

Create basic stack

The basic stack is :

- A Dynamodb table
- Insert data into the table
- Create a VPC and a subnet to get Internet access
- Pull the Kong AMI and starts it

Prerequisites

In order to deploy the stack you need :

- awscli (for windows only)
- terraform
- the aws access keys (received by email amongst your AWS console's credentials)

You may receive an email with a wrong name. Ignore the incorrect information. It is a known issue.
You can safely use the credentials from the email.

- Accept the EULA <https://aws.amazon.com/marketplace/pp/B06WP4TNKL> of Kong appliance while connected to AWS Console. (**Needed** otherwise terraform won't be able to pull the AMI). **Click Continue to Subscribe**

 **Kong**
By: [Kong Inc.](#) Latest Version: 0.14.1
Kong was created to secure, manage and extend Microservices & APIs. Kong is powered by the battle-tested tech of NGINX with a focus on scalability, high performance & reliability.
[Show more](#)

[Continue to Subscribe](#)
[Save to List](#)
Typical Total Price
\$1.680/hr

- And then **Accept Terms**

Subscribe to this software

To create a subscription, review the pricing information and accept the terms for this software.

Terms and Conditions

Kong Inc. Offer

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the [AWS Customer Agreement](#)

[Accept Terms](#)

- Generate a **MapQuest** API token :
 - Go to <https://developer.mapquest.com/>
 - Click “Get your Free API key”
 - Fill the Form
 - Once you’ve received the email, log in with your account
 - Go to <https://developer.mapquest.com/user/me/profile>
 - Select “Manage Key” in the left menu
 - And generate a new key by clicking the “Create a new Key” button

macOs & Linux

Terraform

1. Download and install [Terraform](#) appropriate package for your OS
 - [Linux](#)
 - [macOS](#)
2. Copy files from the downloaded zip to ~/terraform (Create terraform folder).
3. Open a terminal Window and set the PATH to use terraform binary :
`export PATH=$PATH:$HOME/terraform`

Environment variables

- Open a terminal window and replace the values with the ones from the email.

```
$ export AWS_ACCESS_KEY_ID="YOURaccesskey"  
$ export AWS_SECRET_ACCESS_KEY="YOURsecretkey"  
$ export AWS_DEFAULT_REGION="eu-west-2"
```

Deploy the stack

- Once all the prerequisites have been met run from a terminal window:

```
$ cd ~/terraform  
$ curl -s -LO https://github.com/tr00mb/api-kong-lambda-christmas/archive/master.zip  
$ unzip master.zip  
$ cd api-kong-lambda-christmas-master/tf
```

- Then execute

```
$ terraform init  
$ terraform apply -auto-approve
```

Windows

awscli

1. You first need to install awscli
 - [64-bit](#)
 - [32-bit](#)
2. Run the downloaded MSI installer or the setup file.
3. Follow the on-screen instructions

Terraform

1. Download and install [Terraform](#) Windows appropriate package.
[32-bit](#)
[64-bit](#)
2. Copy files from the downloaded zip to C:\terraform (Create terraform folder).
3. Open the command prompt as an administrator and set the PATH to use terraform binaries :

```
set PATH=%PATH%;C:\terraform
```

Environment variables

Open a command prompt window and replace the value with the ones in the email.
(start -> run -> cmd)

```
set AWS_ACCESS_KEY_ID="anaccesskey"  
set AWS_SECRET_ACCESS_KEY="asecretkey"  
set AWS_DEFAULT_REGION="eu-west-3"
```

Deploy the stack

- Download using your favourite web browser the link below and copy the file to
C:\terraform
<https://github.com/tr00mb/api-kong-lambda-christmas/archive/master.zip>
- Extract

From a console prompt:

```
C:\> cd C:\terraform\api-kong-lambda-christmas-master\tf
```

- Then execute

```
C:\terraform> terraform init  
C:\terraform> terraform apply -auto-approve
```

After the command ran the stack is ready to be used.

