

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

▼ Set up a Fabric client

Network configuration

Update Cloud9 Networking

Create VPC endpoint

► Configure client instance

▼ AWS account access

[Open AWS console](#)

(us-east-1) 

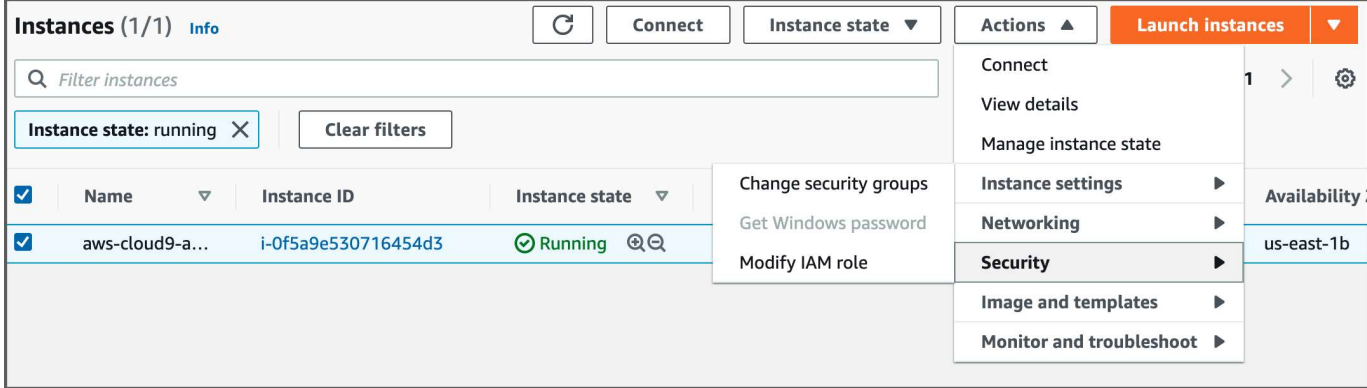
[Get AWS CLI credentials](#)

Exit event

[Event dashboard](#) > [Set up a Fabric client](#) > Update Cloud9 Networking

Update Cloud9 Networking

Your Cloud9 environment will be used as the Fabric Client. In order for it to communicate with the blockchain network over the VPC endpoint, it needs to be in the same security group. To update its networking configuration, go to the EC2 Management Console and select Instances from the left sidebar, then check the box next to your cloud9 instance. Then select **Actions**, then scroll down to **Security**, then select **Change security groups**.



The screenshot shows the AWS Management Console 'Instances' page. At the top, there's a header 'Instances (1/1)' with an 'Info' link. Below this is a search bar 'Filter instances' and a filter button 'Instance state: running'. A table lists the instances:

	Name	Instance ID	Instance state
<input checked="" type="checkbox"/>	aws-cloud9-a...	i-Of5a9e530716454d3	Running

To the right of the table, the 'Actions' dropdown menu is open, showing options: 'Connect', 'View details', 'Manage instance state', 'Change security groups', 'Get Windows password', and 'Modify IAM role'. The 'Security' option is highlighted in the dropdown.

On the next page, begin to type **HFClientAndEndpoint** and then select it from the displayed options, then click **AddSecurityGroup**, then click **Save**.

**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

▼ Set up a Fabric client

Network configuration

**Update Cloud9
Networking**

Create VPC endpoint

► Configure client instance

▼ AWS account access

[Open AWS console](#)

(us-east-1) 

[Get AWS CLI credentials](#)

Exit event

Change security groups [Info](#)

Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic to and from your instance. You can use this window to add and remove security groups.

Instance details

aws-cloud9-amb-development-1eab62beb967400385be75aa98d20ab2-
InstanceSecurityGroup-IDGYB479YY2G (sg-014e1b3eae293de81)
aws-cloud9-amb-development-1eab62beb967400385be75aa98d20ab2-InstanceSecurityGroup-
IDGYB479YY2G
aws-cloud9-amb-development-1eab62beb967400385be75aa98d20ab2

13

HFClientSSH (sg-030e87f22e0139539)
HFClientSSH

HFClientAndEndpoint (sg-0c8d90d557c2aae9a)
HFClientAndEndpoint

default (sg-53287475)
default

 *Select security groups*

Add security group

Security groups associated with the network interface (eni-032cad2d02a95c413)

Security group name	Security group ID	
aws-cloud9-amb-development-1eab62beb967400385be75aa98d20ab2-InstanceSecurityGroup-IDGYB479YY2G	sg-014e1b3eae293de81	<button>Remove</button>

Cancel

Save

Previous

Next