**Cross-Region Lambda Execution:**

1. **IAM Policy for Lambda Execution Role**:
   * Go to the IAM console in the source AWS account.
   * Create or update the IAM policy attached to the Lambda function's execution role to include permissions for cross-region snapshot creation and deletion.
   * Here's an example IAM policy allowing ec2:CreateSnapshot and ec2:DeleteSnapshot actions across all regions:

json

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"ec2:CreateSnapshot",

"ec2:DeleteSnapshot"

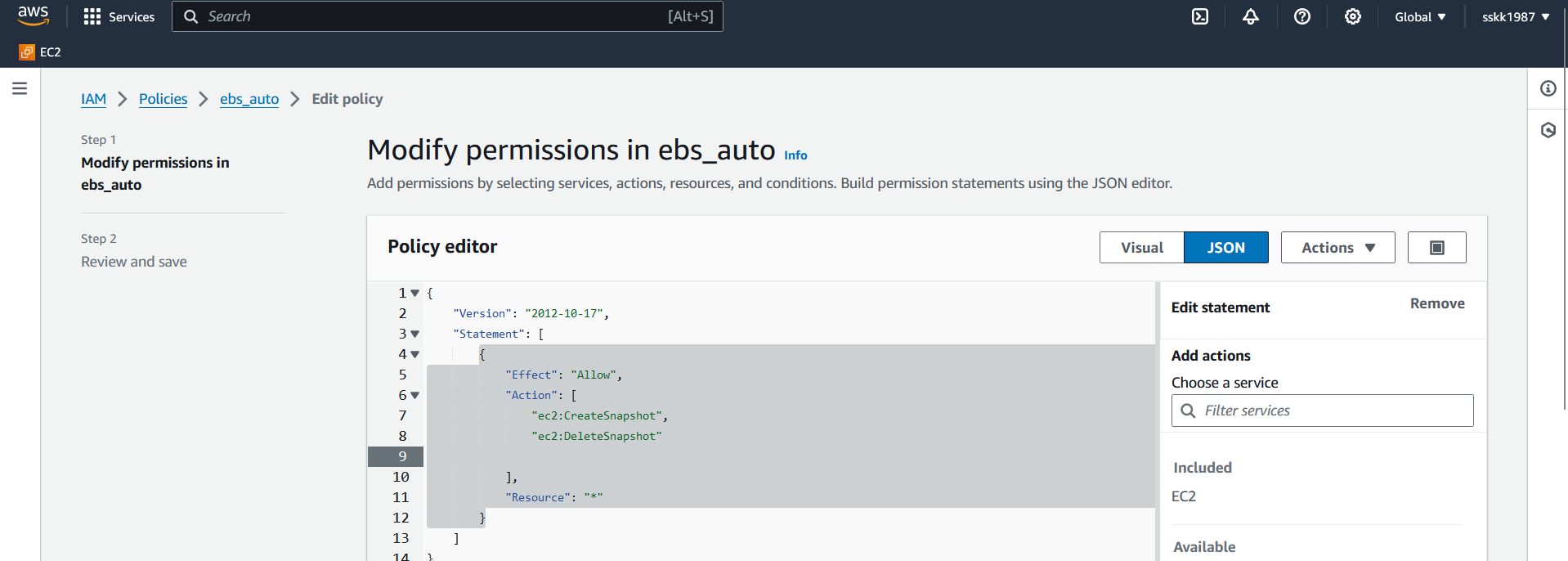
],

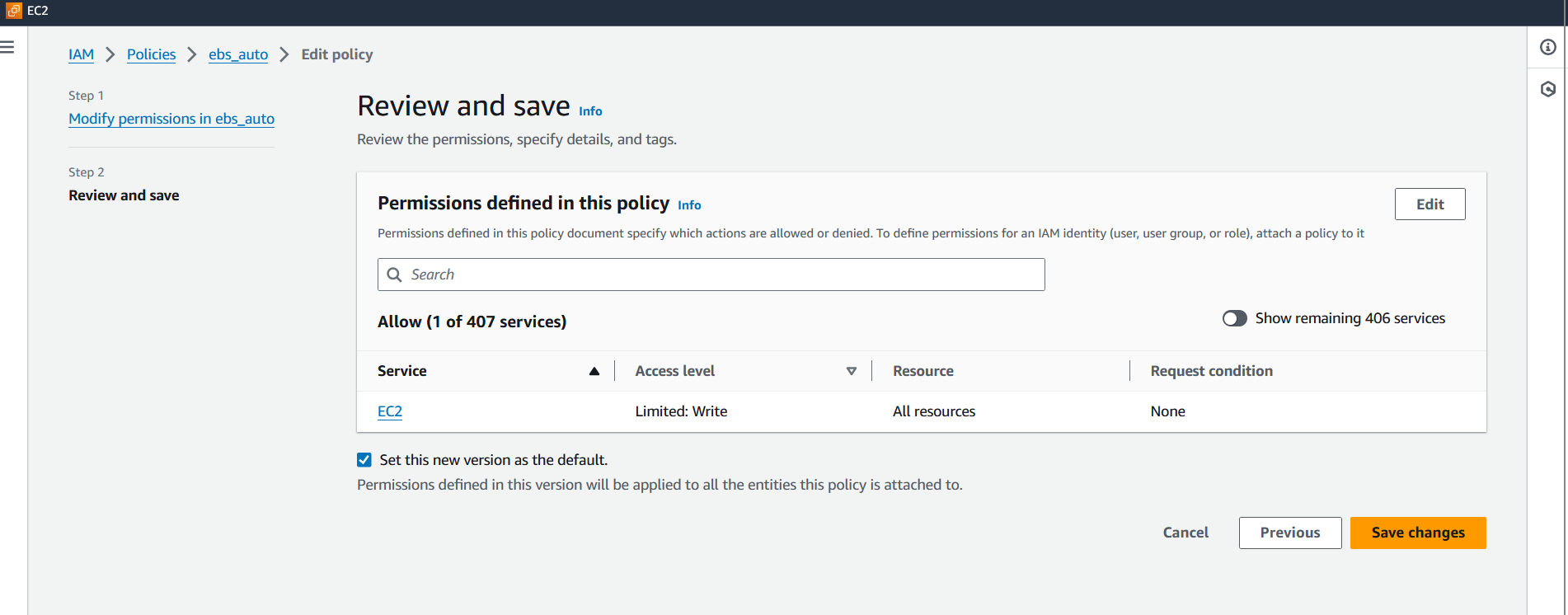
"Resource": "\*"

