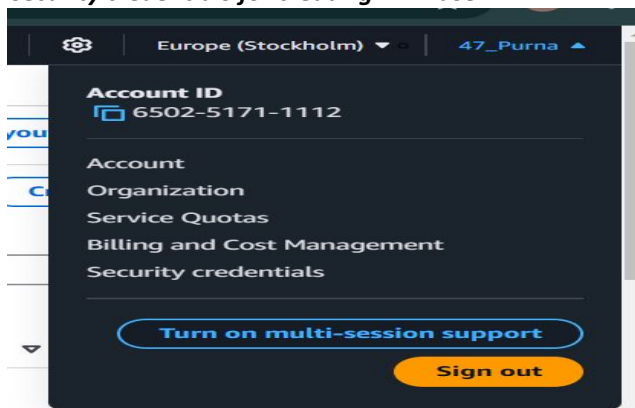


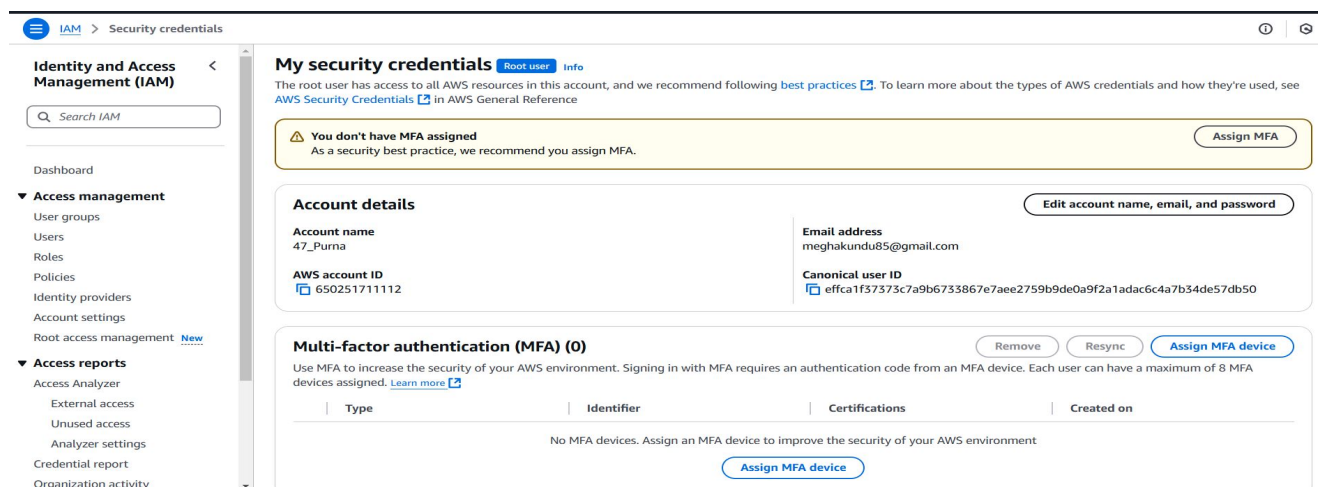
Assignment :- 2

Title :- Create MFA for authentication.

Step 1:- At first Go to security credentials for creating MFA user.



Step 2:- Then Click on assign MFA for create an MFA code.



Step 3: Then set the device name like PK_MFA and select the MFA device option like Authentication app.

Select MFA device [Info](#)

MFA device name

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


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 Hardware TOTP token or other hardware devices.

Step 4: Then scan the QR code in Google authentication app and type two consecutive codes for security reasons.

Set up device [Info](#)

Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#)

2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key. [Show secret key](#)

3

Type two consecutive MFA codes below

Enter a code from your virtual app below

912168

Wait 30 seconds, and enter a second code entry.

394152

[Cancel](#)

[Previous](#)

[Add MFA](#)

Step 5: The MFA is created successfully.

