Amazon Q is helping you resolve the following error:

A security group rule with the same protocol, port range, and source has already been added to this security group. Each rule must have a unique combination of protocol, port range, and source.

**Analysis**

The error is occurring because you have attempted to add a duplicate security group rule to your security group. Each rule in a security group must have a unique combination of protocol, port range, and source to avoid conflicts.

**Resolution**

Amazon Q recommends the following steps to resolve your error

1. Go to the EC2 console and navigate to the Security Groups section.
2. Identify the security group you are trying to modify.
3. Review the existing inbound and outbound rules for that security group.
4. If you find a rule with the same protocol, port range, and source as the one you are trying to add, you cannot add a duplicate rule.
5. If you need to modify an existing rule, select the rule and click "Edit Inbound Rules" or "Edit Outbound Rules" as applicable.
6. If you need to add a new rule with a unique combination of protocol, port range, and source, click "Add Rule" and specify the required settings.
7. Describe terminology and concepts related to AWS services
8. Navigate the AWS Management Console
9. Articulate key concepts of AWS security measures and AWS Identity and Access Management (IAM)
10. Distinguish among several AWS compute services, including Amazon Elastic Compute Cloud
11. (Amazon EC2), AWS Lambda, Amazon Elastic Container Service (Amazon ECS), and Amazon Elastic Kubernetes Service (Amazon EKS)
12. Understand AWS database and storage offerings, including Amazon Relational Database Service (Amazon RDS), Amazon DynamoDB, and Amazon Simple Storage Service (Amazon S3)
13. Explore AWS networking services
14. Access and configure Amazon CloudWatch monitoring fe

Explain the topics with examples and steps for

**Module 1: Introduction to Amazon Web Services**

* Introduction to AWS Cloud
* Security in the AWS Cloud
* Hosting the employee directory application in AWS
* Hands-On Lab: Introduction to AWS Identity and Access Management (IAM)

**Module 2: AWS Compute**

* Compute as a service in AWS
* Introduction to Amazon Elastic Compute Cloud
* Amazon EC2 instance lifecycle
* AWS container services
* What is serverless?
* Introduction to AWS Lambda
* Choose the right compute service
* Hands-On Lab: Launch the Employee Directory Application on Amazon EC2

**Module 3: AWS Networking**

* Networking in AWS
* Introduction to Amazon Virtual Private Cloud (Amazon VPC)
* Amazon VPC routing
* Amazon VPC security
* Hands-On Lab: Create a VPC and Relaunch the Corporate Directory Application in Amazon EC2

**Module 4: AWS Storage**

* AWS storage types
* Amazon EC2 instance storage and Amazon Elastic Block Store (Amazon EBS)
* Object storage with Amazon S3
* Choose the right storage service
* Hands-On Lab: Create an Amazon S3 Bucket

**Module 5: Databases**

* Explore databases in AWS
* Amazon Relational Database Service
* Purpose-built databases
* Introduction to Amazon DynamoDB
* Choose the right AWS database service
* Hands-On Lab: Implement and manage Amazon DynamoDB

**Module 6: Monitoring, Optimization, and Serverless**

* Monitoring
* Optimization
* Alternate serverless employee directory application architecture
* Hands-On Lab: Configure High Availability for Your Application

Describe terminology and concepts related to AWS services Navigate the AWS Management Console• Articulate key concepts of AWS security measures and AWS Identity and Access Management (IAM)• Distinguish among several AWS compute services, including Amazon Elastic Compute Cloud• (Amazon EC2), AWS Lambda, Amazon Elastic Container Service (Amazon ECS), and Amazon Elastic Kubernetes Service (Amazon EKS) Understand AWS database and storage offerings, including Amazon Relational Database Service• (Amazon RDS), Amazon DynamoDB, and Amazon Simple Storage Service (Amazon S3) Explore AWS networking services• Access and configure Amazon CloudWatch monitoring feature•