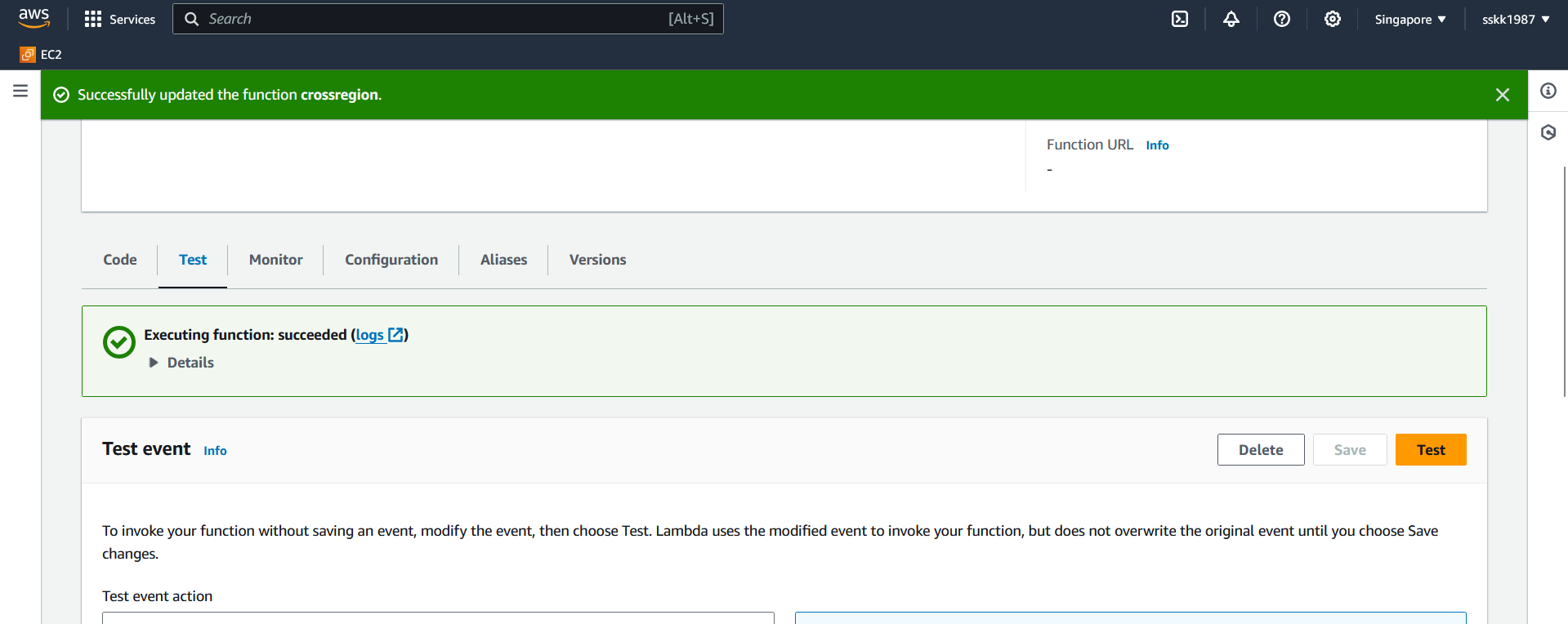
}

