IAM Configuration

Make sure that both members of the consortium perform this setup in their respective AWS accounts.

Your Cloud9 environment will need some privileges in order to access your blockchain network. First, you will create a policy that defines the actions your Cloud9 machine will be able to take on the Amazon Managed Blockchain service.

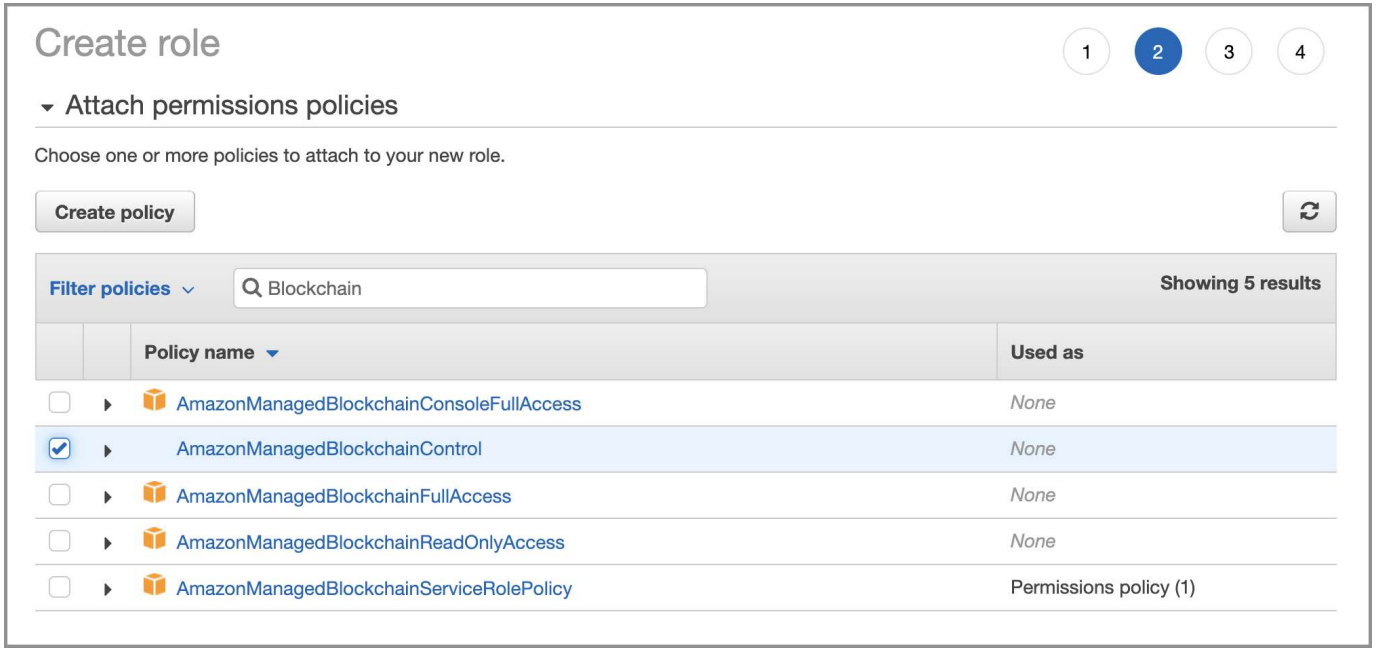
```
cat <<EOT > ~/amb-access-policy.json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ListNetworkMembers",
      "Effect": "Allow",
      "Action": [
          "managedblockchain:GetNetwork",
          "managedblockchain:ListMembers"
      ],
      "Resource": [
          "arn:aws:managedblockchain:*:$THIS_AWS_ID:networks/*"
      ]
    },
    {
      "Sid": "ManageNetworkResources",
      "Effect": "Allow",
      "Action": [
        "managedblockchain:CreateProposal",
        "managedblockchain:GetProposal",
        "managedblockchain:DeleteMember",
        "managedblockchain:VoteOnProposal",
        "managedblockchain:ListProposals",
        "managedblockchain:GetNetwork",
        "managedblockchain:ListMembers",
        "managedblockchain:ListProposalVotes",
        "managedblockchain:RejectInvitation",
        "managedblockchain:GetNode",
        "managedblockchain:GetMember",
        "managedblockchain:DeleteNode",
        "managedblockchain:CreateNode",
        "managedblockchain:CreateMember",
        "managedblockchain:ListNodes"
      ],
      "Resource": [
        "arn:aws:managedblockchain:*::networks/*",
        "arn:aws:managedblockchain:*::proposals/*",
        "arn:aws:managedblockchain:*:$THIS_AWS_ID:members/*",
```

```
        "arn:aws:managedblockchain:*:$THIS_AWS_ID:invitations/*",
        "arn:aws:managedblockchain:*:$THIS_AWS_ID:nodes/*"
      ]
    },
    {
      "Sid": "WorkWithNetworksForAcct",
      "Effect": "Allow",
      "Action": [
        "managedblockchain:ListNetworks",
        "managedblockchain:ListInvitations",
        "managedblockchain:CreateNetwork"
      ],
      "Resource": "*"
    }
  ]
}
EOT
```

Then, run the following command in your Cloud9 terminal to create the policy with the name `AmazonManagedBlockchainControl`.

```
aws iam create-policy --policy-name AmazonManagedBlockchainControl --policy-document file://$HOME/amb-access-policy.json | jq -r .Policy
```

Now, from the Identity and Access Management (IAM) service on the (AWS Management Console)[http://console.aws.amazon.com/iamv2], select **Roles** from the left-hand sidebar, and then **Create role**. Select **AWS service** as the type of trusted entity and choose EC2 as your use case, then select **Next: permissions**. Narrow down the options by searching in the filter and then check the box next to the policies you just created. Also attach **AdministratorAccess**. So many different IAM permissions are needed in subsequent modules, that it is easier to configure this machine with administrator access during setup. After the workshop is finished, the **AdministratorAccess** policy may be removed, leaving only the **AmazonManagedBlockchainControl** policy attached to the Fabric client. This ensures that you follow the Principle of Least Privilege during your day-to-day use.



Select **Next: Tags** and then **Next: Review**. Call the role `ServiceLinkedRoleForAmazonManagedBlockchain` and select **Create role**.

Previous Next