### 

[**Activity: Permitting EC2 access to DynamoDB using IAM Roles 2**](#_plu2jzjoe94j)

[Step 1: Create the DynamoDB table with data 2](#_wydkpzcm47j4)

[Step 2: Create the Policy 2](#_6lf1n0gilaxa)

[Step 3: Create the IAM Role 4](#_quxnoya1czrg)

[Step 4: Create the EC2 5](#_ee9vsuizund7)

[Step 4: Verify permissions 5](#_tw064379tk6)

[Step 5: Detach IAM role 5](#_mjfhbhc88jxu)

### 

### 

### Activity: Permitting EC2 access to DynamoDB using IAM Roles

In this activity, we want to allow our EC2 to access our DynamoDB table through an IAM Role. This demonstrates the use of identity-based permission without having to issue api credentials.

#### Prerequisites

* Existing VPC

#### Step 1: Create the DynamoDB table with data

Create table

New table with the following configuration:

* Table Name: **<yourname>-bookinventory**
* Partition Key: ISBN (String)
* Sort Key: Genre (String)
* Leave all other settings as default.

Add data to the table

Remember to replace <your table> with your own table name as created above

|  |
| --- |
| aws dynamodb **put**-item \  --table-name <your table> \  --item \  '{"ISBN": {"S": "978-0134685991"}, "Genre": {"S": "Technology"}, "Title": {"S": "Effective Java"}, "Author": {"S": "Joshua Bloch"}, "Stock": {"N": "1"}}'  aws dynamodb **put**-item \  --table-name <your table> \  --item \  '{"ISBN": {"S": "978-0134685009"}, "Genre": {"S": "Technology"}, "Title": {"S": "Learning Python"}, "Author": {"S": "Mark Lutz"}, "Stock": {"N": "2"}}'  aws dynamodb **put**-item \  --table-name <your table> \  --item \  '{"ISBN": {"S": "974-0134789698"}, "Genre": {"S": "Fiction"}, "Title": {"S": "The Hitchhiker"}, "Author": {"S": "Douglas Adams"}, "Stock": {"N": "10"}}' |