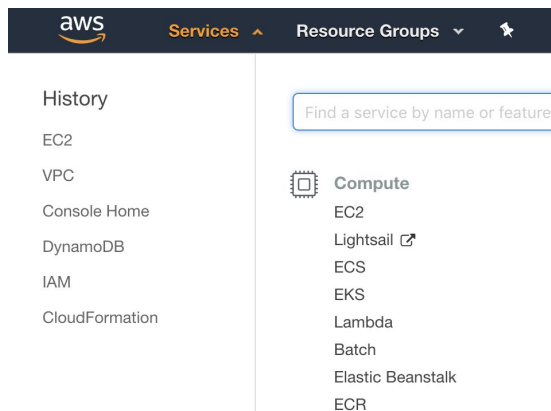
The public IP address of the Kong instance is displayed as well as the S3 bucket id. You will need both afterwards. You also need the url of the website.

```
Outputs:

ec2_global_ips = [
    52.47.199.154
]
s3_arn = [
    arn:aws:s3:::kong-bucket-40bb71317b15840dbb535627
]
s3_bucket_id = [
    kong-bucket-40bb71317b15840dbb535627
]
s3_website_url = [
    kong-bucket-40bb71317b15840dbb535627.s3-website.eu-west-3.amazonaws.com
]
```

You can check the instance public IP value directly from the AWS Console:

- To do so you need to click on **Services > EC2**



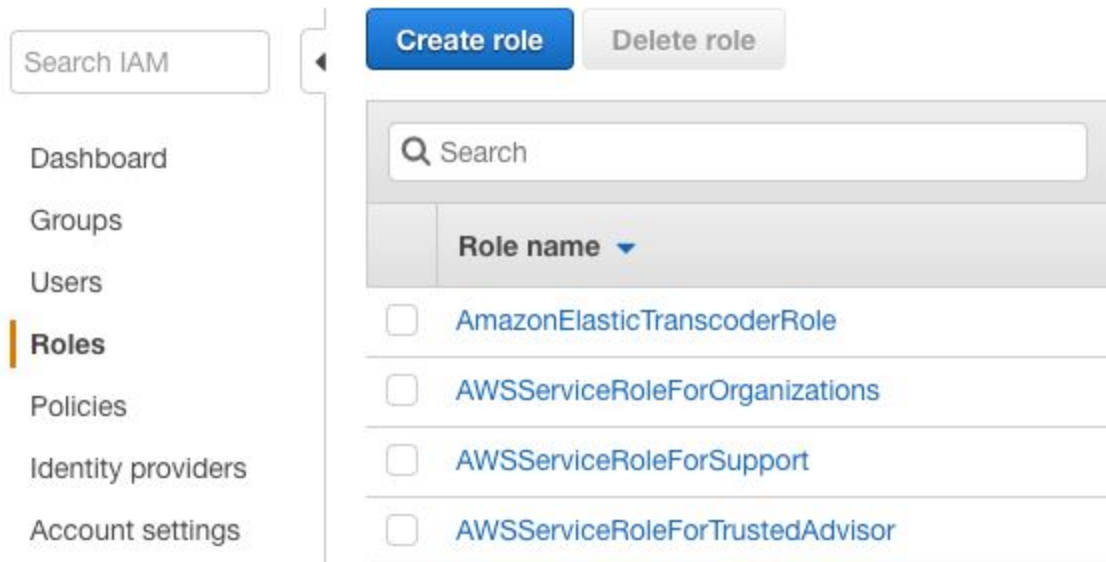
- Then from the **EC2 Dashboard** click on *Instances* to list all the instances in the account
- On the main panel the instances will show up and then you can easily find out the public IP of the instance

Status Checks ▾	Alarm Status	Public DNS (IPv4) ▾	IPv4 Public IP
✓ 2/2 checks ...	None		52.47.154.206

Create IAM roles for Lambda functions

We need to create an IAM role for our future Lambda functions. This role will allow functions to interact with DynamoDB and the S3 bucket.





