Secure Starter Kit Cloud Connect Quick Start Guide

Date: June 15, 2021 | Version 1.2

CONTENTS

1 INTRODUCTION

1.1 Purpose of the Document

The Cloud Connect Quick Start Guide provides an overview of How to Provision/Create and configure EC2 instance, RDS, S3 buckets and IAM User. This AWS services required to run the demo's provided in the Security Starter Quick Start Guides, as well as detailed instructions to setup and configure those required services. Each of these services MUST be setup and configured (only once), prior to running the demo's outlined in the Security Starter Quick Start Guides.

1.2 AWS Cloud Services Descriptions and its background information

For AWS Cloud Services descriptions and its background information, follow the SSK_Cloud_Connect Installation Setup Guide

2 AWS ACCOUNT CREATION

2.1 Login or Create your AWS Account

Note: If the User does not have an AWS Account, you will need to create one. This is used as the basis for the configuration of the other services required to run the demo's provided in the Security Starter Kits.

Login URL: https://aws.amazon.com/console/

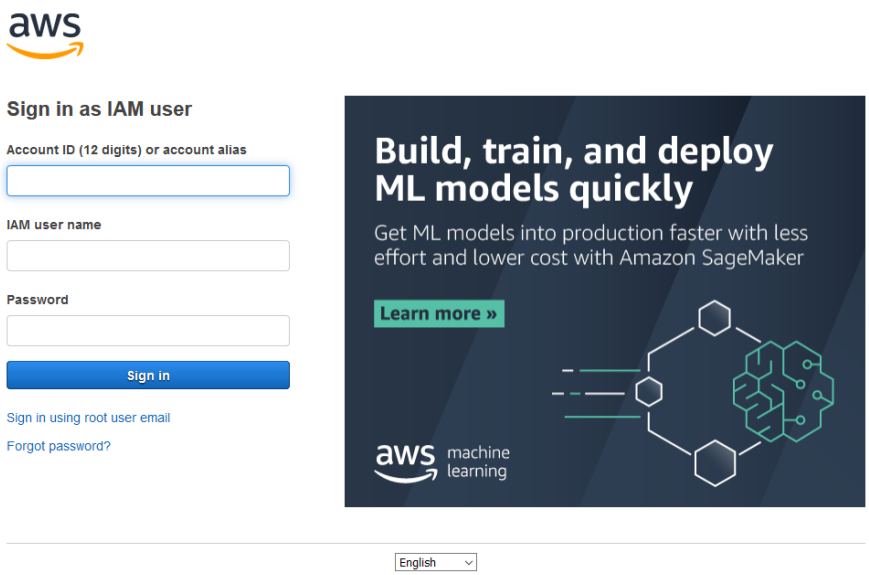


Figure 1: Login page

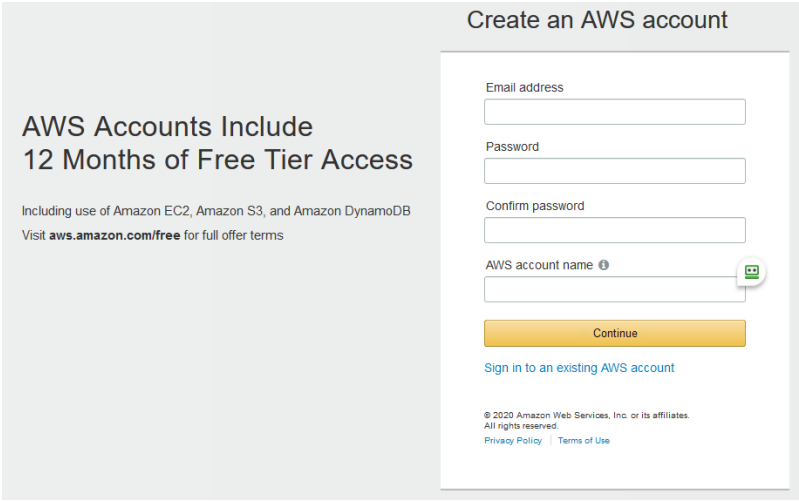


Figure 2: Create New Account page

2.2 Create New Key Pair to enable SSH access to the EC2 instance

1. Please choose **AWS Console** >> **Services** >> Select **EC2** (Under Compute section) >> **Network & Security** >> **Select Key Pairs**
2. Click on "**Create key pair**" as shown in below image

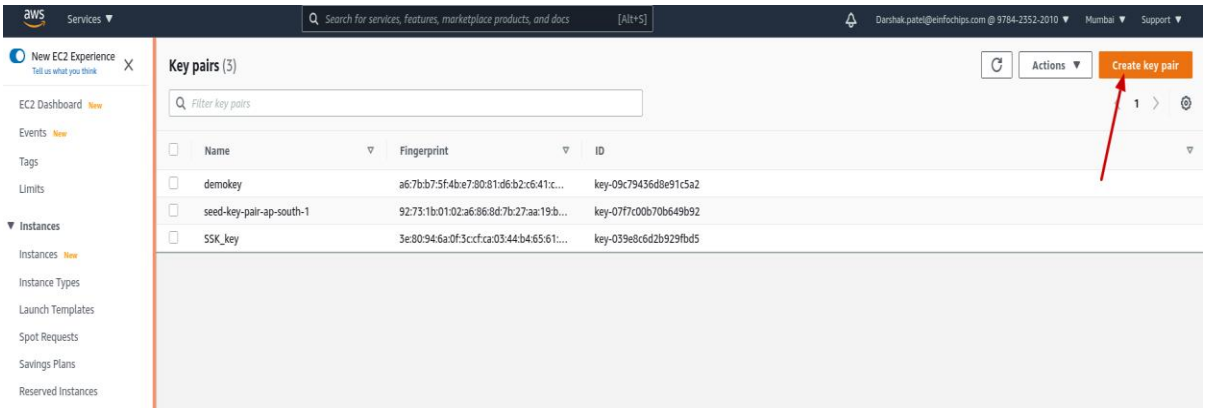


Figure 1: Create Key Pair page

3. Follow the below instructions as depicted in screenshot:
   - Enter a Name for the key pair
   - Select appropriate file format (**.pem** for Linux users and **.ppk** for Windows user) to download private key
   - Add tags (Optional)
   - Click on Create key pair

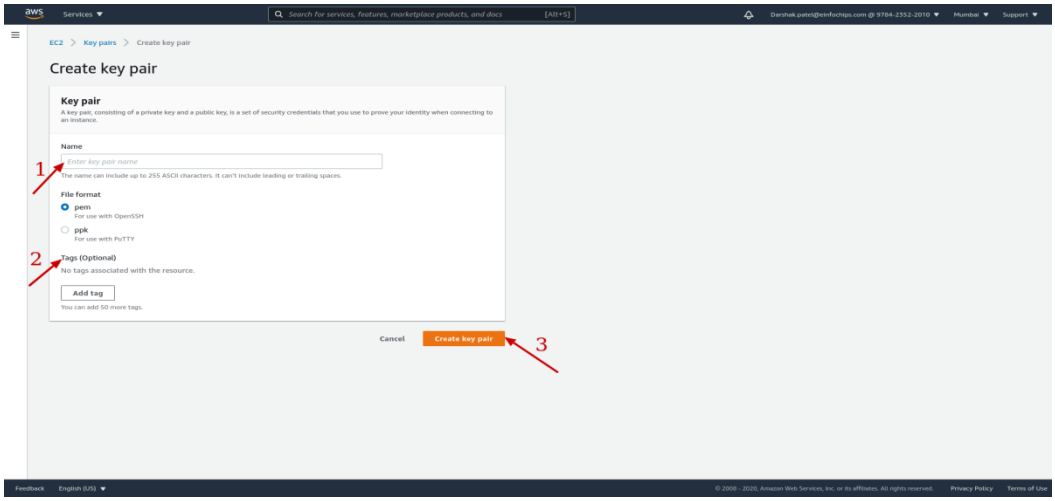


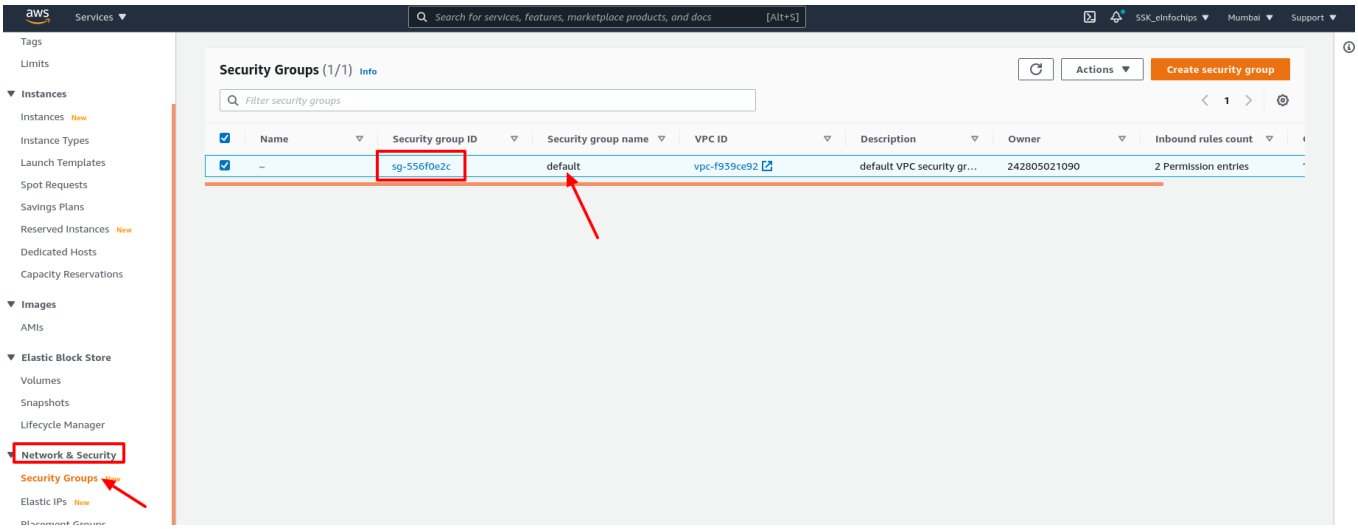
Figure 2: Creating Key Pair page

   - It will Download key pair as per the file format you have selected (To Connect EC2 Instance)

