

Secure Starter Kit Cloud Connect Quick Start Guide

Date: June 15, 2021 | Version 1.2



The Solutions People



CONTENTS

1 INTRODUCTION3

1.1 Purpose of the Document3

1.2 AWS Cloud Services Descriptions and its background information3

2 AWS ACCOUNT CREATION4

2.1 Login or Create your AWS Account4

2.2 Create New Key Pair to enable SSH access to the EC2 instance5

2.3 Check Security group rules of Default Security Group6

3 CLOUDFORMATION CODE EXECUTION8

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

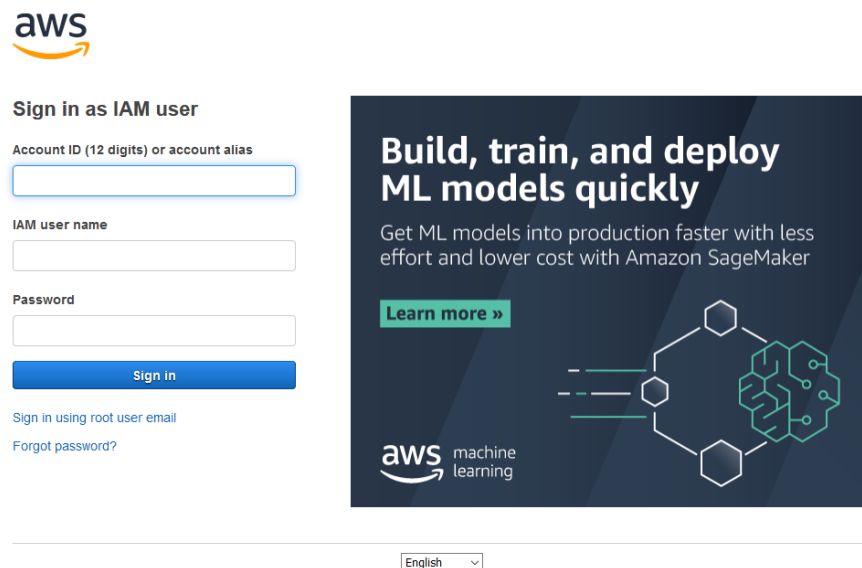
For AWS Cloud Services descriptions and its background information, follow the [SSK Cloud Connect Installation Setup Guide](#)

2 AWS ACCOUNT CREATION

2.1 Login or Create your AWS Account

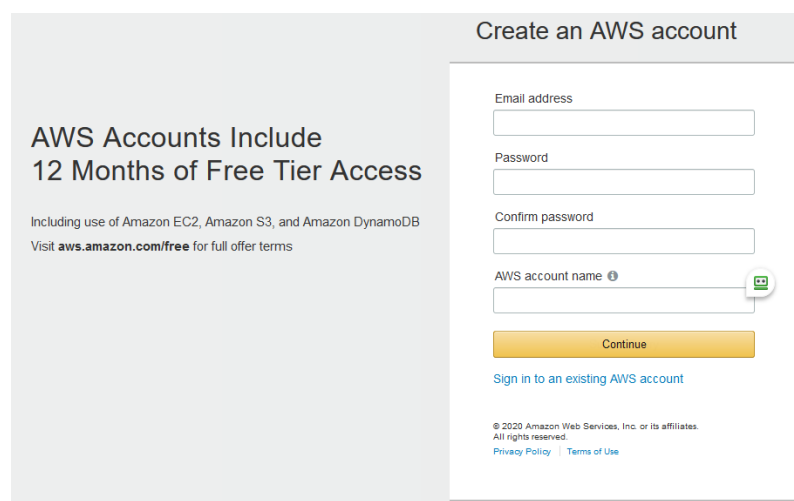
Note: If the User does not have an AWS Account, you will need to create one. This is used as the basis for the configuration of the other services required to run the demo's provided in the Security Starter Kits.

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



The screenshot shows the AWS login page. On the left, under the AWS logo, is the 'Sign in as IAM user' section. It contains three input fields: 'Account ID (12 digits) or account alias', 'IAM user name', and 'Password'. Below these is a blue 'Sign in' button. Underneath the button are two links: 'Sign in using root user email' and 'Forgot password?'. On the right is a large promotional banner for Amazon SageMaker with the text 'Build, train, and deploy ML models quickly' and a 'Learn more »' button. At the bottom center, there is a language dropdown menu set to 'English'.

Figure 1: Login page



The screenshot shows the 'Create an AWS account' page. On the left, a grey box contains the text 'AWS Accounts Include 12 Months of Free Tier Access' and a link to 'aws.amazon.com/free'. On the right, a white box contains the registration form with fields for 'Email address', 'Password', 'Confirm password', and 'AWS account name'. A yellow 'Continue' button is at the bottom of the form. Below the button is a link to 'Sign in to an existing AWS account'. At the very bottom, there is a copyright notice for 2020 Amazon Web Services, Inc. and links to 'Privacy Policy' and 'Terms of Use'.