Account details

Edit account name, email, and password

Account name
47_Purna

AWS account ID
650251711112

Email address
meghakundu85@gmail.com

Canonical user ID
effca1f37373c7a9b6733867e7aee2759b9de0a9f2a1adac6c4a7b34de57db50

Multi-factor authentication (MFA) (1)

[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
<input type="radio"/> Virtual	arn:aws:iam::650251711112:mfa/PK_MFA	Not Applicable	Sun Jan 26 2025

Step 6: Then sign out. The next step is log in using root user then give the email id and password for login, and click the next button.

Sign in

☒ **Root user**
Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ **IAM user**
User within an account that performs daily tasks. [Learn more](#)

Root user email address

[Next](#)

Step 7: Then provide the multi factor authentication code which is provided by the authenticator app.

Multi-factor authentication

Your account is secured using multi-factor authentication (MFA). To finish signing in, turn on or view your MFA device and type the authentication code below.

Email address: meghakundu85@gmail.com

MFA code

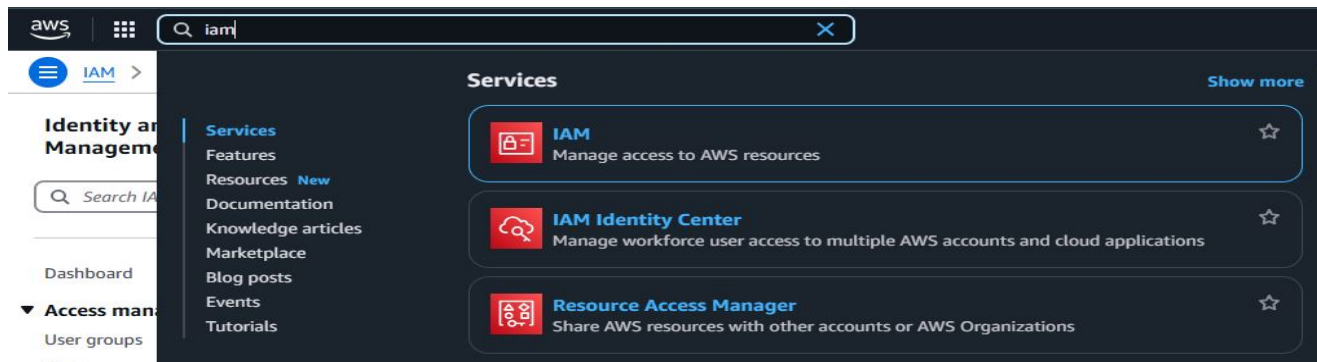
257764

[Submit](#)

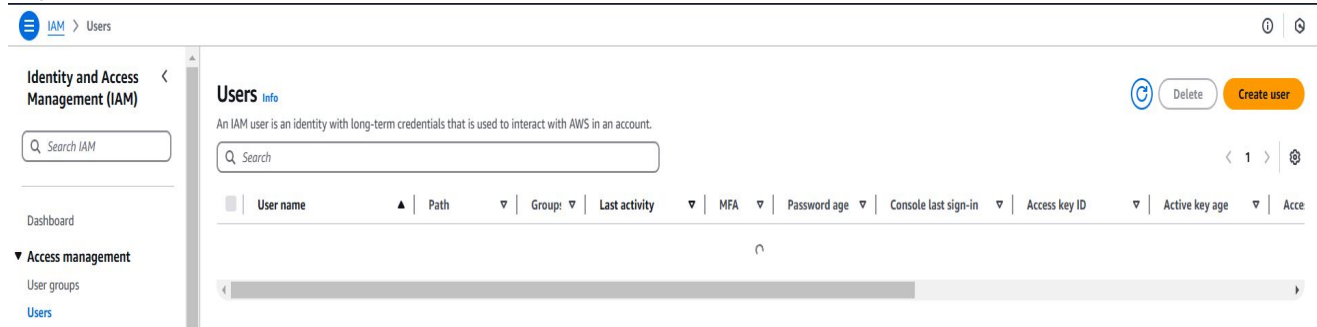
Assignment :- 3

Title :- Create IAM user and give full access to s3.

