

Operationalizing-an-AWS-ML-Project

Dog Image Classification

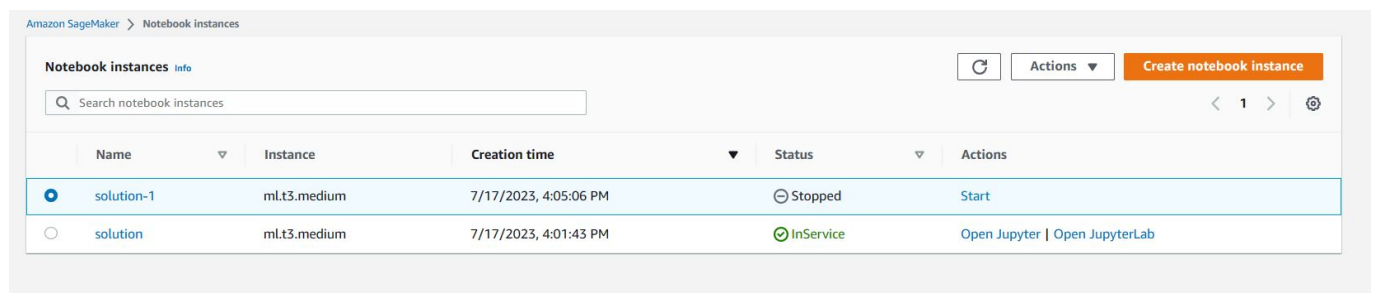
The completed project contains code that trains and deploys an image classification model on AWS Sagemaker. Your goal in this project will be to use several important tools and features of AWS to adjust, improve, configure, and prepare the model you started with for production-grade deployment.

In this project, you will complete the following steps:

1. Train and deploy a model on Sagemaker, using the most appropriate instances. Set up multi-instance training in your Sagemaker notebook.
2. Adjust your Sagemaker notebooks to perform training and deployment on EC2.
3. Set up a Lambda function for your deployed model. Set up auto-scaling for your deployed endpoint as well as concurrency for your Lambda function.
4. Ensure that the security on your ML pipeline is set up properly.

Step 1: Training and deployment on Sagemaker

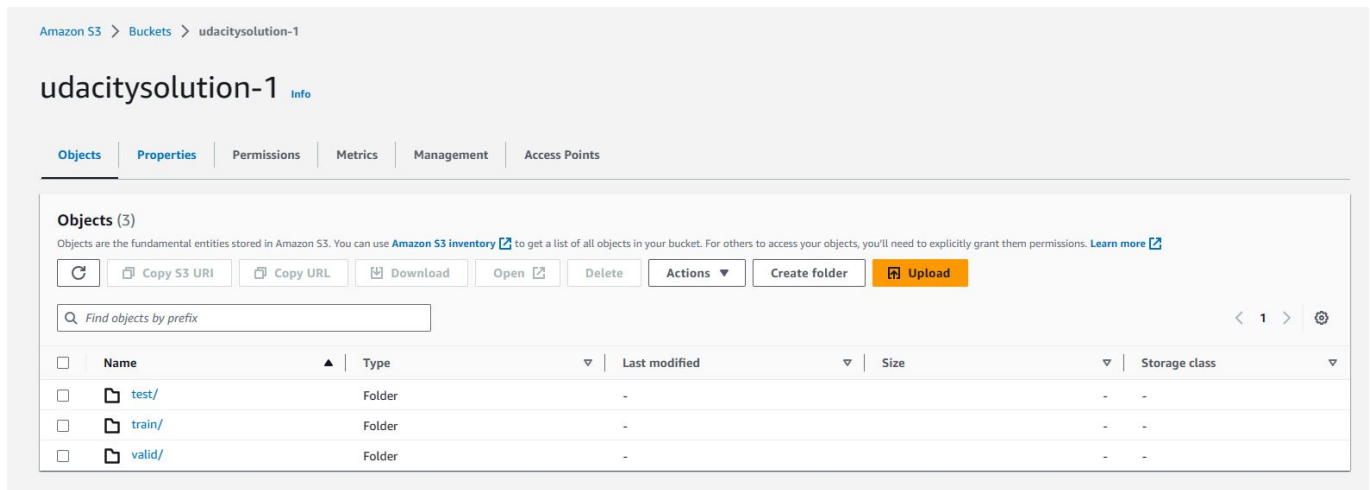
- **Created sagemaker notebook instance** For creating sagemaker notebook, I used ml.t3.medium because it is a low cost instance and would be sufficient to run my notebook.