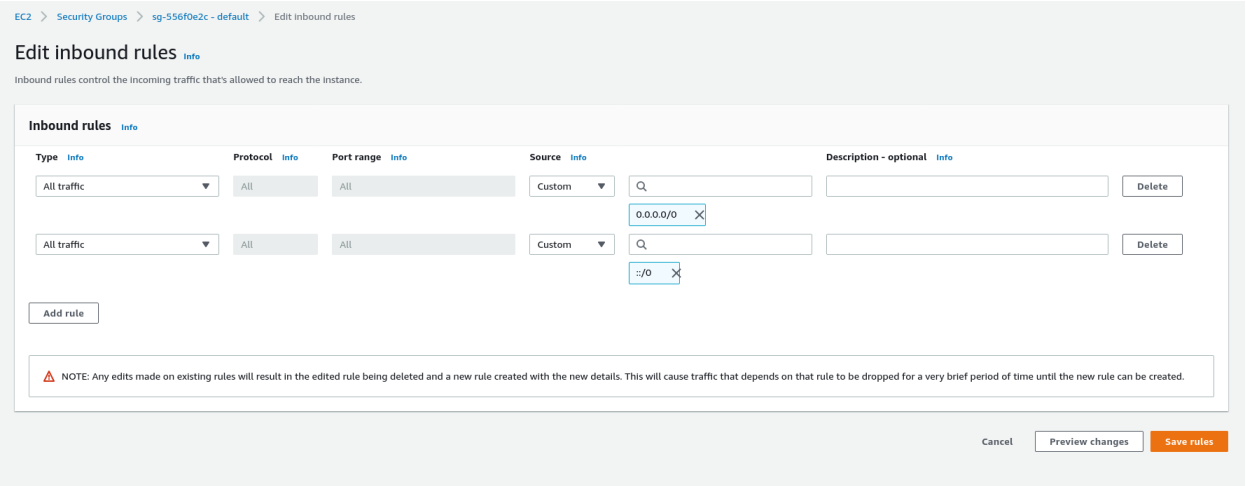
Note: Keep key file at secure place, which will be used to connect Ec2 instance.

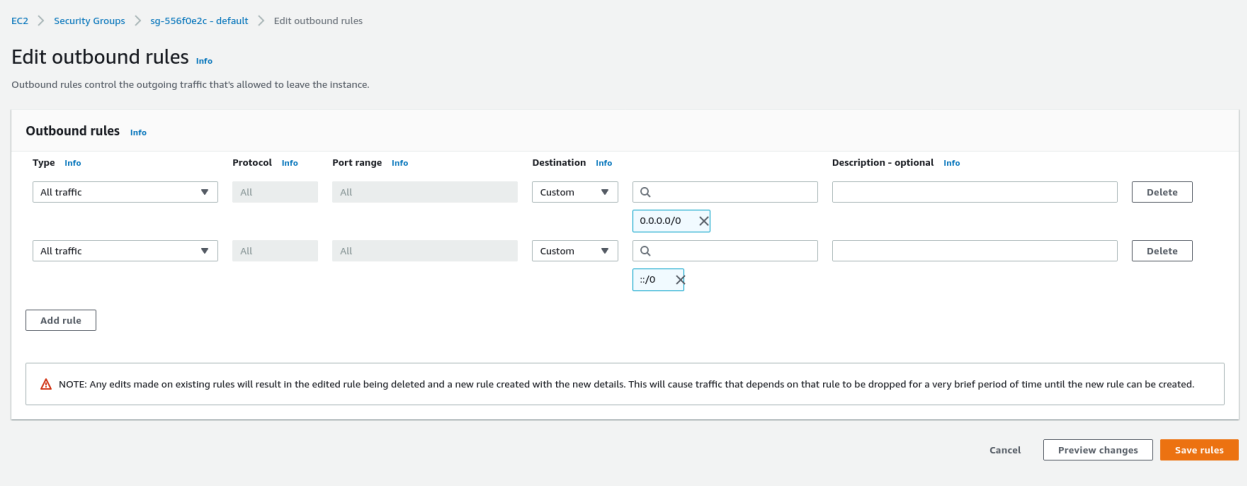
2.3 Check Security group rules of Default Security Group

1. Click on https://console.aws.amazon.com/ec2/.
   a) From the left side menu, under the **Network & Security**, select **Security Groups**.
   b) Click on the Group ID (ID can be different) of **default** security group as shown in below image.



2. Ensure the below Security group rules are set for Inbound as well as for Outbound for default security group. If is not there then please update rules as per the below images.




EC2 > Security Groups > sg-556f0e2c - default > Edit outbound rules
Edit outbound rules Info
Outbound rules control the outgoing traffic that's allowed to leave the instance.
Outbound rules Info
Type Info
Protocol Info
Port range Info
Destination Info
Description - optional Info
All traffic
All
All
Custom
0.0.0.0/0
Delete
All traffic
All
All
Custom
::/0
Delete
Add rule
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.
Cancel
Preview changes
Save rules