Step 1: From the search bar search IAM for create and IAM user.



Step 2: Go to user and click on create user.



Step 3 : Select user name and click on check box. Click on custom password and create your own password .And go next.

Step 1
Step 2
Step 3
Step 4

Specify user details

User details

User name

PK_IAM

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

You can view the password after you create the user.

☒ Custom password

Enter a custom password for the user.

CSEDS_047

Must be at least 8 characters long

Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols !@#\$%^&*()_+- (hyphen) = [] { } ' .

☒ Show password

☒ Users must create a new password at next sign-in - Recommended

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user.

Learn more

Cancel Next

Step 4 : Click on Next.

- Step 1
Specify user details
- Step 2
Set permissions
- Step 3
Review and create
- Step 4
Retrieve password

Set permissions

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](#)

Permissions options

☒ Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

☐ Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

☐ Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Get started with groups

Create a group and select policies to attach to the group. We recommend using groups to manage user permissions by job function, AWS service access, or custom permissions.

[Learn more](#)

Create group

► Set permissions boundary - optional

Cancel

Previous

Next

Step 5:click on create user .

- Step 1
Specify user details
- Step 2
Set permissions
- Step 3
Review and create
- Step 4
Retrieve password

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
PK_IAM

Console password type
Custom password

Require password reset
Yes

Permissions summary

< 1 >

Name

▲

Type

▼

Used as

▼

[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

Step 6: User is created successfully and download the csv file.

🟢 User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

View user

×

- Step 1
Specify user details
- Step 2
Set permissions
- Step 3
Review and create
- Step 4
Retrieve password

Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Email sign-in instructions

Console sign-in URL

<https://65025171112.signin.aws.amazon.com/console>

User name

PK_IAM

Console password

***** Show

Cancel

Download .csv file

Return to users list

Step 7:log in again using IAM code. Give the password and IAM user name and sign in again.

IAM user sign in ⓘ

Account ID (12 digits) or account alias

IAM username

Password


☒ Show Password [Having trouble?](#)

Sign in

Amazon Lightsail

Lightsail is the easiest way to get started on AWS

[Learn more »](#)



Step 8:Go to policies and click on AmazonS3FullAccess for giving the access of S3.From the action button click on attach.

us-east-1.console.aws.amazon.com/iam/home?region=eu-north-1#/policies

Search [Alt+S]

Incognito

Global 47_Purna

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles
- Policies**
- Identity providers

Policies (1/1319) ⓘ

A policy is an object in AWS that defines permissions.

Filter by Type

Q s3 All types 16 matches

	Policy name	Type	Used as	Description
<input type="radio"/>	AmazonDMSRedshiftS3Role	AWS managed	None	Provides access to manage S3 settings for ...
<input checked="" type="radio"/>	AmazonS3FullAccess	AWS managed	None	Provides full access to all buckets via the A...
<input type="radio"/>	AmazonS3ObjectLambdaExecutionRolePolicy	AWS managed	None	Provides AWS Lambda functions permisso...
<input type="radio"/>	AmazonS3OutpostsFullAccess	AWS managed	None	Provides full access to Amazon S3 on Out...
<input type="radio"/>	AmazonS3OutpostsReadOnlyAccess	AWS managed	None	Provides read only access to Amazon S3 o...

Actions Attach Detach Delete Create policy

Step 9:Now click on attach policy and the policy is attached successfully and the access of S3 is granted.

Attach as a permissions policy

To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

IAM Entities (1/1)

Entities are IAM users, user groups and roles.

