

**Blueventure:
Blockchain Lab**

Track-and-Trace Blockchain
Workshop for Hyperledger
Fabric 2.2 (BETA)

▼ Create a Hyperledger Fabric
Network

- Create Network & Member
- Accept invite and create
Supplier member

Congratulations

▼ Setup Development
Environment

Create a Cloud9
environment

IAM Configuration

Modify Cloud9 IAM role

- Set up a Fabric client
- Write and deploy chaincode

▼ AWS account access

[Open AWS console](#)

(us-east-1)

[Get AWS CLI credentials](#)

Exit event

[Event dashboard](#) > [Setup Development Environment](#) > IAM Configuration

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.

```
1  cat <<EOT > ~/amb-access-policy.json
2  {
3      "Version": "2012-10-17",
4      "Statement": [
5          {
6              "Sid": "ListNetworkMembers",
7              "Effect": "Allow",
8              "Action": [
9                  "managedblockchain:GetNetwork",
10                 "managedblockchain:ListMembers"
11             ],
12             "Resource": [
13                 "arn:aws:managedblockchain:*:${THIS_AWS_ID}:networks/*"
14             ]
15         },
16         {
17             "Sid": "ManageNetworkResources",
18             "Effect": "Allow",
19             "Action": [
20                 "managedblockchain:CreateProposal",
21                 "managedblockchain:GetProposal",
22                 "managedblockchain>DeleteMember",
23                 "managedblockchain:VoteOnProposal",
24                 "managedblockchain:ListProposals",
25                 "managedblockchain:GetNetwork",
26                 "managedblockchain:ListMembers",
27                 "managedblockchain:ListProposalVotes",
28                 "managedblockchain:RejectInvitation",
29                 "managedblockchain:GetNode",
30                 "managedblockchain:GetMember",
31                 "managedblockchain>DeleteNode",
32                 "managedblockchain:CreateNode",
33                 "managedblockchain:CreateMember",
34                 "managedblockchain:ListNodes"
35             ],
36             "Resource": [
37                 "arn:aws:managedblockchain:*:networks/*",
38                 "arn:aws:managedblockchain:*:proposals/*",
39                 "arn:aws:managedblockchain:*:${THIS_AWS_ID}:members/*",
```



Blueventure: Blockchain Lab

Track-and-Trace Blockchain
Workshop for Hyperledger
Fabric 2.2 (BETA)

▼ Create a Hyperledger Fabric Network

- Create Network & Member
- Accept invite and create Supplier member
- Congratulations

▼ Setup Development Environment

Create a Cloud9
environment

IAM Configuration

Modify Cloud9 IAM role

- Set up a Fabric client
- Write and deploy chaincode

▼ AWS account access

- [Open AWS console \(us-east-1\)](#)
- [Get AWS CLI credentials](#)

Exit event

```

40     "arn:aws:managedblockchain:*$THIS_AWS_ID:invitations/*",
41     "arn:aws:managedblockchain:*$THIS_AWS_ID:nodes/*"
42   ]
43 },
44 {
45   "Sid": "WorkWithNetworksForAcct",
46   "Effect": "Allow",
47   "Action": [
48     "managedblockchain:ListNetworks",
49     "managedblockchain:ListInvitations",
50     "managedblockchain:CreateNetwork"
51   ],
52   "Resource": "*"
53 }
54 ]
55 }
56 EOT

```

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

```
1 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.

**Blueventure:
Blockchain Lab**

Track-and-Trace Blockchain
Workshop for Hyperledger
Fabric 2.2 (BETA)

▼ Create a Hyperledger Fabric
Network

- ▶ Create Network & Member
- ▶ Accept invite and create
Supplier member
- Congratulations

▼ Setup Development
Environment

Create a Cloud9
environment

[IAM Configuration](#)

Modify Cloud9 IAM role

- ▶ Set up a Fabric client
- ▶ Write and deploy chaincode

▼ AWS account access

[Open AWS console](#)
(us-east-1)

[Get AWS CLI credentials](#)

Exit event

Create role

1

2

3

4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy



Filter policies ▼

Q Blockchain

Showing 5 results

	Policy name ▼	Used as
<input type="checkbox"/>	▶ AmazonManagedBlockchainConsoleFullAccess	None
<input checked="" type="checkbox"/>	▶ AmazonManagedBlockchainControl	None
<input type="checkbox"/>	▶ AmazonManagedBlockchainFullAccess	None
<input type="checkbox"/>	▶ AmazonManagedBlockchainReadOnlyAccess	None
<input type="checkbox"/>	▶ AmazonManagedBlockchainServiceRolePolicy	Permissions policy (1)

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

Previous

Next