

1-) create aws account and set billing alarm

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

Specify metric and conditions

Metric Edit

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

No unit: 2

Namespace: AWS/Billing

Metric name: EstimatedCharges

Currency: USD

Statistic: Minimum

Period: 1 day

Warning! Your billing alarm may be set up incorrectly. To make it work as expected please set "Period" to 6 hours, "Statistic" to Maximum and set alarm to trigger on 1 consecutive period.

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:
1 USD
Must be a number

► Additional configuration

Cancel **Next**

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 Remove

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.

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...

Default_CloudWatch_Alarms_Topic

Default_CloudWatch_Alarms_Topic

khaledalaa58@yahoo.com - [View in SNS Console](#)

Add notification

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

Add name and description

Name and description

Alarm name
billing alert email

Alarm description - optional [View formatting guidelines](#)

EditPreview

This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

Cancel

Previous

Next

CloudWatch

Successfully created alarm billing alert email. [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 >

Name	State	Last state update	Conditions	Actions
billing alert email	Insufficient data	2023-05-30 21:21:38	EstimatedCharges > 1 for 1 datapoints within 1 day	Actions enabled Warning

Or

Choose budget type [Info](#)

Budget setup

☒ Use a template (simplified)

Use the recommended configurations. You can change some configuration options after the budget is created.

☐ Customize (advanced)

Customize a budget to set parameters specific to your use case. You can customize the time period, the start month, and specific account

Templates - *new*

Choose a template that best matches your use case.

☒ Zero spend budget

Create a budget that notifies you once your spending exceeds \$0.01 which is above the AWS Free Tier limits.

☐ Monthly cost budget

Create a monthly budget that notifies you if exceed, or are forecasted to exceed, the budget amount.

☐ Daily Savings Plans coverage budget

Create a coverage budget for your Savings Plans that notifies you when you fall below the defined target.

☐ Daily reservation utilization budget

Create a utilization budget for your reservation that notifies you when you fall below the defined target.

Zero spend budget - Template

Budget name

Provide a descriptive name for this budget.

alert email for budget

Names must be between 1-100 characters.

Email recipients

Specify the email recipients you want to notify when the threshold has exceeded.

khaledalaa58@yahoo.com

[AWS Billing](#) > [Budgets](#) > [Overview](#)

Overview [Info](#)

Budgets (1) info

Download CSV

Actions

Create budget

Find a budget

Show all budgets

<input type="checkbox"/>	Name	▲	Thresholds	▼	Budget	Amount used	Forecasted amount	Current vs. budgeted	▼	Forecasted vs. budgeted
<input type="checkbox"/>	alert email for budget		OK			\$1.00	\$0.00	-	<div><div></div></div>	0.00%

2-)

Create 2 groups one admin and one for development

IAM > User groups

User groups (2) [Info](#)
A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

<input type="checkbox"/>	Group name	Users	Permissions	Creation time
<input type="checkbox"/>	admin	2	Defined	1 hour ago
<input type="checkbox"/>	development	1	Defined	1 hour ago

Create 1 user console and 1 user prog in admin group

User _ cons in admin group

ARN
[arn:aws:iam::268138953875:user:user_cons](#)

Created
May 30, 2023, 21:27 (UTC+03:00)

Console access
Enabled with MFA

Last console sign-in
Never

Access key 1
Not enabled

Access key 2
Not enabled

Permissions | Groups | Tags | **Security credentials** | Access Advisor

Console sign-in [Manage console sign-in](#)
Console sign-in link
<https://268138953875.signin.aws.amazon.com/console>
Console password
Updated 1 hour ago (2023-05-30 21:27 GMT+3)
Last console sign-in
Never

Multi-factor authentication (MFA) (1) [Remove](#) [Resync](#) [Assign](#)
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](#)

Device type	Identifier	Created on
<input type="radio"/> Virtual	arn:aws:iam::268138953875:mfa/user_cons	1 hour ago

Access keys (0) [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](#)

No access keys
As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

User _prog in admin group

Summary

ARN
arn:aws:iam::268138953875:user/user_prog

Created
May 30, 2023, 21:27 (UTC+05:00)

Console access
Disabled

Last console sign-in
-

Access key 1
AKIAT435TXSJ6UHMUXZD - Active
Never used. Created today.