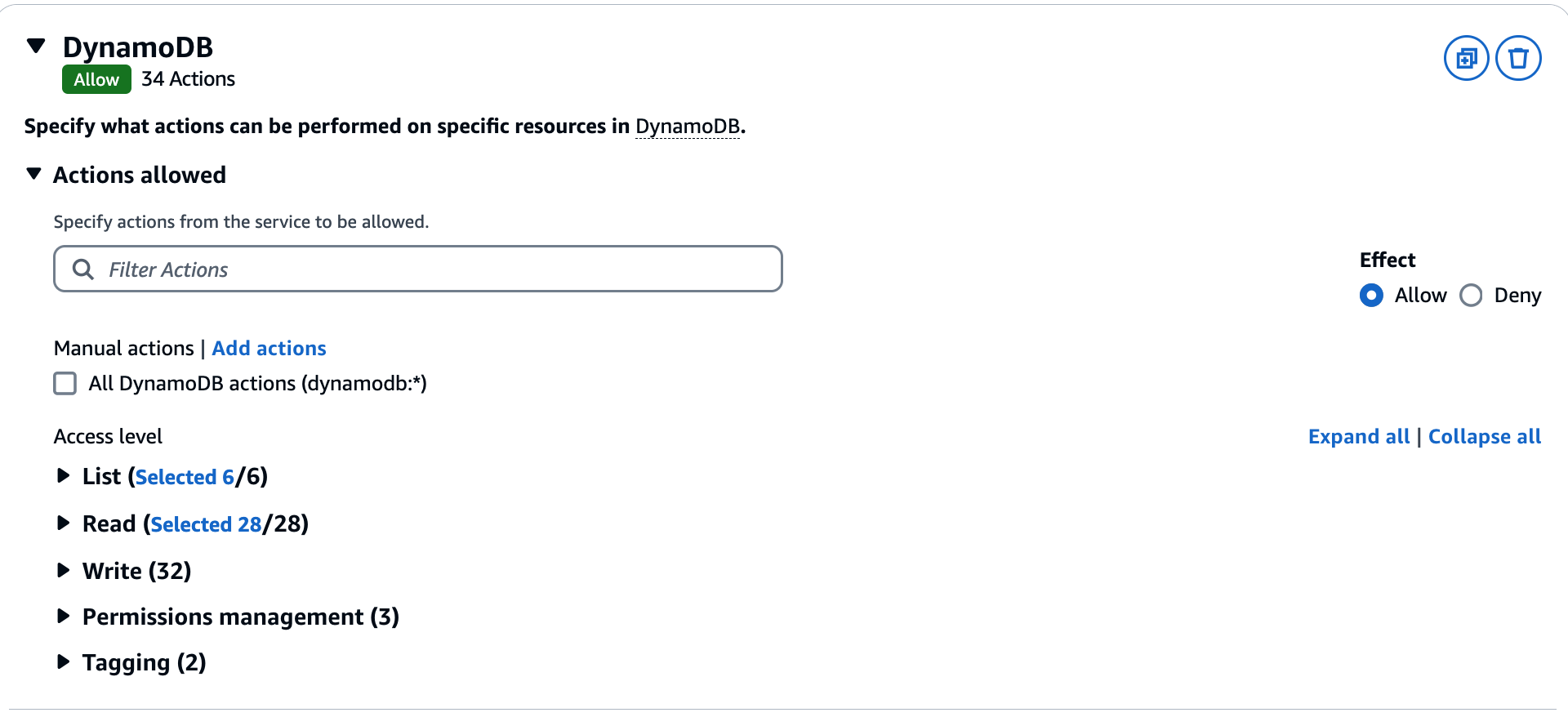
#### Step 2: Create the Policy

Go to IAM -> policy

Service: DynamoDB

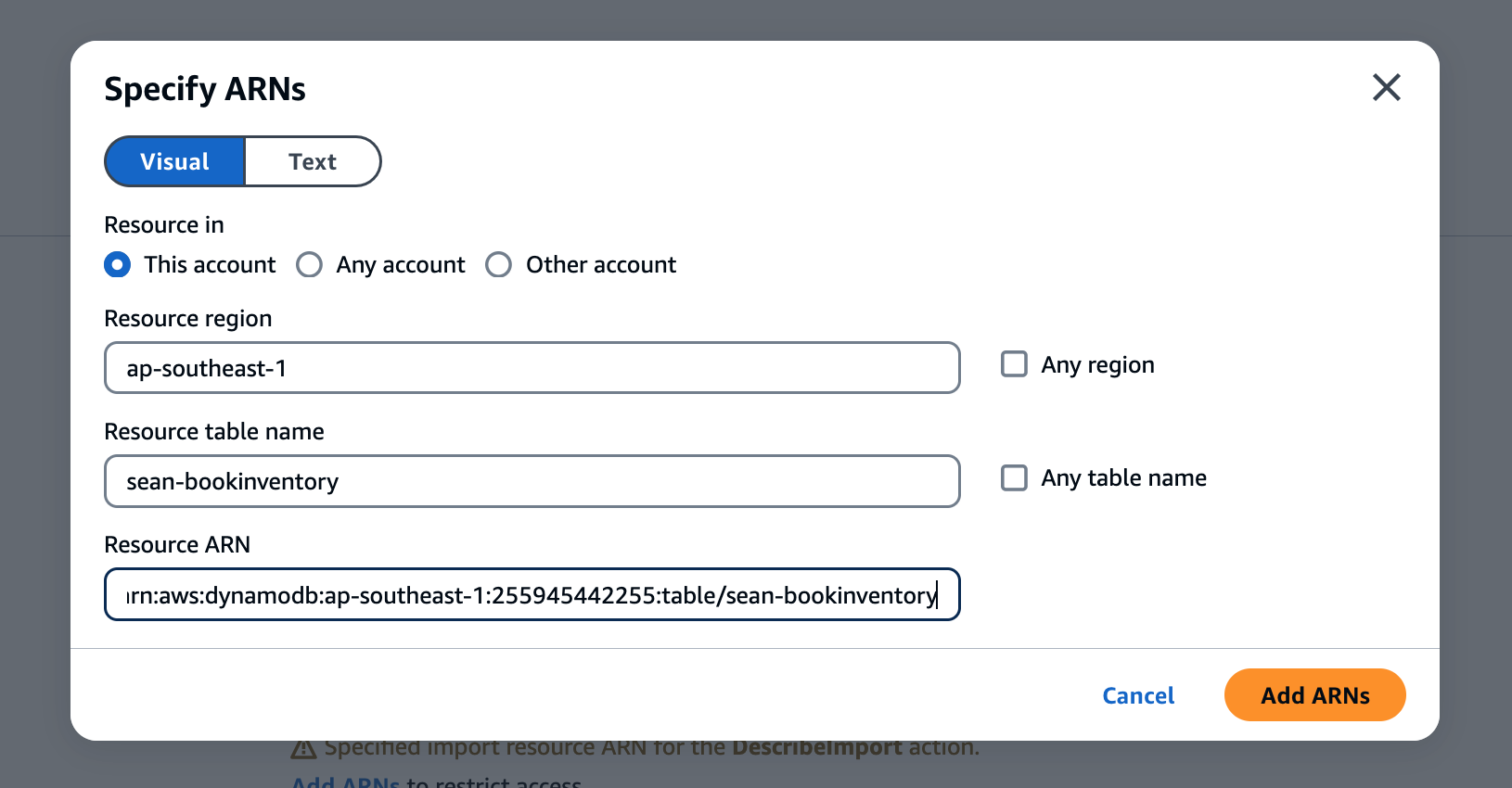
Actions allowed:

* All list
* All read



Resources:

* Specific to your table using arn

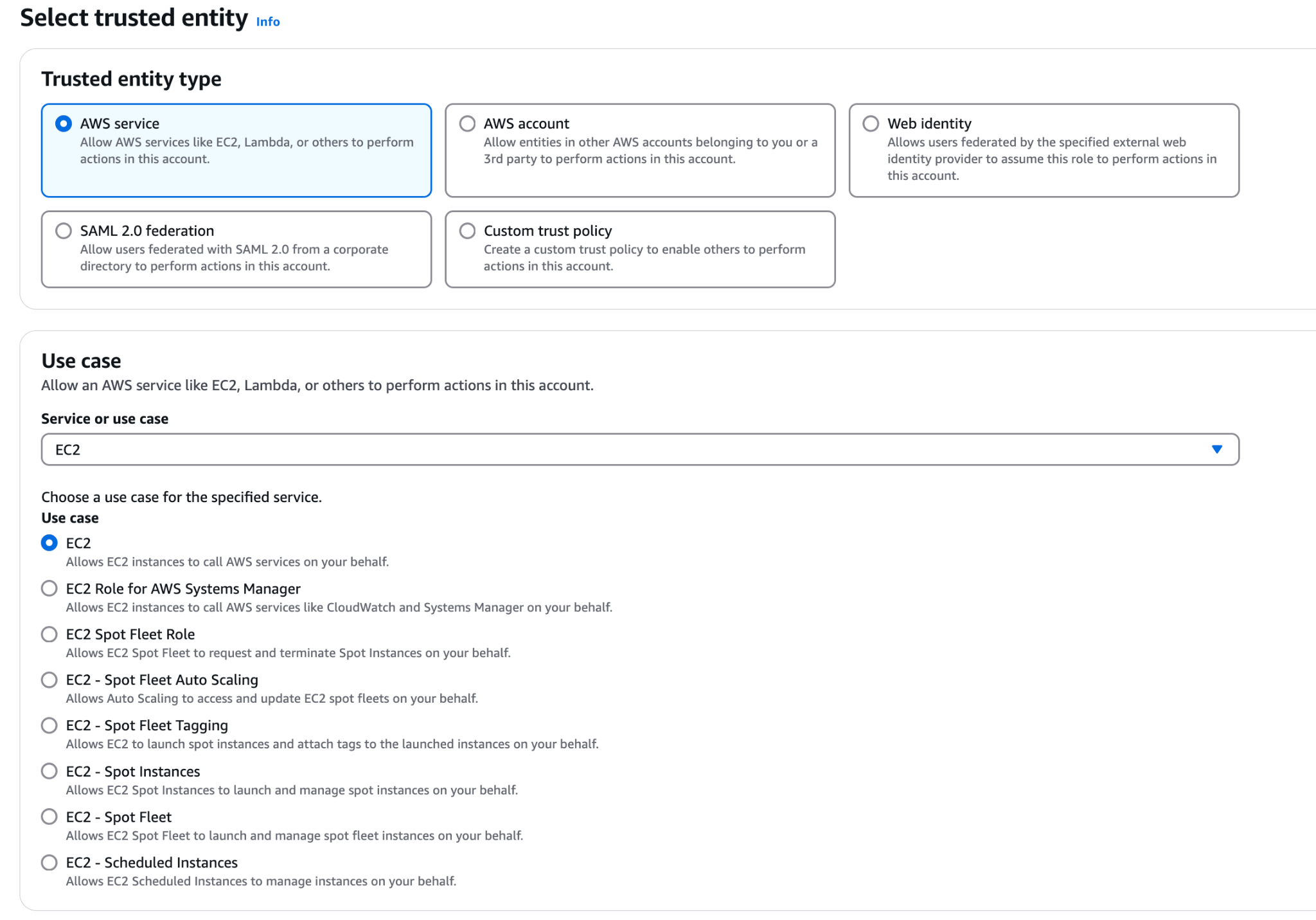


Name: <yourname>-dynamodb-read

#### 

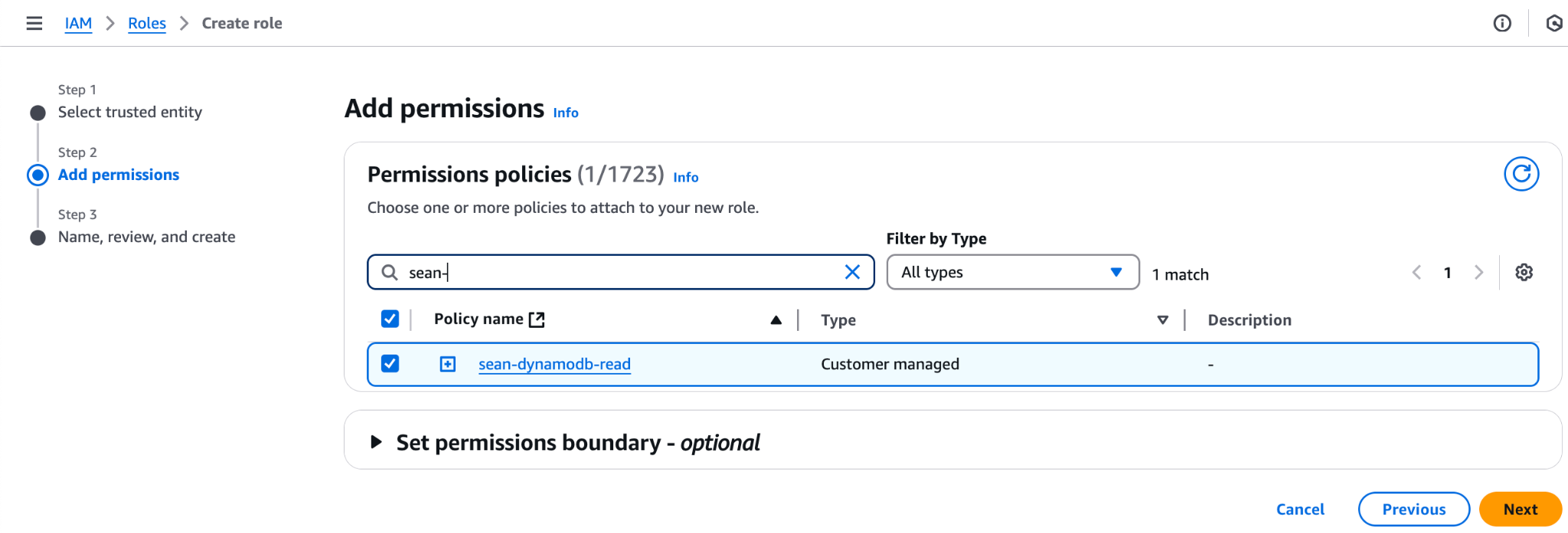
#### Step 3: Create the IAM Role

Create Role



Assign Policy

Assign the policy created earlier to the role

****

Review

Role name: <yourname>-dynamodb-read-role

#### Step 4: Create the EC2

EC2 name: <yourname>-dynamodb-reader

Image: Amazon Linux 2023 AMI (default)

Network requirements:

* EC2 to accept SSH requests from home
* EC2 to be able to reach https endpoints
* Note: just SSH with default setting can alrdy (1 SSH)

Bef we launch instance, go to the last part and expand advanced details.

IAM instance profile: (Pick the profile you created)

Leave the rest as default

#### Step 4: Verify permissions

In the EC2 instance, use the following commands to verify the permissions

aws dynamodb list-tables

aws dynamodb scan --table-name <table-name>

aws dynamodb delete-table --table-name <table-name>

* Does it match the permissions you’ve assigned to it?

#### Step 5: Detach IAM role

Detach the IAM role then verify if the instance is still permissioned as before.