3 CLOUDFORMATION CODE EXECUTION

1. Go to the AWS console and search for the S3 services and click on it to launch as shown in the below image:

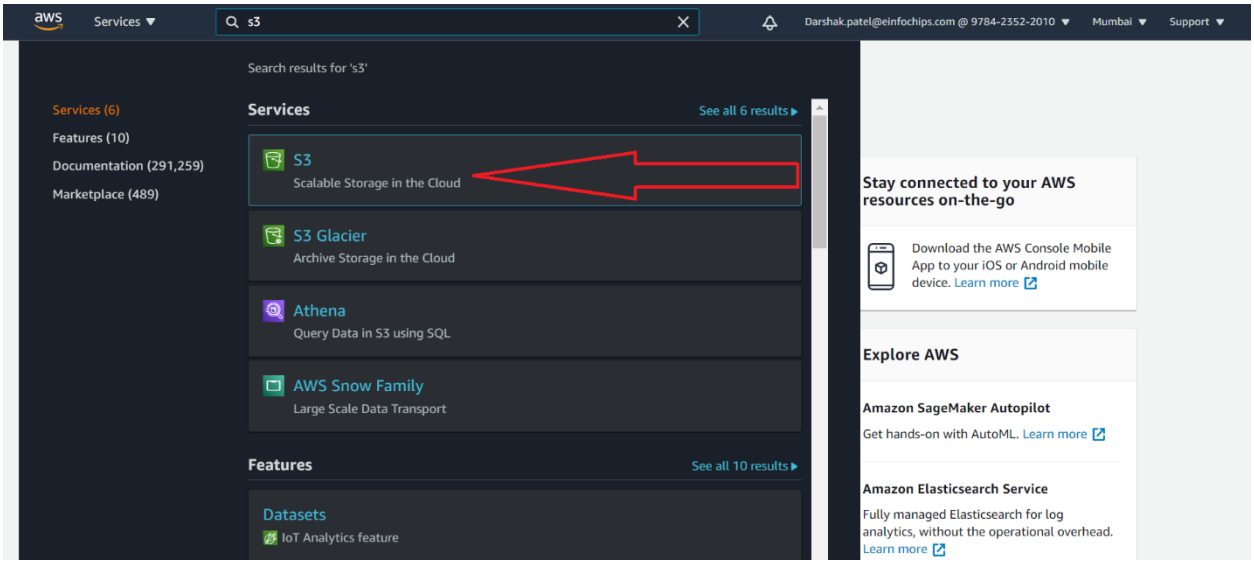


Figure 1: Searching for S3 service in Home Page

2. Click on create bucket as shown in figure below:

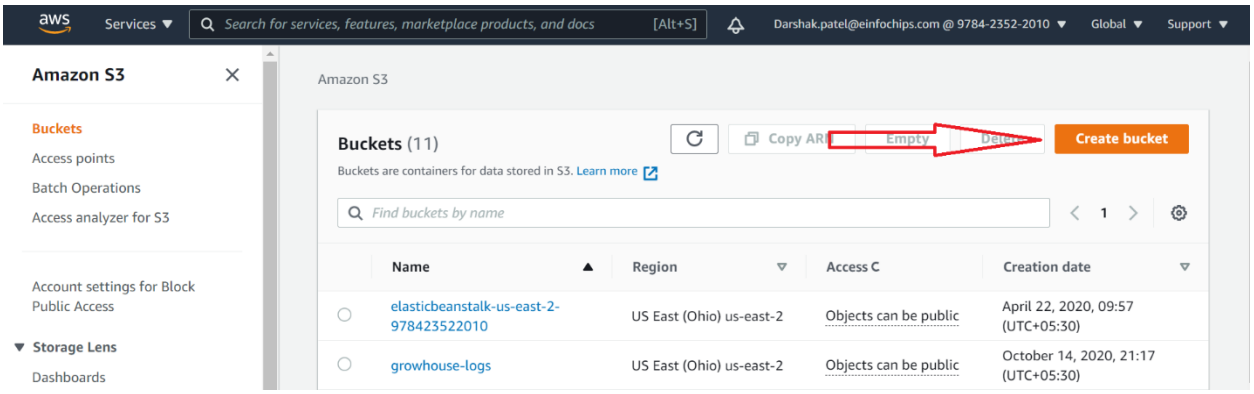


Figure 2: Create bucket

3. Enter unique bucket name after create bucket page is launched as shown below and then click on create bucket option provided at the end of the page. This will create your S3 bucket with the unique

name you provided.

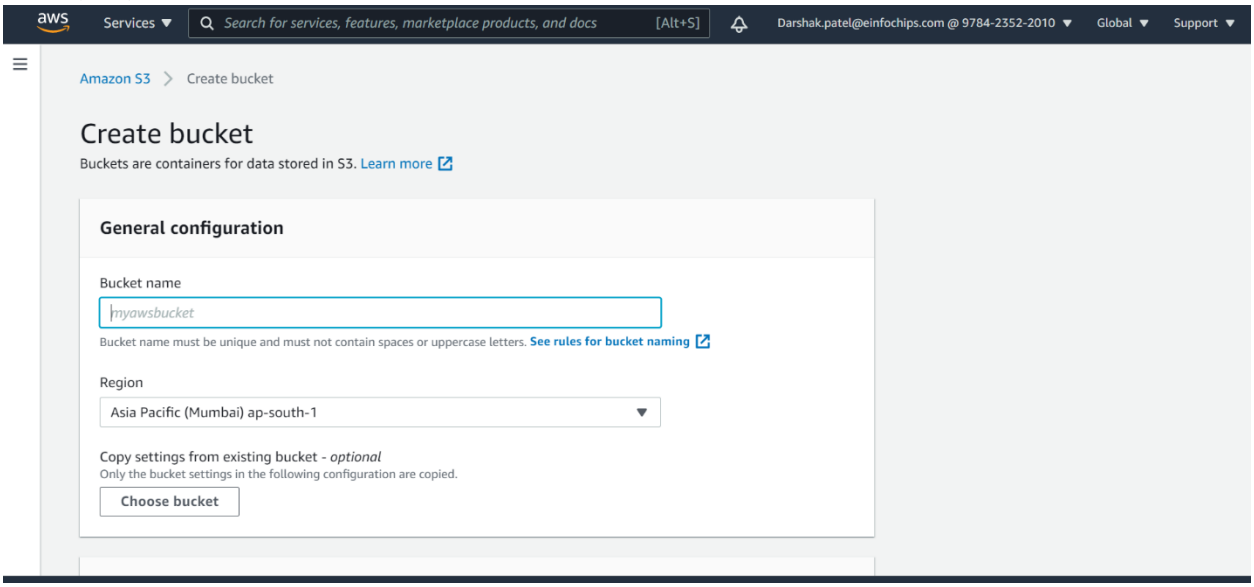
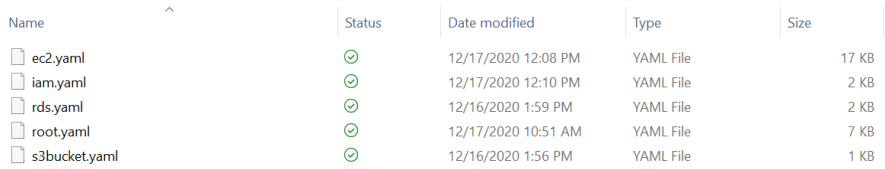


Figure 3: Creating S3 bucket

4. After creating bucket successfully, download the provided SSK_Database.zip from the Cloud-Connect-Tool branch on GitHub to upload files to the newly created S3 bucket.
5. Unzip the **SSK_Database.zip** and you will find below contents:



Name	Status	Date modified	Type	Size
ec2.yaml	✓	12/17/2020 12:08 PM	YAML File	17 KB
iam.yaml	✓	12/17/2020 12:10 PM	YAML File	2 KB
rds.yaml	✓	12/16/2020 1:59 PM	YAML File	2 KB
root.yaml	✓	12/17/2020 10:51 AM	YAML File	7 KB
s3bucket.yaml	✓	12/16/2020 1:56 PM	YAML File	1 KB

Figure 4: Extracting Contents of SSK_Database.zip

6. Open the newly created S3 Bucket and choose “upload” option as shown below:

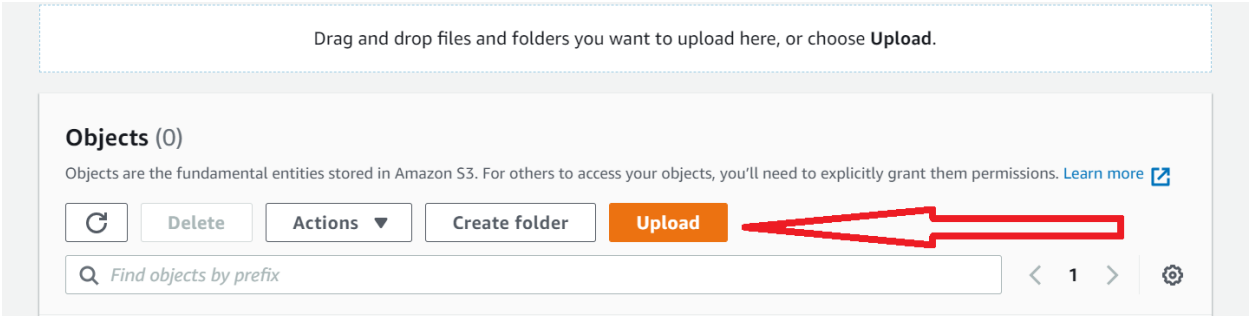


Figure 5: To upload files in S3 bucket

7. Choose the “Add files“ option provided in your S3 bucket and select all files from provided folder “SSK_Database”, then click on “upload” and this will upload files like shown below:

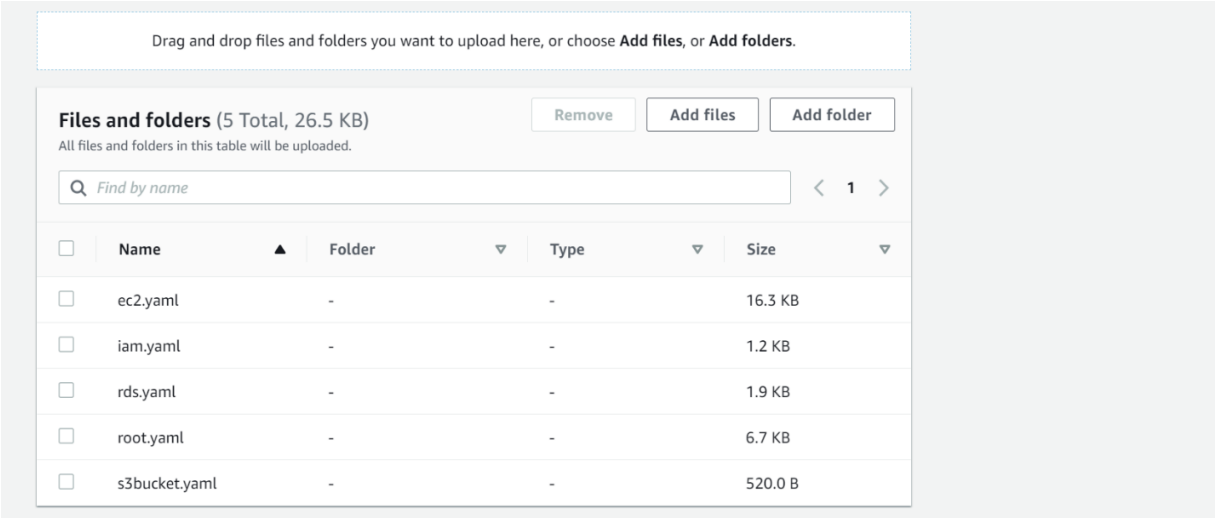


Figure 6: Uploading files in S3 bucket

8. Select each of the uploaded “.yaml” files as depicted below and copy the object URLs; you will need these to modify the “root.yaml” with your new s3-bucket name.

