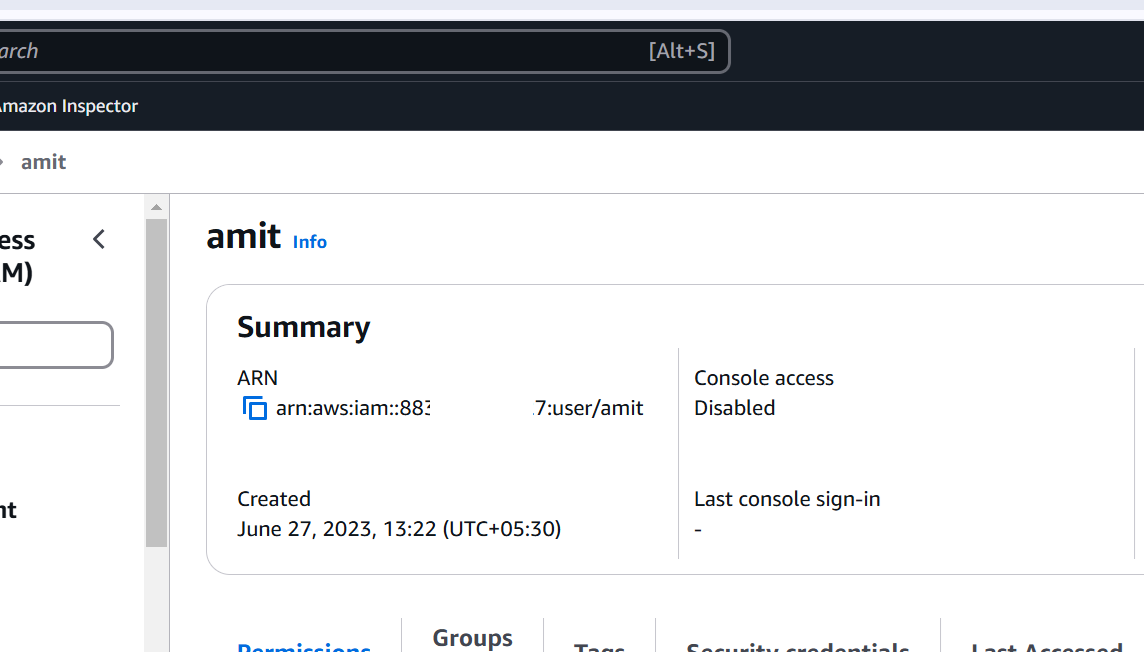
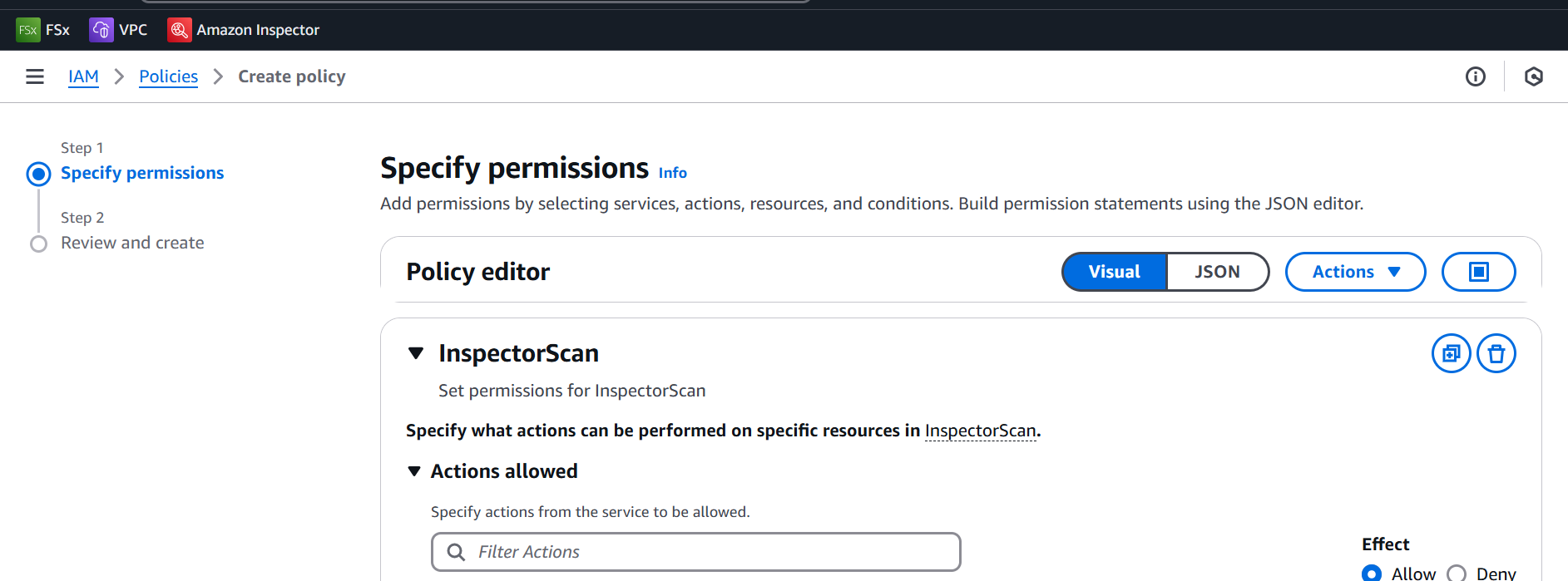
Lab: CICD Scan [AWS Inspector]