Explain the topics with examples and steps for

* Describe terminology and concepts related to AWS services
* Navigate the AWS Management Console
* Articulate key concepts of AWS security measures and AWS Identity and Access Management (IAM)
* Distinguish among several AWS compute services, including Amazon Elastic Compute Cloud (Amazon EC2), AWS Lambda, Amazon Elastic Container Service (Amazon ECS), and Amazon Elastic  
  Kubernetes Service (Amazon EKS)
* Understand AWS database and storage offerings, including Amazon Relational Database Service (Amazon RDS), Amazon DynamoDB, and Amazon Simple Storage Service (Amazon S3)
* Explore AWS networking services
* Access and configure Amazon CloudWatch monitoring feat

Policy templates - *optional*Info

Choose one or more policy templates.

## Function permissions

AWS offers managed permissions policies that you can add to your IAM role. Choose all the policies that apply to your function.

Resource-based policies enable you to grant usage permissions to other accounts on a per-resource basis. You use a resource-based policy to allow an AWS service to invoke your function.

* AMI read-only permissionsEC2
* AWS Batch access permissionsBatch
* AWS CloudFormation stack read-only permissionsCloudFormation
* AWS Config Rules permissionsConfigS3
* Basic Lambda@Edge permissions (for CloudFront trigger)CloudWatch Logs
* Elasticsearch permissionsElasticsearch
* AWS IoT Button permissionsSNS
* Simple microservice permissionsDynamoDB
* Amazon Rekognition no data permissionsRekognition
* Amazon Rekognition read-only permissionsRekognition
* Amazon Rekognition write-only permissionsRekognition
* roleTemplates.SecretsManagerSecrets Manager
* Amazon S3 object read-only permissionsS3
* Amazon SES bounce permissionsSES
* Amazon SNS publish policySNS
* Amazon SQS poller permissionsSQS
* Test harness permissionsDynamoDBLambda
* VPN Connection Monitor permissionsCloudWatchEC2

<https://us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#Home>:

djs-vp-project1

1. [Amazon S3](https://us-east-1.console.aws.amazon.com/s3/get-started?region=us-east-1&bucketType=general)
2. [Buckets](https://us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general)
3. **djsbucketemployee**

# djsbucketemployee

 Info

* Objects
* Properties
* Permissions
* Metrics
* Management
* Access Points

## Bucket overview

AWS Region

US East (N. Virginia) us-east-1

Amazon Resource Name (ARN)

arn:aws:s3:::djsbucketemployee

Creation date

June 3, 2024, 15:12:08 (UTC+05:30)

## Bucket Versioning

Edit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](https://docs.aws.amazon.com/console/s3/enable-bucket-versioning)

Bucket Versioning

Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](https://docs.aws.amazon.com/console/s3/bucket-versioning-mfa-delete)

Disabled

## Tags (0)

Edit

You can use bucket tags to track storage costs and organize buckets. [Learn more](https://docs.aws.amazon.com/console/s3/cost-allocation-tagging)

| **Key** | **Value** |
| --- | --- |
| No tags associated with this resource. | |

## Default encryptionInfo

Edit

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption typeInfo

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](https://docs.aws.amazon.com/console/s3/bucket-key)

Enabled

## Intelligent-Tiering Archive configurations (0)

View details

Edit

Delete

Create configuration

Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. [Learn more](https://docs.aws.amazon.com/console/s3/intelligent-tiering)

| **Table Selection** | **Name** | **Status** | **Scope** | **Days until transition to Archive Access tier** | **Days until transition to Deep Archive Access tier** |
| --- | --- | --- | --- | --- | --- |
| **No archive configurations**  No configurations to display.  Create configuration | | | | | |

## Server access logging

Edit

Log requests for access to your bucket. Use [CloudWatch](https://console.aws.amazon.com/cloudwatch/home?region=us-east-1" \t "_blank) to check the health of your server access logging. [Learn more](https://docs.aws.amazon.com/console/s3/server-access-logging)