Search

Filter by Entity type

All types

☒ Entity name

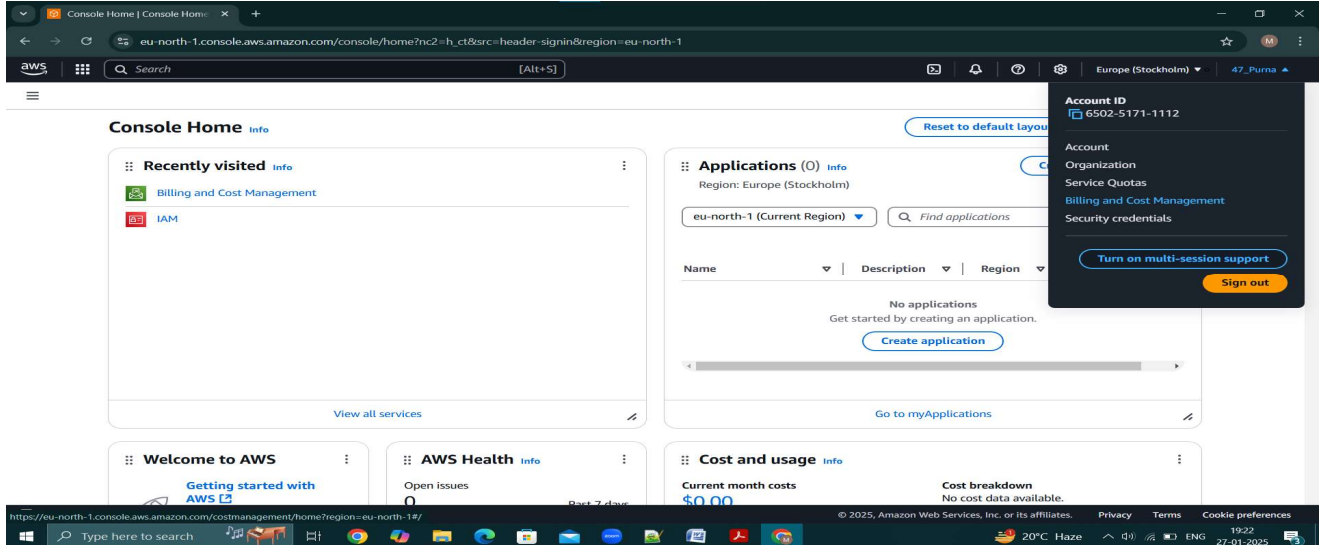
	Entity name	Entity type
<input checked="" type="checkbox"/>	PK_IAM	IAM Users

[Cancel](#) [Attach policy](#)

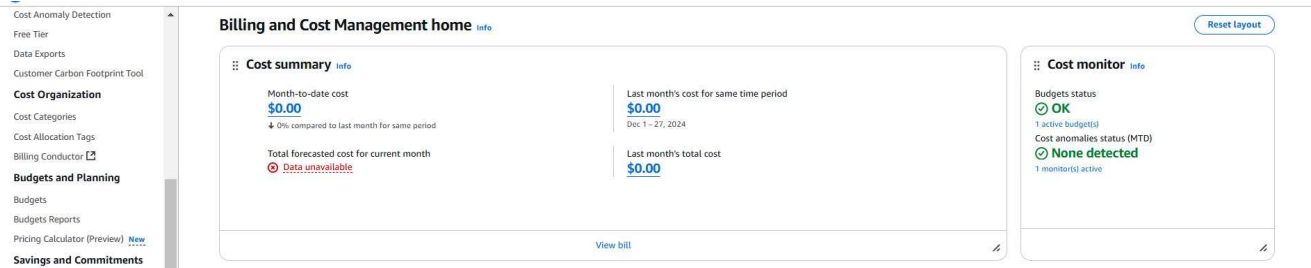
Assignment :- 1

Title: Configure a budget in AWS.