1. Go to IAM, and create an user with administrator access and note down the arn of the root user



1. In iam create a policy for inspector



Json

{

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

"Statement": [

{

"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": "inspector-scan:\*",

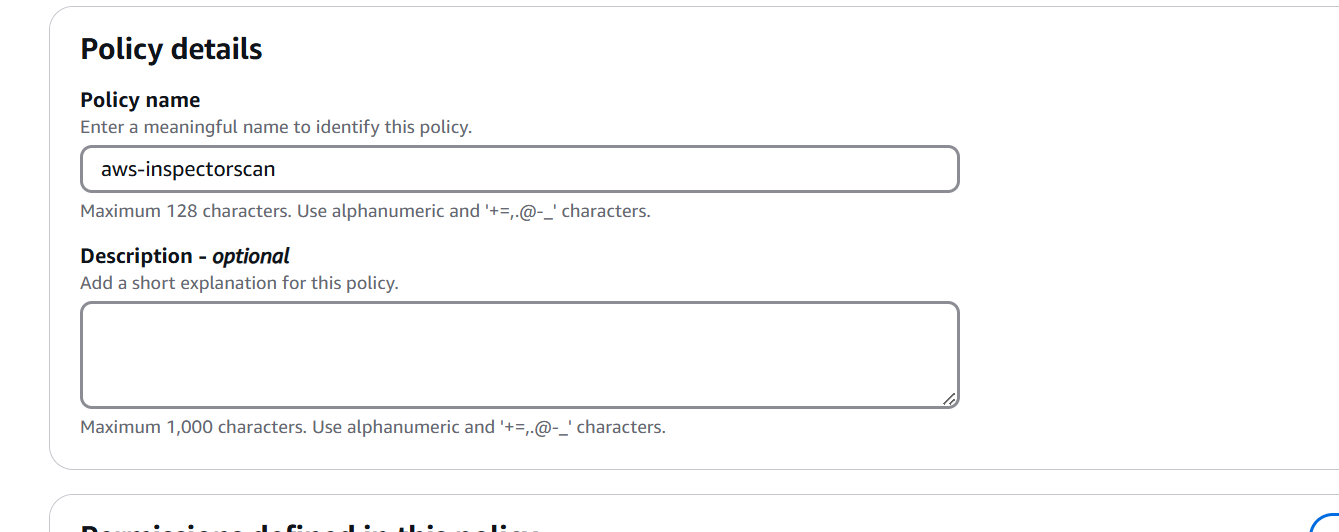
"Resource": "\*"

}

]