- In the AWS console's Services tab, click IAM under Security, Identity & Compliance, and then click Roles from the left navigation menu.
- Click Create Role



- In the Trust step, choose AWS Service and Lambda, and then click Next: Permissions

Create role 1 2 3 4

Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web Identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
--	---	---	--

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

- In the Permissions step, search for and check the boxes next to:
 - AWSLambdaExecute
 - AmazonS3ReadOnlyAccess
 - AmazonDynamoDBReadOnlyAccess

Create role



▼ Attach permissions policies

Choose one or more policies to attach to your new role.


Create policy

↺

Filter policies ▼

Q Execute

Showing 1 result

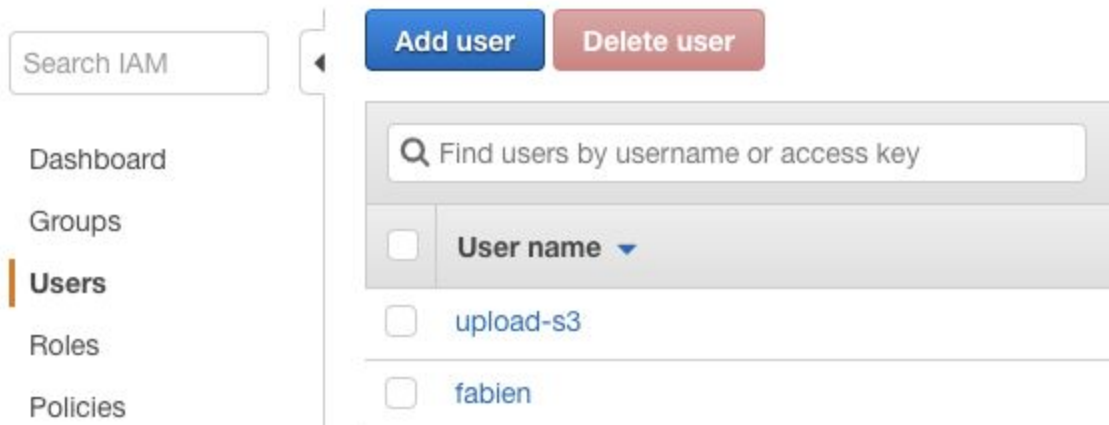
	Policy name ▼	Used as	Description
<input checked="" type="checkbox"/>	 AWSLambdaExecute	Permissions policy (1)	Provides Put, Get access to S3 and full a...

Note: Make sure the names you select match exactly what is shown here.

- Click Next: Review to attach both policies to the role.
- In the Review step, name the role **lambda-dynamo-execution-role**, and then click Create role to save.

Create user for Kong to execute Lambda

- In the AWS console's Services tab, click IAM under Security, Identity & Compliance, and then click Roles from the left navigation menu.
- Click Create User



- Next, set the user name and select as access type **only** Programmatic access as shown below

Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+ Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type* ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☐ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.


Then, we need to attach the permissions for this user


- Select **Attach existing policies directly**
- And select AWSLambdaFullAccess
- Click **Next** and then **Create user**


Add user

1 2 3 4 5


▼ Set permissions

 Add user to group


 Copy permissions from existing user

 Attach existing policies directly

Create policy




Filter policies ▼ Showing 1 result


	Policy name ▼	Type	Used as	Description
<input checked="" type="checkbox"/>	 AWSLambdaFullAc...	AWS managed	None	Provides full access to Lambda, S3, Dynam...


You should see a Success message

- Download the .csv file and save it somewhere safe. You will need it later.

 **Success**
You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://carre-d2si.signin.aws.amazon.com/console>

 Download .csv

	User	Access key ID	Secret access key
▶ 	apiday-kong	AKIAJ5XHCJHNZD5BFMFQ	***** Show