10/19/23, 8:41 AM Blueventure: Blockchain Lab

Blueventure: Blockchain Lab

Naturali

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

- 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 > Network configuration

## Network configuration

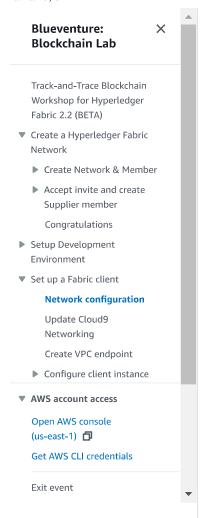
## Create security groups

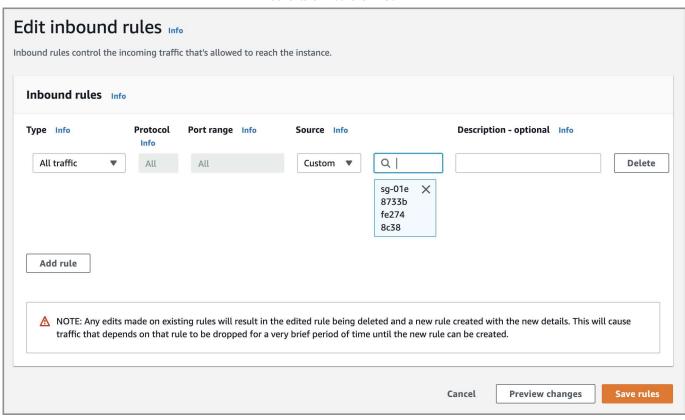
Begin by creating network security groups for the Fabric client instance. Open the AWS Management Console and go to the EC2 service. Select **Security groups** from the left-hand sidebar, then **Create security group**. Call the group *HFClientAndEndpoint*, set the description to "Allows internal traffic between Fabric client and VPC endpoint" and make sure your default VPC is selected. Make sure that all inbound and outbound rules are deleted, then select **Create security group**.



Edit the inbound rules of the security group you just created. Add a rule that allows all traffic from a custom source. Clicking in the field with the magnifying glass will display several options. Select the current security group (the one you just created) and then **Save rules**. This allows all traffic to flow between network interfaces in this security group. Specifically, it enables traffic between the Fabric client and the VPC endpoint on your blockchain network.







Now create another outbound rule on that security group with the same settings (all traffic allowed from a custom source that belongs to the same security group).



**(1)**