secrets.AWS\_SECRET\_KEY }}  
   aws-secret-access-key: ${{ secrets.AWS\_SECRET\_ACCESS\_KEY }}  
   aws-region: us-east-1  
   role-to-assume: ${{ secrets.AWS\_IAM }}  
   role-duration-seconds: 1200  
   role-session-name: cleanup
* For AWS\_IAM, provide the value of Role ARN.