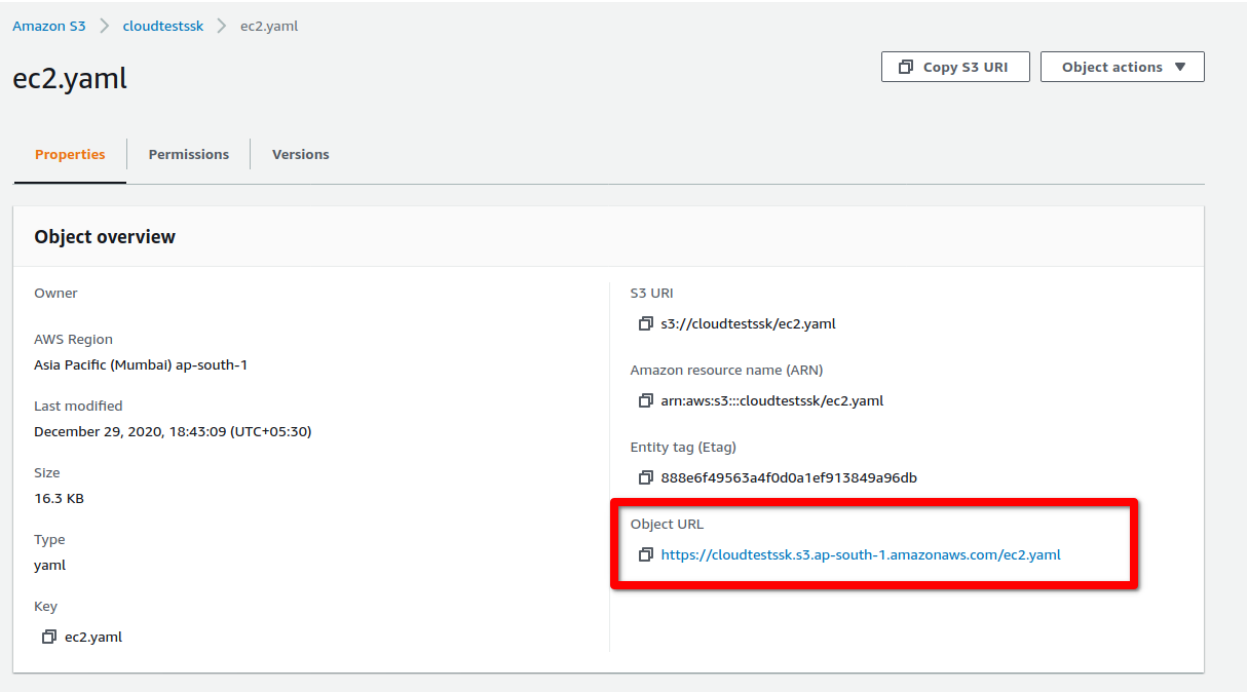


Figure 7: copying object URL

9. Please update the root.yaml file using a text editor with the copied Object URLs from above steps.

```
127     Type: AWS::CloudFormation::Stack
128     Properties:
129       TemplateURL: "https://cloudtestssk.s3.ap-south-1.amazonaws.com/rds.yaml"
130       Parameters:
131         DBInstanceID: !Ref DBInstanceID
132         DBName: !Ref DBName
133         DBInstanceClass: !Ref DBInstanceClass
134         DBAllocatedStorage: !Ref DBAllocatedStorage
135         DBUsername: !Ref DBUsername
136         DBPassword: !Ref DBPassword
137         ProjectName: !Ref ProjectName
138
139   # Create webserver (Ec2 instance)
140   ServerStack:
141     Type: AWS::CloudFormation::Stack
142     DependsOn: ['DatabaseStack', 'IAMStack']
143     Properties:
144       TemplateURL: "https://cloudtestssk.s3.ap-south-1.amazonaws.com/ec2.yaml"
145       Parameters:
146         AWSIOTCoreEndpoint: !Ref AWSIOTCoreEndpoint
147         InstanceType: !Ref InstanceType
148         KeyName: !Ref KeyName
149         SSHLocation: !Ref SSHLocation
150         DBUsername: !GetAtt DatabaseStack.Outputs.DBUserName
151         DBPassword: !GetAtt DatabaseStack.Outputs.DBPassword
152         DBName: !GetAtt DatabaseStack.Outputs.DBName
153         DBHost: !GetAtt DatabaseStack.Outputs.DBEndpointAddress
154         IAMUserID:  !GetAtt IAMStack.Outputs.UserID
155         IAMUserName: !Ref IAMUserName
156         IAMAccessKey: !GetAtt IAMStack.Outputs.AccessKey
157         IAMSecretKey: !GetAtt IAMStack.Outputs.SecretKey
158         DockerHubUserName: !Ref DockerHubUserName
159         DockerHubPassword: !Ref DockerHubPassword
160         OTABucketName: !GetAtt S3BucketStack.Outputs.OTABucketName
161         LogBucketName: !GetAtt S3BucketStack.Outputs.LogBucketName
162
163   # Create IAM Group and User
164   IAMStack:
165     Type: AWS::CloudFormation::Stack
166     Properties:
167       TemplateURL: "https://cloudtestssk.s3.ap-south-1.amazonaws.com/iam.yaml"
168       Parameters:
169         IAMUserName: !Ref IAMUserName
170         ProjectName: !Ref ProjectName
171
172   # Create S3 Bucket
173   S3BucketStack:
174     Type: AWS::CloudFormation::Stack
175     Properties:
176       TemplateURL: "https://cloudtestssk.s3.ap-south-1.amazonaws.com/s3bucket.yaml"
177       Parameters:
178         ProjectName: !Ref ProjectName
179
```

Figure 8: Updating object URL into the “root.yaml”.

10. Upload your edited root.yaml again to your s3-bucket. After successfully uploading, click on the newly uploaded **“root.yaml”** file.