Name	Instance	Creation time	Status	Actions
solution-1	ml.t3.medium	7/17/2023, 4:05:06 PM	Stopped	Start
solution	ml.t3.medium	7/17/2023, 4:01:43 PM	InService	Open Jupyter Open JupyterLab

- **S3 bucket for the job** I created a bucket name "udacitysolution-1" and upload data into it using the following code:

```
!wget https://s3-us-west-1.amazonaws.com/udacity-aind/dog-project/dogImages.zip
!unzip dogImages.zip
!aws s3 cp dogImages s3://udacitysolution/ --recursive
```



For this model, there are two hyperparameters: learning rate and batch size.

```
hyperparameter_ranges = {
    "learning_rate": ContinuousParameter(0.001, 0.1),
    "batch_size": CategoricalParameter([32, 64, 128, 256, 512]),
}
```

I used a py script (hpo.py) as entry point to the estimator, this script contains the code need to train model with different hyperparameters values.

```
estimator = PyTorch(
    entry_point="hpo.py",
    base_job_name='pytorch_dog_hpo',
    role=role,
    framework_version="1.4.0",
    instance_count=1,
    instance_type="ml.g4dn.xlarge",
    py_version='py3'
)

tuner = HyperparameterTuner(
    estimator,
    objective_metric_name,
    hyperparameter_ranges,
    metric_definitions,
    max_jobs=2,
    max_parallel_jobs=1, # you once have one ml.g4dn.xlarge instance available
    objective_type=objective_type
)
```

Here I passed some paths to our S3 which will be used by the notebook instance to get data, save model and output

```
os.environ['SM_CHANNEL_TRAINING']='s3://udacitysolution-1/'
os.environ['SM_MODEL_DIR']='s3://udacitysolution-1/model/'
os.environ['SM_OUTPUT_DATA_DIR']='s3://udacitysolution-1/output/'
tuner.fit({"training": "s3://udacitysolution-1/"})
```

I started the model training we can see the training job status at SageMaker -> Training -> Training Jobs

Best training job

Training jobs

Training job definitions

Tuning Job configuration

Tags

Training job status counter

Completed 2In Progress 0Stopped 0Failed 0 (Retryable: 0, Non-retryable: 0)

Training jobs

Sorting by objective metric value will display only jobs that have metric values.

View logs

View instance metrics

Stop

Create model

Search training jobs

<1>

	Name	Status	Final objective metric value	Creation time	Training Duration
<input type="radio"/>	pytorch-training-230717-0922-002-f37839c7	Completed	129	7/17/2023, 4:47:09 PM	17 minute(s)
<input type="radio"/>	pytorch-training-230717-0922-001-1a41923c	Completed	474	7/17/2023, 4:22:32 PM	21 minute(s)

Then I got the best model

Best training job hyperparameters

Search

Name	Type	Value
_tuning_objective_metric	FreeText	Test Loss
batch_size	Categorical	"32"
learning_rate	Continuous	0.007770519608421199
sagemaker_container_log_level	FreeText	20
sagemaker_estimator_class_name	FreeText	"PyTorch"
sagemaker_estimator_module	FreeText	"sagemaker.pytorch.estimator"
sagemaker_job_name	FreeText	"pytorch_dog_hpo-2023-07-17-09-22-26-957"
sagemaker_program	FreeText	"hpo.py"
sagemaker_region	FreeText	"us-east-1"
sagemaker_submit_directory	FreeText	"s3://sagemaker-us-east-1-856800247221/pytorch_dog_hpo-2023-07-17-09-22-26-957/source/sourcedir.tar.gz"

- Single instance training with best hyperparameters values

CloudWatch > Log groups > /aws/sagemaker/TrainingJobs

/aws/sagemaker/TrainingJobs

ActionsView in Logs InsightsStart tailingSearch log group

▼ Log group details

ARN
arn:aws:logs:us-east-1:856800247221:log-group:/aws/sagemaker/TrainingJobs:*

Creation time
3 hours ago

Retention
Never expire

Stored bytes
-

Metric filters
0

Subscription filters
0

Contributor Insights rules
-

Data protection
-

Sensitive data count
-

KMS key ID
-

Log streamsMetric filtersSubscription filtersContributor InsightsTagsData protection