Server access logging

Disabled

## AWS CloudTrail data events

 Info

[Configure in CloudTrail](https://console.aws.amazon.com/cloudtrail/home?region=us-east-1#/configuration)

Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. [Learn more](https://docs.aws.amazon.com/console/s3/cloudtrail-logging)

| **Name** | **Access** |
| --- | --- |
| **No data events**  No data events to display.  [Configure in CloudTrail](https://console.aws.amazon.com/cloudtrail/home?region=us-east-1#/configuration) | |

## Event notifications (0)

Edit

Delete

Create event notification

Send a notification when specific events occur in your bucket. [Learn more](https://docs.aws.amazon.com/console/s3/enable-event-notifications)

|  | **Name** | **Event types** | **Filters** | **Destination type** | **Destination** |
| --- | --- | --- | --- | --- | --- |
| **No event notifications**  Choose **Create event notification** to be notified when a specific event occurs.  Create event notification | | | | | |

## Amazon EventBridge

Edit

For additional capabilities, use Amazon EventBridge to build event-driven applications at scale using S3 event notifications. [Learn more](https://docs.aws.amazon.com/console/s3/eventbridge-what-is) or [see EventBridge pricing](https://aws.amazon.com/eventbridge/pricing)

Send notifications to Amazon EventBridge for all events in this bucket

Off

## Transfer acceleration

Edit

Use an accelerated endpoint for faster data transfers. [Learn more](https://docs.aws.amazon.com/console/s3/transfer-acceleration)

Transfer acceleration

Disabled

## Object Lock

Edit

Store objects using a write-once-read-many (WORM) model to help you prevent objects from being deleted or overwritten for a fixed amount of time or indefinitely. Object Lock works only in versioned buckets. [Learn more](https://docs.aws.amazon.com/console/s3/object-lock)

Object Lock

Disabled

## Requester pays

Edit

When enabled, the requester pays for requests and data transfer costs, and anonymous access to this bucket is disabled. [Learn more](https://docs.aws.amazon.com/console/s3/requesterpaysbucket)

Requester pays

Disabled

## Static website hosting

Edit

Use this bucket to host a website or redirect requests. [Learn more](https://docs.aws.amazon.com/console/s3/hostingstaticwebsite)

Static website hosting

Enabled

Hosting type

Bucket hosting

Bucket website endpoint

When you configure your bucket as a static website, the website is available at the AWS Region-specific website endpoint of the bucket. [Learn more](https://docs.aws.amazon.com/console/s3/website-endpoints)

[http://djsbucketemployee.s3-website-us-east-1.amazonaws.com](http://djsbucketemployee.s3-website-us-east-1.amazonaws.com/)

djsdb

Master username

admin789

Master password

admin789Copy

Role details

Role name

Enter a meaningful name to identify this role.



Maximum 64 characters. Use alphanumeric and '+=,.@-\_' characters.

Description

Add a short explanation for this role.



Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: \_+=,. @-/\[{}]!#$%^&\*():;"'<>`

**Step 1: Select trusted entities**

Edit

Trust policy



1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"sts:AssumeRole"

],

"Principal": {

"Service": [

"ec2.amazonaws.com"

]

}

}

]

}

**Step 2: Add permissions**

Edit

Permissions policy summary

| **Policy name** | **Type** | **Attached as** |
| --- | --- | --- |
| [AmazonDynamoDBFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonDynamoDBFullAccess) | AWS managed | Permissions policy |
| [AmazonRDSFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonRDSFullAccess) | AWS managed | Permissions policy |
| [AmazonS3FullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonS3FullAccess) | AWS managed | Permissions policy |

**Step 3: Add tags**

Add tags - *optional*

 Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

Route Table Edit Route and Edit subnet associations

https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:

[**https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ConnectToInstance:instanceId=i-05c1b59a4eb78e528**](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ConnectToInstance:instanceId=i-05c1b59a4eb78e528)

[**http://djsbucketproject.s3-website.ap-south-1.amazonaws.com/**](http://djsbucketproject.s3-website.ap-south-1.amazonaws.com/)

