

AWS LAB1:

1- Create aws account and set billing alarm

The image displays two screenshots of the AWS Management Console. The top screenshot shows the 'Console Home' dashboard with a sidebar on the left containing 'Recently visited' services like IAM, AWS Budgets, AWS Cost Explorer, VPC, EC2, DynamoDB, and RDS. The main area features a 'Welcome to AWS' section with links for 'Getting started with AWS', 'Training and certification', and 'What's new with AWS?'. Below this, there are sections for 'AWS Health' and 'Cost and usage', with a message stating 'No cost and usage data to show'. The bottom screenshot shows the 'Billing Preferences' page. The left sidebar lists various account management options, with 'Billing preferences' highlighted. The main content area includes sections for 'Billing Preferences' (with a checkbox for 'Receive PDF Invoice By Email'), 'Cost Management Preferences' (with checkboxes for 'Receive Free Tier Usage Alerts' and 'Receive Billing Alerts'), and 'Detailed Billing Reports [Legacy]'. A 'Save preferences' button is located at the bottom of the main content area. The footer of both screenshots includes a 'Feedback' link, a language selection prompt, and copyright information for Amazon Web Services, Inc.

Console Home

Reset to default layout Add widgets

Recently visited

- IAM
- AWS Budgets
- AWS Cost Explorer
- VPC
- EC2
- DynamoDB
- RDS

View all services

Welcome to AWS

- Getting started with AWS**
Learn the fundamentals and find valuable information to get the most out of AWS.
- Training and certification**
Learn from AWS experts and advance your skills and knowledge.
- What's new with AWS?**
Discover new AWS services, features, and Regions.

AWS Health

Open issues

Cost and usage

No cost and usage data to show

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Billing Preferences

☐ **Receive PDF Invoice By Email**
Turn on this feature to receive a PDF version of your invoice by email. Invoices are generally available within the first three days of the month.

Cost Management Preferences

☒ **Receive Free Tier Usage Alerts**
Turn on this feature to receive email alerts when your AWS service usage is approaching, or has exceeded, the AWS Free Tier usage limits. If you wish to receive these alerts at an email address that is not the primary email address associated with this account, please specify the email address below.

Email Address:

☒ **Receive Billing Alerts**
Turn on this feature to monitor your AWS usage charges and recurring fees automatically, making it easier to track and manage your spending on AWS. You can set up billing alerts to receive email notifications when your charges reach a specified threshold. Once enabled, this preference cannot be disabled. [Manage Billing Alerts](#) or [try the new budgets feature!](#)

Detailed Billing Reports [Legacy]

Save preferences

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

← → ↺

https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:1-(namespace--AWS%2FBilling)

☆

🔔

🔍

📄

📌

🔔

N. Virginia

AmrGomaa

aws

Services

Search

[Alt+S]

CloudWatch

×

Favorites and recents

Dashboards

Alarms

In alarm

All alarms

Billing

Logs

Metrics

X-Ray traces

Events

Application monitoring

Insights

Settings

Getting Started

CloudWatch > Alarms

Billing alarms (0)

☐ Hide Auto Scaling alarms

Clear selection

↺

Create composite alarm

Actions

Create alarm

Search

Any state

Any type

Any actions ...

< 1 >

🔍

	Name	State	Last state update	Conditions	Actions
<div>Amazon CloudWatch can help you monitor the charges on your AWS bill by sending you email alerts when charges exceed a threshold you define.</div> <div>Once you update your preferences in the Account Billing console, you will begin receiving Amazon CloudWatch metrics that reflect your month-to-date AWS charges. Then, you can create a billing alarm by specifying a spending threshold and an e-mail address to notify. Learn more about billing alerts</div> <div>You get 10 free alarms and 1,000 free e-mail notifications each month as part of the AWS Free Tier</div> <div>Create alarm</div>					

aws

Services

Search

[Alt+S]

EstimatedCharges

Maximum

Period

6 hours

Conditions

Threshold type

☒ Static

Use a value as a threshold

☐ Anomaly detection

Use a band as a threshold

Whenever EstimatedCharges is...

Define the alarm condition.

☒ Greater

> threshold

☐ Greater/Equal

>= threshold

☐ Lower/Equal

<= threshold

☐ Lower

< threshold

than...