Log streams (7)

dog-pytorch-2023-07-17-10-10-25-3891 matchExact matchShow expiredInfo

Log stream▼Last event time▼

dog-pytorch-2023-07-17-10-25-389/algo-1-16895886952023-07-17 17:29:28 (UTC+07:00)

- Multi-instance training with best hyperparameters values (4 instances)

CloudWatch > Log groups > /aws/sagemaker/TrainingJobs

/aws/sagemaker/TrainingJobs

ActionsView in Logs InsightsStart tailingSearch log group

▼ Log group details

ARN
arn:aws:logs:us-east-1:856800247221:log-group:/aws/sagemaker/TrainingJobs:*

Creation time
3 hours ago

Retention
Never expire

Stored bytes
-

Metric filters
0

Subscription filters
0

Contributor Insights rules
-

Data protection
-

Sensitive data count
-

KMS key ID
-

Log streamsMetric filtersSubscription filtersContributor InsightsTagsData protection

Log streams (7)

dog-pytorch-2023-07-17-10-50-15-6504 matchesExact matchShow expiredInfo

Log stream▼Last event time▼

dog-pytorch-2023-07-17-10-50-15-650/algo-1-16895910932023-07-17 18:09:28 (UTC+07:00)

dog-pytorch-2023-07-17-10-50-15-650/algo-3-16895910932023-07-17 18:09:24 (UTC+07:00)

dog-pytorch-2023-07-17-10-50-15-650/algo-2-16895910932023-07-17 18:09:21 (UTC+07:00)

dog-pytorch-2023-07-17-10-50-15-650/algo-4-16895910932023-07-17 18:09:17 (UTC+07:00)

- Deployment

Amazon SageMaker > Endpoints

Endpoints

Update endpointActionsCreate endpoint

Search endpoints

< 1 >

Name▼ARNCreation time▼Status▼Last updated

pytorch-inference-2023-07-17-11-56-14-371arn:aws:sagemaker:us-east-1:856800247221:endpoint/pytorch-inference-2023-07-17-11-56-14-3717/17/2023, 6:56:15 PMInService7/17/2023, 6:58:34 PM

Step 2: EC2 Training

I chose AMI with "Deep Learning AMI GPU PyTorch 1.13.1" and instance type selected was t2.xlarge because it is low cost and sufficient to train model.

4 / 11

Instances (1) [Info](#)

Find instance by attribute or tag (case-sensitive)

Instance ID = i-008b846a83d2b323d [Clear filters](#)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP	IPv6 IPs	Monitoring
<input type="checkbox"/>	MLops	i-008b846a83d2b323d	Pending	t2.xlarge	-	No alarms +	us-east-1d	ec2-3-85-27-248.comp...	3.85.27.248	-	-	disabled

If everything works well we are connected to our instance. The last step is activate pytorch virtual enviroment on terminal by typing:

```
source activate pytorch
```