[**https://ap-south-1.console.aws.amazon.com/s3/buckets/djsbucketproject?region=ap-south-1&bucketType=general&tab=properties**](https://ap-south-1.console.aws.amazon.com/s3/buckets/djsbucketproject?region=ap-south-1&bucketType=general&tab=properties)

[**https://www.youtube.com/channel/UCCktnahuRFYIBtNnKT5IYyg**](https://www.youtube.com/channel/UCCktnahuRFYIBtNnKT5IYyg)

[**https://ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#databases**](https://ap-south-1.console.aws.amazon.com/rds/home?region=ap-south-1#databases)**: (addiontal)**

[**https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html**](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html)

[**https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-tutorial.html**](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-tutorial.html)

[**https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ManageEC2SerialConsole**](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#ManageEC2SerialConsole)**:**

[**https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateTargetGroup:protocol=HTTP;vpc=vpc-0bd6f2985d7b9eb18**](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#CreateTargetGroup:protocol=HTTP;vpc=vpc-0bd6f2985d7b9eb18)

**database-1**

**djsprojectdb**

**djs19782**

arn:aws:elasticbeanstalk:ap-south-1:944346522085:application/DjsWebApplication

Master username

djs19782

Master password

djs19782

**Windows Instance Login**

DjsWindowsInstance (1)

%sLgAwV3d$Z?g)mg$7SCsf$X?=0@gQ!\*

**{**

**"Version": "2012-10-17",**

**"Id": "\_\_default\_policy\_ID",**

**"Statement": [**

**{**

**"Sid": "\_\_owner\_statement",**

**"Effect": "Allow",**

**"Principal": {**

**"AWS": "944346522085"**

**},**

**"Action": [**

**"SQS:\*"**

**],**

**"Resource": "arn:aws:sqs:ap-south-1:944346522085:Hello-lambda-**

**-----------------------------------------**

**{**

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Allow",**

**"Action": [**

**"sts:AssumeRole"**

**],**

**"Principal": {**

**"Service": [**

**"lambda.amazonaws.com"**

**]**

**}**

**}**

**]**

**}**

**# This AWS SAM template has been generated from your function's configuration. If**

**# your function has one or more triggers, note that the AWS resources associated**

**# with these triggers aren't fully specified in this template and include**

**# placeholder values. Open this template in AWS Application Composer or your**

**# favorite IDE and modify it to specify a serverless application with other AWS**

**# resources.**

**AWSTemplateFormatVersion: '2010-09-09'**

**Transform: AWS::Serverless-2016-10-31**

**Description: An AWS Serverless Application Model template describing your function.**

**Resources:**

**STOPINSTANCE:**

**Type: AWS::Serverless::Function**

**Properties:**

**CodeUri: .**

**Description: ''**

**MemorySize: 128**

**Timeout: 3**

**Handler: index.handler**

**Runtime: nodejs20.x**

**Architectures:**

**- x86\_64**

**EphemeralStorage:**

**Size: 512**

**EventInvokeConfig:**

**MaximumEventAgeInSeconds: 21600**

**MaximumRetryAttempts: 2**

**PackageType: Zip**

**Policies:**

**- Statement:**

**- Sid: VisualEditor0**

**Effect: Allow**

**Action:**

**- ec2:StartInstances**

**- ec2:StopInstances**

**Resource: '\*'**

**SnapStart:**

**ApplyOn: None**

**RuntimeManagementConfig:**

**UpdateRuntimeOn: Auto**

**index.js**

**Index.js**

|  |
| --- |
| const AWS = require('aws-sdk'); |
|  |  |
|  | exports.handler = (event, context, callback) => { |
|  | const ec2 = new AWS.EC2({ region: event.instanceRegion }); |
|  |  |
|  | ec2.stopInstances({ InstanceIds: [event.instanceId] }).promise() |
|  | .then(() => callback(null, `Successfully stopped ${event.instanceId}`)) |
|  | .catch(err => callback(err)); |
|  | }; |

**const AWS** = **require('aws**-**sdk'); exports**.**handler** = async (**event**) => { **const ec2** = **new AWS**.**EC2**({ **region**: **event**.**instanceRegion });**

1. Take the AMI of the existing machine.
2. Copy the AMI to the new region.
3. Launch new machine from the AMI.

NOTE: You can't keep the existing public IP because AWS has different set of IP's for different regions. To overcome this create a public domain in Route53 and create a A record and change the value of A record to new public IP, use your DNS name instead of public IP everywhere.