Define the threshold value.

5

USD

Must be a number

Additional configuration

Cancel

Next

conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Notification

Alarm state trigger

Define the alarm state that will trigger this action.

☒ In alarm
The metric or expression is outside of the defined threshold.

☐ OK
The metric or expression is within the defined threshold.

☐ Insufficient data
The alarm has just started or not enough data is available.

[Remove](#)

Send a notification to the following SNS topic

Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ Select an existing SNS topic

☐ Create new topic

☐ Use topic ARN to notify other accounts

Send a notification to...

Only email lists for this account are available.

Email (endpoints)

amr.gomaa966@gmail.com - [View in SNS Console](#)

[Add notification](#)

Auto Scaling action

Feedback

Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)

[Terms](#)

[Cookie preferences](#)

CloudWatch > Alarms > Create alarm

Step 1
Specify metric and conditions

Step 2
Configure actions

Step 3
Add name and description

Step 4
Preview and create

Preview and create

Step 1: Specify metric and conditions

[Edit](#)

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 6 hours.

6

5.5

5

4.5

4

12/10

12/12

12/14

12/16

☒ EstimatedCharges

Namespace
AWS/Billing

Metric name
EstimatedCharges

Currency
USD

Statistic
Maximum

Period
6 hours

Feedback

Looking for language selection? Find it in the new [Unified Settings](#)

© 2022, Amazon Web Services, Inc. or its affiliates.

[Privacy](#)

[Terms](#)

[Cookie preferences](#)

aws

Services

Search

[Alt+S]

N. Virginia

AmrGomaa

CloudWatch

Favorites and recents

Dashboards

Alarms

In alarm

All alarms

Billing

Logs

Metrics

X-Ray traces

Events

Application monitoring

Insights

Settings

Getting Started

Successfully created alarm my_alarm.

View alarm

Some subscriptions are pending confirmation

Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed

View SNS Subscriptions

CloudWatch > Alarms

Billing alarms (1)

☐ Hide Auto Scaling alarms

Clear selection

Create composite alarm

Actions

Create alarm

Search

Any state

Any type

Any actions ...

< 1 >

<input type="checkbox"/>	Name	State	Last state update	Conditions	Actions
<input type="checkbox"/>	my_alarm	Insufficient data	2022-12-17 15:53:24	EstimatedCharges > 5 for 1 datapoints within 6 hours	Actions enabled

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

- create 2 groups one admin and one for development
- in the admin group it has admin permission , and in the development only access to s3

Identity and Access Management (IAM)

Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)

IAM > User groups > admin

admin

Delete

Edit

Summary

User group name

admin

Creation time

December 17, 2022, 14:26 (UTC+02:00)

ARN

arn:aws:iam::832675747098:group/admin

Users
Permissions
Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

< 1 >

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to AWS services and resources.

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Identity and Access Management (IAM)

Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)

IAM > User groups > development

development

Delete

Edit

Summary

User group name

development

Creation time

December 17, 2022, 14:28 (UTC+02:00)

ARN

arn:aws:iam::832675747098:group/development

Users
Permissions
Access Advisor

Permissions policies (1) Info

You can attach up to 10 managed policies.

< 1 >

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via the AWS Management Console.

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

- create admin-1 user console access and mfa enabled

This screenshot shows the 'Add user' wizard in the AWS IAM console, specifically the 'Set permissions' step. The user name 'admin-1' has been entered. The 'Select AWS access type' section has 'Password - AWS Management Console access' selected. The 'Console password' is set to 'Autogenerated password'. The 'Require password reset' checkbox is checked. At the bottom, there are 'Cancel' and 'Next: Permissions' buttons.

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

User name* admin-1

[Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

☐ Access key - Programmatic access
Enables an access key ID and secret access key for the AWS API, CLI, SDK, and other development tools.

☒ Password - AWS Management Console access
Enables a password that allows users to sign-in to the AWS Management Console.

Console password*

☒ Autogenerated password

☐ Custom password

Require password reset ☒ User must create a new password at next sign-in
Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

* Required

[Cancel](#) [Next: Permissions](#)

[Feedback](#) Looking for language selection? Find it in the new Unified Settings [\[?\]](#) © 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

This screenshot shows the 'Add user' wizard in the AWS IAM console, specifically the 'Set permissions' step. The 'Add user to group' button is highlighted. Below it, a table shows two groups: 'admin' with 'AdministratorAccess' policy and 'development' with 'AmazonS3FullAccess' policy. The 'admin' group is selected. At the bottom, there are 'Cancel', 'Previous', and 'Next: Tags' buttons.

