# AWS auto onboarding lambda Function

Code and components:

<https://github.com/smakineni-panw/aws-cft-pc>

**Note**: If cloud provisioning admin service account is used then the account group id in code must match the one assigned to the access key.

**Limitations**:

Lambdas have a 15 minute maximum timeout and the stack must be created within this time period for initial onboarding. This does not apply to template updates. Individual account stack creation occurs quickly and should not pose a problem but large organizations where stack creation takes longer than 14 minutes could fail.

**Use case**:

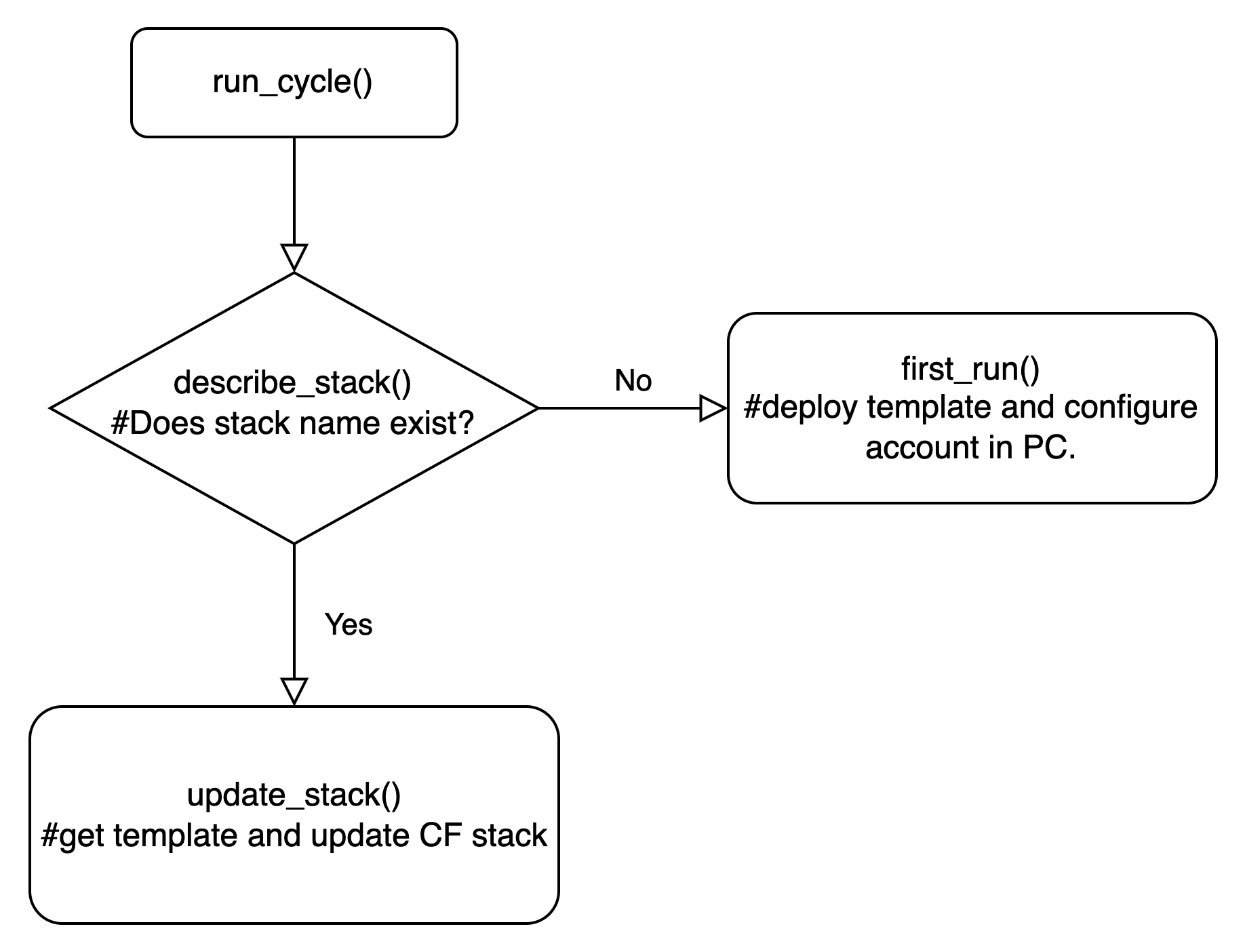
Third party vendor account with no access

Auto-pilot-permissions

**Pre-requisites**:

* Prisma cloud access key.
* Cloud account access.
* Lambda layer with PCPI built into the zip file.

**Workflow:**



**Build lambda layer:**

#/bin/bash

mkdir lambda-maker

cd lambda-maker/

mkdir python

cd python/

pip3 install pcpi -t .