[Share](https://stackoverflow.com/a/62099787)

Follow

answered May 30, 2020 at 8:25

[[](https://stackoverflow.com/users/7519440/deepanmurugan)](https://stackoverflow.com/users/7519440/deepanmurugan)

[deepanmurugan](https://stackoverflow.com/users/7519440/deepanmurugan)

**2,003**1414 silver badges1919 bronze badges

[Add a comment](https://stackoverflow.com/questions/62088892/how-can-we-change-aws-instances-region-from-us-east-n-virginia-us-east-1-to-a)

4

You'll need to take an image (AMI) of the instance in US-East-1 and copy the image to the target region (ap-south-1) and then launch the AMI in the ap-south-1 region.

From AWS console, do the following:

1. Go to EC2 console.
2. Clock 'Running instances'.
3. Find the instance you want to move. Click the check box for that instance.
4. If you want to move the instance, shut it down here, first, by clicking Actions->Instance State-Stop
5. Actions->Image->Create Image
6. Give a name, optionally a description.
7. If you didn't previously shutdown the instance, you have an option of whether to reboot the box when taking AMI.
8. Click 'Create Image'.
9. Wait for the image creation to complete, and you can see the new AMI in the the AMI page of the EC2 console.
10. In the left column of the EC2 console, go to 'AMIs'.
11. When you see the new AMI in the list, and it's available, click the checkbox to the left of the name.
12. Actions->Copy AMI
13. For Desination Region, selECT 'Asia Pacific (Mumbai)'.
14. Enter name, description, and whether you want the AMI in the destination region to be encrypted.
15. Click 'Copy AMI'.
16. Wait for copy to complete.
17. Switch to ap-south-1 region.
18. Find the AMI and select it.
19. click 'Launch Instance'.
20. Make your choices.
21. Wait for instance to launch.

You are getting this error because the file is set to private and you don't have the permission do download it. To do so, you must set a [Bucket Policy](https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html) according to the permissions you with to use.

If you want any user to be able to download bucket objects, you can set a policy such as:

{

"Version":"2012-10-17",

"Statement":[

{

"Sid":"PublicRead",

"Effect":"Allow",

"Principal": "\*",

"Action":["s3:GetObject"],

"Resource":["arn:aws:s3:::examplebucket/\*"]

}

]

}

{

    "Resources": {

        "BucketStackcf": {

            "Type": "AWS::S3::Bucket",

            "Properties": {

                "BucketName": {

                    "Fn::Sub": "${AWS::StackName}-bucketsta-${AWS::AccountId}"

                },

                "BucketEncryption": {

                    "ServerSideEncryptionConfiguration": [

                        {

                            "ServerSideEncryptionByDefault": {

                                "SSEAlgorithm": "aws:kms",

                                "KMSMasterKeyID": "alias/aws/s3"

                            }

                        }

AWS CloudFormation Sample Template LAMP\_Single\_Instance: Create a LAMP stack using a single EC2 instance and a local MySQL database for storage. This template demonstrates using the AWS CloudFormation bootstrap scripts to install the packages and files necessary to deploy the Apache web server, PHP and MySQL at instance launch time. \*\*WARNING\*\* This template creates an Amazon EC2 instance. You will be billed for the AWS resources used if you create a stack from this template.