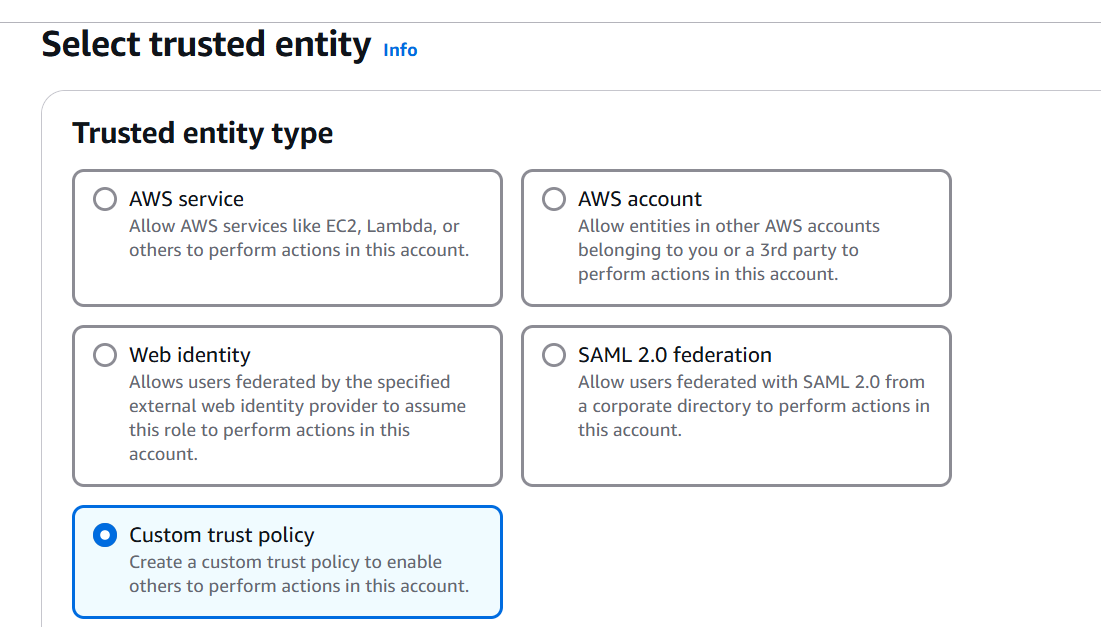
}

Create the policy



Configure an IAM role for CI/CD integration

1. Create role
2. Select Custom trust policy



{

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

"Statement": [

{

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::{ACCOUNT\_ID}:root"