and train model as usually

```

AWS Deep Learning AMI GPU PyTorch 1.13.1 (Amazon Linux 2)

* Please note that Amazon EC2 F2 Instance is not supported on current DLAMI.
* Supported EC2 instances: G3, F3, F3dn, F4d, G5, G5dn.
* To activate pre-built pytorch environment, run: 'source activate pytorch'
* To activate base conda environment upon login, run: 'conda config --set auto_activate_base true'
* NVIDIA driver version: 525.65.12
* CUDA version: 11.7

AWS Deep Learning AMI Homepage: https://aws.amazon.com/machine-learning/amis/
Release Notes: https://docs.aws.amazon.com/dlami/latest/dg/deguide/appendix-ami-release-notes.html
Support: https://forums.aws.amazon.com/forum.jspa?forumID=263
For a fully managed experience, check out Amazon SageMaker at https://aws.amazon.com/sagemaker
Security scan reports for python packages are located at: /opt/aws/dlami/info/

28 package(s) needed for security, out of 52 available
Run "sudo yum update" to apply all updates.
[root@ip-172-31-26-56 ~]# ls
dogImages dogImages.zip solution.py TrainedModels
[root@ip-172-31-26-56 ~]# source activate pytorch
bash: activate: No such file or directory
[root@ip-172-31-26-56 ~]# source activate pytorch
ERROR: Please note that the Amazon EC2 t2.xlarge instance type is not supported by current Deep Learning AMI.
Please try one of the supported EC2 instances: G3, F3, F3dn, F4d, G5, G5dn.
Please refer the DLAMI release notes https://aws.amazon.com/releases/notes/aws-deep-learning-ami-gpu-pytorch-1-13-1-aws-linux-2/ for more information.
(pytorch) python solution.py
WARNING: /opt/conda/envs/pytorch/lib/python3.9/site-packages/torchvision/models/_utils.py:208: UserWarning: The parameter 'pretrained' is deprecated since 0.13 and may be removed in the future, please use 'weights' instead.
  warnings.warn(
/opt/conda/envs/pytorch/lib/python3.9/site-packages/torchvision/models/_utils.py:223: UserWarning: Arguments other than a weight enum or 'None' for 'weights' are deprecated since 0.13 and may be removed in the future. The current behavior
is equivalent to passing 'weights=ResNet50_Weights.IMAGENET1K_V1'. You can also use 'weights=ResNet50_Weights.DEFAULT' to get the most up-to-date weights.
  warnings.warn(msg)
Downloading: "https://download.pytorch.org/models/resnet50-0676ba61.pth" to /root/.cache/torch/hub/checkpoints/resnet50-0676ba61.pth
100%
Starting Model Training
sawed
(pytorch) ls
dogImages dogImages.zip solution.py TrainedModels
(pytorch) ls TrainedModels/
model.pth
(pytorch)

```

Step 3: Lambda function setup

After training and deploying your model, setting up a Lambda function is an important next step. Lambda functions enable your model and its inferences to be accessed by API's and other programs, so it's a crucial part of production deployment.

Step 4: Lambda security setup and testing

Adding endpoints permission to lambda fucntions Lambda function is going to invoke deployed endpoint. Therefore, we should search for SageMaker and select an appropriate policy. While the full access option may be the simplest choice (as below).

[Permissions](#)
[Trust relationships](#)
[Tags](#)
[Access Advisor](#)
[Revoke sessions](#)

Permissions policies (2) [Info](#)

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

<
1
>

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AWSLambdaBasicExecutionRole-1d9e5a62-feb5-45...	Customer managed	
<input type="checkbox"/>	AmazonSageMakerFullAccess	AWS managed	Provides full access to Amazon S...

Vulnerability Assessment:

Granting "Full Access" has the potential to be exploited by malicious actors. Roles that are old and inactive pose a risk of compromising the lambda function, and it is essential to delete such roles. Additionally, roles with policies that are no longer in use may lead to unauthorized access, making it crucial to remove these policies.

I also create policy with permission to only invoke specific endpoint. Two security policy has been attached to the role :

1. Basic Lambda function execution
2. Sagemaker endpoint invocation permission

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": "sagemaker:InvokeEndpoint",
      "Resource": "arn:aws:sagemaker:us-east-1:856800247221:endpoint/pytorch-inference-2023-07-17-11-56-14-371"
    }
  ]
}
```

I got the results after running the test with json:

Code
Test
Monitor
Configuration
Aliases
Versions

Code source
Info

Upload from

File
Edit
Find
View
Go
Tools
Window
Test
Deploy

Go to Anything (Ctrl-P)

lambda_function
Environment Var
Execution result

Environment
inference
lambda_function.py

Execution results

Test Event Name
Test

Response

```

{
  "statusCode": 200,
  "headers": {
    "Content-Type": "text/plain",
    "Access-Control-Allow-Origin": ""
  },
  "type-result": "<class 'str>",
  "Content-Type-In": "<_main_.LambdaContext object at 0x7fce162d9c70",
  "body": "[[([0.11569850146770477, 0.07335714258802994, -0.004642227198928595, 0.05507751926779747, 0.2541041970252991, 0.14660333096981049, -0.08659107983112335, 0.12284155189990997, -0.27110689878463745, -0.00010000000000000002])]]"
```

Function Logs