**"Version": "2012-10-17",**

**"Statement": [**

**{**

**"Effect": "Allow",**

**"Action": "sts:AssumeRoleWithWebIdentity",**

**"Principal": {**

**"Federated": "graph.facebook.com"**

**},**

**"Condition": {**

**"StringEquals": {**

**"graph.facebook.com:app\_id": [**

**"Asasasas123"**

**]**

**}**

**}**

**}**

**]**

**}**

[**https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/GettingStarted.Walkthrough.html**](https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/GettingStarted.Walkthrough.html)

[**https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/appinsights-logs-and-metrics.html**](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/appinsights-logs-and-metrics.html)

[**https://resource-explorer.console.aws.amazon.com/resource-explorer/home?region=ap-south-1#/onboarding**](https://resource-explorer.console.aws.amazon.com/resource-explorer/home?region=ap-south-1#/onboarding)

[**https://aws.amazon.com/getting-started/hands-on/?amp;getting-started-all.q\_operator=AND&awsf.getting-started-category=\*all&trk=e1e67116-7cd7-4fc3-98dc-598cfb47b9ca&sc\_channel=em&mkt\_tok=MTEyLVRaTS03NjYAAAGTinZ1ddCfMy\_EG2S0wp4li8N1Q-r9Ujr3kBWr8fIJyUmO58dOlXL43c0T1YbMe1\_VuzmIq9nUhyAJw36i1MDtiqHzWrVIIqfPt54IvMaGOBzxmbRIYiIYpw&getting-started-all.sort-by=item.additionalFields.content-latest-publish-date&getting-started-all.sort-order=desc**](https://aws.amazon.com/getting-started/hands-on/?amp;getting-started-all.q_operator=AND&awsf.getting-started-category=*all&trk=e1e67116-7cd7-4fc3-98dc-598cfb47b9ca&sc_channel=em&mkt_tok=MTEyLVRaTS03NjYAAAGTinZ1ddCfMy_EG2S0wp4li8N1Q-r9Ujr3kBWr8fIJyUmO58dOlXL43c0T1YbMe1_VuzmIq9nUhyAJw36i1MDtiqHzWrVIIqfPt54IvMaGOBzxmbRIYiIYpw&getting-started-all.sort-by=item.additionalFields.content-latest-publish-date&getting-started-all.sort-order=desc)

AKIA5XX3QMHSUPUANXN7

**BUWzM0MFfyq/Y1UKHaDuJPfnbmBoxkCFrCrbiotK**

**944346522085**

[**https://944346522085.signin.aws.amazon.com/console**](https://944346522085.signin.aws.amazon.com/console)

| **ccess key** | **Secret access key** |
| --- | --- |
| AKIA5XX3QMHSXMWKBCFY | 6iW9AK7btCQsQWzT2xxWK093A22aF6NtILnM2oEP  **Hide** |

[**https://944346522085.signin.aws.amazon.com/console**](https://944346522085.signin.aws.amazon.com/console)

**Dharam**

**Djs#1978**

ttps://944346522085.signin.aws.amazon.com/console

**User people(Policy)**

**Roles Application**

**Policy ec2 instance, s3, lamba etc**

Role name

aws-elasticbeanstalk-service-role

Trusted entity

elasticbeanstalk.amazonaws.com

Permissions

**AWSElasticBeanstalkEnhancedHealth**

{

"Version": "2012-10-17",

"Statement": [

{

"Effect": "Allow",

"Action": [

"elasticloadbalancing:DescribeInstanceHealth",

"elasticloadbalancing:DescribeLoadBalancers",

"elasticloadbalancing:DescribeTargetHealth",

"ec2:DescribeInstances",

"ec2:DescribeInstanceStatus",

"ec2:GetConsoleOutput",

"ec2:AssociateAddress",

"ec2:DescribeAddresses",

"ec2:DescribeSecurityGroups",

"sqs:GetQueueAttributes",

"sqs:GetQueueUrl",

"autoscaling:DescribeAutoScalingGroups",

"autoscaling:DescribeAutoScalingInstances",

"autoscaling:DescribeScalingActivities",

"autoscaling:DescribeNotificationConfigurations",

"sns:Publish"

