

Objective: Create AWS account, set billing alarm, create 2 IAM groups (admin-developer), admin group has admin permissions, developer group only access to ec2, create admin-1 user with console access only and enable MFA & admin-2-prog user with cli access only and list all users and groups using commands, create dev-user with programmatic and console access and try to access EC2 and S3 from dev user.

Enable Billing Alerts

1. Navigate to **Billing** in the AWS Console.
2. Click on **Preferences**.
3. Enable **Receive Billing Alerts** and save changes.

Create a Billing Alarm

1. Go to the **CloudWatch** service in the AWS Console.
2. Navigate to **Alarms > Create Alarm**.
3. Select **Billing > Total Estimated Charge** as the metric.
4. Set the threshold (e.g., USD 10).
5. Configure notifications via SNS (e.g., email alerts).
6. Complete the alarm creation.

The screenshot shows the 'Create Alarm' wizard in the AWS CloudWatch console. The interface is divided into several sections:

- Configure actions:** A sidebar on the left with steps: Step 3 (Add name and description), Step 4 (Preview and create), and Step 5 (Configure actions).
- Metric:** A graph showing 'EstimatedCharges' over time. The y-axis ranges from 0 to 1. The x-axis shows dates from 11/29 to 12/05. A blue line represents the metric data.
- Conditions:** A section for defining the alarm condition. It includes:
 - Threshold type:** Radio buttons for 'Static' (selected) and 'Anomaly detection'.
 - Whenever EstimatedCharges is...:** Radio buttons for 'Greater' (selected), 'Greater/Equal', 'Lower/Equal', and 'Lower'.
 - than...:** A text input field with '10' and a dropdown for 'USD'.
- Additional configuration:** A section for further settings, currently collapsed.

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

Configure actions

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

☒ In alarm
This 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.

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...
Select an SNS topic.
Only topics belonging to this account are listed here. All persons and applications subscribed to the selected topic will receive notifications.

Add notification

Lambda action
Add Lambda action

Auto Scaling action
Add Auto Scaling action

EC2 action
This action is only available for EC2 Per Instance Metrics.
Add EC2 action

Create user: admin-1

User details

User name

admin-1

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ **Provide user access to the AWS Management Console - optional**
If you're providing console access to a person, it's a **best practice** to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

☒ **Specify a user in Identity Center - Recommended**
We recommend that you use Identity Center to provide console access to a person. With Identity Center you can centrally manage user access to their AWS accounts and cloud applications.

Attach user to group admin-1 to admin

Review and create

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

User details

User name admin-1	Console password type Custom password	Require password reset Yes
-----------------------------	---	--------------------------------------

Permissions summary

< 1 >

Name	Type	Used as
admin	Group	Permissions group
IAMUserChangePassword	AWS managed	Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag



You can add up to 50 more tags.

Cancel

Previous

Create user

Change MFA:unable to enable:

Summary		
ARN  arn:aws:iam::160337832336:user/admin-1	Console access  Enabled without MFA	Access key 1 Create access key
Created December 05, 2024, 15:30 (UTC+02:00)	Last console sign-in  Never	

Select MFA device [Info](#)

MFA device name

Device name

This name will be used within the identifying ARN for this device.


google

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


MFA device

Device options


In addition to username and password, you will use this device to authenticate into your account.

- 

Passkey or security key

Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.
- 

Authenticator app

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

Hardware TOTP token

Authenticate using a code generated by

Create admin-2-prog

admin-2-prog

Info

Delete

Summary

ARN
arn:aws:iam:160337832336:user/admin-2-prog

Created
December 05, 2024, 15:46 (UTC+02:00)

Console access
Disabled

Last console sign-in
-

Access key 1
AKIASKVHBF53OKT6H - Active
Never used. Created today.

Access key 2
Create access key

Permissions

Groups
(1)

Tags
(1)

Security credentials

Last Accessed

Console sign-in

Enable console access

Console sign-in link
https://160337832336.signin.aws.amazon.com/console

Console password
Not enabled

Multi-factor authentication (MFA) (0)

Remove Resync Assign MFA device

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

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			

Assign MFA device

Access keys (1)

Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

AKIASKVHBF53OKT6H

Description
ivovle

Last used
None

Status
Active

Created
Now

Actions

Access key best practices & alternatives

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.

Local code

You plan to use this access key to enable application code in a local development environment to access your AWS account.

Application running on an AWS compute service

List username & group by AWS CLI

```
: \Users\admin>aws configure
AWS Access Key ID [None]: AKIASKVHBF530KT6H
AWS Secret Access Key [None]: bnDKGfOnmMawaZPFuHhOeVX3lz99rWE/LBxxYVRf
default region name [None]:
default output format [None]:
```

```
: \Users\admin>aws iam list-users
```

```
    "Users": [
```

```
: \Users\admin>aws iam list-users
```

```
    "Users": [
      {
        "Path": "/",
        "UserName": "abdallah",
        "UserId": "AIDASKVHBF530KT6H",
        "Arn": "arn:aws:iam::160337832336:user/abdallah",
        "CreateDate": "2024-11-24T21:10:43+00:00",
        "PasswordLastUsed": "2024-12-05T12:40:23+00:00"
      },
      {
        "Path": "/",
        "UserName": "admin-1",
        "UserId": "AIDASKVHBF530KT6H",
        "Arn": "arn:aws:iam::160337832336:user/admin-1",
        "CreateDate": "2024-12-05T13:30:51+00:00"
      },
      {
        "Path": "/",
        "UserName": "admin-2-p",
        "UserId": "AIDASKVHBF530KT6H",
        "Arn": "arn:aws:iam::160337832336:user/admin-2-p",
        "CreateDate": "2024-12-05T13:50:08+00:00"
      },
      {
        "Path": "/",
        "UserName": "admin-2-prog",
        "UserId": "AIDASKVHBF530KT6H",
        "Arn": "arn:aws:iam::160337832336:user/admin-2-prog",
```

Create dev-user

User details

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

☒ **Provide user access to the AWS Management Console - *optional***

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

Are you providing console access to a person?

User type

☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☒ Autogenerated password

dev-user

Info

Delete

Summary

ARN
arn:aws:iam::160337832336:user/dev-user

Created
December 05, 2024, 16:13 (UTC+02:00)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
AKIA5KVHBFIIQ6Z6LLA - Active
Never used. Created today.

Access key 2
Create access key

Permissions

Groups
(1)

Tags
(1)

Security credentials

Last Accessed

Console sign-in

Manage console access

Console sign-in link
http://160337832336.signin.aws.amazon.com/console

Console password
Updated 6 minutes ago (2024-12-05 16:13 GMT+2)

Last console sign-in
Never

Multi-factor authentication (MFA) (0)

Remove Resync Assign MFA device

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](#)

Type

Identifier

Certifications

Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

Access keys (1)

Create access key

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

AKIA5KVHBFIIQ6Z6LLA

Actions

Description
dev

Status
Active

Last used
None

Created
Now

Last used region
N/A

Last used service
N/A