},

"Action": "sts:AssumeRole",

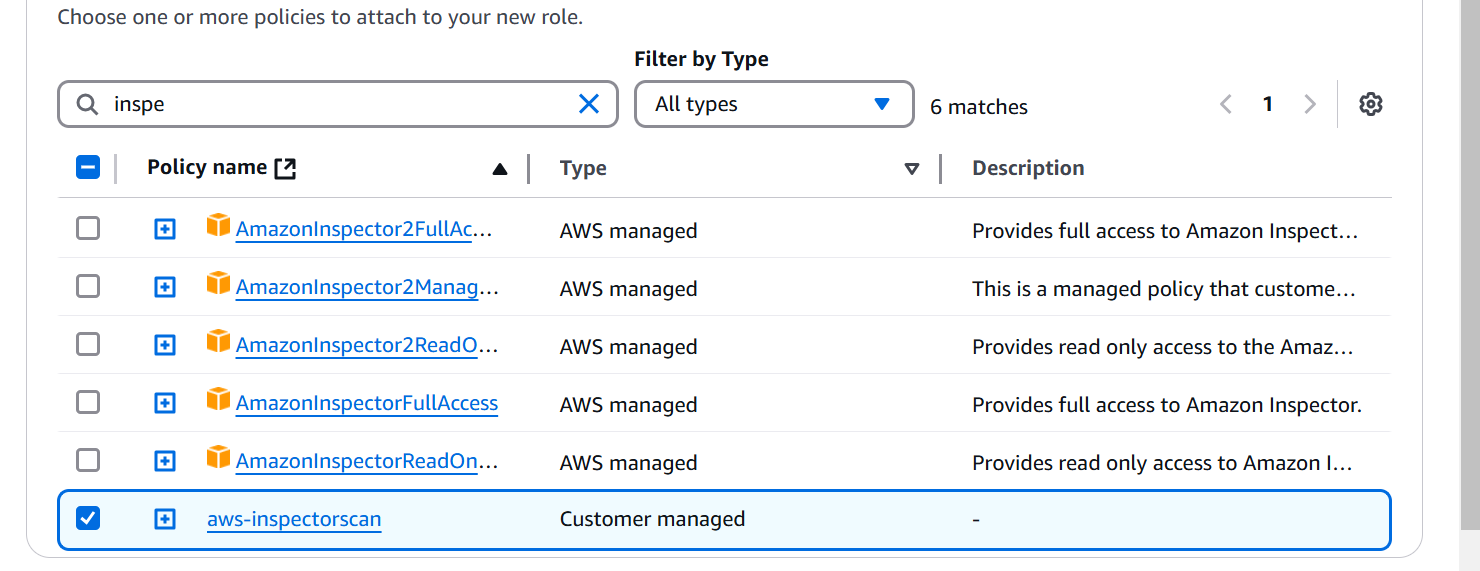
"Condition": {}

}

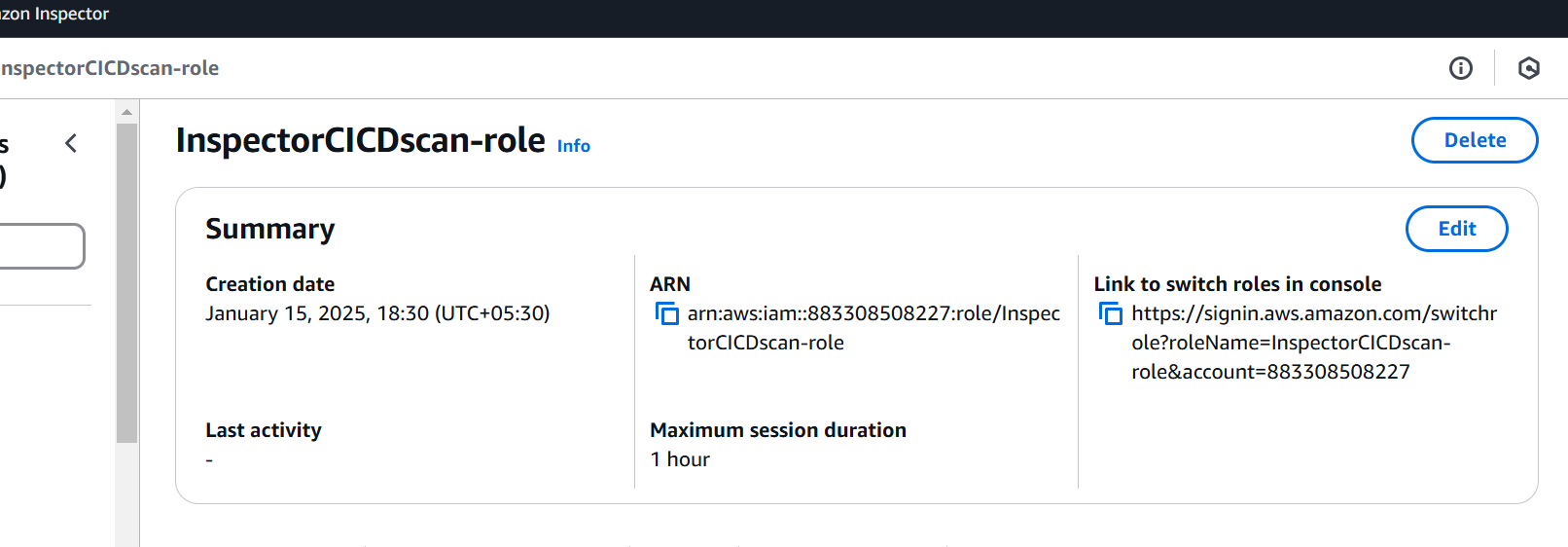
]

}

* Choose **Next**.
* In **Add permissions** search for and select the policy you created earlier, then choose **Next**.



* Give the role a name, for example InspectorCICDscan-role, and add an optional description, then choose Create Role.
* Go to role, and copy link to switch role



Enable the inspector for your account [15 days trail is free]