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

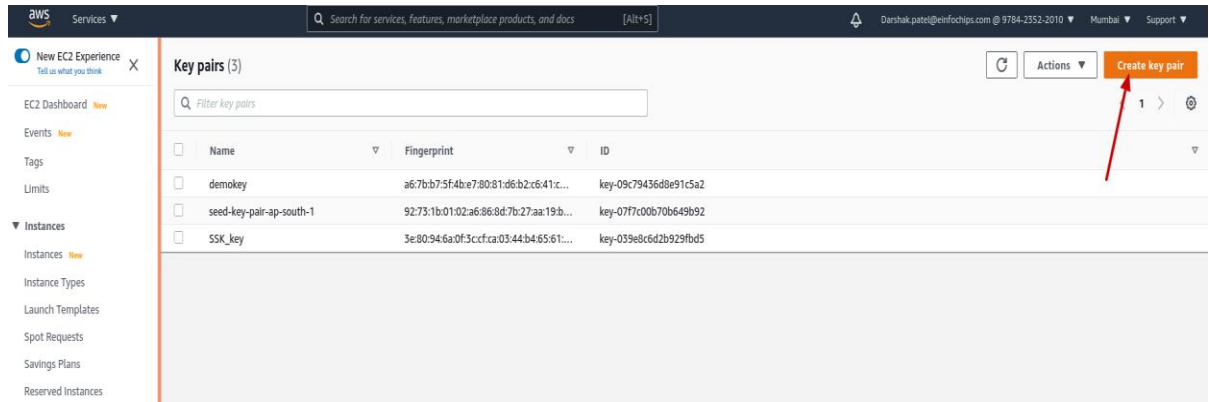


Figure 1: Create Key Pair page

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

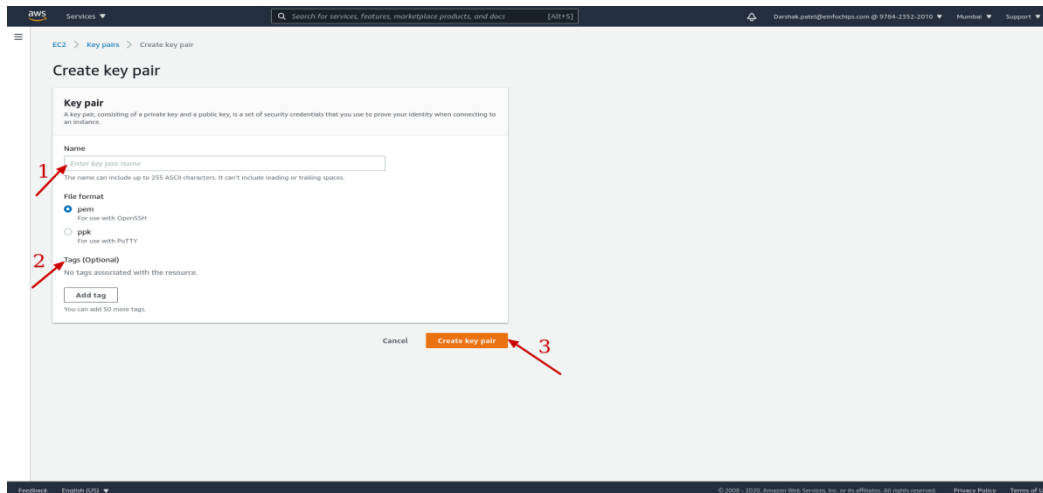


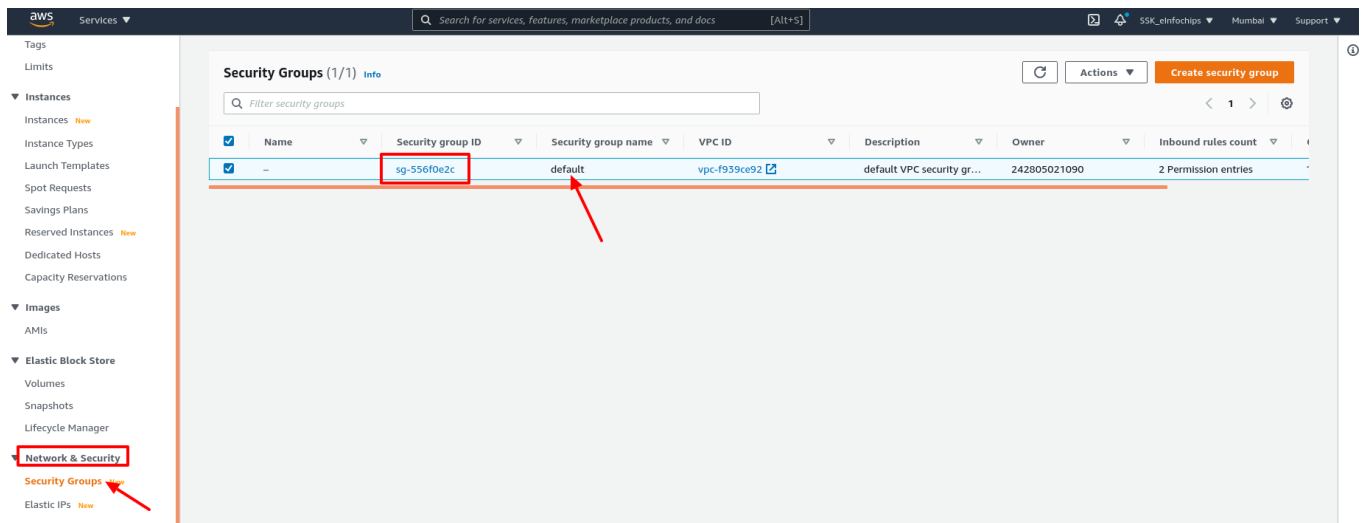
Figure 2: Creating Key Pair page

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

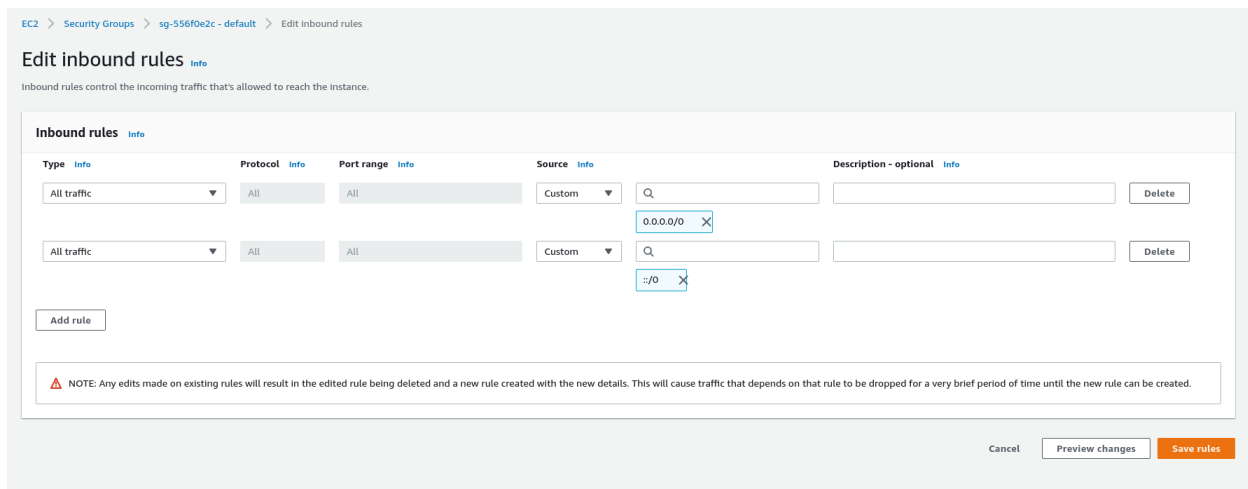
Note: Keep key file at secure place, which will be used to connect Ec2 instance.

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.