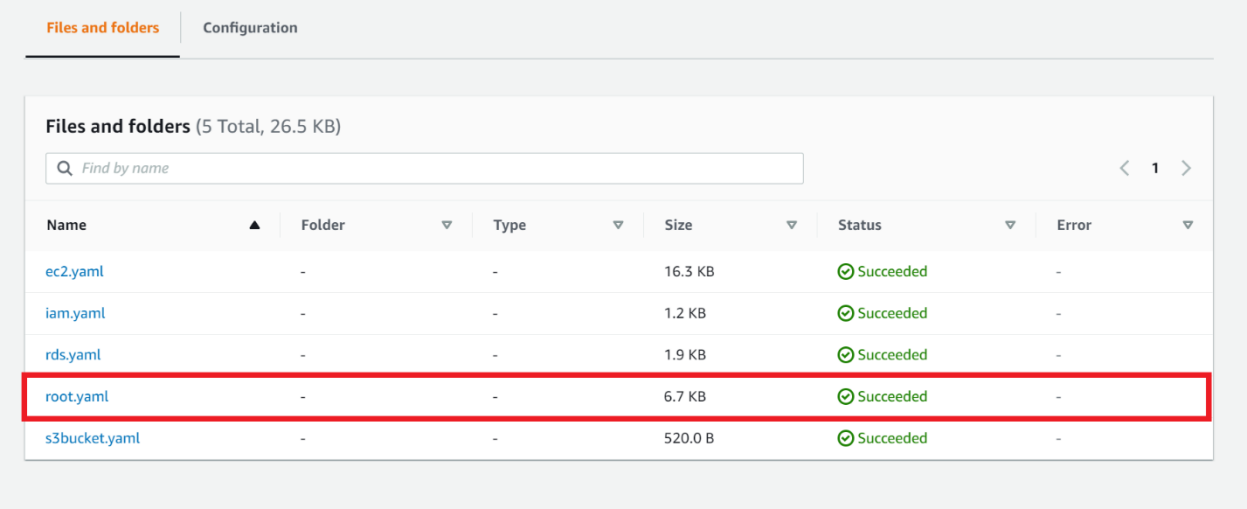


Figure 9: Launching root.yaml page

11. Once **root.yaml** page is launched, copy **object URL** for further use in step 14 as shown below.

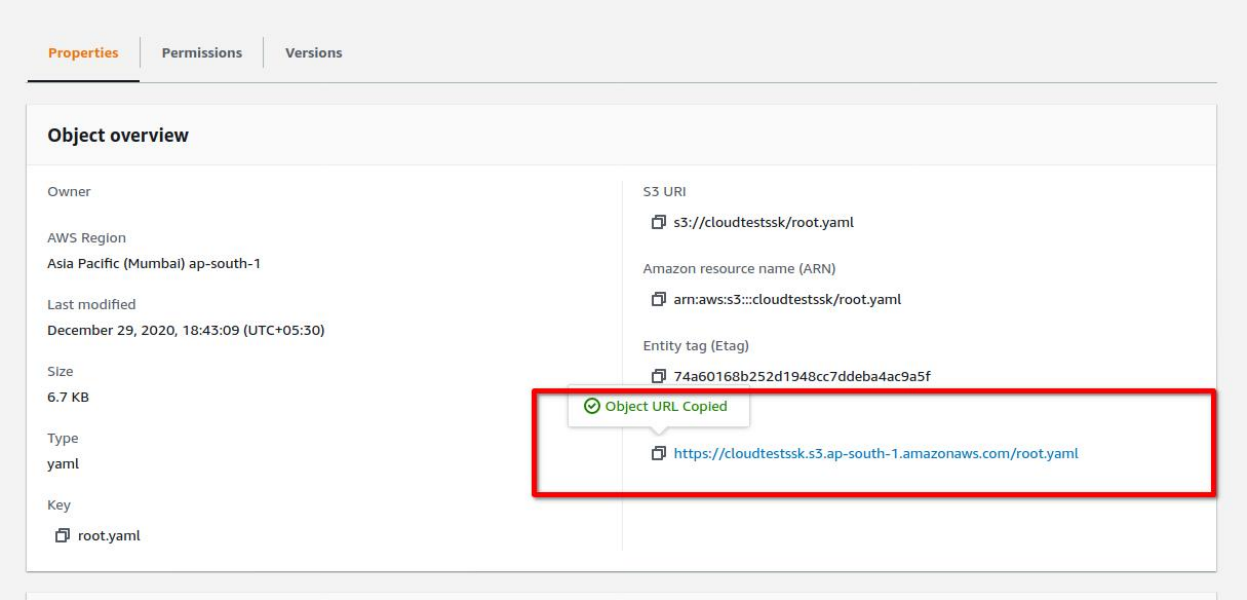


Figure 10: Copying Object URL

12. Now search for the **CloudFormation** service as shown in the below image and click on it.

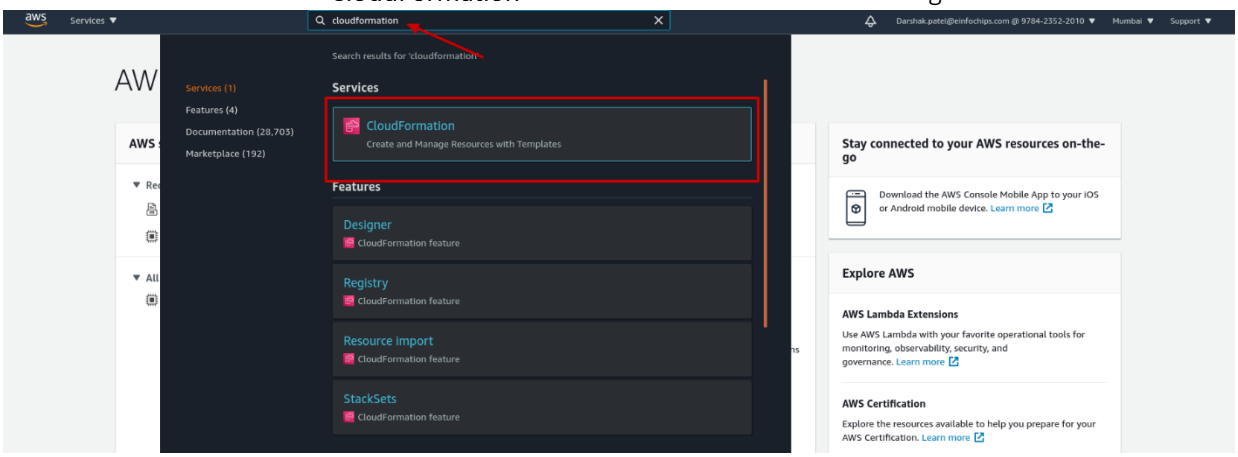


Figure 11: Searching for CloudFormation in Home Page

13. It will display page as shown below, Click on Create Stack button.

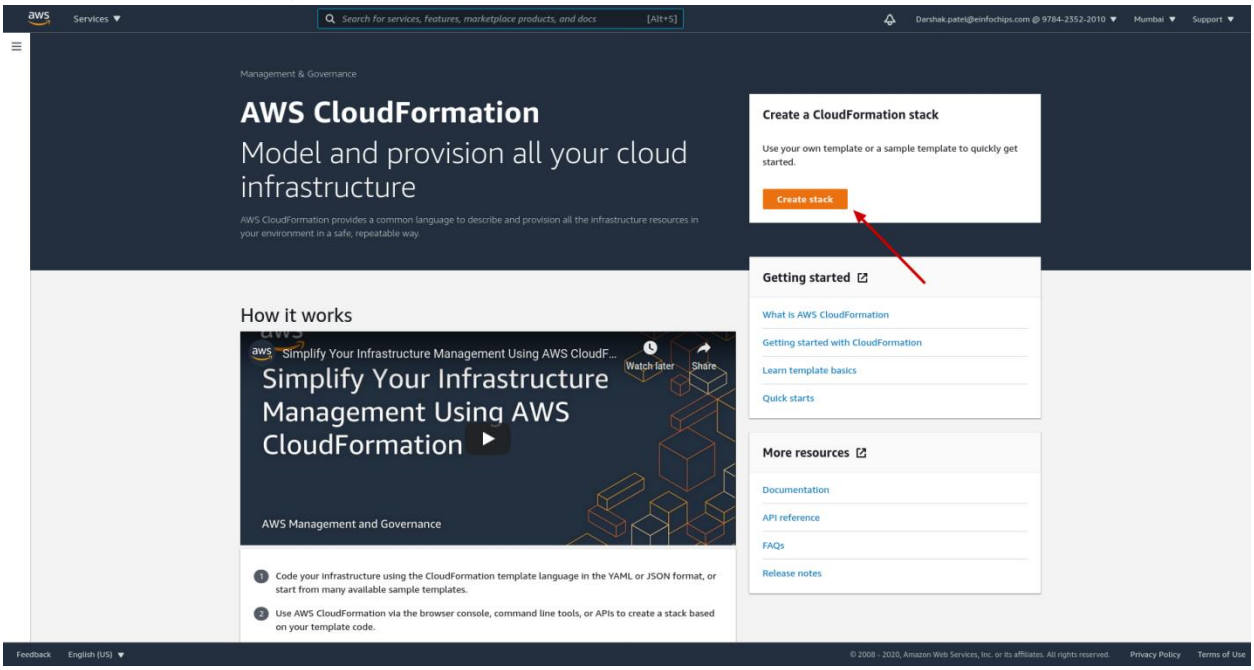


Figure 12: Create Stack

14. Enter the Object URL for your root.yaml which you have copied from step 11 in Amazon S3 URL and click on **Next** Button.

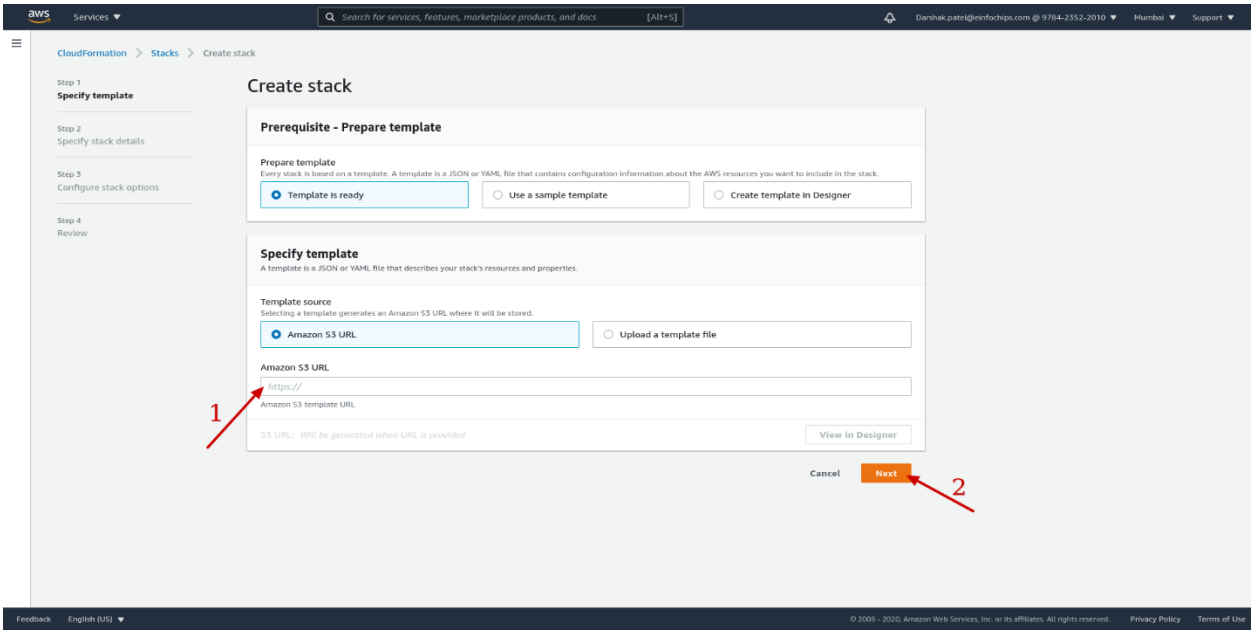


Figure 13: Creating Stack step1

15. Enter the **unique** stack **name** and fill the required parameters in the page while keeping in mind the below rules:
    - In **KeyName** parameter, need to select **keypair** name which we have created in section 2.2.
    - For **DBUsername** parameter, username should not contain any special characters.
    - Enter **unique IAMUserName** and **ProjectName** here. Remember-repeat use of IAMUsername and ProjectName can create problem while creating stack.
    - For Dockerhub username and Password, please provide below credentials:
        - **Dockerhub ID**: arrowelectronics
        - **Password**: Arrow1234
    - After filling all the details, click next.