```

START RequestId: eee2a880-818a-4778-a597-aebc4dda6bb9 Version: $LATEST
Context::: <_main_.LambdaContext object at 0x7fce162d9c70>
EventType:: <class 'dict'>
END RequestId: eee2a880-818a-4778-a597-aebc4dda6bb9
REPORT RequestId: eee2a880-818a-4778-a597-aebc4dda6bb9 Duration: 1149.47 ms Billed Duration: 1150 ms Memory Size: 128 MB Max Memory Used: 79 MB
```

Request ID
eee2a880-818a-4778-a597-aebc4dda6bb9

Status: Succeeded
Max memory used: 79 MB
Time: 1149.47 ms

```
{
  "statusCode": 200,
  "headers": {
    "Content-Type": "text/plain",
    "Access-Control-Allow-Origin": "*"
  },
  "type-result": "<class 'str'>",
  "Content-Type-In": "<__main__.LambdaContext object at 0x7f9f7186eb50>",
  "body": "[[0.11569850146770477, 0.07335714250802994, -0.004642227198928595,
0.05507751926779747, 0.2541041970252991, 0.14660333096981049,
-0.08659107983112335, 0.12284155189990997, -0.27110689878463745,
-0.05761592835187912, 0.1601676344871521, 0.13573479652404785,
-0.04377829283475876, 0.17616261541843414, 0.20801971852779388,
0.07003931701183319, 0.006634952500462532, -0.05516386032104492,
```