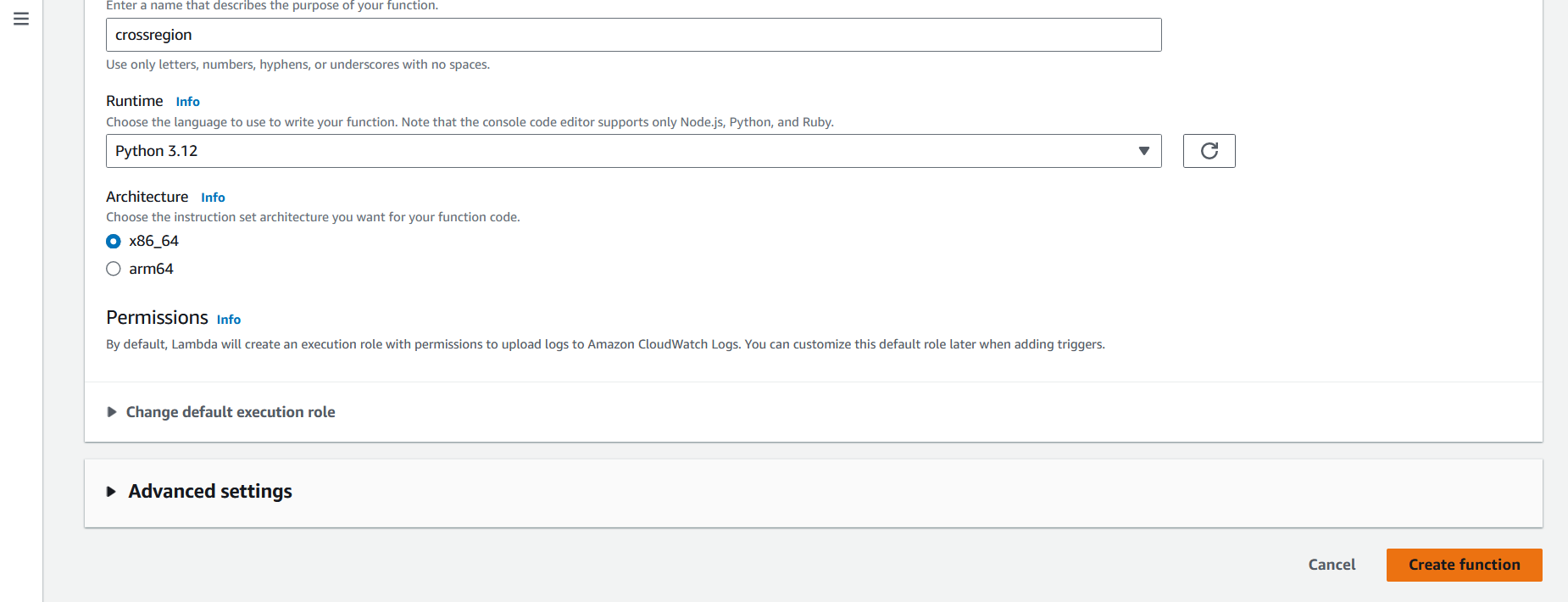
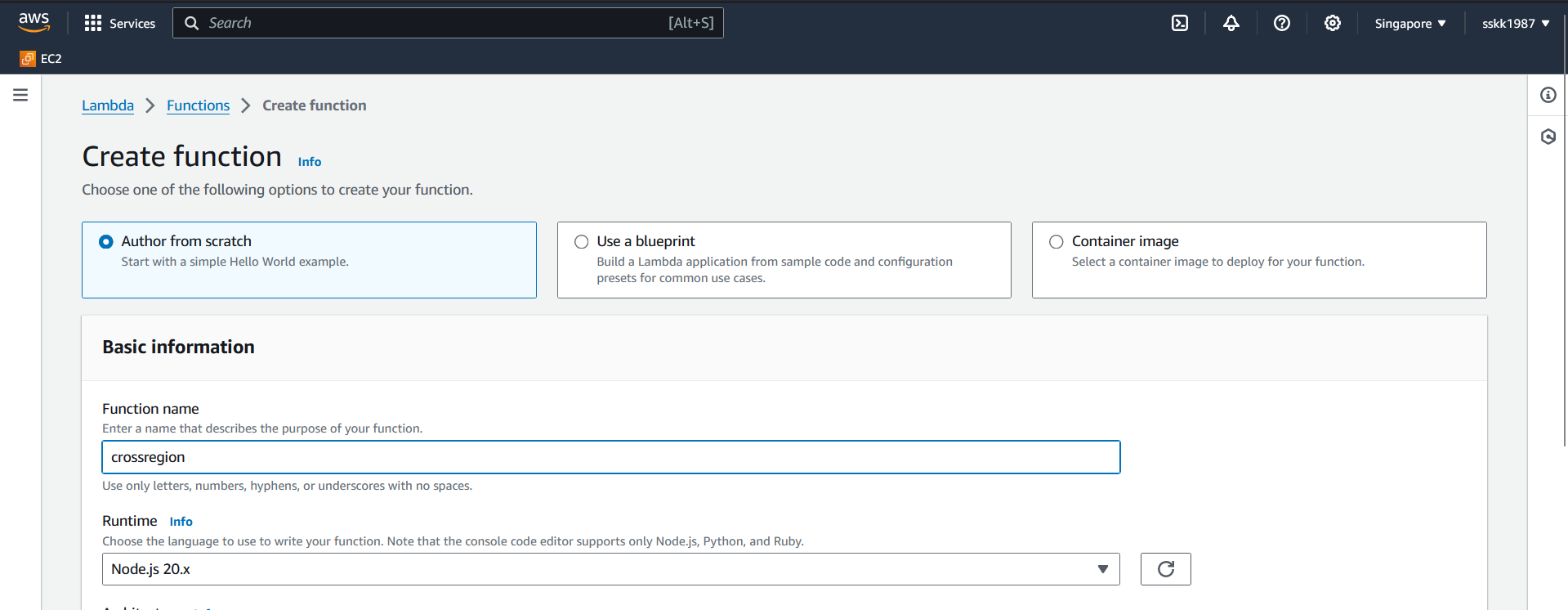
]