SECURITY STARTER KIT CLOUD CONNECT QUICK START GUIDE


[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 ▼ Q 0.0.0.0/0 X		Delete
All traffic ▼	All	All	Custom ▼ Q ::/0 X		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:

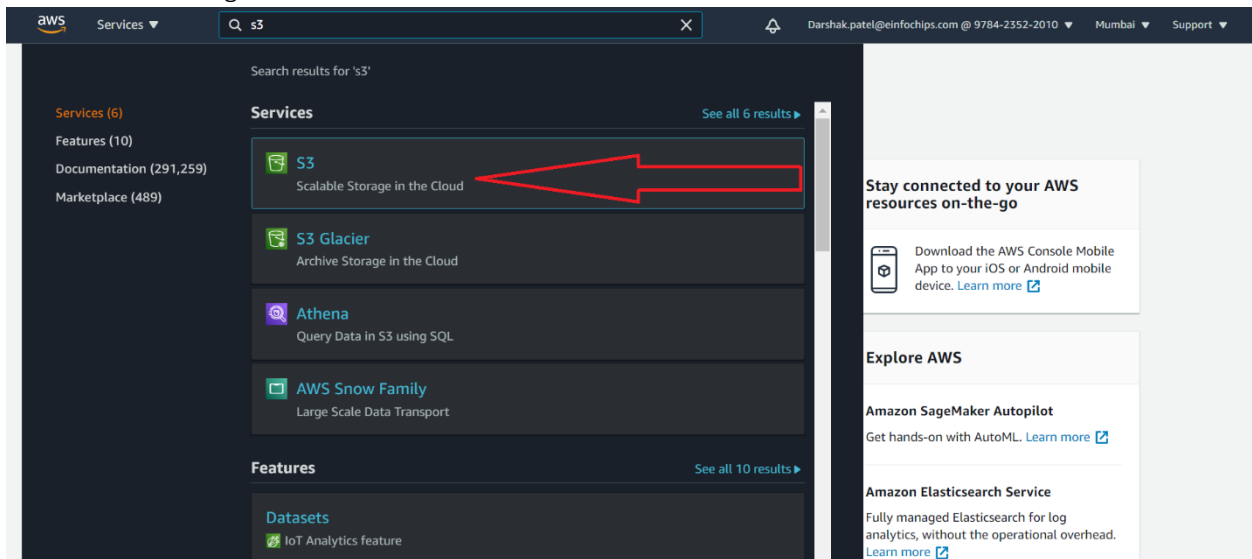


Figure 1: Searching for S3 service in Home Page

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

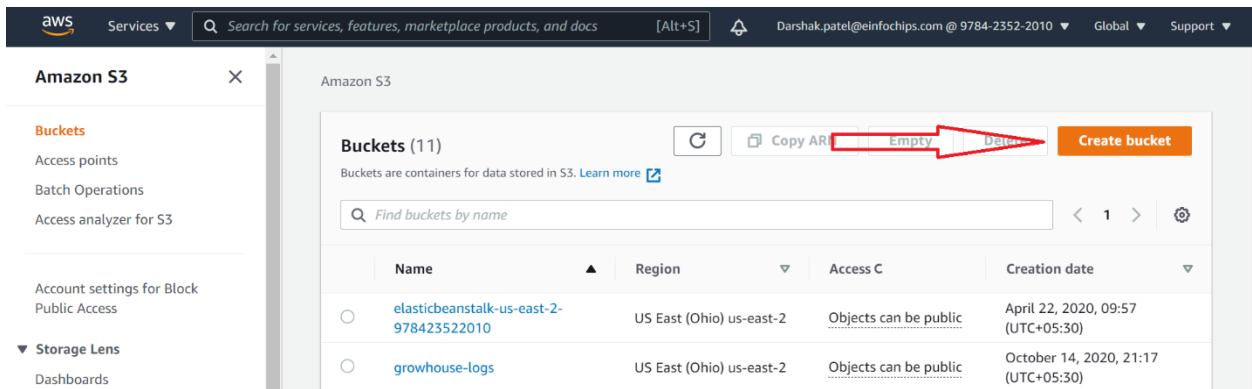


Figure 2: Create bucket

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.

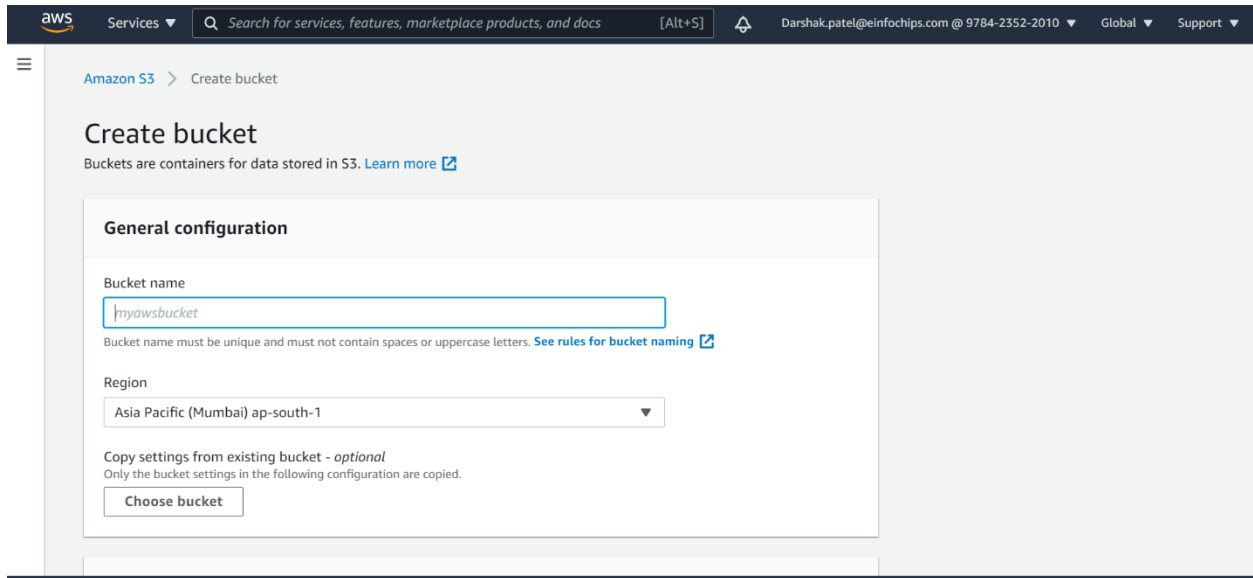


Figure 3: Creating S3 bucket

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
<input type="checkbox"/> ec2.yaml	✓	12/17/2020 12:08 PM	YAML File	17 KB
<input type="checkbox"/> iam.yaml	✓	12/17/2020 12:10 PM	YAML File	2 KB
<input type="checkbox"/> rds.yaml	✓	12/16/2020 1:59 PM	YAML File	2 KB
<input type="checkbox"/> root.yaml	✓	12/17/2020 10:51 AM	YAML File	7 KB
<input type="checkbox"/> 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:

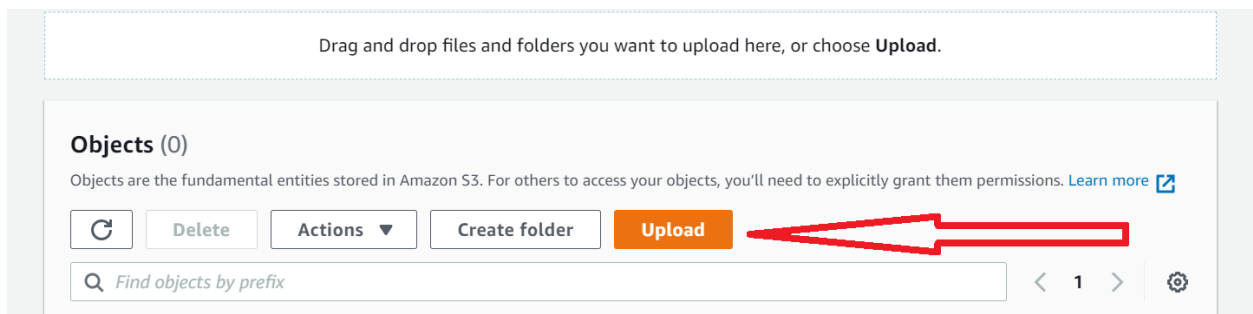


Figure 5: To upload files in S3 bucket

- 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:

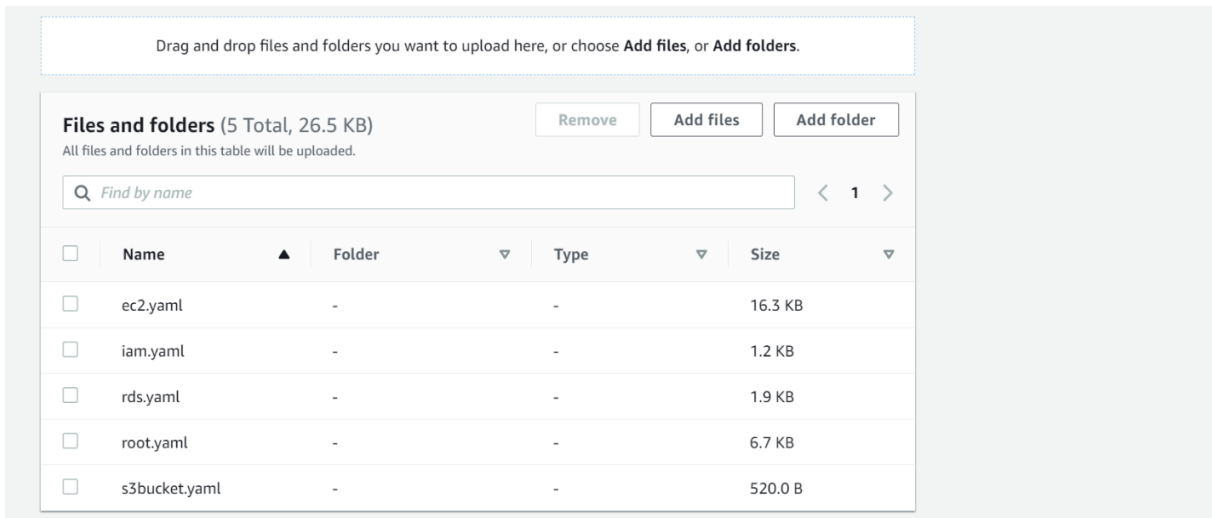


Figure 6: Uploading files in S3 bucket

- 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.