```
-0.008051948621869087, 0.09924852848052979, 0.06310422718524933,
-0.09785448759794235, 0.1348874866962433, 0.10004594177007675,
-0.15410198271274567, -0.1506362110376358, 0.13724784553050995,
-0.2381516396999359, 0.21443870663642883, -0.022219419479370117,
0.022774580866098404, 0.1424022763967514, -0.09266003966331482,
0.15716803073883057, -0.005540584214031696, 0.07141581177711487,
0.02648269385099411, 0.029948465526103973, 0.14251919090747833,
0.0003836420364677906, 0.18289466202259064, 0.09956419467926025,
-0.016542645171284676, 0.12330365180969238, -0.06826964765787125,
0.10950853675603867, 0.00013788638170808554, 0.0727255791425705,
-0.058358386158943176, 0.003316437127068639, 0.10138405114412308,
-0.07430241256952286, -0.10718905180692673, 0.07025771588087082,
0.026771383360028267, 0.12740181386470795, 0.1721392124891281,
-0.007699458859860897, -0.02812434732913971, 0.1198265552520752,
0.10443335026502609, 0.02795330062508583, 0.003968058619648218,
-0.13816413283348083, -0.10980987548828125, -0.2712988257408142,
-0.2463635802268982, 0.06604889035224915, -0.05209902673959732,
-0.07528180629014969, 0.13434217870235443, -0.027880359441041946,
-0.04343372583389282, -0.09682810306549072, -0.060933806002140045,
0.11835910379886627, -0.14867043495178223, -0.12432146817445755,
0.05317588150501251, -0.030270373448729515, 0.08195175230503082,
0.10219918936491013, -0.1233593076467514, -0.03832899406552315,
-0.16496337950229645, -0.04051525145769119, 0.12668175995349884,
-0.048126108944416046, 0.012375004589557648, 0.05743524804711342,
-0.016821622848510742, -0.05881795659661293, -0.21024014055728912,
-0.09414805471897125, -0.01778138428926468, -0.13120634853839874,
0.018554866313934326, -0.022576672956347466, -0.10938028991222382,
-0.2355252504348755, -0.018498489633202553, -0.344592422246933,
0.0326075553894043, -0.13647782802581787, -0.24241623282432556,
0.012452196329832077, -0.0677172988653183, -0.3188721537590027,
-0.12630920112133026, -0.20892879366874695, -0.04780663922429085,
0.005423912778496742, -0.12631963193416595, -0.21945923566818237,
0.1325729638338089, -0.3307647705078125, -0.011895101517438889,
0.01852065697312355, -0.30218175053596497, -0.15051314234733582,
-0.36914318799972534, -0.23682250082492828, -0.10944990813732147,
-0.04332536458969116, -0.22717122733592987, -0.33725765347480774,
-0.16539357602596283, -0.2591378092765808, -0.08885806053876877,