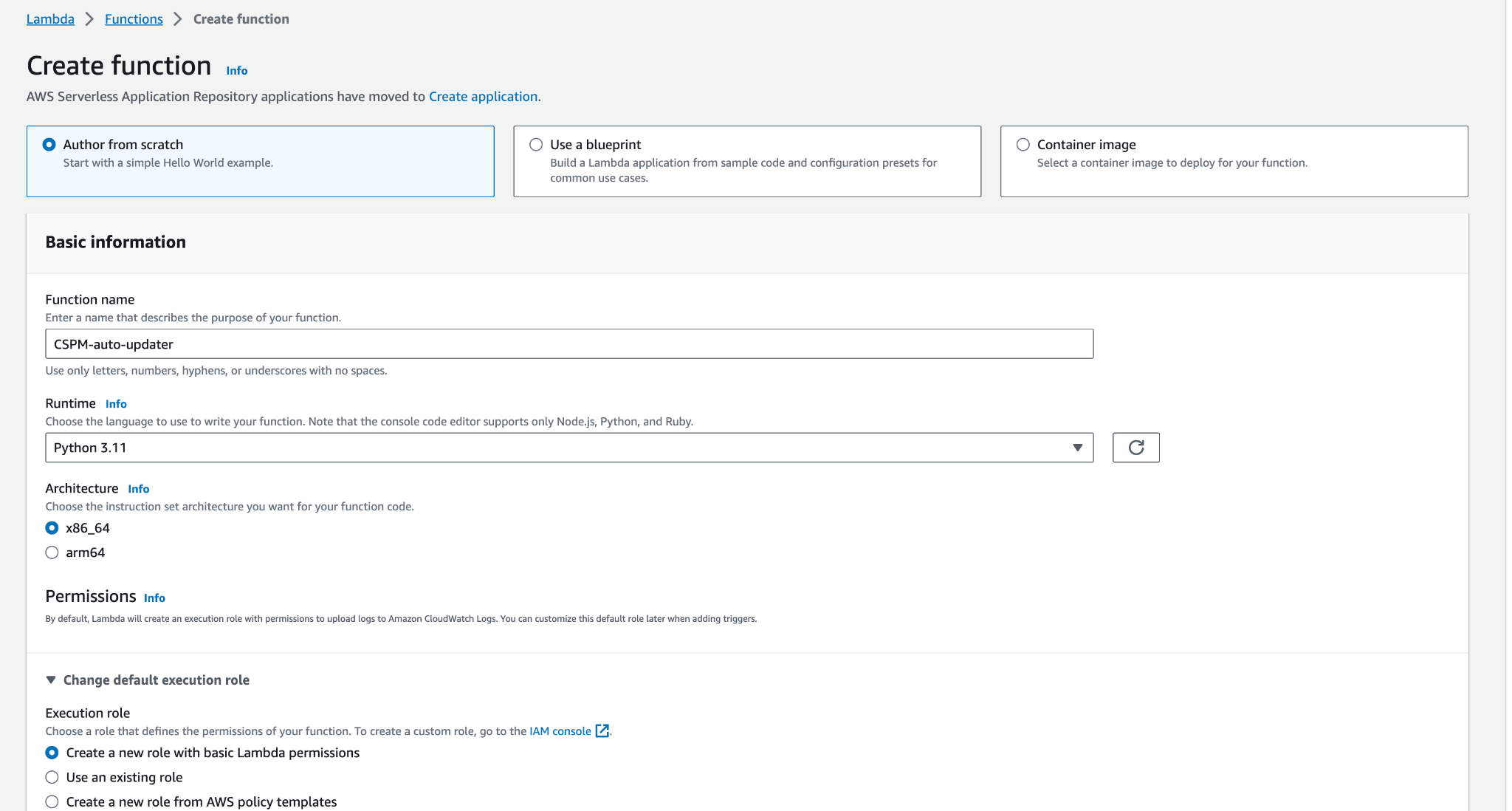
rm -rf \*.dist-info

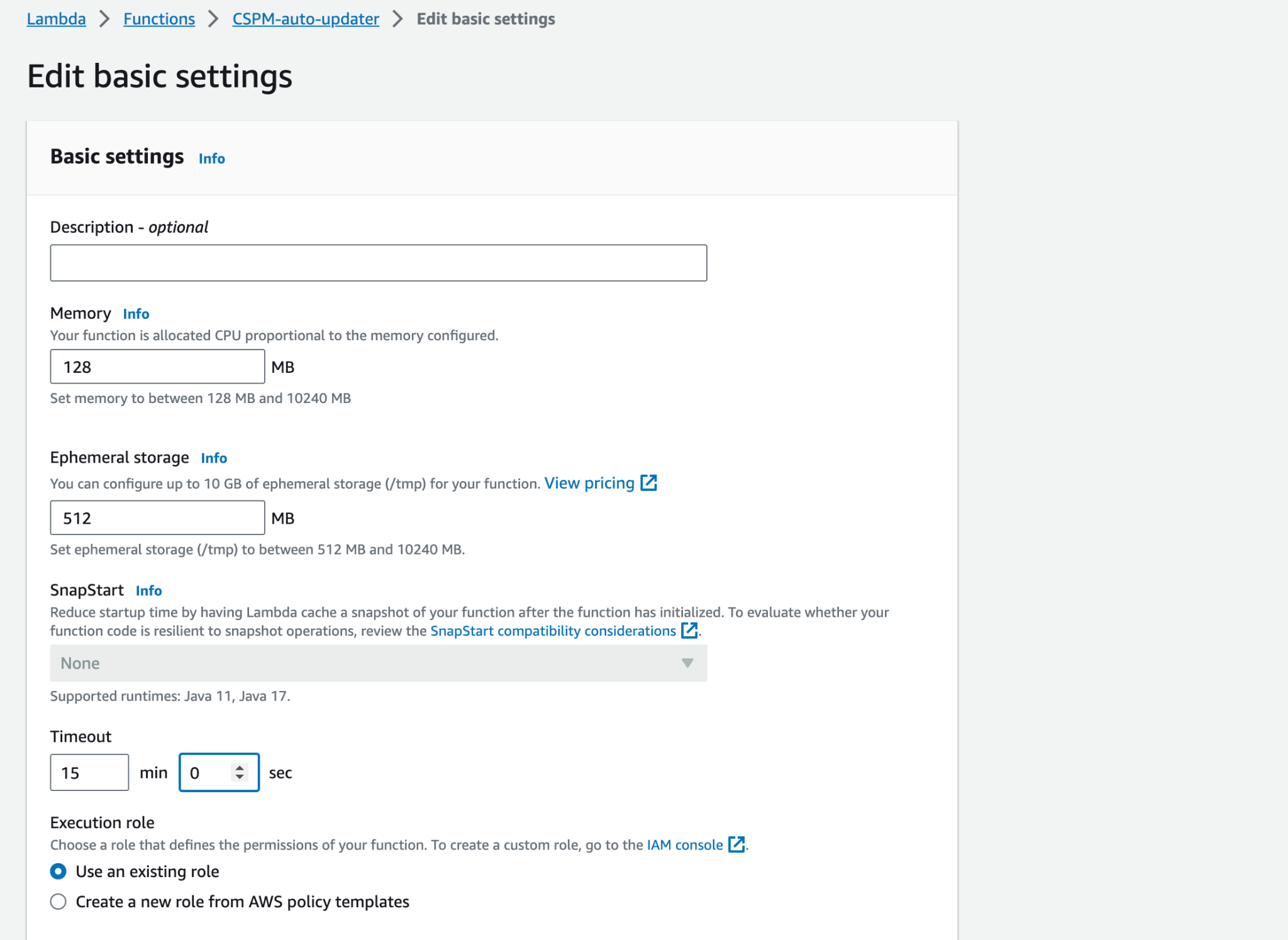
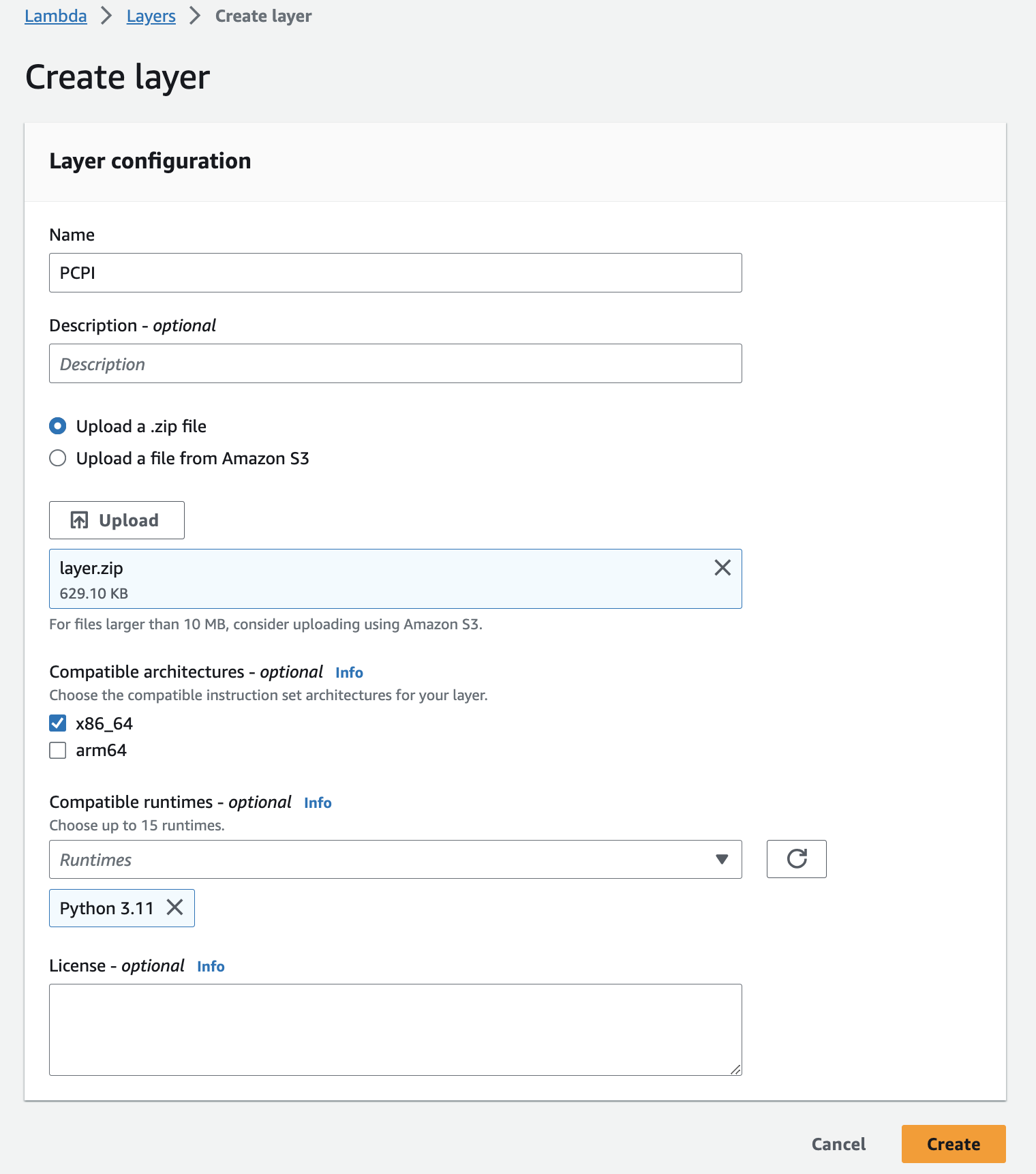
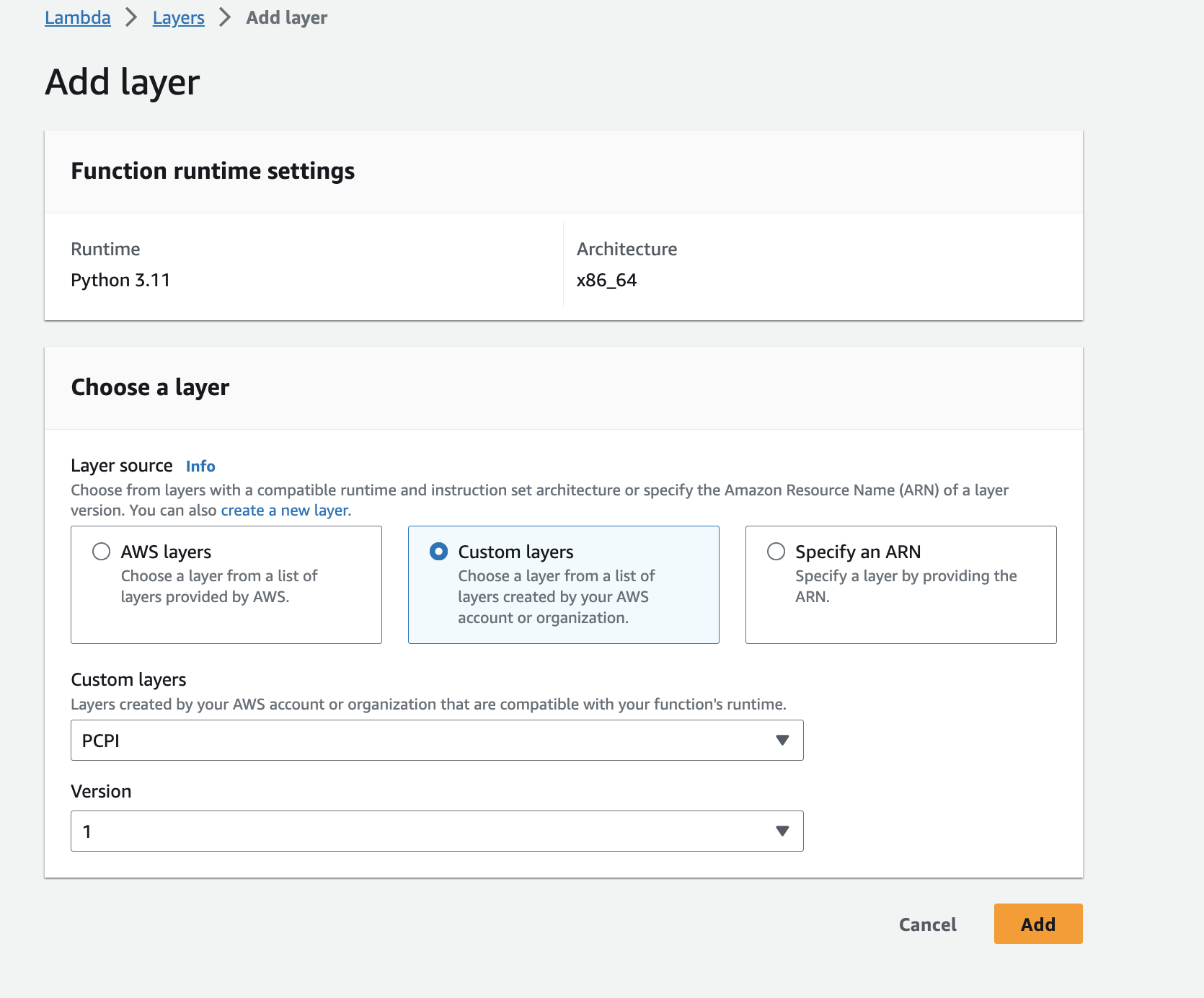