ADD USER

1 2 3 4 5

Set permissions

[Add user to group](#) [Copy permissions from existing user](#) [Attach existing policies directly](#)

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

[Create group](#) [Refresh](#)

Search Showing 2 results

Group	Attached policies
<input checked="" type="checkbox"/> admin	AdministratorAccess
<input type="checkbox"/> development	AmazonS3FullAccess

Set permissions boundary

[Cancel](#) [Previous](#) [Next: Tags](#)

[Feedback](#) Looking for language selection? Find it in the new Unified Settings [\[?\]](#) © 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Add user

1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
admin1	console access	✕
Add new key		

You can add 49 more tags.

Cancel Previous Next: Review

Add user

1 2 3 4 5

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://632675747098.signin.aws.amazon.com/console>

Download .csv

	User	Password	Email login instructions
▶	admin-1	+Rl0naVBZj Pb Hide	Send email

Close

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

Access reports

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

IAM > Security credentials

My security credentials [Info](#)

Use this page to manage the credentials for your currently active user.

You don't have MFA assigned

As a security best practice, we recommend you assign MFA to your user.

Account details

User name

admin-1

AWS account ID

832675747098

AWS IAM credentials

AWS CodeCommit credentials

Console sign-in

Console sign-in link

new_user_credentials.csv - Notepad

File Edit View

User name,Password,Access key ID,Secret access key,Console login link
admin-1,+Rf6naVBZ[jpb{T,,,https://832675747098.signin.aws.amazon.com/console

Ln 3, Col 1 100% Windows (CRLF) UTF-8

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 1

Select MFA device

Step 2

Set up device

Select MFA device

Select MFA device [Info](#)

Select an MFA device to use, in addition to your username and password, whenever you need to authenticate.

Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.

Security Key

Authenticate using a code generated by touching a YubiKey or other supported FIDO security key.

Hardware TOTP token

Authenticate using a code generated by a hardware token.

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

Access reports

- Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

MFA device assigned

You can register up to 8 MFA devices of any combination of the currently supported MFA types with your AWS account root and IAM user. With multiple MFA devices, you only need one MFA device to sign in to the AWS console or create a session through the AWS CLI with that user.

IAM > Security credentials

My security credentials

Use this page to manage the credentials for your currently authenticated IAM user. To learn more about the types of AWS credentials, see [AWS Security Credentials](#).

Account details

User name

admin-1

User ARN

arn:aws:iam::832675747098:user/admin-1

AWS account ID

832675747098

Canonical user ID

f241c1fb39b7ac737f32c4850f2c0b361040dd98a3305cf1f378e428749d877d

AWS IAM credentials

AWS CodeCommit credentials

Amazon Keyspaces credentials

Console sign-in

Console sign-in link

https://832675747098.signin.aws.amazon.com/console

Console password

Enabled 13 minutes ago (2022-12-17 14:33 GMT+2)

Update console password

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Multi-factor authentication (MFA) (1)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Remove

Resync

Assign MFA device

	Device type	Identifier	Created on
<input type="radio"/>	Virtual	arn:aws:iam::832675747098:mfa/my-authenticator	Now

- and admin2-prog with cli access only and list all users and groups using it commands not console

The screenshot shows the 'Add user' wizard in the AWS IAM console. The top navigation bar includes the AWS logo, 'Services', a search bar, and the user 'admin-1 @ 8526-7574-7098'. The wizard has five steps, with step 1 'Set user details' selected. Below the step indicator, the section 'Set user details' is active. It contains a text input for 'User name*' with the value 'admin-2' and a blue button 'Add another user'. Below this is the 'Select AWS access type' section, which instructs the user on how to access AWS. It has two options: 'Access key - Programmatic access' (selected with a checkmark) and 'Password - AWS Management Console access' (unselected). The footer of the wizard shows a 'Cancel' button and a 'Next: Permissions' button.