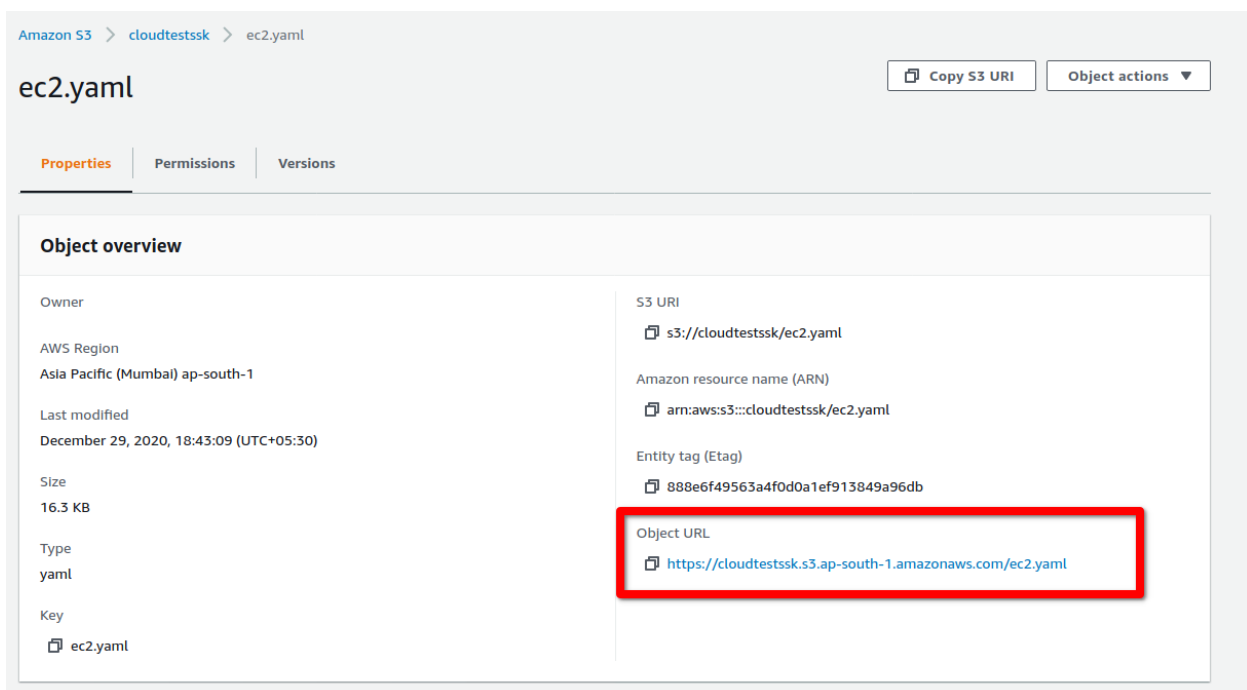


Figure 7: copying object URL

- 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   DBInstanceName: !Ref DBInstanceName
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
146   AWSTOTCoreEndpoint: !Ref AWSTOTCoreEndpoint
147   InstanceType: !Ref InstanceType
148   KeyName: !Ref KeyName
149   SSHLocation: !Ref SSHLocation
150   DBInstanceName: !GetAtt DatabaseStack.Outputs.DBInstanceName
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
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   ProjectName: !Ref ProjectName
178
179

```

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

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

Files and folders

Configuration

Files and folders (5 Total, 26.5 KB)

Find by name

<

1

>

Name	Folder	Type	Size	Status	Error
ec2.yaml	-	-	16.3 KB	✔ Succeeded	-
iam.yaml	-	-	1.2 KB	✔ Succeeded	-
rds.yaml	-	-	1.9 KB	✔ Succeeded	-
root.yaml	-	-	6.7 KB	✔ Succeeded	-
s3bucket.yaml	-	-	520.0 B	✔ Succeeded	-

Figure 9: Launching root.yaml page

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

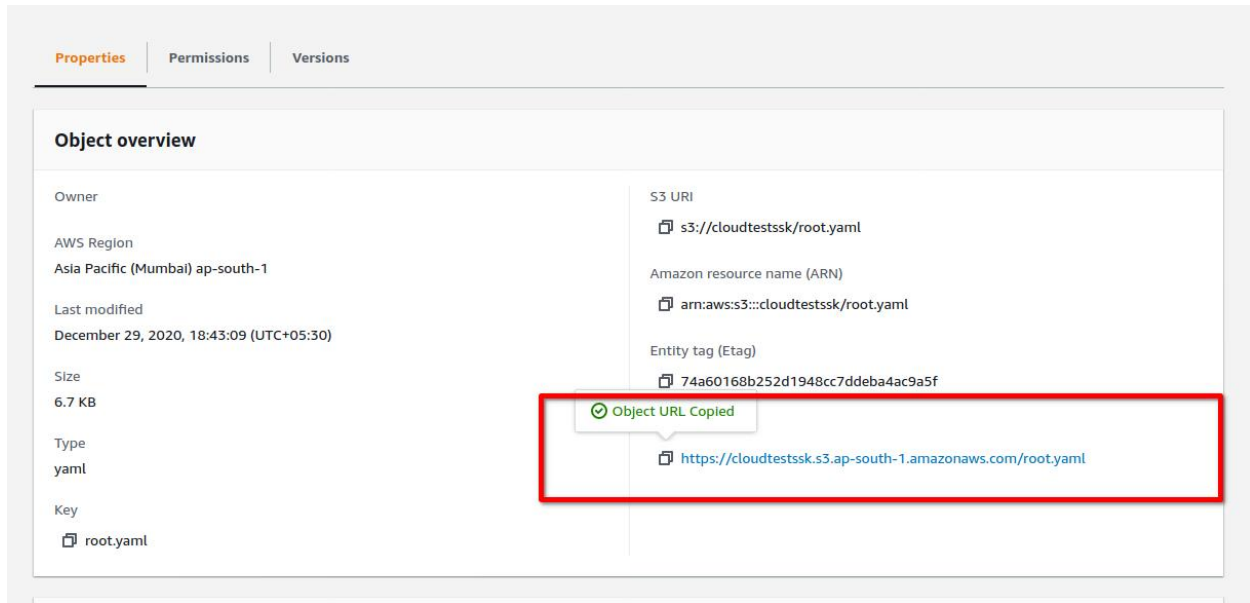


Figure 10: Copying Object URL

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

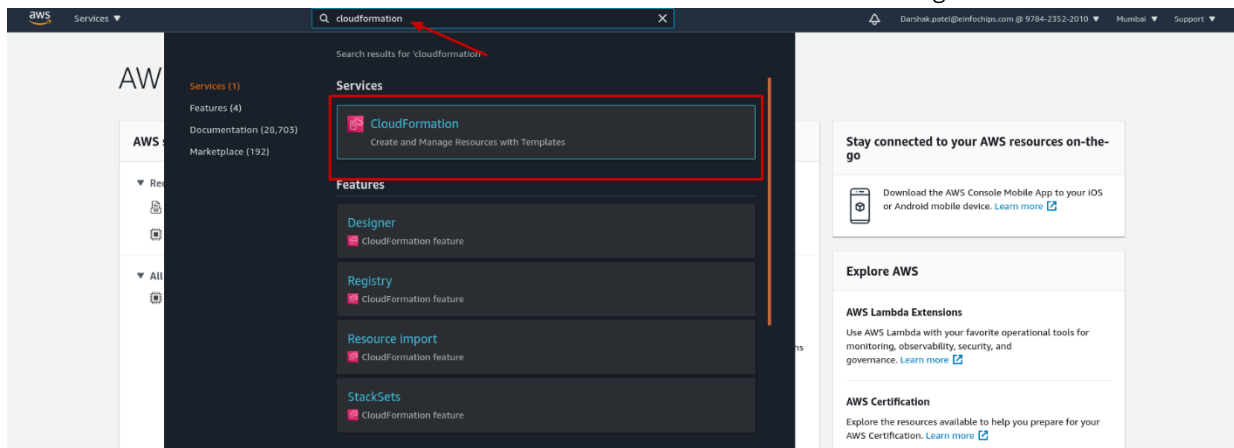


Figure 11: Searching for CloudFormation in Home Page

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

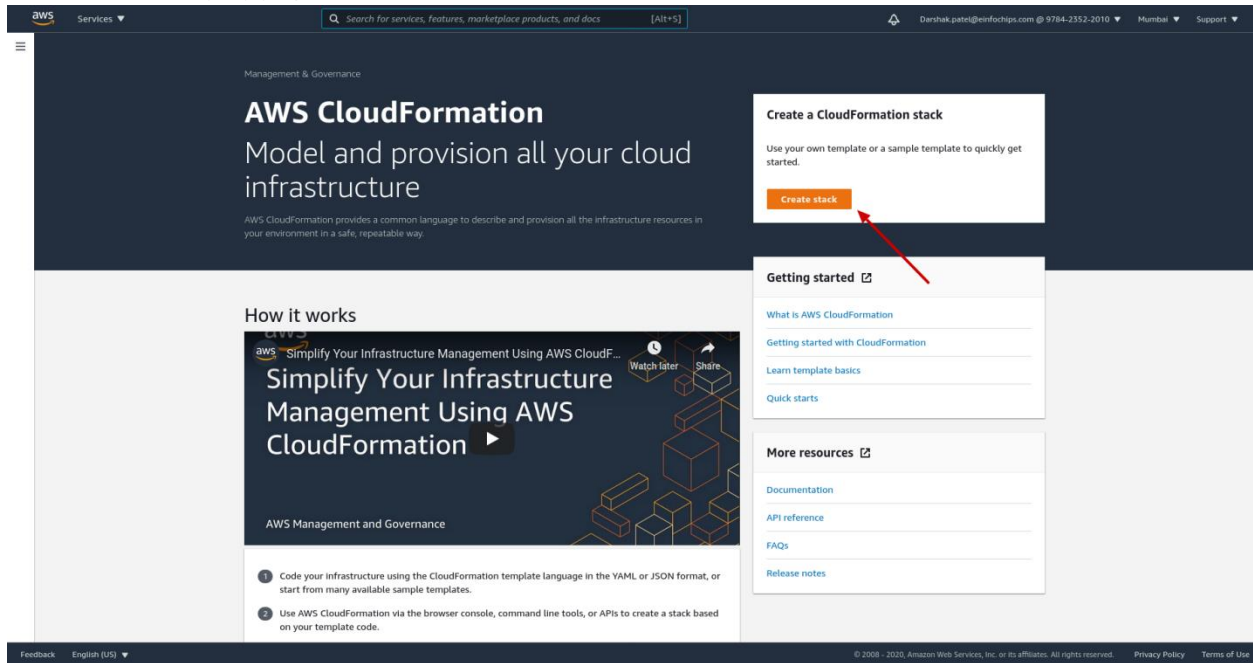


Figure 12: Create Stack

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.

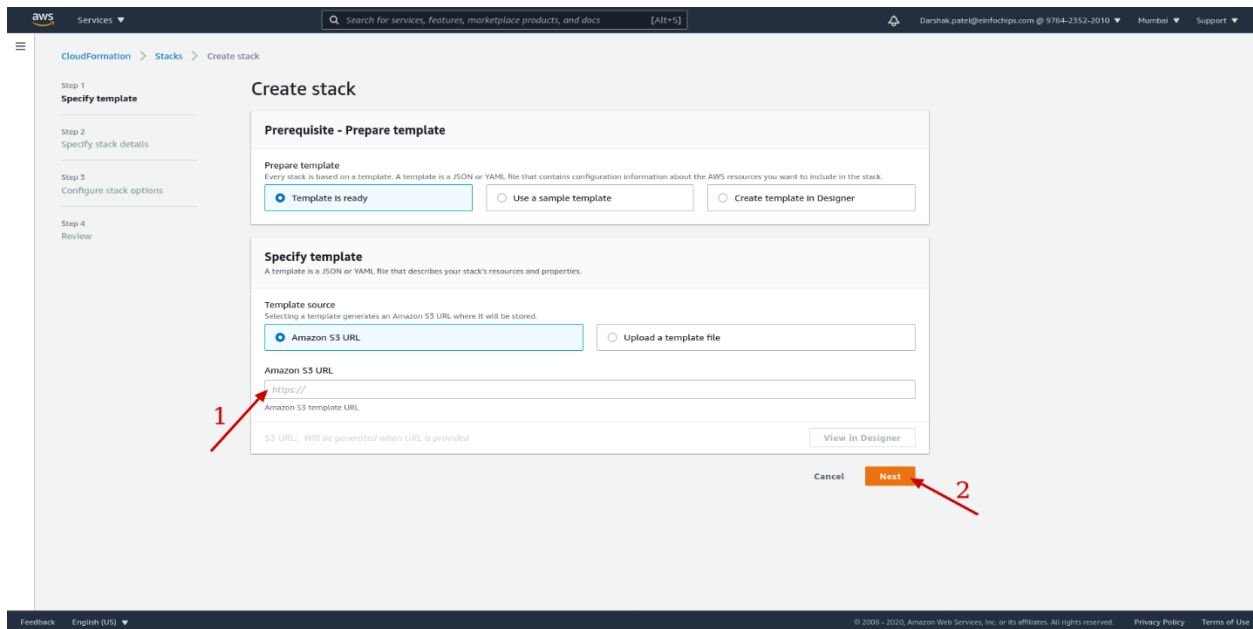


Figure 13: Creating Stack step1

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

SECURITY STARTER KIT CLOUD CONNECT QUICK START GUIDE

The screenshot shows the AWS CloudFormation console interface for creating a new stack. The breadcrumb navigation at the top indicates the path: CloudFormation > Stacks > Create stack. On the left, a sidebar shows the progress through four steps: Step 1: Specify template, Step 2: Specify stack details (current step), Step 3: Configure stack options, and Step 4: Review. The main content area is titled 'Specify stack details' and contains several input sections. The 'Stack name' section has a text input field with a placeholder 'Enter a stack name' and a note that stack names can include letters (A-Z and a-z), numbers (0-9), and