Example:

AWSIOTCoreEndpoint	xxxxxx-ats.iot.ap-south-1.amazonaws.com
DBAllocatedStorage	20
DBInstanceClass	db.t2.micro
DBInstanceID	sskdbinstance
DBPassword	einfochips123 (should be alpha-numeric)
DBUsername	admin
DockerHubPassword	Arrow1234
DockerHubUserName	arrowelectronics
IAMUserName	testusr (should be unique)
InstanceType	t2.micro
KeyName	SSK_Test
ProjectName	abcseed (should be unique)

Note : AWSIOTCoreEndpoint URL can be found in AWS Account > IoT Core Service > Settings

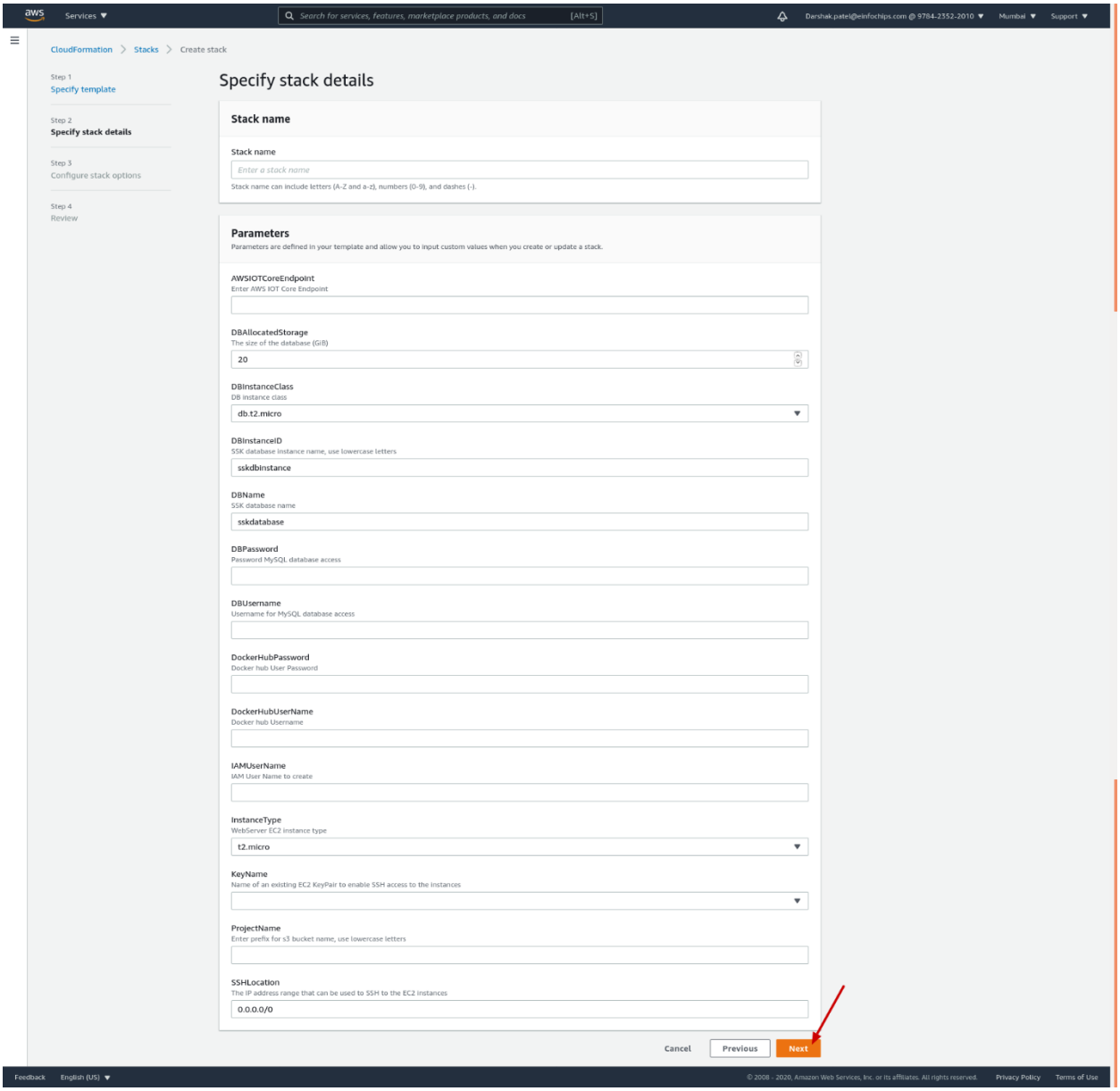


Figure 14: Creating Stack step2

16. On the next page, you can optionally add tags (Tags are used for billing/cost management). Click on **Next** Button.

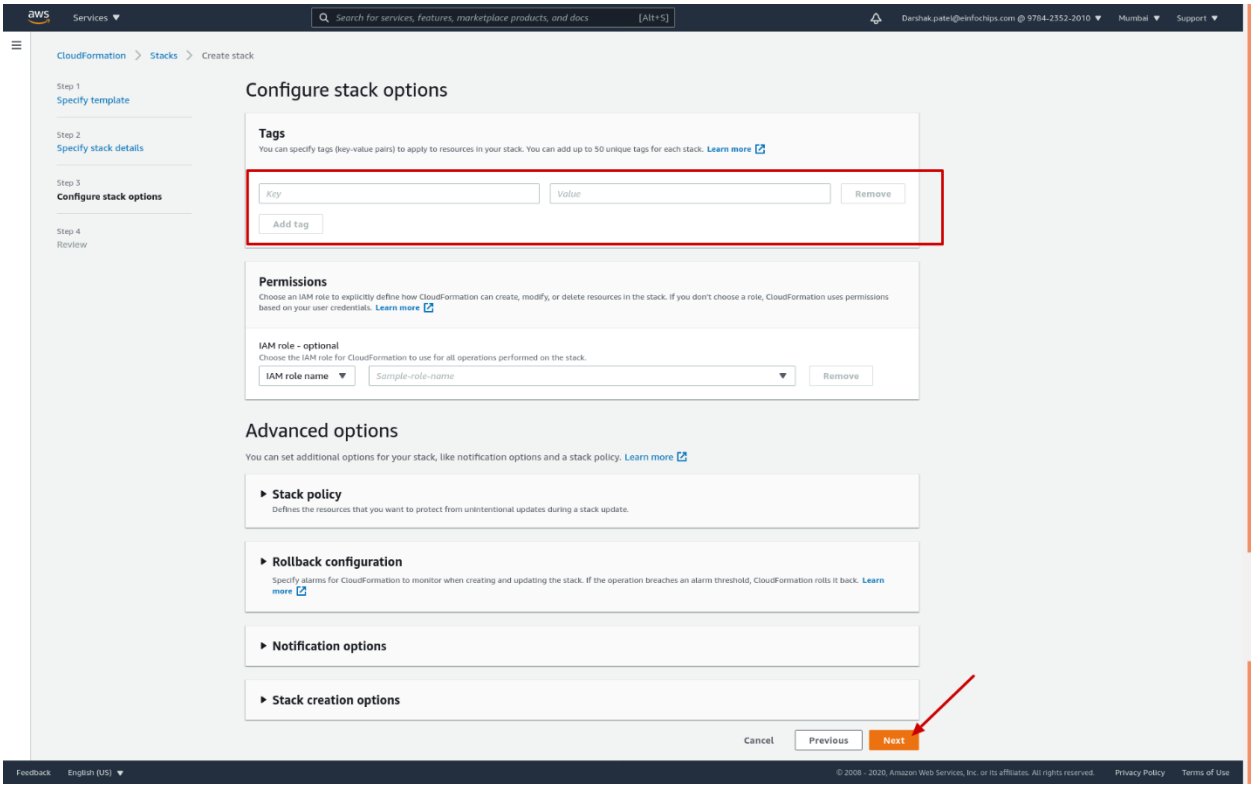


Figure 15: Creating Stack step3

17. Review the stack details (for parameters value and tags value). Then select the checkboxes for acknowledgment as shown in below image and Click on **Create Stack** Button.