aws Services Search [Alt+S] Global admin-1 @ 8526-7574-7098

ADD USER 1 2 3 4 5

Set user details

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

User name* admin-2

+ Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type* ☒ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☐ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required Cancel Next: Permissions

Feedback Looking for language selection? Find it in the new Unified Settings. © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the 'Add user' wizard in the AWS IAM console, step 2 'Set permissions'. The top navigation bar is the same as the previous screenshot. The wizard has five steps, with step 2 'Set permissions' selected. Below the step indicator, the section 'Set permissions' is active. It contains three buttons: 'Add user to group' (highlighted with a blue border), 'Copy permissions from existing user', and 'Attach existing policies directly'. Below these buttons is a text input for 'Add user to group' and a 'Create group' button. Below the text input is a table with two columns: 'Group' and 'Attached policies'. The table shows two results: 'admin' with 'AdministratorAccess' and 'development' with 'AmazonS3FullAccess'. The footer of the wizard shows a 'Cancel' button, a 'Previous' button, and a 'Next: Tags' button.

aws Services Search [Alt+S] Global admin-1 @ 8526-7574-7098

ADD USER 1 2 3 4 5

Set permissions

+ Add user to group Copy permissions from existing user Attach existing policies directly

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Add user to group

Create group Refresh

Q Search Showing 2 results

Group	Attached policies
<input checked="" type="checkbox"/> admin	AdministratorAccess
<input type="checkbox"/> development	AmazonS3FullAccess

Set permissions boundary

Cancel Previous Next: Tags

Feedback Looking for language selection? Find it in the new Unified Settings. © 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

aws

Services

Search

[Alt+S]

Global

admin-1 @ 8326-7574-7098

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	admin-2
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	admin

Tags

The new user will receive the following tag

Key	Value
admin-2	programmatic access

[Cancel](#) [Previous](#) [Create user](#)

[Feedback](#) [Looking for language selection? Find it in the new Unified Settings.](#) © 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

gomaa@localhost:~

File Edit View Search Terminal Help

[gomaa@localhost ~]\$ aws configure

AWS Access Key ID [None]: AKIA4DX2XSUNLY5JPDUG

I

```
gomaa@localhost:~  
File Edit View Search Terminal Help  
AWS Secret Access Key [None]: iScZqZb4GLetohp0S40a3y4lC0irAaVvKDtqwTjf  
Default region name [None]: Global  
Default output format [None]:  
[gomaa@localhost ~]$ aws iam list-users  
{  
  "Users": [  
    {  
      "Path": "/",  
      "UserName": "admin-1",  
      "UserId": "AIDA4DX2XSUNFGV7BH7P4",  
      "Arn": "arn:aws:iam::832675747098:user/admin-1",  
      "CreateDate": "2022-12-17T12:33:04Z",  
      "PasswordLastUsed": "2022-12-17T12:40:06Z"  
    },  
    {  
      "Path": "/",  
      "UserName": "admin-2",  
      "UserId": "AIDA4DX2XSUNJVV762YXAL",  
      "Arn": "arn:aws:iam::832675747098:user/admin-2",  
      "CreateDate": "2022-12-17T12:53:26Z"  
    }  
  ]  
}  
[gomaa@localhost ~]$
```

```
gomaa@localhost:~  
File Edit View Search Terminal Help  
Invalid choice: 'list--groups', maybe you meant:  
* list-groups  
[gomaa@localhost ~]$ aws iam list-groups  
{  
  "Groups": [  
    {  
      "Path": "/",  
      "GroupName": "admin",  
      "GroupId": "AGPA4DX2XSUNPLCTLPEQT",  
      "Arn": "arn:aws:iam::832675747098:group/admin",  
      "CreateDate": "2022-12-17T12:26:20Z"  
    },  
    {  
      "Path": "/",  
      "GroupName": "development",  
      "GroupId": "AGPA4DX2XSUNCMA3NU3SB",  
      "Arn": "arn:aws:iam::832675747098:group/development",  
      "CreateDate": "2022-12-17T12:28:37Z"  
    }  
  ]  
}  
[gomaa@localhost ~]$
```

- in the development group create user with name dev-user with programmatic and.
- Admin access try to access aws using it (take a screenshot from accessing ec2 and s3 console)
- Also access cli using it and try to get all users and groups using i

