

Connecting Two EC2 Instances to an SQS Queue

Goal

- EC2-1 → Producer (sends messages)
- EC2-2 → Consumer (receives & deletes messages)
- Both talk to **Amazon Simple Queue Service**
- No direct EC2-to-EC2 communication

Architecture (Simple View)

EC2 (Producer) ---> SQS Queue ---> EC2 (Consumer)

STEP 1: Create IAM Roles (MOST IMPORTANT STEP)

EC2 instances must be **allowed** to talk to SQS.

1A. Create Producer IAM Role

1. Go to **IAM** → **Roles**
2. Click **Create role**
3. Select **AWS service**
4. Choose **EC2**
5. Click **Next**

Attach Policy

- Attach **AmazonSQSFullAccess**

(or custom policy with sqs:SendMessage)

6. Role name: EC2-SQS-Producer-Role
7. Create role

1B. Create Consumer IAM Role

Repeat same steps, but permissions differ.

Attach Policy

- **AmazonSQSFullAccess**

(or custom with Receive/Delete permissions)

Role name: EC2-SQS-Consumer-Role

STEP 2: Attach Roles to EC2 Instances

Attach Producer Role

1. Go to **EC2**
2. Select **Producer EC2**
3. Actions → Security → **Modify IAM role**
4. Select **EC2-SQS-Producer-Role**
5. Save

Attach Consumer Role

Repeat for **Consumer EC2**, attach **EC2-SQS-Consumer-Role**

📌 This removes the need for access keys.

STEP 3: Install AWS CLI on Both EC2s

Login to **both EC2 instances**.

For Amazon Linux:

```
sudo yum install aws-cli -y
```

Verify:

```
aws --version
```

STEP 4: Get Your SQS Queue URL

1. Go to **SQS Console**
2. Click your queue
3. Copy **Queue URL**

Example:

<https://sns.ap-south-1.amazonaws.com/123456789012/my-queue>

STEP 5: Configure AWS Region (Both EC2s)

```
aws configure set region ap-south-1
```

(No access key needed because IAM role is attached)

STEP 6: Producer EC2 – Send Message to SQS

Login to **Producer EC2** and run:

```
aws sqs send-message \  
--queue-url <QUEUE_URL> \  
--message-body "Hello from Producer EC2"
```

 If successful → message is now in SQS

STEP 7: Consumer EC2 – Receive Message from SQS

Login to **Consumer EC2** and run:

```
aws sqs receive-message \  
--queue-url <QUEUE_URL>
```

You will see:

- Message body
- ReceiptHandle (important)

STEP 8: Delete Message (VERY IMPORTANT)

If you don't delete it, SQS will resend it.

```
aws sqs delete-message \  
--queue-url <QUEUE_URL> \  
--receipt-handle <RECEIPT_HANDLE>
```

 Message is now fully processed.

STEP 9: Verify from SQS Console

1. Open SQS → your queue
2. Monitoring tab:
 - a. Messages available → 0
 - b. Messages in flight → 0

This confirms **end-to-end success**.

What You Just Achieved (Plain English)

- EC2 #1 successfully **sent work**
- SQS safely **stored it**
- EC2 #2 **picked it up and processed it**
- No EC2 talked directly to another EC2
- System is **scalable and fault-tolerant**

Common Mistakes to Avoid

- ✖ Using access keys instead of IAM roles
- ✖ Forgetting to delete message
- ✖ Wrong region
- ✖ No permission on EC2 role

One-Line Interview Answer

Two EC2 instances connect to SQS by attaching IAM roles with SQS permissions and using the queue URL to send and receive messages.