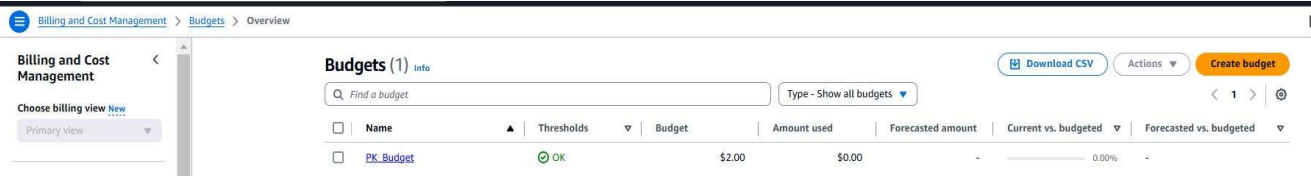
Step 1 : After creating a aws account, In the AWS Console, search for and open **Billing and Cost Management**.



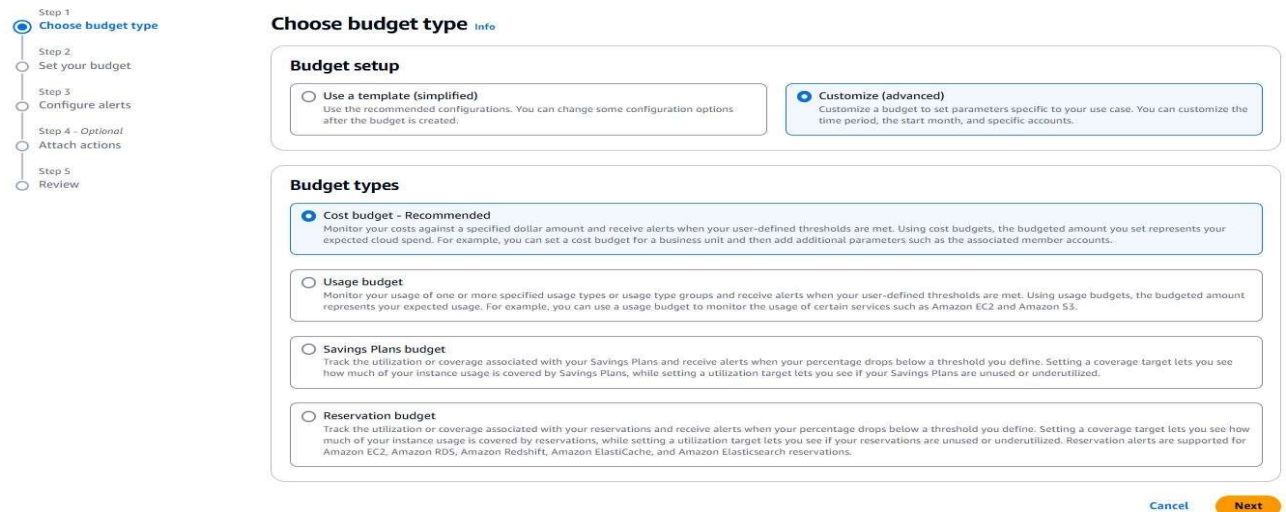
Step 2: Navigate to the **Budgets** section in the left-hand menu.



Step 3: Select on the create budget option.



Step 4: Choose budget type and click on customize budget option and click on 'Next'.



Step 5: Configure Budget Details as Budget Name, Period, set Budget Limits For cost budgets, enter the maximum amount you're willing to spend (e.g., \$200) and **Save** all the details.

Details

Budget name

Provide a descriptive name for this budget.

MP_Budget

Names must be between 1-100 characters.

Set budget amount

Period

Daily budgets do not support enabling forecasted alerts, or daily budget planning.

Monthly

Budget renewal type

☒ Recurring budget

Recurring budgets renew on the first day of every monthly billing period.

☐ Expiring budget

Expiring monthly budgets stop renewing at the end of the selected expiration month.

Start month

Jan

2025

Budgeting method

Fixed

Create a budget that tracks against a single monthly budgeted amount.

Enter your budgeted amount (\$)

Last month's cost: \$0.00

2.00

Budget scope

Add filtering and use advanced options to narrow the set of cost information tracked as part of this budget.

Cost Data

Jan 2024 - Jan 2025 (MTD) | Unblended costs



Actual cost Budget

[View in AWS Cost Explorer](#)

Alerts

No alerts configured.