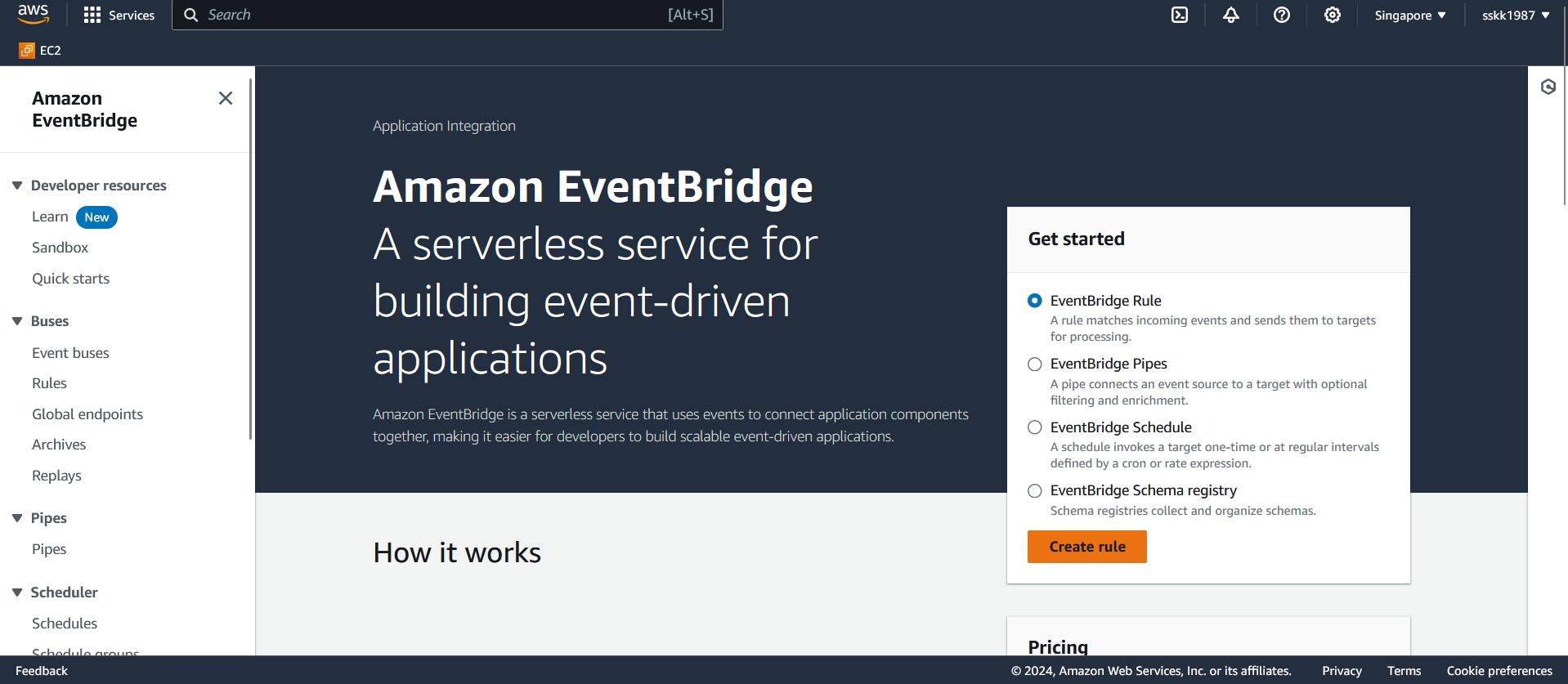
}

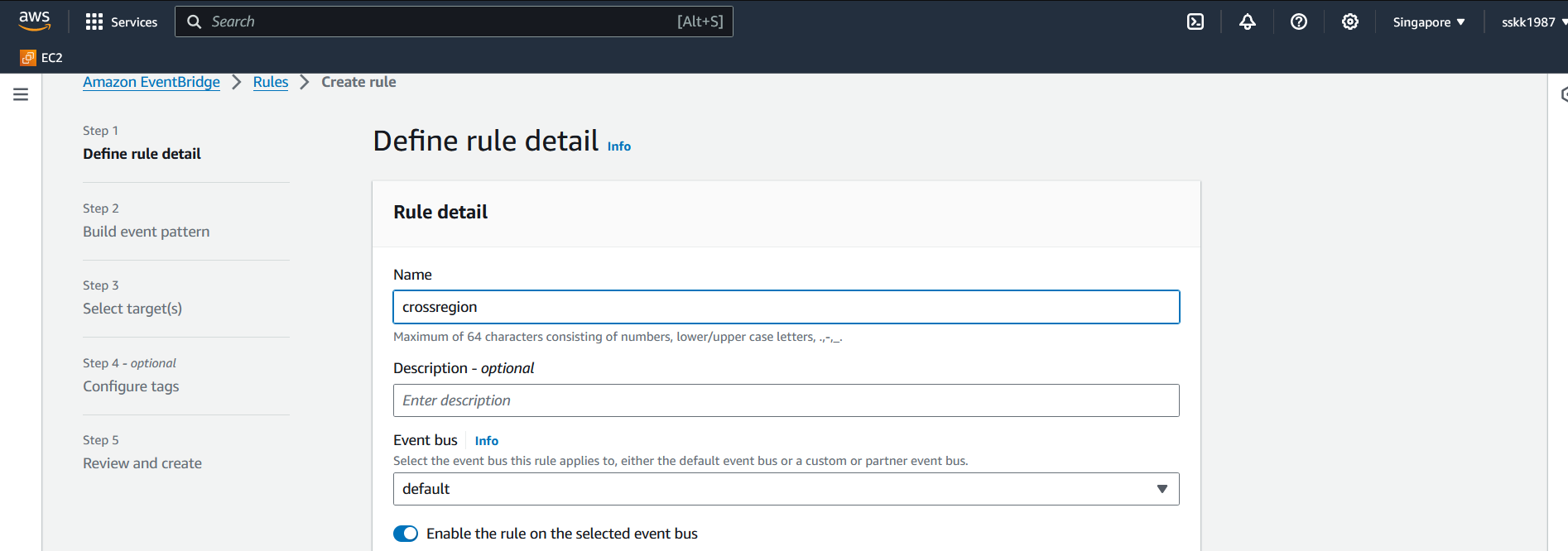