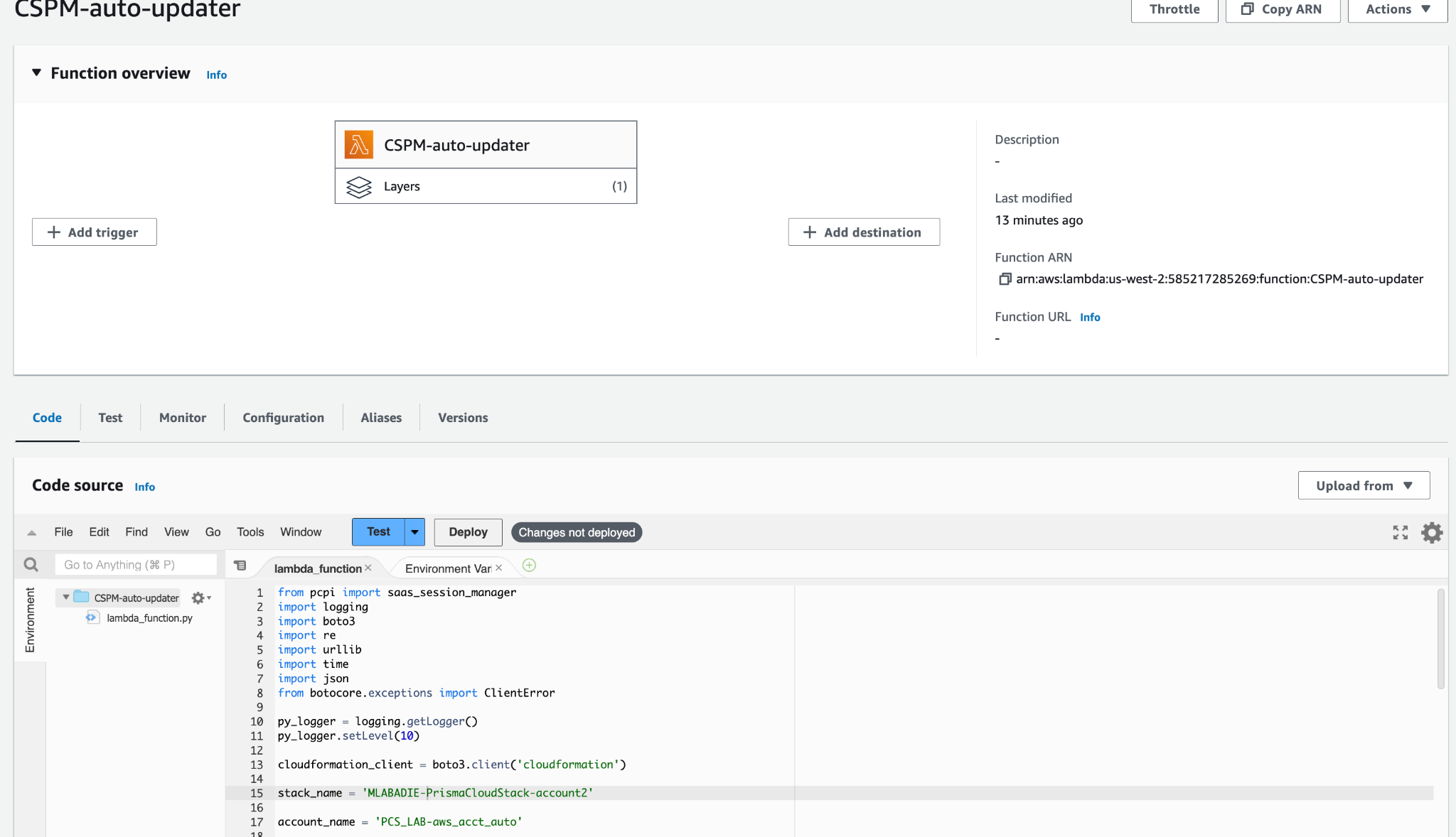
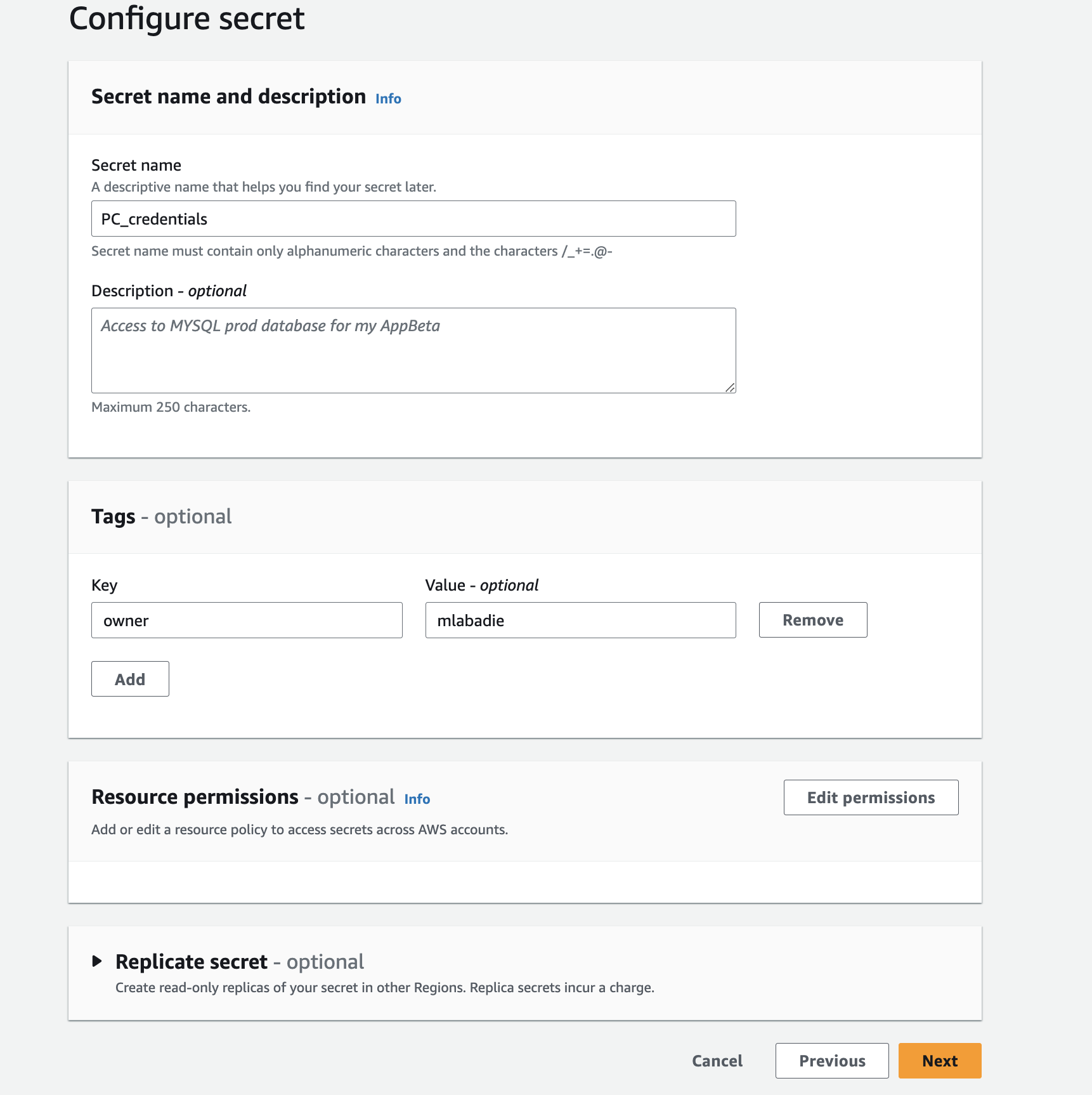
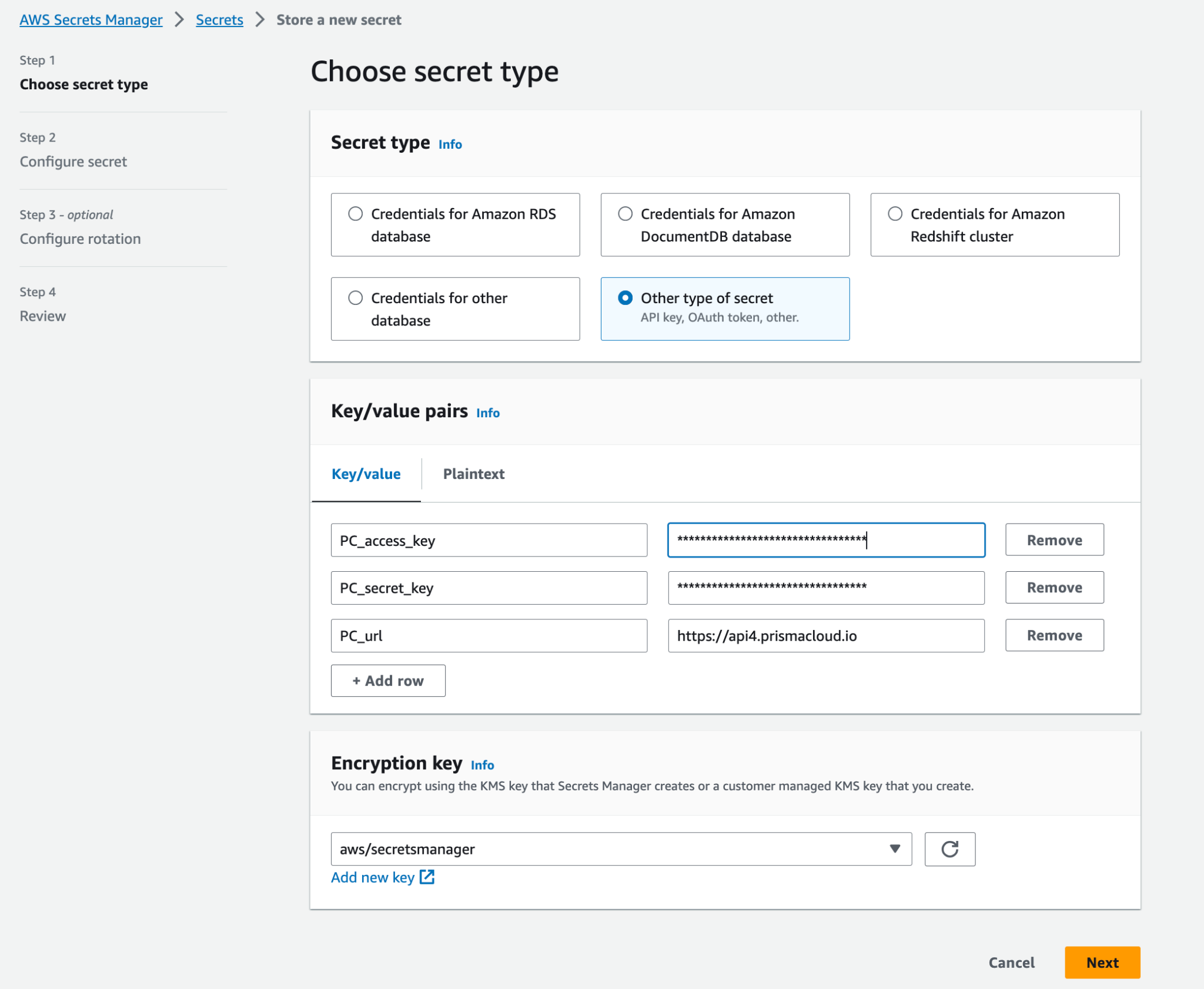
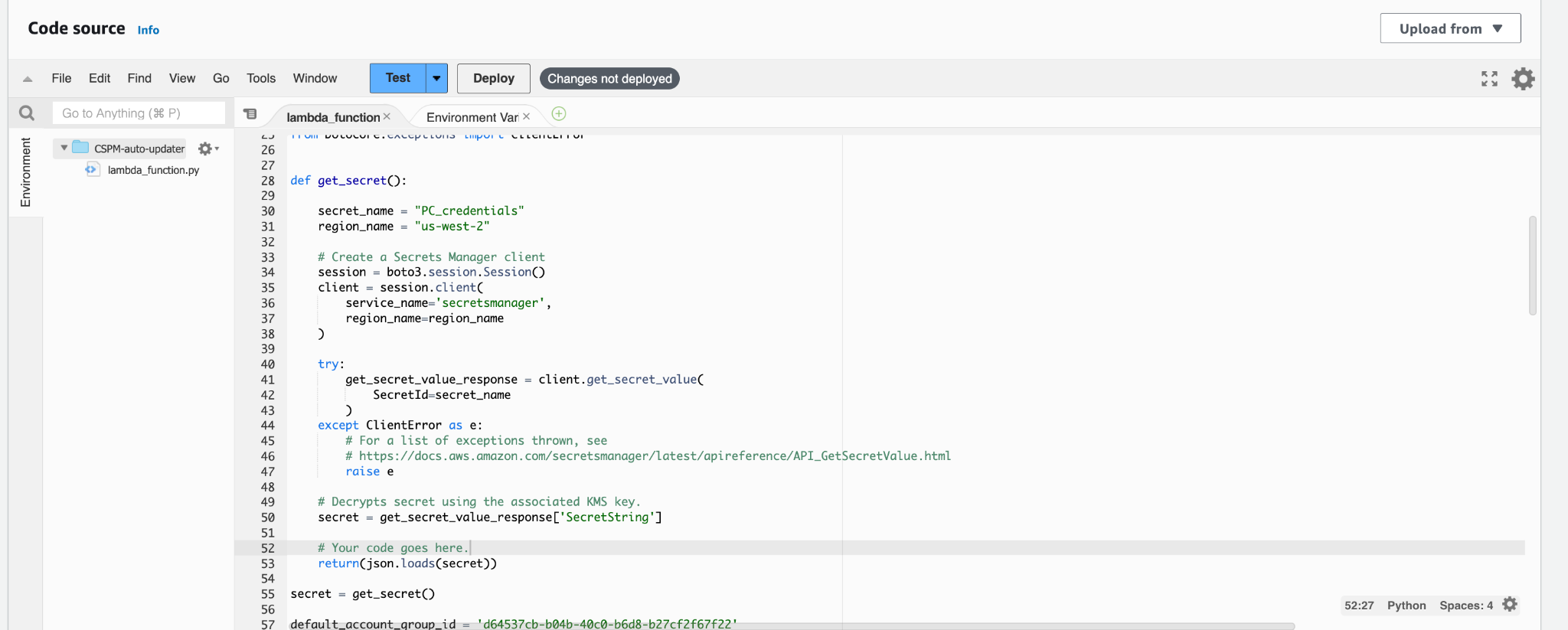
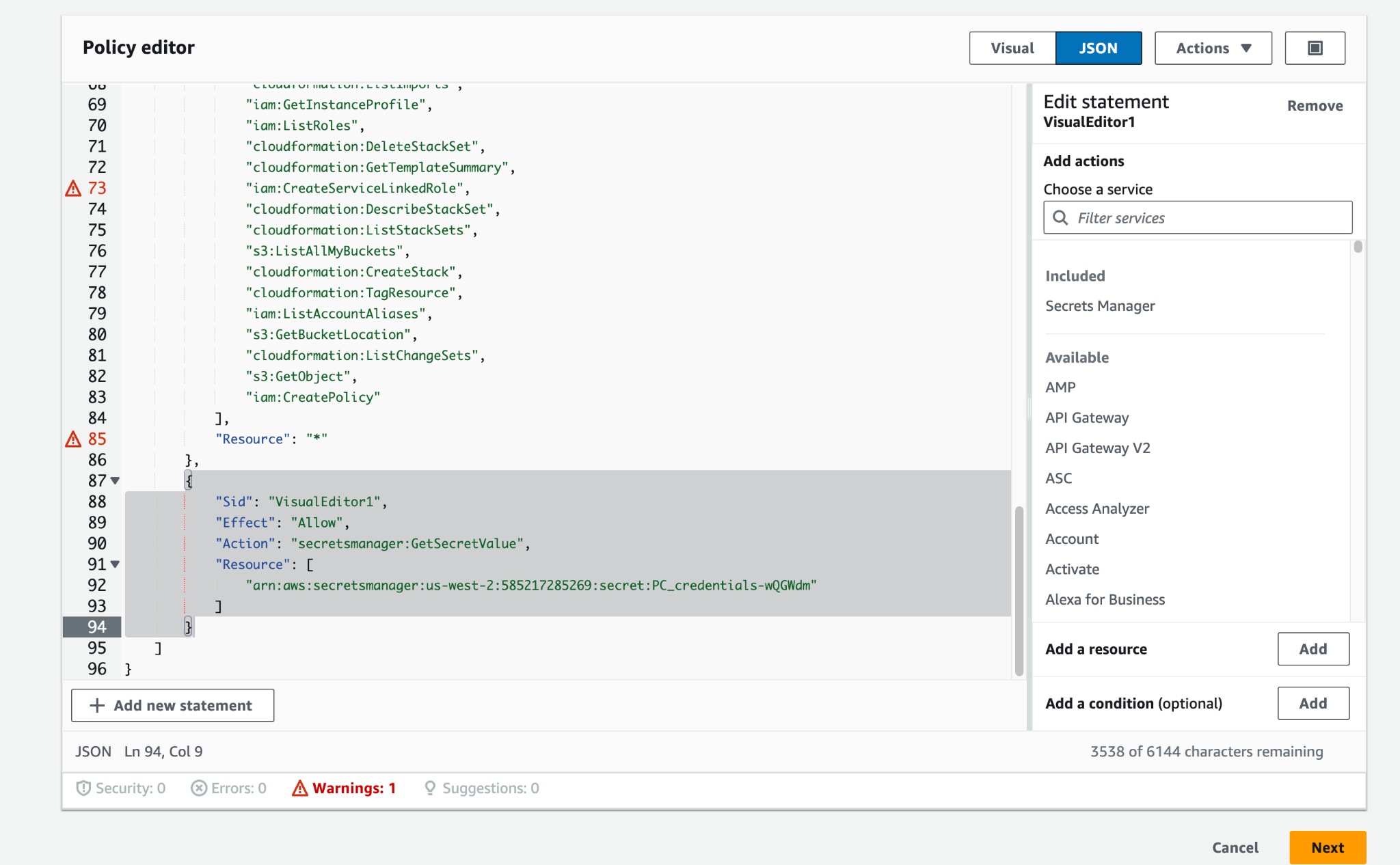