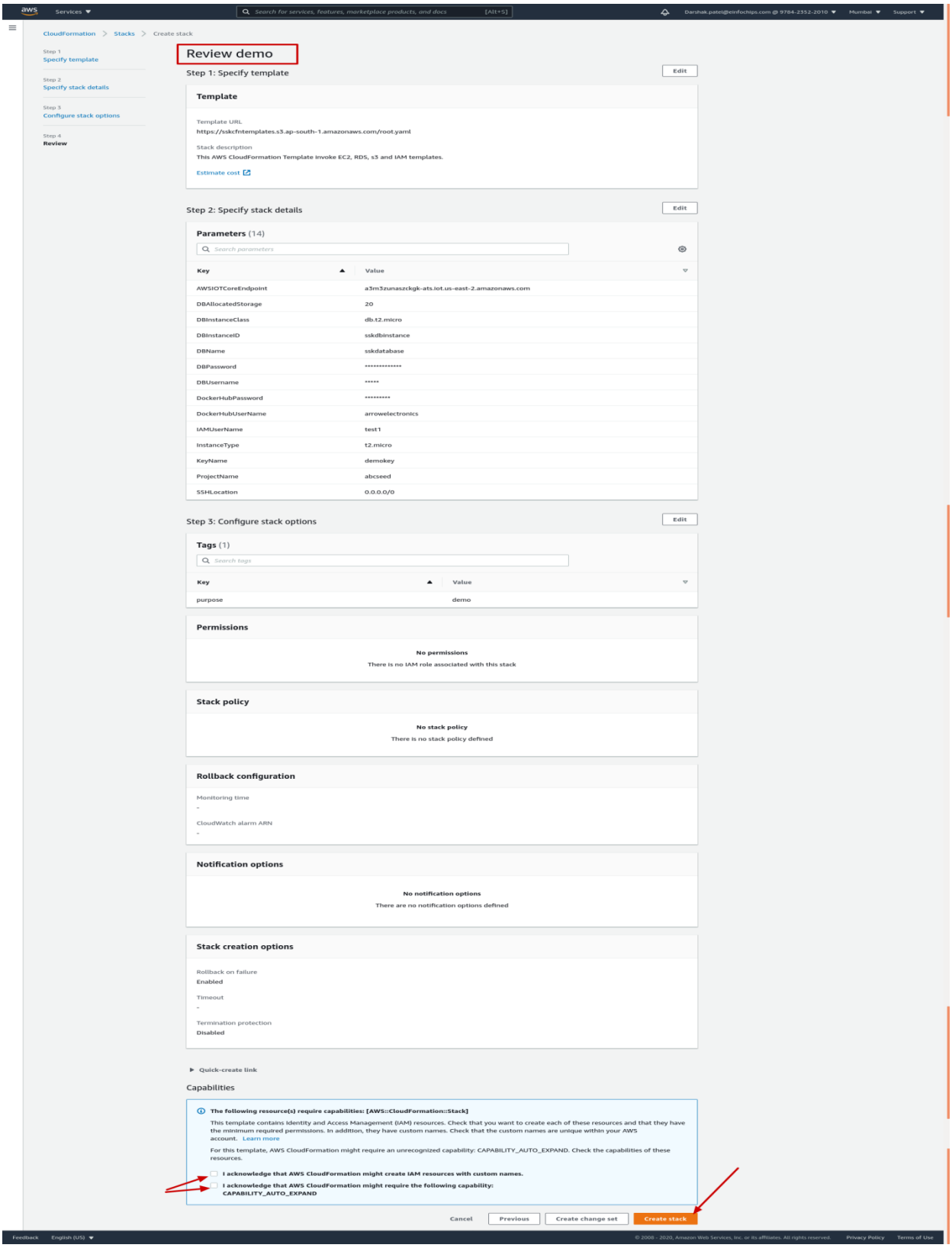


Figure 16: Creating Stack step4

18. It will start creating stacks for IAM User, RDS, EC2 instance and S3 Bucket. You can see the stack status and refresh the events as shown in below image.

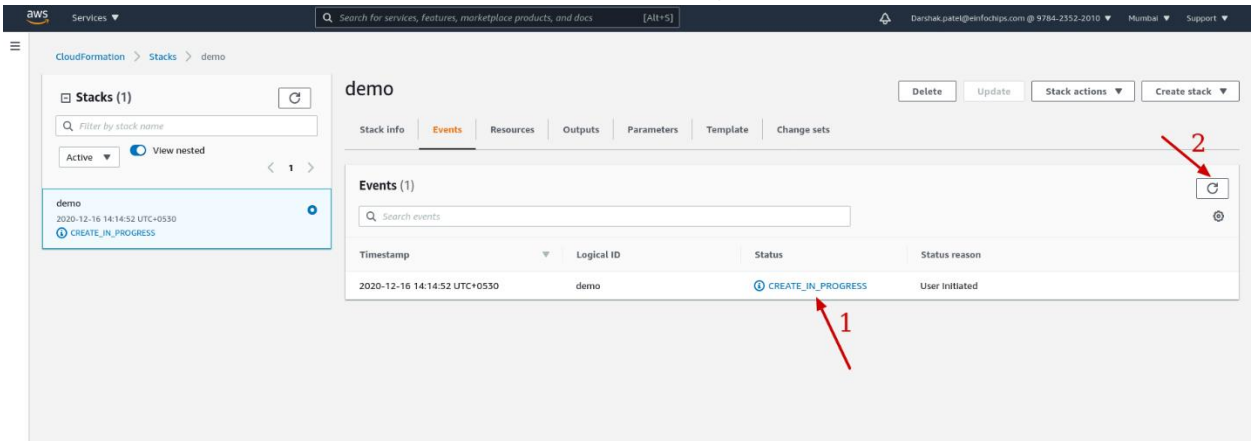


Figure 17: Stack Creation event/status page

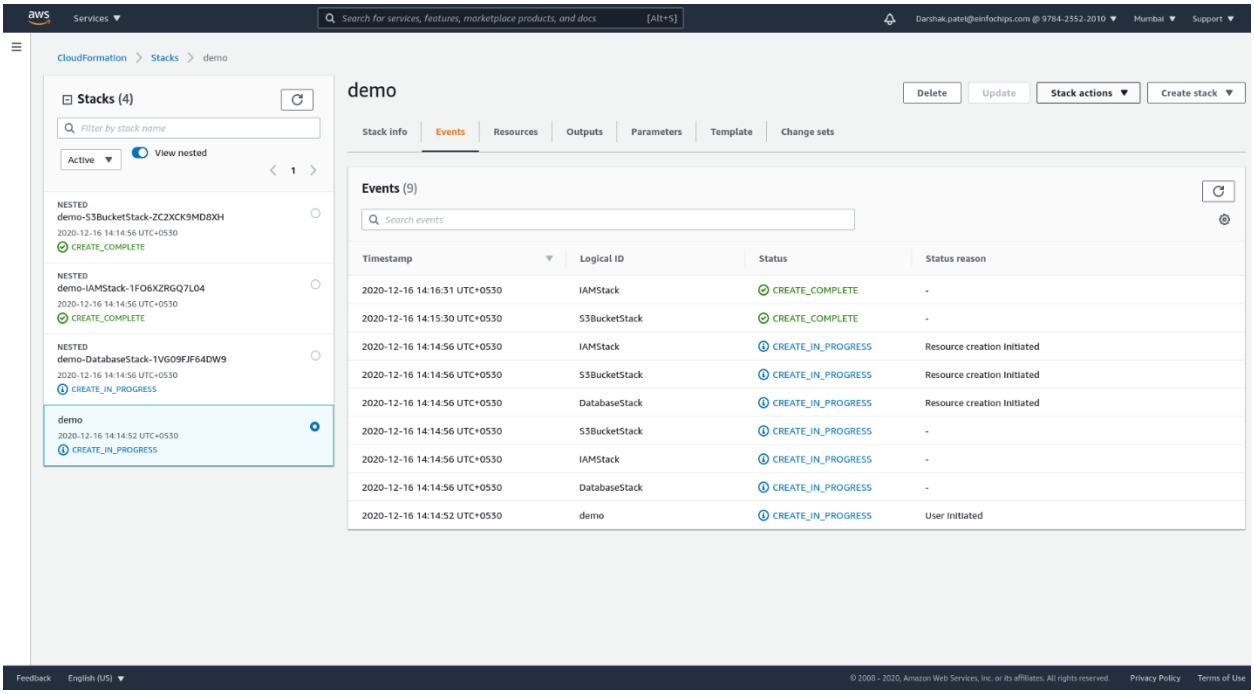


Figure 18: Stack Creation event/status page

19. After Stack creation, you can check for the website URL in the last row of the Output section.

Outputs (11)

Search outputs

Key	Value	Description	Export name
PublicIP	65.0.173.53	EC2 public IP	-
RDSInstanceId	seeeedsskdbinstance	InstanceId of the newly created RDS Instance	-
SecretKey	j1qtUQafzaWoDkeAPoRryUM3k+3Zsk+DHj5P85sA	the Access Key Secret	-
UserName	kaushalava1	Master Username of DB	-
WebsiteURL	http://ec2-65-0-173-53.ap-south-1.compute.amazonaws.com	Website URL	-

Figure 19: Checking Website URL in output tab after Stack Creation

---

Note:

[Please login once with the below api link in order to provide access

http://<ec2 domain name>/api/v1/aws/thing/configthingtypeandbucket

i.e.

http://ec2-xx-xxx-xxx-xx.ap-south 1.compute.amazonaws.com/api/v1/aws/thing/configthingtypeandbucket]

User will be able to check the thing created successful page as per below.