dashes (-). The 'Parameters' section lists various parameters defined in the template, each with a corresponding input field: AWSIoTCoreEndpoint (text), DBAllocatedStorage (numeric, value 20), DBInstanceClass (dropdown, value db.t2.micro), DBInstanceID (text, value sskdbinstance), DBName (text, value sskdatabase), DBPassword (text), DBUsername (text), DockerHubPassword (text), DockerHubUserName (text), IAMUserName (text), InstanceType (dropdown, value t2.micro), KeyName (dropdown), ProjectName (text), and SSHLocation (text, value 0.0.0.0/0). At the bottom right of the form, there are three buttons: 'Cancel', 'Previous', and 'Next'. A red arrow points to the 'Next' button. The footer of the console shows 'Feedback', 'English (US)', and copyright information for Amazon Web Services, Inc. or its affiliates.

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.

The screenshot displays the AWS CloudFormation console's 'Configure stack options' page. The left sidebar shows the progress: Step 1 (Specify template), Step 2 (Specify stack details), Step 3 (Configure stack options), and Step 4 (Review). The main content area is titled 'Configure stack options'. It features a 'Tags' section where users can add key-value pairs for resource tagging, highlighted with a red box. Below this is the 'Permissions' section, which includes an 'IAM role - optional' dropdown menu. The 'Advanced options' section at the bottom contains expandable panels for 'Stack policy', 'Rollback configuration', 'Notification options', and 'Stack creation options'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons, with a red arrow pointing to the '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.

SECURITY STARTER KIT CLOUD CONNECT QUICK START GUIDE

CloudFormation

Stacks

Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Review demo

Step 1: Specify template

Template

Template URL
https://s3.amazonaws.com/stack-templates/s3-ap-south-1.amazonaws.com/root.yaml

Stack description
This AWS CloudFormation Template invoke EC2, RDS, s3 and IAM templates.

Estimate cost

Step 2: Specify stack details

Parameters (14)

Search parameters

Key	Value
AWSIoTCoreEndpoint	a5m3zumazczgk-atk-iot-us-east-2.amazonaws.com
DBAllocatedStorage	20
DBInstanceClass	db.t2.micro
DBInstanceID	sskdbinstance
DBName	sskdatabase