Access key 2
Not enabled

Permissions

Groups

Tags

Security credentials

Access Advisor

Console sign-in Enable console access

Console sign-in link
<https://268138953875.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 3 MFA devices assigned. [Learn more](#)

Device type	Identifier	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](#)

AKIAT435TXSJ6UHMUXZD		Actions
Description -	Status Active	
Last used None	Created 1 hour ago	
Last used region N/A	Last used service N/A	

SSH public keys for AWS CodeCommit (0) Actions Upload SSH public key
Use SSH public keys to authenticate access to AWS CodeCommit repositories. You can have a maximum of five SSH public keys (active or inactive) at a time. [Learn more](#)

SSH Key ID	Unloaded	Status
------------	----------	--------

development group create user with name dev-user with programmatic and console access then try to access aws using it (take a screenshot from accessing ec2 and s3 console)

dev-user Delete

Summary

ARN
arn:aws:iam::268138953875:user/dev-user

Created
May 30, 2023, 21:37 (UTC+05:00)

Console access
Enabled without MFA

Last console sign-in
Never

Access key 1
AKIAT435TXSJZGNVWBO - Active
Never used. Created today.

Access key 2
Not enabled

Permissions

Groups

Tags

Security credentials

Access Advisor

Console sign-in Manage console access

Console sign-in link
<https://268138953875.signin.aws.amazon.com/console>

Console password
Updated 1 hour ago (2023-05-30 21:37 GMT+05)
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 3 MFA devices assigned. [Learn more](#)

Device type	Identifier	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](#)

AKIAT435TXSJZGNVWBO		Actions
Description -	Status Active	
Last used None	Created 1 hour ago	
Last used region N/A	Last used service N/A	

Specify permissions [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor

[Visual](#)[JSON](#)[Actions](#) ▼

► S3

[Allow](#) 3 Actions

► EC2

[Allow](#) 3 Actions[+ Add more permissions](#)

🛡️ Security: 0 ❌ Errors: 0 ⚠️ Warnings: 0 💡 Suggestions: 0

[Cancel](#)[Next](#)

User-prog in admin group with cli access only and list all users and groups using commands
not console

```
Default output format [None]:
[root@khaled-o4 ~]# aws iam list-users
{
  "Users": [
    {
      "Path": "/",
      "UserName": "dev-user",
      "UserId": "AIDAT43STXSJTLQT05P6Z",
      "Arn": "arn:aws:iam::268138953875:user/dev-user",
      "CreateDate": "2023-05-30T18:37:05Z"
    },
    {
      "Path": "/",
      "UserName": "user_cons",
      "UserId": "AIDAT43STXSJ730WZPTBP",
      "Arn": "arn:aws:iam::268138953875:user/user_cons",
      "CreateDate": "2023-05-30T18:27:36Z"
    },
    {
      "Path": "/",
      "UserName": "user_prog",
      "UserId": "AIDAT43STXSJ57NGZKVL6",
      "Arn": "arn:aws:iam::268138953875:user/user_prog",
      "CreateDate": "2023-05-30T18:27:57Z"
    }
  ]
}
[root@khaled-o4 ~]# aws iam list-groups
{
  "Groups": [
    {
      "Path": "/",
      "GroupName": "admin",
      "GroupId": "AGPAT43STXSJYIIX3QJA4",
      "Arn": "arn:aws:iam::268138953875:group/admin",
      "CreateDate": "2023-05-30T18:35:56Z"
    },
    {
      "Path": "/",
      "GroupName": "development",
      "GroupId": "AGPAT43STXSJQ7KWKTOIC",
      "Arn": "arn:aws:iam::268138953875:group/development",
      "CreateDate": "2023-05-30T18:39:32Z"
    }
  ]
}
[root@khaled-o4 ~]#
```

Also access cli using dev-user and try to get all users and groups using it

```
[root@khaled-o4 ~]#
[root@khaled-o4 ~]# aws iam list-groups
An error occurred (AccessDenied) when calling the ListGroups operation: User: arn:aws:iam::268138953875:user/dev-user is not authorized to perform: iam:ListGroups on resource: arn:aws:iam::268138953875:group/ because no identity-based policy allows the iam:ListGroups action
[root@khaled-o4 ~]# aws iam list-users
An error occurred (AccessDenied) when calling the ListUsers operation: User: arn:aws:iam::268138953875:user/dev-user is not authorized to perform: iam:ListUsers on resource: arn:aws:iam::268138953875:user/ because no identity-based policy allows the iam:ListUsers action
[root@khaled-o4 ~]#
```