],

"Resource": [

"\*"

]

}

]

[**https://github.com/shadman/aws-pipeline-sample**](https://github.com/shadman/aws-pipeline-sample)

[**https://github.com/ajit-dherange/AWS\_Codepipleline\_Tutorial**](https://github.com/ajit-dherange/AWS_Codepipleline_Tutorial)

**https://github.com/search?q=shadman&type=repositories**

**AWS-Codepipleline-s3-linux**

<https://api.github.com/repos/babbus78/aws-codepipeline-s3-codedeploy-linux/git/commits/8be52cbae505bfa39bd17845c336ac55a4e3027e>

**{**

**"NotificationRules": [**

**{**

**"Id": "dc82df7a-EXAMPLE",**

**"Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/dc82df7a-EXAMPLE"**

**},**

**{**

**"Id": "8d1f0983-EXAMPLE",**

**"Arn": "arn:aws:codestar-notifications:us-east-1:123456789012:notificationrule/8d1f0983-EXAMPLE"**

**}**

**]**

**}**

Mostly this happens when you try to enable the ufw. So, follow the below actions to gain access again over SSH:

1. Go to your AWS EC2 console
2. Select your instance that is not able to connect
3. Stop your instance
4. Go to Actions -> Instance Settings -> Edit User Data
5. Add this user data in user data.

Content-Type: multipart/mixed; boundary="//"

MIME-Version: 1.0

--//

Content-Type: text/cloud-config; charset="us-ascii"

MIME-Version: 1.0

Content-Transfer-Encoding: 7bit

Content-Disposition: attachment; filename="cloud-config.txt"

#cloud-config

cloud\_final\_modules:

- [scripts-user, always]

--//

Content-Type: text/x-shellscript; charset="us-ascii"

MIME-Version: 1.0

Content-Transfer-Encoding: 7bit

Content-Disposition: attachment; filename="userdata.txt"

#!/bin/bash

ufw disable

iptables -L

iptables -F

--//

1. Go to the CloudWatch Logs service in the AWS Management Console
2. Under "Log Groups", click "Create log group"
3. For "Log group name", enter "/aws/lambda/awslambda1"
4. Click "Create log group"
5. After the log group is created, retry the action that caused the error

{

"Version": "2012-10-17",

"Statement": [

{

"Sid": "BucketAccess",

"Action": [

"s3:Get\*",

"s3:List\*",

"s3:PutObject"

],

"Effect": "Allow",

"Resource": [

"arn:aws:s3:::elasticbeanstalk-\*",

"arn:aws:s3:::elasticbeanstalk-\*/\*"

]

},

{



* 1

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Name** | | **Security group rule ID** | | | | **IP version** | | | | **Type** | | **Protocol** | **Port range** | **Source** | **Description** |
| **Name** | **Security group rule ID** | | **IP version** | **Type** | **Protocol** | | **Port range** | **Source** | **Description** | |
| – | sgr-08a9d49e37aaadb63 | | IPv4 | HTTP | TCP | | 80 | 0.0.0.0/0 | – | |
| – | sgr-0090837ad172c5b6e | | IPv4 | SSH | TCP | | 22 | 0.0.0.0/0 | – | |

[**https://www.coursera.org/learn/create-lead-generation-messenger-chatbot-using-chatfuel/ungradedLab/57OFi/create-a-lead-generation-messenger-chatbot-using-chatfuel/lab?path=%2F**](https://www.coursera.org/learn/create-lead-generation-messenger-chatbot-using-chatfuel/ungradedLab/57OFi/create-a-lead-generation-messenger-chatbot-using-chatfuel/lab?path=%2F)

## Associate Cloud Engineer

**Access key**

**AKIA5XX3QMHST5WFB72B**

**Secret access key**

**gjNta+XYDHtICPHYdwotZL8NKegHD36D+ht6fcQ1**