Step 6: Create an alert and keep the threshold value as 80. means when the 80% of budget amount is used it gives a alert. Write email where the alert msg will be send. And click on next.

Your budgeted amount: \$2.00
To change your budgeted amount, go back to step 2.

Alert #1

Remove

Set alert threshold

Threshold

When should this alert be triggered?

80

% of budgeted amount

Trigger

How should this alert be triggered?

Actual

Summary: When your actual cost is greater than 80.00% (\$1.60) of your budgeted amount (\$2.00), the alert threshold will be exceeded.

Notification preferences

Select one or more notification preferences to receive alerts.

Email recipients

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

meghakundu85@gmail.com

Maximum number of email recipients is 10.

[Amazon SNS Alerts - Optional info](#)

[AWS Chatbot Alerts](#)

[+ Add alert threshold](#)

Cancel

Previous

Next

Cost Data

Jan 2024 - Jan 2025 (MTD) | Unblended costs



Actual cost Budget Alert #1 (actual)

[View in AWS Cost Explorer](#)

Alerts

▶ Actual cost > 80% | No actions

Step 7: The alert is set successfully. And click on next.

- Step 1 Choose budget type
- Step 2 Set your budget
- Step 3 Configure alerts
- Step 4 - Optional Attach actions
- Step 5 Review

Attach actions - Optional [info](#)

Using budgets actions



What is a budget action?

A budget action allows you to define and trigger cost saving responses to reinforce a cost-conscious culture. You have the option to attach actions that run whenever your alert threshold has been exceeded, such as stopping an EC2 instance from incurring any further costs. You can select the alerts to which you would like to attach actions, then define these actions.



How to get started?

To create a budget action, you will first need an alert threshold created from step 2. If you have already created an alert threshold select the type of action you want.

Alert #1 (0 actions attached)

Threshold
80%
Threshold measured against
Actual Costs

Email recipients
meghakundu85@gmail.com
Amazon SNS
Not configured

[Add action](#)

[Cancel](#)

[Previous](#)

[Next](#)

Cost Data

Jan 2024 - Jan 2025 (MTD) | Unblended costs



Actual cost Budget Alert #1 (actual)

[View in AWS Cost Explorer](#)

Alerts

Actual cost > 80% | No actions

Step 8: Review the budget details. After double checking all configuration, if everything is accurate, click on 'Create Budget'

- Step 1 Choose budget type
- Step 2 Set your budget
- Step 3 Configure alerts
- Step 4 - Optional Attach actions
- Step 5 Review

Review [info](#)

Step 1: Choose budget type

[Edit](#)

Budget type

Cost budget

Monitor your costs against a specified dollar amount and receive alerts when your user-defined thresholds are met.

Step 2: Set up your budget

[Edit](#)

Budget details

Name
MP_Budget
Period
Monthly

Start date
Jan 2025
End date
-

Budget amount
\$2.00

Additional budget parameters

Tags

Key Value

There are no tags associated with this resource.

Step 3: Configure alerts

[Edit](#)

Alerts

Alert #1

Threshold
80% of budgeted amount
Threshold measured against
Actual costs

Step 4: Attach actions - optional

[Edit](#)

Actions

You have no budgets actions

[Cancel](#)

[Previous](#)

[Create budget](#)

Step 9: Budget is created successfully.

✓ Your budget MP_Budget has been created successfully.

[Submit feedback](#) ✕

Budgets (1) [info](#)

[Download CSV](#)

[Actions](#)

[Create budget](#)

Find a budget

Type - Show all budgets

< 1 > ⓘ

<input type="checkbox"/>	Name	▲	Thresholds ▼	Budget	Amount used	Forecasted amount	Current vs. budgeted ▼	Forecasted vs. budgeted ▼
<input type="checkbox"/>	MP_Budget		OK		\$2.00	\$0.00	-	0.00% -