JSON Raw Data Headers

Save Copy Collapse All Expand All Filter JSON

```
success:   true
message:   "Thing Type & S3 Bucket created successfully"
result:    null
```

---

20. Double clicking on above **website URL**, user will be launched to the login SSK Cloud Connect Portal as shown below:

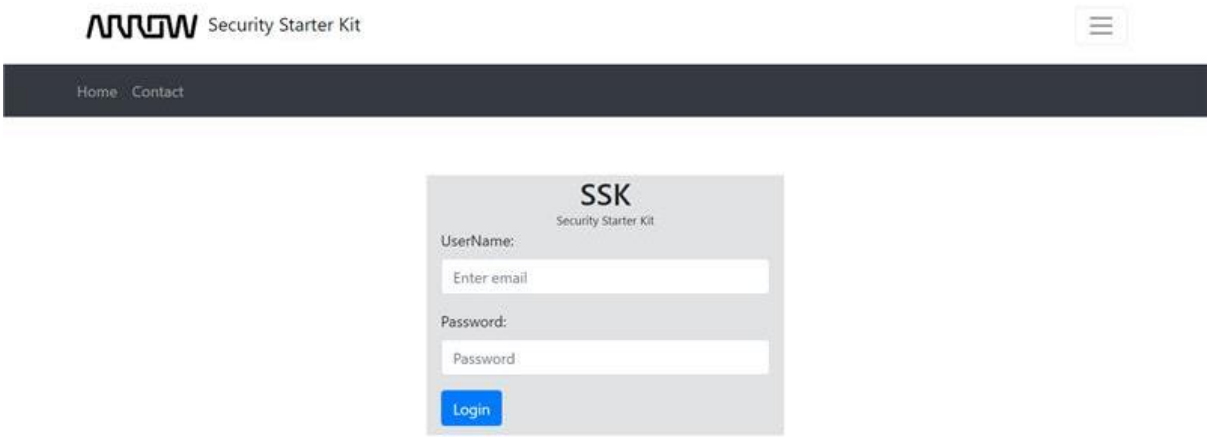


Figure 20: SSK Login page

Note: **Username**: IAMUsername (User entered while creating Cloud Stack)
Password: ArrowSSKportal@2020 (Created for Temporary use only)

21. After logging in, user can also edit default username "null null" with their desired name.

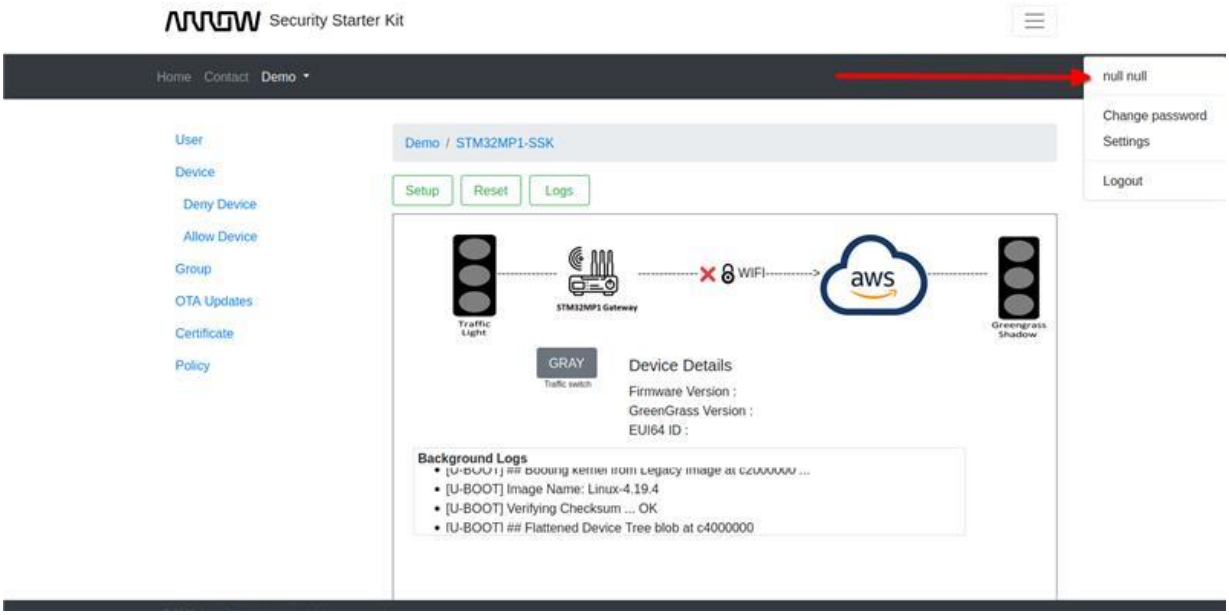


Figure 21: SSK Home page

22. By clicking on “null null”, the below screen will display for the user to change their details as they want them to be displayed.

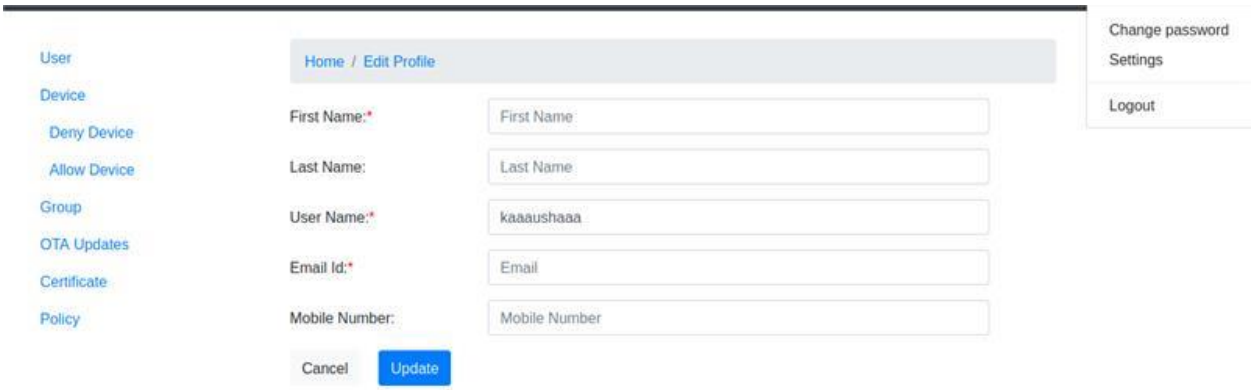
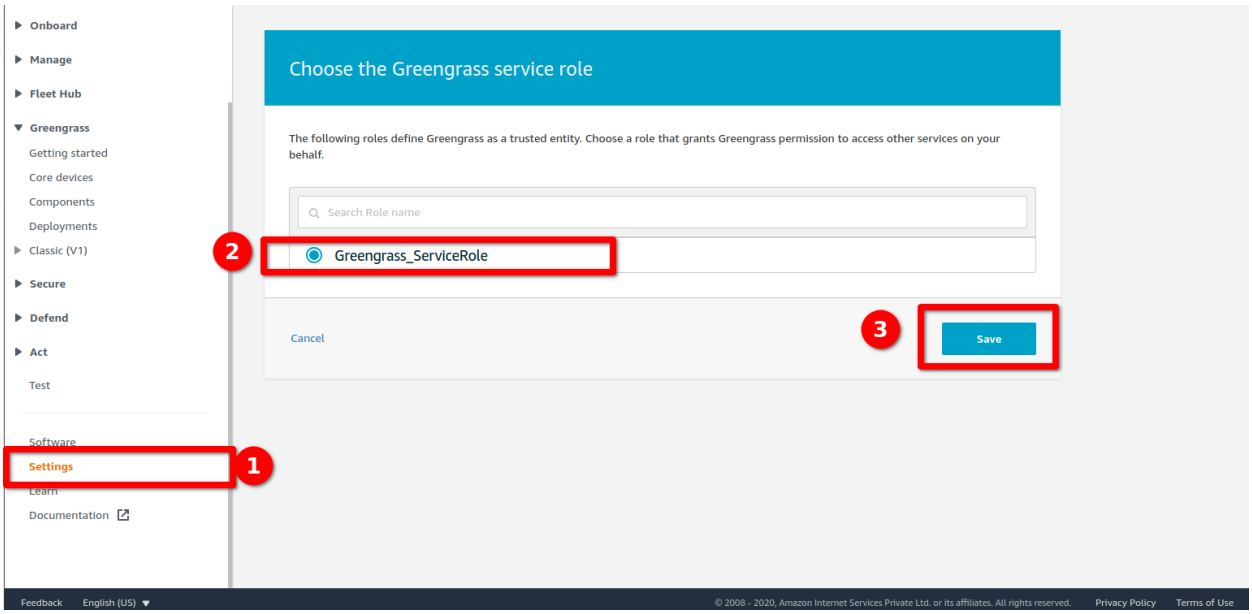


Figure 22: SSK Home/Edit profile page

23. User needs to Login into the AWS Console Account. Now search for **IOT Greengrass>>Settings>>Greengrass service role**

Now select Attach role option available there.

Greengrass Service role will act as a service enabling AWS lambda and IoT shadow activity i.e. while performing SSK Demo. This will gets add into your AWS Account by default upon selection.



Note : If you are facing issue enabling this feature , kindly follow greengrass service role

As we have successfully installed the cloud connect portal, please refer SSK Quick Start Guides to ensure performance of SSK Demos.