-0.07989415526390076, -0.3424559235572815, -0.34604254364967346,
-0.2824306786060333]]"
```

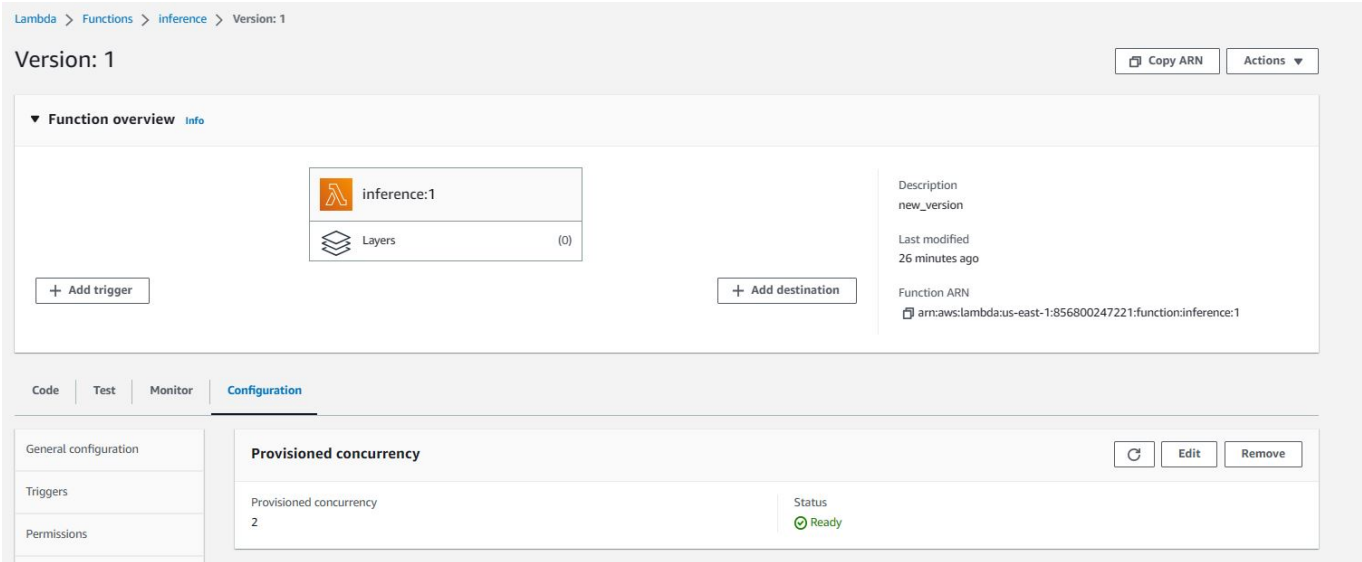
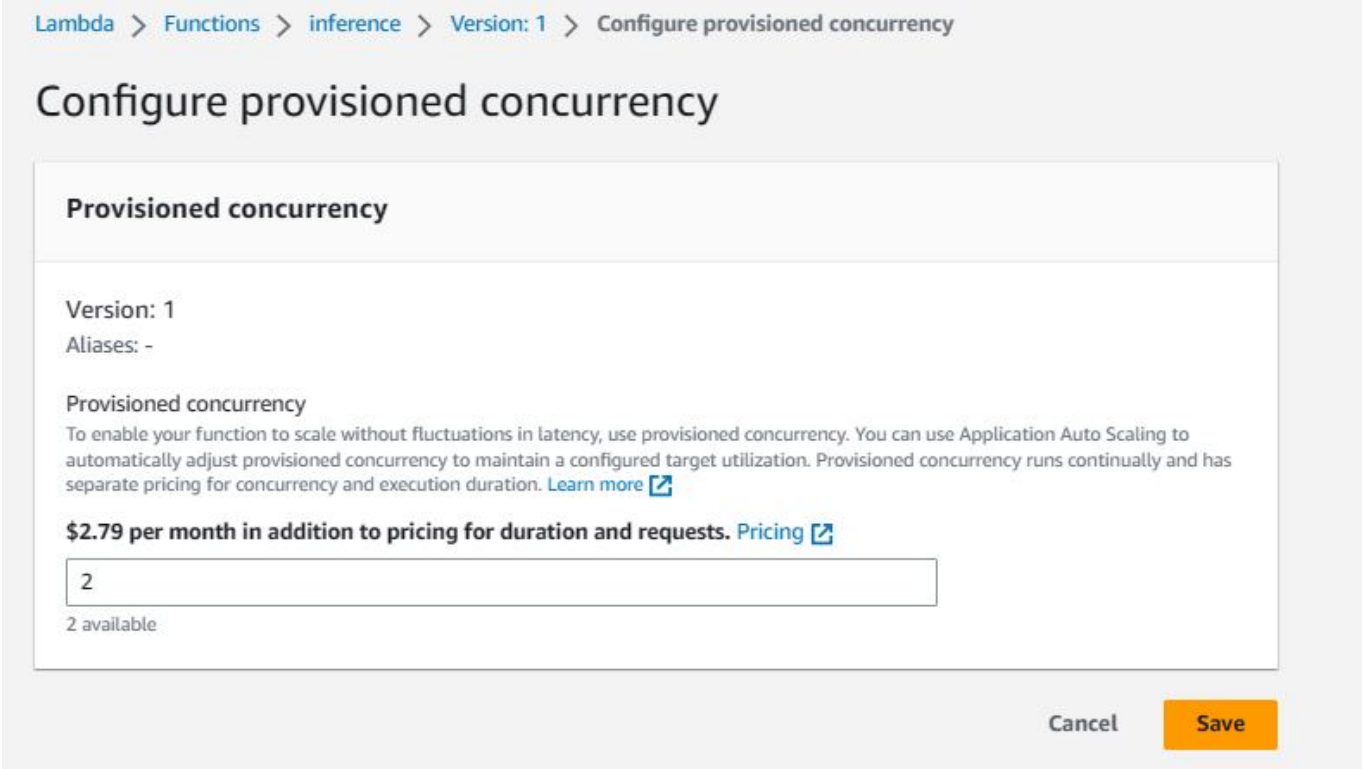
```
}
```

Step 5: Concurrency and auto-scaling

By default a Lambda Function can only respond one request at once. One way to change that is to use concurrency so that the Lambda Function can be responds to multiple requests at once.

To set up concurrency on your Lambda function, you will need to open your Lambda function in the Lambda section of AWS. Next, you should open the Configuration tab. Then, you should configure a Version for your function, in the Version section of the Configuration tab.

After configuring a Version for your Lambda function, navigate to the Concurrency section of the Configuration tab of your function. Use this section to configure concurrency for your Lambda function.



In addition to setting up concurrency for your Lambda function, you should also set up auto-scaling for your deployed endpoint.

Variant automatic scaling [Learn more](#)

Variant name
AllTraffic

Instance type
ml.m5.large

Elastic Inference
-

Current instance count
1

Current weight
1

Minimum instance count
1

-

Maximum instance count
3

IAM role
Amazon SageMaker uses the following service-linked role for automatic scaling. [Learn more](#)

AWSServiceRoleForApplicationAutoScaling_SageMaker
Endpoint

Built-in scaling policy [Learn more](#)

Policy name
SageMakerEndpointInvocationScalingPolicy

Target metric
[SageMakerVariantInvocationsPerInstance](#)

Target value
20

Scale in cool down (seconds)
- optional
30

Scale out cool down (seconds)
- optional
30

☐ Disable scale in

Select if you don't want automatic scaling to delete instances when traffic decreases. [Learn more](#)

Endpoint runtime settings										Update weights	Update instance count	Configure auto scaling
	Variant name	Current weight	Desired weight	Elastic Inference	Instance type	Current instance count	Desired instance count	Instance min - max	Automatic scaling			
<input type="radio"/>	AllTraffic	1	1	-	ml.m5.large	1	1	1 - 3	Yes			

Endpoint configuration settings

[Change](#)[Clone](#)

Endpoint configuration

Name pytorch-inference-2023-07-17-11-56-14-371	ARN arn:aws:sagemaker:us-east-1:856800247221:endpoint-config/pytorch-inference-2023-07-17-11-56-14-371	Encryption key -	Creation time 7/17/2023, 6:56:14 PM
---	---	---------------------	--

Data capture