DBPassword	*****
DBUsername	*****
DockerHubPassword	*****
DockerHubUserName	arrowelectronics
IAMUserName	test1
InstanceType	t2.micro
KeyName	demokey
ProjectName	abcseed
SSHLocation	0.0.0.0/0

Step 3: Configure stack options

Tags (1)

Search tags

Key	Value
purpose	demo

Permissions

No permissions
There is no IAM role associated with this stack

Stack policy

No stack policy
There is no stack policy defined

Rollback configuration

Monitoring time
-
CloudWatch alarm ARN
-

Notification options

No notification options
There are no notification options defined

Stack creation options

Rollback on failure
Enabled
Timeout
-
Termination protection
Disabled

Quick-create link

Capabilities

The following resource(s) require capabilities: [AWS::CloudFormation::Stack]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more](#)

For this template, AWS CloudFormation might require an unrecognized capability: CAPABILITY_AUTO_EXPAND. Check the capabilities of these resources.

☐ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

☐ I acknowledge that AWS CloudFormation might require the following capability: CAPABILITY_AUTO_EXPAND

Cancel

Previous

Create change set

Create stack

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.

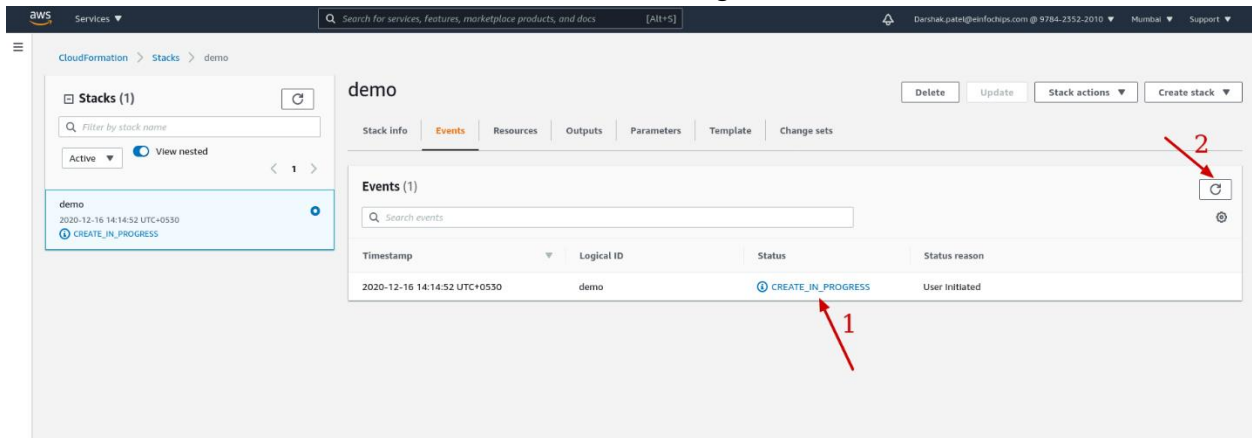


Figure 17: Stack Creation event/status page

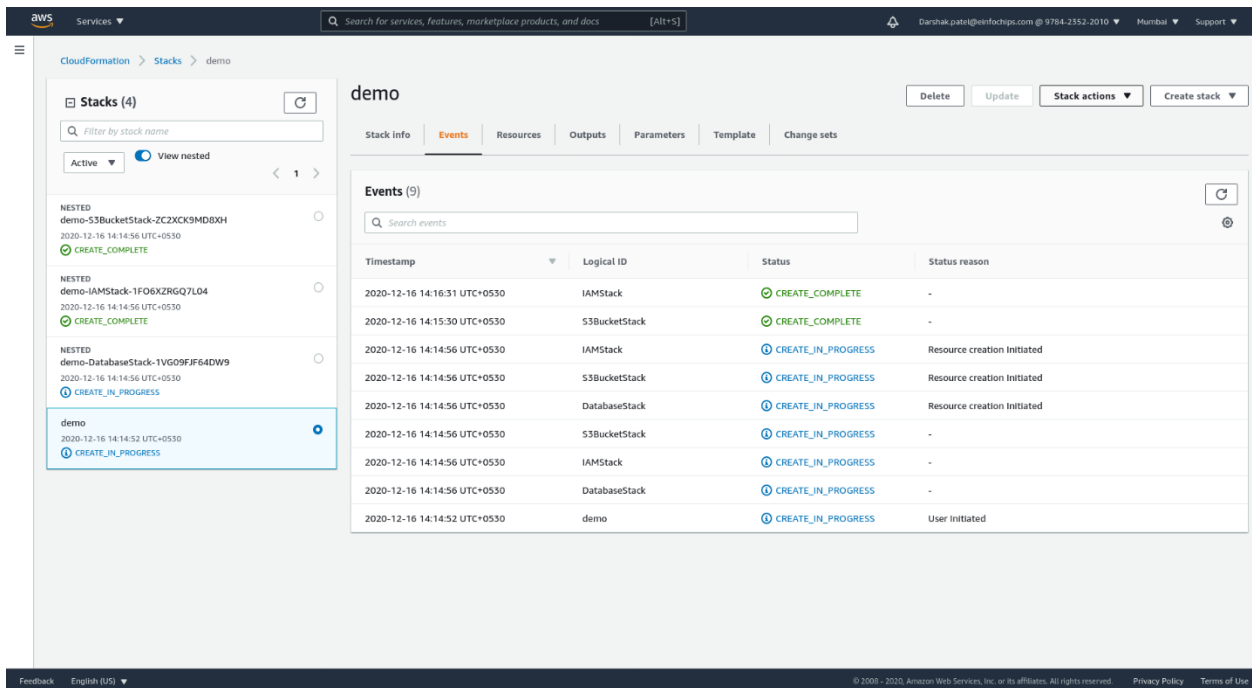


Figure 18: Stack Creation event/status page

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

Outputs (11)				
<input type="text" value="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	j1qtUQafzaWoDke APoRryUM3k+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.

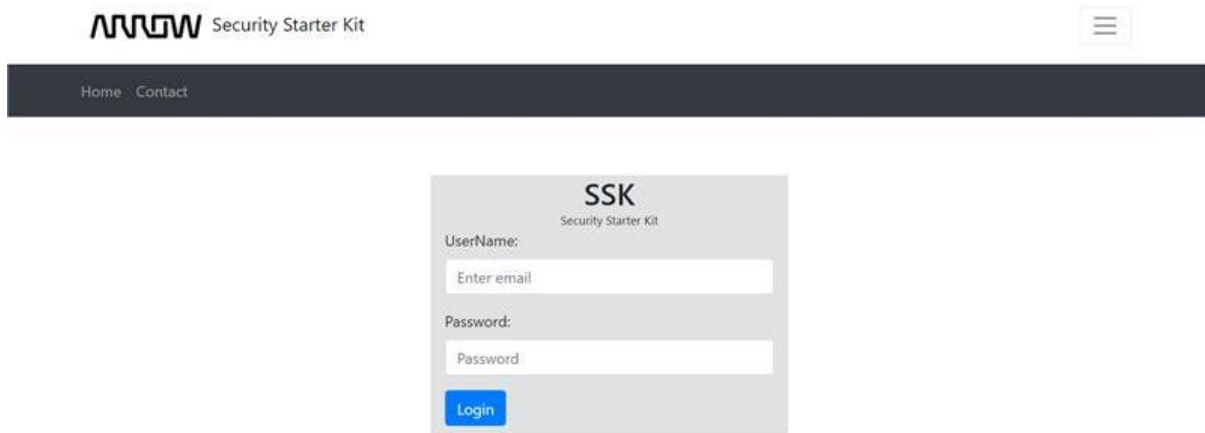
<http://ec2-xx-xxx-xxx-xx.ap-south>

[1.compute.amazonaws.com/api/v1/aws/thing/configthingtypeandbucket](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		
<pre> success: true message: "Thing Type & S3 Bucket created successfully" result: null </pre>		

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

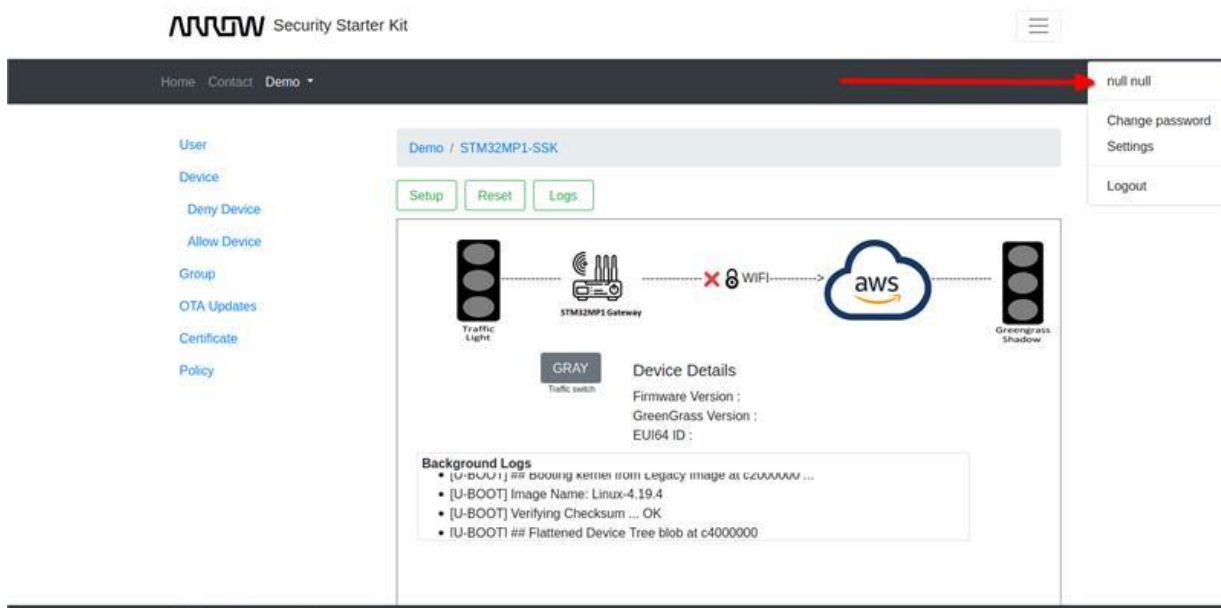