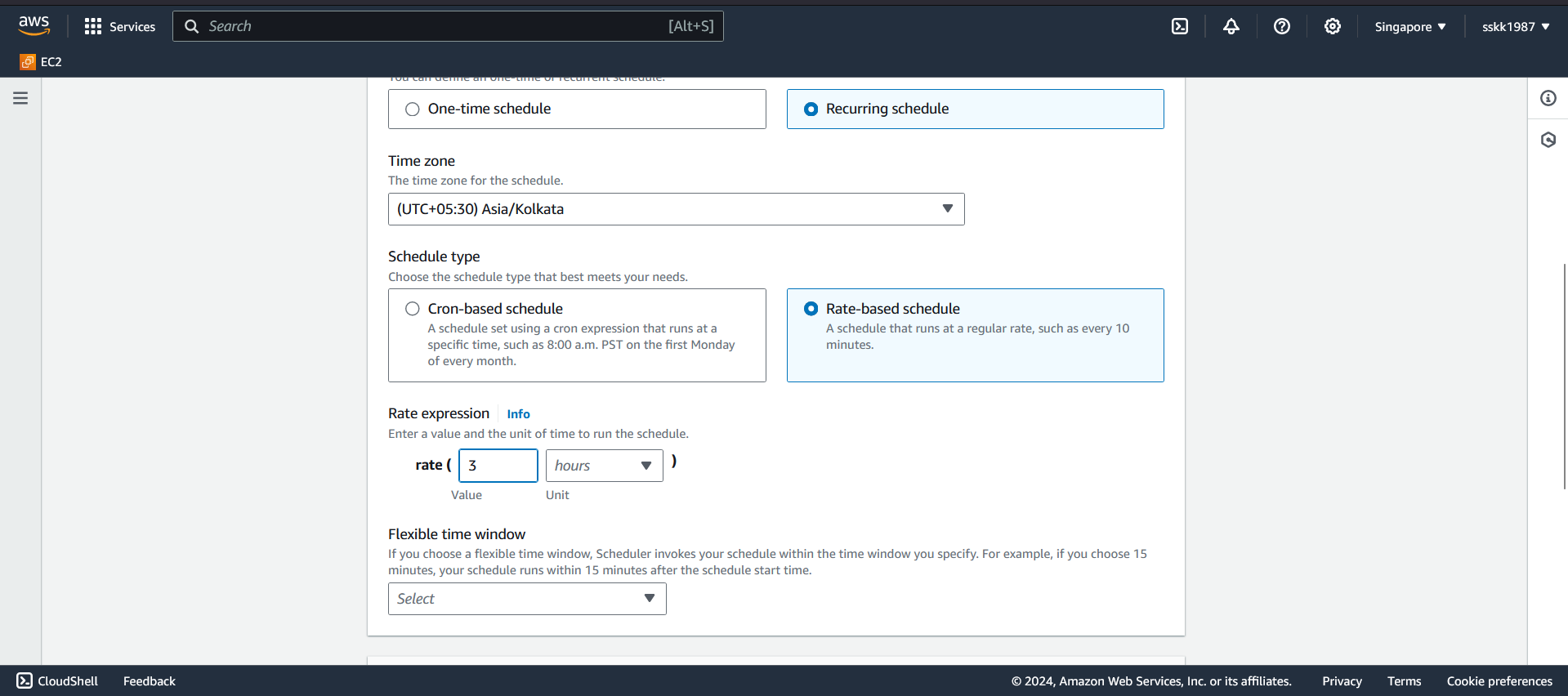