Services
Search
[Alt+S]
Global
admin-1 @ 8526-7574-7098

Add user
1 2 3 4 5

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

User name*
dev-user
Add another user

Select AWS access type
Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

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

Console password*
Autogenerated password
Custom password

* Required
Cancel
Next: Permissions

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Services
Search
[Alt+S]
Global
admin-1 @ 8526-7574-7098

Add user
1 2 3 4 5

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

Add user to group
Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Create group
Refresh

Search
Showing 2 results

Group
Attached policies

admin
AdministratorAccess

development
AmazonS3FullAccess

Set permissions boundary

Cancel
Previous
Next: Tags

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Add user

12345

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://832675747098.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key	Password	Email login instructions
	dev-user	AKIA4DX2XSUNNETZ2B46	***** Show	***** Show	Send email

Close

Console Home

Reset to default layout + Add widgets

Recently visited

- AWS Budgets

AWS Cost Explorer

VPC

EC2

DynamoDB

RDS

Cloud9
- Step Functions

IAM

[View all services](#)

Welcome to AWS

- Getting started with AWS

Learn the fundamentals and find valuable information to get the most out of AWS.
- Training and certification

Learn from AWS experts and advance your skills and knowledge.
- What's new with AWS?

Discover new AWS services, features, and Regions.

AWS Health

Cost and usage

aws

Services

Search

[Alt+S]

N. Virginia

dev-user @ 8326-7574-7098

New EC2 Experience

Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Resources

EC2 Global view

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running) API Error

Dedicated Hosts API Error

Elastic IPs API Error

Instances API Error

Key pairs API Error

Load balancers API Error

Placement groups API Error

Security groups API Error

Snapshots API Error

Volumes API Error

Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS using the AWS Launch Wizard for SQL Server. Learn more

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance

Migrate a server

Note: Your instances will launch in the US East (N. Virginia) Region

Service health

AWS Health Dashboard

Region

US East (N. Virginia)

Status

This service is operating normally

Account attributes

Supported platforms

An error occurred

An error occurred retrieving supported platforms

An error occurred

An error occurred checking for a default VPC

Settings

EBS encryption

Zones

EC2 Serial Console

Default credit specification

Console experiments

Explore AWS

Enable Best Price-Performance with AWS Graviton2

AWS Graviton2-powered EC2 instances enable up to

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search

[Alt+S]

Global

dev-user @ 8326-7574-7098

Storage

Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

How it works

aws

Introduction to Amazon S3

Copy link

aws

Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

Resources

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

aws

Services

Search

[Alt+S]

Global

dev-user @ 8326-7574-7098

Amazon S3 > Buckets > Create bucket

Create bucket

Info

Buckets are containers for data stored in S3. [Learn more](#)

General configuration

Bucket name

myawsbucket

Bucket name must be globally unique and must not contain spaces or uppercase letters. [See rules for bucket naming](#)

AWS Region

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

Copy settings from existing bucket - optional

Only the bucket settings in the following configuration are copied.

Choose bucket

Object Ownership

Info

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

☒ ACLs disabled (recommended)

All objects in this bucket are owned by this account.

☐ ACLs enabled

Objects in this bucket can be owned by other AWS

Feedback

Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

gomaa@localhost:~

File Edit View Search Terminal Help

[gomaa@localhost ~]\$ aws configure

AWS Access Key ID [*****PDUG]: AKIA4DX2XSUNETZ2B46

AWS Secret Access Key [*****wTjf]: Zp/9yJ+G5+Eelc0FYgVI7p6IBU4PpefKrzZguwuJ

Default region name [Global]:

Default output format [None]:

[gomaa@localhost ~]\$


```
gomaa@localhost:~/aws
File Edit View Search Terminal Help
[gomaa@localhost .aws]$ aws iam list-users
An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::832675747098:user/dev-user is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::832675747098:user/ because no identity-based policy allows the iam:ListUsers action
[gomaa@localhost .aws]$ aws iam list-groups
An error occurred (AccessDenied) when calling the ListGroups operation: User: arn:aws:iam::832675747098:user/dev-user is not authorized to perform: iam:ListGroups on resource: arn:aws:iam::832675747098:group/ because no identity-based policy allows the iam:ListGroups action
[gomaa@localhost .aws]$
```