The screenshot shows the SSK Security Starter Kit login page. At the top, there is a logo for 'Arrow Security Starter Kit' and a hamburger menu icon. Below the logo is a dark navigation bar with 'Home' and 'Contact' links. The main content area is a light gray box titled 'SSK Security Starter Kit'. It contains a 'UserName:' label followed by a text input field with the placeholder 'Enter email'. Below that is a 'Password:' label followed by a password input field with the placeholder 'Password'. At the bottom of the form is a blue 'Login' button.

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.



The screenshot shows the SSK Home page after login. The top navigation bar includes 'Home', 'Contact', and 'Demo'. A red arrow points to a dropdown menu in the top right corner, which contains the text 'null null', 'Change password', 'Settings', and 'Logout'. The main content area is titled 'Demo / STM32MP1-SSK' and features three buttons: 'Setup', 'Reset', and 'Logs'. Below these buttons is a diagram showing a 'Traffic Light' connected to a 'STM32MP1 Gateway' (labeled 'GRAY Traffic switch'), which is connected to 'WiFi' (with a red 'X' indicating a connection issue) and then to 'aws' (Amazon Web Services). To the right of the diagram is a 'GreenGrass Shadow' icon. Below the diagram is a 'Device Details' section with the following information: 'Firmware Version:', 'GreenGrass Version:', and 'EUI64 ID:'. At the bottom is a 'Background Logs' section with a list of log entries: '[U-BOOT] ## Booting kernel from Legacy image at c2000000 ...', '[U-BOOT] Image Name: Linux-4.19.4', '[U-BOOT] Verifying Checksum ... OK', and '[U-BOOT] ## Flattened Device Tree blob at c4000000'.

Figure 21: SSK Home page

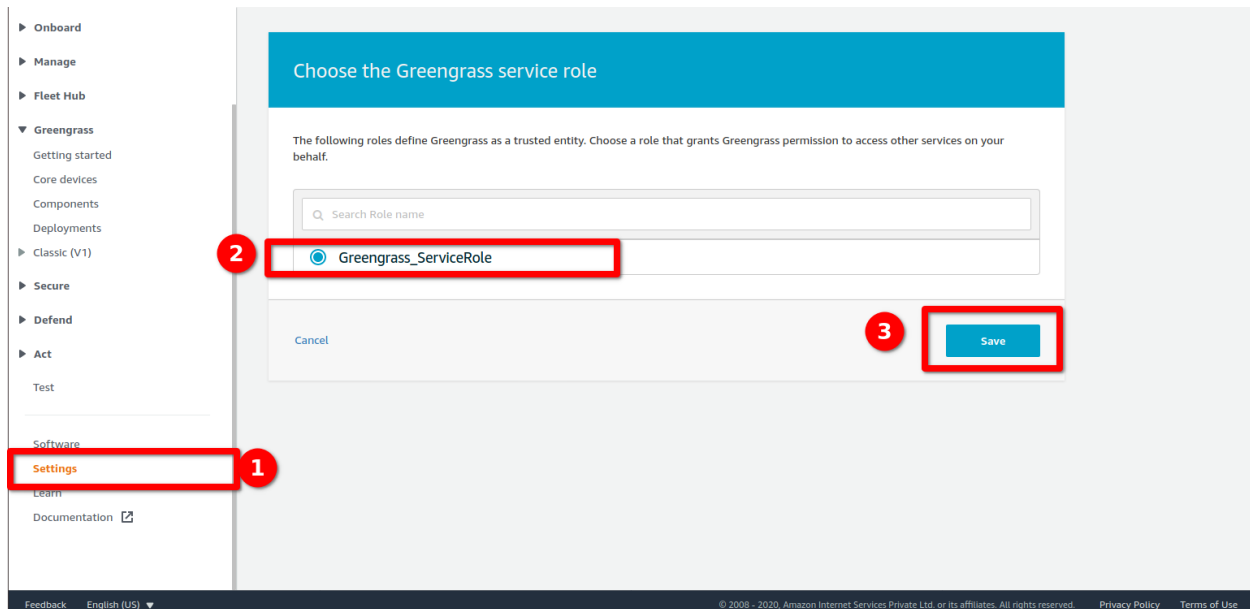
22. By clicking on “null null”, the below screen will display for the user to change their details as they want them to be displayed.

The screenshot shows the 'Edit Profile' page in the SSK application. On the left is a navigation menu with options: User, Device, Deny Device, Allow Device, Group, OTA Updates, Certificate, and Policy. The main area has a breadcrumb 'Home / Edit Profile' and a form with the following fields: First Name (with a red asterisk), Last Name, User Name (containing 'kaaaushaaa'), Email Id (with a red asterisk), and Mobile Number. Below the form are 'Cancel' and 'Update' buttons. On the right side, there is a vertical menu with 'Change password', 'Settings', and 'Logout'.

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 get added 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.