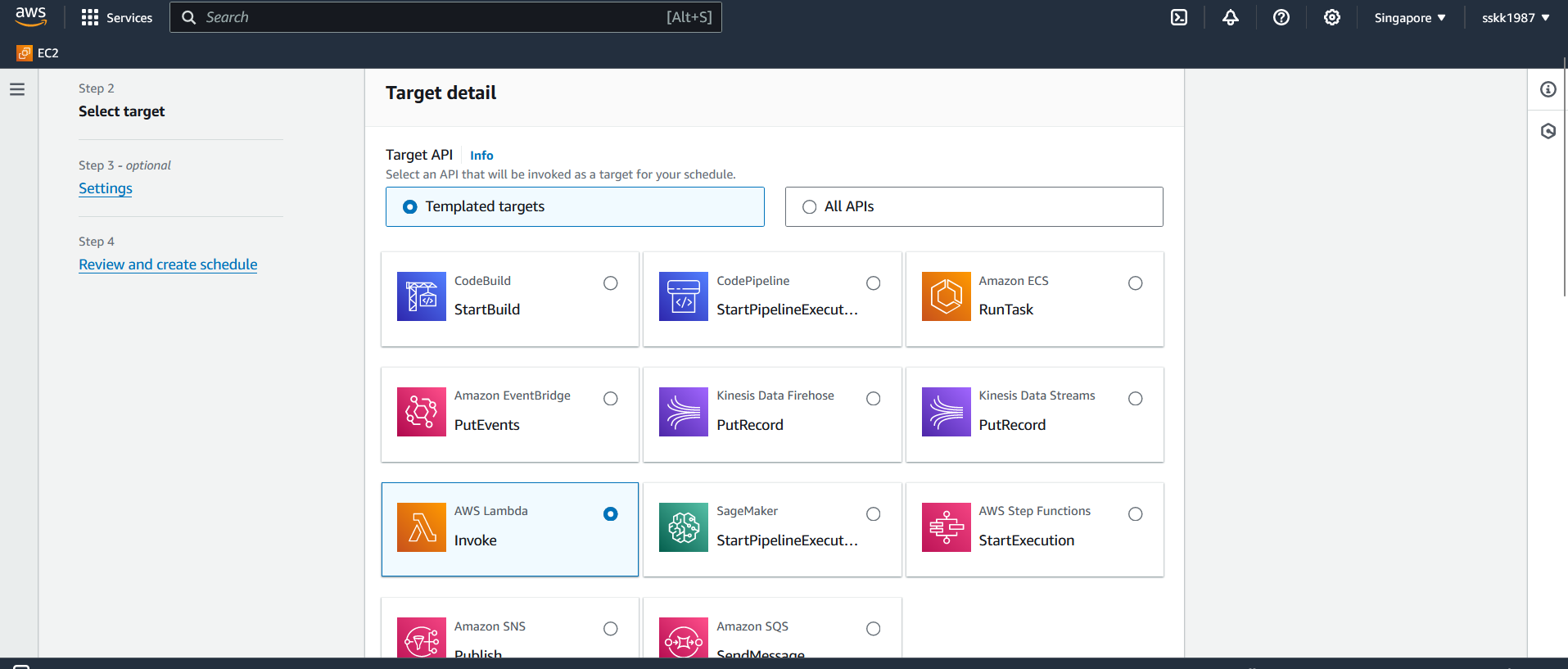
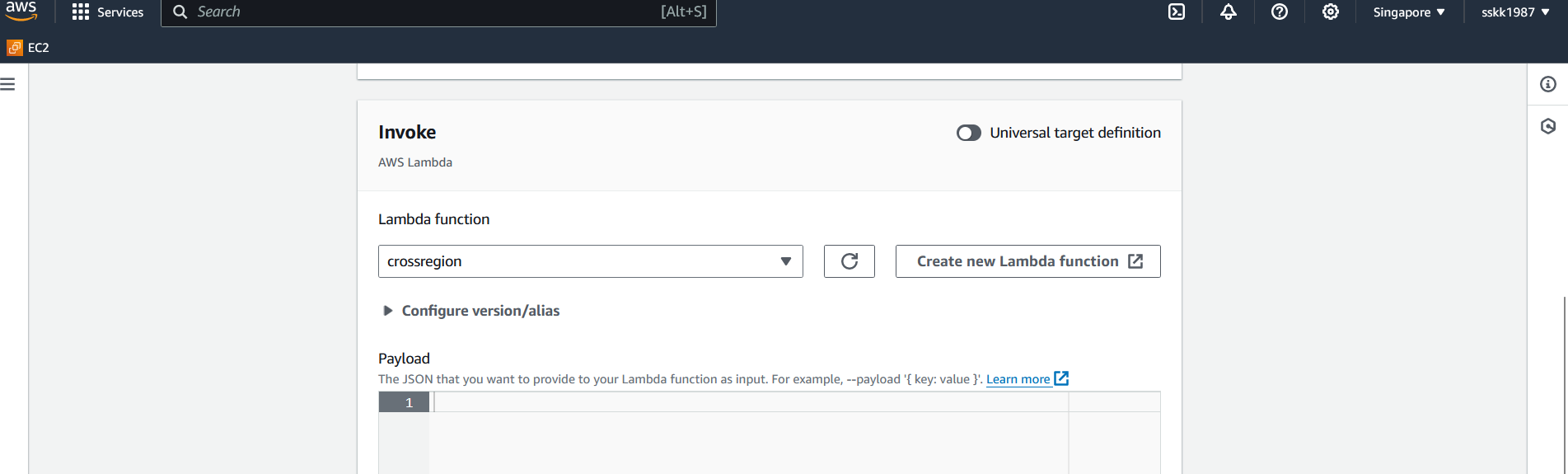