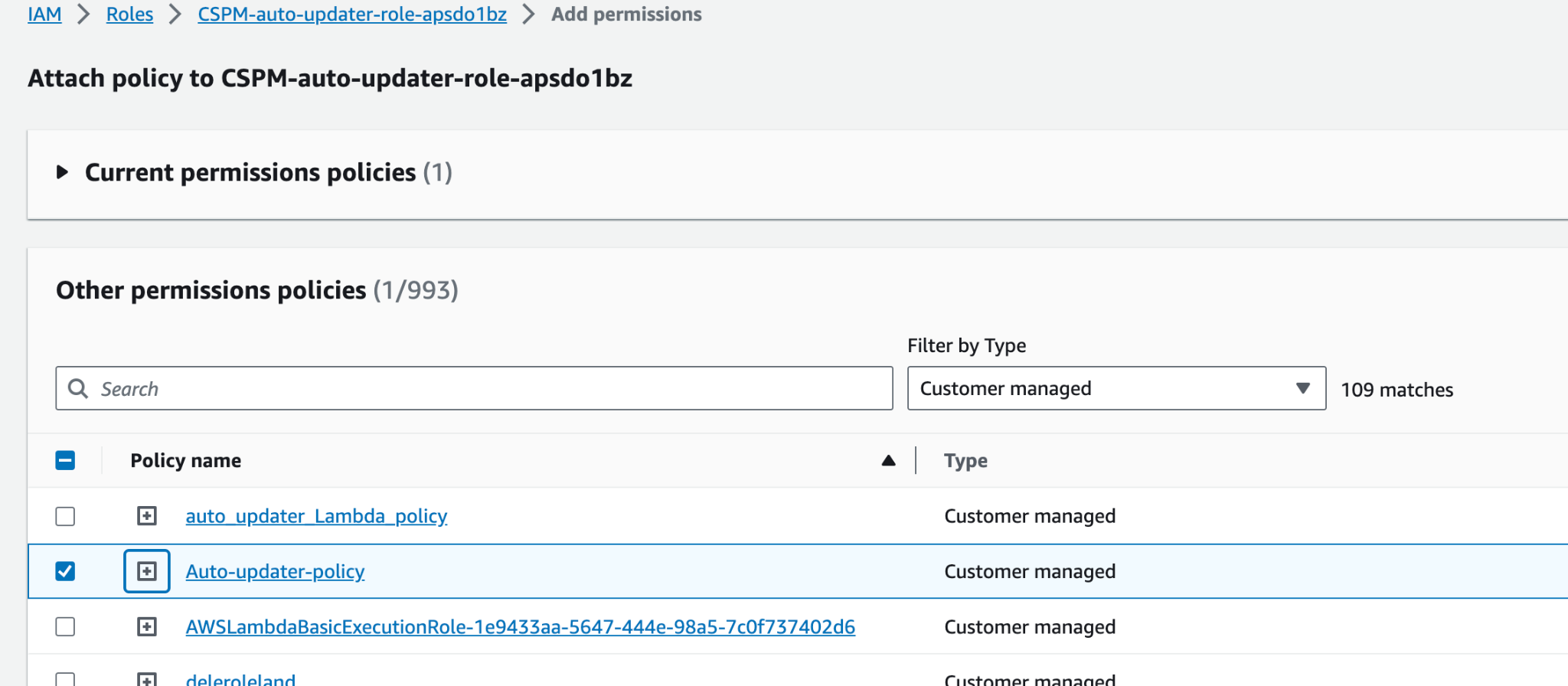
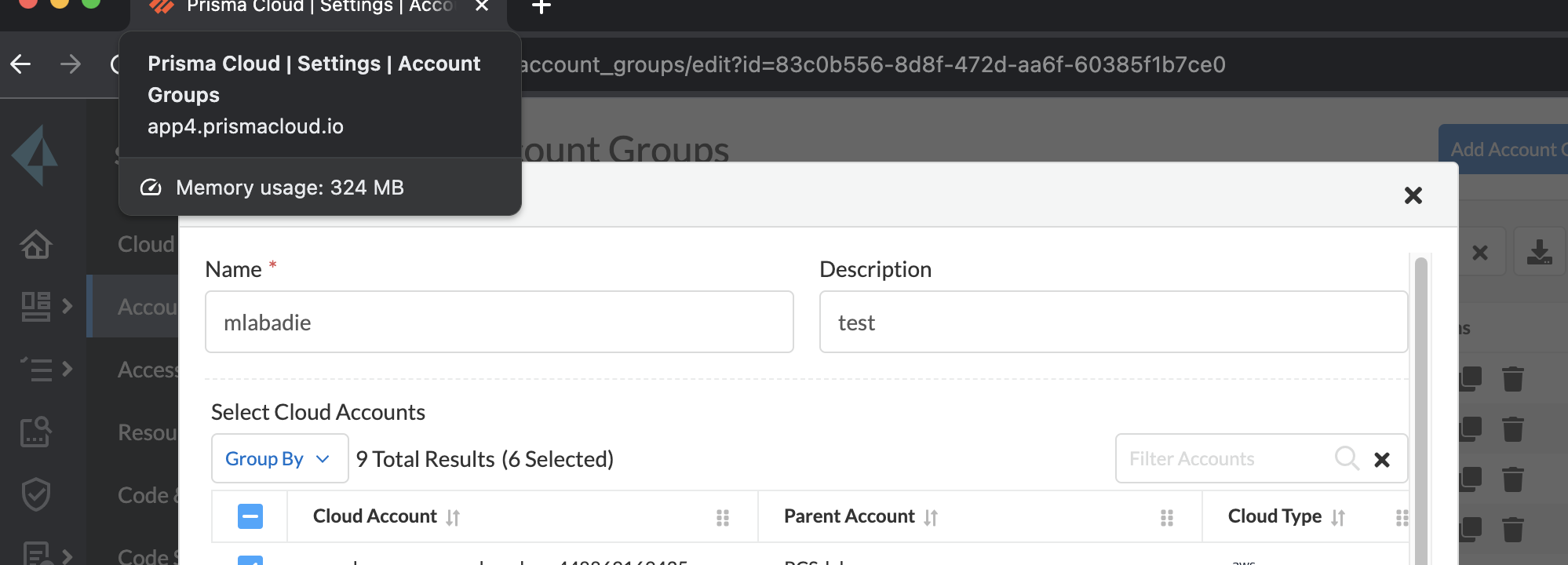
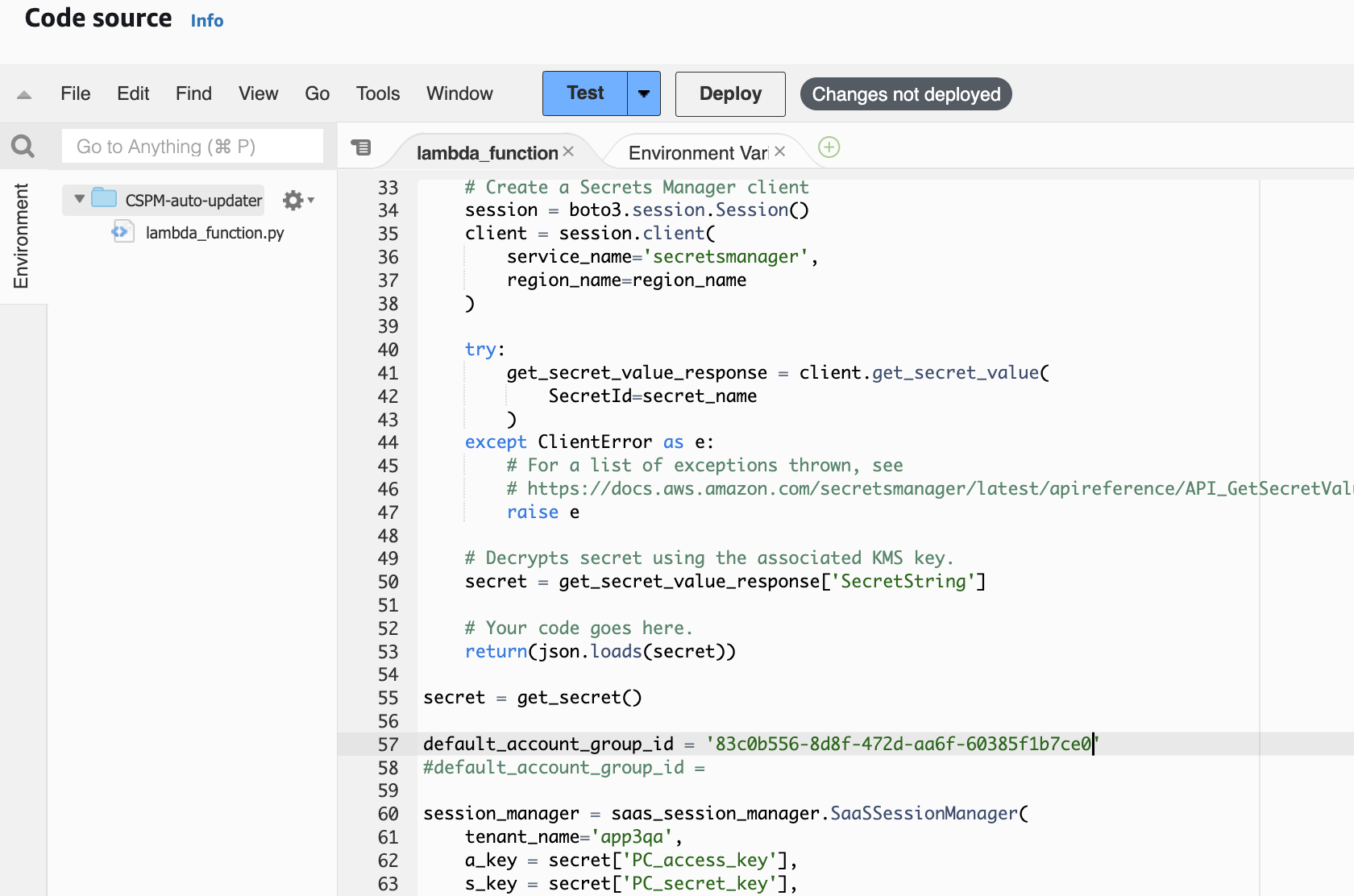
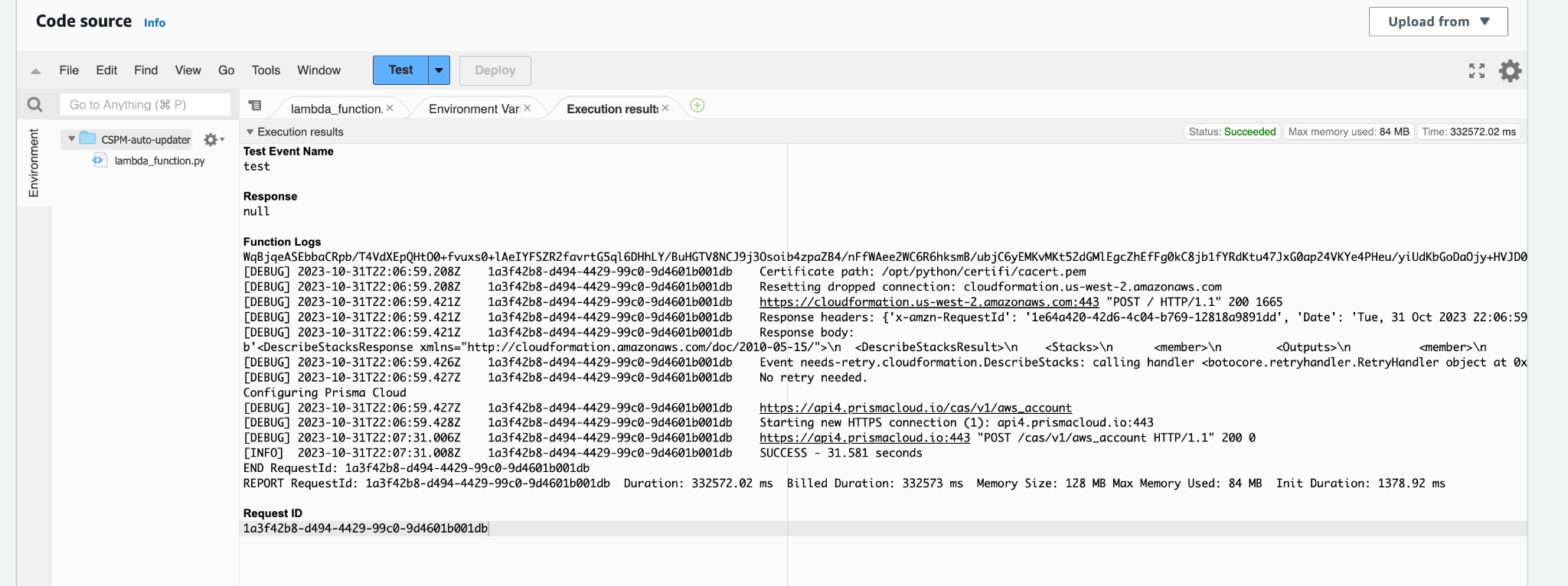
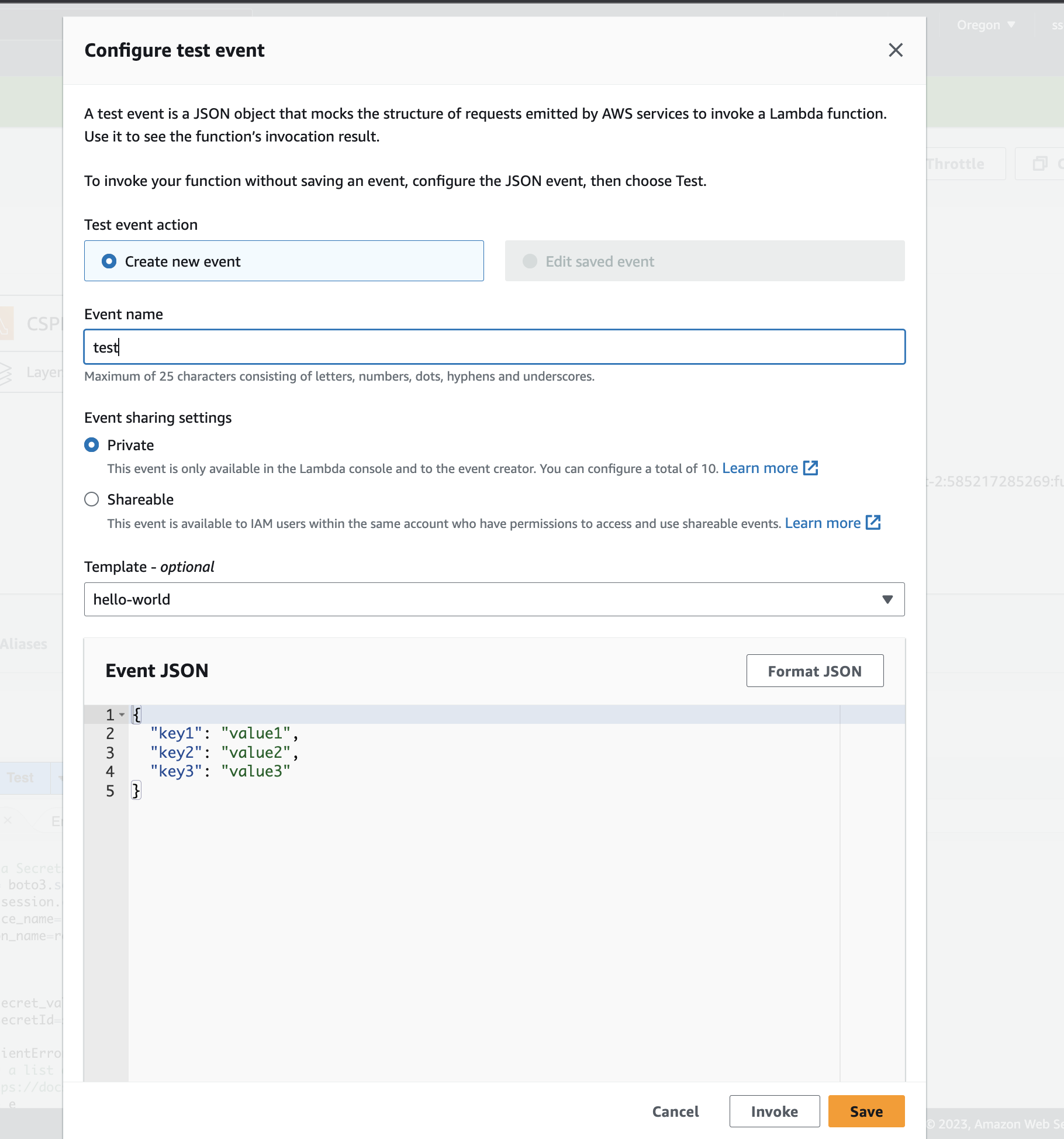
cd ..

zip -r PCPI-lambda-layer.zip python/

**Setup instructions:**

1. Create python Lambda with a new execution role.



1. Increase Lambda timeout to the 15 minutes maximum.
2. Create a layer with layer.zip containing the PCPI library.
3. Add layer to function.
4. Add code to lambda.
5. Create “other type” secret with 3 keys: PC\_access\_key,PC\_secret\_key,PC\_url.
6. Add get secret function to code while keeping return line.
7. Create IAM policy with JSON template and add previously created secret ARN.
8. Attach policy to lambda execution role.
9. Edit default account group ID in code. 
10. Deploy & Test with blank event, doesn’t use event or context.
11. Schedule using trigger with eventbridge and new rule: cron(15 10 ? \* 6L \*)