**Cross-Account Access:**

1. **IAM Role for Destination AWS Account**:
   * Go to the IAM console in the destination AWS account.
   * Create an IAM role that allows assuming the IAM role in the source AWS account.
   * Here's an example trust policy allowing the destination account to assume the source account's IAM role:

json

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Principal": {

"AWS": "arn:aws:iam::<source-account-id>:root"

},

"Action": "sts:AssumeRole",

"Condition": {}

}

]

}

1. **Attach Permissions Policy**:
   * Attach a permissions policy to the IAM role in the destination account that allows the necessary actions, such as invoking Lambda functions or any other required operations.

**Additional Steps:**

* **Test Access**: Ensure that cross-region Lambda execution and cross-account access work as expected by testing the Lambda function from the destination AWS account.
* **Monitoring and Logging**: Set up CloudWatch Logs and alarms to monitor the execution of the Lambda function and capture any errors or unexpected behavior.
* **Security Considerations**: Always follow the principle of least privilege when granting permissions to IAM roles and regularly review permissions to ensure they remain appropriate.

By following these steps, you can configure cross-region Lambda execution and cross-account access using IAM, enabling seamless integration and collaboration between AWS accounts and regions.

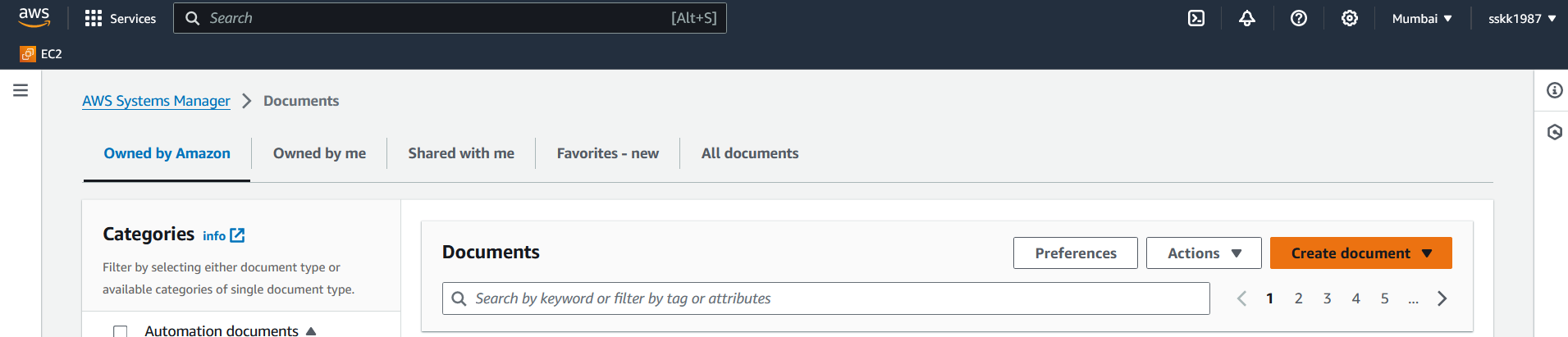
To configure data migration between AWS regions for EBS snapshots, you can use AWS Systems Manager Automation. Below are the steps to achieve this:

**Step 1: Create an Automation Document**

1. **Navigate to AWS Systems Manager**:
   * Go to the AWS Management Console and open the Systems Manager service.



1. **Create Automation Document**:
   * In the Systems Manager console, select "Documents" from the left navigation pane.
   * Click on the "Create document" button.



1. **Specify Document Details**:
   * Provide a name for your document, such as "CrossRegionSnapshotCopy".
   * Optionally, provide a description for the document.
2. **Define Automation Steps**:
   * Define the necessary steps to copy snapshots from the source region to the destination region. This typically involves the following:
     + Identify the snapshots to be copied.
     + Copy each identified snapshot to the destination region.
     + Optionally, tag the copied snapshots with relevant metadata.

**Step 2: Configure Automation Execution**

1. **Set Execution Options**:
   * Choose the execution mode for the Automation document (e.g., "Run Command", "Step Functions").
   * Specify the concurrency and error handling options according to your requirements.
2. **Specify Parameters**:
   * Define any input parameters required for the Automation document, such as source and destination region information.
3. **Review and Create**:
   * Review the document configuration to ensure everything is set up correctly.
   * Click on the "Create automation" button to create the Automation document.

**Step 3: Schedule or Trigger the Automation Document**

1. **Schedule Automation Execution**:
   * If you want the cross-region snapshot copying to occur on a scheduled basis, you can configure a CloudWatch Events rule to trigger the Automation document at specific intervals.
2. **Manual Triggering**:
   * Alternatively, you can manually trigger the Automation document whenever you need to initiate the cross-region snapshot copying process.

**Step 4: Set Up IAM Roles**

1. **Create IAM Roles**:
   * Create an IAM role that grants permissions for cross-region snapshot copying. This role should have permissions to read snapshots from the source region and create snapshots in the destination region.
2. **Assign Roles to Automation Execution Role**:
   * Assign the IAM roles created in the previous step to the Automation execution role. This allows the Automation document to assume the necessary roles to perform the snapshot copying operations.

**Step 5: Testing and Validation**

1. **Test the Automation Document**:
   * Run the Automation document manually or trigger it using the scheduled CloudWatch Events rule to test the cross-region snapshot copying process.
   * Verify that snapshots are successfully copied from the source region to the destination region.
2. **Validate Permissions and Configuration**:
   * Ensure that the IAM roles have appropriate permissions and that the Automation document is configured correctly for seamless cross-region snapshot migration.